II

(Acte fără caracter legislativ)

REGULAMENTE

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2016/799 AL COMISIEI

din 18 martie 2016

de punere în aplicare a Regulamentului (UE) nr. 165/2014 al Parlamentului European și al Consiliului de stabilire a cerințelor pentru construirea, testarea, instalarea, operarea și repararea tahografelor și a componentelor acestora

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) nr. 165/2014 al Parlamentului European și al Consiliului din 4 februarie 2014 privind tahografele în transportul rutier ([1]), în special articolul 11 și articolul 12 alineatul (7),

întrucât:

(1) Regulamentul (UE) nr. 165/2014 a introdus tahografele digitale de a doua generație, numite tahografe inteligente, care includ o legătură cu sistemul global de navigație prin satelit (GNSS), un echipament de comunicare în scopul detectării timpurii la distanță și o interfață cu sistemele de transport inteligente. Ar trebui să fie stabilite specificațiile pentru cerințele tehnice privind construcția tahografelor inteligente.

(2) Echipamentul de detectare timpurie la distanță introdus prin articolul 9 alineatul (4) din Regulamentul (UE) nr. 165/2014 ar trebui să transmită unui agent de control în trafic datele din tahograful digital și informațiile referitoare la masele și la masa pe axe ale vehiculului complet (autotractor și remorci sau semiremorci), în conformitate cu Directiva 96/53/CE a Parlamentului European și a Consiliului ([2]). Aceasta ar trebui să permită un control eficace și rapid al vehiculelor de către autoritățile de control, cu mai puține dispozitive electronice în cabina vehiculului.

(3) În conformitate cu Directiva 96/53/CE, echipamentul de detectare timpurie la distanță ar trebui să utilizeze standardele CEN DSRC ([3]) menționate în directiva respectivă, în banda de frecvențe de la 5 795 la 5 805 MHz. Deoarece această bandă de frecvențe este utilizată și pentru taxarea rutieră electronică, pentru a evita interferențele dintre aplicațiile de taxare rutieră și cele de control, agenții de control ar trebui să nu utilizeze echipamentul de detectare timpurie la o stație de taxare rutieră.

(4) Odată cu tahograful inteligent, ar trebui introduse noi mecanisme de securitate pentru menținerea nivelului de securitate al tahografului digital, pentru a aborda aspectele vulnerabile actuale în materie de securitate. Unul dintre aceste aspecte vulnerabile este absența datelor de expirare a certificatelor digitale. Pentru a asigura conformitatea cu cele mai bune practici în materie de securitate, se recomandă evitarea utilizării certificatelor digitale fără date de expirare. Perioada de valabilitate în condiții normale de funcționare a unităților montate pe vehicule ar trebui să fie de 15 ani de la data eliberării certificatelor digitale pentru unitățile montate pe vehicul. Unitățile montate pe vehicule ar trebui să fie înlocuite după expirarea perioadei de valabilitate menționate.

([1]) JO L 60, 28.2.2014, p. 1.

([2]) Directiva 96/53/CE a Consiliului din 25 iulie 1996 de stabilire, pentru anumite vehicule rutiere care circulă în interiorul Comunității, a dimensiunilor maxime autorizate în traficul național și internațional și a greutății maxime autorizate în traficul internațional (JO L 235, 17.9.1996, p. 59).

([3]) Standardele privind comunicațiile specializate cu rază scurtă de acțiune (*Dedicated Short Range Communications*) ale Comitetului European de Standardizare (CEN) EN 12253, EN 12795, EN 12834, EN 13372 și ISO 14906.

(5) Furnizarea de informații de poziționare securizate și fiabile reprezintă un element esențial al funcționării eficace a tahografelor inteligente. Prin urmare, este oportun să se asigure compatibilitatea acestora cu serviciile cu valoare adăugată furnizate de programul Galileo, astfel cum este prevăzut în Regulamentul (UE) nr. 1285/2013 al Parlamentului European și al Consiliului ([1]), în scopul îmbunătățirii securității tahografului inteligent.

(6) În conformitate cu articolul 8 alineatul (1), articolul 9 alineatul (1) și articolul 10 alineatele (1) și (2) din Regulamentul (UE) nr. 165/2014, mecanismele de securitate introduse de regulamentul menționat ar trebui să se aplice la 36 de luni de la data intrării în vigoare a actelor de punere în aplicare necesare, pentru a permite producătorilor să dezvolte noua generație de tahografe inteligente și să obțină certificatele de omologare de tip aferente de la autoritățile competente.

(7) În conformitate cu Regulamentul (UE) nr. 165/2014, vehiculele înmatriculate pentru prima dată într-un stat membru la 36 de luni de la intrarea în vigoare a prezentului regulament al Comisiei ar trebui să fie echipate cu un tahograf inteligent care respectă cerințele prezentului regulament al Comisiei. În orice caz, toate vehiculele care circulă într-un stat membru diferit de statul lor membru de înmatriculare ar trebui să fie echipate cu un tahograf inteligent conform la 15 ani de la data aplicării acestor cerințe.

(8) Regulamentul (CE) nr. 68/2009 al Comisiei ([2]) a permis, în cursul unei perioade de tranziție care expiră la 31 decembrie 2013, utilizarea unui adaptor pentru a face posibilă instalarea tahografelor în vehiculele de tip M1 și N1. Din cauza dificultăților tehnice legate de găsirea unei alternative la utilizarea unui adaptor, experții din industria automobilelor și din industria tahografelor, împreună cu Comisia, au concluzionat că nu există o soluție alternativă la adaptor care să nu presupună costuri ridicate pentru industrie, disproporționate față de dimensiunea pieței. Prin urmare, utilizarea unui adaptor în cazul vehiculelor de tip M1 și N1 ar trebui să fie permisă pe o perioadă nedeterminată.

(9) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul comitetului menționat la articolul 42 alineatul (3) din Regulamentul (UE) nr. 165/2014,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Obiect și domeniu de aplicare

(1) Prezentul regulament stabilește dispozițiile necesare pentru aplicarea uniformă a următoarelor aspecte referitoare la tahografe:

(a) înregistrarea poziției vehiculului în anumite puncte în timpul zilei de lucru a conducătorului auto;

(b) detectarea timpurie la distanță a posibilelor manipulări sau utilizări abuzive ale tahografelor inteligente;

(c) interfața cu sistemele de transport inteligente;

(d) cerințele administrative și tehnice pentru procedurile de omologare de tip a tahografelor, inclusiv a mecanismelor de securitate.

(2) Construirea, testarea, instalarea, inspectarea, operarea și repararea tahografelor inteligente și a componentelor acestora trebuie să respecte cerințele tehnice stabilite în anexa 1C la prezentul regulament.

(3) Celelalte tahografe, în afara tahografelor inteligente, trebuie să respecte în continuare, în ceea ce privește construirea, testarea, instalarea, inspectarea, operarea și repararea, cerințele din anexa 1 sau din anexa 1B la Regulamentul (CEE) nr. 3821/85 al Consiliului ([3]), după caz.

([1]) Regulamentul (UE) nr. 1285/2013 al Parlamentului European și al Consiliului din 11 decembrie 2013 privind punerea în aplicare și exploatarea sistemelor europene de radionavigație prin satelit și de abrogare a Regulamentului (CE) nr. 876/2002 al Consiliului și a Regulamentului (CE) nr. 683/2008 al Parlamentului European și al Consiliului (JO L 347, 20.12.2013, p. 1).

([2]) Regulamentul (CE) nr. 68/2009 al Comisiei din 23 ianuarie 2009 de adaptare pentru a noua oară la progresul tehnic a Regulamentului (CEE) nr. 3821/85 al Consiliului privind aparatura de înregistrare în transportul rutier (JO L 21, 24.1.2009, p. 3).

([3]) Regulamentul (CEE) nr. 3821/85 al Consiliului din 20 decembrie 1985 privind aparatura de înregistrare în transportul rutier (JO L 370, 31.12.1985, p. 8).

(4) În temeiul articolului 10d din Directiva 96/53/CE, echipamentul de detectare timpurie la distanță trebuie să transmită, de asemenea, datele referitoare la greutate furnizate de un sistem intern de cântărire la bord, în scopul detectării timpurii a fraudelor.

Articolul 2

Definiții

În scopul prezentului regulament, se aplică definițiile prevăzute la articolul 2 din Regulamentul (UE) nr. 165/2014.

În plus, se aplică următoarele definiții:

1. „tahograf digital" sau „tahograf de primă generație" înseamnă un tahograf digital care nu este un tahograf inteligent;

2. „echipament GNSS extern" înseamnă un echipament care conține receptorul GNSS atunci când unitatea montată pe vehicul nu este o unitate compactă, precum și alte componente necesare pentru protecția comunicării datelor de poziționare către restul unității montate pe vehicul;

3. „dosar informativ" înseamnă dosarul complet, în format electronic sau pe hârtie, care conține toate informațiile furnizate de producător sau de agentul său autorității de omologare de tip în scopul omologării de tip a unui tahograf sau a unei componente a acestuia, inclusiv certificatele menționate la articolul 12 alineatul (3) din Regulamentul (UE) nr. 165/2014, rezultatele testelor definite în anexa 1C la prezentul regulament, precum și schițe, fotografii și alte documente relevante;

4. „dosar de omologare" înseamnă dosarul informativ, în format electronic sau pe hârtie, însoțit de orice alte documente adăugate de autoritatea de omologare de tip la dosarul informativ în cursul exercitării funcțiilor sale, inclusiv, la sfârșitul procesului de omologare de tip, certificatul de omologare CE de tip a tahografului sau a unei componente a acestuia;

5. „opisul dosarului de omologare" înseamnă documentul care enumeră conținutul numerotat al dosarului de omologare, care identifică toate părțile relevante din acest dosar. Formatul acestui document evidențiază etapele succesive ale procesului de omologare CE de tip și include datele de revizuire și de actualizare a dosarului respectiv;

6. „echipament de detectare timpurie la distanță" înseamnă aparatura unității montate pe vehicul care este folosită pentru efectuarea de controale selective în trafic;

7. „tahograf inteligent" sau „tahograf de a doua generație" înseamnă un tahograf digital care este în conformitate cu articolele 8, 9 și 10 din Regulamentul (UE) nr. 165/2014, precum și cu anexa 1C la prezentul regulament;

8. „componentă a tahografului" sau „componentă" înseamnă oricare dintre următoarele elemente: unitatea montată pe vehicul, senzorul de mișcare, cardul de tahograf, foaia de înregistrare, echipamentul GNSS extern și echipamentul de detectare timpurie la distanță;

9. „autoritate de omologare de tip" înseamnă autoritatea unui stat membru care are competența de a efectua omologarea de tip a tahografului sau a componentelor sale și de a desfășura procesul de autorizare, precum și de a elibera și, dacă este cazul, de a retrage certificatele de omologare de tip, care acționează ca punct de contact cu autoritățile de omologare de tip ale altor state membre și care garantează că producătorii își îndeplinesc obligațiile în ceea ce privește conformitatea cu cerințele prezentului regulament.

Articolul 3

Servicii bazate pe localizare

(1) Producătorii trebuie să se asigure că tahografele inteligente sunt compatibile cu serviciile de poziționare furnizate de sistemele Galileo și Serviciul european geostaționar mixt de navigare (EGNOS).

(2) Pe lângă sistemele menționate la alineatul (1), producătorii pot alege, de asemenea, să asigure compatibilitatea cu alte sisteme de navigație prin satelit.

Articolul 4

Procedura de omologare de tip a unui tahograf și a componentelor tahografului

(1) Un producător sau agentul său trebuie să depună o cerere pentru omologarea de tip a unui tahograf, a oricăreia dintre componentele acestuia sau a oricărui grup de componente, la autoritățile de omologare de tip desemnate de fiecare stat membru. Cererea constă într-un dosar informativ care conține informațiile referitoare la fiecare dintre componentele vizate, inclusiv, acolo unde este cazul, certificatele de omologare de tip ale celorlalte componente necesare pentru a completa tahograful, precum și orice alte documente relevante.

(2) Un stat membru acordă omologarea de tip pentru orice tahograf, componentă sau grup de componente care respectă cerințele administrative și tehnice menționate la articolul 1 alineatul (2) sau (3), după caz. În acest caz, autoritatea de omologare de tip eliberează solicitantului un certificat de omologare de tip care respectă modelul stabilit în anexa II la prezentul regulament.

(3) Autoritatea de omologare de tip poate solicita producătorului sau agentului acestuia să furnizeze orice informații suplimentare.

(4) Producătorul sau agentul său pune la dispoziția autorităților de omologare de tip, precum și a entităților responsabile cu eliberarea certificatelor menționate la articolul 12 alineatul (3) din Regulamentul (UE) nr. 165/2014, numărul de tahografe sau de componente de tahograf care este necesar pentru a permite ca procedura de omologare de tip să se desfășoare în mod satisfăcător.

(5) În cazul în care producătorul sau agentul său dorește să obțină o omologare de tip a anumitor componente sau grupuri de componente ale unui tahograf, acesta furnizează autorităților de omologare de tip celelalte componente deja omologate de tip, precum și alte piese necesare pentru construirea tahografului complet, pentru a permite autorităților respective să efectueze testele necesare.

Articolul 5

Modificarea omologărilor de tip

(1) Producătorul sau agentul său informează fără întârziere autoritățile de omologare de tip care au acordat omologarea de tip inițială, în legătură cu orice modificare a software-ului sau a hardware-ului tahografului sau a naturii materialelor utilizate la fabricarea acestuia care sunt înregistrate în dosarul de omologare, și depune o cerere de modificare a omologării de tip.

(2) Autoritățile de omologare de tip pot revizui sau extinde o omologare de tip existentă, sau pot acorda o nouă omologare de tip în funcție de natura și de caracteristicile modificărilor.

În cazul în care autoritatea de omologare de tip consideră că modificările software-ului, ale hardware-ului tahografului sau ale naturii materialelor utilizate la fabricarea acestuia sunt minore, are loc o „revizuire". În astfel de cazuri, autoritatea de omologare de tip eliberează documentele revizuite din dosarul de omologare, indicând natura modificărilor realizate și data aprobării lor. O versiune actualizată a dosarului de omologare într-o formă consolidată, însoțită de o descriere detaliată a modificărilor aduse, este suficientă pentru a îndeplini această cerință.

În cazul în care autoritatea de omologare de tip consideră că modificările software-ului, ale hardware-ului tahografului sau ale naturii materialelor utilizate la fabricarea acestuia sunt substanțiale, are loc o „extindere". În astfel de cazuri, autoritatea de omologare de tip poate solicita să se efectueze noi teste și informează în mod corespunzător producătorul sau agentul acestuia. Dacă aceste teste sunt satisfăcătoare, autoritatea de omologare de tip eliberează un certificat de omologare de tip ce conține un număr care se referă la extinderea acordată. Certificatul de omologare de tip precizează motivul extinderii și data eliberării.

(3) În opisul dosarului de omologare se indică data celei mai recente extinderi sau revizuiri a omologării de tip sau data celei mai recente consolidări a versiunii actualizate a omologării de tip.

(4) Este necesară o nouă omologare de tip atunci când modificările aduse tahografului omologat de tip sau componentelor sale omologate de tip ar conduce la eliberarea unui nou certificat de securitate sau a unui nou certificat de interoperabilitate.

Articolul 6

Intrare în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Se aplică de la 2 martie 2016.

Cu toate acestea, anexele se aplică de la 2 martie 2019, cu excepția apendicelui 16, care se aplică de la 2 martie 2016.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 18 martie 2016.

Pentru Comisie

Președintele

Jean-Claude JUNCKER

ANEXA I C

Cerințe privind construcția, testarea, instalarea și inspecția

INTRODUCERE		12
1.	DEFINIȚII	13
2.	CARACTERISTICI ȘI FUNCȚII GENERALE ALE APARATURII DE ÎNREGISTRARE	19
2.1	Caracteristici generale	19
2.2	Funcții	20
2.3	Moduri de funcționare	21
2.4	Securitate	22
3.	CERINȚE DE CONSTRUCȚIE ȘI DE FUNCȚIONARE APLICABILE APARATURII DE ÎNREGISTRARE	22
3.1	Monitorizarea introducerii și retragerii cardurilor	22
3.2	Măsurarea vitezei, a poziției și a distanței	23
3.2.1	Măsurarea distanței parcurse	23
3.2.2	Măsurarea vitezei	23
3.2.3	Măsurarea poziției	24
3.3	Măsurarea timpului	24
3.4	Monitorizarea activităților conducătorului auto	24
3.5	Monitorizarea regimului de conducere	25
3.6	Înregistrări realizate de conducătorii auto	25
3.6.1	Înregistrarea locurilor în care încep și/sau se încheie zilele de lucru	25
3.6.2	Introducerea manuală a activităților conducătorului auto și acordul conducătorului auto pentru interfața ITS	25
3.6.3	Înregistrarea condițiilor specifice	27
3.7	Gestionarea blocărilor efectuate de societate	27
3.8	Monitorizarea activităților de control	28
3.9	Detectarea evenimentelor și/sau a anomaliilor	28
3.9.1	Evenimentul „Introducerea unui card nevalabil”	28
3.9.2	Evenimentul „Conflict de carduri”	28
3.9.3	Evenimentul „Suprapunere a timpului”	28
3.9.4	Evenimentul „Conducere fără un card adecvat”	29
3.9.5	Evenimentul „Introducerea cardului în timpul conducerii”	29
3.9.6	Evenimentul „Încheierea incorectă a ultimei sesiuni”	29
3.9.7	Evenimentul „Depășirea limitei de viteză”	29
3.9.8	Evenimentul „Întreruperea alimentării cu energie electrică”	29
3.9.9	Evenimentul „Eroare de comunicare cu echipamentul de comunicare la distanță”	29
3.9.10	Evenimentul „Absența informațiilor de poziționare de la receptorul GNSS”	29

3.9.11 Evenimentul „Eroare de comunicare cu echipamentul GNSS extern” 30

3.9.12 Evenimentul „Eroare privind datele de la senzorul de mișcare” 30

3.9.13 Evenimentul „Conflict privind deplasarea vehiculului” 30

3.9.14 Evenimentul „Tentativă de încălcare a securității” 30

3.9.15 Evenimentul „Conflict oră” 30

3.9.16 Anomalia „Card” 30

3.9.17 Anomalia „Aparatura de înregistrare” 30

3.10 Teste integrate și autoteste 31

3.11 Citirea din memoria de date 31

3.12 Înregistrarea și stocarea în memoria de date 31

3.12.1 Date de identificare a aparaturii 32

3.12.1.1 Date de identificare a unității montate pe vehicul 32

3.12.1.2 Date de identificare a senzorului de mișcare 32

3.12.1.3 Date de identificare a sistemului global de navigație prin satelit 33

3.12.2 Chei și certificate 33

3.12.3 Date privind introducerea și retragerea cardului de conducător auto sau ale cardului de atelier 33

3.12.4 Date privind activitatea conducătorului auto 34

3.12.5 Locuri și poziții în care încep și se încheie zilele de lucru și/sau în care se atinge timpul de conducere continuă de 3 ore 34

3.12.6 Date privind odometrul 35

3.12.7 Date privind viteza detaliată 35

3.12.8 Date privind evenimentele 35

3.12.9 Date privind anomaliile 37

3.12.10 Date privind etalonarea 38

3.12.11 Date privind reglarea orei 39

3.12.12 Date privind activitățile de control 39

3.12.13 Date privind blocările efectuate de societate 39

3.12.14 Date privind activitățile de descărcare 39

3.12.15 Date privind condițiile specifice 40

3.12.16 Date privind cardul de tahograf 40

3.13 Citirea de pe cardurile de tahograf 40

3.14 Înregistrarea și stocarea pe cardurile de tahograf 40

3.14.1 Înregistrarea și stocarea pe cardurile de tahograf de primă generație; 40

3.14.2 Înregistrarea și stocarea pe cardurile de tahograf de a doua generație 41

3.15 Afișare 41

3.15.1 Afișaj implicit 42

3.15.2	Afișaj de avertizare	43
3.15.3	Accesul la meniu	43
3.15.4	Alte afișaje	43
3.16	Imprimare	43
3.17	Avertismente	44
3.18	Descărcarea datelor pe suporturi externe	45
3.19	Comunicare la distanță pentru controalele selective în trafic	45
3.20	Date de ieșire transmise unor dispozitive externe suplimentare	46
3.21	Etalonare	47
3.22	Verificarea etalonării în trafic	47
3.23	Reglarea orei	48
3.24	Caracteristici de performanță	48
3.25	Materiale	48
3.26	Inscripții	49
4.	CERINȚE FUNCȚIONALE ȘI DE CONSTRUCȚIE PENTRU CARDURILE DE TAHOGRAF	49
4.1	Date vizibile	49
4.2	Securitate	52
4.3	Standarde	53
4.4	Specificații de mediu și electrice	53
4.5	Stocarea datelor	53
4.5.1	Fișierele elementare pentru identificare și pentru gestionarea cardului	54
4.5.2	Identificarea cardurilor cu circuite integrate (IC)	54
4.5.2.1	Identificarea cipului	54
4.5.2.2	DIR (prezent numai pe cardurile de tahograf de a doua generație)	54
4.5.2.3	Informații RLR (în anumite condiții, prezente numai pe cardurile de tahograf de a doua generație)	54
4.5.2.4	Informații privind lungimea extinsă (în anumite condiții, prezente numai pe cardurile de tahograf de a doua generație)	55
4.5.3	Cardul de conducător auto	55
4.5.3.1	Aplicație pentru tahograf (accesibilă pentru unitățile montate pe vehicul de prima și a doua generație)	55
4.5.3.1.1	Identificarea aplicației	55
4.5.3.1.2	Chei și certificate	55
4.5.3.1.3	Identificarea cardului	55
4.5.3.1.4	Identificarea titularului cardului	55
4.5.3.1.5	Descărcarea informațiilor de pe card	55
4.5.3.1.6	Informații privind permisul de conducere	55
4.5.3.1.7	Date privind evenimentele	56

4.5.3.1.8 Date privind anomaliile 56

4.5.3.1.9 Date privind activitatea conducătorului auto 57

4.5.3.1.10 Date privind vehiculele utilizate 57

4.5.3.1.11 Locurile în care încep și/sau se încheie zilele de lucru 58

4.5.3.1.12 Date privind sesiunile de utilizare a cardului 58

4.5.3.1.13 Date privind activitățile de control 58

4.5.3.1.14 Date privind condițiile specifice 58

4.5.3.2 Aplicație pentru tahograf de a 2-a generație (inaccesibilă unităților montate pe vehicul de primă generație) 59

4.5.3.2.1 Identificarea aplicației 59

4.5.3.2.2 Chei și certificate 59

4.5.3.2.3 Identificarea cardului 59

4.5.3.2.4 Identificarea titularului cardului 59

4.5.3.2.5 Descărcarea informațiilor de pe card 59

4.5.3.2.6 Informații privind permisul de conducere 59

4.5.3.2.7 Date privind evenimentele 59

4.5.3.2.8 Date privind anomaliile 60

4.5.3.2.9 Date privind activitatea conducătorului auto 61

4.5.3.2.10 Date privind vehiculele folosite 61

4.5.3.2.11 Locurile și pozițiile în care încep și/sau se încheie zilele de lucru 62

4.5.3.2.12 Date privind sesiunile de utilizare a cardului 62

4.5.3.2.13 Date privind activitățile de control 62

4.5.3.2.14 Date privind condițiile specifice 63

4.5.3.2.15 Date privind unitățile montate pe vehicul utilizate 63

4.5.3.2.16 Date privind locurile în care se încheie o perioadă de conducere continuă de trei ore 63

4.5.4 Cardul de atelier 63

4.5.4.1 Aplicație pentru tahograf (accesibilă pentru unitățile montate pe vehicul de prima și a doua generație) 63

4.5.4.1.1 Identificarea aplicației 63

4.5.4.1.2 Chei și certificate 63

4.5.4.1.3 Identificarea cardului 64

4.5.4.1.4 Identificarea titularului cardului 64

4.5.4.1.5 Descărcarea informațiilor de pe card 64

4.5.4.1.6 Date privind etalonarea și reglarea orei 64

4.5.4.1.7 Date privind evenimentele și anomaliile 65

4.5.4.1.8 Date privind activitatea conducătorului auto 65

4.5.4.1.9 Date privind vehiculele utilizate 65

4.5.4.1.10 Date privind începutul și/sau sfârșitul zilelor de lucru 65

4.5.4.1.11 Date privind sesiunile de utilizare a cardului 65

4.5.4.1.12 Date privind activitățile de control 65

4.5.4.1.13 Date privind condițiile specifice 65

4.5.4.2 Aplicația pentru tahograf de a 2-a generație (inaccesibilă unităților montate pe vehicul de primă generație) 65

4.5.4.2.1 Identificarea aplicației 65

4.5.4.2.2 Chei și certificate 66

4.5.4.2.3 Identificarea cardului 66

4.5.4.2.4 Identificarea titularului cardului 66

4.5.4.2.5 Descărcarea informațiilor de pe card 66

4.5.4.2.6 Date privind etalonarea și reglarea orei 66

4.5.4.2.7 Date privind evenimentele și anomaliile 67

4.5.4.2.8 Date privind activitatea conducătorului auto 67

4.5.4.2.9 Date privind vehiculele utilizate 67

4.5.4.2.10 Date privind începutul și/sau sfârșitul zilelor de lucru 67

4.5.4.2.11 Date privind sesiunile de utilizare a cardului 67

4.5.4.2.12 Date privind activitățile de control 67

4.5.4.2.13 Date privind unitățile montate pe vehicul utilizate 67

4.5.4.2.14 Date privind locurile în care se încheie o perioadă de conducere continuă de trei ore 68

4.5.4.2.15 Date privind condițiile specifice 68

4.5.5 Cardul de control 68

4.5.5.1 Aplicație pentru tahograf (accesibilă pentru unitățile montate pe vehicul de prima și a doua generație) 68

4.5.5.1.1 Identificarea aplicației 68

4.5.5.1.2 Chei și certificate 68

4.5.5.1.3 Identificarea cardului 68

4.5.5.1.4 Identificarea titularului cardului 68

4.5.5.1.5 Date privind activitățile de control 69

4.5.5.2 Aplicația pentru tahograf G2 (inaccesibilă unităților montate pe vehicul de primă generație) 69

4.5.5.2.1 Identificarea aplicației 69

4.5.5.2.2 Chei și certificate 69

4.5.5.2.3	Identificarea cardului	69
4.5.5.2.4	Identificarea titularului cardului	69
4.5.5.2.5	Date privind activitățile de control	70
4.5.6	Card de societate	70
4.5.6.1	Aplicație pentru tahograf (accesibilă pentru unitățile montate pe vehicul de prima și a doua generație)	70
4.5.6.1.1	Identificarea aplicației	70
4.5.6.1.2	Chei și certificate	70
4.5.6.1.3	Identificarea cardului	70
4.5.6.1.4	Identificarea titularului cardului	70
4.5.6.1.5	Date privind activitatea societății	70
4.5.6.2	Aplicația pentru tahograf G2 (inaccesibilă unităților montate pe vehicul de primă generație)	71
4.5.6.2.1	Identificarea aplicației	71
4.5.6.2.2	Chei și certificate	71
4.5.6.2.3	Identificarea cardului	71
4.5.6.2.4	Identificarea titularului cardului	71
4.5.6.2.5	Date privind activitatea societății	71
5.	INSTALAREA APARATURII DE ÎNREGISTRARE	72
5.1	Instalare	72
5.2	Plăcuța de instalare	73
5.3	Sigilarea	74
6.	CONTROALE, INSPECȚII ȘI REPARAȚII	74
6.1	Aprobarea montatorilor, a atelierelor și a producătorilor de vehicule	74
6.2	Verificarea instrumentelor noi și a celor reparate	75
6.3	Inspecția instalației	75
6.4	Inspecții periodice	75
6.5	Măsurarea erorilor	76
6.6	Reparații	76
7.	EMITEREA CARDURILOR	76
8.	OMOLOGAREA DE TIP A APARATURII DE ÎNREGISTRARE ȘI A CARDURILOR DE TAHOGRAF	77
8.1	Generalități	77
8.2	Certificatul de securitate	78
8.3	Certificatul de funcționare	78
8.4	Certificatul de interoperabilitate	78
8.5	Certificatul de omologare de tip	79
8.6	Procedură extraordinară: primele certificate de interoperabilitate pentru aparatura de înregistrare și cardurile de tahograf de a 2-a generație	80

INTRODUCERE

Sistemul tahografic digital de primă generație este în vigoare de la 1 mai 2006. Acesta poate fi utilizat până la finalul ciclului său de viață pentru transportul intern. În schimb, pentru transportul internațional, după 15 ani de la intrarea în vigoare a prezentului regulament al Comisiei, toate vehiculele trebuie să fie echipate cu un tahograf inteligent conform de a doua generație, introdus prin prezentul regulament.

Prezenta anexă conține cerințe privind aparatura de înregistrare și cardurile de tahograf de a doua generație. Începând de la data introducerii, se instalează aparatura de înregistrare de a doua generație pe vehiculele înmatriculate pentru prima dată și se emit carduri de tahograf de a doua generație.

Pentru a favoriza o introducere fără probleme a sistemului tahografic de a doua generație,

— cardurile de tahograf de a doua generație trebuie concepute astfel încât să poată fi utilizate și în unitățile montate pe vehicule de primă generație;

— nu este obligatorie înlocuirea cardurilor de tahograf de primă generație valabile la data introducerii.

Acest lucru le va permite conducătorilor auto să își păstreze cardul unic de conducător auto și să îl folosească pentru ambele sisteme.

Cu toate acestea, aparatura de înregistrare de a doua generație se etalonează numai utilizând carduri de atelier de a doua generație.

Prezenta anexă conține toate cerințele referitoare la interoperabilitatea dintre sistemele tahografice de prima și de a doua generație.

Apendicele 15 conține detalii suplimentare privind modul de gestionare a coexistenței celor două sisteme.

Lista apendicelor

Apendicele 1: DICȚIONAR DE DATE

Apendicele 2: SPECIFICAȚIE PRIVIND CARDURILE DE TAHOGRAF

Apendicele 3: PICTOGRAME

Apendicele 4: DOCUMENTE IMPRIMATE

Apendicele 5: AFIȘAJUL

Apendicele 6: CONECTOR FRONTAL PENTRU ETALONARE ȘI DESCĂRCARE

Apendicele 7: PROTOCOALE DE DESCĂRCARE A DATELOR

Apendicele 8: PROTOCOL DE ETALONARE

Apendicele 9: OMOLOGAREA DE TIP ȘI LISTA TESTELOR MINIME OBLIGATORII

Apendicele 10: CERINȚE DE SECURITATE

Apendicele 11: MECANISME DE SECURITATE COMUNE

Apendicele 12: POZIȚIONAREA BAZATĂ PE SISTEMUL GLOBAL DE NAVIGAȚIE PRIN SATELIT (GNSS)

Apendicele 13: INTERFAȚA ITS

Apendicele 14: FUNCȚIA DE COMUNICARE LA DISTANȚĂ

Apendicele 15: MIGRAȚIE: GESTIONAREA COEXISTENȚEI MAI MULTOR GENERAȚII DE ECHIPAMENTE

Apendicele 16: ADAPTOR PENTRU VEHICULELE DIN CATEGORIILE M1 ȘI N1

1. DEFINIȚII

În prezenta anexă:

(a) „activare” înseamnă:

etapa în care tahograful devine complet operațional și asigură toate funcțiile, inclusiv funcțiile de securitate, prin utilizarea unui card de atelier;

(b) „autentificare” înseamnă:

o funcție destinată stabilirii și verificării unei identități declarate;

(c) „autenticitate” înseamnă:

faptul că informațiile provin de la o sursă a cărei identitate poate fi verificată;

(d) „test integrat (BIT)” înseamnă:

un test executat la comandă, declanșat de operator sau de dispozitive externe;

(e) „zi calendaristică” înseamnă:

o zi cuprinsă între ora 00.00 și ora 24.00. Toate zilele calendaristice se raportează la ora UTC (ora universală coordonată);

(f) „etalonarea” unui tahograf inteligent înseamnă:

actualizarea sau confirmarea parametrilor vehiculului care urmează să fie stocați în memoria de date. Parametrii vehiculului includ identificarea vehiculului (VIN, VRN și statul membru de înmatriculare) și caracteristicile vehiculului [w, k, l, dimensiunea pneurilor, reglajele limitatorului de viteză (dacă este cazul), ora UTC din momentul respectiv, valoarea înregistrată de odometru în momentul respectiv]; în cursul etalonării unei aparaturi de înregistrare, tipurile și identificatorii tuturor sigiliilor relevante de omologare de tip montate se stochează, de asemenea, în memoria de date;

orice actualizare sau confirmare exclusiv a orei UTC este considerată o reglare a orei și nu o etalonare, cu condiția ca aceasta să nu contravină cerinței 409;

pentru etalonarea unei aparaturi de înregistrare trebuie folosit un card de atelier;

(g) „numărul cardului” înseamnă:

un cod format din 16 caractere alfanumerice, care reprezintă numărul unic de identificare al unui card de tahograf într-un stat membru. Numărul cardului conține un indice secvențial al cardului (dacă este cazul), un indice de înlocuire a cardului și un indice de reînnoire a cardului;

prin urmare, un card poate fi identificat exclusiv pe baza codului statului membru emitent și a numărului cardului;

(h) „indice secvențial al cardului” înseamnă:

al 14-lea caracter alfanumeric din numărul unui card, folosit pentru a deosebi diferitele carduri emise unei societăți, unui atelier sau unei autorități de control care au dreptul de a li se emite mai multe carduri de tahograf. Societatea, atelierul sau autoritatea de control sunt identificate în mod unic pe baza primelor 13 caractere ale numărului cardului;

(i) „indice de reînnoire a cardului” înseamnă:

al 16-lea caracter alfanumeric din numărul unui card, care este incrementat la fiecare reînnoire a cardului de tahograf;

(j) „indice de înlocuire a cardului” înseamnă:

al 15-lea caracter alfanumeric din numărul unui card, care este incrementat la fiecare înlocuire a cardului de tahograf;

(k) „coeficient caracteristic al vehiculului" înseamnă:

caracteristica numerică ce indică valoarea semnalului de ieșire emis de acel element al vehiculului care face legătura dintre acesta și aparatura de înregistrare (axul sau cilindrul de ieșire al cutiei de viteze), în timp ce vehiculul parcurge o distanță de un kilometru măsurată în condiții normale de testare, astfel cum sunt definite la cerința 414. Coeficientul caracteristic este exprimat în impulsuri pe kilometru (w = … imp/km);

(l) „card de societate" înseamnă:

un card de tahograf emis de autoritățile unui stat membru unei întreprinderi de transport obligată să utilizeze vehicule echipate cu un tahograf, care identifică întreprinderea de transport și permite afișarea, descărcarea și imprimarea datelor, stocate în tahograf, care au fost blocate de respectiva întreprindere de transport;

(m) „constanta aparaturii de înregistrare" înseamnă:

caracteristica numerică reprezentând valoarea semnalului de intrare necesar pentru a indica și a înregistra o distanță de un kilometru parcursă; această constantă este exprimată în impulsuri pe kilometru (k = … imp/km);

(n) „timpul de conducere continuă" este calculat de aparatura de înregistrare astfel ([1]):

timpul de conducere continuă se calculează ca fiind timpii de conducere acumulați la un moment dat de un anumit conducător auto după încheierea ultimei sale perioade de minimum 45 de minute de DISPONIBILITATE sau de PAUZĂ/ODIHNĂ sau NECUNOSCUTĂ ([2]) [este posibil ca această perioadă să fi fost împărțită în conformitate cu Regulamentul (CE) nr. 561/2006 al Parlamentului European și al Consiliului ([3])]. Pentru calculele care trebuie efectuate se iau în considerare, după cum este necesar, activitățile anterioare stocate pe cardul de conducător auto. În cazul în care conducătorul auto nu și-a introdus cardul, calculele necesare se bazează pe înregistrările din memoria de date pentru perioada în curs în care niciun card nu a fost introdus și legate de slotul relevant;

(o) „card de control" înseamnă:

un card de tahograf emis de autoritățile unui stat membru autorității naționale de control competente, care identifică organismul de control și, opțional, agentul de control și care permite accesul la datele stocate în memoria de date sau pe cardul de conducător auto și, opțional, pe cardul de atelier în vederea citirii, a imprimării și/sau a descărcării acestora;

Acest card permite, de asemenea, accesul la funcția de verificare a etalonării în trafic și la datele din cititorul pentru comunicarea în scopul detectării timpurii la distanță.

(p) „durata cumulată a pauzelor" este calculată de aparatura de înregistrare astfel ([1]):

durata cumulată a pauzelor care întrerup timpul de conducere se calculează ca fiind perioadele de DISPONIBILITATE sau de PAUZĂ/ODIHNĂ sau NECUNOSCUTE ([2]) de minimum 15 minute pentru un anumit conducător auto, acumulate după încheierea ultimei sale perioade de DISPONIBILITATE sau de PAUZĂ/ODIHNĂ sau NECUNOSCUTE ([2]) de minimum 45 de minute [este posibil ca această perioadă să fi fost împărțită în conformitate cu Regulamentul (CE) nr. 561/2006].

Pentru calculele care trebuie efectuate se iau în considerare, după cum este necesar, activitățile anterioare stocate pe cardul de conducător auto. Perioadele necunoscute cu durată negativă (începutul perioadei necunoscute > sfârșitul perioadei necunoscute) cauzate de suprapunerile de timp dintre două aparate de înregistrare diferite nu sunt luate în considerare la realizarea acestor calcule.

În cazul în care conducătorul auto nu și-a introdus cardul, calculele necesare se bazează pe înregistrările din memoria de date pentru perioada în curs în care niciun card nu a fost introdus și legate de slotul relevant;

([1]) Această modalitate de calculare a timpului de conducere continuă și a duratei cumulate a pauzelor este utilizată de aparatura de înregistrare pentru calcularea avertismentului legat de timpul de conducere continuă. Ea nu aduce atingere interpretării legale a acestor timpi. Modalitățile alternative de calculare a timpului de conducere continuă și a duratei cumulate a pauzelor pot fi utilizate pentru a înlocui aceste definiții dacă acestea au devenit caduce în urma actualizării unor alte texte legislative în materie.

([2]) Perioadele NECUNOSCUTE corespund perioadelor în care cardul de conducător auto nu a fost introdus în aparatul de înregistrare și în care nu au fost introduse manual date privind activitățile conducătorului auto.

([3]) Regulamentul (CE) nr. 561/2006 al Parlamentului European și al Consiliului din 15 martie 2006 privind armonizarea anumitor dispoziții ale legislației sociale în domeniul transporturilor rutiere, de modificare a Regulamentelor (CEE) nr. 3821/85 și (CE) nr. 2135/98 ale Consiliului și de abrogare a Regulamentului (CEE) nr. 3820/85 al Consiliului (JO L 102, 11.4.2006, p. 1).

(q) „memorie de date” înseamnă:

un dispozitiv de stocare a datelor electronice încorporat în aparatura de înregistrare;

(r) „semnătură digitală” înseamnă:

datele atașate unui bloc de date sau o transformare criptografică a acestuia, care permite destinatarului blocului de date să dovedească autenticitatea și integritatea respectivului bloc de date;

(s) „descărcare” înseamnă:

copierea, împreună cu semnătura digitală, a unei părți sau a unui set complet de fișiere de date înregistrate în memoria de date a unității montate pe vehicul sau în memoria cardului de tahograf, cu condiția ca acest proces să nu modifice sau să șteargă eventuale date stocate;

Producătorii de unități montate pe vehicul pentru tahografele inteligente și producătorii de dispozitive proiectate și concepute pentru a descărca fișiere de date trebuie să ia toate măsurile rezonabile pentru a se asigura că descărcarea acestor date poate fi efectuată cu o întârziere minimă de către întreprinderile de transport sau de către conducătorii auto.

Descărcarea fișierului care conține viteza detaliată nu este necesară pentru stabilirea conformității cu Regulamentul (CE) nr. 561/2006, dar poate fi folosită, printre altele, în anchetarea unui accident.

(t) „card de conducător auto” înseamnă:

un card de tahograf emis de autoritățile unui stat membru unui anumit conducător auto, care identifică conducătorul auto și permite stocarea datelor privind activitatea acestuia;

(u) „circumferință efectivă a roților” înseamnă:

media distanțelor parcurse de fiecare dintre roțile care acționează vehiculul (roți motoare) în cursul unei rotații complete. Măsurarea acestor distanțe trebuie efectuată în condiții normale de testare, astfel cum sunt definite la cerința 414 și se exprimă în format „l = … mm”. Producătorii de vehicule pot înlocui măsurarea acestor distanțe cu un calcul teoretic care ia în considerare distribuirea masei pe axe atunci când vehiculul este neîncărcat și în stare normală de funcționare ([1]). Metodele pe care se bazează aceste calcule teoretice trebuie aprobate de o autoritate competentă a statului membru și pot fi utilizate numai înainte de activarea tahografului;

(v) „eveniment” înseamnă:

o operațiune anormală detectată de tahograful inteligent care poate decurge dintr-o tentativă de fraudă;

(w) „echipament GNSS extern” înseamnă:

un echipament care conține receptorul GNSS atunci când unitatea montată pe vehicul nu este o unitate individuală, precum și alte componente necesare pentru protecția comunicării datelor de poziționare către restul unității montate pe vehicul;

(x) „anomalie” înseamnă:

o operațiune anormală detectată de tahograful inteligent care poate decurge dintr-un deranjament sau o defecțiune a aparaturii;

(y) „receptor GNSS” înseamnă:

un dispozitiv electronic care recepționează și prelucrează digital semnale de la unul sau mai multe sisteme globale de navigație prin satelit (GNSS), pentru a furniza informații privind poziția, viteza și timpul;

(z) „instalare” înseamnă:

montarea unui tahograf într-un vehicul;

([1]) Regulamentul (UE) nr. 1230/2012 al Comisiei din 12 decembrie 2012 de punere în aplicare a Regulamentului (CE) nr. 661/2009 al Parlamentului European și al Consiliului privind cerințele de omologare de tip pentru masele și dimensiunile autovehiculelor și ale remorcilor acestora și de modificare a Directivei 2007/46/CE a Parlamentului European și a Consiliului (JO L 353, 21.12.2012, p. 31), astfel cum a fost modificat ultima dată.

(aa) „interoperabilitate” înseamnă:

capacitatea sistemelor și a proceselor de lucru care se află la baza acestora de a face schimb de date și de informații;

(bb) „interfață” înseamnă:

un dispozitiv între sisteme care asigură mijlocul prin care acestea se pot conecta și pot interacționa;

(cc) „poziție” înseamnă:

coordonatele geografice ale vehiculului la un moment dat;

(dd) „senzor de mișcare” înseamnă:

o parte a tahografului care furnizează un semnal reprezentând viteza vehiculului și/sau distanța parcursă;

(ee) „card nevalabil” înseamnă:

un card pentru care s-a detectat o anomalie sau a cărui autentificare inițială a eșuat sau a cărui dată de început al valabilității nu a fost încă atinsă sau a cărui dată de expirare a fost depășită;

(ff) „standard deschis” înseamnă:

un standard prevăzut într-un document cu specificațiile standardului, disponibil gratuit sau contra unei taxe nominale, care poate fi copiat, distribuit sau utilizat fără taxă sau contra unei taxe nominale;

(gg) „în afara zonei de aplicare a reglementărilor” înseamnă:

cazurile în care utilizarea aparatului de înregistrare nu este necesară în conformitate cu dispozițiile Regulamentului (CEE) nr. 561/2006;

(hh) „depășirea limitei de viteză” înseamnă:

depășirea vitezei autorizate a vehiculului, definită ca orice perioadă de peste 60 de secunde pe parcursul căreia viteza măsurată a vehiculului depășește limita stabilită pentru limitatorul de viteză prevăzută în Directiva 92/6/CEE a Consiliului ([1]), astfel cum a fost modificată ultima dată;

(ii) „inspecție periodică” înseamnă:

un set de operațiuni realizate pentru a verifica dacă tahograful funcționează corespunzător, dacă reglajele acestuia corespund parametrilor vehiculului și dacă nu sunt atașate dispozitive de manipulare la tahograf;

(jj) „imprimantă” înseamnă:

o componentă a aparaturii de înregistrare cu ajutorul căreia se pot imprima datele stocate;

(kk) „comunicare în scopul detectării timpurii la distanță” înseamnă:

comunicarea între echipamentul de comunicare în scopul detectării timpurii la distanță și cititorul pentru comunicarea în scopul detectării timpurii la distanță în timpul controalelor selective în trafic, cu scopul de a detecta la distanță eventualele cazuri de manipulare sau de utilizare abuzivă a aparaturii de înregistrare;

(ll) „echipament de comunicare la distanță” înseamnă:

echipamentul din cadrul unității montate pe vehicul utilizat pentru efectuarea controalelor selective în trafic;

([1]) Directiva 92/6/CEE a Consiliului din 10 februarie 1992 privind instalarea și utilizarea dispozitivelor limitatoare de viteză pentru anumite categorii de vehicule din cadrul Uniunii (JO L 57, 2.3.1992, p. 27).

(mm) „cititor pentru comunicarea în scopul detectării timpurii la distanță” înseamnă:

sistemul utilizat de agenții de control pentru controalele selective în trafic;

(nn) „reînnoire” înseamnă:

emiterea unui nou card de tahograf la data expirării cardului existent sau dacă acesta nu funcționează corect și a fost returnat autorității emitente. Reînnoirea implică întotdeauna certitudinea că nu coexistă două carduri valabile;

(oo) „reparație” înseamnă:

orice reparație efectuată la un senzor de mișcare sau la o unitate montată pe vehicul sau la un cablu, care impune deconectarea de la sursa de alimentare cu electricitate sau deconectarea de la alte componente ale tahografului sau deschiderea senzorului de mișcare sau a unității montate pe vehicul;

(pp) „înlocuire a cardului” înseamnă:

emiterea unui card de tahograf care să înlocuiască un card existent care a fost declarat pierdut, furat sau care nu funcționează corespunzător și care nu a fost returnat autorității emitente. Înlocuirea implică întotdeauna riscul ca două carduri valabile să coexiste;

(qq) „certificare a securității” înseamnă:

proces prin care un organism de certificare pe baza criteriilor comune certifică faptul că aparatura de înregistrare (sau o componentă) sau cardul de tahograf investigat îndeplinesc cerințele de securitate definite în profilurile de protecție aferente;

(rr) „autotest” înseamnă:

teste efectuate în mod ciclic și automat de către aparatura de înregistrare pentru a detecta anomalii;

(ss) „măsurarea timpului” înseamnă:

o înregistrare digitală permanentă a datei și orei UTC (timpul universal coordonat);

(tt) „reglarea orei” înseamnă:

o reglare automată a orei curente la intervale periodice și cu o toleranță maximă de un minut, sau o reglare efectuată în timpul etalonării;

(uu) „dimensiunea pneurilor” înseamnă:

desemnarea dimensiunilor pneurilor (de la roțile motoare externe) în conformitate cu Directiva 92/23/CEE a Consiliului ([1]), astfel cum a fost modificată ultima dată;

(vv) „identificarea vehiculului” înseamnă:

numerele de identificare ale vehiculului: numărul de înmatriculare al vehiculului (VRN), care indică și statul membru de înmatriculare, și numărul de identificare al vehiculului (VIN) ([2]);

(ww) „săptămână” înseamnă, în scopul calculelor efectuate de aparatura de înregistrare:

perioada cuprinsă între ziua de luni, ora 00.00 UTC și duminica următoare, ora 24.00 UTC;

([1]) Directiva 92/23/CEE a Consiliului din 31 martie 1992 privind pneurile autovehiculelor și ale remorcilor acestora, precum și montarea lor (JO L 129, 14.5.1992, p. 95).

([2]) Directiva 76/114/CEE a Consiliului din 18 decembrie 1975 privind apropierea legislațiilor statelor membre referitoare la plăcuțele și inscripționările regulamentare ale autovehiculelor și ale remorcilor, precum și la amplasamentul și modul de aplicare a acestora (JO L 24, 30.1.1976, p. 1).

(xx) „card de atelier” înseamnă:

un card de tahograf emis de autoritățile unui stat membru personalului desemnat al unui producător de tahografe, montator, producător de vehicule sau atelier aprobat de statul membru respectiv, care identifică titularul cardului și permite testarea, etalonarea și activarea tahografelor și/sau descărcarea din acestea;

(yy) „adaptor” înseamnă:

un dispozitiv care emite în permanență un semnal reprezentativ pentru viteza vehiculului și/sau distanța parcursă de acesta, altul decât cel utilizat pentru detectarea independentă a deplasărilor, și care este:

— instalat și utilizat numai pe vehiculele de tip M1 și N1 (conform definițiilor din anexa II la Directiva 2007/46/CE a Parlamentului European și a Consiliului ([1]), astfel cum a fost modificată ultima dată) puse în funcțiune începând de la data de 1 mai 2006;

— instalat acolo unde este imposibil din punct de vedere mecanic să se instaleze orice alt tip de senzor de mișcare existent care respectă, în rest, dispozițiile prezentei anexe și ale apendicelor 1-15 la aceasta;

— instalat între unitatea montată pe vehicul și locul unde impulsurile de viteză/distanță sunt generate de senzori integrați sau de interfețe alternative;

— din perspectiva unității montate pe vehicul, comportamentul adaptorului este același ca în situația în care la unitatea montată pe vehicul ar fi conectat un senzor de mișcare care respectă dispozițiile prezentei anexe și ale apendicelor 1-16 la aceasta;

utilizarea unui astfel de adaptor în vehiculele menționate mai sus permite instalarea și utilizarea corectă a unei unități montate pe vehicul care respectă toate cerințele prezentei anexe;

în cazul vehiculelor respective, tahograful inteligent include cabluri, un adaptor și o unitate montată pe vehicul;

(zz) „integritatea datelor” înseamnă:

precizia și compatibilitatea datelor stocate, indicate prin absența oricărei modificări a datelor între două actualizări ale unei înregistrări de date. Integritatea implică faptul că datele constituie o copie fidelă a versiunii originale, de exemplu faptul că datele nu au fost deteriorate în cursul procesului de scriere pe sau de citire dintr-un card de tahograf sau dintr-un dispozitiv corespunzător sau în cursul transmisiei prin intermediul oricărui canal de comunicare;

(aaa) „confidențialitatea datelor” înseamnă:

măsurile tehnice generale luate cu scopul de a asigura punerea corespunzătoare în aplicare a principiilor prevăzute în Directiva 95/46/CE a Parlamentului European și a Consiliului ([2]), precum și a principiilor prevăzute în Directiva 2002/58/CE a Parlamentului European și a Consiliului ([3]);

(bbb) „sistem tahografic inteligent” înseamnă:

aparatura de înregistrare, cardurile de tahograf și ansamblul tuturor echipamentelor cu interacțiune directă sau indirectă în cursul etapelor de construcție, instalare, utilizare, testare și control ale acestora, precum cardurile, cititorul pentru comunicarea la distanță și orice alte echipamente pentru descărcarea datelor, analizarea datelor, etalonare, generarea, gestionarea sau introducerea elementelor de securitate etc.;

(ccc) „data introducerii” înseamnă:

36 de luni de la intrarea în vigoare a dispozițiilor detaliate menționate la articolul 11 din Regulamentul (UE) nr. 165/2014 al Parlamentului European și al Consiliului ([4]).

([1]) Directiva 2007/46/CE a Parlamentului European și a Consiliului din 5 septembrie 2007 de stabilire a unui cadru pentru omologarea autovehiculelor și remorcilor acestora, precum și a sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective (Directivă-cadru) (JO L 263, 9.10.2007, p. 1).

([2]) Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).

([3]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

([4]) Regulamentul (UE) nr. 165/2014 al Parlamentului European și al Consiliului din 4 februarie 2014 privind tahografele în transportul rutier, de abrogare a Regulamentului (CEE) nr. 3821/85 al Consiliului privind aparatura de înregistrare în transportul rutier și de modificare a Regulamentului (CE) nr. 561/2006 al Parlamentului European și al Consiliului privind armonizarea anumitor dispoziții ale legislației sociale în domeniul transporturilor rutiere (JO L 60, 28.2.2014, p. 1).

Este data începând de la care vehiculele înmatriculate pentru prima dată:

— *trebuie să fie echipate cu un tahograf conectat la un serviciu de poziționare bazat pe un sistem de navigație prin satelit;*

— *trebuie să poată comunica autorităților de control competente date pentru controalele selective în trafic, în timp ce vehiculul se află în mișcare;*

— *și pot fi echipate cu interfețe standardizate care să permită utilizarea în modul operațional, de către un dispozitiv extern, a datelor înregistrate sau produse de tahografe;*

(ddd) „profil de protecție" înseamnă:

un document utilizat ca parte a procesului de certificare în conformitate cu criteriile comune, care definește, independent de punerea în aplicare, cerințele de securitate pentru garantarea protecției informațiilor;

(eee) „precizia GNSS" înseamnă:

în contextul înregistrării poziției de către un sistem global de navigație prin satelit (GNSS) cu ajutorul tahografelor, înseamnă valoarea scăderii preciziei în plan orizontal (HDOP – *Horizontal Dilution of Precision*), calculată ca cea mai mică dintre valorile HDOP colectate de la sistemele GNSS disponibile.

2. CARACTERISTICI ȘI FUNCȚII GENERALE ALE APARATURII DE ÎNREGISTRARE

2.1 **Caracteristici generale**

Scopul aparaturii de înregistrare este de a înregistra, a stoca, a afișa, a imprima și a genera date privind activitatea șoferului.

Orice vehicul dotat cu aparatură de înregistrare conformă cu dispozițiile prezentei anexe trebuie să fie echipat, de asemenea, cu un vitezometru și cu un odometru. Aceste funcții pot fi incluse în aparatura de înregistrare.

(1) Aparatura de înregistrare include cabluri, un senzor de mișcare și o unitate montată pe vehicul.

(2) Interfața dintre senzorii de mișcare și unitățile montate pe vehicul respectă cerințele specificate în apendicele 11.

(3) Unitatea montată pe vehicul este conectată la sistemul (sistemele) global(e) de navigație prin satelit, în conformitate cu apendicele 12.

(4) Unitatea montată pe vehicul comunică cu cititoarele pentru comunicarea în scopul detectării timpurii la distanță, în conformitate cu apendicele 14.

(5) Unitatea montată pe vehicul poate include o interfață ITS, specificată în apendicele 13.

Aparatura de înregistrare poate fi conectată la alte echipamente prin intermediul unor interfețe suplimentare și/sau prin interfața ITS opțională.

(6) Includerea în sau conectarea la aparatura de înregistrare a oricărei funcții, dispozitiv sau dispozitive, omologate sau de alt tip, nu trebuie să interfereze sau să fie susceptibilă de a interfera cu funcționarea corespunzătoare și sigură a aparaturii de înregistrare, nici să încalce sau să fie susceptibilă de a încălca dispozițiile prezentului regulament.

Utilizatorii aparaturii de înregistrare se identifică prin intermediul cardurilor de tahograf.

(7) Aparatura de înregistrare oferă drepturi selective de acces la date și la funcții, pe baza tipului și/sau a identității utilizatorului.

Aparatura de înregistrare înregistrează și stochează date în memoria sa de date, în echipamentul de comunicare la distanță și pe cardurile de tahograf.

Acest lucru se face în conformitate cu Directiva 95/46/CE din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date ([1]), cu Directiva 2002/58/CE din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice ([2]) și cu articolul 7 din Regulamentul (UE) nr. 165/2014.

2.2 **Funcții**

(8) Aparatura de înregistrare asigură următoarele funcții:

— monitorizarea introducerilor și a retragerilor cardurilor;

— măsurarea vitezei, a distanței și a poziției;

— măsurarea timpului;

— monitorizarea activităților conducătorului auto;

— monitorizarea regimului de conducere;

— introducerea manuală a datelor de către conducătorul auto;

— înregistrarea locurilor în care încep și/sau se încheie zilele de lucru;

— introducerea manuală a activităților conducătorului auto;

— înregistrarea condițiilor specifice;

— gestionarea blocărilor efectuate de societate;

— monitorizarea activităților de control;

— detectarea evenimentelor și/sau a anomaliilor;

— testele integrate și autotestele;

— citirea din memoria de date;

— înregistrarea și stocarea în memoria de date;

— citirea de pe cardurile de tahograf;

— înregistrarea și stocarea pe cardurile de tahograf;

— afișarea;

— imprimarea;

— avertizarea;

— descărcarea de date pe suporturi externe;

— comunicarea la distanță pentru controalele selective în trafic;

— date de ieșire transmise unor echipamente suplimentare;

— etalonarea;

— verificarea etalonării în trafic;

— reglarea orei.

([1]) JO L 281, 23.11.1995, p.31.
([2]) JO L 201, 31.7.2002, p.37.

2.3 **Moduri de funcționare**

(9) Aparatura de înregistrare are patru moduri de operare:

— modul operațional;

— modul control;

— modul etalonare;

— modul societate.

(10) Aparatura de înregistrare este comutată la următoarele moduri de funcționare pe baza cardurilor de tahograf valabile introduse în dispozitivele de interfață pentru card. Generația cardului de tahograf nu este relevantă pentru determinarea modului de funcționare, cu condiția să fie introdus un card valabil. Un card de atelier de primă generație este întotdeauna considerat nevalabil atunci când este introdus într-o unitate montată pe vehicul (VU) de a doua generație.

Mod de funcționare		Slot pentru cardul de conducător auto				
		Niciun card	Card de conducător auto	Card de control	Card de atelier	Card de societate
Slot pentru cardul copilotului	Niciun card	Operațional	Operațional	Control	Etalonare	Societate
	Card de conducător auto	Operațional	Operațional	Control	Etalonare	Societate
	Card de control	Control	Control	Control (*)	Operațional	Operațional
	Card de atelier	Etalonare	Etalonare	Operațional	Etalonare (*)	Operațional
	Card de societate	Societate	Societate	Operațional	Operațional	Societate (*)

(*) În aceste situații, aparatura de înregistrare utilizează numai cardul de tahograf introdus în slotul pentru cardul de conducător auto.

(11) Aparatura de înregistrare refuză cardurile nevalabile introduse, permițând în astfel de cazuri numai afișarea, imprimarea sau descărcarea datelor stocate pe cardurile expirate.

(12) Toate funcțiile enumerate la punctul 2.2 sunt disponibile în orice mod de funcționare, cu următoarele excepții:

— funcția de etalonare este accesibilă numai în modul etalonare;

— funcția de verificare a etalonării în trafic este accesibilă numai în modul etalonare;

— funcția de gestionare a blocărilor efectuate de societate este accesibilă numai în modul societate;

— funcția de monitorizare a activităților de control este accesibilă numai în modul control;

— funcția de descărcare nu este accesibilă în modul operațional (cu excepția cazurilor prevăzute la cerința 193) și cu excepția descărcării de pe un card de conducător auto atunci când în unitatea montată pe vehicul nu este introdus niciun alt tip de card.

(13) Aparatura de înregistrare poate extrage orice date în vederea afișării, imprimării sau descărcării pe suporturi externe, cu următoarele excepții:

— în modul operațional, orice identificare personală (nume și prenume) care nu corespunde unui card de tahograf introdus este mascată și orice număr de card care nu corespunde unui card de tahograf introdus este mascat parțial (fiecare caracter de pe pozițiile cu număr impar – de la stânga la dreapta – este mascat);

— în modul societate, datele privind conducătorul auto (cerințele 102, 105 și 108) pot fi extrase numai pentru perioadele în care nu există nicio blocare sau în care nicio o altă societate (astfel cum este identificată pe baza primelor 13 caractere din numărul cardului de societate) nu a activat vreo blocare;

— dacă în aparatura de înregistrare nu a fost introdus niciun card, nu pot fi extrase date privind conducătorul auto decât pentru ziua respectivă și pentru cele opt zile calendaristice anterioare zilei respective;

— datele cu caracter personal provenind din VU nu se extrag prin interfața ITS a VU, cu excepția cazului în care a fost verificat acordul conducătorului auto la care se referă datele respective;

— unitățile montate pe vehicul au, în mod normal, o perioadă de funcționare de 15 ani, începând de la data eliberării certificatelor aferente unităților montate pe vehicul, însă ele pot fi utilizate încă trei luni după această perioadă numai pentru descărcarea de date.

2.4 **Securitate**

Scopul sistemului de securitate este de a proteja memoria de date astfel încât să împiedice accesul neautorizat la date și manipularea acestora și de a detecta orice astfel de tentative, protejând integritatea și autenticitatea datelor transmise între senzorul de mișcare și unitatea montată pe vehicul, integritatea și autenticitatea datelor transmise între aparatura de înregistrare și cardurile de tahograf, integritatea și autenticitatea datelor transmise între aparatura de înregistrare și echipamentul GNSS extern, precum și confidențialitatea, integritatea și autenticitatea datelor transmise, în scopuri de control, prin comunicarea la distanță în scopul detectării timpurii, precum și verificând integritatea și autenticitatea datelor descărcate.

(14) Pentru a garanta securitatea sistemului, următoarele componente trebuie să îndeplinească cerințele de securitate specificate în profilurile de protecție, în conformitate cu apendicele 10:

— unitatea montată pe vehicul;

— cardul de tahograf;

— senzorul de mișcare;

— echipamentul GNSS extern (acest profil este necesar și aplicabil numai pentru varianta externă a GNSS).

3. CERINȚE DE CONSTRUCȚIE ȘI DE FUNCȚIONARE APLICABILE APARATURII DE ÎNREGISTRARE

3.1 **Monitorizarea introducerii și retragerii cardurilor**

(15) Aparatura de înregistrare monitorizează dispozitivele de interfață pentru card pentru a detecta introducerile și retragerile cardurilor.

(16) La introducerea unui card, aparatura de înregistrare verifică valabilitatea cardului de tahograf introdus și, dacă acesta este valabil, identifică tipul și generația cardului.

Dacă în aparatura de înregistrare a fost deja introdus un card cu același număr și cu un indice de reînnoire mai mare, cardul în cauză este declarat nevalabil.

Dacă în aparatura de înregistrare a fost deja introdus un card cu același număr și cu același indice de reînnoire, dar cu un indice de înlocuire mai mare, cardul în cauză este declarat nevalabil.

(17) Cardurile de tahograf de primă generație sunt considerate nevalabile de către aparatura de înregistrare după ce posibilitatea de a utiliza carduri de tahograf de primă generație a fost suprimată de un atelier, în conformitate cu apendicele 15 (cerința MIG003).

(18) Cardurile de atelier de primă generație care sunt introduse într-o aparatură de înregistrare de a doua generație sunt considerate nevalabile.

(19) Aparatura de înregistrare este proiectată astfel încât cardurile de tahograf să fie blocate în poziția corectă la introducerea lor în dispozitivul de interfață pentru card.

(20) Retragerea cardurilor de tahograf este posibilă numai după oprirea vehiculului și după stocarea datelor relevante pe carduri. Retragerea cardului necesită o intervenție concretă a utilizatorului.

3.2 **Măsurarea vitezei, a poziției și a distanței**

(21) Senzorul de mișcare (integrat eventual în adaptor) reprezintă principala sursă de măsurare a vitezei și a distanței.

(22) Această funcție asigură măsurarea continuă și poate indica valoarea înregistrată de odometru care corespunde distanței totale parcurse de vehicul, pe baza impulsurilor emise de senzorul de mișcare.

(23) Această funcție asigură măsurarea continuă și poate indica viteza vehiculului, pe baza impulsurilor emise de senzorul de mișcare.

(24) Funcția de măsurare a vitezei indică, de asemenea, dacă vehiculul se deplasează sau este oprit. Se consideră că vehiculul se deplasează în momentul în care funcția detectează o valoare mai mare de 1 imp/sec de la senzorul de mișcare timp de cel puțin cinci secunde, în caz contrar vehiculul fiind considerat oprit.

(25) Dispozitivele pentru afișarea vitezei (vitezometrul) și a distanței totale parcurse (odometrul) instalate în orice vehicul prevăzut cu o aparatură de înregistrare care respectă dispozițiile prezentului regulament trebuie să respecte cerințele privind toleranțele maxime (a se vedea punctele 3.2.1 și 3.2.2.) prevăzute în prezenta anexă.

(26) Pentru detectarea manipulării datelor de la senzorul de mișcare, informațiile provenite de la senzorul de mișcare sunt coroborate cu informațiile privind deplasarea vehiculului derivate din receptorul GNSS și, în mod opțional, din altă (alte) sursă (surse) independentă (independente) de senzorul de mișcare.

(27) Această funcție măsoară poziția vehiculului pentru a permite înregistrarea automată:

— a pozițiilor în care conducătorul auto și/sau copilotul își încep(e) ziua de lucru;

— a pozițiilor în care timpul de conducere continuă al conducătorului auto atinge un multiplu de trei ore;

— a pozițiilor în care conducătorul auto și/sau copilotul își încheie ziua de lucru.

3.2.1 *Măsurarea distanței parcurse*

(28) Distanța parcursă poate fi măsurată:

— fie cumulând deplasările înainte și înapoi;

— fie cumulând numai deplasările înainte.

(29) Aparatura de înregistrare măsoară distanța parcursă între 0 și 9 999 999,9 km.

(30) Distanța măsurată respectă următoarele limite de toleranță (distanțe de cel puțin 1 000 m):

— ± 1 % înainte de instalare;

— ± 2 % în cursul instalării și al inspecțiilor periodice;

— ± 4 % în timpul funcționării.

(31) Distanța măsurată trebuie să aibă o rezoluție de 0,1 km sau mai bună.

3.2.2 *Măsurarea vitezei*

(32) Aparatura de înregistrare măsoară viteza între 0 și 220 km/h.

(33) Pentru a asigura o toleranță maximă de ± 6 km/h pentru viteza afișată în timpul funcționării și luând în considerare:

— o toleranță de ± 2 km/h pentru variațiile semnalului de intrare (variații provocate de pneuri, …);

— o toleranță de ± 1 km/h la măsurătorile efectuate în timpul instalării sau al inspecțiilor periodice;

aparatura de înregistrare trebuie să măsoare viteza cu o toleranță de ± 1 km/h (la viteză constantă) dacă vitezele se încadrează între 20 și 180 km/h, iar coeficienții caracteristici ai vehiculului între 4 000 și 25 000 imp/km.

Notă: Datorită rezoluției stocării de date, se adaugă o toleranță suplimentară de ± 0,5 km/h la viteza stocată de aparatura de înregistrare.

(34) Viteza trebuie măsurată corect, în limitele normale de toleranță, în primele două secunde de după finalizarea unei modificări a vitezei, dacă viteza s-a modificat într-un ritm de până la 2 m/s^2.

(35) Măsurarea vitezei trebuie să aibă o rezoluție de 1 km/h sau mai bună.

3.2.3 *Măsurarea poziției*

(36) Aparatura de înregistrare măsoară poziția absolută a vehiculului cu ajutorul receptorului GNSS.

(37) Poziția absolută se măsoară în coordonate geografice de latitudine și longitudine, în grade și minute, cu o rezoluție de 1/10 de minut.

3.3 **Măsurarea timpului**

(38) Funcția de măsurare a timpului măsoară în permanență data și ora UTC și le furnizează în format digital.

(39) Data și ora UTC se utilizează pentru datarea datelor din aparatura de înregistrare (înregistrări, schimburi de date) și pentru toate materialele imprimate menționate la apendicele 4 „Materiale imprimate”.

(40) Pentru afișarea orei locale este posibilă modificarea decalajului orar al orei afișate, în intervale de o jumătate de oră. Nu este admis niciun alt decalaj în afara celor care reprezintă multipli negativi sau pozitivi de jumătate de oră;

(41) Abaterea de timp nu trebuie să depășească ± 2 secunde pe zi în condiții de omologare de tip, în absența oricărei reglări a orei.

(42) Timpul se măsoară cu o rezoluție de o secundă sau mai bună.

(43) Măsurarea timpului nu este afectată de întreruperile alimentării cu energie electrică din exterior care durează mai puțin de 12 luni în condiții de omologare de tip.

3.4 **Monitorizarea activităților conducătorului auto**

(44) Această funcție monitorizează, în mod permanent și separat, activitățile unui conducător auto și ale unui copilot.

(45) Activitățile conducătorului auto sunt CONDUCERE, MUNCĂ, DISPONIBILITATE sau PAUZĂ/ ODIHNĂ.

(46) Pilotul și/sau copilotul pot selecta manual MUNCĂ, DISPONIBILITATE sau PAUZĂ/ODIHNĂ.

(47) Când vehiculul este în mișcare, se selectează automat activitatea CONDUCERE pentru conducătorul auto și DISPONIBILITATE pentru copilot.

(48) Când vehiculul se oprește, pentru conducătorul auto se selectează automat MUNCĂ.

(49) Se consideră că prima modificare a activității în ODIHNĂ sau DISPONIBILITATE în termen de 120 de secunde de la selectarea automată a activității MUNCĂ din cauza opririi vehiculului s-a produs în momentul în care vehiculul s-a oprit (fiind astfel posibilă anularea modificării în MUNCĂ).

(50) Această funcție transmite modificările activităților către funcțiile de înregistrare cu o rezoluție de un minut.

(51) Dacă o activitate de CONDUCERE este înregistrată ca activitate atât în minutul imediat anterior, cât și în minutul imediat ulterior unui minut calendaristic dat, minutul respectiv va fi considerat în întregime drept minut de CONDUCERE.

(52) Dacă un minut calendaristic dat nu este considerat minut de CONDUCERE conform cerinței 051, întregul minut este considerat ca aparținând aceluiași tip de activitate ca cea mai lungă activitate continuă derulată în minutul respectiv (sau cea mai recentă activitate în cazul unor activități cu durată egală).

(53) Această funcție permite, de asemenea, monitorizarea permanentă a timpului de conducere continuă și a duratei cumulate a pauzelor conducătorului auto.

3.5 **Monitorizarea regimului de conducere**

(54) Această funcție monitorizează, în mod permanent și automat, regimul de conducere.

(55) Când în aparat sunt introduse două carduri de conducător auto valabile, se selectează regimul de conducere ECHIPAJ, iar în toate celelalte cazuri se selectează regimul SINGUR.

3.6 **Înregistrări realizate de conducătorii auto**

3.6.1 *Înregistrarea locurilor în care încep și/sau se încheie zilele de lucru*

(56) Această funcție permite înregistrarea locurilor în care, potrivit conducătorului auto și/sau copilotului, încep și/sau se încheie zilele sale (lor) de lucru.

(57) Un loc înseamnă țara și, dacă este cazul, și regiunea care sunt înregistrate sau confirmate manual.

(58) În momentul retragerii unui card de conducător auto, aparatura de înregistrare îi solicită conducătorului auto (copilotului) să introducă un „loc în care se încheie ziua de lucru”.

(59) Conducătorul auto introduce atunci locul în care se află vehiculul în momentul respectiv, acest lucru fiind considerat o înregistrare temporară.

(60) Înregistrarea locurilor în care încep și/sau se încheie zilele de lucru este posibilă prin intermediul comenzilor din meniuri. Dacă într-un minut calendaristic se efectuează mai multe astfel de înregistrări, nu vor rămâne înregistrate decât locul de începere cel mai recent introdus și locul de încheiere cel mai recent introdus.

3.6.2 *Introducerea manuală a activităților conducătorului auto și acordul conducătorului auto pentru interfața ITS*

(61) Aparatura de înregistrare permite introducerea manuală a activităților numai în momentul introducerii cardului de conducător auto (sau de atelier). Introducerea manuală a activităților se efectuează utilizând valorile datei și orei locale corespunzătoare fusului orar (decalaj UTC) setat la momentul respectiv pentru unitatea montată pe vehicul.

La introducerea cardului de conducător auto sau de atelier, titularului cardului i se vor reaminti următoarele:

— data și ora ultimei retrageri a cardului;

— în mod opțional: decalajul orei locale setat la momentul respectiv pentru unitatea montată pe vehicul.

La prima introducere a unui card de conducător auto sau de atelier care nu este recunoscut, la momentul respectiv, de unitatea montată pe vehicul, titularul cardului este invitat să își exprime acordul privind extragerea datelor cu caracter personal din tahograf prin intermediul interfeței ITS opționale.

Acordul conducătorului auto (respectiv al atelierului) poate fi activat sau dezactivat în orice moment prin comenzile din meniu, cu condiția să fie introdus cardul de conducător auto (respectiv de atelier).

Este posibil să se introducă activități, cu următoarele restricții:

— tipul de activitate trebuie să fie MUNCĂ, DISPONIBILITATE sau PAUZĂ/ODIHNĂ;

— ora de începere și de încheiere ale fiecărei activități trebuie să se situeze numai între momentul ultimei retrageri a cardului și cel al introducerii sale curente;

— activitățile nu trebuie să se suprapună în timp.

Este posibil să se introducă manual date, dacă este necesar, la prima introducere a unui card de conducător auto (sau de atelier) care nu a mai fost utilizat.

Procedura de introducere manuală a activităților include toate etapele consecutive necesare pentru stabilirea tipului, a orei de începere și a orei de încheiere a fiecărei activități. Pentru oricare subdiviziune a perioadei de timp dintre ultima retragere a cardului și inserarea curentă a acestuia, titularul cardului are opțiunea de a nu declara nicio activitate.

În timpul introducerii manuale a datelor asociate introducerii cardului, titularul cardului are posibilitatea de a introduce, dacă este cazul:

— locul unde s-a încheiat o zi de lucru anterioară, asociat orei relevante (suprascriind astfel înregistrarea efectuată cu ocazia ultimei retrageri a cardului);

— locul unde începe ziua de lucru curentă, asociată orei relevante.

Dacă titularul cardului nu înregistrează locul în care își începe sau își încheie ziua de lucru în cursul introducerii manuale a datelor asociate introducerii cardului, acest lucru se consideră drept o declarație a faptului că ziua sa de lucru nu s-a modificat de la ultima retragere a cardului. Următoarea înregistrare a unui loc în care se încheie o zi de lucru anterioară superscrie apoi înregistrarea temporară efectuată cu ocazia ultimei retrageri a cardului.

Dacă se introduce un loc, acesta se înregistrează pe cardul de tahograf relevant.

Introducerea manuală a datelor se întrerupe dacă:

— cardul este retras; sau

— vehiculul este în mișcare, iar cardul se află în slotul pentru cardul de conducător auto.

Sunt permise întreruperi suplimentare, de exemplu o pauză după o anumită perioadă de inactivitate a utilizatorului. Dacă introducerea manuală a datelor este întreruptă, aparatura de înregistrare validează orice date complete privind locul și activitatea (care indică, fără ambiguitate, fie locul și timpul, fie tipul de activitate, ora de începere și ora încheiere) care au fost deja înregistrate.

Dacă, în cursul introducerii manuale a datelor pentru un card introdus anterior, se introduce un al doilea card de conducător auto sau de atelier, introducerea manuală a datelor pentru primul card poate fi finalizată înainte de a începe introducerea manuală a datelor pentru cel de al doilea card.

Titularul cardului are opțiunea de a introduce manual date conform următoarei proceduri minime:

— Se introduc activitățile manual, în ordine cronologică, pentru intervalul dintre ultima retragere a cardului și introducerea curentă a acestuia.

— Ora începerii primei activități se setează la ora retragerii cardului. Pentru fiecare înregistrare ulterioară, ora începerii este presetată să urmeze imediat orei de încheiere a înregistrării anterioare. Pentru fiecare activitate se selectează tipul activității și ora încheierii.

Procedura se încheie în momentul în care ora de încheiere a unei activități introduse manual este aceeași cu ora inserării cardului. Aparatura de înregistrare poate apoi permite, opțional, titularului cardului să modifice orice activitate introdusă manual, până în momentul validării prin selectarea unei comenzi specifice. Ulterior, orice astfel de modificări sunt interzise.

3.6.3 *Înregistrarea condițiilor specifice*

(62) Aparatura de înregistrare permite conducătorului auto să introducă, în timp real, următoarele două condiții specifice:

— „ÎN AFARA ZONEI DE APLICARE A REGLEMENTĂRILOR” (început, sfârșit)

— „TRASEU PARCURS PE FERIBOT/ÎN TREN” (început, sfârșit).

O condiție de tip „TRASEU PARCURS PE FERIBOT/ÎN TREN” nu se poate produce dacă este deschisă o condiție de tip „ÎN AFARA ZONEI DE APLICARE A REGLEMENTĂRILOR”.

O condiție deschisă de tip „ÎN AFARA ZONEI DE APLICARE A REGLEMENTĂRILOR” trebuie să fie închisă în mod automat de către aparatura de înregistrare dacă este introdus sau retras un card de conducător auto.

O condiție deschisă de tip „ÎN AFARA ZONEI DE APLICARE A REGLEMENTĂRILOR” împiedică apariția următoarelor evenimente și avertismente:

— conducere fără un card adecvat;

— avertismente asociate timpului de conducere continuă.

Indicatorul de început al condiției „TRASEU PARCURS PE FERIBOT/ÎN TREN” se setează înainte de oprirea motorului pe feribot/în tren.

O condiție deschisă de tip „TRASEU PARCURS PE FERIBOT/ÎN TREN” trebuie să se încheie atunci când se produce oricare dintre următoarele evenimente:

— conducătorul auto încheie manual condiția „TRASEU PARCURS PE FERIBOT/ÎN TREN”;

— conducătorul auto își retrage cardul;

O condiție deschisă de tip „TRASEU PARCURS PE FERIBOT/ÎN TREN” se încheie atunci când nu mai este valabilă în temeiul normelor prevăzute în Regulamentul (CE) nr. 561/2006.

3.7 **Gestionarea blocărilor efectuate de societate**

(63) Această funcție permite gestionarea blocărilor efectuate de o societate pentru a-și asigura accesul exclusiv la date în modul societate.

(64) Blocările efectuate de societate constau într-o dată și o oră de începere (blocare) și într-o dată și o oră de sfârșit (deblocare) asociate identificării societății pe baza numărului cardului de societate (la blocare).

(65) Blocările pot fi „activate” sau „dezactivate” numai în timp real.

(66) Deblocarea poate fi efectuată numai de către societatea a cărei blocare este „activă” (conform identificării pe baza primelor 13 caractere din numărul cardului de societate) sau

(67) Deblocarea este automată dacă o altă societate efectuează o blocare.

(68) Dacă o societate efectuează o blocare și dacă blocarea anterioară a fost efectuată de aceeași societate, se consideră că blocarea anterioară nu a fost „dezactivată” și este încă „activă”.

3.8 **Monitorizarea activităților de control**

(69) Această funcție monitorizează activitățile de AFIȘARE, IMPRIMARE, DESCĂRCARE din VU și de pe card și de verificare a ETALONĂRII ÎN TRAFIC, realizate în modul control.

(70) Această funcție monitorizează, de asemenea, activitățile de CONTROL AL DEPĂȘIRII LIMITEI DE VITEZĂ în modul control. Se consideră că a avut loc un control al depășirii limitei de viteză dacă, în modul control, mesajul „depășirea limitei de viteză” a fost trimis spre imprimantă sau pe ecran sau dacă din memoria de date a VU au fost descărcate date privind „evenimente sau anomalii”.

3.9 **Detectarea evenimentelor și/sau a anomaliilor**

(71) Această funcție detectează următoarele evenimente și/sau anomalii:

3.9.1 *Evenimentul „Introducerea unui card nevalabil”*

(72) Acest eveniment este declanșat de introducerea oricărui card nevalabil, de introducerea unui card de conducător auto deja înlocuit și/sau la expirarea unui card valabil introdus.

3.9.2 *Evenimentul „Conflict de carduri”*

(73) Acest eveniment este declanșat la producerea oricăreia dintre combinațiile de carduri valabile notate cu X din tabelul următor:

Conflict de carduri		Slot pentru cardul de conducător auto				
		Niciun card	Card de conducător auto	Card de control	Card de atelier	Card de societate
Slot pentru cardul copilotului	Niciun card					
	Card de conducător auto				X	
	Card de control			X	X	X
	Card de atelier		X	X	X	X
	Card de societate			X	X	X

3.9.3 *Evenimentul „Suprapunere a timpului”*

(74) Acest eveniment este declanșat atunci când ora/data ultimei retrageri a unui card de conducător auto, așa cum este citită de pe card, sunt ulterioare datei/orei curente înregistrate de aparatura de înregistrare în care este introdus cardul respectiv.

3.9.4 *Evenimentul „Conducere fără un card adecvat”*

(75) Acest eveniment este declanșat de oricare dintre combinațiile de carduri de tahograf valabile notate cu X din tabelul următor, atunci când activitatea conducătorului auto se modifică devenind CONDUCERE sau când intervine o schimbare a modului de funcționare în timp ce activitatea conducătorului auto este CONDUCERE:

Conducere fără un card adecvat		Slot pentru cardul de conducător auto				
		Niciun card (sau card nevalabil)	Card de conducător auto	Card de control	Card de atelier	Card de societate
Slot pentru cardul copilotului	Niciun card (sau card nevalabil)	X		X		X
	Card de conducător auto	X		X	X	X
	Card de control	X	X	X	X	X
	Card de atelier	X	X	X		X
	Card de societate	X	X	X	X	X

3.9.5 *Evenimentul „Introducerea cardului în timpul conducerii”*

(76) Acest eveniment este declanșat la introducerea unui card de tahograf în orice slot în timp ce activitatea conducătorului auto este CONDUCERE.

3.9.6 *Evenimentul „Încheierea incorectă a ultimei sesiuni”*

(77) Acest eveniment este declanșat atunci când, la introducerea unui card, aparatura de înregistrare detectează faptul că, în pofida dispozițiilor de la punctul 3.1, sesiunea anterioară de utilizare a cardului nu a fost încheiată corect (cardul a fost retras înainte ca toate datele relevante să fi fost stocate pe el). Acest eveniment este declanșat numai de cardul de conducător auto și de cardul de atelier.

3.9.7 *Evenimentul „Depășirea limitei de viteză”*

(78) Acest eveniment este declanșat pentru fiecare depășire a limitei de viteză.

3.9.8 *Evenimentul „Întreruperea alimentării cu energie electrică”*

(79) Acest eveniment este declanșat, în celelalte moduri decât modul etalonare sau control, în cazul oricărei întreruperi a alimentării cu energie electrică a senzorului de mișcare și/sau a unității montate pe vehicul, care durează mai mult de 200 de milisecunde. Pragul de întrerupere este stabilit de producător. Scăderea nivelului de alimentare cu energie datorată pornirii motorului nu declanșează acest eveniment.

3.9.9 *Evenimentul „Eroare de comunicare cu echipamentul de comunicare la distanță”*

(80) Acest eveniment se declanșează, **în celelalte moduri decât modul etalonare**, dacă echipamentul de comunicare la distanță nu confirmă recepționarea cu succes a datelor de comunicare la distanță transmise de unitatea montată pe vehicul după mai mult de trei încercări.

3.9.10 *Evenimentul „Absența informațiilor de poziționare de la receptorul GNSS”*

(81) Acest eveniment se declanșează, **în celelalte moduri decât modul etalonare**, în cazul absenței informațiilor de poziționare provenind de la receptorul GNSS (intern sau extern) timp de peste trei ore de timp de conducere acumulat.

3.9.11 *Evenimentul „Eroare de comunicare cu echipamentul GNSS extern”*

(82) Acest eveniment se declanșează, **în celelalte moduri decât modul etalonare**, în cazul întreruperii comunicării între echipamentul GNSS extern și unitatea montată pe vehicul, timp de peste 20 de minute în continuu, atunci când vehiculul este în mișcare.

3.9.12 *Evenimentul „Eroare privind datele de la senzorul de mișcare”*

(83) Acest eveniment este declanșat, **în celelalte moduri decât modul etalonare**, în cazul întreruperii fluxului normal de date dintre senzorul de mișcare și unitatea montată pe vehicul și/sau în cazul unor erori de integritate sau de autentificare a datelor survenite în timpul schimbului de date dintre senzorul de mișcare și unitatea montată pe vehicul.

3.9.13 *Evenimentul „Conflict privind deplasarea vehiculului”*

(84) Acest eveniment se declanșează, **în celelalte moduri decât modul etalonare**, în cazul în care informațiile privind deplasarea calculate de senzorul de mișcare sunt contrazise de informațiile privind deplasarea calculate de receptorul GNSS intern sau de echipamentul GNSS extern și, opțional, de alte surse independente, după cum se specifică în apendicele 12. Acest eveniment nu se declanșează în timpul unui traseu parcurs pe feribot/în tren, în timpul afișării condiției „ÎN AFARA ZONEI DE APLICARE A REGLEMENTĂRILOR” sau atunci când informațiile de poziționare transmise de receptorul GNSS nu sunt disponibile.

3.9.14 *Evenimentul „Tentativă de încălcare a securității”*

(85) Acest eveniment este declanșat, în celelalte moduri decât modul etalonare, în cazul survenirii oricărui alt eveniment care afectează securitatea senzorului de mișcare și/sau a unității montate pe vehicul și/sau a echipamentului GNSS extern, în conformitate cu apendicele 10.

3.9.15 *Evenimentul „Conflict oră”*

(86) Acest eveniment este declanșat, în celelalte moduri decât modul etalonare, atunci când VU detectează o diferență de peste 1 minut între ora calculată de funcția de măsurare a timpului a VU și ora transmisă de receptorul GNSS. Acest eveniment este înregistrat împreună cu valoarea indicată de ceasul intern al unității montate pe vehicul și este însoțit de o reglare automată a orei. După declanșarea unui eveniment de tip „Conflict oră”, VU nu va mai genera alte evenimente de tip „Conflict oră” în următoarele 12 ore. Acest eveniment nu se declanșează în cazul în care receptorul GNSS nu a putut detecta niciun semnal GNSS valabil în cursul ultimelor 30 de zile. Cu toate acestea, de îndată ce informațiile de poziționare de la receptorul GNSS devin din nou disponibile, se efectuează reglarea automată a orei.

3.9.16 *Anomalia „Card”*

(87) Această anomalie este declanșată în cazul unei disfuncții a unui card de tahograf în curs de funcționare.

3.9.17 *Anomalia „Aparatura de înregistrare”*

(88) Această anomalie este declanșată în cazul survenirii oricăreia dintre următoarele defecțiuni, în celelalte moduri decât modul etalonare:

— Anomalie internă a VU

— Anomalie a imprimantei

— Anomalie a afișajului

— Anomalie la descărcare

— Anomalie a senzorului

— Anomalie a receptorului GNSS sau a echipamentului GNSS extern

— Anomalie a echipamentului de comunicare la distanță

3.10 **Teste integrate și autoteste**

(89) Aparatura de înregistrare detectează singură anomaliile prin autoteste și teste integrate, în conformitate cu tabelul următor:

Subansamblu de testat	Autotest	Test integrat
Software		Integritate
Memorie de date	Acces	Acces, integritatea datelor
Dispozitive de interfață pentru card	Acces	Acces
Tastatură		Verificare manuală
Imprimantă	(la latitudinea producătorului)	Imprimare
Afișaj		Verificare vizuală
Descărcare (se efectuează numai în timpul descărcărilor)	Funcționare corespunzătoare	
Senzor	Funcționare corespunzătoare	Funcționare corespunzătoare
Echipament de comunicare la distanță	Funcționare corespunzătoare	Funcționare corespunzătoare
Echipament GNSS	Funcționare corespunzătoare	Funcționare corespunzătoare

3.11 **Citirea din memoria de date**

(90) Aparatura de înregistrare trebuie să poată citi orice date stocate în memoria sa de date.

3.12 **Înregistrarea și stocarea în memoria de date**

În sensul prezentului alineat,

— „365 de zile” înseamnă 365 de zile calendaristice de activitate medie a conducătorilor auto într-un vehicul. Activitatea medie pe zi într-un vehicul implică cel puțin 6 conducători auto sau copiloți, 6 cicluri de introducere și retragere de carduri și 256 de schimbări de activitate. Prin urmare, „365 de zile” implică cel puțin 2 190 de conducători auto (copiloți), 2 190 de cicluri de introducere și retragere de carduri și 93 440 de schimbări de activitate;

— numărul mediu de poziții pe zi înseamnă cel puțin 6 poziții în care începe ziua de lucru, 6 poziții în care timpul de conducere continuă al conducătorului auto atinge un multiplu de trei ore și 6 poziții în care se încheie ziua de lucru, astfel încât „365” de zile includ cel puțin 6 570 de poziții;

— orele sunt înregistrate cu o rezoluție de un minut, cu excepția cazurilor în care se specifică altfel;

— valorile odometrului sunt înregistrate cu o rezoluție de un kilometru;

— vitezele sunt înregistrate cu o rezoluție de 1 km/h;

— pozițiile (latitudinile și longitudinile) sunt înregistrate în grade și minute, cu o rezoluție de 1/10 de minut, cu precizia și cu timpul de achiziție ale GNSS aferente.

(91) Datele stocate în memoria de date nu trebuie să fie afectate de o întrerupere a alimentării externe cu energie electrică cu durata mai scurtă de douăsprezece luni, în condiții de omologare de tip. În plus, datele stocate în echipamentul extern de comunicare la distanță, astfel cum este definit în apendicele 14, nu trebuie să fie afectate de întreruperi ale alimentării cu energie electrică cu durata mai scurtă de 28 de zile.

(92) Aparatura de înregistrare poate înregistra și stoca implicit sau explicit în memoria sa de date următoarele detalii:

3.12.1 *Date de identificare a aparaturii*

3.12.1.1 Date de identificare a unității montate pe vehicul

(93) Aparatura de înregistrare permite stocarea, în memoria sa de date, a următoarelor date de identificare a unității montate pe vehicul:

— denumirea producătorului;

— adresa producătorului;

— numărul de componentă;

— numărul de serie;

— generația VU;

— capacitatea de a utiliza carduri de tahograf de primă generație;

— numărul versiunii de software;

— data de instalare a versiunii de software;

— anul fabricației aparaturii;

— numărul de omologare;

(94) Datele de identificare a unității montate pe vehicul sunt înregistrate și stocate definitiv de producătorul unității montate pe vehicul, cu excepția datelor legate de software și a numărului de omologare, care pot fi modificate în cazul modernizării software-ului, precum și al capacității de utilizare a cardurilor de tahograf de primă generație.

3.12.1.2 Date de identificare a senzorului de mișcare

(95) Senzorul de mișcare trebuie să poată stoca în memoria sa următoarele date de identificare:

— denumirea producătorului;

— numărul de serie;

— numărul de omologare;

— identificatorul componentei integrate de securitate (de exemplu, numărul de componentă al cipului/procesorului intern);

— identificatorul sistemului de operare (de exemplu, numărul versiunii de software).

(96) Datele de identificare a senzorului de mișcare sunt înregistrate și stocate definitiv în senzorul de mișcare de producătorul acestuia.

(97) Unitatea montată pe vehicul trebuie să poată înregistra și stoca în memoria sa de date următoarele date legate de cele mai recente 20 de asocieri ale senzorilor de mișcare (dacă, în cursul unei zile calendaristice, au loc mai multe asocieri, se stochează numai prima și ultima asociere din ziua respectivă):

Pentru fiecare dintre aceste asocieri se înregistrează următoarele date:

— datele de identificare a senzorului de mișcare:

— numărul de serie;

— numărul de omologare;

— datele privind asocierea senzorului de mișcare:

— data asocierii.

3.12.1.3 Date de identificare a sistemului global de navigație prin satelit

(98) Echipamentul GNSS extern trebuie să poată stoca în memoria sa următoarele date de identificare:

— denumirea producătorului;

— numărul de serie;

— numărul de omologare;

— identificatorul componentei integrate de securitate (de exemplu numărul de componentă al cipului/procesorului intern);

— identificatorul sistemului de operare (de exemplu numărul versiunii de software).

(99) Datele de identificare a echipamentului GNSS extern sunt înregistrate și stocate definitiv în echipamentul GNSS extern de producătorul acestuia.

(100) Unitatea montată pe vehicul trebuie să poată înregistra și stoca în memoria sa de date următoarele date legate de cele mai recente 20 de cuplări ale echipamentelor GNSS externe (dacă, în cursul unei zile calendaristice, au loc mai multe cuplări, se stochează numai prima și ultima cuplare din ziua respectivă):

Pentru fiecare dintre aceste cuplări se înregistrează următoarele date:

— datele de identificare a echipamentului GNSS extern:

— numărul de serie;

— numărul de omologare;

— date privind cuplarea echipamentului GNSS extern:

— data cuplării.

3.12.2 *Chei și certificate*

(101) Aparatura de înregistrare poate stoca o serie de chei și certificate criptografice, în conformitate cu apendicele 11 părțile A și B.

3.12.3 *Date privind introducerea și retragerea cardului de conducător auto sau ale cardului de atelier*

(102) Pentru fiecare ciclu de introducere și retragere a unui card de conducător auto sau a unui card de atelier, aparatura de înregistrare înregistrează și stochează în memoria sa de date următoarele detalii:

— numele și prenumele titularului cardului, astfel cum sunt stocate pe card;

— numărul cardului, statul membru emitent și data expirării, astfel cum sunt stocate pe card;

— generația cardului;

— ora și data introducerii cardului;

— valoarea indicată de odometrul vehiculului în momentul introducerii cardului;

— slotul în care este introdus cardul;

— data și ora retragerii cardului;

— valoarea indicată de odometrul vehiculului în momentul retragerii cardului;

— următoarele informații privind vehiculul utilizat anterior de conducătorul auto, astfel cum sunt stocate pe card:

— VRN și statul membru de înmatriculare;

— generația VU (atunci când această informație este disponibilă);

— data și ora retragerii cardului;

— un indicator de stare care arată dacă, la introducerea cardului, titularul acestuia a introdus manual activități sau nu.

(103) Memoria de date trebuie să poată stoca aceste date timp de cel puțin 365 de zile.

(104) La epuizarea capacității de stocare, datele noi înlocuiesc datele cele mai vechi.

3.12.4 *Date privind activitatea conducătorului auto*

(105) Aparatura de înregistrare înregistrează și stochează în memoria sa de date următoarele informații de fiecare dată când survine o modificare a activității conducătorului auto și/sau a copilotului și/sau de fiecare dată când se modifică regimul de conducere și/sau de fiecare dată când este introdus sau retras un card de conducător auto sau de atelier:

— regimul de conducere (ECHIPAJ, SINGUR);

— slotul (CONDUCĂTOR AUTO, COPILOT);

— starea cardului în slotul relevant (INTRODUS, NEINTRODUS);

— activitatea (CONDUCERE, DISPONIBILITATE, MUNCĂ, PAUZĂ/ODIHNĂ);

— data și ora modificării.

INTRODUS înseamnă că în slot este introdus un card de conducător auto sau un card de atelier valabil. NEINTRODUS înseamnă starea opusă, și anume faptul că în slot nu este introdus un card de conducător auto sau de atelier valabil (de exemplu, este introdus un card de societate sau nu este introdus niciun card).

Datele privind activitatea introduse manual de un conducător auto nu sunt înregistrate în memoria de date.

(106) Memoria de date trebuie să poată stoca datele privind activitatea conducătorului auto timp de cel puțin 365 de zile.

(107) La epuizarea capacității de stocare, datele noi înlocuiesc datele cele mai vechi.

3.12.5 *Locuri și poziții în care încep și se încheie zilele de lucru și/sau în care se atinge timpul de conducere continuă de 3 ore*

(108) Aparatura de înregistrare înregistrează și stochează în memoria sa de date:

— locurile și pozițiile în care conducătorul auto și/sau copilotul își începe(e) ziua de lucru;

— pozițiile în care timpul de conducere continuă al conducătorului auto atinge un multiplu de trei ore;

— locurile și pozițiile în care conducătorul auto și/sau copilotul își încheie ziua de lucru.

(109) Atunci când poziția vehiculului nu este disponibilă din receptorul GNSS în momentele respective, aparatura de înregistrare utilizează ultima poziție disponibilă, precum și data și ora aferente.

(110) Aparatura de înregistrare înregistrează și stochează în memoria sa de date, împreună cu fiecare loc sau poziție, următoarele elemente:

— numărul cardului conducătorului auto (copilotului) și statul membru emitent al cardului;

— generația cardului;

— data și ora introducerii;

— tipul de introducere (început, încheiere sau timp de conducere continuă de 3 ore);

— precizia GNSS, data și ora aferente, dacă este cazul;

— valoarea indicată de odometrul vehiculului.

(111) Memoria de date trebuie să poată păstra, timp de cel puțin 365 de zile, locurile și pozițiile în care încep și se încheie zilele de lucru și/sau în care se atinge timpul de conducere continuă de 3 ore.

(112) La epuizarea capacității de stocare, datele noi înlocuiesc datele cele mai vechi.

3.12.6 *Date privind odometrul*

(113) Aparatura de înregistrare înregistrează în memoria sa de date valoarea indicată de odometrul vehiculului și data respectivă la ora 00.00 a fiecărei zile calendaristice.

(114) Memoria de date trebuie să poată stoca valorile indicate de odometru la ora 00.00 timp de cel puțin 365 de zile calendaristice.

(115) La epuizarea capacității de stocare, datele noi înlocuiesc datele cele mai vechi.

3.12.7 *Date privind viteza detaliată*

(116) Aparatura de înregistrare înregistrează și stochează în memoria sa de date viteza detaliată a vehiculului, precum și data și ora corespunzătoare în fiecare secundă, cel puțin pe parcursul ultimelor 24 de ore în care vehiculul a fost în mișcare.

3.12.8 *Date privind evenimentele*

În sensul prezentului paragraf, timpul se înregistrează cu o rezoluție de 1 secundă.

(117) Aparatura de înregistrare înregistrează și stochează în memoria sa de date următoarele date pentru fiecare eveniment detectat, conform următoarelor reguli de stocare:

Eveniment	Reguli de stocare	Date de înregistrat pentru fiecare eveniment
Introducerea unui card nevalabil	— cele mai recente 10 evenimente.	— data și ora evenimentului; — tipul și numărul cardului (cardurilor), statul membru emitent și generația cardului care a creat evenimentul; — numărul de evenimente similare din ziua respectivă.
Conflict de carduri	— cele mai recente 10 evenimente.	— data și ora începerii evenimentului; — data și ora încheierii evenimentului; — tipul și numărul cardului (cardurilor), statul membru emitent și generația celor două carduri care au creat conflictul.
Conducere fără un card adecvat	— evenimentul cel mai de durată survenit în fiecare din ultimele 10 zile de producere; — cele mai de durată 5 evenimente din ultimele 365 de zile;	— data și ora începerii evenimentului; — data și ora încheierii evenimentului; — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului; — numărul de evenimente similare din ziua respectivă.

Eveniment	Reguli de stocare	Date de înregistrat pentru fiecare eveniment
Introducerea cardului în timpul conducerii	— ultimul eveniment din fiecare dintre ultimele 10 zile de producere;	— data și ora evenimentului; — tipul, numărul, statul membru emitent și generația cardului (cardurilor); — numărul de evenimente similare din ziua respectivă.
Încheiere incorectă a ultimei sesiuni	— cele mai recente 10 evenimente.	— data și ora introducerii cardului; — tipul, numărul, statul membru emitent și generația cardului (cardurilor); — datele privind ultima sesiune așa cum au fost citite de pe card: — data și ora introducerii cardului; — VRN, statul membru de înmatriculare și generația VU.
Depășirea limitei de viteză (1)	— cel mai grav eveniment survenit în fiecare din ultimele 10 zile de producere (și anume, cea mai mare viteză medie înregistrată); — cele mai grave 5 evenimente survenite în ultimele 365 de zile; — primul eveniment survenit după ultima etalonare;	— data și ora începerii evenimentului; — data și ora încheierii evenimentului; — viteza maximă măsurată în cursul evenimentului; — media aritmetică a vitezei măsurate în cursul evenimentului; — tipul și numărul cardului (cardurilor), statul membru emitent și generația cardului de conducător auto (dacă este cazul); — numărul de evenimente similare din ziua respectivă.
Întreruperea alimentării cu energie electrică (2)	— evenimentul cel mai de durată din fiecare dintre ultimele 10 zile de producere; — cele mai de durată 5 evenimente din ultimele 365 de zile;	— data și ora începerii evenimentului; — data și ora încheierii evenimentului; — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului; — numărul de evenimente similare din ziua respectivă.
Eroare de comunicare cu echipamentul de comunicare la distanță	— evenimentul cel mai de durată din fiecare dintre ultimele 10 zile de producere; — cele mai de durată 5 evenimente din ultimele 365 de zile;	— data și ora începerii evenimentului; — data și ora încheierii evenimentului; — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului; — numărul de evenimente similare din ziua respectivă.
Absența informațiilor de poziționare de la receptorul GNSS	— evenimentul cel mai de durată din fiecare dintre ultimele 10 zile de producere; — cele mai de durată 5 evenimente din ultimele 365 de zile;	— data și ora începerii evenimentului; — data și ora încheierii evenimentului; — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului; — numărul de evenimente similare din ziua respectivă.

Eveniment	Reguli de stocare	Date de înregistrat pentru fiecare eveniment
Eroare privind datele de la senzorul de mișcare	— evenimentul cel mai de durată din fiecare dintre ultimele 10 zile de producere; — cele mai de durată 5 evenimente din ultimele 365 de zile;	— data și ora începerii evenimentului; — data și ora încheierii evenimentului; — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului; — numărul de evenimente similare din ziua respectivă.
Conflict privind deplasarea vehiculului	— evenimentul cel mai de durată din fiecare dintre ultimele 10 zile de producere; — cele mai de durată 5 evenimente din ultimele 365 de zile;	— data și ora începerii evenimentului; — data și ora încheierii evenimentului; — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului; — numărul de evenimente similare din ziua respectivă.
Tentativă de încălcare a securității	— cele mai recente 10 evenimente, per tip de eveniment.	— data și ora începerii evenimentului; — data și ora sfârșitului evenimentului (dacă sunt relevante); — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului; — tipul evenimentului.
Conflict oră	— evenimentul cel mai de durată din fiecare dintre ultimele 10 zile de producere; — cele mai de durată 5 evenimente din ultimele 365 de zile;	— data și ora indicate de aparatura de înregistrare; — data și ora GNSS; — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului; — numărul de evenimente similare din ziua respectivă.

(1) Aparatura de înregistrare înregistrează și stochează, de asemenea, în memoria sa de date:

— data și ora ultimului CONTROL AL DEPĂȘIRII LIMITEI DE VITEZĂ;

— data și ora primului eveniment de tip „Depășirea limitei de viteză”survenit după efectuarea respectivului CONTROL AL DEPĂȘIRII LIMITEI DE VITEZĂ.

— numărul de evenimente de tip „Depășirea limitei de viteză” survenite de la ultimul CONTROL AL DEPĂȘIRII LIMITEI DE VITEZĂ.

(2) Aceste date pot fi înregistrate numai în momentul reconectării la sursa de energie electrică, orele pot fi cunoscute cu o precizie de un minut.

3.12.9 *Date privind anomaliile*

În sensul prezentului paragraf, timpul se înregistrează cu o rezoluție de 1 secundă.

(118) Aparatura de înregistrare încearcă să înregistreze și să stocheze în memoria sa de date următoarele date pentru fiecare anomalie detectată conform următoarelor reguli de stocare:

Anomalie	Reguli de stocare	Date care trebuie înregistrate pentru fiecare anomalie
Anomalie a cardului	— cele mai recente 10 anomalii ale cardului de conducător auto.	— data și ora începerii anomaliei; — data și ora încheierii anomaliei; — tipul, numărul, statul membru emitent și generația cardului (cardurilor).
Anomalii ale aparaturii de înregistrare	— cele mai recente 10 anomalii pentru fiecare tip de anomalie; — prima anomalie survenită după ultima etalonare.	— data și ora începerii anomaliei; — data și ora încheierii anomaliei; — tipul de anomalie; — tipul, numărul și statul membru emitent al cardului (cardurilor), precum și generația oricărui card introdus la începutul și/sau la încheierea anomaliei;

3.12.10 *Date privind etalonarea*

(119) Aparatura de înregistrare înregistrează și stochează în memoria sa de date următoarele date relevante privind:

— parametrii de etalonare cunoscuți în momentul activării;

— prima sa etalonare după activare;

— prima sa etalonare după instalarea în vehiculul respectiv (identificat pe baza VIN);

— cele mai recente 20 de etalonări (dacă pe parcursul unei zile calendaristice se efectuează mai multe etalonări, nu este stocată decât ultima etalonare efectuată în ziua respectivă).

(120) Pentru fiecare dintre aceste etalonări se înregistrează următoarele date:

— scopul etalonării (activare, prima instalare, instalare, inspecție periodică);

— denumirea și adresa atelierului;

— numărul cardului de atelier, statul membru emitent al cardului și data expirării cardului;

— identificarea vehiculului;

— parametrii actualizați sau confirmați: w, k, l, dimensiunea pneurilor, reglajul limitatorului de viteză, odometrul (valorile vechi și cele noi), data și ora (valorile vechi și cele noi);

— tipurile și identificatorii tuturor sigiliilor montate.

(121) În plus, aparatura de înregistrare înregistrează și stochează în memoria sa de date capacitatea sa de a utiliza carduri de tahograf de primă generație (încă activate sau nu).

(122) Senzorul de mișcare înregistrează și stochează în memoria sa următoarele date privind instalarea senzorului de mișcare:

— prima asociere la o VU (data, ora, numărul de omologare al VU, numărul de serie al VU);

— ultima asociere la o VU (data, ora, numărul de omologare al VU, numărul de serie al VU).

(123) Echipamentul GNSS extern înregistrează și stochează în memoria sa următoarele date privind instalarea echipamentului GNSS extern:

— prima cuplare la o VU (data, ora, numărul de omologare al VU, numărul de serie al VU);

— prima cuplare la o VU (data, ora, numărul de omologare al VU, numărul de serie al VU).

3.12.11 *Date privind reglarea orei*

(124) Aparatura de înregistrare înregistrează și stochează în memoria sa de date următoarele date legate de reglările orei efectuate în modul etalonare, în afara cadrului unei etalonări normale [a se vedea definiția de la litera (f)]:

— cea mai recentă reglare a orei;

— cele mai importante 5 reglări ale orei.

(125) Pentru fiecare dintre aceste reglări ale orei se înregistrează următoarele date:

— data și ora, valoarea veche;

— data și ora, valoarea nouă;

— denumirea și adresa atelierului;

— numărul cardului de atelier, statul membru emitent al cardului și data expirării cardului.

3.12.12 *Date privind activitățile de control*

(126) Aparatura de înregistrare înregistrează și stochează în memoria sa de date următoarele date privind cele mai recente 20 de activități de control:

— data și ora controlului;

— numărul cardului de control, statul membru emitent al cardului și generația cardului;

— tipul de control (afișare și/sau imprimare și/sau descărcare din VU și/sau descărcare de pe card și/sau verificare a etalonării în trafic).

(127) Pentru descărcări se înregistrează și datele descărcate privind ziua cea mai îndepărtată și ziua cea mai recentă.

3.12.13 *Date privind blocările efectuate de societate*

(128) Aparatura de înregistrare înregistrează și stochează în memoria sa de date următoarele date privind cele mai recente 255 de blocări efectuate de societate:

— data și ora blocării;

— data și ora deblocării;

— numărul cardului de societate, statul membru emitent al cardului și generația cardului;

— denumirea și adresa societății.

Datele blocate anterior printr-un blocaj scos din memorie din cauza limitei de mai sus se consideră a nu fi blocate.

3.12.14 *Date privind activitățile de descărcare*

(129) Aparatura de înregistrare înregistrează și stochează în memoria sa de date următoarele date privind ultima descărcare de date din memorie de date pe un suport extern efectuată în modul societate sau etalonare:

— data și ora descărcării;

— numărul cardului de societate sau al cardului de atelier, statul membru emitent al cardului și generația cardului;

— denumirea societății sau a atelierului.

3.12.15 *Date privind condițiile specifice*

(130) Aparatura de înregistrare înregistrează și stochează în memoria sa de date următoarele date privind situațiile speciale:

— data și ora înregistrării;

— tipul condiției speciale.

(131) Memoria de date permite stocarea de date privind condițiile specifice timp de cel puțin 365 de zile (presupunând că pe zi se deschide și se închide în medie o condiție specifică). La epuizarea capacității de stocare, datele noi înlocuiesc datele cele mai vechi.

3.12.16 *Date privind cardul de tahograf*

(132) Aparatura de înregistrare permite stocarea următoarelor date referitoare la diferitele carduri de tahograf care au fost utilizate în VU:

— numărul și numărul de serie al cardului de tahograf;

— producătorul cardului de tahograf;

— tipul cardului de tahograf;

— versiunea cardului de tahograf.

(133) Aparatura de înregistrare permite stocarea a cel puțin 88 de astfel de înregistrări.

3.13 **Citirea de pe cardurile de tahograf**

(134) Aparatura de înregistrare permite citirea de pe cardurile de tahograf de prima și a doua generație, dacă este cazul, a datelor necesare:

— pentru a identifica tipul de card, titularul cardului, vehiculul utilizat anterior, data și ora ultimei retrageri a cardului și activitatea selectată în momentul respectiv;

— pentru a verifica dacă ultima sesiune de utilizare a cardului a fost încheiată corect;

— pentru a calcula timpul de conducere continuă, durata cumulată a pauzelor și durata cumulată a orelor de conducere ale conducătorului auto pentru săptămâna respectivă și pentru cea anterioară;

— pentru a imprima documentele necesare referitoare la datele înregistrate pe un card de conducător auto;

— pentru a descărca datele de pe un card de conducător auto pe un suport extern.

Această cerință se aplică numai cardurilor de tahograf de primă generație, dacă utilizarea acestora nu a fost invalidată de un atelier.

(135) În cazul unei erori de citire, aparatura de înregistrare încearcă din nou, de maximum trei ori, să efectueze aceeași comandă de citire, iar dacă nu reușește declară cardul deficient și nevalabil.

3.14 **Înregistrarea și stocarea pe cardurile de tahograf**

3.14.1 *Înregistrarea și stocarea pe cardurile de tahograf de primă generație;*

(136) În cazul în care utilizarea cardurilor de tahograf de primă generație nu a fost suprimată de un atelier, aparatura de înregistrare înregistrează și stochează date exact în același fel ca aparatura de înregistrare de primă generație.

(137) Aparatura de înregistrare setează „datele privind sesiunea de utilizare a cardului" pe cardul de conducător auto sau de atelier imediat după introducerea cardului.

(138) Aparatura de înregistrare actualizează datele stocate pe cardurile de conducător auto, de atelier, de societate și/sau de control valabile cu toate datele necesare relevante pentru perioada în care este introdus cardul și pentru titularul cardului. Datele stocate pe aceste carduri sunt specificate în capitolul 4.

(139) Aparatura de înregistrare actualizează datele privind activitatea conducătorului auto și locurile (după cum se specifică la punctele 4.5.3.1.9 și 4.5.3.1.11) stocate pe cardurile de conducător auto și/sau de atelier valabile cu datele privind activitatea și locurile care au fost introduse manual de titularul cardului.

(140) Toate evenimentele care nu sunt definite în aparatura de înregistrare de primă generație nu se stochează pe cardurile de conducător auto și de atelier.

(141) Actualizarea datelor de pe cardurile de tahograf se face astfel încât, atunci când este necesar din punctul de vedere al capacității de stocare a cardului din momentul respectiv, datele cele mai recente să le înlocuiască pe cele mai vechi.

(142) În cazul unei erori de scriere, aparatura de înregistrare încearcă din nou, de maximum trei ori, să efectueze aceeași comandă de scriere, iar dacă nu reușește declară cardul deficient și nevalabil.

(143) Înainte de a elibera cardul de conducător auto și după ce toate datele relevante au fost stocate pe card, aparatura de înregistrare resetează „datele privind sesiunea de utilizare a cardului".

3.14.2 *Înregistrarea și stocarea pe cardurile de tahograf de a doua generație*

(144) Cardurile de tahograf de a doua generație conțin 2 aplicații de card diferite, dintre care prima este identică cu aplicația TACHO pentru cardurile de tahograf de primă generație, iar a doua este aplicația „TACHO_G2", astfel cum este menționată la capitolul 4 și în apendicele 2.

(145) Aparatura de înregistrare setează „datele privind sesiunea de utilizare a cardului" pe cardul de conducător auto sau de atelier imediat după introducerea cardului.

(146) Aparatura de înregistrare actualizează datele stocate în cele 2 aplicații de card de pe cardurile de conducător auto, de atelier, de societate, și/sau de control valabile cu toate datele necesare relevante pentru perioada în care este introdus cardul și pentru titularul cardului. Datele stocate pe aceste carduri sunt specificate la capitolul 4.

(147) Aparatura de înregistrare actualizează datele privind activitatea conducătorului auto și pozițiile (după cum se specifică la punctele 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 și 4.5.3.2.11) stocate pe cardurile de conducător auto și/sau de atelier valabile cu datele privind activitatea și locurile care au fost introduse manual de titularul cardului.

(148) Actualizarea datelor de pe cardurile de tahograf se face astfel încât, dacă este necesar din punctul de vedere al capacității de stocare a cardului din momentul respectiv, datele cele mai recente să le înlocuiască pe cele mai vechi.

(149) În cazul unei erori de scriere, aparatul de înregistrare încearcă, de maximum trei ori, să efectueze aceeași comandă de scriere, iar dacă nu reușește declară cardul deficient și nevalabil.

(150) Înainte de a elibera cardul de conducător auto și după ce toate datele relevante au fost stocate în cele două aplicații de pe card, aparatura de înregistrare resetează „datele privind sesiunea de utilizare a cardului".

3.15 **Afișare**

(151) Afișajul include cel puțin 20 de caractere.

(152) Dimensiunile minime ale caracterelor sunt de 5 mm înălțime și 3,5 mm lățime.

(153) Afișajul trebuie să fie compatibil cu caracterele specificate în apendicele 1 capitolul 4 „Seturi de caractere”. Afișajul poate utiliza simboluri simplificate (de exemplu, caracterele cu accent pot fi afișate fără accent sau minusculele pot fi afișate ca majuscule).

(154) Afișajul este prevăzut cu iluminare corespunzătoare, fără efect de orbire.

(155) Indicațiile trebuie să fie vizibile din exteriorul aparaturii de înregistrare.

(156) Aparatura de înregistrare trebuie să poată afișa:

— date implicite;

— date privind avertismentele;

— date privind accesul la meniu;

— alte date solicitate de utilizator.

Aparatura de înregistrare poate afișa și informații suplimentare, cu condiția ca acestea să poată fi distinse în mod clar de informațiile menționate anterior.

(157) Afișajul aparaturii de înregistrare poate folosi pictogramele sau combinațiile de pictograme enumerate în apendicele 3. Aparatura de înregistrare poate afișa și pictograme sau combinații de pictograme suplimentare, cu condiția ca acestea să poată fi distinse în mod clar de pictogramele sau combinațiile de pictograme menționate anterior.

(158) Afișajul trebuie să fie întotdeauna PORNIT atunci când vehiculul este în mișcare.

(159) Aparatura de înregistrare poate include o funcție manuală sau automată care să treacă afișajul în poziția OPRIT atunci când vehiculul nu este în mișcare.

Formatul de afișare este descris în apendicele 5.

3.15.1 *Afișaj implicit*

(160) Atunci când nu este necesar să se afișeze nicio altă informație, aparatura de înregistrare afișează, implicit, următoarele:

— ora locală (ca rezultat al adunării: ora UTC + decalajul setat de conducătorul auto);

— modul de funcționare;

— activitatea conducătorului auto în momentul respectiv și activitatea copilotului în momentul respectiv,

— informații privind conducătorul auto:

— dacă activitatea curentă a acestuia este CONDUCERE, timpul de conducere continuă și durata cumulată a pauzelor în momentul respectiv;

— dacă activitatea curentă a acestuia nu este CONDUCERE, durata activității curente în cauză (începând de la selectarea acesteia) și durata cumulată a pauzelor sale în momentul respectiv.

(161) Afișarea datelor referitoare la fiecare conducător auto în parte trebuie să fie clară, simplă și lipsită de ambiguități. Dacă informațiile privind conducătorul auto și copilotul nu pot fi afișate în același timp, aparatura de înregistrare afișează implicit informațiile privind conducătorul auto și îi permite utilizatorului să afișeze informațiile privind copilotul.

(162) Dacă lățimea afișajului nu permite afișarea implicită a modului de funcționare, aparatura de înregistrare afișează, pentru scurt timp, noul mod de funcționare, în momentul oricărei modificări a acestuia.

(163) Aparatul de înregistrare afișează pentru scurt timp, la introducerea cardului, numele titularului acestuia.

(164) La deschiderea unei condiții de tip „ÎN AFARA ZONEI DE APLICARE A REGLEMENTĂRILOR" sau „TRASEU PARCURS PE FERIBOT/ÎN TREN", afișajul implicit trebuie să indice, prin intermediul pictogramei relevante, că respectiva condiție este deschisă (se acceptă posibilitatea ca activitatea curentă a conducătorului auto să nu fie indicată în același timp).

3.15.2 *Afișaj de avertizare*

(165) Aparatura de înregistrare afișează informații de avertizare folosind în primul rând pictogramele din apendicele 3, completate dacă este necesar cu informații suplimentare codate numeric. Se poate adăuga de asemenea o descriere textuală a avertismentului, în limba selectată de conducătorul auto.

3.15.3 *Accesul la meniu*

(166) Comenzile aparaturii de înregistrare sunt accesibile prin intermediul unui meniu cu structură adecvată.

3.15.4 *Alte afișaje*

(167) Următoarele informații trebuie să poată fi afișate selectiv, la cerere:

— data și ora UTC, precum și decalajul orar local;

— conținutul oricăruia dintre cele șase documente imprimate, în format identic cu al acestora;

— timpul de conducere continuă și durata cumulată a pauzelor conducătorului auto;

— timpul de conducere continuă și durata cumulată a pauzelor copilotului;

— timpul de conducere continuă al conducătorului auto pentru săptămâna în curs și pentru săptămâna anterioară;

— timpul de conducere continuă al copilotului pentru săptămâna în curs și pentru săptămâna anterioară,

opțional:

— durata activității copilotului în momentul respectiv (începând de la selectarea acesteia);

— timpul de conducere continuă al conducătorului auto pentru săptămâna în curs;

— timpul de conducere continuă al copilotului pentru programul zilnic de lucru în curs;

— timpul de conducere continuă al conducătorului auto pentru ziua de lucru în curs.

(168) Afișarea conținutului documentelor imprimate este secvențială, structurată pe rânduri. Dacă lățimea afișajului este mai mică de 24 de caractere, utilizatorul trebuie să aibă acces la informațiile complete printr-un mijloc adecvat (mai multe rânduri, derulare etc.).

Nu este obligatorie afișarea rândurilor rezervate pentru informațiile scrise de mână din documentele imprimate.

3.16 **Imprimare**

(169) Aparatura de înregistrare permite imprimarea de informații din memoria sa de date și/sau de pe cardurile de tahograf, astfel încât să se obțină următoarele șapte tipuri de documente imprimate:

— document imprimat zilnic privind activitățile conducătorului auto stocate pe card;

— document imprimat zilnic privind activitățile zilnice ale conducătorului auto stocate în unitatea montată pe vehicul;

— document imprimat privind evenimentele și anomaliile stocate pe card;

— document imprimat privind evenimentele și anomaliile stocate în unitatea montată pe vehicul;

— document imprimat privind datele tehnice;

— document imprimat privind depășirea limitei de viteză;

— istoricul datelor de pe cardul de tahograf pentru o anumită VU (a se vedea capitolul 3.12.16).

Formatul detaliat și conținutul acestor documente imprimate sunt descrise în apendicele 4.

La sfârșitul documentelor imprimate pot fi furnizate și date suplimentare.

Aparatura de înregistrare poate furniza și alte documente imprimate, cu condiția ca acestea să poată fi deosebite în mod clar de cele șapte tipuri menționate anterior.

(170) „Documentul imprimat zilnic privind activitățile conducătorului auto stocate pe card” și „documentul imprimat privind evenimentele și anomaliile stocate pe card” trebuie să fie disponibile numai atunci când în aparatura de înregistrare este introdus un card de conducător auto sau de atelier. Aparatura de înregistrare actualizează datele stocate pe cardul relevant înainte de a iniția imprimarea.

(171) Pentru a genera „documentul imprimat zilnic privind activitățile conducătorului auto stocate pe card” și „documentul imprimat privind evenimentele și anomaliile stocate pe card”, aparatura de înregistrare:

— fie selectează automat cardul de conducător auto sau cardul de atelier dacă numai unul dintre acestea a fost introdus;

— fie dispune de o comandă care permite selectarea cardului sursă sau a cardului din slotul pentru cardul de conducător auto dacă în aparatura de înregistrare au fost introduse două astfel de carduri.

(172) Imprimanta permite imprimarea a 24 de caractere pe fiecare rând.

(173) Dimensiunile minime ale caracterelor sunt de 2,1 mm înălțime și 1,5 mm lățime.

(174) Imprimanta permite utilizarea caracterelor specificate în apendicele 1 capitolul 4 „Seturi de caractere”.

(175) Imprimantele trebuie proiectate astfel încât să producă aceste documente imprimate cu o rezoluție care să elimine orice eventuală ambiguitate la citire.

(176) Documentele imprimate trebuie să își păstreze dimensiunile și înregistrările în condiții normale de umiditate (10-90 %) și de temperatură.

(177) Hârtia omologată de tip folosită de aparatura de înregistrare trebuie să fie prevăzută cu marca de omologare de tip adecvată și să conțină o indicație privind tipul sau tipurile de aparatură de înregistrare pentru care poate fi folosită.

(178) Documentele imprimate trebuie să își păstreze lizibilitatea și să poată fi identificate în condiții normale de depozitare privind intensitatea luminii, umiditatea și temperatura, timp de cel puțin doi ani.

(179) Documentele imprimate trebuie să respecte cel puțin specificațiile de testare definite în apendicele 9.

(180) De asemenea, pe aceste documente trebuie să se poată adăuga și note scrise de mână, cum ar fi semnătura conducătorului auto

(181) Aparatura de înregistrare gestionează întreruperile cauzate de terminarea hârtiei în timpul activității de imprimare, după realimentarea cu hârtie, fie reluând imprimarea de la început, fie continuând imprimarea și făcând clar referire la partea imprimată anterior.

3.17 **Avertismente**

(182) Aparatura de înregistrare trebuie să avertizeze conducătorul auto atunci când detectează orice eveniment și/sau anomalie.

(183) Este posibil ca avertismentul referitor la evenimentul „Întreruperea alimentării cu energie electrică” să fie amânat până la reconectarea la sursă de electricitate.

(184) În ceea ce privește depășirea timpului de conducere continuă maxim autorizat, aparatura de înregistrare trebuie să avertizeze conducătorul auto cu 15 minute înainte de expirarea timpului respectiv și în momentul depășirii.

(185) Avertismentele trebuie să fie vizuale. avertismentele vizuale pot fi însoțite și de avertismente sonore.

(186) Avertismentele vizuale trebuie să poată fi recunoscute în mod clar de către utilizator, trebuie să se afle în câmpul vizual al conducătorului auto și trebuie să fie perfect lizibile atât ziua cât și noaptea.

(187) Avertismentele vizuale pot fi integrate în aparatura de înregistrare și/sau pot fi externe.

(188) În cel de-al doilea caz, avertismentele trebuie să fie marcate cu simbolul „T".

(189) Avertismentele trebuie să dureze cel puțin 30 de secunde, cu excepția cazurilor când șoferul confirmă luarea lor la cunoștință prin apăsarea uneia sau mai multor taste specifice ale aparatului de înregistrare. Această primă confirmare nu anulează afișarea cauzei avertismentului descrisă la punctul următor.

(190) Cauza avertismentului trebuie afișată de aparatura de înregistrare și trebuie să rămână vizibilă până când utilizatorul confirmă luarea acesteia la cunoștință cu ajutorul unei anumite taste sau comenzi a aparaturii de înregistrare.

(191) Pot fi prevăzute și avertismente suplimentare, cu condiția ca acestea să nu poată fi confundate de conducătorii auto cu cele descrise anterior.

3.18 **Descărcarea datelor pe suporturi externe**

(192) Aparatura de înregistrare permite descărcarea la cerere a datelor din memoria sa de date sau de pe un card de conducător auto pe suporturi externe de stocare prin intermediul conectorului pentru etalonare/descărcare. Aparatura de înregistrare actualizează datele stocate pe cardul relevant înainte de a începe descărcarea.

(193) În plus, ca o caracteristică opțională, aparatura de înregistrare poate, în orice mod de funcționare, să descarce date prin orice alt mijloc către o societate autentificată prin intermediul acestui canal. În acest caz, pentru astfel de descărcări se aplică drepturile de acces la date în modul societate.

(194) Descărcarea nu modifică și nici nu șterge datele stocate.

(195) Interfața electrică a conectorului pentru etalonare/descărcare este descrisă în apendicele 6.

(196) Protocoalele de descărcare sunt descrise în apendicele 7.

3.19 **Comunicare la distanță pentru controalele selective în trafic**

(197) Atunci când motorul vehiculului este pornit, unitatea montată pe vehicul stochează, la fiecare 60 de secunde, în echipamentul de comunicare la distanță, cele mai recente date necesare pentru controalele selective în trafic. Aceste date trebuie criptate și semnate în conformitate cu indicațiile din apendicele 11 și 14.

(198) Datele de verificat de la distanță trebuie să poată fi accesate de cititoarele pentru comunicarea la distanță prin intermediul comunicării fără fir (*wireless*), în conformitate cu apendicele 14.

(199) Datele necesare în scopul controalelor selective în trafic se referă la:

— ultima tentativă de încălcare a securității;

— cea mai lungă întrerupere a alimentării cu energie electrică;

— anomalia senzorului;

— eroare privind datele de la senzorul de mișcare;

— conflict privind deplasarea vehiculului;

— conducere fără un card valabil;

— introducerea cardului în timpul conducerii;

— date privind reglarea orei;

— date de etalonare, inclusiv datele ultimelor două înregistrări de etalonare stocate;

— numărul de înmatriculare al vehiculului;

— viteza înregistrată de tahograf.

3.20 **Date de ieșire transmise unor dispozitive externe suplimentare**

(200) Aparatura de înregistrare poate fi dotată și cu interfețe standardizate care permit utilizarea în modul operațional sau în modul etalonare, de către un dispozitiv extern, a datelor înregistrate sau produse de tahograf.

În apendicele 13 este specificată și standardizată o interfață ITS opțională. Alte interfețe similare pot coexista, cu condiția să respecte pe deplin cerințele din apendicele 13 în ceea ce privește lista minimă de date, securitatea și acordul conducătorului auto.

Cerințele următoare se aplică datelor ITS puse la dispoziție prin intermediul interfeței respective:

— aceste date reprezintă un set de date existente selectate din dicționarul de date al tahografului (apendicele 1);

— un subset al acestor date selectate constituie „date cu caracter personal";

— subsetul de „date cu caracter personal" este disponibil numai dacă este activat acordul verificabil al conducătorului auto, care acceptă ca datele sale cu caracter personal să părăsească rețeaua vehiculului.

— Acordul conducătorului auto poate fi activat sau dezactivat în orice moment prin comenzile din meniu, cu condiția să fie introdus cardul de conducător auto;

— setul și subsetul de date vor fi transmise prin protocolul fără fir *Bluetooth* pe raza cabinei vehiculului, cu o rată de reîmprospătare de un minut;

— asocierea dispozitivului extern la interfața ITS va fi protejată cu ajutorul unui PIN special și aleatoriu de cel puțin patru cifre, înregistrat în fiecare unitate montată pe vehicul și disponibil prin intermediul afișajului acesteia;

— prezența interfeței ITS nu poate, în nicio situație, să perturbe sau să influențeze funcționarea corectă și securitatea unității montate pe vehicul;

Pe lângă setul de date existente selectate, considerate drept lista minimă, pot fi extrase și alte date, cu condiția să nu poată fi considerate date cu caracter personal.

Aparatura de înregistrare notifică altor echipamente externe acordul conducătorului auto.

Atunci când motorul vehiculului este PORNIT, aceste date sunt transmise în mod permanent.

(201) În scopul retrocompatibilității, tahografele pot rămâne în continuare echipate cu interfața de legătură serială menționată în anexa 1B la Regulamentul (CEE) 3821/85, astfel cum a fost modificat ultima dată. Oricum, acordul conducătorului auto este în continuare necesar în cazul în care sunt transmise date cu caracter personal.

3.21 **Etalonare**

(202) Funcția de etalonare permite:

— asocierea automată a senzorului de mișcare la VU;

— cuplarea automată a echipamentului GNSS extern la VU, dacă este cazul;

— adaptarea digitală a constantei aparaturii de înregistrare (k) la coeficientul caracteristic al vehiculului (w);

— ajustarea orei curente în cadrul perioadei de valabilitate a cardului de atelier introdus;

— ajustarea valorii curente a odometrului;

— actualizarea datelor de identificare a senzorului de mișcare stocate în memoria de date;

— actualizarea, dacă este cazul, a datelor de identificare a echipamentului GNSS extern stocate în memoria de date;

— actualizarea tipurilor și a identificatorilor tuturor sigiliilor montate;

— actualizarea sau confirmarea altor parametri cunoscuți de aparatura de înregistrare: identificarea vehiculului, w, l, dimensiunea pneurilor și reglajele limitatorului de viteză, dacă este cazul.

(203) În plus, funcția de etalonare permite anularea utilizării cardurilor de tahograf de primă generație în aparatura de înregistrare, dacă sunt îndeplinite condițiile specificate în apendicele 15.

(204) Asocierea senzorului de mișcare la VU implică cel puțin:

— actualizarea datelor privind instalarea senzorului de mișcare reținute de senzorul de mișcare (după caz);

— copierea, din senzorul de mișcare în memoria de date a VU, a datelor necesare pentru identificarea senzorului de mișcare.

(205) Cuplarea echipamentului GNSS extern la VU implică cel puțin:

— actualizarea datelor privind instalarea echipamentului GNSS extern reținute de echipamentul GNSS extern (după caz);

— copierea, din echipamentul GNSS extern în memoria de date a VU, a datelor necesare pentru identificarea echipamentului GNSS extern, inclusiv a numărului de serie al echipamentului GNSS extern.

Cuplarea este urmată de verificarea informațiilor de poziționare de la GNSS.

(206) Funcția de etalonare trebuie să permită înregistrarea datelor necesare prin intermediul conectorului pentru etalonare/descărcare, în conformitate cu protocolul de etalonare descris în apendicele 8. Funcția de etalonare permite înregistrarea datelor necesare și prin alte mijloace.

3.22 **Verificarea etalonării în trafic**

(207) Funcția de verificare a etalonării în trafic permite citirea numărului de serie al senzorului de mișcare (eventual integrat în adaptor) și a numărului de serie al echipamentului GNSS extern (atunci când este cazul), care sunt conectate la unitatea montată pe vehicul, în momentul solicitării.

(208) Această citire trebuie să fie posibilă cel puțin pe afișajul unității montate pe vehicul, prin intermediul unor comenzi aflate în meniuri.

(209) Funcția de verificare a etalonării în trafic permite, de asemenea, controlarea selecției modulului de intrare/ieșire (I/O) al liniei de semnalizare I/O de etalonare, specificat în apendicele 6, prin interfața liniei K. Acest lucru se realizează prin intermediul sesiunii „ECUAdjustmentSession”, în conformitate cu apendicele 8 secțiunea 7 Controlul impulsurilor de test – Unitatea funcțională de control al intrărilor/ieșirilor.

3.23 **Reglarea orei**

(210) Funcția de reglare a orei trebuie să permită reglarea automată a orei. În scopul reglării orei, aparatura de înregistrare utilizează două surse de măsurare a timpului: 1) ceasul intern al VU; 2) receptorul GNSS.

(211) Setarea orei ceasului intern al VU se reajustează automat la intervale de maximum 12 ore. După expirarea acestui termen și atunci când semnalul GNSS nu este disponibil, reglarea orei se realizează de îndată ce VU poate avea acces la o oră valabilă furnizată de receptorul GNSS, în funcție de condițiile de pornire a motorului vehiculului. Referința temporală pentru setarea automată a orei ceasului intern al VU se determină pe baza orei furnizate de receptorul GNSS. Dacă ora curentă diferă cu mai mult de un (1) minut față de ora furnizată de receptorul GNSS, se declanșează un eveniment de tip „Conflict oră”.

(212) Funcția de reglare a orei trebuie să permită, de asemenea, reglarea declanșată a orei curente, în modul etalonare.

3.24 **Caracteristici de performanță**

(213) Unitatea montată pe vehicul este complet operațională în intervalul de temperatură cuprins între – 20 °C și 70 °C, echipamentul GNSS extern în intervalul de temperatură cuprins între – 20 °C și 70 C, iar senzorul de mișcare în intervalul de temperatură cuprins între – 40 °C și 135 °C. Conținutul memoriei de date se păstrează până la temperaturi de – 40 °C.

(214) Tahograful trebuie să funcționeze corect într-un interval de umiditate de 10 % până la 90 %.

(215) Sigiliile utilizate în tahograful inteligent trebuie să îndeplinească aceleași condiții ca cele aplicabile componentelor tahografului de care sunt atașate.

(216) Aparatura de înregistrare trebuie protejată de supratensiune, de inversarea polarității sursei de alimentare și de scurt-circuite.

(217) Senzorii de mișcare trebuie:

— fie să reacționeze la un câmp magnetic care perturbă detectarea deplasării vehiculului. În acest caz, unitatea montată pe vehicul va înregistra și stoca o eroare a senzorului (cerința 88), fie

— să aibă un element detector protejat împotriva câmpurilor magnetice sau imun la acestea.

(218) Aparatura de înregistrare și echipamentul GNSS extern trebuie să fie conforme cu regulamentul internațional CEE-ONU R10 și protejate împotriva descărcărilor electrostatice și împotriva șocurilor de instalare.

3.25 **Materiale**

(219) Toate părțile componente ale aparaturii de înregistrare trebuie să fie confecționate din materiale suficient de stabile și cu o rezistență mecanică suficientă și să aibă caracteristici electrice și magnetice stabile.

(220) În condiții normale de utilizare, toate componentele interne al aparaturii trebuie să fie protejate de umezeală și de praf.

(221) Unitatea montată pe vehicul și echipamentul GNSS extern trebuie să respecte nivelul de protecție IP 40, iar senzorul de mișcare trebuie să respecte nivelul de protecție IP 64, conform standardului IEC 60529:1989, inclusiv A1:1999 și A2:2013.

(222) Aparatura de înregistrare trebuie să respecte specificațiile tehnice aplicabile în domeniul proiectării ergonomice.

(223) Aparatura de înregistrare trebuie să fie protejată împotriva deteriorărilor accidentale.

3.26 **Inscripții**

(224) Dacă aparatura de înregistrare afișează valoarea odometrului și viteza vehiculului, pe afișajul său apar următoarele detalii:

— lângă cifra care indică distanța, unitatea de măsură a distanței, indicată prin abrevierea „km”;

— lângă cifra care indică viteza, indicația „km/h”.

Aparatura de înregistrare poate fi comutată astfel încât să afișeze viteza în mile pe oră, în acest caz unitatea de măsură a vitezei fiind indicată prin abrevierea „mph”. Aparatura de înregistrare poate fi comutată astfel încât să afișeze distanța în mile, în acest caz unitatea de măsură a distanței fiind indicată prin abrevierea „mi”.

(225) Pe fiecare componentă separată a aparaturii de înregistrare se atașează o plăcuță descriptivă care conține următoarele detalii:

— numele și adresa producătorului aparaturii;

— numărul de componentă furnizat de producător și anul de fabricație al aparaturii;

— numărul de serie al aparaturii;

— marca de omologare pentru tipul de aparatură.

(226) Dacă spațiul fizic nu este suficient pentru afișarea tuturor detaliilor menționate anterior, plăcuța descriptivă trebuie să conțină cel puțin: numele și sigla producătorului și numărul de componentă al aparaturii.

4. CERINȚE FUNCȚIONALE ȘI DE CONSTRUCȚIE PENTRU CARDURILE DE TAHOGRAF

4.1 **Date vizibile**

Pe recto figurează:

(227) cuvintele „Card de conducător auto” sau „Card de control” sau „Card de atelier” sau „Card de societate”, tipărite cu majuscule în limba sau limbile oficiale ale statului membru emitent, în funcție de tipul cardului;

(228) denumirea statului membru emitent al cardului (opțional);

(229) indicativul statului membru emitent al cardului, tipărit în negativ într-un dreptunghi albastru și înconjurat de 12 stele galbene. Indicativele sunt următoarele:

B	Belgia	LV	Letonia
BG	Bulgaria	L	Luxemburg
CZ	Republica Cehă	LT	Lituania
CY	Cipru	M	Malta
DK	Danemarca	NL	Țările de Jos

D EST	Germania Estonia	A PL	Austria Polonia
GR	Grecia	P RO SK SLO	Portugalia România Slovacia Slovenia
E	Spania	FIN	Finlanda
F HR H	Franța Croația Ungaria	S	Suedia
IRL	Irlanda	UK	Regatul Unit
I	Italia		

(230) informații specifice pentru cardul emis, numerotate după cum urmează:

	Card de conducător auto	Card de control	Card de societate sau card de atelier
1.	numele conducătorului auto	denumirea organismului de control	denumirea societății sau a atelierului.
2.	prenumele conducătorului auto	numele agentului de control (dacă este cazul)	numele titularului cardului (dacă este cazul)
3.	data nașterii conducătorului auto	prenumele agentului de control (dacă este cazul)	prenumele titularului cardului (dacă este cazul)
4.a	data de la care este valabil cardul		
4.b	data expirării cardului		
4.c	denumirea autorității emitente (poate fi imprimată pe verso)		
4.d	un număr diferit de cel de la rubrica 5, în scop administrativ (opțional)		
5. a	numărul permisului de conducere (la data emiterii cardului de conducător auto)	—	—
5. b	numărul cardului		
6.	fotografia conducătorului auto	fotografia agentului de control (opțional)	fotografia montatorului (opțional)-

	Card de conducător auto	Card de control	Card de societate sau card de atelier
7.	Semnătura titularului (opțional)		
8.	Adresa oficială sau adresa poștală a titularului (opțional)	Adresa poștală a organismului de control	Adresa poștală a societății sau a atelierului

(231) datele se scriu în format „zz/ll/aaaa” sau „zz.ll.aaaa” (zi, lună, an).

Pe verso figurează:

(232) explicații pentru elementele numerotate de pe recto-ul cardului;

(233) cu acordul special al titularului, exprimat în scris, pot fi adăugate informații care nu sunt legate de administrarea cardului, dar acestea nu trebuie să modifice în niciun fel utilizarea modelului drept card de tahograf.

(234) Cardurile de tahograf se imprimă pe fonduri având următoarele culori predominante:

— cardul de conducător auto: alb;

— cardul de control: albastru;

— cardul de atelier: roșu;

— cardul de societate: galben.

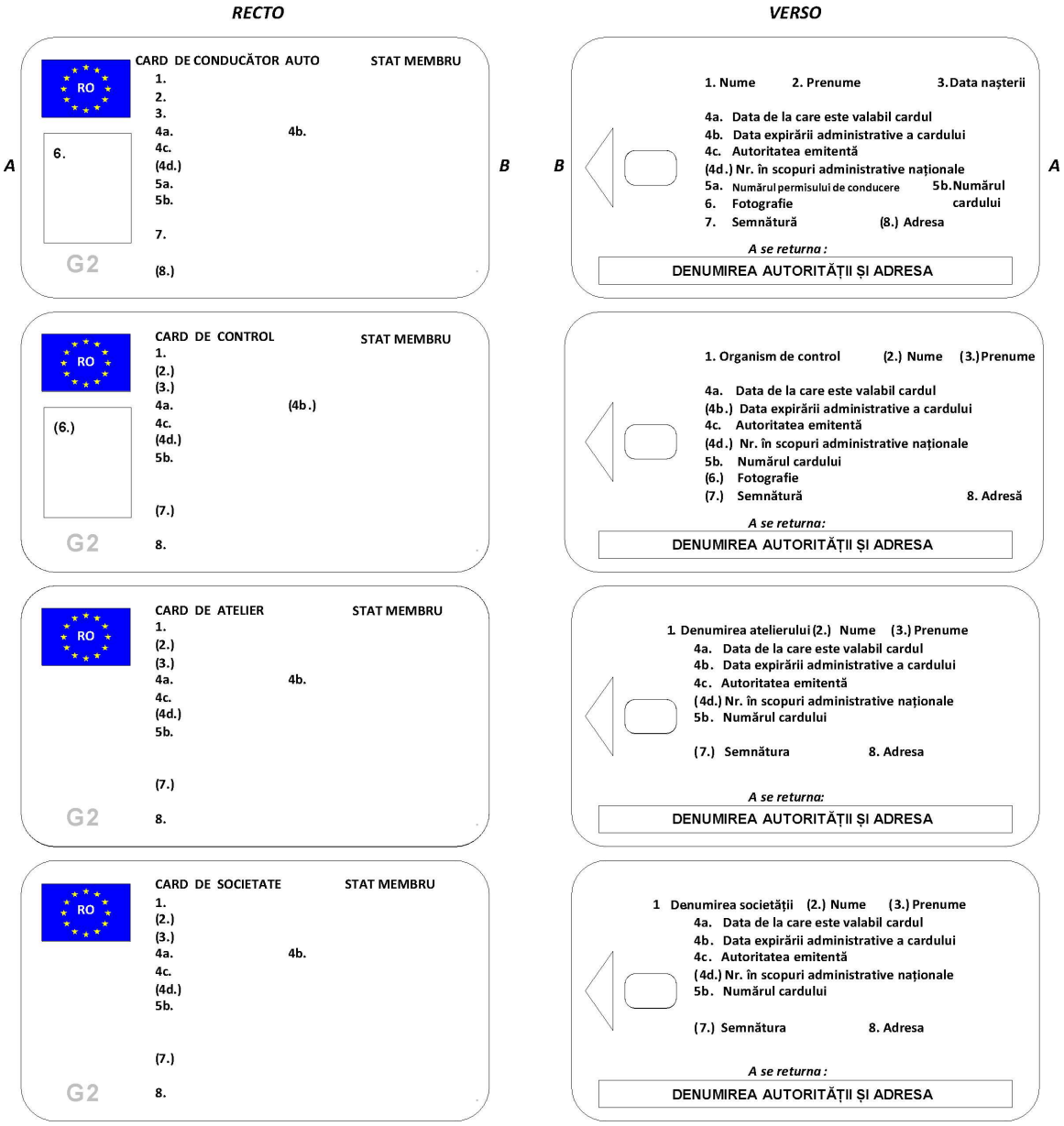
(235) Cardurile de tahograf trebuie să aibă cel puțin următoarele caracteristici pentru protecția corpului cardului împotriva falsificării și a manipulării neadecvate:

— un fond de securitate cu ghioșe și irizat;

— în zona fotografiei, fondul de securitate și fotografia se suprapun;

— cel puțin o linie bicoloră microimprimată.

MODELE DE CARDURI DE TAHOGRAF UTILIZATE ÎN UNIUNE



(236) După consultarea Comisiei, statele membre pot adăuga culori sau inscripții cum ar fi simboluri naționale sau caracteristici de securitate, fără a aduce atingere celorlalte dispoziții din prezenta anexă.

(237) Cardurile temporare menționate la articolul 26 alineatul (4) din Regulamentul (UE) nr.165/2014 trebuie să respecte dispozițiile prezentei anexe.

4.2 **Securitate**

Scopul securității sistemului este de a proteja integritatea și autenticitatea datelor schimbate între carduri și aparatura de înregistrare, de a proteja integritatea și autenticitatea datelor descărcate de pe carduri, de a permite aparaturii de înregistrare să efectueze numai anumite operațiuni de scriere pe carduri, de a decripta anumite date, de a elimina orice posibilitate de falsificare a datelor stocate pe carduri, de a preveni manipulările neadecvate și de a detecta orice tentativă de acest gen.

(238) Pentru a asigura securitatea sistemului, cardurile de tahograf trebuie să îndeplinească cerințele de securitate definite în apendicele 10 și 11.

(239) Cardurile de tahograf trebuie să poată fi citite și de alte echipamente, cum ar fi computerele personale.

4.3 **Standarde**

(240) Cardurile de tahograf trebuie să respecte următoarele standarde:

— ISO/IEC 7810 Identification cards – Physical characteristics;

— ISO/IEC 7816 Identification cards – Integrated circuit cards:

— Part 1: Physical characteristics,

— Part 2: Dimensions and position of the contacts (ISO/IEC 7816-2:2007),

— Part 3: Electrical interface and transmission protocols (ISO/IEC 7816-3:2006),

— Part 4: Organisation, security and commands for interchange (ISO/IEC 7816-4:2013 + Cor 1:2014),

— Part 6: Interindustry data elements for interchange (ISO/IEC 7816-6:2004 + Cor 1:2006),

— Part 8: Commands for security operations (ISO/IEC 7816-8:2004).

— Cardurile de tahograf se testează în conformitate cu standardul ISO/IEC 10373-3:2010 Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices.

4.4 **Specificații de mediu și electrice**

(241) Cardurile de tahograf pot funcționa corect în toate condițiile climatice întâlnite în mod normal pe teritoriul Uniunii și cel puțin în intervalul de temperatură cuprins între – 25 °C și + 70 °C, cu creșteri ocazionale ale temperaturii de până la + 85 °C; „ocazional" înseamnă timp de cel mult 4 ore o dată și de cel mult 100 de ori pe întreaga durată de viață a cardului.

(242) Cardurile de tahograf pot funcționa corect în intervalul de umiditate cuprins între 10 % și 90 %.

(243) Cardurile de tahograf pot funcționa corect timp de cinci ani dacă sunt folosite conform specificațiilor de mediu și electrice.

(244) În cursul funcționării, cardurile de tahograf respectă Regulamentul CEE-ONU R10, referitor la compatibilitatea electromagnetică, și sunt protejate împotriva descărcărilor electrostatice.

4.5 **Stocarea datelor**

În sensul prezentului alineat,

— orele sunt înregistrate cu o rezoluție de un minut, cu excepția cazurilor în care se specifică altfel;

— valorile odometrului sunt înregistrate cu o rezoluție de un kilometru;

— vitezele sunt înregistrate cu o rezoluție de 1 km/h;

— pozițiile (latitudinile și longitudinile) sunt înregistrate în grade și minute, cu o rezoluție de 1/10 de minut.

Funcțiile, comenzile și structurile logice ale cardurilor de tahograf care îndeplinesc cerințele de stocare a datelor sunt menționate în apendicele 2.

În absența unor dispoziții contrare, stocarea datelor pe cardurile de tahograf trebuie organizată astfel încât datele noi să înlocuiască datele cele mai vechi în cazul epuizării capacității prevăzute a memoriei destinate anumitor înregistrări.

(245) Prezentul paragraf stabilește capacitatea minimă de stocare pentru diversele fișiere de date pentru aplicații. Cardurile de tahograf trebuie să poată transmite aparaturii de înregistrare capacitatea de stocare din momentul respectiv a respectivelor fișiere de date.

(246) Orice date suplimentare care pot fi stocate pe cardurile de tahograf, referitoare la alte eventuale aplicații existente pe card, se stochează în conformitate cu Directiva 95/46/CE, cu Directiva 2002/58/CE și cu articolul 7 din Regulamentul (UE) nr. 165/2014.

(247) Fiecare fișier principal (MF – *Master File*) al unui card de tahograf conține până la cinci fișiere de bază (EF – *Elementary Files*) pentru gestionarea cardului și pentru identificarea aplicațiilor și a cipurilor, precum și două fișiere speciale (DF – *Dedicated Files*):

— DF Tachograph, care conține aplicația accesibilă pentru unitățile montate pe vehicul de primă generație, prezentă și pe cardurile de tahograf de primă generație;

— DF Tachograph_G2, care conține aplicația accesibilă numai pentru unitățile montate pe vehicul de a doua generație, prezentă numai pe cardurile de tahograf de a doua generație.

Detaliile complete ale structurii cardurilor de tahograf sunt specificate în apendicele 2.

4.5.1 *Fișierele elementare pentru identificare și pentru gestionarea cardului*

4.5.2 *Identificarea cardurilor cu circuite integrate (IC)*

(248) Cardurile de tahograf permit stocarea următoarelor date de identificare a cardurilor inteligente:

— *clock stop*;

— numărul de serie al cardului (inclusiv referințele de fabricație);

— numărul de omologare de tip al cardului;

— ID-ul de personalizare a cardului;

— ID-ul integratorului;

— identificatorul circuitului integrat (IC).

4.5.2.1 Identificarea cipului

(249) Cardurile de tahograf permit stocarea următoarelor date de identificare a circuitelor integrate (IC):

— numărul de serie al IC;

— referințele de fabricație ale IC.

4.5.2.2 DIR (prezent numai pe cardurile de tahograf de a doua generație)

(250) Cardurile de tahograf permit stocarea obiectelor de date pentru identificarea aplicației, specificate în apendicele 2.

4.5.2.3 Informații RLR (în anumite condiții, prezente numai pe cardurile de tahograf de a doua generație)

(251) Cardurile de tahograf permit stocarea următorului obiect de date informativ cu lungime extinsă:

— în cazul în care cardul de tahograf utilizează câmpuri cu lungime extinsă, obiectul de date informativ cu lungime extinsă specificat în apendicele 2.

4.5.2.4 Informații privind lungimea extinsă (în anumite condiții, prezente numai pe cardurile de tahograf de a doua generație)

(252) Cardurile de tahograf permit stocarea următoarelor obiecte de date informative cu lungime extinsă:

— în cazul în care cardul de tahograf utilizează câmpuri cu lungime extinsă, obiectele de date informative cu lungime extinsă specificate în apendicele 2.

4.5.3 *Cardul de conducător auto*

4.5.3.1 Aplicație pentru tahograf (accesibilă pentru unitățile montate pe vehicul de prima și a doua generație)

4.5.3.1.1 Identificarea aplicației

(253) Cardul de conducător auto permite stocarea următoarelor date de identificare a aplicației:

— identificarea aplicației pentru tahograf;

— identificarea tipului de card de tahograf.

4.5.3.1.2 Chei și certificate

(254) Cardul de conducător auto permite stocarea unei serii de chei și certificate criptografice, în conformitate cu apendicele 11 partea A.

4.5.3.1.3 Identificarea cardului

(255) Cardul de conducător auto permite stocarea următoarelor date de identificare a cardului:

— numărul cardului;

— statul membru emitent, denumirea autorității emitente, data emiterii;

— data de la care este valabil cardul, data expirării cardului.

4.5.3.1.4 Identificarea titularului cardului

(256) Cardul de conducător auto permite stocarea următoarelor date de identificare a titularului cardului:

— numele titularului;

— prenumele titularului;

— data nașterii;

— limba preferată de titular.

4.5.3.1.5 Descărcarea informațiilor de pe card

(257) Cardul de conducător auto permite stocarea următoarelor date legate de descărcarea informațiilor de pe card:

— data și ora la care s-a efectuat ultima descărcare a informațiilor de pe card (în alte scopuri decât în vederea unui control).

(258) Cardul de conducător auto permite stocarea unei singure astfel de înregistrări.

4.5.3.1.6 Informații privind permisul de conducere

(259) Cardul de conducător auto permite stocarea următoarelor date privind permisul de conducere:

— statul membru emitent, denumirea autorității emitente;

— numărul permisului de conducere (la data emiterii cardului).

4.5.3.1.7 Date privind evenimentele

În sensul prezentului paragraf, ora se înregistrează cu o rezoluție de 1 secundă.

(260) Cardul de conducător auto permite stocarea de date legate de următoarele evenimente detectate de aparatura de înregistrare în perioada în care cardul este introdus:

— suprapunere a timpului (dacă evenimentul este provocat de cardul respectiv);

— introducerea cardului în timpul conducerii (dacă evenimentul afectează cardul respectiv);

— încheierea incorectă a ultimei sesiuni de utilizare a cardului (dacă evenimentul afectează cardul respectiv);

— întreruperea alimentării cu energie electrică;

— eroare privind datele de la senzorul de mișcare;

— tentative de încălcare a securității.

(261) Cardul de conducător auto permite stocarea următoarelor date privind aceste evenimente:

— codul evenimentului;

— data și ora începerii evenimentului (sau a introducerii cardului dacă evenimentul era în curs la momentul respectiv);

— data și ora încheierii evenimentului (sau a retragerii cardului dacă evenimentul era în curs la momentul respectiv);

— VRN și statul membru de înmatriculare a vehiculului afectat de eveniment.

Notă: Pentru evenimentul „Suprapunere a timpului”:

— data și ora începerii evenimentului trebuie să corespundă datei și orei retragerii cardului din vehiculul precedent;

— data și ora încheierii evenimentului trebuie să corespundă datei și orei introducerii cardului în vehiculul folosit la momentul respectiv;

— datele privind vehiculul trebuie să corespundă vehiculului din momentul respectiv (cel care a declanșat evenimentul).

Notă: Pentru evenimentul: „Încheiere incorectă a ultimei sesiuni de utilizare a cardului”:

— data și ora începerii evenimentului trebuie să corespundă datei și orei de introducere a cardului pentru sesiunea care nu a fost încheiată corect;

— data și ora încheierii evenimentului trebuie să corespundă datei și orei introducerii cardului pentru sesiunea în cursul căreia a fost detectat evenimentul (sesiunea din momentul respectiv);

— datele privind vehiculul trebuie să corespundă vehiculului în care s-a desfășurat sesiunea care nu a fost încheiată corect.

(262) Cardul de conducător auto permite stocarea de date privind cele mai recente șase evenimente din fiecare tip (și anume, 36 de evenimente).

4.5.3.1.8 Date privind anomaliile

În sensul prezentului paragraf, ora se înregistrează cu o rezoluție de 1 secundă.

(263) Cardul de conducător auto permite stocarea de date privind următoarele anomalii detectate de aparatura de înregistrare în timp ce cardul este introdus:

— anomalie a cardului (dacă anomalia afectează cardul);

— anomalie a aparaturii de înregistrare.

(264) Cardul de conducător auto permite stocarea următoarelor date privind aceste anomalii:

— codul anomaliei;

— data și ora începerii anomaliei (sau a introducerii cardului dacă anomalia era în curs la momentul respectiv);

— data și ora încheierii anomaliei (sau a retragerii cardului dacă anomalia era în curs la momentul respectiv);

— VRN și statul membru de înmatriculare a vehiculului afectat de anomalie.

(265) Cardul de conducător auto permite stocarea de date privind cele mai recente douăsprezece anomalii din fiecare tip (și anume, 24 de anomalii).

4.5.3.1.9 Date privind activitatea conducătorului auto

(266) Cardul de conducător auto permite stocarea, pentru fiecare zi calendaristică în care a fost folosit cardul sau pentru care conducătorul auto a introdus manual activități, următoarelor informații:

— data;

— un contor de prezență zilnică (a cărui valoare crește cu o unitate pentru fiecare dintre zilele calendaristice respective);

— distanța totală parcursă de conducătorul auto în decursul zilei respective;

— regimul de conducere la ora 00.00;

— în cazul oricăror modificări ale activității conducătorului auto și/sau ale regimului de conducere și/sau ale oricărei introduceri sau retrageri a cardului de conducător auto:

— regimul de conducere (ECHIPAJ, SINGUR);

— slotul (CONDUCĂTOR AUTO, COPILOT);

— starea cardului (INTRODUS, NEINTRODUS);

— activitatea (CONDUCERE, DISPONIBILITATE, MUNCĂ, PAUZĂ/ODIHNĂ);

— ora modificării.

(267) Memoria cardului de conducător auto permite stocarea de date privind activitățile conducătorului auto timp de cel puțin 28 de zile (activitatea medie a unui conducător auto este definită ca incluzând 93 de schimbări de activitate pe zi).

(268) Datele enumerate la cerințele 261, 264 și 266 se stochează astfel încât să permită extragerea activităților în ordinea desfășurării lor, chiar și în cazul unei suprapuneri a timpului.

4.5.3.1.10 Date privind vehiculele utilizate

(269) Cardul de conducător auto permite stocarea, pentru fiecare zi calendaristică în care a fost utilizat cardul și pentru fiecare perioadă de utilizare a unui anumit vehicul din ziua respectivă (o perioadă de utilizare include toate ciclurile consecutive de introducere/retragere a cardului desfășurate în vehiculul respectiv, din punctul de vedere al cardului), a următoarelor date:

— data și ora primei utilizări a vehiculului (și anume, prima introducere a cardului pentru respectiva perioadă de utilizare, sau ora 00.00 dacă perioada de utilizare este în curs la ora respectivă);

— valoarea indicată de odometrul vehiculului în momentul respectiv;

— data și ora ultimei utilizări a vehiculului (și anume,ultima retragere a cardului pentru respectiva perioadă de utilizare sau ora 23:59 dacă perioada de utilizare este în curs la ora respectivă);

— valoarea indicată de odometrul vehiculului în momentul respectiv;

— VRN și statul membru de înmatriculare a vehiculului.

(270) Cardul de conducător auto permite stocarea a cel puțin 84 de astfel de înregistrări.

4.5.3.1.11 Locurile în care încep și/sau se încheie zilele de lucru

(271) Cardul de conducător auto permite stocarea următoarelor date privind locurile în care încep și/sau se încheie zilele de lucru, introduse de conducătorul auto:

— data și ora introducerii (sau data/ora legate de introducerea datelor, dacă aceasta se efectuează pe parcursul procedurii de introducere manuală);

— tipul datelor introduse (început sau sfârșit, condiția introducerii);

— țara și regiunea introduse;

— valoarea indicată de odometrul vehiculului.

(272) Memoria cardului de conducător auto permite stocarea a cel puțin 42 de perechi de astfel de înregistrări.

4.5.3.1.12 Date privind sesiunile de utilizare a cardului

(273) Cardul de conducător auto permite stocarea următoarelor date privind vehiculul în care a fost deschisă sesiunea în curs:

— data și ora deschiderii sesiunii (și anume, ale introducerii cardului), cu o rezoluție de o secundă;

— VRN și statul membru de înmatriculare.

4.5.3.1.13 Date privind activitățile de control

(274) Cardul de conducător auto permite stocarea următoarelor date privind activitățile de control:

— data și ora controlului;

— numărul cardului de control și statul membru emitent;

— tipul controlului [afișare și/sau imprimare și/sau descărcare din VU și/sau de pe card (a se vedea nota)];

— perioada descărcată, dacă a avut loc o descărcare;

— VRN și statul membru de înmatriculare a vehiculului controlat.

Notă: descărcarea informațiilor de pe card va fi înregistrată numai dacă se realizează prin intermediul unei aparaturi de înregistrare.

(275) Cardul de conducător auto permite stocarea unei singure astfel de înregistrări.

4.5.3.1.14 Date privind condițiile specifice

(276) Cardul de conducător auto permite stocarea următoarelor date legate de condițiile specifice introduse în timp ce cardul este introdus (indiferent de slot):

— data și ora introducerii;

— tipul de condiție specifică.

(277) Cardul de conducător auto permite stocarea a cel puțin 56 de astfel de înregistrări.

4.5.3.2 Aplicație pentru tahograf de a 2-a generație (inaccesibilă unităților montate pe vehicul de primă generație)

4.5.3.2.1 Identificarea aplicației

(278) Cardul de conducător auto permite stocarea următoarelor date de identificare a aplicației:

— identificarea aplicației pentru tahograf;

— identificarea tipului de card de tahograf.

4.5.3.2.2 Chei și certificate

(279) Cardul de conducător auto permite stocarea unei serii de chei și certificate criptografice, în conformitate cu apendicele 11 partea B.

4.5.3.2.3 Identificarea cardului

(280) Cardul de conducător auto permit stocarea următoarelor date de identificare a cardului:

— numărul cardului;

— statul membru emitent, denumirea autorității emitente, data emiterii;

— data de la care este valabil cardul, data expirării cardului.

4.5.3.2.4 Identificarea titularului cardului

(281) Cardul de conducător auto permite stocarea următoarelor date de identificare a titularului cardului:

— numele titularului;

— prenumele titularului;

— data nașterii;

— limba preferată de titular.

4.5.3.2.5 Descărcarea informațiilor de pe card

(282) Cardul de conducător auto permite stocarea următoarelor date legate de descărcarea informațiilor de pe card:

— data și ora la care s-a efectuat ultima descărcare a informațiilor de pe card (în alte scopuri decât în vederea unui control).

(283) Cardul de conducător auto permite stocarea unei singure astfel de înregistrări.

4.5.3.2.6 Informații privind permisul de conducere

(284) Cardul de conducător auto permite stocarea următoarelor date privind permisul de conducere:

— statul membru emitent, denumirea autorității emitente;

— numărul permisului de conducere (la data emiterii cardului).

4.5.3.2.7 Date privind evenimentele

În sensul prezentului paragraf, ora se înregistrează cu o rezoluție de 1 secundă.

(285) Cardul de conducător auto permite stocarea de date legate de următoarele evenimente detectate de aparatura de înregistrare în timp ce cardul este introdus:

— suprapunere a timpului (dacă evenimentul este provocat de cardul respectiv);

— introducerea cardului în timpul conducerii (dacă evenimentul afectează cardul respectiv);

— încheierea incorectă a ultimei sesiuni de utilizare a cardului (dacă evenimentul afectează cardul respectiv);

— întreruperea alimentării cu energie electrică;

— eroare de comunicare cu echipamentul de comunicare la distanță;

— evenimentul „Absența informațiilor de poziționare de la receptorul GNSS”;

— eroare de comunicare cu echipamentul GNSS extern;

— eroare privind datele de la senzorul de mișcare;

— conflict privind deplasarea vehiculului;

— tentative de încălcare a securității;

— conflict de oră.

(286) Cardul de conducător auto permite stocarea următoarelor date privind aceste evenimente:

— codul evenimentului;

— data și ora începerii evenimentului (sau a introducerii cardului dacă evenimentul era în curs la momentul respectiv);

— data și ora încheierii evenimentului (sau a retragerii cardului dacă evenimentul era în curs la momentul respectiv);

— VRN și statul membru de înmatriculare a vehiculului afectat de eveniment.

Notă: Pentru evenimentul „Suprapunere a timpului”:

— data și ora începerii evenimentului trebuie să corespundă datei și orei retragerii cardului din vehiculul precedent;

— data și ora încheierii evenimentului trebuie să corespundă datei și orei introducerii cardului în vehiculul utilizat la momentul respectiv;

— datele privind vehiculul trebuie să corespundă vehiculului din momentul respectiv (cel care a declanșat evenimentul).

Notă: Pentru evenimentul: „Încheiere incorectă a ultimei sesiuni de utilizare a cardului”:

— data și ora începerii evenimentului trebuie să corespundă datei și orei de introducere a cardului pentru sesiunea care nu a fost încheiată corect;

— data și ora încheierii evenimentului trebuie să corespundă datei și orei introducerii cardului pentru sesiunea pe parcursul căreia a fost detectat evenimentul (sesiunea din momentul respectiv);

— datele privind vehiculul trebuie să corespundă vehiculului în care s-a desfășurat sesiunea care nu a fost încheiată corect.

(287) Cardul de conducător auto permite stocarea de date privind cele mai recente șase evenimente din fiecare tip (și anume, 66 de evenimente).

4.5.3.2.8 Date privind anomaliile

În sensul prezentului paragraf, ora se înregistrează cu o rezoluție de 1 secundă.

(288) Cardul de conducător auto permite stocarea de date privind următoarele anomalii detectate de aparatura de înregistrare în timp ce cardul este introdus:

— anomalie a cardului (dacă anomalia afectează cardul);

— anomalie a aparaturii de înregistrare.

(289) Cardul de conducător auto permite stocarea următoarelor date privind aceste anomalii:

— codul anomaliei;

— data și ora începerii anomaliei (sau a introducerii cardului dacă anomalia era în curs la momentul respectiv);

— data și ora încheierii anomaliei (sau a retragerii cardului dacă anomalia era în curs la momentul respectiv);

— VRN și statul membru de înmatriculare a vehiculului afectat de anomalie.

(290) Cardul de conducător auto permite stocarea de date privind cele mai recente douăsprezece anomalii din fiecare tip (și anume, 24 de anomalii).

4.5.3.2.9 Date privind activitatea conducătorului auto

(291) Cardul de conducător auto permite stocarea, pentru fiecare zi calendaristică în care a fost folosit cardul sau pentru care conducătorul auto a introdus manual activități, următoarelor informații:

— data;

— un contor de prezență zilnică (a cărui valoare crește cu o unitate pentru fiecare dintre zilele calendaristice respective);

— distanța totală parcursă de conducătorul auto în cursul zilei respective;

— regimul de conducere la ora 00.00;

— în cazul oricăror modificări ale activității conducătorului auto și/sau ale regimului de conducere și/sau ale oricărei introduceri sau retrageri a cardului de conducător auto:

— regimul de conducere (ECHIPAJ, SINGUR);

— slotul (CONDUCĂTOR AUTO, COPILOT);

— starea cardului (INTRODUS, NEINTRODUS);

— activitatea (CONDUCERE, DISPONIBILITATE, MUNCĂ, PAUZĂ/ODIHNĂ);

— ora modificării.

(292) Memoria cardului de conducător auto permite stocarea de date privind activitățile conducătorului auto timp de cel puțin 28 de zile (activitatea medie a unui conducător auto este definită ca incluzând 93 de schimbări de activitate pe zi).

(293) Datele enumerate la cerințele 286, 289 și 291 se stochează astfel să permită extragerea activităților în ordinea desfășurării lor, chiar și în cazul unei suprapuneri a timpului.

4.5.3.2.10 Date privind vehiculele folosite

(294) Cardul de conducător auto permite stocarea, pentru fiecare zi calendaristică în care a fost utilizat cardul și pentru fiecare perioadă de utilizare a unui anumit vehicul din ziua respectivă (o perioadă de utilizare include toate ciclurile consecutive de introducere/retragere a cardului desfășurate în vehiculul respectiv, din punctul de vedere al cardului), a următoarelor date:

— data și ora primei utilizări a vehiculului (și anume, prima introducere a cardului pentru respectiva perioadă de utilizare, sau ora 00.00 dacă perioada de utilizare este în curs la ora respectivă);

— valoarea indicată de odometrul vehiculului la ora respectivă a primei utilizări;

— data și ora ultimei utilizări a vehiculului (și anume, ultima retragere a cardului pentru respectiva perioadă de utilizare sau ora 23:59 dacă perioada de utilizare este în curs la ora respectivă);

— valoarea indicată de odometrul vehiculului la ora respectivă a ultimei utilizări;

— VRN și statul membru de înmatriculare a vehiculului;

— VIN al vehiculului respectiv.

(295) Cardul de conducător auto permite stocarea a cel puțin 84 de astfel de înregistrări.

4.5.3.2.11 Locurile și pozițiile în care încep și/sau se încheie zilele de lucru

(296) Cardul de conducător auto permite stocarea următoarelor date privind locurile în care încep și/sau se încheie zilele de lucru, introduse de conducătorul auto:

— data și ora introducerii (sau data/ora legate de introducerea datelor, dacă aceasta se efectuează pe parcursul procedurii de introducere manuală);

— tipul introducerii (început sau sfârșit, condiția introducerii);

— țara și regiunea introduse;

— valoarea indicată de odometrul vehiculului;

— poziția vehiculului;

— precizia GNSS, data și ora determinării poziției.

(297) Memoria cardului de conducător auto permite stocarea a cel puțin 84 de perechi de astfel de înregistrări.

4.5.3.2.12 Date privind sesiunile de utilizare a cardului

(298) Cardul de conducător auto permite stocarea următoarelor date privind vehiculul în care a fost deschisă sesiunea în curs:

— data și ora deschiderii sesiunii (și anume, a introducerii cardului), cu o rezoluție de o secundă;

— VRN și statul membru de înmatriculare.

4.5.3.2.13 Date privind activitățile de control

(299) Cardul de conducător auto permite stocarea următoarelor date privind activitățile de control:

— data și ora controlului;

— numărul cardului de control și statul membru emitent;

— tipul controlului [afișare și/sau imprimare și/sau descărcare din VU și/sau de pe card (a se vedea nota)];

— perioada descărcată, dacă a avut loc o descărcare;

— VRN și statul membru de înmatriculare a vehiculului controlat.

Notă: cerințele de securitate impun ca descărcarea de pe card să poată fi înregistrată numai dacă se realizează prin intermediul unei aparaturi de înregistrare.

(300) Cardul de conducător auto permite stocarea unei singure astfel de înregistrări.

4.5.3.2.14 Date privind condițiile specifice

(301) Cardul de conducător auto permite stocarea următoarelor date legate de condițiile specifice introduse în timp ce cardul este introdus (indiferent de slot):

— data și ora introducerii;

— tipul de condiție specifică.

(302) Cardul de conducător auto permite stocarea a cel puțin 56 de astfel de înregistrări.

4.5.3.2.15 Date privind unitățile montate pe vehicul utilizate

(303) Cardul de conducător auto permite stocarea următoarelor date referitoare la diferitele unități montate pe vehicul în care a fost utilizat cardul:

— data și ora începerii perioadei utilizare a unității montate pe vehicul (și anume, prima introducere a cardului în unitatea montată pe vehicul pentru perioada respectivă);

— numele producătorului unității montate pe vehicul;

— tipul de unitate montată pe vehicul;

— numărul versiunii software-ului unității montate pe vehicul.

(304) Cardul de conducător auto permite stocarea a cel puțin 84 de astfel de înregistrări.

4.5.3.2.16 Date privind locurile în care se încheie o perioadă de conducere continuă de trei ore

(305) Cardul de conducător auto permite stocarea următoarelor date legate de poziția vehiculului atunci când timpul de conducere continuă al conducătorului auto atinge un multiplu de trei ore:

— data și ora la care timpul de conducere continuă al titularului cardului atinge un multiplu de trei ore;

— poziția vehiculului;

— precizia GNSS, data și ora determinării poziției.

(306) Cardul de conducător auto permite stocarea a cel puțin 252 de astfel de înregistrări.

4.5.4 *Cardul de atelier*

4.5.4.1 Aplicație pentru tahograf (accesibilă pentru unitățile montate pe vehicul de prima și a doua generație)

4.5.4.1.1 Identificarea aplicației

(307) Cardul de atelier permite stocarea următoarelor date de identificare a aplicației:

— identificarea aplicației pentru tahograf;

— identificarea tipului de card de tahograf.

4.5.4.1.2 Chei și certificate

(308) Cardul de atelier permite stocarea unei serii de chei și certificate criptografice, în conformitate cu apendicele 11 partea A.

(309) Cardul de atelier permite stocarea unui număr de identificare personal (cod PIN).

4.5.4.1.3 Identificarea cardului

(310) Cardul de atelier permite stocarea următoarelor date de identificare a cardului:

— numărul cardului;

— statul membru emitent, denumirea autorității emitente, data emiterii;

— data de la care este valabil cardul, data expirării cardului.

4.5.4.1.4 Identificarea titularului cardului

(311) Cardul de atelier permite stocarea următoarelor date de identificare a titularului cardului:

— denumirea atelierului;

— adresa atelierului;

— numele titularului;

— prenumele titularului;

— limba preferată de titular.

4.5.4.1.5 Descărcarea informațiilor de pe card

(312) Cardul de atelier permite stocarea unei înregistrări a datelor privind descărcarea informațiilor de pe card, în același mod ca un card de conducător auto.

4.5.4.1.6 Date privind etalonarea și reglarea orei

(313) Cardul de atelier permite stocarea de înregistrări privind etalonările și/sau reglările orei realizate în timp ce cardul este introdus în aparatura de înregistrare.

(314) Fiecare înregistrare de etalonare conține următoarele date:

— scopul etalonării (activare, prima instalare, instalare, inspecție periodică);

— identificarea vehiculului;

— parametrii actualizați sau confirmați [w, k, l, dimensiunea pneurilor, reglajul limitatorului de viteză, odometrul (valorile vechi și cele noi), data și ora (valorile vechi și cele noi)];

— identificarea aparaturii de înregistrare (numărul de componentă al VU, numărul de serie al VU, numărul de serie al senzorului de mișcare).

(315) Cardul de atelier permite stocarea a cel puțin 88 de astfel de înregistrări.

(316) Cardul de atelier este prevăzut cu un contor care indică numărul total de etalonări efectuate cu cardul respectiv.

(317) Cardul de atelier este prevăzut cu un contor care indică numărul total de etalonări efectuate după ultima descărcare de date.

4.5.4.1.7 Date privind evenimentele și anomaliile

(318) Cardul de atelier permite stocarea de înregistrări de date privind evenimentele și anomaliile, în același mod ca un card de conducător auto.

(319) Cardul de atelier permite stocarea de date privind cele mai recente trei evenimente de fiecare tip (și anume, 18 evenimente) și cele mai recente șase erori de fiecare tip (și anume, 12 erori).

4.5.4.1.8 Date privind activitatea conducătorului auto

(320) Cardul de atelier permite stocarea de date privind activitatea conducătorului auto, în același mod ca un card de conducător auto.

(321) Cardul de atelier permite stocarea de date privind activitatea conducătorului auto pentru cel puțin o zi de activitate medie a conducătorului auto.

4.5.4.1.9 Date privind vehiculele utilizate

(322) Cardul de atelier permite stocarea de înregistrări de date privind vehiculele utilizate, în același mod ca un card de conducător auto.

(323) Cardul de atelier permite stocarea a cel puțin patru astfel de înregistrări.

4.5.4.1.10 Date privind începutul și/sau sfârșitul zilelor de lucru

(324) Cardul de atelier permite stocarea de înregistrări de date privind începutul și/sau sfârșitul zilelor de lucru, în același mod ca un card de conducător auto.

(325) Cardul de atelier permite stocarea a cel puțin trei perechi de astfel de înregistrări.

4.5.4.1.11 Date privind sesiunile de utilizare a cardului

(326) Cardul de atelier permite stocarea unei înregistrări a datelor privind sesiunile de utilizare a cardului, în același mod ca un card de conducător auto.

4.5.4.1.12 Date privind activitățile de control

(327) Cardul de atelier permite stocarea unei înregistrări a datelor privind activitățile de control, în același mod ca un card de conducător auto.

4.5.4.1.13 Date privind condițiile specifice

(328) Cardul de atelier permite stocarea de date relevante privind condițiile specifice, în același mod ca un card de conducător auto.

(329) Cardul de atelier permite stocarea a cel puțin două astfel de înregistrări.

4.5.4.2 Aplicația pentru tahograf de a 2-a generație (inaccesibilă unităților montate pe vehicul de primă generație)

4.5.4.2.1 Identificarea aplicației

(330) Cardul de atelier permite stocarea următoarelor date de identificare a aplicației:

— identificarea aplicației pentru tahograf;

— identificarea tipului de card de tahograf.

4.5.4.2.2 Chei și certificate

(331) Cardul de atelier permite stocarea unei serii de chei și certificate criptografice, în conformitate cu apendicele 11 partea B.

(332) Cardul de atelier permite stocarea unui număr de identificare personal (cod PIN).

4.5.4.2.3 Identificarea cardului

(333) Cardul de atelier permite stocarea următoarelor date de identificare a cardului:

— numărul cardului;

— statul membru emitent, denumirea autorității emitente, data emiterii;

— data de la care este valabil cardul, data expirării cardului.

4.5.4.2.4 Identificarea titularului cardului

(334) Cardul de atelier permite stocarea următoarelor date de identificare a titularului cardului:

— denumirea atelierului;

— adresa atelierului;

— numele titularului;

— prenumele titularului;

— limba preferată de titular.

4.5.4.2.5 Descărcarea informațiilor de pe card

(335) Cardul de atelier permite stocarea unei înregistrări a datelor privind descărcarea informațiilor de pe card, în același mod ca un card de conducător auto.

4.5.4.2.6 Date privind etalonarea și reglarea orei

(336) Cardul de atelier permite stocarea de înregistrări privind etalonările și/sau reglările orei realizate în timp ce cardul este introdus în aparatura de înregistrare.

(337) Fiecare înregistrare de etalonare conține următoarele date:

— scopul etalonării (activare, prima instalare, instalare, inspecție periodică);

— identificarea vehiculului;

— parametrii actualizați sau confirmați [w, k, l, dimensiunea pneurilor, reglajul limitatorului de viteză, odometrul (valorile vechi și cele noi), data și ora (valorile vechi și cele noi)];

— identificarea aparaturii de înregistrare (numărul de componentă al VU, numărul de serie al VU, numărul de serie al senzorului de mișcare, numărul de serie al echipamentului de comunicare la distanță și numărul de serie al echipamentului GNSS extern, dacă este cazul);

— tipurile și identificatorii tuturor sigiliilor montate;

— capacitatea VU de a utiliza carduri de tahograf de primă generație (activate sau neactivate).

(338) Cardul de atelier permite stocarea a cel puțin 88 astfel de înregistrări.

(339) Cardul de atelier este prevăzut cu un contor care indică numărul total de etalonări efectuate cu cardul respectiv.

(340) Cardul de atelier este prevăzut cu un contor care indică numărul total de etalonări efectuate după ultima descărcare de date.

4.5.4.2.7 Date privind evenimentele și anomaliile

(341) Cardul de atelier permite stocarea de înregistrări de date privind evenimentele și anomaliile, în același mod ca un card de conducător auto.

(342) Cardul de atelier permite stocarea de date privind cele mai recente trei evenimente de fiecare tip (și anume, 33 evenimente) și cele mai recente șase erori de fiecare tip (și anume, 12 erori).

4.5.4.2.8 Date privind activitatea conducătorului auto

(343) Cardul de atelier permit stocarea de date privind activitatea conducătorului auto, în același mod ca un card de conducător auto.

(344) Cardul de atelier permite stocarea de date privind activitatea conducătorului auto pentru cel puțin o zi de activitate medie a conducătorului auto.

4.5.4.2.9 Date privind vehiculele utilizate

(345) Cardul de atelier permite stocarea de înregistrări de date privind vehiculele utilizate, în același mod ca un card de conducător auto.

(346) Cardul de atelier permite stocarea a cel puțin patru astfel de înregistrări.

4.5.4.2.10 Date privind începutul și/sau sfârșitul zilelor de lucru

(347) Cardul de atelier permite stocarea de înregistrări de date privind începutul și/sau sfârșitul zilelor de lucru, în același mod ca un card de conducător auto.

(348) Cardul de atelier permite stocarea a cel puțin trei perechi de astfel de înregistrări.

4.5.4.2.11 Date privind sesiunile de utilizare a cardului

(349) Cardul de atelier permite stocarea unei înregistrări a datelor privind sesiunile de utilizare a cardului, în același mod ca un card de conducător auto.

4.5.4.2.12 Date privind activitățile de control

(350) Cardul de atelier permite stocarea unei înregistrări a datelor privind activitățile de control, în același mod ca un card de conducător auto.

4.5.4.2.13 Date privind unitățile montate pe vehicul utilizate

(351) Cardul de atelier permite stocarea următoarelor date referitoare la diferitele unități montate pe vehicul în care a fost utilizat cardul:

— data și ora începerii perioadei de utilizare a unității montate pe vehicul (și anume, prima introducere a cardului în unitatea montată pe vehicul pentru perioada respectivă);

— numele producătorului unității montate pe vehicul;

— tipul de unitate montată pe vehicul;

— numărul versiunii software-ului unității montate pe vehicul.

(352) Cardul de atelier permite stocarea a cel puțin patru astfel de înregistrări.

4.5.4.2.14 Date privind locurile în care se încheie o perioadă de conducere continuă de trei ore

(353) Cardul de atelier permite stocarea următoarelor date legate de poziția vehiculului atunci când timpul de conducere continuă al conducătorului auto atinge un multiplu de trei ore:

— data și ora la care timpul de conducere continuă al titularului cardului atinge un multiplu de trei ore;

— poziția vehiculului;

— precizia GNSS, data și ora determinării poziției.

(354) Cardul de atelier permite stocarea a cel puțin 18 astfel de înregistrări.

4.5.4.2.15 Date privind condițiile specifice

(355) Cardul de atelier permite stocarea de date relevante privind condițiile specifice, în același mod ca un card de conducător auto.

(356) Cardul de atelier permite stocarea a cel puțin două astfel de înregistrări.

4.5.5 *Cardul de control*

4.5.5.1 Aplicație pentru tahograf (accesibilă pentru unitățile montate pe vehicul de prima și a doua generație)

4.5.5.1.1 Identificarea aplicației

(357) Cardul de control permite stocarea următoarelor date de identificare a aplicației:

— identificarea aplicației pentru tahograf;

— identificarea tipului de card de tahograf.

4.5.5.1.2 Chei și certificate

(358) Cardul de control permite stocarea unei serii de chei și certificate criptografice, în conformitate cu apendicele 11 partea A.

4.5.5.1.3 Identificarea cardului

(359) Cardul de control permite stocarea următoarelor date de identificare a cardului:

— numărul cardului;

— statul membru emitent, denumirea autorității emitente, data emiterii;

— data de la care este valabil cardul, data expirării cardului (dacă există).

4.5.5.1.4 Identificarea titularului cardului

(360) Cardul de control permite stocarea următoarelor date de identificare a titularului cardului:

— denumirea organismului de control;

— adresa organismului de control;

— numele titularului;

— prenumele titularului;

— limba preferată de titular.

4.5.5.1.5 Date privind activitățile de control

(361) Cardul de control permite stocarea următoarelor date privind activitățile de control:

— data și ora controlului;

— tipul controlului (afișare și/sau imprimare și/sau descărcare din VU și/sau descărcare de pe card și/sau verificare a etalonării în trafic);

— perioada descărcată (dacă este cazul);

— VRN și autoritatea competentă din statul membru de înmatriculare a vehiculului controlat;

— numărul cardului și statul membru emitent al cardului de conducător auto controlat.

(362) Cardul de control permite stocarea a cel puțin 230 de astfel de înregistrări.

4.5.5.2 Aplicația pentru tahograf G2 (inaccesibilă unităților montate pe vehicul de primă generație)

4.5.5.2.1 Identificarea aplicației

(363) Cardul de control permite stocarea următoarelor date de identificare a aplicației:

— identificarea aplicației pentru tahograf;

— identificarea tipului de card de tahograf.

4.5.5.2.2 Chei și certificate

(364) Cardul de control permite stocarea unei serii de chei și certificate criptografice, în conformitate cu apendicele 11 partea B.

4.5.5.2.3 Identificarea cardului

(365) Cardul de control permite stocarea următoarelor date de identificare a cardului:

— numărul cardului;

— statul membru emitent, denumirea autorității emitente, data emiterii;

— data de la care este valabil cardul, data expirării cardului (dacă este cazul).

4.5.5.2.4 Identificarea titularului cardului

(366) Cardul de control permite stocarea următoarelor date de identificare a titularului cardului:

— denumirea organismului de control;

— adresa organismului de control;

— numele titularului;

— prenumele titularului;

— limba preferată de titular.

4.5.5.2.5 Date privind activitățile de control

(367) Cardul de control permite stocarea următoarelor date privind activitățile de control:

— data și ora controlului;

— tipul controlului (afișare și/sau imprimare și/sau descărcare din VU și/sau descărcare de pe card și/sau verificare a etalonării în trafic);

— perioada aferentă datelor descărcate (dacă este cazul);

— VRN și autoritatea competentă din statul membru de înmatriculare a vehiculului controlat;

— numărul cardului și statul membru emitent al cardului de conducător auto controlat.

(368) Cardul de control permite stocarea a cel puțin 230 de astfel de înregistrări.

4.5.6 *Card de societate*

4.5.6.1 Aplicație pentru tahograf (accesibilă pentru unitățile montate pe vehicul de prima și a doua generație)

4.5.6.1.1 Identificarea aplicației

(369) Cardul de societate permite stocarea următoarelor date de identificare a aplicației:

— identificarea aplicației pentru tahograf;

— identificarea tipului de card de tahograf.

4.5.6.1.2 Chei și certificate

(370) Cardul de societate permite stocarea unei serii de chei și certificate criptografice, în conformitate cu apendicele 11 partea A.

4.5.6.1.3 Identificarea cardului

(371) Cardul de societate permite stocarea următoarelor date de identificare a cardului:

— numărul cardului;

— statul membru emitent, denumirea autorității emitente, data emiterii;

— data de la care este valabil cardul, data expirării cardului (dacă există).

4.5.6.1.4 Identificarea titularului cardului

(372) Cardul de societate permite stocarea următoarelor date de identificare a titularului cardului:

— denumirea societății;

— adresa societății.

4.5.6.1.5 Date privind activitatea societății

(373) Cardul de societate permite stocarea următoarelor date privind activitatea societății:

— data și ora activității;

— tipul activității (blocare și/sau deblocare a VU și/sau descărcare din VU și/sau de pe card);

— perioada descărcată (dacă este cazul);

— numărul de înmatriculare al vehiculului și autoritatea competentă din statul membru de înmatriculare a vehiculului;

— numărul cardului și statul membru emitent (în cazul unei descărcări de pe card).

(374) Cardul de societate permite stocarea a cel puțin 230 de astfel de înregistrări.

4.5.6.2 Aplicația pentru tahograf G2 (inaccesibilă unităților montate pe vehicul de primă generație)

4.5.6.2.1 Identificarea aplicației

(375) Cardul de societate permite stocarea următoarelor date de identificare a aplicației:

— identificarea aplicației pentru tahograf;

— identificarea tipului de card de tahograf.

4.5.6.2.2 Chei și certificate

(376) Cardul de societate permite stocarea unei serii de chei și certificate criptografice, în conformitate cu apendicele 11 partea B.

4.5.6.2.3 Identificarea cardului

(377) Cardul de societate permite stocarea următoarelor date de identificare a cardului:

— numărul cardului;

— statul membru emitent, denumirea autorității emitente, data emiterii;

— data de la care este valabil cardul, data expirării cardului (dacă există).

4.5.6.2.4 Identificarea titularului cardului

(378) Cardul de societate permite stocarea următoarelor date de identificare a titularului cardului:

— denumirea societății;

— adresa societății.

4.5.6.2.5 Date privind activitatea societății

(379) Cardul de societate permite stocarea următoarelor date privind activitatea societății:

— data și ora activității;

— tipul activității (blocare și/sau deblocare a VU și/sau descărcare din VU și/sau de pe card);

— perioada aferentă datelor descărcate (dacă este cazul);

— numărul de înmatriculare al vehiculului și autoritatea competentă din statul membru de înmatriculare a vehiculului;

— numărul cardului și statul membru emitent al cardului (în cazul unei descărcări de pe card).

(380) Cardul de societate permite stocarea a cel puțin 230 de astfel de înregistrări.

5. INSTALAREA APARATURII DE ÎNREGISTRARE

5.1 **Instalare**

(381) Aparaturile de înregistrare noi sunt livrate neactivate montatorilor sau producătorilor de vehicule, cu toți parametrii de etalonare prevăzuți în capitolul 3.21 setați la valori implicite adecvate și valabile. În cazurile în care nu se aplică nicio valoare specială, parametrii alfabetici sunt înlocuiți cu șiruri de „?”, iar parametrii numerici cu „0”. Furnizarea componentelor de securitate ale aparaturii de înregistrare poate fi restricționată, dacă este necesar, în timpul certificării de securitate

(382) Înainte de activare, aparatura de înregistrare trebuie să permită accesul la funcția de etalonare, chiar dacă aparatura nu este în modul etalonare.

(383) Înainte de activare, aparatura de înregistrare nu înregistrează și nici nu stochează datele menționate la punctele 3.12.3, 3.12.9 și 3.12.12 – 3.12.15 inclusiv.

(384) În timpul instalării, producătorii de vehicule presetează toți parametrii cunoscuți.

(385) Producătorii de vehicule sau montatorii activează aparatura de înregistrare montată cel târziu înainte ca vehiculul să fie utilizat în conformitate cu Regulamentul (CE) nr. 561/2006.

(386) Activarea aparaturii de înregistrare se declanșează automat la prima introducere a unui card de atelier valabil în oricare dintre dispozitivele de interfață pentru card.

(387) Dacă este cazul, operațiunile speciale necesare pentru asocierea senzorului de mișcare la unitatea montată pe vehicul se realizează automat, înainte sau în timpul activării.

(388) În mod similar, dacă este cazul, operațiunile speciale de cuplare a echipamentului GNSS extern la unitatea montată pe vehicul se realizează automat, înainte sau în timpul activării.

(389) După activare, aparatura de înregistrare controlează integral drepturile de acces la funcții și date.

(390) După activare, aparatura de înregistrare comunică echipamentului de comunicare la distanță datele securizate necesare în scopul controalelor selective în trafic.

(391) Funcțiile de înregistrare și stocare ale aparaturii de înregistrare trebuie să funcționeze integral după activarea acesteia.

(392) Instalarea este urmată de o etalonare. Nu este necesar ca prima etalonare să includă introducerea numărului de înmatriculare al vehiculului (VRN) în cazul în care acesta nu este cunoscut de atelierul aprobat care trebuie să efectueze etalonarea. În aceste condiții și numai în acest moment, este posibil ca proprietarul vehiculului să introducă VRN folosind cardul de societate înainte de utilizarea vehiculului în conformitate cu Regulamentul (CE) nr. 561/2006 (de exemplu, utilizând comenzile prin intermediul unei structuri corespunzătoare a meniului interfeței om-mașină a unității montate pe vehicul) ([1]). Actualizarea sau confirmarea acestei introduceri este posibilă numai atunci când se folosește un card de atelier.

(393) Instalarea unui echipament GNSS extern necesită cuplarea la unitatea montată pe vehicul și verificarea ulterioară a informațiilor de poziționare de la GNSS.

(394) Aparatura de înregistrare trebuie poziționată în vehicul astfel încât conducătorul auto să poată accesa toate funcțiile necesare de pe scaunul său.

([1]) JO L 102, 11.4.2006, p. 1.

5.2 **Plăcuța de instalare**

(395) După instalarea și verificarea aparaturii de înregistrare, pe acesta se aplică o plăcuță de instalare gravată sau imprimată în mod permanent, care să fie clar vizibilă și ușor accesibilă. În cazurile în care acest lucru nu este posibil, plăcuța se montează pe stâlpul „B" al vehiculului pentru a fi clar vizibilă. La vehiculele care nu au un stâlp „B", plăcuța de instalare trebuie montată pe cadrul ușii de pe latura unde se află volanul și trebuie să fie clar vizibilă în toate situațiile.

După fiecare inspecție efectuată de un montator sau de un atelier aprobat, în locul plăcuței existente se aplică una nouă.

(396) Plăcuța trebuie să conțină cel puțin următoarele informații:

— numele, adresa sau denumirea comercială a montatorului sau a atelierului aprobat;

— coeficientul caracteristic al vehiculului, sub forma „w = … imp/km";

— constanta aparaturii de înregistrare, sub forma „k = … imp/km";

— circumferința efectivă a pneurilor roților, sub forma „l = … mm";

— dimensiunea pneurilor;

— data la care au fost măsurate coeficientul caracteristic al vehiculului și circumferința efectivă a pneurilor roților;

— numărul de identificare al vehiculului;

— prezența (sau absența) unui echipament GNSS extern;

— numărul de serie al echipamentului GNSS extern;

— numărul de serie al echipamentului de comunicare la distanță;

— numerele de serie ale tuturor sigiliilor montate;

— partea vehiculului unde este instalat adaptorul (dacă este cazul);

— partea vehiculului unde este instalat senzorul de mișcare, dacă acesta nu este conectat la cutia de viteze sau dacă nu se folosește un adaptor;

— o descriere a culorii cablului dintre adaptor și partea vehiculului care îi furnizează impulsurile de intrare;

— numărul de serie al senzorului de mișcare integrat al adaptorului.

(397) Folosirea unei plăcuțe suplimentare este permisă numai în cazul vehiculelor M1 și N1 prevăzute cu un adaptor în conformitate cu Regulamentul (CE) nr. 68/2009 ([1]), astfel cum a fost modificat ultima dată, și dacă nu este posibilă includerea tuturor informațiilor necesare prevăzute la cerința 396. În aceste cazuri, plăcuța suplimentară trebuie să conțină cel puțin ultimele patru liniuțe de la cerința 396.

Dacă se folosește o plăcuță suplimentară, aceasta se montează lângă prima plăcuță, descrisă la cerința 396, și trebuie să aibă același nivel de protecție. În plus, pe plăcuța suplimentară figurează numele, adresa sau denumirea comercială a montatorului sau a atelierului mecanic aprobat care a efectuat instalarea, precum și data instalării.

([1]) Regulamentul (CE) nr. 68/2009 al Comisiei din 23 ianuarie 2009 de adaptare pentru a noua oară la progresul tehnic a Regulamentului (CEE) nr. 3821/85 al Consiliului privind aparatura de înregistrare în transportul rutier (JO L 21, 24.1.2009, p. 3).

5.3 **Sigilarea**

(398) Se sigilează următoarele părți:

— orice conexiune care, în cazul deconectării, ar cauza producerea unor modificări indetectabile sau pierderea indetectabilă a unor date (acest lucru poate fi valabil, de exemplu, pentru senzorul de mișcare montat pe cutia de viteze, pentru adaptorul destinat vehiculelor M1/N1, pentru conexiunea GNSS externă sau pentru unitatea montată pe vehicul);

— plăcuța de instalare, în afară de cazul în care aceasta este aplicată astfel încât nu poate fi îndepărtată fără a distruge inscripțiile.

(399) Sigiliile menționate anterior pot fi îndepărtate:

— în caz de urgență;

— pentru instalarea, ajustarea sau repararea unui limitator de viteză sau a oricărui alt dispozitiv care contribuie la siguranța rutieră, cu condiția ca aparatura de înregistrare să funcționeze în continuare în mod corect și fiabil și să fie resigilat de un montator sau de un atelier aprobat (în conformitate cu dispozițiile capitolului 6) imediat după montarea limitatorului de viteză sau a oricărui alt dispozitiv care contribuie la siguranța rutieră, sau în termen de șapte zile în celelalte cazuri.

(400) De fiecare dată când aceste sigilii sunt rupte, se elaborează și se transmite autorității competente o declarație scrisă cu privire la motivele acțiunii respective.

(401) Sigiliile trebuie să poarte un număr de identificare atribuit de producătorul de sigilii. Acest număr trebuie să fie unic și diferit de orice alt număr de sigiliu atribuit de orice alt producător de sigilii.

Acest număr unic de identificare se înscrie astfel încât să nu poată fi șters si are următoarea configurație: MM NNNNNN, unde MM reprezintă numărul unic de identificare a producătorului (înregistrarea în baza de date urmează să fie gestionată e CE), iar NNNNNN reprezintă numărul alfanumeric unic al sigiliului, atribuit de producător.

(402) Sigiliile trebuie să aibă un spațiu liber unde montatorii, atelierele sau producătorii de vehicule aprobați să poată adăuga o marcă specială în conformitate cu articolul 22 alineatul (3) din Regulamentul (UE) nr. 165/2014.

Această marcă nu acoperă numărul de identificare al sigiliului.

(403) Producătorii de sigilii trebuie să se înregistreze într-o bază de date și să facă publice numerele de identificare atribuite sigiliilor fabricate de ei, printr-o procedură care urmează să fie stabilită de Comisia Europeană.

(404) Atelierele și producătorii de vehicule aprobați trebuie să utilizeze, în temeiul Regulamentului (UE) nr. 165/2014, numai sigilii produse de producătorii de sigilii înregistrați în baza de date menționată anterior.

(405) Producătorii de sigilii și distribuitorii acestora trebuie să păstreze evidențe de trasabilitate complete ale sigiliilor vândute pentru a fi utilizate în cadrul Regulamentului (UE) nr. 165/2014 și trebuie să fie pregătiți să le prezinte autorităților naționale competente ori de câte ori este necesar.

(406) Numerele de identificare unice ale sigiliilor trebuie să fie vizibile pe plăcuța de instalare.

6. CONTROALE, INSPECȚII ȘI REPARAȚII

Cerințele privind situațiile în care pot fi îndepărtate sigiliile, astfel cum sunt prevăzute la articolul 22 alineatul (5) din Regulamentul (UE) nr. 165/2014, sunt definite în capitolul 5.3 din prezenta anexă.

6.1 **Aprobarea montatorilor, a atelierelor și a producătorilor de vehicule**

Statele membre aprobă, controlează în mod regulat și certifică organismele însărcinate cu efectuarea de:

— instalări;

— controale;

— inspecții;

— reparații.

Cardurile de atelier sunt emise numai montatorilor și/sau atelierelor aprobate pentru activarea și/sau etalonarea aparaturii de înregistrare în conformitate cu prezenta anexă și, cu excepția cazurilor justificate în mod corespunzător:

— care nu sunt eligibile pentru acordarea unui card de societate și

— ale căror activități profesionale nu sunt susceptibile de a compromite securitatea globală a sistemului, astfel cum se prevede în apendicele 10.

6.2 **Verificarea instrumentelor noi și a celor reparate**

(407) Fiecare dispozitiv în parte, indiferent dacă este nou sau reparat, trebuie verificat pentru a se constata dacă funcționează corespunzător și dacă citirile și înregistrările pe care le efectuează sunt precise și respectă limitele prevăzute în capitolul 3.2.1, 3.2.2, 3.2.3 și 3.3, precum și dacă este sigilat și etalonat în conformitate cu capitolul 5.3.

6.3 **Inspecția instalației**

(408) La instalarea pe un vehicul, întreaga instalație (inclusiv aparatura de înregistrare) trebuie să respecte dispozițiile privind toleranțele maxime prevăzute în capitolul 3.2.1, 3.2.2, 3.2.3 și 3.3.

6.4 **Inspecții periodice**

(409) Inspecțiile periodice ale aparaturii montate pe vehicule se efectuează după orice reparație a aparaturii sau după orice modificare a coeficientului caracteristic al vehiculului sau a circumferinței efective ale pneurilor sau după ce aparatura a indicat ora UTC cu o eroare de peste 20 de minute sau dacă VRN a fost modificat și cel puțin o dată în termen de doi ani (24 de luni) de la ultima inspecție.

(410) În cadrul acestor inspecții se verifică, printre altele:

— dacă aparatura de înregistrare funcționează corespunzător, inclusiv în ceea ce privește funcția de stocare a datelor pe cardurile de tahograf și comunicarea cu cititoarele pentru comunicarea la distanță;

— dacă este asigurată conformitatea cu dispozițiile capitolului 3.2.1 și 3.2.2 privind toleranțele maxime la instalare;

— dacă este asigurată conformitatea cu dispozițiile capitolului 3.2.3 și 3.3;

— dacă aparatura de înregistrare poartă marca de omologare de tip;

— dacă plăcuța de instalare, astfel cum este definită la cerința 396, și plăcuța descriptivă, astfel cum este definită la cerința 225, sunt fixate;

— dimensiunea pneurilor și circumferința efectivă a pneurilor;

— dacă la aparatură nu sunt atașate dispozitive de manipulare;

— dacă sigiliile sunt amplasate în mod corect, dacă sunt în stare bună, dacă numerele lor de identificare sunt valabile (dacă producătorul de sigilii este înregistrat în baza de date a CE) și dacă numerele lor de identificare corespund inscripțiilor de pe plăcuța de instalare (a se vedea cerința 401).

(411) Dacă se constată că unul din evenimentele enumerate în capitolul 3.9 (Detectarea evenimentelor și/sau a anomaliilor) a avut loc după ultima inspecție și, conform producătorilor de tahografe și/sau autorităților naționale, poate pune în pericol securitatea echipamentului, atelierul:

a. face o comparație între datele de identificare a senzorului de mișcare conectat la cutia de viteze și cele de identificare a senzorului de mișcare asociat la unitatea montată pe vehicul;

b. verifică dacă informațiile înscrise pe plăcuța de instalare coincid cu informațiile înregistrate în unitatea montată pe vehicul;

c. verifică dacă numărul de serie și numărul de omologare ale senzorului de mișcare, în cazul în care acestea sunt imprimate pe carcasa senzorului de mișcare, coincid cu informațiile stocate în memoria de date a aparaturii de înregistrare;

d. compară datele de identificare inscripționate pe plăcuța descriptivă a echipamentului GNSS extern, dacă este cazul, cu cele stocate în memoria de date a unității montate pe vehicul.

(412) În rapoartele lor de inspecție, atelierele țin evidența oricăror constatări referitoare la existența unor sigilii rupte sau a unor dispozitive de manipulare. Atelierele păstrează aceste rapoarte cel puțin 2 ani și le pun la dispoziția autorității competente ori de câte ori li se cere să facă acest lucru.

(413) Aceste inspecții includ o etalonare și o înlocuire preventivă a sigiliilor a căror montare ține de responsabilitatea atelierelor.

6.5 **Măsurarea erorilor**

(414) Măsurarea erorilor la instalare și în timpul utilizării se realizează în următoarele condiții, considerate drept condiții standard de testare:

— vehicul fără încărcătură, în stare normală de funcționare;

— presiunea pneurilor în conformitate cu instrucțiunile producătorului;

— uzura pneurilor în limitele permise de legislația națională;

— deplasarea vehiculului:

— vehiculul avansează, pe baza acțiunii motorului propriu, în linie dreaptă, pe teren plat, cu o viteză de 50 ± 5 km/h. Distanța de măsurare trebuie să fie de cel puțin 1 000 m.

— pentru testare pot fi folosite și metode alternative, de exemplu un banc dinamometric adecvat, cu condiția ca acesta să aibă o precizie comparabilă.

6.6 **Reparații**

(415) Atelierele trebuie să poată descărca date din aparatura de înregistrare pentru a le transmite societății de transport în cauză.

(416) Atelierele autorizate emit societăților de transport un certificat care atestă că datele nu pot fi descărcate, în cazul în care o defecțiune a aparaturii de înregistrare împiedică descărcarea datelor înregistrate anterior, chiar și după reparațiile efectuate de atelierul respectiv. Atelierul păstrează timp de cel puțin doi ani un exemplar din fiecare certificat emis.

7. EMITEREA CARDURILOR

Procedurile de emitere a cardurilor stabilite de statele membre respectă următoarele dispoziții:

(417) Numărul de card al primului card de tahograf emis unui solicitant conține un indice secvențial (dacă este cazul), un indice de înlocuire și un indice de reînnoire setate la „0”.

(418) Numerele de card ale tuturor cardurilor nenominale de tahograf emise unui singur organism de control, unui singur atelier sau unei singure societăți au primele 13 cifre identice și un indice secvențial diferit.

(419) Un card de tahograf emis în scopul înlocuirii unui card de tahograf existent are același număr de card ca și cardul înlocuit, cu excepția indicelui de înlocuire, a cărui valoare se mărește cu „1” (în ordinea 0, …9, A, … Z).

(420) Un card de tahograf emis în scopul înlocuirii unui card de tahograf existent are aceeași dată de expirare ca și cardul înlocuit.

(421) Un card de tahograf emis în scopul reînnoirii unui card de tahograf existent are același număr de card ca și cardul înlocuit, cu excepția indicelui de înlocuire, a cărui valoare trebuie resetată la „0", și cu excepția indicelui de reînnoire a cărui valoare se mărește cu „1" (în ordinea 0, …, 9, A, …, Z).

(422) În vederea modificării datelor administrative, schimbarea unui card de tahograf existent respectă regulile de reînnoire dacă se produce în același stat membru sau regulile aplicabile primei emiteri în cazul în care se produce în alt stat membru.

(423) În cazul cardurilor de atelier sau de control nenominale, rubrica „Numele titularului cardului" se completează cu denumirea atelierului sau a organismului de control ori cu numele montatorului sau al agentului de control, în cazul în care statele membre decid astfel.

(424) Statele membre fac schimb de date prin mijloace electronice pentru a asigura unicitatea cardurilor de conducător auto pe care le emit în conformitate cu articolul 31 din Regulamentul (UE) nr. 165/2014.

8. OMOLOGAREA DE TIP A APARATURII DE ÎNREGISTRARE ȘI A CARDURILOR DE TAHOGRAF

8.1 **Generalități**

În sensul prezentului capitol, termenul „aparatură de înregistrare" înseamnă „aparatura de înregistrare sau componentele acesteia". Nu este necesară omologarea de tip pentru cablul sau cablurile care conectează senzorul de mișcare, echipamentul GNSS extern sau echipamentul de comunicare la distanță cu VU. Hârtia utilizată de aparatura de înregistrare este considerată o componentă a aparaturii de înregistrare.

Orice producător poate solicita omologarea de tip a componentei sale cu orice tip de senzor de mișcare sau echipament GNSS extern și invers, cu condiția ca fiecare componentă să respecte cerințele prezentei anexe. Alternativ, producătorii pot să solicite, de asemenea, omologarea de tip a aparaturii de înregistrare.

(425) Aparatura de înregistrare trebuie prezentată spre omologare în întregime, incluzând eventualele dispozitive suplimentare integrate.

(426) Omologarea aparaturii de înregistrare și a cardurilor de tahograf trebuie să cuprindă teste de securitate, teste de funcționare și teste de interoperabilitate. Rezultatele pozitive obținute la fiecare dintre aceste teste sunt confirmate printr-un certificat corespunzător.

(427) Autoritățile însărcinate cu omologarea de tip din statele membre nu acordă certificate de omologare de tip atât timp cât nu dețin:

— un certificat de securitate

— un certificat de funcționare

— și un certificat de interoperabilitate

aferente aparaturii de înregistrare sau cardului de tahograf care face obiectul cererii de omologare de tip.

(428) Orice modificare a software-ului sau a hardware-ului aparaturii sau a naturii materialelor utilizate pentru producerea acesteia se notifică, înainte de utilizare, autorității care a acordat omologarea de tip pentru aparatura în cauză. Autoritatea respectivă îi confirmă producătorului extinderea omologării de tip sau poate solicita o actualizare sau o confirmare a certificatelor de funcționare, de securitate și/sau de interoperabilitate relevante.

(429) Procedurile de actualizare in situ a software-ului aparaturii de înregistrare trebuie aprobate de autoritatea care a acordat omologarea de tip pentru aparatura de înregistrare în cauză. Actualizarea software-ului nu trebuie să modifice și nici să șteargă niciun fel de date privind activitatea conducătorului auto stocate în aparatura de înregistrare. Software-ul poate fi actualizat numai pe răspunderea producătorului aparaturii.

(430) Omologarea de tip a modificărilor aduse software-ului în scopul actualizării unei aparaturi de înregistrare deja omologate de tip nu poate fi refuzată dacă modificările respective vizează numai funcții nespecificate în prezenta anexă. Actualizarea software-ului unei aparaturi de înregistrare poate să nu implice introducerea de noi seturi de caractere, dacă acest lucru nu este fezabil din punct de vedere tehnic.

8.2 **Certificatul de securitate**

(431) Certificatul de securitate se eliberează în conformitate cu dispozițiile apendicelui 10 la prezenta anexă. Componentele aparaturii de înregistrare care trebuie certificate sunt unitatea montată pe vehicul, senzorul de mișcare, echipamentul GNSS extern și cardurile de tahograf.

(432) În situația excepțională în care autoritățile de certificare a securității refuză certificarea unei aparaturi noi din cauza mecanismelor de securitate învechite, omologarea de tip se va acorda în continuare numai în acest gen de situații particulare și excepționale și numai dacă nu există nicio altă soluție conformă cu regulamentul.

(433) În această situație, statul membru în cauză informează fără întârziere Comisia Europeană care, în termen de douăsprezece luni calendaristice de la acordarea omologării de tip, lansează o procedură menită să garanteze că securitatea este readusă la nivelul inițial.

8.3 **Certificatul de funcționare**

(434) Fiecare candidat la omologarea de tip furnizează autorității de omologare de tip a statului membru toate materialele și întreaga documentație pe care aceasta le consideră necesare.

(435) În termen de o lună de la depunerea cererii, producătorii furnizează eșantioanele relevante din produsele pentru care se solicită omologarea de tip și documentația aferentă cerute de laboratoarele desemnate să efectueze testele de funcționare. Toate costurile care derivă din această cerere sunt suportate de entitatea solicitantă. Laboratoarele asigură confidențialitatea informațiilor comerciale sensibile.

(436) Producătorului i se eliberează un certificat de funcționare numai după obținerea de rezultate satisfăcătoare cel puțin la toate testele de funcționare prevăzute în apendicele 9.

(437) Autoritatea de omologare de tip eliberează certificatul de funcționare. Acest certificat indică, pe lângă numele beneficiarului și identificarea modelului, o listă detaliată a testelor efectuate și a rezultatelor obținute.

(438) Certificatul de funcționare al oricărei componente a aparaturii de înregistrare indică, de asemenea, numerele de omologare de tip ale celorlalte componente compatibile și omologate de tip ale aparaturii de înregistrare, testate în vederea certificării.

(439) Certificatul de funcționare al oricărei componente a aparaturii de înregistrare indică, de asemenea, standardul ISO sau CEN pe baza căruia a fost certificată interfața de funcționare.

8.4 **Certificatul de interoperabilitate**

(440) Testele de interoperabilitate sunt realizate de un singur laborator, aflat sub autoritatea și responsabilitatea Comisiei Europene.

(441) Laboratorul înregistrează cererile de teste de interoperabilitate depuse de producători în ordinea cronologică a primirii lor.

(442) Cererile se înregistrează oficial numai în momentul în care laboratorul deține:

— toate materialele și documentele necesare pentru realizarea acestor teste de interoperabilitate;

— certificatul de securitate corespunzător;

— certificatul de funcționare corespunzător.

Data înregistrării cererii se notifică producătorului.

(443) Laboratorul nu efectuează niciun test de interoperabilitate pentru aparatura de înregistrare sau cardurile de tahograf care nu au primit un certificat de securitate și un certificat de funcționare, în afară de situațiile excepționale descrise la cerința 432.

(444) Orice producător care solicită teste de interoperabilitate se angajează să cedeze laboratorului însărcinat cu efectuarea testelor respective toate materialele și documentele pe care le-a furnizat în vederea realizării testelor.

(445) Testele de interoperabilitate se efectuează în conformitate cu dispozițiile apendicelui 9 la prezenta anexă, pentru toate tipurile de aparatură de înregistrare sau de carduri de tahograf:

— a căror omologare de tip este încă valabilă; sau

— care nu au primit încă omologarea de tip și care dețin un certificat de interoperabilitate valabil.

(446) Testele de interoperabilitate vizează toate generațiile aparaturii de înregistrare sau ale cardurilor de tahograf aflate încă în uz.

(447) Certificatul de interoperabilitate este eliberat de către laborator producătorului numai după obținerea de rezultate satisfăcătoare la toate testele de interoperabilitate solicitate.

(448) Dacă rezultatele testelor de interoperabilitate nu sunt satisfăcătoare pentru unul sau mai multe aparaturi de înregistrare sau carduri de tahograf, certificatul de interoperabilitate nu se eliberează decât după ce producătorul a efectuat modificările necesare și a obținut rezultate satisfăcătoare la testele de interoperabilitate. Laboratorul identifică sursa problemei împreună cu producătorii afectați de respectiva anomalie de interoperabilitate și încearcă să îi ajute să găsească o soluție tehnică. În cazul în care producătorul și-a modificat produsul, acesta este obligat să se informeze pe lângă autoritățile competente dacă certificatul de securitate și certificatul de funcționare sunt încă valabile.

(449) Certificatul de interoperabilitate este valabil șase luni. Acesta expiră la sfârșitul perioadei respective dacă producătorul nu primește un certificat de omologare relevant. Certificatul este transmis de producător autorității de omologare de tip a statului membru care a emis certificatul de funcționare.

(450) Niciun element care ar putea sta la originea unei anomalii de interoperabilitate nu trebuie folosit în scopul obținerii de profit sau pentru obținerea unei poziții dominante.

8.5 **Certificatul de omologare de tip**

(451) Autoritatea de omologare de tip a statului membru poate elibera certificatul de omologare de tip de îndată ce se află în posesia celor trei certificate solicitate.

(452) Certificatul de omologare de tip al oricărei componente a aparaturii de înregistrare trebuie să indice, de asemenea, numerele de omologare de tip ale celorlalte aparaturi de înregistrare interoperabile care dețin omologarea de tip.

(453) Autoritatea de omologare de tip transmite laboratorului însărcinat cu efectuarea testelor de interoperabilitate un exemplar al certificatului de omologare de tip în momentul eliberării acestuia către producător.

(454) Laboratorul însărcinat cu efectuarea testelor de interoperabilitate creează un site web public care conține o listă actualizată a modelelor de aparaturi de înregistrare sau de carduri de tahograf:

— pentru care a fost înregistrată o cerere de efectuare a unor teste de interoperabilitate;

— care au primit un certificat de interoperabilitate (chiar dacă acesta este provizoriu);

— care au primit un certificat de omologare de tip.

8.6 **Procedură extraordinară: primele certificate de interoperabilitate pentru aparatura de înregistrare și cardurile de tahograf de a 2-a generație**

(455) Pe parcursul unei perioade de patru luni de la certificarea interoperabilității unui prim ansamblu de aparatură de înregistrare de a 2-a generație și carduri de tahograf de a 2-a generație (card de conducător auto, de atelier, de control și de societate), orice certificat de interoperabilitate eliberat (inclusiv primele) în urma cererilor înregistrate pe parcursul acestei perioade este considerat provizoriu.

(456) Dacă, la sfârșitul perioadei menționate anterior, toate produsele în cauză sunt reciproc interoperabile, toate certificatele de interoperabilitate aferente devin definitive.

(457) Dacă, pe parcursul acestei perioade, apar anomalii de interoperabilitate, laboratorul însărcinat cu efectuarea testelor de interoperabilitate trebuie să identifice cauzele problemelor cu ajutorul producătorilor implicați și îi invită să facă modificările necesare.

(458) Dacă, la sfârșitul acestei perioade, problemele de interoperabilitate persistă, laboratorul însărcinat cu realizarea testelor de interoperabilitate, în colaborare cu producătorii în cauză și cu autoritățile de omologare de tip care au eliberat certificatul de funcționare aferent, trebuie să identifice cauzele anomaliilor de interoperabilitate și să stabilească modificările care ar trebui efectuate de către fiecare dintre producătorii în cauză. Căutarea de soluții tehnice durează maximum două luni, după care, dacă nu se găsește nicio soluție comună, Comisia, după consultarea laboratorului însărcinat cu efectuarea testelor de interoperabilitate, decide care aparatură și care carduri primesc un certificat de interoperabilitate definitiv și precizează motivele pe baza cărora a fost adoptată decizia respectivă.

(459) Orice cerere de efectuare a unor teste de interoperabilitate înregistrată de laborator între sfârșitul perioadei de patru luni de la eliberarea primului certificat provizoriu de interoperabilitate și data deciziei adoptate de Comisie menționată la cerința 455 trebuie amânată până la rezolvarea problemelor inițiale de interoperabilitate. Cererile respective se prelucrează apoi în ordinea cronologică a înregistrării.

Apendicele 1

DICȚIONAR DE DATE

CUPRINS

1. INTRODUCERE 88

1.1. Metoda de stabilire a definițiilor tipurilor de date 88

1.2. Referințe 88

2. DEFINIȚIILE TIPURILOR DE DATE 89

2.1. ActivityChangeInfo 89

2.2. Address 90

2.3. AESKey 91

2.4. AES128Key 91

2.5. AES192Key 91

2.6. AES256Key 92

2.7. BCDString 92

2.8. CalibrationPurpose 92

2.9. CardActivityDailyRecord 93

2.10. CardActivityLengthRange 93

2.11. CardApprovalNumber 93

2.12. CardCertificate 94

2.13. CardChipIdentification 94

2.14. CardConsecutiveIndex 94

2.15. CardControlActivityDataRecord 94

2.16. CardCurrentUse 95

2.17. CardDriverActivity 95

2.18. CardDrivingLicenceInformation 95

2.19. CardEventData 96

2.20. CardEventRecord 96

2.21. CardFaultData 96

2.22. CardFaultRecord 97

2.23. CardIccIdentification 97

2.24. CardIdentification 97

2.25. CardMACertificate 98

2.26. CardNumber 98

2.27. CardPlaceDailyWorkPeriod 99

2.28. CardPrivateKey 99

2.29. CardPublicKey 99
2.30. CardRenewalIndex 99
2.31. CardReplacementIndex 99
2.32. CardSignCertificate 100
2.33. CardSlotNumber 100
2.34. CardSlotsStatus 100
2.35. CardSlotsStatusRecordArray 100
2.36. CardStructureVersion 101
2.37. CardVehicleRecord 101
2.38. CardVehiclesUsed 102
2.39. CardVehicleUnitRecord 102
2.40. CardVehicleUnitsUsed 102
2.41. Certificat 103
2.42. CertificateContent 103
2.43. CertificateHolderAuthorisation 104
2.44. CertificateRequestID 104
2.45. CertificationAuthorityKID 104
2.46. CompanyActivityData 105
2.47. CompanyActivityType 106
2.48. CompanyCardApplicationIdentification 106
2.49. CompanyCardHolderIdentification 106
2.50. ControlCardApplicationIdentification 106
2.51. ControlCardControlActivityData 107
2.52. ControlCardHolderIdentification 107
2.53. ControlType 108
2.54. CurrentDateTime 109
2.55. CurrentDateTimeRecordArray 109
2.56. DailyPresenceCounter 109
2.57. Datef 109
2.58. DateOfDayDownloaded 110
2.59. DateOfDayDownloadedRecordArray 110
2.60. Distance 110
2.61. DriverCardApplicationIdentification 110
2.62. DriverCardHolderIdentification 111
2.63. DSRCSecurityData 112
2.64. EGFCertificate 112
2.65. EmbedderIcAssemblerId 112

2.66. EntryTypeDailyWorkPeriod 113
2.67. EquipmentType 113
2.68. EuropeanPublicKey 114
2.69. EventFaultRecordPurpose 114
2.70. EventFaultType 114
2.71. ExtendedSealIdentifier 115
2.72. ExtendedSerialNumber 116
2.73. FullCardNumber 116
2.74. FullCardNumberAndGeneration 117
2.75. Generation 117
2.76. GeoCoordinates 117
2.77. GNSSAccuracy 118
2.78. GNSSContinuousDriving 118
2.79. GNSSContinuousDrivingRecord 118
2.80. GNSSPlaceRecord 118
2.81. HighResOdometer 119
2.82. HighResTripDistance 119
2.83. HolderName 119
2.84. InternalGNSSReceiver 119
2.85. K-ConstantOfRecordingEquipment 119
2.86. KeyIdentifier 120
2.87. KMWCKey 120
2.88. Language 120
2.89. LastCardDownload 120
2.90. LinkCertificate 120
2.91. L-TyreCircumference 121
2.92. MAC 121
2.93. ManualInputFlag 121
2.94. ManufacturerCode 121
2.95. ManufacturerSpecificEventFaultData 121
2.96. MemberStateCertificate 122
2.97. MemberStateCertificateRecordArray 122
2.98. MemberStatePublicKey 122
2.99. Name 122
2.100. NationAlpha 123
2.101. NationNumeric 123
2.102. NoOfCalibrationRecords 123

2.103. NoOfCalibrationsSinceDownload 123
2.104. NoOfCardPlaceRecords 123
2.105. NoOfCardVehicleRecords 124
2.106. NoOfCardVehicleUnitRecords 124
2.107. NoOfCompanyActivityRecords 124
2.108. NoOfControlActivityRecords 124
2.109. NoOfEventsPerType 124
2.110. NoOfFaultsPerType 124
2.111. NoOfGNSSCDRecords 124
2.112. NoOfSpecificConditionRecords 125
2.113. OdometerShort 125
2.114. OdometerValueMidnight 125
2.115. OdometerValueMidnightRecordArray 125
2.116. OverspeedNumber 125
2.117. PlaceRecord 126
2.118. PreviousVehicleInfo 126
2.119. PublicKey 127
2.120. RecordType 127
2.121. RegionAlpha 128
2.122. RegionNumeric 128
2.123. RemoteCommunicationModuleSerialNumber 129
2.124. RSAKeyModulus 129
2.125. RSAKeyPrivateExponent 129
2.126. RSAKeyPublicExponent 129
2.127. RtmData 129
2.128. SealDataCard 129
2.129. SealDataVu 130
2.130. SealRecord 130
2.131. SensorApprovalNumber 130
2.132. SensorExternalGNSSApprovalNumber 131
2.133. SensorExternalGNSSCoupledRecord 131
2.134. SensorExternalGNSSIdentification 131
2.135. SensorExternalGNSSInstallation 132
2.136. SensorExternalGNSSOSIdentifier 132
2.137. SensorExternalGNSSSCIdentifier 132
2.138. SensorGNSSCouplingDate 133

2.139. SensorGNSSSerialNumber 133
2.140. SensorIdentification 133
2.141. SensorInstallation 133
2.142. SensorInstallationSecData 134
2.143. SensorOSIdentifier 134
2.144. SensorPaired 134
2.145. SensorPairedRecord 135
2.146. SensorPairingDate 135
2.147. SensorSCIdentifier 135
2.148. SensorSerialNumber 135
2.149. Signature 135
2.150. SignatureRecordArray 136
2.151. SimilarEventsNumber 136
2.152. SpecificConditionRecord 136
2.153. SpecificConditions 136
2.154. SpecificConditionType 137
2.155. Speed 137
2.156. SpeedAuthorised 137
2.157. SpeedAverage 138
2.158. SpeedMax 138
2.159. TachographPayload 138
2.160. TachographPayloadEncrypted 138
2.161. TDesSessionKey 138
2.162. TimeReal 139
2.163. TyreSize 139
2.164. VehicleIdentificationNumber 139
2.165. VehicleIdentificationNumberRecordArray 139
2.166. VehicleRegistrationIdentification 139
2.167. VehicleRegistrationNumber 140
2.168. VehicleRegistrationNumberRecordArray 140
2.169. VuAbility 140
2.170. VuActivityDailyData 141
2.171. VuActivityDailyRecordArray 141
2.172. VuApprovalNumber 141
2.173. VuCalibrationData 142
2.174. VuCalibrationRecord 142
2.175. VuCalibrationRecordArray 143

2.176. VuCardIWData 144
2.177. VuCardIWRecord 144
2.178. VuCardIWRecordArray 145
2.179. VuCardRecord 145
2.180. VuCardRecordArray 146
2.181. VuCertificate 146
2.182. VuCertificateRecordArray 146
2.183. VuCompanyLocksData 147
2.184. VuCompanyLocksRecord 147
2.185. VuCompanyLocksRecordArray 148
2.186. VuControlActivityData 148
2.187. VuControlActivityRecord 148
2.188. VuControlActivityRecordArray 149
2.189. VuDataBlockCounter 149
2.190. VuDetailedSpeedBlock 149
2.191. VuDetailedSpeedBlockRecordArray 150
2.192. VuDetailedSpeedData 150
2.193. VuDownloadablePeriod 150
2.194. VuDownloadablePeriodRecordArray 151
2.195. VuDownloadActivityData 151
2.196. VuDownloadActivityDataRecordArray 151
2.197. VuEventData 152
2.198. VuEventRecord 152
2.199. VuEventRecordArray 153
2.200. VuFaultData 154
2.201. VuFaultRecord 154
2.202. VuFaultRecordArray 155
2.203. VuGNSSCDRecord 155
2.204. VuGNSSCDRecordArray 156
2.205. VuIdentification 156
2.206. VuIdentificationRecordArray 157
2.207. VuITSConsentRecord 157
2.208. VuITSConsentRecordArray 158
2.209. VuManufacturerAddress 158
2.210. VuManufacturerName 158
2.211. VuManufacturingDate 158

2.212. VuOverSpeedingControlData 159
2.213. VuOverSpeedingControlDataRecordArray 159
2.214. VuOverSpeedingEventData 159
2.215. VuOverSpeedingEventRecord 159
2.216. VuOverSpeedingEventRecordArray 160
2.217. VuPartNumber 161
2.218. VuPlaceDailyWorkPeriodData 161
2.219. VuPlaceDailyWorkPeriodRecord 161
2.220. VuPlaceDailyWorkPeriodRecordArray 162
2.221. VuPrivateKey 162
2.222. VuPublicKey 162
2.223. VuSerialNumber 162
2.224. VuSoftInstallationDate 162
2.225. VuSoftwareIdentification 163
2.226. VuSoftwareVersion 163
2.227. VuSpecificConditionData 163
2.228. VuSpecificConditionRecordArray 163
2.229. VuTimeAdjustmentData 164
2.230. VuTimeAdjustmentGNSSRecord 164
2.231. VuTimeAdjustmentGNSSRecordArray 164
2.232. VuTimeAdjustmentRecord 165
2.233. VuTimeAdjustmentRecordArray 165
2.234. WorkshopCardApplicationIdentification 166
2.235. WorkshopCardCalibrationData 166
2.236. WorkshopCardCalibrationRecord 167
2.237. WorkshopCardHolderIdentification 168
2.238. WorkshopCardPIN 168
2.239. W-VehicleCharacteristicConstant 169
2.240. VuPowerSupplyInterruptionRecord 169
2.241. VuPowerSupplyInterruptionRecordArray 169
2.242. VuSensorExternalGNSSCoupledRecordArray 170
2.243. VuSensorPairedRecordArray 170
3. DEFINIREA INTERVALELOR DE VALORI ȘI DE DIMENSIUNI 171
4. SETURI DE CARACTERE 171
5. CODAREA 171
6. IDENTIFICATORII DE OBIECT ȘI IDENTIFICATORII DE APLICAȚIE 171
6.1. Identificatorii de obiect 171
6.2. Identificatorii de aplicație 172

1. INTRODUCERE

Prezentul apendice cuprinde precizări privind formatele de date, elementele de date și structurile de date care trebuie utilizate de aparatura de înregistrare și de cardurile de tahograf.

1.1. **Metoda de stabilire a definițiilor tipurilor de date**

În prezentul apendice se recurge la *Abstract Syntax Notation One* (ASN.1) pentru a defini tipurile de date. Acest lucru permite definirea unor date simple și structurate, fără a fi necesară o sintaxă specifică de transfer (reguli de codare) care să depindă de aplicație și de mediu.

Convențiile de denumire a tipurilor ASN.1 sunt realizate conform standardului ISO/IEC 8824-1. Aceasta implică faptul că:

— acolo unde este posibil, semnificația tipului de date este indicată prin intermediul denumirilor alese;

— dacă un tip de date reprezintă o combinație de alte tipuri de date, denumirea tipului de date în cauză constituie totuși o singură secvență de caractere alfabetice care începe cu o majusculă, dar se mai utilizează și alte majuscule în cadrul denumirii pentru a atribui semnificația corespondentă fiecărei părți;

— în general, denumirile tipurilor de date sunt legate de denumirile tipurilor de date din care sunt alcătuite, ale echipamentelor în care sunt stocate datele și ale funcției atribuite datelor în cauză.

Dacă un tip ASN.1 este deja definit în cadrul unui alt standard și dacă trebuie utilizat de aparatura de înregistrare, atunci tipul ASN.1 în cauză este definit în prezentul apendice.

Pentru a permite aplicarea mai multor tipuri de reguli de codare, anumite tipuri ASN.1 cuprinse în prezentul apendice sunt condiționate de identificatorii intervalelor de valori. Identificatorii intervalelor de valori sunt definiți la punctul 3 și în apendicele 2.

1.2. **Referințe**

În prezentul apendice se utilizează următoarele referințe:

ISO 639	Code for the representation of names of languages. First Edition: 1988.
ISO 3166	Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, 2013
ISO 3779	Road vehicles – Vehicle identification number (VIN) – Content and structure. 2009
ISO/IEC 7816-5	Identification cards – Integrated circuit cards – Part 5: Registration of application providers. Second edition: 2004.
ISO/IEC 7816-6	Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange, 2004 + Technical Corrigendum 1: 2006
ISO/IEC 8824-1	Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2008 + Technical Corrigendum 1: 2012 and Technical Corrigendum 2: 2014.
ISO/IEC 8825-2	Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). 2008.
ISO/IEC 8859-1	Information technology – 8 bit single-byte coded graphic character sets – Part 1: Latin alphabet No.1. First edition: 1998.
ISO/IEC 8859-7	Information technology – 8 bit single-byte coded graphic character sets – Part 7: Latin/Greek alphabet. 2003.

ISO 16844-3	Road vehicles – Tachograph systems – Motion Sensor Interface. 2004 + Technical Corrigendum 1: 2006..
TR-03110-3	BSI / ANSSI Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3 Common Specifications, version 2.20, 3. February 2015

2. DEFINIȚIILE TIPURILOR DE DATE

Pentru fiecare din următoarele tipuri de date, valoarea implicită pentru un conținut „necunoscut" sau care „nu se aplică" va consta în completarea elementului de date cu octeți 'FF'.

Toate tipurile de date sunt utilizate pentru aplicațiile de generația 1 și de generația 2, cu excepția cazului în care se prevede altfel.

2.1. **ActivityChangeInfo**

Acest tip de date permite codarea, într-un cuvânt de doi octeți, a stării slotului la 00.00 și/sau a regimului de conducere la 00.00 și/sau a modificărilor de activitate și/sau a modificărilor regimului de conducere și/sau a modificărilor stării cardului pentru un conducător auto sau un copilot. Acest tip de date se raportează la cerințele 105, 266, 291, 320, 321, 343 și 344 din anexa 1C.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Atribuirea valorii – Octet aliniat: 'scpaatttttttttt'B (16 biți)

Pentru înregistrările în memoria de date (sau starea slotului):

's'B	Slot:
	'0'B: CONDUCĂTOR AUTO,
	'1'B: COPILOT,
'c'B	Regim de conducere:
	'0'B: SINGUR,
	'1'B: ECHIPAJ,
'p'B	Starea cardului de conducător auto (sau de atelier) din slotul relevant:
	'0'B: INTRODUS, este introdus un card,
	'1'B: NEINTRODUS, nu este introdus niciun card (sau este retras un card),
'aa'B	Activitate:
	'00'B: PAUZĂ/PERIOADĂ DE ODIHNĂ,
	'01'B: DISPONIBILITATE,
	'10'B: LUCRU,
	'11'B: CONDUCERE,
'ttttttttttt'B	Ora modificării: Numărul de minute de la 00h00 în ziua dată.

Pentru înregistrările de pe cardul de conducător auto (sau de atelier) (și regimul de conducere):

‘s’B	Slot (nu este relevant când ‘p’=1 cu excepția notei de mai jos):
	‘0’B: CONDUCĂTOR AUTO,
	‘1’B: COPILOT,
‘c’B	Regim de conducere (caz ‘p’=0) sau
	Starea activității următoare (caz ‘p’=1):
	‘0’B: SINGUR,
	‘0’B: NECUNOSCUTĂ
	‘1’B: ECHIPAJ,
	‘1’B: CUNOSCUTĂ (= introdusă manual)
‘p’B	Starea cardului:
	‘0’B: INTRODUS, cardul este introdus în aparatura de înregistrare,
	‘1’B: NEINTRODUS, cardul nu este introdus (sau cardul este retras),
‘aa’B	Activitate (nu este relevantă când ‘p’=1 și ‘c’=0, cu excepția notei de mai jos):
	‘00’B: PAUZĂ/PERIOADĂ DE ODIHNĂ,
	‘01’B: DISPONIBILITATE,
	‘10’B: LUCRU,
	‘11’B: CONDUCERE,
‘ttttttttttt’B	Ora modificării: Numărul de minute de la 00h00 în ziua dată.

Notă pentru cazul de „retragere a cardului”:

Atunci când cardul este retras:

— ‘s’ este relevant și indică slotul din care este retras cardul,

— ‘c’ trebuie să fie setat la 0,

— ‘p’ trebuie să fie setat la 1,

— ‘aa’ trebuie să codeze activitatea curentă selectată în momentul respectiv,

Ca urmare a unei introduceri manuale de date, biții ‘c’ și ‘aa’ din cuvânt (stocați pe un card) pot fi suprascriși mai târziu pentru a reflecta introducerea de date.

2.2. **Address**

O adresă.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage indică un set de caractere definit în capitolul 4,

address este o adresă codată cu ajutorul setului de caractere precizat.

2.3. **AESKey**

Generația 2:

O cheie AES cu o lungime de 128, 192 sau 256 de biți.

```
AESKey ::= CHOICE {
   aes128Key                          AES128Key,
   aes192Key                          AES192Key,
   aes256Key                          AES256Key
}
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.4. **AES128Key**

Generația 2:

O cheie AES128.

```
AES128Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes128Key                          OCTET STRING (SIZE(16))
}
```

length denotă lungimea cheii AES128 în octeți.

aes128Key este o cheie AES cu o lungime de 128 de biți.

Atribuirea valorii:

lungimea trebuie să aibă valoarea 16.

2.5. **AES192Key**

Generația 2:

O cheie AES192.

```
AES192Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes192Key                          OCTET STRING (SIZE(24))
}
```

length denotă lungimea cheii AES192 în octeți.

aes192Key este o cheie AES cu o lungime de 192 de biți.

Atribuirea valorii:

lungimea trebuie să aibă valoarea 24.

2.6. **AES256Key**

Generația 2:

O cheie AES256.

```
AES256Key ::= SEQUENCE {
   length                                INTEGER(0..255),
   aes256Key                             OCTET STRING (SIZE(32))
}
```

length denotă lungimea cheii AES256 în octeți.

aes256Key este o cheie AES cu o lungime de 256 de biți.

Atribuirea valorii:

lungimea trebuie să aibă valoarea 32.

2.7. **BCDString**

BCDString se aplică pentru o reprezentare a zecimalei în cod binar (*Binary Code Decimal*, BCD). Acest tip de date se utilizează pentru a reprezenta o unitate zecimală într-un semioctet (4 biți). BCDString se bazează pe ISO/IEC 8824-1 'CharacterStringType'.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString folosește o notație „hstring". Cifra din extremitatea stângă a șirului hexadecimal este cel mai important semioctet din primul octet. Pentru a obține un multiplu de octeți, se inserează semiocteți nuli, în cantitatea necesară, din poziția semioctetului din extremitatea stângă a primului octet.

Cifrele permise sunt: 0, 1, .. 9.

2.8. **CalibrationPurpose**

Cod care explică de ce s-a înregistrat un set de parametri de etalonare. Acest tip de date se raportează la cerințele 097 și 098 din anexa 1B și la cerința 119 din anexa 1C.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Atribuirea valorii:

Generația 1:

'00'H	valoare rezervată,
'01'H	activare: înregistrarea parametrilor de etalonare cunoscuți, în momentul activării VU,
'02'H	prima instalare: prima etalonare a VU după activarea ei,
'03'H	instalare: prima etalonare a VU în vehiculul actual,
'04'H	inspecție periodică.

Generația 2:

În plus față de generația 1, se utilizează următoarele valori:

'05'H	introducerea VRN de către societate,
'06'H	reglarea orei fără etalonare,
de la '07'H până la '7F'H	RFU,
de la '80'H până la 'FF'H	Specific producătorului.

2.9. **CardActivityDailyRecord**

Informații, stocate pe un card, privind activitățile conducătorului auto într-o anumită zi calendaristică. Acest tip de date se raportează la cerințele 266, 291, 320 și 343 din anexa 1C.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength este lungimea totală în octeți a înregistrării zilnice anterioare. Valoarea maximă este dată de lungimea ȘIRULUI DE OCTEȚI care conține aceste înregistrări [a se vedea *CardActivityLengthRange* din apendicele 2 punctul 4.]. Atunci când această înregistrare este cea mai veche înregistrare zilnică, valoarea pentru *activityPreviousRecordLength* trebuie setată la 0.

activityRecordLength este lungimea totală în octeți a acestei înregistrări. Valoarea maximă este dată de lungimea ȘIRULUI DE OCTEȚI care conține aceste înregistrări.

activityRecordDate este data înregistrării.

activityDailyPresenceCounter este contorul prezenței zilnice pentru card în ziua respectivă.

activityDayDistance este distanța totală parcursă în ziua respectivă.

activityChangeInfo este setul de date *ActivityChangeInfo* pentru conducătorul auto în ziua respectivă. Acesta poate conține maximum 1 440 de valori (o schimbare de activitate pe minut). Acest set de date cuprinde întotdeauna *activityChangeInfo* care codează regimul de conducere la 00.00.

2.10. **CardActivityLengthRange**

Numărul de octeți de pe un card de conducător auto sau de pe un card de atelier, disponibil pentru stocarea înregistrărilor privind activitatea conducătorului auto.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Atribuirea valorii: a se vedea apendicele 2.

2.11. **CardApprovalNumber**

Numărul de omologare de tip al cardului.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Atribuirea valorii:

Numărul de omologare trebuie să fie furnizat așa cum este publicat pe site-ul web corespunzător al Comisiei Europene, de exemplu inclusiv cu liniuțe dacă este cazul. Numărul de omologare trebuie să fie aliniat la stânga.

2.12. **CardCertificate**

Generația 1:

Certificatul cheii publice a unui card.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Informații, stocate pe un card, privind identificarea circuitului integrat (*Integrated Circuit*, IC) al cardului (cerința 249 din anexa 1C). *icSerialNumber*, împreună cu *icManufacturingReferences*, identifică în mod unic cipul cardului. Doar *icSerialNumber* nu este suficient pentru a identifica în mod unic cipul cardului.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber este numărul de serie al IC.

icManufacturingReferences reprezintă identificatorul specific al producătorului IC.

2.14. **CardConsecutiveIndex**

Un indice secvențial al cardului [definiția h)].

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Atribuirea valorii: (a se vedea anexa 1C capitolul 7)

Ordinea de creștere: '0, …, 9, A, …, Z, a, …, z'

2.15. **CardControlActivityDataRecord**

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind ultimul control la care a fost supus conducătorul auto (cerințele 274, 299, 327 și 350 din anexa 1C).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                       ControlType,
   controlTime                       TimeReal,
   controlCardNumber                 FullCardNumber,
   controlVehicleRegistration        VehicleRegistrationIdentification,
   controlDownloadPeriodBegin        TimeReal,
   controlDownloadPeriodEnd          TimeReal
}
```

controlType este tipul de control.

controlTime este data și ora la care a avut loc controlul.

controlCardNumber este *FullCardNumber* al agentului de control care a efectuat controlul.

controlVehicleRegistration reprezintă VRN și statul membru de înmatriculare ale vehiculului în care a avut loc controlul.

controlDownloadPeriodBegin și **controlDownloadPeriodEnd** reprezintă perioada descărcată, în cazul unei descărcări.

2.16. CardCurrentUse

Informații privind utilizarea efectivă a cardului (cerințele 273, 298, 326 și 349 din anexa 1C).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                    TimeReal,
   sessionOpenVehicle                 VehicleRegistrationIdentification
}
```

sessionOpenTime este ora la care cardul a fost introdus pentru utilizarea curentă. Acest element se setează la 0 în momentul retragerii cardului.

sessionOpenVehicle este identificarea vehiculului utilizat în prezent, setată la introducerea cardului. Acest element se setează la 0 în momentul retragerii cardului.

2.17. CardDriverActivity

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind activitățile conducătorului auto (cerințele 267, 268, 292, 293, 321 și 344 din anexa 1C).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord     INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord        INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords               OCTET STRING
                                      (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord este specificarea începutului locului de stocare în memorie (numărul de octeți de la începutul șirului) a celei mai vechi înregistrări complete aferente unei zile din șirul *activityDailyRecords*. Valoarea maximă este dată de lungimea șirului.

activityPointerNewestRecord este specificarea începutului locului de stocare în memorie (numărul de octeți de la începutul șirului) a celei mai recente înregistrări complete aferente unei zile din șirul *activityDailyRecords*. Valoarea maximă este dată de lungimea șirului.

activityDailyRecords este spațiul disponibil pentru stocarea datelor privind activitatea conducătorului auto (structura datelor: *CardActivityDailyRecord*) pentru fiecare zi calendaristică în care s-a utilizat cardul.

Atribuirea valorii: acest șir de octeți este completat în mod ciclic cu înregistrări din *CardActivityDailyRecord*. La prima utilizare, stocarea începe la primul octet din șir. Toate înregistrările noi se adaugă la sfârșitul înregistrării anterioare. Atunci când șirul devine complet, stocarea se reia de la primul octet din șir, indiferent dacă există o întrerupere în interiorul unui element de date. Înainte de a plasa în șir noi date privind activitatea (prin extinderea *activityDailyRecord* curent sau prin introducerea unui nou *activityDailyRecord*) care să înlocuiască datele mai vechi privind activitatea, *activityPointerOldestDayRecord* trebuie actualizat pentru a indica noul loc al celei mai vechi înregistrări complete aferente unei zile, iar *activityPreviousRecordLength* pentru această (nouă) cea mai veche înregistrare zilnică completă trebuie resetat la 0.

2.18. CardDrivingLicenceInformation

Informații, stocate pe un card de conducător auto, privind datele permisului de conducere al titularului cardului (cerințele 259 și 284 din anexa 1C).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority este autoritatea responsabilă pentru eliberarea permisului de conducere.

drivingLicenceIssuingNation este naționalitatea autorității care a eliberat permisul de conducere.

drivingLicenceNumber este numărul permisului de conducere.

2.19. **CardEventData**

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind evenimentele asociate cu titularul cardului (cerințele 260, 285, 318 și 341 din anexa 1C).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData este o secvență, în ordine crescătoare a valorilor *EventFaultType*, a *cardEventRecords* (cu excepția înregistrărilor privind tentativele de încălcare a securității, care sunt cuprinse în ultimul set al secvenței).

cardEventRecords este un set de înregistrări de evenimente pentru un anumit tip de evenimente (sau categorie pentru evenimentele care țin de tentativele de încălcare a securității).

2.20. **CardEventRecord**

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind un eveniment asociat cu titularul cardului (cerințele 261, 286, 318 și 341 din anexa 1C).

```
CardEventRecord ::= SEQUENCE {
   eventType                            EventFaultType,
   eventBeginTime                       TimeReal,
   eventEndTime                         TimeReal,
   eventVehicleRegistration             VehicleRegistrationIdentification
}
```

eventType este tipul de eveniment.

eventBeginTime este data și ora la care a început evenimentul.

eventEndTime este data și ora la care s-a încheiat evenimentul.

eventVehicleRegistration reprezintă VRN și statul membru de înmatriculare ale vehiculului în care a avut loc evenimentul.

2.21. **CardFaultData**

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind anomaliile asociate cu titularul cardului (cerințele 263, 288, 318 și 341 din anexa 1C).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                     SET SIZE(NoOfFaultsPerType) OF
                                        CardFaultRecord
}
```

CardFaultData este o secvență care cuprinde un set de înregistrări ale anomaliilor aparaturii de înregistrare, urmat de un set de înregistrări privind anomaliile cardului.

cardFaultRecords este un set de înregistrări de anomalii dintr-o anumită categorie de anomalii (aparatură de înregistrare sau card).

2.22. **CardFaultRecord**

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind o anomalie asociată cu titularul cardului (cerințele 264, 289, 318 și 341 din anexa 1C).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType este tipul de anomalie.

faultBeginTime este data și ora la care a început anomalia.

faultEndTime este data și ora la care s-a încheiat anomalia.

faultVehicleRegistration reprezintă VRN și statul membru de înmatriculare ale vehiculului în care s-a produs anomalia.

2.23. **CardIccIdentification**

Informații, stocate pe un card, privind identificarea cardului cu circuite integrate (IC) (cerința 248 din anexa 1C).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop este modul Clockstop definit în apendicele 2.

cardExtendedSerialNumber este numărul de serie unic al cardului cu IC, așa cum este specificat de tipul de date *ExtendedSerialNumber*.

cardApprovalNumber este numărul omologării de tip a cardului.

CardPersonaliserID este ID-ul de personalizare a cardului codat ca *ManufacturerCode*.

embedderIcAssemblerId oferă informații despre integratorul/asamblorul IC.

icIdentifier este identificatorul circuitului integrat de pe card și al producătorului circuitului integrat așa cum este definit în standardul ISO/IEC 7816-6.

2.24. **CardIdentification**

Informații, stocate pe un card, referitoare la identificarea cardului (cerințele 255, 280, 310, 333, 359, 365, 371 și 377 din anexa 1C).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState              NationNumeric,
   cardNumber                          CardNumber,
   cardIssuingAuthorityName            Name,
   cardIssueDate                       TimeReal,
   cardValidityBegin                   TimeReal,
   cardExpiryDate                      TimeReal
}
```

cardIssuingMemberState este codul statului membru care eliberează cardul.

cardNumber este numărul de card al cardului.

cardIssuingAuthorityName este denumirea autorității care a eliberat cardul.

cardIssueDate este data eliberării cardului pentru titularul actual.

cardValidityBegin este data inițială de la care este valabil cardul.

cardExpiryDate este data la care expiră valabilitatea cardului.

2.25. **CardMACertificate**

Generația 2:

Certificatul cheii publice a cardului pentru autentificarea reciprocă cu o VU. Structura acestui certificat este specificată în apendicele 11.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Un număr de card conform definiției g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification             IA5String(SIZE(14)),
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification              IA5String(SIZE(13)),
      cardConsecutiveIndex             CardConsecutiveIndex,
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   }
}
```

driverIdentification este identificarea unică a unui conducător auto într-un stat membru.

ownerIdentification este identificarea unică a unei societăți, a unui atelier sau a unui organism de control în cadrul unui stat membru.

cardConsecutiveIndex este indicele secvențial al cardului.

cardReplacementIndex este indicele de înlocuire a cardului.

cardRenewalIndex este indicele de reînnoire a cardului.

Prima secvență din selecție este adecvată pentru a coda un număr de card de conducător auto, a doua secvență din selecție este adecvată pentru a coda numărul de card de atelier, numărul de card de control și, respectiv, numărul de card de societate.

2.27. **CardPlaceDailyWorkPeriod**

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind locurile în care încep și/sau se încheie zilele de lucru (cerințele 272, 297, 325 și 348 din anexa 1C).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord este indicele ultimei înregistrări actualizate a locului.

Atribuirea valorii: număr care corespunde numărătorului înregistrării privind locul, începând de la '0' pentru prima ocurență a înregistrărilor privind locurile în structură.

placeRecords este setul de înregistrări care conțin informații privind locurile introduse.

2.28. **CardPrivateKey**

Generația 1:

Cheia privată a unui card.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Cheia publică a unui card.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Un indice de reînnoire a cardului [definiția i)].

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Atribuirea valorii: (a se vedea capitolul VII din prezenta anexă).

'0' Cardul original.

Ordinea de creștere: '0, …, 9, A, …, Z'

2.31. **CardReplacementIndex**

Un indice de înlocuire a cardului [definiția j)].

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Atribuirea valorii: (a se vedea capitolul VII din prezenta anexă).

'0' Cardul original.

Ordinea de creștere: '0, …, 9, A, …, Z'

2.32. **CardSignCertificate**

Generația 2:

Certificatul cheii publice a cardului pentru semnătură. Structura acestui certificat este specificată în apendicele 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Cod care face distincția între cele două sloturi ale unei unități montate pe vehicul.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.34. **CardSlotsStatus**

Cod care indică tipurile de carduri introduse în cele două sloturi ale unității montate pe vehicul.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Atribuirea valorii – Octet aliniat: 'ccccdddd'B

'cccc'B Identificarea tipului de card introdus în slotul pentru cardul de copilot,

'dddd'B Identificarea tipului de card introdus în slotul pentru cardul de conducător auto,

cu următoarele coduri de identificare:

'0000'B niciun card introdus,

'0001'B un card de conducător auto introdus,

'0010'B un card de atelier introdus,

'0011'B un card de control introdus,

'0100'B un card de societate introdus.

2.35. **CardSlotsStatusRecordArray**

Generația 2:

CardSlotsStatus și metadatele utilizate în protocolul de descărcare.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType reprezintă tipul înregistrării (*CardSlotsStatus*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *CardSlotsStatus* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul de înregistrări *CardSlotsStatus*.

2.36. **CardStructureVersion**

Cod care indică versiunea structurii implementate într-un card de tahograf.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Atribuirea valorii: 'aabb'H:

'aa'H Indice pentru modificări ale structurii.

'00'H pentru aplicații de generația 1

'01'H pentru aplicații de generația 2

'bb'H Indice pentru schimbările privind utilizarea elementelor de date definite pentru structura dată de octetul cel mai semnificativ.

'00'H pentru această versiune a aplicațiilor de generația 1

'00'H pentru această versiune a aplicațiilor de generația 2

2.37. **CardVehicleRecord**

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind o perioadă de utilizare a unui vehicul pe durata unei zile calendaristice (cerințele 269, 294, 322 și 345 din anexa 1C).

Generația 1:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin este valoarea indicată de contorul de parcurs al vehiculului la începutul perioadei de utilizare a vehiculului.

vehicleOdometerEnd este valoarea indicată de odometrul vehiculului la sfârșitul perioadei de utilizare a vehiculului.

vehicleFirstUse reprezintă data și ora la care începe perioada de utilizare a vehiculului.

vehicleLastUse este data și ora la care se încheie perioada de utilizare a vehiculului.

vehicleRegistration reprezintă VRN și statul membru de înmatriculare a vehiculului.

vuDataBlockCounter este valoarea *VuDataBlockCounter* la ultima extragere de date din perioada de utilizare a vehiculului.

Generația 2:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

În plus față de generația 1, se utilizează următorul element de date:

VehicleIdentificationNumber este numărul de identificare a vehiculului care se referă la vehicul în ansamblul său.

2.38. **CardVehiclesUsed**

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind vehiculele utilizate de titularul cardului (cerințele 270, 295, 323 și 346 din anexa 1C).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord este indicele ultimei înregistrări actualizate a vehiculului.

Atribuirea valorii: număr care corespunde numărătorului înregistrării privind vehiculul, începând de la '0' pentru prima ocurență a înregistrărilor privind vehiculele în structură.

cardVehicleRecords este setul de înregistrări care conțin informații privind vehiculele utilizate.

2.39. **CardVehicleUnitRecord**

Generația 2:

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind o unitate montată pe vehicul care a fost utilizată (cerințele 303 și 351 din anexa 1C).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                           TimeReal,
   manufacturerCode                    ManufacturerCode,
   deviceID                            INTEGER(0..255),
   vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp este începutul perioadei de utilizare a unității montate pe vehicul (și anume, prima introducere a cardului în unitatea montată pe vehicul pentru perioada respectivă).

manufacturerCode identifică producătorul unității montate pe vehicul.

deviceID identifică tipul unității montate pe vehicul a unui producător. Valoarea este specifică producătorului.

vuSoftwareVersion este numărul versiunii software-ului instalat pe unitatea montată pe vehicul.

2.40. **CardVehicleUnitsUsed**

Generația 2:

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind unitățile montate pe vehicul utilizate de titularul cardului (cerințele 306 și 352 din anexa 1C).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord este indicele ultimei înregistrări actualizate privind unitatea montată pe vehicul.

Atribuirea valorii: număr care corespunde numărătorului înregistrării privind unitatea montată pe vehicul, începând de la '0' pentru prima ocurență a înregistrărilor privind unitățile montate pe vehicul în structură.

cardVehicleUnitRecords este setul de înregistrări care conțin informații privind unitățile montate pe vehicul utilizate.

2.41. **Certificat**

Certificatul unei chei publice emise de o autoritate de certificare.

Generația 1:

```
Certificate ::= OCTET STRING (SIZE(194))
```

Atribuirea valorii: semnătură digitală cu recuperarea parțială a *CertificateContent* conform apendicelui 11 „Mecanisme de securitate comune": Semnătura (128 de octeți) || Restul cheii publice (58 de octeți) || Identificatorul autorității de certificare (8 octeți).

Generația 2:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Atribuirea valorii: a se vedea apendicele 11.

2.42. **CertificateContent**

Generația 1:

Conținutul (în clar) al certificatului unei chei publice conform apendicelui 11 „Mecanisme de securitate comune".

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier         INTEGER(0..255),
   certificationAuthorityReference      KeyIdentifier,
   certificateHolderAuthorisation       CertificateHolderAuthorisation,
   certificateEndOfValidity             TimeReal,
   certificateHolderReference           KeyIdentifier,
   publicKey                            PublicKey
}
```

certificateProfileIdentifier este versiunea certificatului corespunzător.

Atribuirea valorii: '01h'pentru această versiune.

certificationAuthorityReference identifică autoritatea de certificare care a emis certificatul. De asemenea, identifică cheia publică a autorității de certificare în cauză.

certificateHolderAuthorisation identifică drepturile deținătorului certificatului.

certificateEndOfValidity este data la care certificatul expiră din punct de vedere administrativ.

certificateHolderReference identifică deținătorul certificatului. De asemenea, identifică cheia publică a acestuia.

publicKey este cheia publică care este certificată prin intermediul certificatului respectiv.

2.43. **CertificateHolderAuthorisation**

Identificarea drepturilor unui deținător de certificat.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

Generația 1:

tachographApplicationID este identificatorul de aplicație pentru aplicația tahografică.

Atribuirea valorii: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Acest AID este un identificator exclusiv de aplicație neînregistrat conform standardului ISO/IEC 7816-5.

equipmentType este identificarea tipului de echipament pentru care se emite certificatul.

Atribuirea valorii: în conformitate cu tipul de date *EquipmentType*. **0** dacă certificatul este emis de unul din statele membre.

Generația 2:

tachographApplicationID reprezintă cei mai importanți 6 octeți din identificatorul de aplicație pentru cardurile de tahograf de generația 2 (AID). AID pentru aplicația de card de tahograf este specificat în capitolul 6.2.

Atribuirea valorii: 'FF 53 4D 52 44 54'.

equipmentType este identificarea tipului de echipament specificat pentru generația 2, pentru care se emite certificatul.

Atribuirea valorii: în conformitate cu tipul de date *EquipmentType*.

2.44. **CertificateRequestID**

Cod unic de identificare a unei cereri de certificat. Se poate utiliza și ca identificator al cheii publice a unității montate pe vehicul dacă numărul de serie al unității montate pe vehicul căreia îi este destinată cheia nu este cunoscut în momentul generării certificatului.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber este un număr de serie aferent cererii de certificat, fiind un număr unic pentru producător și pentru luna definită mai jos.

requestMonthYear este identificarea lunii și a anului în care s-a depus cererea de certificat.

Atribuirea valorii: codarea BCD a lunii (două cifre) și a anului (ultimele două cifre).

crIdentifier: este un identificator care are rolul de a face distincția între o cerere de certificat și un număr de serie lung.

Atribuirea valorii: 'FFh'.

manufacturerCode: este codul numeric al producătorului care solicită certificatul.

2.45. **CertificationAuthorityKID**

Identificatorul cheii publice a unei autorități de certificare (un stat membru sau Autoritatea europeană de certificare).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric este codul numeric național al autorității de certificare.

nationAlpha este codul alfanumeric național al autorității de certificare.

keySerialNumber este numărul de serie care face distincția între diferitele chei ale autorității de certificare dacă aceste chei se modifică.

additionalInfo este un câmp de doi octeți pentru codări suplimentare (specifice autorității de certificare).

caIdentifier este un identificator care face distincția dintre un identificator al cheii autorității de certificare și identificatorii altor chei.

Atribuirea valorii: '01h'.

2.46. **CompanyActivityData**

Informații, stocate pe un card de societate, privind activitățile efectuate cu cardul (cerințele 373 și 379 din anexa 1C).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord        INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords            SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord             SEQUENCE {
     companyActivityType               CompanyActivityType,
     companyActivityTime               TimeReal,
     cardNumberInformation             FullCardNumber,
     vehicleRegistrationInformation    VehicleRegistrationIdentification,
     downloadPeriodBegin               TimeReal,
     downloadPeriodEnd                 TimeReal
    }
}
```

companyPointerNewestRecord este indicele ultimei *companyActivityRecord* actualizate.

Atribuirea valorii: număr care corespunde numărătorului înregistrării privind activitatea societății, începând cu '0' pentru prima ocurență a unei înregistrări privind activitatea societății în structură.

companyActivityRecords este setul tuturor înregistrărilor privind activitățile societății.

companyActivityRecord este o secvență de informații referitoare la o activitate a societății.

companyActivityType este tipul de activitate a societății.

companyActivityTime este data și ora activității societății.

cardNumberInformation este numărul cardului și statul membru emitent al cardului descărcat, dacă este cazul.

vehicleRegistrationInformation reprezintă VRN și statul membru de înmatriculare a vehiculului care au fost descărcate, blocate sau deblocate.

downloadPeriodBegin și **downloadPeriodEnd** reprezintă perioada descărcată din VU, dacă este cazul.

2.47. **CompanyActivityType**

Cod care indică o activitate desfășurată de o societate prin utilizarea propriului card de societate.

```
CompanyActivityType ::= INTEGER {
   card downloading                    (1),
   VU downloading                      (2),
   VU lock-in                          (3),
   VU lock-out                         (4)
}
```

2.48. **CompanyCardApplicationIdentification**

Informații, stocate pe un card de societate, privind identificarea aplicației cardului (cerințele 369 și 375 din anexa 1C).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId precizează tipul de card implementat.

cardStructureVersion precizează versiunea structurii implementate în card.

noOfCompanyActivityRecords este numărul de înregistrări privind activitățile societății care pot fi stocate pe card.

2.49. **CompanyCardHolderIdentification**

Informații, stocate pe un card de societate, privind identificarea titularului cardului (cerințele 372 și 378 din anexa 1C).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName este denumirea societății deținătoare.

companyAddress este adresa societății deținătoare.

cardHolderPreferredLanguage este limba preferată de titularul cardului.

2.50. **ControlCardApplicationIdentification**

Informații, stocate pe un card de control, privind identificarea aplicației cardului (cerințele 357 și 363 din anexa 1C).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId precizează tipul de card implementat.

cardStructureVersion precizează versiunea structurii implementate în card.

noOfControlActivityRecords este numărul înregistrărilor privind activitățile de control care pot fi stocate pe card.

2.51. **ControlCardControlActivityData**

Informații, stocate pe un card de control, privind activitățile de control efectuate cu cardul (cerințele 361 și 367 din anexa 1C).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord        INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords            SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord             SEQUENCE {
     controlType                       ControlType,
     controlTime                       TimeReal,
     controlledCardNumber              FullCardNumber,
     controlledVehicleRegistration     VehicleRegistrationIdentification,
     controlDownloadPeriodBegin        TimeReal,
     controlDownloadPeriodEnd          TimeReal
    }
}
```

controlPointerNewestRecord este indicele ultimei înregistrări actualizate privind activitățile de control.

Atribuirea valorii: număr care corespunde numărătorului înregistrării privind activitatea de control, începând cu '0' pentru prima ocurență a unei înregistrări privind activitatea de control în structură.

controlActivityRecords este setul tuturor înregistrărilor privind activitățile de control.

controlActivityRecord este secvența de informații privind o activitate de control.

controlType este tipul de control.

controlTime este data și ora la care a avut loc controlul.

controlledCardNumber reprezintă numărul cardului și statul membru emitent al cardului controlat.

controlledVehicleRegistration reprezintă VRN și statul membru de înmatriculare ale vehiculului în care a avut loc controlul.

controlDownloadPeriodBegin și **controlDownloadPeriodEnd** reprezintă perioada descărcată.

2.52. **ControlCardHolderIdentification**

Informații, stocate pe un card de control, privind identificarea titularului cardului (cerințele 360 și 366 din anexa 1C).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                    Name,
   controlBodyAddress                 Address,
   cardHolderName                     HolderName,
   cardHolderPreferredLanguage        Language
}
```

controlBodyName este denumirea organismului de control al titularului cardului.

controlBodyAddress este adresa organismului de control al titularului cardului.

cardHolderName reprezintă numele și prenumele titularului cardului de control.

cardHolderPreferredLanguage este limba preferată de titularul cardului.

2.53. **ControlType**

Cod care indică activitățile desfășurate în timpul unui control. Acest tip de date se raportează la cerințele 126, 274, 299, 327 și 350 din anexa 1C.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Generația 1:

Atribuirea valorii – Octet aliniat: 'cvpdxxxx'B (8 biți)

'c'B descărcare de pe card:

'0'B: informațiile de pe card nu sunt descărcate în timpul acestei activități de control,

'1'B: informațiile de pe card sunt descărcate în timpul acestei activități de control

'v'B descărcare din VU:

'0'B: informațiile din VU nu sunt descărcate în timpul acestei activități de control,

'1'B: informațiile din VU sunt descărcate în timpul acestei activități de control

'p'B imprimare:

'0'B: nu s-a imprimat nimic în timpul acestei activități de control,

'1'B: s-au imprimat informații în timpul acestei activități de control

'd'B afișaj:

'0'B: nu s-a utilizat afișajul în timpul acestei activități de control,

'1'B: s-a utilizat afișajul în timpul acestei activități de control

'xxxx'B Neutilizat.

Generația 2:

Atribuirea valorii – Octet aliniat: 'cvpdexxx'B (8 biți)

'c'B descărcare de pe card:

'0'B: informațiile de pe card nu sunt descărcate în timpul acestei activități de control,

'1'B: informațiile de pe card sunt descărcate în timpul acestei activități de control

'v'B descărcare din VU:

'0'B: informațiile din VU nu sunt descărcate în timpul acestei activități de control,

'1'B: informațiile din VU sunt descărcate în timpul acestei activități de control

'p'B imprimare:

'0'B: nu s-a imprimat nimic în timpul acestei activități de control,

'1'B: s-au imprimat informații în timpul acestei activități de control

'd'B afișaj:

'0'B: nu s-a utilizat afișajul în timpul acestei activități de control,

'1'B: s-a utilizat afișajul în timpul acestei activități de control

'e'B	verificarea etalonării în trafic:
	'0'B: parametrii de etalonare nu sunt verificați în timpul acestei activități de control,
	'1'B: parametrii de etalonare sunt verificați în timpul acestei activități de control
'xxx'B	RFU.

2.54. **CurrentDateTime**

Data și ora curente, afișate de aparatul de înregistrare.

```
CurrentDateTime ::= TimeReal
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.55. **CurrentDateTimeRecordArray**

Generația 2:

Data și ora curente, plus metadatele utilizate în protocolul de descărcare.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType reprezintă tipul înregistrării (*CurrentDateTime*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *CurrentDateTime* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări ale datei și orei curente.

2.56. **DailyPresenceCounter**

Contor, stocat pe un card de conducător auto sau pe un card de atelier, incrementat cu o unitate pentru fiecare zi calendaristică în care cardul a fost introdus într-o VU. Acest tip de date se raportează la cerințele 266, 299, 320 și 343 din anexa 1C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Atribuirea valorii: număr consecutiv cu valoare maximă = 9 999, începând apoi din nou de la 0. În momentul primei emiteri a cardului, numărul este setat la 0.

2.57. **Datef**

Data exprimată într-un format numeric care poate fi imprimat imediat.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Atribuirea valorii:

yyyy	Anul
mm	Luna
dd	Ziua
'00000000'H	reprezintă în mod explicit „nicio dată".

2.58. **DateOfDayDownloaded**

Generația 2:

Data și ora descărcării.

```
DateOfDayDownloaded ::= TimeReal
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.59. **DateOfDayDownloadedRecordArray**

Generația 2:

Data și ora descărcării plus metadate, astfel cum se utilizează în protocolul de descărcare.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType reprezintă tipul înregistrării (*DateOfDayDownloaded*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *CurrentDateTime* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul de înregistrări ale datei și orei de descărcare.

2.60. **Distance**

O distanță parcursă (rezultatul calculării diferenței dintre două valori afișate de odometrul unui vehicul, în kilometri).

```
Distance ::= INTEGER(0..2^16-1)
```

Atribuirea valorii: Binar fără semn. Valoarea în kilometri în intervalul operațional 0 – 9 999 km.

2.61. **DriverCardApplicationIdentification**

Informații, stocate pe un card de conducător auto, privind identificarea aplicației cardului (cerințele 253 și 278 din anexa 1C).

Generația 1:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId precizează tipul de card implementat.

cardStructureVersion precizează versiunea structurii implementate în card.

noOfEventsPerType reprezintă numărul de evenimente, per tip de eveniment, pe care cardul le poate înregistra.

noOfFaultsPerType reprezintă numărul de anomalii, per tip de anomalie, pe care cardul le poate înregistra.

activityStructureLength indică numărul de octeți disponibili pentru stocarea înregistrărilor privind activitățile.

noOfCardVehicleRecords este numărul de înregistrări privind vehiculele pe care cardul le poate conține.

noOfCardPlaceRecords este numărul de locuri pe care cardul le poate înregistra.

Generația 2:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

În plus față de generația 1, se utilizează următoarele elemente de date:

noOfGNSSCDRecords este numărul de înregistrări GNSS privind timpul de conducere continuă care pot fi stocate pe card.

noOfSpecificConditionRecords este numărul de înregistrări privind condițiile specifice care pot fi stocate pe card.

2.62. DriverCardHolderIdentification

Informații, stocate pe un card de conducător auto, privind identificarea titularului cardului (cerințele 256 și 281 din anexa 1C).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

cardHolderName reprezintă numele și prenumele titularului cardului de conducător auto.

cardHolderBirthDate este data de naștere a titularului cardului de conducător auto.

cardHolderPreferredLanguage este limba preferată de titularul cardului.

2.63. **DSRCSecurityData**

Generația 2:

Informații sub formă de text în clar și MAC care urmează a fi transmise prin DSRC de la tahograf la echipamentul de interogare la distanță (RI), pentru mai multe detalii a se vedea apendicele 11 partea B capitolul 13.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength face parte din codarea DER-TLV și trebuie setată la '81 10' (a se vedea apendicele 11 partea B capitolul 13).

currentDateTime este data și ora curentă a unității montate pe vehicul**.**

counter enumeră mesajele RTM.

vuSerialNumber este numărul de serie al unității montate pe vehicul.

dSRCMKVersionNumber numărul versiunii cheii *master* DSRC din care derivă cheile DSRC specifice ale VU.

tagLengthMac reprezintă eticheta și lungimea obiectului de date MAC ca parte a codării DER-TLV. Eticheta se setează la '8E', lungimea codează lungimea MAC în octeți (a se vedea apendicele 11 partea B capitolul 13).

mac reprezintă MAC calculat pe mesajul RTM (a se vedea apendicele 11 partea B capitolul 13).

2.64. **EGFCertificate**

Generația 2:

Certificatul cheii publice a echipamentului GNSS extern pentru autentificarea reciprocă cu o VU. Structura acestui certificat este specificată în apendicele 11.

```
EGFCertificate ::= Certificate
```

2.65. **EmbedderIcAssemblerId**

Oferă informații referitoare la integratorul IC.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode este codul de țară format din 2 litere al integratorului modulului conform ISO 3166**.**

moduleEmbedder identifică integratorul modulului.

manufacturerInformation pentru uzul intern al producătorului.

2.66. **EntryTypeDailyWorkPeriod**

Cod care face distincția între începutul și sfârșitul unei introduceri de date privind locul unde s-a desfășurat o zi de lucru și condițiile în care s-a realizat introducerea de date respectivă.

Generația 1

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Atribuirea valorii: conform standardului ISO/IEC 8824-1.

Generația 2

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Atribuirea valorii: conform standardului ISO/IEC 8824-1.

2.67. **EquipmentType**

Cod care face distincția între diferite tipuri de aparatură pentru aplicația tahografică.

```
EquipmentType ::= INTEGER(0..255)
```

Generația 1:

```
--Reserved                          (0),
--Driver Card                       (1),
--Workshop Card                     (2),
--Control Card                      (3),
--Company Card                      (4),
--Manufacturing Card                (5),
--Vehicle Unit                      (6),
--Motion Sensor                     (7),
--RFU                               (8..255)
```

Atribuirea valorii: conform standardului ISO/IEC 8824-1.

Valoarea 0 este rezervată pentru a desemna un stat membru sau Europa în câmpul CHA al certificatelor.

Generația 2:

Sunt utilizate aceleași valori ca în generația 1, cu următoarele completări:

```
--GNSS Facility                          (8),
--Remote Communication Module            (9),
--ITS interface module                   (10),
--Plaque                                 (11), -- may be used in SealRecord
--M1/N1 Adapter                          (12), -- may be used in SealRecord
--European Root CA (ERCA)                (13),
--Member State CA (MSCA)                 (14),
--External GNSS connection               (15), -- may be used in SealRecord
--Unused                                 (16), -- used in SealDataVu
--RFU                                    (17..255)
```

Notă: valorile aferente generației 2 pentru plăcuță, pentru adaptor și pentru conexiunea GNSS externă, precum și valorile aferente generației 1 pentru unitatea montată pe vehicul și pentru senzorul de mișcare pot fi utilizate în *SealRecord*, adică dacă este cazul.

2.68. **EuropeanPublicKey**

Generația 1:

Cheia publică europeană.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Cod care explică de ce s-a înregistrat un anumit eveniment sau o anumită anomalie.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Atribuirea valorii:

'00'H	unul/una dintre cele mai recente (sau ultimele) 10 evenimente sau anomalii
'01'H	evenimentul cel mai de durată pentru una din ultimele 10 zile de producere a unui eveniment
'02'H	unul dintre cele mai de durată 5 evenimente din ultimele 365 de zile
'03'H	ultimul eveniment pentru una din ultimele 10 zile de producere a unui eveniment
'04'H	cel mai grav eveniment pentru una din ultimele 10 zile de producere a unui eveniment
'05'H	unul dintre cele mai grave 5 evenimente din ultimele 365 de zile
'06'H	primul eveniment sau prima anomalie care a survenit după ultima etalonare
'07'H	un eveniment activ/în curs sau o anomalie activă/în curs
'08'H to '7F'H	RFU
'80'H to 'FF'H	specific producătorului

2.70. **EventFaultType**

Cod prin care se caracterizează un eveniment sau o anomalie.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Atribuirea valorii:

Generația 1:

'0x'H	Evenimente generale,
'00'H	Nu sunt disponibile detalii suplimentare,
'01'H	Introducerea unui card nevalabil,
'02'H	Conflict de carduri,
'03'H	Suprapunerea timpului,
'04'H	Conducere fără un card adecvat,
'05'H	Introducerea cardului în timpul conducerii,
'06'H	Ultima sesiune a cardului nu a fost încheiată corect,
'07'H	Depășire a limitei de viteză,
'08'H	Întrerupere a alimentării cu energie electrică,
'09'H	Eroare privind datele de la senzorul de mișcare,
'0A'H	Conflict privind deplasarea vehiculului,
'0B' to '0F'H	RFU,

'1x'H	Evenimente care țin de tentativele de încălcare a securității privind unitatea montată pe vehicul,
'10'H	Nu sunt disponibile detalii suplimentare,
'11'H	Eroare de autentificare a senzorului de mișcare,
'12'H	Eroare de autentificare a cardului de tahograf,
'13'H	Înlocuirea neautorizată a senzorului de mișcare,
'14'H	Eroare de integritate care afectează introducerea datelor pe card,
'15'H	Eroare de integritate a datelor stocate privind utilizatorul,
'16'H	Eroare de transfer intern de date,
'17'H	Deschidere neautorizată a carcasei,
'18'H	Sabotarea hardware-ului,
'19'H to '1F'H	RFU,
'2x'H	Evenimente care țin de tentativele de încălcare a securității privind senzorul,
'20'H	Nu sunt disponibile detalii suplimentare,
'21'H	Eroare de autentificare,
'22'H	Eroare de integritate a datelor stocate,
'23'H	Eroare de transfer intern de date,
'24'H	Deschidere neautorizată a carcasei,
'25'H	Sabotarea hardware-ului,
'26'H to '2F'H	RFU,
'3x'H	Anomalii ale aparaturii de înregistrare,
'30'H	Nu sunt disponibile detalii suplimentare,
'31'H	Anomalie internă a VU,
'32'H	Anomalie a imprimantei,
'33'H	Anomalie a afișajului,
'34'H	Anomalie la descărcare,
'35'H	Anomalie a senzorului,
'36'H to '3F'H	RFU,
'4x'H	Anomalii ale cardului,
'40'H	Nu sunt disponibile detalii suplimentare,
'41'H to '4F'H	RFU,
'50'H to '7F'H	RFU,
'80'H to 'FF'H	Specific producătorului.

Generația 2:

Sunt utilizate aceleași valori ca în generația 1, cu următoarele completări:

'0B'H	Conflict oră (GNSS față de ceasul intern al VU),
'0C' to '0F'H	RFU,
'5x'H	Anomalii legate de GNSS,
'50'H	Nu sunt disponibile detalii suplimentare,
'51'H	Anomalie a receptorului GNSS intern,
'52'H	Anomalie a receptorului GNSS extern,
'53'H	Anomalie de comunicare GNSS externă,
'54'H	Nu sunt disponibile date de poziționare GNSS,
'55'H	Detectare a manipulării frauduloase a GNSS,
'56'H	Certificatul echipamentului GNSS extern a expirat,
'57'H to '5F'H	RFU,
'6x'H	Anomalii legate de modulul de comunicare la distanță,
'60'H	Nu sunt disponibile detalii suplimentare,
'61'H	Anomalie a modulului de comunicare la distanță,
'62'H	Anomalie de comunicare a modulului de comunicare la distanță,
'63'H to '6F'H	RFU,
'7x'H	Anomalii ale interfeței ITS,
'70'H	Nu sunt disponibile detalii suplimentare,
'71'H to '7F'H	RFU.

2.71. **ExtendedSealIdentifier**

Generația 2:

Identificatorul lung al sigiliului identifică în mod unic un sigiliu (cerința 401 din anexa 1C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode este codul producătorului sigiliului.

sealIdentifier este un identificator al sigiliului care este unic pentru producător.

2.72. **ExtendedSerialNumber**

Identificare unică a unui echipament. Poate fi utilizat și ca identificator al cheii publice a unui echipament.

Generația 1:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber este numărul de serie al echipamentului, unic pentru producător, tipul echipamentului, luna și anul descrise în continuare.

monthYear este identificarea lunii și a anului de producție (sau de atribuire a numărului de serie).

Atribuirea valorii: codarea BCD a lunii (două cifre) și a anului (ultimele două cifre).

type este un identificator al tipului de echipament.

Atribuirea valorii: specifică producătorului, cu valoarea rezervată 'FFh'.

manufacturerCode: este codul numeric care identifică un producător de echipamente omologate de tip.

Generația 2:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                EquipmentType,
   manufacturerCode                    ManufacturerCode
}
```

serialNumber a se vedea generația 1.

monthYear a se vedea generația 1.

type indică tipul de echipament.

manufacturerCode: a se vedea generația 1.

2.73. **FullCardNumber**

Cod prin care se identifică complet un card de tahograf.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType este tipul cardului de tahograf.

cardIssuingMemberState este codul statului membru care a emis cardul.

cardNumber este numărul cardului.

2.74. **FullCardNumberAndGeneration**

Generația 2:

Cod prin care se identifică complet un card de tahograf și generația sa.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identifică cardul de tahograf.

generation indică generația cardului de tahograf utilizat.

2.75. **Generation**

Generația 2:

Indică generația tahografului utilizat.

```
Generation ::= INTEGER(0..255)
```

Atribuirea valorii:

'00'H	RFU
'01'H	Generația 1
'02'H	Generația 2
'03'H .. 'FF'H	RFU

2.76. **GeoCoordinates**

Generația 2:

Coordonatele geografice sunt codate sub formă de numere întregi. Aceste numere întregi sunt multipli ai codării ±DDMM.M pentru latitudine și ±DDDMM.M pentru longitudine. Aici ±DD, respectiv ± DDD, denotă gradele, iar MM.M minutele.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude este codată ca multiplu (factor 10) al reprezentării ±DDMM.M.

longitude este codată ca multiplu (factor 10) al reprezentării ±DDDMM.M.

2.77. **GNSSAccuracy**

Generația 2:

Precizia datelor de poziționare GNSS [definiția eee)]. Această precizie este codată ca număr întreg și este un multiplu (factor 10) al valorii X.Y furnizate de propoziția GSA NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Generația 2:

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind poziția GNSS a vehiculului dacă timpul de conducere continuă al conducătorului auto ajunge la un multiplu de trei ore (cerințele 306 și 354 din anexa 1C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord            INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords         SET SIZE(NoOfGNSSCDRecords) OF
                                        GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord este indicele ultimei înregistrări actualizate GNSS a timpului de conducere continuă.

Atribuirea valorii: număr care corespunde numărătorului înregistrării GNSS privind conducerea continuă, începând de la '0' pentru prima ocurență a înregistrării GNSS privind conducerea continuă în structură.

gnssContinuousDrivingRecords este setul de înregistrări care conțin data și ora la care timpul de conducere continuă atinge un multiplu de trei ore și informații privind poziția vehiculului.

2.79. **GNSSContinuousDrivingRecord**

Generația 2:

Informații, stocate pe un card de conducător auto sau pe un card de atelier, privind poziția GNSS a vehiculului dacă timpul de conducere continuă al conducătorului auto ajunge la un multiplu de trei ore (cerințele 305 și 353 din anexa 1C).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssPlaceRecord                      GNSSPlaceRecord
}
```

timeStamp este data și ora la care timpul de conducere continuă al titularului cardului ajunge la un multiplu de trei ore.

gnssPlaceRecord conține informații referitoare la poziția vehiculului.

2.80. **GNSSPlaceRecord**

Generația 2:

Informații referitoare la poziția GNSS a vehiculului (cerințele 108, 109, 110, 296, 305, 347 și 353 din anexa 1C).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssAccuracy                         GNSSAccuracy,
   geoCoordinates                       GeoCoordinates
}
```

timeStamp este data și ora la care a fost stabilită poziția GNSS a vehiculului.

gnssAccuracy este precizia datelor de poziționare GNSS.

geoCoordinates este locul înregistrat folosind GNSS.

2.81. **HighResOdometer**

Valoarea indicată de odometrul vehiculului: distanța cumulată parcursă de vehicul în timpul exploatării acestuia.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Atribuirea valorii: binar fără semn. Valoare în 1/200 km cuprinsă în intervalul operațional 0 – 21 055 406 km.

2.82. **HighResTripDistance**

O distanță parcursă pe întreaga durată sau într-o parte a cursei.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Atribuirea valorii: binar fără semn. Valoare în 1/200 km cuprinsă în intervalul operațional 0 – 21 055 406 km.

2.83. **HolderName**

Numele și prenumele titularului cardului.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname este numele (numele de familie) al titularului. Acest nume de familie nu cuprinde titluri.

Atribuirea valorii: dacă un card nu este personal, *holderSurname* conține aceleași informații ca și *companyName*, *workshopName* sau *controlBodyName*.

holderFirstNames reprezintă prenumele și inițialele titularului.

2.84. **InternalGNSSReceiver**

Generația 2:

Informații care specifică dacă receptorul GNSS este intern sau extern unității montate pe vehicul. *True* înseamnă că receptorul GNSS este o parte internă a VU. *False* înseamnă că receptorul GNSS este extern.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Constanta aparaturii de înregistrare [definiția (m)].

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Atribuirea valorii: impulsuri pe kilometru într-un interval operațional de la 0 la 64 255 impulsuri/km.

2.86. **KeyIdentifier**

Un identificator unic al unei chei publice utilizat pentru a identifica și a selecta cheia. Acesta identifică și titularul cheii.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber                ExtendedSerialNumber,
   certificateRequestID                CertificateRequestID,
   certificationAuthorityKID           CertificationAuthorityKID
}
```

Prima opțiune este adecvată pentru a identifica cheia publică a unei unități montate pe vehicul sau a unui card de tahograf.

A doua opțiune este adecvată pentru a identifica cheia publică a unei unități montate pe vehicul (în cazul în care numărul de serie al unității montate pe vehicul nu poate fi cunoscut în momentul generării certificatului).

A treia opțiune este adecvată pentru a identifica cheia publică a unui stat membru.

2.87. **KMWCKey**

Generația 2:

Cheia AES și versiunea cheii care îi este asociată, utilizată pentru asocierea VU – senzor de mișcare. Pentru detalii, a se vedea apendicele 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                             AESKey,
   keyVersion                          INTEGER (SIZE(1))
}
```

kMWCKey este lungimea cheii AES concatenate cu cheia care este folosită pentru asocierea VU – senzor de mișcare.

keyVersion reprezintă versiunea cheii AES.

2.88. **Language**

Codul de identificare a unei limbi.

```
Language ::= IA5String(SIZE(2))
```

Atribuirea valorii: O codare de două litere minuscule conform standardului ISO 639.

2.89. **LastCardDownload**

Data și ora, stocate pe un card de conducător auto, la care s-a efectuat ultima descărcare a informațiilor de pe card (în alte scopuri decât în vederea unui control)(cerințele 257 și 282 din anexa 1C). Această dată poate fi actualizată de o VU sau de orice cititor de card.

```
LastCardDownload ::= TimeReal
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.90. **LinkCertificate**

Generația 2:

Certificatul de legătură între perechi de chei *European Root CA*.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Circumferința efectivă a roților [definiția u)].

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

Atribuirea valorii: binar fără semn, valoare în 1/8 mm cuprinsă în intervalul operațional 0 – 8 031 mm.

2.92. **MAC**

Generația 2:

O sumă de verificare criptografică cu lungimea de 8, 12 sau 16 octeți, care corespunde suitelor cifru specificate în apendicele 11.

```
MAC ::= CHOICE {
   mac8                                 OCTET STRING (SIZE(8)),
   mac12                                OCTET STRING (SIZE(12)),
   mac16                                OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Cod care specifică dacă un titular de card a introdus manual activitățile conducătorului auto la introducerea cardului sau nu (cerința 081 din anexa 1B și cerința 102 din anexa 1C).

```
ManualInputFlag ::= INTEGER {
   noEntry                              (0)
   manualEntries                        (1)
}
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.94. **ManufacturerCode**

Cod de identificare al unui producător de echipamente omologate de tip.

```
ManufacturerCode ::= INTEGER(0..255)
```

Laboratorul responsabil cu efectuarea testelor de interoperabilitate menține și publică lista codurilor de producător pe site-ul său web (cerința 454 din anexa 1C).

ManufacturerCodes se alocă provizoriu producătorilor de echipamente tahografice în urma depunerii unei cereri la laboratorul responsabil cu efectuarea testelor de interoperabilitate.

2.95. **ManufacturerSpecificEventFaultData**

Generația 2:

Codurile de eroare specifice producătorului simplifică analiza erorilor și întreținerea unităților montate pe vehicule.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                     ManufacturerCode,
   manufacturerSpecificErrorCode        OCTET STRING(SIZE(3))
}
```

manufacturerCode identifică producătorul unității montate pe vehicul.

manufacturerSpecificErrorCode este un cod de eroare specific producătorului.

2.96. **MemberStateCertificate**

Certificatul unei chei publice a unui stat membru, eliberat de autoritatea europeană de certificare.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Generația 2:

Certificatul statului membru plus metadatele utilizate în protocolul de descărcare.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType reprezintă tipul înregistrării (*MemberStateCertificate*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *MemberStateCertificate* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*. Valoarea se setează la 1 deoarece certificatele pot avea diferite lungimi.

records este setul de certificate ale statelor membre.

2.98. **MemberStatePublicKey**

Generația 1:

Cheia publică a unui stat membru.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Un nume.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage indică un set de caractere definit în capitolul 4,

name este un nume codat cu ajutorul setului de caractere precizat.

2.100. **NationAlpha**

Trimiterea alfabetică la o țară se face în conformitate cu semnele distinctive utilizate pentru vehicule în traficul internațional (Convenția ONU de la Viena asupra circulației rutiere, 1968).

```
NationAlpha ::= IA5String(SIZE(3))
```

Codurile *Nation Alpha* și *Numeric* trebuie să figureze pe o listă menținută pe site-ul web al laboratorului desemnat să efectueze testele de interoperabilitate, astfel cum se prevede la cerința 440 din anexa 1C.

2.101. **NationNumeric**

Cod numeric care desemnează o țară.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Atribuirea valorii: a se vedea tipul de date 2.100 (*NationAlpha*).

Orice modificare sau actualizare a specificației *Nation Alpha* sau *Numeric* descrise în paragraful anterior se efectuează numai după ce laboratorul desemnat s-a consultat cu producătorii unităților de tahograf digital și inteligent montate pe vehicule, care dețin omologare de tip.

2.102. **NoOfCalibrationRecords**

Numărul de înregistrări ale operațiunilor de etalonare care pot fi stocate pe un card de atelier.

Generația 1:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Atribuirea valorii: a se vedea apendicele 2.

Generația 2:

$$\texttt{NoOfCalibrationRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Atribuirea valorii: a se vedea apendicele 2.

2.103. **NoOfCalibrationsSinceDownload**

Contor care indică numărul de operațiuni de etalonare efectuate cu un card de atelier de la ultima descărcare a datelor de pe cardul respectiv (cerințele 317 și 340 din anexa 1C).

$$\texttt{NoOfCalibrationsSinceDownload ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.104. **NoOfCardPlaceRecords**

Numărul de înregistrări privind locurile care pot fi stocate pe un card de conducător auto sau de atelier.

Generația 1:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Atribuirea valorii: a se vedea apendicele 2.

Generația 2:

$$\texttt{NoOfCardPlaceRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Atribuirea valorii: a se vedea apendicele 2.

2.105. **NoOfCardVehicleRecords**

Numărul de înregistrări privind vehiculele utilizate care pot fi stocate pe un card de conducător auto sau de atelier.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Atribuirea valorii: a se vedea apendicele 2.

2.106. **NoOfCardVehicleUnitRecords**

Generația 2:

Numărul de înregistrări privind unitățile montate pe vehicul utilizate care pot fi stocate pe un card de conducător auto sau de atelier.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Atribuirea valorii: a se vedea apendicele 2.

2.107. **NoOfCompanyActivityRecords**

Numărul de înregistrări privind activitățile societății care pot fi stocate pe un card de societate.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Atribuirea valorii: a se vedea apendicele 2.

2.108. **NoOfControlActivityRecords**

Numărul de înregistrări privind activitățile de control care pot fi stocate pe un card de control.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Atribuirea valorii: a se vedea apendicele 2.

2.109. **NoOfEventsPerType**

Numărul de evenimente, per tip de eveniment, care pot fi stocate pe un card.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Atribuirea valorii: a se vedea apendicele 2.

2.110. **NoOfFaultsPerType**

Numărul de anomalii, per tip de anomalie, care pot fi stocate pe un card.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Atribuirea valorii: a se vedea apendicele 2.

2.111. **NoOfGNSSCDRecords**

Generația 2:

Numărul de înregistrări GNSS privind timpul de conducere continuă care pot fi înregistrate pe un card.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Atribuirea valorii: a se vedea apendicele 2.

2.112. **NoOfSpecificConditionRecords**

Generația 2:

Numărul de înregistrări privind condițiile specifice care pot fi înregistrate pe un card.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Atribuirea valorii: a se vedea apendicele 2.

2.113. **OdometerShort**

Valoarea indicată de odometrul vehiculului, în formă prescurtată.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Atribuirea valorii: binar fără semn. Valoare exprimată în kilometri și cuprinsă în intervalul operațional 0 – 9 999 999 km.

2.114. **OdometerValueMidnight**

Valoarea indicată de odometrul vehiculului la miezul nopții într-o zi dată (cerința 090 din anexa 1B și cerința 113 din anexa 1C).

```
OdometerValueMidnight ::= OdometerShort
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.115. **OdometerValueMidnightRecordArray**

Generația 2:

OdometerValueMidnight plus metadatele utilizate în protocolul de descărcare.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

RecordType reprezintă tipul înregistrării (*OdometerValueMidnight*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *OdometerValueMidnight* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul de înregistrări *OdometerValueMidnight*.

2.116. **OverspeedNumber**

Numărul evenimentelor de depășire a limitei de viteză de la ultimul control privind depășirea limitei de viteză.

```
OverspeedNumber ::= INTEGER(0..255)
```

Atribuirea valorii: 0 înseamnă că nu s-a produs niciun eveniment de depășire a limitei de viteză de la ultimul control privind depășirea limitei de viteză, 1 înseamnă că s-a produs un eveniment de depășire a limitei de viteză de la ultimul control privind depășirea limitei de viteză, iar …255 înseamnă că s-au produs 255 sau mai multe evenimente de depășire a limitei de viteză de la ultimul control privind depășirea limitei de viteză.

2.117. **PlaceRecord**

Informații privind un loc unde începe sau se încheie o zi de lucru (cerințele 108, 271, 296, 324 și 347 din anexa 1C).

Generația 1:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort
}
```

entryTime reprezintă data și ora aferente introducerii datelor.

entryTypeDailyWorkPeriod este tipul de introducere de date.

dailyWorkPeriodCountry este țara introdusă.

dailyWorkPeriodRegion este regiunea introdusă.

vehicleOdometerValue este valoarea indicată de odometru în momentul introducerii datelor privind locul.

Generația 2:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort,
   entryGNSSPlaceRecord               GNSSPlaceRecord
}
```

În plus față de generația 1, se utilizează următoarea componentă:

entryGNSSPlaceRecord reprezintă locul și ora înregistrate.

2.118. **PreviousVehicleInfo**

Informații privind vehiculul utilizat anterior de un conducător auto atunci când acesta își introduce cardul într-o unitate montată pe vehicul (cerința 081 din anexa 1B și cerința 102 din anexa 1C).

Generația 1:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification reprezintă VRN și statul membru de înmatriculare a vehiculului.

cardWithdrawalTime reprezintă data și ora la care a fost retras cardul.

Generația 2:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

În plus față de generația 1, se utilizează următorul element de date:

vuGeneration identifică generația unității montate pe vehicul.

2.119. **PublicKey**

Generația 1:

O cheie publică RSA.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                    RSAKeyModulus,
   rsaKeyPublicExponent             RSAKeyPublicExponent
}
```

rsaKeyModulus este modulul perechii de chei.

rsaKeyPublicExponent este exponentul public al perechii de chei.

2.120. **RecordType**

Generația 2:

Trimitere la un tip de înregistrare. Acest tip de date se utilizează în *RecordArrays*.

```
RecordType ::= OCTET STRING(SIZE(1))
```

Atribuirea valorii:

'01'H	ActivityChangeInfo,
'02'H	CardSlotsStatus,
'03'H	CurrentDateTime,
'04'H	MemberStateCertificate,
'05'H	OdometerValueMidnight,
'06'H	DateOfDayDownloaded,
'07'H	SensorPaired,
'08'H	Signature,
'09'H	SpecificConditionRecord,
'0A'H	VehicleIdentificationNumber,
'0B'H	VehicleRegistrationNumber,
'0C'H	VuCalibrationRecord,
'0D'H	VuCardIWRecord,
'0E'H	VuCardRecord,
'0F'H	VuCertificate,
'10'H	VuCompanyLocksRecord,
'11'H	VuControlActivityRecord,
'12'H	VuDetailedSpeedBlock,
'13'H	VuDownloadablePeriod,
'14'H	VuDownloadActivityData,
'15'H	VuEventRecord,
'16'H	VuGNSSCDRecord,
'17'H	VuITSConsentRecord,
'18'H	VuFaultRecord,
'19'H	VuIdentification,
'1A'H	VuOverSpeedingControlData,
'1B'H	VuOverSpeedingEventRecord,
'1C'H	VuPlaceDailyWorkPeriodRecord,
'1D'H	VuTimeAdjustmentGNSSRecord,
'1E'H	VuTimeAdjustmentRecord,
'1F'H	VuPowerSupplyInterruptionRecord,
'20'H	SensorPairedRecord,
'21'H	SensorExternalGNSSCoupledRecord,
'22'H to '7F'H	RFU,
'80'H to 'FF'H	Specific producătorului.

2.121. **RegionAlpha**

Trimitere alfabetică la o regiune dintr-o anumită țară.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Generația 1:

Atribuirea valorii:

```
‘   ’        No information available,
Spain:
‘AN ’        Andalucía,
‘AR ’        Aragón,
‘AST’        Asturias,
‘C  ’        Cantabria,
‘CAT’        Cataluña,
‘CL ’        Castilla-León,
‘CM ’        Castilla-La-Mancha,
‘CV’         Valencia,
‘EXT’        Extremadura,
‘G  ’        Galicia,
‘IB ’        Baleares,
‘IC ’        Canarias,
‘LR ’        La Rioja,
‘M  ’        Madrid,
‘MU ’        Murcia,
‘NA ’        Navarra,
‘PV ’        País Vasco
```

Generația 2:

Codurile *RegionAlpha* trebuie să figureze pe o listă menținută pe site-ul web al laboratorului desemnat să efectueze testele de interoperabilitate.

2.122. **RegionNumeric**

Trimitere numerică la o regiune dintr-o anumită țară.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Generația 1:

Atribuirea valorii:

```
‘00’H        No information available,
Spain:
‘01’H        Andalucía,
‘02’H        Aragón,
‘03’H        Asturias,
‘04’H        Cantabria,
‘05’H        Cataluña,
‘06’H        Castilla-León,
‘07’H        Castilla-La-Mancha,
‘08’H        Valencia,
‘09’H        Extremadura,
‘0A’H        Galicia,
‘0B’H        Baleares,
‘0C’H        Canarias,
‘0D’H        La Rioja,
‘0E’H        Madrid,
‘0F’H        Murcia,
‘10’H        Navarra,
‘11’H        País Vasco
```

Generația 2:

Codurile *RegionNumeric* trebuie să figureze pe o listă menținută pe site-ul web al laboratorului desemnat să efectueze testele de interoperabilitate.

2.123. **RemoteCommunicationModuleSerialNumber**

Generația 2:

Numărul de serie al modulului de comunicare la distanță.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Generația 1:

Modulul unei perechi de chei RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Atribuirea valorii: neprecizată.

2.125. **RSAKeyPrivateExponent**

Generația 1:

Exponentul privat al unei perechi de chei RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Atribuirea valorii: neprecizată.

2.126. **RSAKeyPublicExponent**

Generația 1:

Exponentul public al unei perechi de chei RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Atribuirea valorii: neprecizată.

2.127. **RtmData**

Generația 2:

Pentru definiția acestui tip de date, a se vedea apendicele 14.

2.128. **SealDataCard**

Generația 2:

Acest tip de date stochează informații despre sigiliile care sunt atașate la diferitele componente ale unui vehicul și sunt destinate a fi stocate pe un card. Acest tip de date se raportează la cerința 337 din anexa 1C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords este numărul de înregistrări din *sealRecords*.

sealRecords este un set de înregistrări privind sigiliile.

2.129. **SealDataVu**

Generația 2:

Acest tip de date stochează informații despre sigiliile care sunt atașate la diferitele componente ale unui vehicul și sunt destinate a fi stocate într-o unitate montată pe vehicul.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords este un set de înregistrări privind sigiliile. În cazul în care sunt disponibile mai puțin de 5 sigilii, valoarea *EquipmentType* în toate *sealRecords* neutilizate se setează la 16, și anume neutilizate.

2.130. **SealRecord**

Generația 2:

Acest tip de date stochează informații despre un sigiliu care este atașat la o componentă. Acest tip de date se raportează la cerința 337 din anexa 1C.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType identifică tipul de echipament la care este atașat sigiliul.

extendedSealIdentifier este identificatorul sigiliului atașat la echipament.

2.131. **SensorApprovalNumber**

Numărul de omologare de tip al senzorului.

Generația 1:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Atribuirea valorii: neprecizată.

Generația 2:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Atribuirea valorii:

Numărul de omologare trebuie să fie furnizat așa cum este publicat pe site-ul web corespunzător al Comisiei Europene, de exemplu inclusiv cu liniuțe dacă este cazul. Numărul de omologare trebuie să fie aliniat la stânga.

2.132. **SensorExternalGNSSApprovalNumber**

Generația 2:

Numărul de omologare de tip al echipamentului GNSS extern.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Atribuirea valorii:

Numărul de omologare trebuie să fie furnizat așa cum este publicat pe site-ul web corespunzător al Comisiei Europene, de exemplu inclusiv cu liniuțe dacă este cazul. Numărul de omologare trebuie să fie aliniat la stânga.

2.133. **SensorExternalGNSSCoupledRecord**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind identificarea echipamentului GNSS extern cuplat la unitatea montată pe vehicul (cerința 100 din anexa 1C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber este numărul de serie al echipamentului GNSS extern cuplat la unitatea montată pe vehicul.

sensorApprovalNumber este numărul de omologare al respectivului echipament GNSS extern.

sensorCouplingDate este data de cuplare a respectivului echipament GNSS extern la unitatea montată pe vehicul.

2.134. **SensorExternalGNSSIdentification**

Generația 2:

Informații privind identificarea echipamentului GNSS extern (cerința 98 din anexa 1C).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber este numărul de serie lung al echipamentului GNSS extern.

sensorApprovalNumber este numărul de omologare al echipamentului GNSS extern.

sensorSCIdentifier este identificatorul componentei de securitate a echipamentului GNSS extern.

sensorOSIdentifier este identificatorul sistemului de operare al echipamentului GNSS extern.

2.135. **SensorExternalGNSSInstallation**

Generația 2:

Informații, stocate într-un echipament GNSS extern, privind instalarea senzorului GNSS extern (cerința 123 din anexa 1C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst este data la care s-a efectuat prima cuplare a echipamentului GNSS extern la o unitate montată pe vehicul.

firstVuApprovalNumber este numărul de omologare al primei unități montate pe vehicul cuplate la echipamentul GNSS extern.

firstVuSerialNumber este numărul de serie al primei unități montate pe vehicul asociate cu echipamentul GNSS extern.

sensorCouplingDateCurrent este data la care s-a efectuat cuplarea actuală a echipamentului GNSS extern la o unitate montată pe vehicul.

currentVuApprovalNumber este numărul de omologare al unității montate pe vehicul cuplate în prezent la echipamentul GNSS extern.

currentVUSerialNumber este numărul de serie al unității montate pe vehicul cuplate în prezent la echipamentul GNSS extern.

2.136. **SensorExternalGNSSOSIdentifier**

Generația 2:

Identificator al sistemului de operare al echipamentului GNSS extern.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Atribuirea valorii: specifică producătorului.

2.137. **SensorExternalGNSSSCIdentifier**

Generația 2:

Acest tip de date este folosit, de exemplu, pentru identificarea modulului criptografic al echipamentului GNSS extern.

Identificator al componentei de securitate a echipamentului GNSS extern.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Atribuirea valorii: specifică producătorului componentei.

2.138. **SensorGNSSCouplingDate**

Generația 2:

Data cuplării echipamentului GNSS extern la o unitate montată pe vehicul.

```
SensorGNSSCouplingDate ::= TimeReal
```

Atribuirea valorii: neprecizată.

2.139. **SensorGNSSSerialNumber**

Generația 2:

Acest tip de date este utilizat pentru a stoca numărul de serie al receptorului GNSS atât când acesta se află în interiorul VU, cât și când acesta se află în exteriorul VU.

Numărul de serie al receptorului GNSS.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Informații, stocate într-un senzor de mișcare, privind identificarea senzorului de mișcare (cerința 077 din anexa 1B și cerința 95 din anexa 1C).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                SensorSerialNumber,
   sensorApprovalNumber              SensorApprovalNumber,
   sensorSCIdentifier                SensorSCIdentifier,
   sensorOSIdentifier                SensorOSIdentifier
}
```

sensorSerialNumber este numărul de serie lung al senzorului de mișcare (include numărul de componentă și codul producătorului).

sensorApprovalNumber este numărul de omologare al senzorului de mișcare.

sensorSCIdentifier este identificatorul componentei de securitate a senzorului de mișcare.

sensorOSIdentifier este identificatorul sistemului de operare al senzorului de mișcare.

2.141. **SensorInstallation**

Informații, stocate într-un senzor de mișcare, privind instalarea senzorului de mișcare (cerința 099 din anexa 1B și cerința 122 din anexa 1C).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst            SensorPairingDate,
   firstVuApprovalNumber             VuApprovalNumber,
   firstVuSerialNumber               VuSerialNumber,
   sensorPairingDateCurrent          SensorPairingDate,
   currentVuApprovalNumber           VuApprovalNumber,
   currentVUSerialNumber             VuSerialNumber
}
```

sensorPairingDateFirst este data la care s-a efectuat prima asociere a senzorului de mișcare cu o unitate montată pe vehicul.

firstVuApprovalNumber este numărul de omologare al primei unități montate pe vehicul asociate cu senzorul de mișcare.

firstVuSerialNumber este numărul de serie al primei unități montate pe vehicul asociate cu senzorul de mișcare.

sensorPairingDateCurrent este data la care s-a efectuat asocierea actuală a senzorului de mișcare cu unitatea montată pe vehicul.

currentVuApprovalNumber este numărul de omologare al unității montate pe vehicul asociate în prezent cu senzorul de mișcare.

currentVUSerialNumber este numărul de serie al unității montate pe vehicul asociate în prezent cu senzorul de mișcare.

2.142. **SensorInstallationSecData**

Informații, stocate pe un card de atelier, privind datele de securitate necesare pentru asocierea senzorilor de mișcare cu unitățile montate pe vehicule (cerințele 308 și 331 din anexa 1C).

Generația 1:

```
SensorInstallationSecData ::= TdesSessionKey
```

Atribuirea valorii: în conformitate cu standardul ISO 16844-3.

Generația 2:

Conform descrierii din apendicele 11, un card de atelier stochează până la trei chei pentru asocierea unui senzor de mișcare cu VU. Aceste chei au versiuni diferite.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

2.143. **SensorOSIdentifier**

Identificator al sistemului de operare al senzorului de mișcare.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Atribuirea valorii: specifică producătorului.

2.144. **SensorPaired**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind identificarea senzorului de mișcare asociat cu unitatea montată pe vehicul (cerința 079 din anexa 1B).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDateFirst                SensorPairingDate
}
```

sensorSerialNumber este numărul de serie al senzorului de mișcare asociat în prezent cu unitatea montată pe vehicul.

sensorApprovalNumber este numărul de omologare al senzorului de mișcare asociat în prezent cu unitatea montată pe vehicul.

sensorPairingDateFirst este data primei asocieri cu o unitate montată pe vehicul a senzorului de mișcare asociat în prezent cu unitatea montată pe vehicul.

2.145. **SensorPairedRecord**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind identificarea unui senzor de mișcare asociat cu unitatea montată pe vehicul (cerința 97 din anexa 1C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber este numărul de serie al unui senzor de mișcare asociat cu unitatea montată pe vehicul.

sensorApprovalNumber este numărul de omologare al senzorului de mișcare respectiv.

sensorPairingDate este data la care s-a efectuat asocierea senzorului de mișcare respectiv cu unitatea montată pe vehicul.

2.146. **SensorPairingDate**

Data asocierii unui senzor de mișcare cu o unitate montată pe vehicul.

```
SensorPairingDate ::= TimeReal
```

Atribuirea valorii: neprecizată.

2.147. **SensorSCIdentifier**

Identificatorul componentei de securitate a senzorului de mișcare.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Atribuirea valorii: specifică producătorului componentei.

2.148. **SensorSerialNumber**

Numărul de serie al senzorului de mișcare.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

O semnătură digitală.

Generația 1:

```
Signature ::= OCTET STRING (SIZE(128))
```

Atribuirea valorii: în conformitate cu apendicele 11, „Mecanisme de securitate comune”.

Generația 2:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Atribuirea valorii: în conformitate cu apendicele 11, „Mecanisme de securitate comune”.

2.150. **SignatureRecordArray**

Generația 2:

Un set de semnături plus metadatele utilizate în protocolul de descărcare.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType reprezintă tipul înregistrării (*Signature*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *Signature* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*. Valoarea se setează la 1 deoarece semnăturile pot avea diferite lungimi.

records este setul de semnături.

2.151. **SimilarEventsNumber**

Numărul de evenimente similare într-o zi dată (cerința 094 din anexa 1B și cerința 117 din anexa 1C).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Atribuirea valorii: 0 nu se utilizează, 1 înseamnă că s-a produs și s-a stocat în acea zi un singur eveniment de tipul respectiv, 2 înseamnă că s-au produs două evenimente de tipul respectiv în ziua dată (a fost stocat numai unul), …255 înseamnă că s-au produs 255 sau mai multe evenimente de tipul respectiv în ziua dată.

2.152. **SpecificConditionRecord**

Informații, stocate pe un card de conducător auto, pe un card de atelier sau într-o unitate montată pe vehicul, privind o condiție specifică (cerințele 130, 276, 301, 328 și 355 din anexa 1C).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                           TimeReal,
   specificConditionType               SpecificConditionType
}
```

entryTime reprezintă data și ora introducerii datelor.

specificConditionType este codul prin care se identifică condiția specifică.

2.153. **SpecificConditions**

Informații, stocate pe un card de conducător auto, pe un card de atelier sau într-o unitate montată pe vehicul, privind o condiție specifică (cerințele 131, 277, 302, 329 și 356 din anexa 1C).

Generația 2:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                       SpecificConditionRecord
}
```

conditionPointerNewestRecord este indicele ultimei înregistrări actualizate privind condiția specifică.

Atribuirea valorii: număr care corespunde numărătorului înregistrării privind condiția specifică, începând de la '0' pentru prima ocurență a înregistrării privind condiția specifică în structură.

specificConditionRecords este setul de înregistrări care conțin informații privind condițiile specifice înregistrate.

2.154. **SpecificConditionType**

Cod care identifică o condiție specifică (cerințele 050b, 105a, 212a și 230a din anexa 1B și cerința 62 din anexa 1C).

```
SpecificConditionType ::= INTEGER(0..255)
```

Generația 1:

Atribuirea valorii:

'00'H	RFU
'01'H	În afara zonei de aplicare a reglementărilor – Început
'02'H	În afara zonei de aplicare a reglementărilor – Sfârșit
'03'H	Traversare cu feribotul / trenul
'04'H .. 'FF'H	RFU

Generația 2:

Atribuirea valorii:

'00'H	RFU
'01'H	În afara zonei de aplicare a reglementărilor – Început
'02'H	În afara zonei de aplicare a reglementărilor – Sfârșit
'03'H	Traversare cu feribotul / trenul – Început
'04'H	Traversare cu feribotul / trenul – Sfârșit
'05'H .. 'FF'H	RFU

2.155. **Speed**

Viteza vehiculului (km/h).

```
Speed ::= INTEGER(0..255)
```

Atribuirea valorii: kilometri pe oră în intervalul operațional 0 – 220 km/h.

2.156. **SpeedAuthorised**

Viteza maximă autorizată a vehiculului (definiția hh)).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Viteza medie dintr-un interval definit în prealabil (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Viteza maximă măsurată într-un interval definit în prealabil.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Generația 2:

Pentru definiția acestui tip de date, a se vedea apendicele 14.

2.160. **TachographPayloadEncrypted**

Generația 2:

Datele utile ale tahografului criptate DER-TLV, și anume datele transmise criptat în mesajul RTM. Pentru criptare, a se vedea apendicele 11 partea B capitolul 13.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag face parte din codarea DER-TLV și se setează la '87' (a se vedea apendicele 11 partea B capitolul 13).

length face parte din codarea DER-TLV și codează lungimea următorului *paddingContentIndicatorByte* și a *encryptedData*.

paddingContentIndicatorByte se setează la '00'.

encryptedData este *tachographPayload* criptat, astfel cum este specificat în apendicele 11 partea B capitolul 13. Lungimea acestor date în octeți este întotdeauna un multiplu de 16.

2.161. **TDesSessionKey**

Generația 1:

O cheie de sesiune DES triplă.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.162. **TimeReal**

Cod pentru un câmp combinat de dată și oră, unde data și ora sunt exprimate în secunde care depășesc 00h.00m.00s. la 1 ianuarie 1970 GMT.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Atribuirea valorii – Octet aliniat: numărul de secunde începând de la miezul nopții la 1 ianuarie 1970 GMT.

Data/ora maximă posibilă este în anul 2106.

2.163. **TyreSize**

Desemnarea dimensiunilor pneurilor.

```
TyreSize ::= IA5String(SIZE(15))
```

Atribuirea valorii: în conformitate cu Directiva 92/23 (CEE) 31.3.92 JO L 129 p. 95.

2.164. **VehicleIdentificationNumber**

Numărul de identificare a vehiculului (VIN) care desemnează vehiculul în ansamblu, fiind reprezentat în mod normal de numărul de serie al șasiului sau de numărul cadrului.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Atribuirea valorii: conform definiției din standardul ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Generația 2:

Numărul de identificare a vehiculului, plus metadatele utilizate în protocolul de descărcare.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType reprezintă tipul înregistrării (*VehicleIdentificationNumber*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VehicleIdentificationNumber* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul numerelor de identificare a vehiculului.

2.166. **VehicleRegistrationIdentification**

Identificarea unui vehicul, unică în Europa (VRN și statul membru).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation reprezintă statul în care este înmatriculat vehiculul.

vehicleRegistrationNumber este numărul de înmatriculare a vehiculului (VRN).

2.167. **VehicleRegistrationNumber**

Numărul de înmatriculare a vehiculului (VRN). Numărul de înmatriculare este atribuit de autoritatea responsabilă cu înmatricularea vehiculelor.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   vehicleRegNumber                    OCTET STRING (SIZE(13))
}
```

codePage indică un set de caractere definit în capitolul 4,

vehicleRegNumber este un VRN codat cu ajutorul setului de caractere precizat.

Atribuirea valorii: specifică fiecărei țări.

2.168. **VehicleRegistrationNumberRecordArray**

Generația 2:

Numărul de înmatriculare al vehiculului, plus metadatele utilizate în protocolul de descărcare.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleRegistrationNumber
}
```

recordType reprezintă tipul înregistrării (*VehicleRegistrationNumber*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VehicleRegistrationNumber* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul numerelor de înmatriculare a vehiculului.

2.169. **VuAbility**

Generația 2:

Informații stocate într-o VU privind capacitatea VU de a utiliza sau nu carduri de tahograf de generația 1 (cerința 121 din anexa 1C).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Atribuirea valorii – Octet aliniat: 'xxxxxxxa'B (8 biți)

Pentru compatibilitatea cu generația 1:

'a'B	Compatibilitate cu carduri de tahograf de generația 1:
	'0' B Compatibil cu generația 1,
	'1' B Incompatibil cu generația 1,
'xxxxxxx'B	RFU

2.170. **VuActivityDailyData**

Generația 1:

Informații, stocate într-o VU, privind modificările activității și/sau modificările regimului de conducere și/sau modificările stării cardului într-o anumită zi calendaristică (cerința 084 din anexa 1B și cerințele 105, 106, 107 din anexa 1C) și privind starea sloturilor la 00.00 în acea zi.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                INTEGER SIZE(0..1440),
   activityChangeInfos                SET SIZE(noOfActivityChanges) OF
                                      ActivityChangeInfo
}
```

noOfActivityChanges este numărul de cuvinte *ActivityChangeInfo* din setul *activityChangeInfos*.

activityChangeInfos este setul de cuvinte *ActivityChangeInfo* stocate în VU pentru ziua respectivă. Acest set cuprinde întotdeauna două cuvinte *ActivityChangeInfo* care indică starea celor două sloturi la ora 00.00 în ziua respectivă.

2.171. **VuActivityDailyRecordArray**

Generația 2:

Informații, stocate într-o VU, privind modificările activității și/sau modificările regimului de conducere și/sau modificările stării cardului într-o anumită zi calendaristică (cerințele 105, 106, 107 din anexa 1C) și privind starea sloturilor la 00.00 în acea zi.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType reprezintă tipul înregistrării (*ActivityChangeInfo*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *ActivityChangeInfo* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul de cuvinte *ActivityChangeInfo* stocate în VU pentru ziua respectivă. Acest set cuprinde întotdeauna două cuvinte *ActivityChangeInfo* care indică starea celor două sloturi la ora 00.00 în ziua respectivă.

2.172. **VuApprovalNumber**

Numărul de omologare de tip al unității montate pe vehicul.

Generația 1:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Atribuirea valorii: neprecizată.

Generația 2:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

Atribuirea valorii:

Numărul de omologare trebuie să fie furnizat așa cum este publicat pe site-ul web corespunzător al Comisiei Europene, de exemplu inclusiv cu liniuțe dacă este cazul. Numărul de omologare trebuie să fie aliniat la stânga.

2.173. **VuCalibrationData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind operațiunile de etalonare a aparaturii de înregistrare (cerința 098 din anexa 1B).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords             INTEGER(0..255),
   vuCalibrationRecords                 SET SIZE(noOfVuCalibrationRecords) OF
                                        VuCalibrationRecord
}
```

noOfVuCalibrationRecords este numărul de înregistrări cuprinse în setul *vuCalibrationRecords*.

vuCalibrationRecords este setul de înregistrări privind etalonarea.

2.174. **VuCalibrationRecord**

Informații, stocate într-o unitate montată pe vehicul, privind o operațiune de etalonare a aparaturii de înregistrare (cerința 098 din anexa 1B și cerințele 119 și 120 din anexa 1C).

Generația 1:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                   CalibrationPurpose,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber,
   workshopCardExpiryDate               TimeReal,
   vehicleIdentificationNumber          VehicleIdentificationNumber,
   vehicleRegistrationIdentification    VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant       W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment        K-ConstantOfRecordingEquipment,
   lTyreCircumference                   L-TyreCircumference,
   tyreSize                             TyreSize,
   authorisedSpeed                      SpeedAuthorised,
   oldOdometerValue                     OdometerShort,
   newOdometerValue                     OdometerShort,
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   nextCalibrationDate                  TimeReal
}
```

calibrationPurpose este scopul etalonării.

workshopName, workshopAddress reprezintă denumirea și adresa atelierului.

workshopCardNumber identifică cardul de atelier utilizat în timpul operațiunii de etalonare.

workshopCardExpiryDate este data de expirare a cardului.

vehicleIdentificationNumber este VIN.

vehicleRegistrationIdentification conține VRN și statul membru de înmatriculare.

wVehicleCharacteristicConstant este coeficientul caracteristic al vehiculului.

kConstantOfRecordingEquipment este constanta aparaturii de înregistrare.

lTyreCircumference este circumferința efectivă a pneurilor roților.

tyreSize reprezintă desemnarea dimensiunii pneurilor montate pe vehicul.

authorisedSpeed este viteza autorizată a vehiculului.

oldOdometerValue, newOdometerValue reprezintă vechea și, respectiv, noua valoare indicate de odometru.

oldTimeValue, newTimeValue sunt valorile vechi și, respectiv, noi ale datei și orei.

nextCalibrationDate este data următoarei etalonări de tipul specificat în *CalibrationPurpose* care va fi efectuată de autoritatea de inspecție competentă.

Generația 2:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

În plus față de generația 1, se utilizează următorul element de date:

sealDataVu oferă informații cu privire la sigiliile care sunt atașate la diferite componente ale vehiculului.

2.175. **VuCalibrationRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind operațiunile de etalonare a aparaturii de înregistrare (cerințele 119 și 120 din anexa 1C).

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCalibrationRecord
}
```

recordType reprezintă tipul înregistrării (*VuCalibrationRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuCalibrationRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul de înregistrări privind etalonarea.

2.176. **VuCardIWData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind ciclurile de introducere și de retragere a cardurilor de conducător auto sau a cardurilor de atelier din unitatea montată pe vehicul (cerința 081 din anexa 1B și cerința 103 din anexa 1C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords este numărul de înregistrări cuprinse în setul *vuCardIWRecords*.

vuCardIWRecords este un set de înregistrări privind ciclurile de introducere și de retragere a cardurilor.

2.177. **VuCardIWRecord**

Informații, stocate într-o unitate montată pe vehicul, privind un ciclu de introducere și de retragere a unui card de conducător auto sau a unui card de atelier din unitatea montată pe vehicul (cerința 081 din anexa 1B și cerința 102 din anexa 1C).

Generația 1:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

cardHolderName reprezintă numele și prenumele titularului unui card de conducător auto sau al unui card de atelier, așa cum sunt acestea stocate pe card.

fullCardNumber reprezintă tipul cardului, statul membru emitent al cardului și numărul cardului, așa cum sunt stocate pe card.

cardExpiryDate este data de expirare a cardului, așa cum este stocată pe card.

cardInsertionTime reprezintă data și ora introducerii cardului.

vehicleOdometerValueAtInsertion este valoarea indicată de odometrul vehiculului în momentul introducerii cardului.

cardSlotNumber este slotul în care se introduce cardul.

cardWithdrawalTime reprezintă data și ora retragerii cardului.

vehicleOdometerValueAtWithdrawal este valoarea indicată de odometrul vehiculului în momentul retragerii cardului.

previousVehicleInfo conține informații privind vehiculul folosit anterior de conducătorul auto, așa cum este acesta stocat pe card.

manualInputFlag este un indicator prin care se indică dacă titularul cardului a introdus manual activitățile conducătorului auto la introducerea cardului.

Generația 2:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

În loc de *fullCardNumber*, în structura de date aferentă generației 2 se utilizează următorul element de date.

fullCardNumberAndGeneration reprezintă tipul cardului, statul membru emitent al cardului, numărul cardului și generația sa, așa cum sunt stocate pe card.

2.178. **VuCardIWRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind ciclurile de introducere și de retragere a cardurilor de conducător auto sau a cardurilor de atelier din unitatea montată pe vehicul (cerința 103 din anexa 1C).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType reprezintă tipul înregistrării (*VuCardIWRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuCardIWRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind ciclurile de introducere și de retragere a cardurilor.

2.179. **VuCardRecord**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind un card de tahograf utilizat (cerința 132 din anexa 1C).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber așa cum este citit din fișierul EF_ICC din MF al cardului.

cardPersonaliserID așa cum este citit din fișierul EF_ICC din MF al cardului.

typeOfTachographCardId așa cum este citit din fișierul EF_Application_Identification din cadrul DF_Tachograph_G2

cardStructureVersion așa cum este citit din fișierul EF_Application_Identification din cadrul DF_Tachograph_G2.

cardNumber așa cum este citit din fișierul EF_Identification din cadrul DF_Tachograph_G2.

2.180. **VuCardRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind cardurile de tahograf utilizate cu respectiva VU. Aceste informații sunt destinate analizei VU – probleme card (cerința 132 din anexa 1C).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType reprezintă tipul înregistrării (*VuCardRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuCardRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind cardurile de tahograf utilizate cu VU.

2.181. **VuCertificate**

Certificatul cheii publice a unei unități montate pe vehicul.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Generația 2:

Certificatul VU, plus metadatele utilizate în protocolul de descărcare.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType reprezintă tipul înregistrării (*VuCertificate*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuCertificate* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*. Valoarea se setează la 1 deoarece certificatele pot avea diferite lungimi.

records este un set de certificate ale VU.

2.183. **VuCompanyLocksData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind blocările efectuate de societate (cerința 104 din anexa 1B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                          INTEGER(0..255),
   vuCompanyLocksRecords              SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks este numărul de blocări enumerate în *vuCompanyLocksRecords*.

vuCompanyLocksRecords este setul de înregistrări privind blocările efectuate de societate.

2.184. **VuCompanyLocksRecord**

Informații, stocate într-o unitate montată pe vehicul, privind o blocare efectuată de societate (cerința 104 din anexa 1B și cerința 128 din anexa 1C).

Generația 1:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumber                  FullCardNumber
}
```

lockInTime, lockOutTime reprezintă data și ora blocării și, respectiv, a deblocării.

companyName, companyAddress reprezintă denumirea și adresa societății asociate cu blocarea.

companyCardNumber reprezintă cardul utilizat la blocare.

Generația 2:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumberAndGeneration     FullCardNumberAndGeneration
}
```

În loc de *companyCardNumber*, în structura de date aferentă generației 2 se utilizează următorul element de date.

companyCardNumberAndGeneration reprezintă cardul utilizat la blocare, inclusiv generația acestuia.

2.185. **VuCompanyLocksRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind blocările efectuate de societate (cerința 128 din anexa 1C).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType reprezintă tipul înregistrării (*VuCompanyLocksRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuCompanyLocksRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*. Valoare 0..255.

records este setul de înregistrări privind blocările efectuate de societate.

2.186. **VuControlActivityData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind controalele efectuate utilizând VU respectivă (cerința 102 din anexa 1B).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls este numărul de controale enumerate în *vuControlActivityRecords*.

vuControlActivityRecords este setul de înregistrări privind activitățile de control.

2.187. **VuControlActivityRecord**

Informații, stocate într-o unitate montată pe vehicul, privind un control efectuat utilizând respectiva VU (cerința 102 din anexa 1B și cerința 126 din anexa 1C).

Generația 1:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType este tipul de control.

controlTime este data și ora la care a avut loc controlul.

controlCardNumber reprezintă cardul de control utilizat la efectuarea controlului.

downloadPeriodBeginTime este ora de începere a perioadei descărcate, în caz de descărcare.

downloadPeriodEndTime este ora de încheiere a perioadei descărcate, în caz de descărcare.

Generația 2:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

În loc de *controlCardNumber*, în structura de date aferentă generației 2 se utilizează următorul element de date.

controlCardNumberAndGeneration reprezintă cardul de control utilizat la efectuarea controlului, inclusiv generația acestuia.

2.188. **VuControlActivityRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind controalele efectuate utilizând VU respectivă (cerința 126 din anexa 1C).

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuControlActivityRecord
}
```

recordType reprezintă tipul înregistrării (*VuControlActivityRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuControlActivityRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul de înregistrări privind activitățile de control al VU.

2.189. **VuDataBlockCounter**

Contor, stocat pe un card, care indică secvențial ciclurile de introducere și de retragere a cardului din unitățile montate pe vehicul.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Atribuirea valorii: număr consecutiv cu valoarea maximă de 9 999, după care numerotarea reîncepe de la 0.

2.190. **VuDetailedSpeedBlock**

Informații, stocate într-o unitate montată pe vehicul, privind viteza detaliată a vehiculului timp de un minut în care vehiculul s-a aflat în mișcare (cerința 093 din anexa 1B și cerința 116 din anexa 1C).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate reprezintă data și ora primei valori a vitezei din bloc.

speedsPerSecond este secvența cronologică de viteze măsurate în fiecare secundă din minutul care a început cu *speedBlockBeginDate* (inclusiv).

2.191. **VuDetailedSpeedBlockRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind viteza detaliată a vehiculului.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDetailedSpeedBlock
}
```

recordType reprezintă tipul înregistrării (*VuDetailedSpeedBlock*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuDetailedSpeedBlock* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul de blocuri de date privind viteza detaliată.

2.192. **VuDetailedSpeedData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind viteza detaliată a vehiculului.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                     INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks               SET SIZE(noOfSpeedBlocks) OF
                                       VuDetailedSpeedBlock
}
```

noOfSpeedBlocks este numărul de blocuri de date privind viteza din setul *vuDetailedSpeedBlocks*.

vuDetailedSpeedBlocks este setul de blocuri de date privind viteza detaliată.

2.193. **VuDownloadablePeriod**

Cele mai vechi și cele mai recente date pentru care o unitate montată pe vehicul conține informații privind activitățile conducătorului auto (cerințele 081, 084 sau 087 din anexa 1B și cerințele 102,105, 108 din anexa 1C).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                 TimeReal
   maxDownloadableTime                 TimeReal
}
```

minDownloadableTime reprezintă cea mai veche dată și oră stocată în VU la care s-a realizat o introducere a cardului, o modificare a activității sau o introducere de date privind locul.

maxDownloadableTime reprezintă cea mai recentă dată și oră stocată în VU la care s-a realizat o retragere a cardului, o modificare a activității sau o introducere de date privind locul.

2.194. **VuDownloadablePeriodRecordArray**

Generația 2:

VUDownloadablePeriod, plus metadatele utilizate în protocolul de descărcare.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDownloadablePeriod
}
```

recordType reprezintă tipul înregistrării (*VuDownloadablePeriod*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuDownloadablePeriod* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul de înregistrări *VuDownloadablePeriod*.

2.195. **VuDownloadActivityData**

Informații, stocate într-o unitate montată pe vehicul, privind ultima descărcare de date din aceasta (cerința 105 din anexa 1B și cerința 129 din anexa 1C).

Generația 1:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumber                      FullCardNumber,
   companyOrWorkshopName               Name
}
```

downloadingTime reprezintă data și ora la care s-a realizat descărcarea.

fullCardNumber reprezintă cardul utilizat pentru autorizarea descărcării.

companyOrWorkshopName reprezintă denumirea societății sau a atelierului.

Generația 2:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   companyOrWorkshopName               Name
}
```

În loc de *fullCardNumber*, în structura de date aferentă generației 2 se utilizează următorul element de date.

fullCardNumberAndGeneration reprezintă cardul utilizat pentru autorizarea descărcării, inclusiv generația acestuia.

2.196. **VuDownloadActivityDataRecordArray**

Generația 2:

Informații privind ultima descărcare din VU (cerința 129 din anexa 1C).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType reprezintă tipul înregistrării (*VuDownloadActivityData*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuDownloadActivityData* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul de înregistrări de date privind activitățile de descărcare.

2.197. **VuEventData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele (cerința 094 din anexa 1B, cu excepția evenimentului de depășire a limitei de viteză).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents este numărul de evenimente enumerate în setul *vuEventRecords*.

vuEventRecords este un set de înregistrări privind evenimentele.

2.198. **VuEventRecord**

Informații, stocate într-o unitate montată pe vehicul, privind un eveniment (cerința 094 din anexa 1B și cerința 117 din anexa 1C, cu excepția evenimentului de depășire a limitei de viteză).

Generația 1:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType este tipul de eveniment.

eventRecordPurpose este motivul pentru care s-a efectuat înregistrarea evenimentului respectiv.

eventBeginTime este data și ora la care a început evenimentul.

eventEndTime este data și ora la care s-a încheiat evenimentul.

cardNumberDriverSlotBegin identifică cardul introdus în slotul pentru cardul de conducător auto la începutul evenimentului.

cardNumberCodriverSlotBegin identifică cardul introdus în slotul pentru cardul de copilot la începutul evenimentului.

cardNumberDriverSlotEnd identifică cardul introdus în slotul pentru cardul de conducător auto la sfârșitul evenimentului.

cardNumberCodriverSlotEnd identifică cardul introdus în slotul pentru cardul de copilot la sfârșitul evenimentului.

similarEventsNumber este numărul de evenimente similare din ziua respectivă.

Această secvență poate fi utilizată pentru toate evenimentele, cu excepția evenimentelor de depășire a limitei de viteză.

Generația 2:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

În plus față de generația 1, se utilizează următoarele elemente de date:

manufacturerSpecificEventFaultData conține informații suplimentare cu privire la eveniment, specifice producătorului.

În loc de *cardNumberDriverSlotBegin*, *cardNumberCodriverSlotBegin*, *cardNumberDriverSlotEnd* și *cardNumberCodriverSlotEnd*, în structura de date aferentă generației 2 se utilizează următoarele elemente de date:

cardNumberAndGenDriverSlotBegin identifică cardul introdus în slotul pentru cardul de conducător auto la începutul evenimentului, inclusiv generația cardului respectiv.

cardNumberAndGenCodriverSlotBegin identifică cardul introdus în slotul pentru cardul de copilot la începutul evenimentului, inclusiv generația cardului respectiv.

cardNumberAndGenDriverSlotEnd identifică cardul introdus în slotul pentru cardul de conducător auto la sfârșitul evenimentului, inclusiv generația cardului respectiv.

cardNumberAndGenCodriverSlotEnd identifică cardul introdus în slotul pentru cardul de copilot la sfârșitul evenimentului, inclusiv generația cardului respectiv.

În cazul în care evenimentul este un conflict oră, *eventBeginTime* și *eventEndTime* se interpretează după cum urmează:

eventBeginTime este data și ora indicată de aparatura de înregistrare.

eventEndTime reprezintă data și ora GNSS.

2.199. **VuEventRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele (cerința 117 din anexa 1C, cu excepția evenimentului privind depășirea limitei de viteză).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType reprezintă tipul înregistrării (*VuEventRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuEventRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind evenimentele.

2.200. **VuFaultData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind anomaliile (cerința 096 din anexa 1B).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults este numărul anomaliilor enumerate în setul *vuFaultRecords*.

vuFaultRecords este un set de înregistrări privind anomaliile.

2.201. **VuFaultRecord**

Informații, stocate într-o unitate montată pe vehicul, privind o anomalie (cerința 096 din anexa 1B și cerința 118 din anexa 1C).

Generația 1:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType este tipul de anomalie a aparaturii de înregistrare.

faultRecordPurpose este motivul pentru care s-a efectuat înregistrarea anomaliei respective.

faultBeginTime este data și ora la care a început anomalia.

faultEndTime este data și ora la care s-a încheiat anomalia.

cardNumberDriverSlotBegin identifică cardul introdus în slotul pentru cardul de conducător auto la începutul anomaliei.

cardNumberCodriverSlotBegin identifică cardul introdus în slotul pentru cardul de copilot la începutul anomaliei.

cardNumberDriverSlotEnd identifică cardul introdus în slotul pentru cardul de conducător auto la sfârșitul anomaliei.

cardNumberCodriverSlotEnd identifică cardul introdus în slotul pentru cardul de copilot la sfârșitul anomaliei.

Generația 2:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

În plus față de generația 1, se utilizează următorul element de date:

manufacturerSpecificEventFaultData conține informații suplimentare specifice producătorului cu privire la anomalie.

În loc de *cardNumberDriverSlotBegin*, *cardNumberCodriverSlotBegin*, *cardNumberDriverSlotEnd* și *cardNumberCodriverSlotEnd*, în structura de date aferentă generației 2 se utilizează următoarele elemente de date:

cardNumberAndGenDriverSlotBegin identifică cardul introdus în slotul pentru cardul de conducător auto la începutul anomaliei, inclusiv generația cardului respectiv.

cardNumberAndGenCodriverSlotBegin identifică cardul introdus în slotul pentru cardul de copilot la începutul anomaliei, inclusiv generația cardului respectiv.

cardNumberAndGenDriverSlotEnd identifică cardul introdus în slotul pentru cardul de conducător auto la sfârșitul anomaliei, inclusiv generația cardului respectiv.

cardNumberAndGenCodriverSlotEnd identifică cardul introdus în slotul pentru cardul de copilot la sfârșitul anomaliei, inclusiv generația cardului respectiv.

2.202. **VuFaultRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind anomaliile (cerința 118 din anexa 1C).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType reprezintă tipul înregistrării (*VuFaultRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuFaultRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind anomaliile.

2.203. **VuGNSSCDRecord**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind poziția GNSS a vehiculului dacă timpul de conducere continuă al conducătorului auto ajunge la un multiplu de trei ore (cerințele 108, 110 din anexa 1C).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp este data și ora la care timpul de conducere continuă al titularului cardului ajunge la un multiplu de trei ore.

cardNumberAndGenDriverSlot identifică cardul introdus în slotul pentru cardul de conducător auto, inclusiv generația cardului respectiv.

cardNumberAndGenCodriverSlot identifică cardul introdus în slotul pentru cardul de copilot, inclusiv generația cardului respectiv.

gnssPlaceRecord conține informații referitoare la poziția vehiculului.

2.204. **VuGNSSCDRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind poziția GNSS a vehiculului dacă timpul de conducere continuă al conducătorului auto ajunge la un multiplu de trei ore (cerințele 108 și 110 din anexa 1C).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType reprezintă tipul înregistrării (*VuGNSSCDRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuGNSSCDRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări GNSS privind timpul de conducere continuă.

2.205. **VuIdentification**

Informații, stocate într-o unitate montată pe vehicul, privind identificarea unității montate pe vehicul (cerința 075 din anexa 1B și cerințele 93 și 121 din anexa 1C).

Generația 1:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                     VuManufacturerName,
   vuManufacturerAddress                  VuManufacturerAddress,
   vuPartNumber                           VuPartNumber,
   vuSerialNumber                         VuSerialNumber,
   vuSoftwareIdentification               VuSoftwareIdentification,
   vuManufacturingDate                    VuManufacturingDate,
   vuApprovalNumber                       VuApprovalNumber
}
```

vuManufacturerName este numele producătorului unității montate pe vehicul.

vuManufacturerAddress este adresa producătorului unității montate pe vehicul.

vuPartNumber este numărul de componentă al unității montate pe vehicul.

vuSerialNumber este numărul de serie al unității montate pe vehicul.

vuSoftwareIdentification identifică software-ul implementat în unitatea montată pe vehicul.

vuManufacturingDate este data de fabricație a unității montate pe vehicul.

vuApprovalNumber este numărul de omologare de tip al unității montate pe vehicul.

Generația 2:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber,
   vuGeneration                        Generation,
   vuAbility                           VuAbility
}
```

În plus față de generația 1, se utilizează următorul element de date:

vuGeneration identifică generația unității montate pe vehicul.

vuAbility oferă informații cu privire la faptul dacă VU este compatibilă sau nu cu carduri de tahograf de generația 1.

2.206. **VuIdentificationRecordArray**

Generația 2:

VuIdentification, plus metadatele utilizate în protocolul de descărcare.

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType reprezintă tipul înregistrării (*VuIdentification*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuIdentification* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări *VuIdentification*.

2.207. **VuITSConsentRecord**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind aprobarea unui conducător auto de a utiliza sisteme de transport inteligente.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identifică cardul, inclusiv generația sa. Acesta trebuie să fie un card de conducător auto sau un card de atelier.

consent este un indicator care indică dacă conducătorul auto și-a dat consimțământul privind utilizarea sistemelor de transport inteligente cu acest vehicul/cu această unitate montată pe vehicul.

Atribuirea valorii:

TRUE indică consimțământul conducătorului auto de a utiliza sisteme de transport inteligente

FALSE indică refuzul conducătorului auto de a utiliza sisteme de transport inteligente

2.208. **VuITSConsentRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind consimțământul conducătorilor auto de a utiliza sisteme de transport inteligente (cerința 200 din anexa 1C).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType reprezintă tipul înregistrării (*VuITSConsentRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuITSConsentRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este setul de înregistrări privind consimțământul ITS.

2.209. **VuManufacturerAddress**

Adresa producătorului unității montate pe vehicul.

```
VuManufacturerAddress ::= Address
```

Atribuirea valorii: neprecizată.

2.210. **VuManufacturerName**

Numele producătorului unității montate pe vehicul.

```
VuManufacturerName ::= Name
```

Atribuirea valorii: neprecizată.

2.211. **VuManufacturingDate**

Data de fabricație a unității montate pe vehicul.

```
VuManufacturingDate ::= TimeReal
```

Atribuirea valorii: neprecizată.

2.212. **VuOverSpeedingControlData**

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele de depășire a limitei de viteză care s-au produs de la ultimul control privind depășirea limitei de viteză (cerința 095 din anexa 1B și cerința 117 din anexa 1C).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime            TimeReal,
   firstOverspeedSince                 TimeReal,
   numberOfOverspeedSince              OverspeedNumber
}
```

lastOverspeedControlTime reprezintă data și ora la care s-a efectuat ultimul control privind depășirea limitei de viteză.

firstOverspeedSince reprezintă data și ora primei depășiri a limitei de viteză după efectuarea respectivului control al depășirilor limitei de viteză.

numberOfOverspeedSince este numărul de evenimente de depășire a limitei de viteză de la ultimul control al depășirilor limitei de viteză.

2.213. **VuOverSpeedingControlDataRecordArray**

Generația 2:

VuOverSpeedingControlData, plus metadatele utilizate în protocolul de descărcare.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuOverSpeedingControlData
}
```

recordType reprezintă tipul înregistrării (*VuOverSpeedingControlData*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuOverSpeedingControlData* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări de date referitoare la controalele privind depășirea limitei de viteză.

2.214. **VuOverSpeedingEventData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele de depășire a limitei de viteză (cerința 094 din anexa 1B).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents            INTEGER(0..255),
   vuOverSpeedingEventRecords          SET SIZE(noOfVuOverSpeedingEvents) OF
                                       VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents este numărul de evenimente enumerate în setul *vuOverSpeedingEventRecords*.

vuOverSpeedingEventRecords este un set de înregistrări privind evenimentele de depășire a limitei de viteză.

2.215. **VuOverSpeedingEventRecord**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele de depășire a limitei de viteză (cerința 094 din anexa 1B și cerința 117 din anexa 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberDriverSlotBegin          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType este tipul de eveniment.

eventRecordPurpose este motivul pentru care s-a efectuat înregistrarea evenimentului respectiv.

eventBeginTime este data și ora la care a început evenimentul.

eventEndTime este data și ora la care s-a încheiat evenimentul.

maxSpeedValue este viteza maximă măsurată în timpul evenimentului.

averageSpeedValue este media aritmetică a vitezei măsurate în timpul evenimentului.

cardNumberDriverSlotBegin identifică cardul introdus în slotul pentru cardul de conducător auto la începutul evenimentului.

similarEventsNumber este numărul de evenimente similare din ziua respectivă.

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele de depășire a limitei de viteză (cerința 094 din anexa 1B și cerința 117 din anexa 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

În loc de *cardNumberDriverSlotBegin*, în structura de date aferentă generației 2 se utilizează următorul element de date:

cardNumberAndGenDriverSlotBegin identifică cardul, introdus în slotul pentru cardul de conducător auto la începutul evenimentului, inclusiv generația cardului respectiv.

2.216. **VuOverSpeedingEventRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele de depășire a limitei de viteză (cerința 117 din anexa 1C).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuOverSpeedingEventRecord
}
```

recordType reprezintă tipul înregistrării (*VuOverSpeedingEventRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuOverSpeedingEventRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind evenimentele de depășire a limitei de viteză.

2.217. **VuPartNumber**

Numărul de componentă al unității montate pe vehicul.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Atribuirea valorii: specifică producătorului VU.

2.218. **VuPlaceDailyWorkPeriodData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind locurile în care conducătorii auto încep sau încheie o zi de lucru (cerința 087 din anexa 1B sau cerințele 108 și 110 din anexa 1C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords este numărul de înregistrări enumerate în setul *vuPlaceDailyWorkPeriodRecords*.

vuPlaceDailyWorkPeriodRecords este un set de înregistrări privind locurile.

2.219. **VuPlaceDailyWorkPeriodRecord**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind un loc în care un conducător auto începe sau încheie o zi de lucru (cerința 087 din anexa 1B sau cerințele 108 și 110 din anexa 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber reprezintă tipul de card al conducătorului auto, statul membru emitent al cardului și numărul cardului.

placeRecord conține informațiile privind locul introdus.

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind un loc în care un conducător auto începe sau încheie o zi de lucru (cerința 087 din anexa 1B sau cerințele 108 și 110 din anexa 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

În loc de *fullCardNumber*, în structura de date aferentă generației 2 se utilizează următorul element de date:

fullCardNumberAndGeneration reprezintă tipul cardului, statul membru emitent al cardului, numărul cardului și generația sa, așa cum sunt stocate pe card.

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind locurile în care conducătorii auto încep sau încheie o zi de lucru (cerințele 108 și 110 din anexa 1C).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType reprezintă tipul înregistrării (*VuPlaceDailyWorkPeriodRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuPlaceDailyWorkPeriodRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind locurile.

2.221. **VuPrivateKey**

Generația 1:

Cheia privată a unei unități montate pe vehicul.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Generația 1:

Cheia publică a unei unități montate pe vehicul.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Numărul de serie al unității montate pe vehicul (cerința 075 din anexa 1B și cerința 93 din anexa 1C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Data instalării versiunii de software a unității montate pe vehicul.

```
VuSoftInstallationDate ::= TimeReal
```

Atribuirea valorii: neprecizată.

2.225. **VuSoftwareIdentification**

Informații, stocate într-o unitate montată pe vehicul, privind software-ul instalat.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion este numărul versiunii software-ului instalat pe unitatea montată pe vehicul.

vuSoftInstallationDate este data instalării versiunii de software.

2.226. **VuSoftwareVersion**

Numărul versiunii de software al unității montate pe vehicul.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Atribuirea valorii: neprecizată.

2.227. **VuSpecificConditionData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind condițiile specifice.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords este numărul de înregistrări enumerate în setul *specificConditionRecords*.

specificConditionRecords este un set de înregistrări privind condițiile specifice.

2.228. **VuSpecificConditionRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind condițiile specifice (cerința 130 din anexa 1C).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType reprezintă tipul înregistrării (*SpecificConditionRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *SpecificConditionRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind condițiile specifice.

2.229. **VuTimeAdjustmentData**

Generația 1:

Informații, stocate într-o unitate montată pe vehicul, privind operațiunile de reglare a orei efectuate în afara cadrului unei etalonări normale (cerința 101 din anexa 1B).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                INTEGER(0..6),
   vuTimeAdjustmentRecords             SET SIZE(noOfVuTimeAdjRecords) OF
                                       VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords este numărul de înregistrări din *vuTimeAdjustmentRecords*.

vuTimeAdjustmentRecords este un set de înregistrări privind operațiunile de reglare a orei.

2.230. **VuTimeAdjustmentGNSSRecord**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind o operațiune de reglare a orei bazată pe datele privind ora de la GNSS (cerințele 124 și 125 din anexa 1C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal
}
```

oldTimeValue, newTimeValue sunt valorile vechi și, respectiv, noi ale datei și orei.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind o operațiune de reglare a orei bazată pe datele privind ora de la GNSS (cerințele 124 și 125 din anexa 1C).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuTimeAdjustmentGNSSRecord
}
```

recordType reprezintă tipul înregistrării (*VuTimeAdjustmentGNSSRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuTimeAdjustmentGNSSRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind operațiunile de reglare a orei după GNSS.

2.232. **VuTimeAdjustmentRecord**

Informații, stocate într-o unitate montată pe vehicul, privind o operațiune de reglare a orei efectuată în afara cadrului unei etalonări normale (cerința 101 din anexa 1B și cerințele 124 și 125 din anexa 1C).

Generația 1:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue sunt valorile vechi și, respectiv, noi ale datei și orei.

workshopName, workshopAddress reprezintă denumirea și adresa atelierului.

workshopCardNumber reprezintă cardul de atelier utilizat pentru a efectua operațiunea de reglare a orei.

Generația 2:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

În loc de *workshopCardNumber*, în structura de date aferentă generației 2 se utilizează următorul element de date.

workshopCardNumberAndGeneration reprezintă cardul de atelier utilizat pentru a efectua operațiunea de reglare a orei, inclusiv generația acestuia.

2.233. **VuTimeAdjustmentRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind operațiunile de reglare a orei efectuate în afara cadrului unei etalonări normale (cerințele 124 și 125 din anexa 1C).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType reprezintă tipul înregistrării (*VuTimeAdjustmentRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuTimeAdjustmentRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind operațiunile de reglare a orei.

2.234. **WorkshopCardApplicationIdentification**

Informații, stocate pe un card de atelier, privind identificarea aplicației cardului (cerințele 307 și 330 din anexa 1C).

Generația 1:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId precizează tipul de card implementat.

cardStructureVersion precizează versiunea structurii implementate în card.

noOfEventsPerType reprezintă numărul de evenimente, per tip de eveniment, pe care cardul le poate înregistra.

noOfFaultsPerType reprezintă numărul de anomalii, per tip de anomalie, pe care cardul le poate înregistra.

activityStructureLength indică numărul de octeți disponibili pentru stocarea înregistrărilor privind activitățile.

noOfCardVehicleRecords este numărul de înregistrări privind vehiculele pe care cardul le poate conține.

noOfCardPlaceRecords este numărul de locuri pe care cardul le poate înregistra.

noOfCalibrationRecords este numărul de înregistrări privind operațiunile de etalonare care pot fi stocate pe card.

Generația 2:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

În plus față de generația 1, se utilizează următoarele elemente de date:

noOfGNSSCDRecords este numărul de înregistrări GNSS privind timpul de conducere continuă care pot fi stocate pe card.

noOfSpecificConditionRecords este numărul de înregistrări privind condițiile specifice care pot fi stocate pe card.

2.235. **WorkshopCardCalibrationData**

Informații, stocate pe un card de atelier, privind activitățile atelierului efectuate cu cardul (cerințele 314, 316, 337 și 339 din anexa 1C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber este numărul total de operațiuni de etalonare efectuate cu cardul.

calibrationPointerNewestRecordeste indicele ultimei înregistrări actualizate privind etalonarea.

Atribuirea valorii: număr corespunzând numărătorului înregistrării privind etalonarea, începând cu '0' pentru prima ocurență a înregistrărilor privind etalonarea în structură.

calibrationRecords este setul de înregistrări care conțin informații privind etalonarea și/sau operațiunile de reglare a orei.

2.236. **WorkshopCardCalibrationRecord**

Informații, stocate pe un card de atelier, privind activitățile de etalonare efectuate cu cardul (cerințele 314 și 337 din anexa 1C).

Generația 1:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose este scopul etalonării.

vehicleIdentificationNumber este VIN.

vehicleRegistration conține VRN și statul membru de înmatriculare.

wVehicleCharacteristicConstant este coeficientul caracteristic al vehiculului.

kConstantOfRecordingEquipment este constanta aparaturii de înregistrare.

lTyreCircumference este circumferința efectivă a pneurilor roților.

tyreSize reprezintă desemnarea dimensiunilor pneurilor montate pe vehicul.

authorisedSpeed este viteza maximă autorizată a vehiculului.

oldOdometerValue, newOdometerValue reprezintă vechea și, respectiv, noua valoare indicate de odometru.

oldTimeValue, newTimeValue sunt valorile vechi și, respectiv, noi ale datei și orei.

nextCalibrationDate este data următoarei etalonări de tipul specificat în *CalibrationPurpose* care va fi efectuată de autoritatea de inspecție competentă.

vuPartNumber, **vuSerialNumber** și **sensorSerialNumber** sunt elementele de date pentru identificarea aparaturii de înregistrare.

Generația 2:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

În plus față de generația 1, se utilizează următoarele elemente de date:

sensorGNSSSerialNumber care identifică un echipament GNSS extern.

rcmSerialNumber care identifică un modul de comunicare la distanță.

sealDataCard oferă informații cu privire la sigiliile care sunt atașate la diferite componente ale vehiculului.

2.237. **WorkshopCardHolderIdentification**

Informații, stocate pe un card de atelier, privind identificarea titularului cardului (cerințele 311 și 334 din anexa 1C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName este numele atelierului de care aparține titularul cardului.

workshopAddress este adresa atelierului de care aparține titularul cardului.

cardHolderName este numele și prenumele titularului (de exemplu, numele mecanicului).

cardHolderPreferredLanguage este limba preferată de titularul cardului.

2.238. **WorkshopCardPIN**

Numărul de identificare personal al cardului de atelier (cerințele 309 și 332 din anexa 1C).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Atribuirea valorii: PIN-ul cunoscut de titularul cardului, completat la dreapta cu o serie de octeți 'FF' care poate conține până la 8 octeți.

2.239. **W-VehicleCharacteristicConstant**

Coeficientul caracteristic al vehiculului [definiția k)].

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Atribuirea valorii: impulsuri pe kilometru în intervalul operațional de la 0 la 64 255 impulsuri/km.

2.240. **VuPowerSupplyInterruptionRecord**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele de întrerupere a alimentării cu energie electrică (cerința 117 din anexa 1C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType este tipul de eveniment.

eventRecordPurpose este motivul pentru care s-a efectuat înregistrarea evenimentului respectiv.

eventBeginTime este data și ora la care a început evenimentul.

eventEndTime este data și ora la care s-a încheiat evenimentul.

cardNumberAndGenDriverSlotBegin identifică cardul introdus în slotul pentru cardul de conducător auto la începutul evenimentului, inclusiv generația cardului respectiv.

cardNumberAndGenDriverSlotEnd identifică cardul introdus în slotul pentru cardul de conducător auto la sfârșitul evenimentului, inclusiv generația cardului respectiv.

cardNumberAndGenCodriverSlotBegin identifică cardul introdus în slotul pentru cardul de copilot la începutul evenimentului, inclusiv generația cardului respectiv.

cardNumberAndGenCodriverSlotEnd identifică cardul introdus în slotul pentru cardul de copilot la sfârșitul evenimentului, inclusiv generația cardului respectiv.

similarEventsNumber este numărul de evenimente similare din ziua respectivă.

2.241. **VuPowerSupplyInterruptionRecordArray**

Generația 2:

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele de întrerupere a alimentării cu energie electrică (cerința 117 din anexa 1C).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType reprezintă tipul înregistrării (*VuPowerSupplyInterruptionRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *VuPowerSupplyInterruptionRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind evenimentele de întrerupere a alimentării cu energie electrică.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Generația 2:

Un set de *SensorExternalGNSSCoupledRecord,* plus metadatele utilizate în protocolul de descărcare.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType reprezintă tipul înregistrării (*SensorExternalGNSSCoupledRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *SensorExternalGNSSCoupledRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări *Sensor External GNSS Coupled*.

2.243. **VuSensorPairedRecordArray**

Generația 2:

Un set de *SensorPairedRecord,* plus metadatele utilizate în protocolul de descărcare.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType reprezintă tipul înregistrării (*SensorPairedRecord*). **Atribuirea valorii**: A se vedea *RecordType*

recordSize este dimensiunea *SensorPairedRecord* în octeți.

noOfRecords este numărul de înregistrări cuprinse în setul *records*.

records este un set de înregistrări privind senzorul asociat.

3. DEFINIREA INTERVALELOR DE VALORI ȘI DE DIMENSIUNI

Definiția valorilor variabilelor utilizate în definițiile de la punctul 2.

```
TimeRealRange ::= 2^32-1
```

4. SETURI DE CARACTERE

IA5Strings utilizează caracterele ASCII definite în standardul ISO/IEC 8824-1. În scopul lizibilității și pentru a facilita trimiterile, atribuirea valorilor este indicată în continuare. În caz de discrepanțe, aplicarea ISO/IEC 8824-1 are prioritate față de prezenta notă informativă.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

În alte șiruri de caractere (*Address, Name, VehicleRegistrationNumber*) se utilizează, în plus, caracterele din intervalul zecimal de caractere 161 – 255 din următoarele seturi standard de caractere de 8 biți, specificate prin numărul *Code Page*: Set caractere standard	Code Page (Zecimal)
ISO/IEC 8859-1 Latin-1 Western European	1
ISO/IEC 8859-2 Latin-2 Central European	2
ISO/IEC 8859-3 Latin-3 South European	3
ISO/IEC 8859-5 Latin / Cyrillic	5
ISO/IEC 8859-7 Latin / Greek	7
ISO/IEC 8859-9 Latin-5 Turkish	9
ISO/IEC 8859-13 Latin-7 Baltic Rim	13
ISO/IEC 8859-15 Latin-9	15
ISO/IEC 8859-16 Latin-10 South Eastern European	16
KOI8-R Latin / Cyrillic	80
KOI8-U Latin / Cyrillic	85

5. CODAREA

Atunci când sunt codate conform normelor de codare ASN.1, toate tipurile de date definite se codează conform standardului ISO/IEC 8825-2, varianta aliniată.

6. IDENTIFICATORII DE OBIECT ȘI IDENTIFICATORII DE APLICAȚIE

6.1. **Identificatorii de obiect**

Identificatorii de obiect (OID) enumerați în prezentul capitol sunt relevanți numai pentru generația 2. Acești OID sunt specificați în TR-03110-3 și reluați aici din motive de exhaustivitate. Acești OID sunt cuprinși în subarborele bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Identificatori ai protocolului de autentificare a VU

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Exemplu: Să presupunem că autentificarea VU trebuie să se realizeze cu SHA- 384; atunci identificatorul de obiect care trebuie utilizat este (în notație ASN.1) `bsi-de protocols(2) smartcard(2) 2 2 4`. Valoarea respectivului identificator de obiect în notația cu puncte este `0.4.0.127.0.7.2.2.2.2.4`.

	Notația cu puncte	Notația cu octeți
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	‘04 00 7F 00 07 02 02 02 02 03’
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	‘04 00 7F 00 07 02 02 02 02 04’
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	‘04 00 7F 00 07 02 02 02 02 05’

Identificatori ai protocolului de autentificare a cipului

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                          OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Exemplu: Să presupunem că autentificarea cipului trebuie efectuată prin utilizarea algoritmului ECDH, ducând la o lungime a cheii de sesiune AES de 128 de biți. Această cheie de sesiune va fi folosită apoi în modul de operare CBC pentru a asigura confidențialitatea datelor și cu algoritmul CMAC pentru a asigura autenticitatea datelor. Prin urmare, identificatorul de obiect care trebuie utilizat este (în notația ASN.1) `bsi-de protocols(2) smartcard(2) 3 2 2`. Valoarea respectivului identificator de obiect în notația cu puncte este `0.4.0.127.0.7.2.2.3.2.2`.

	Notația cu puncte	Notația cu octeți
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	‘04 00 7F 00 07 02 02 03 02 02’
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	‘04 00 7F 00 07 02 02 03 02 03’
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	‘04 00 7F 00 07 02 02 03 02 04’

6.2. Identificatorii de aplicație

Generația 2:

Identificatorul de aplicație (AID) pentru echipamentul GNSS extern (generația 2) este dat de ‘FF 44 54 45 47 4D’. Acesta este un AID exclusiv în conformitate cu ISO/IEC 7816-4.

Notă: ultimii 5 octeți codează DTEGM pentru echipamentul GNSS extern pentru tahografe inteligente.

Identificatorul de aplicație pentru aplicația cardului de tahograf de generația 2 este dat de 'FF 53 4D 52 44 54'. Acesta este un AID exclusiv în conformitate cu ISO/IEC 7816-4.

Apendicele 2

SPECIFICAȚIE PRIVIND CARDURILE DE TAHOGRAF

CUPRINS

1. INTRODUCERE 175
1.1. Abrevieri 175
1.2. Referințe 176
2. CARACTERISTICI ELECTRICE ȘI FIZICE 176
2.1. Tensiunea de alimentare și consumul de curent 177
2.2. Tensiunea de programare V_{PP} 177
2.3. Generare și frecvență ceas 177
2.4. Contact I/O (intrare/ieșire) 177
2.5. Stări ale cardului 177
3. HARDWARE ȘI COMUNICAȚII 177
3.1. Introducere 177
3.2. Protocolul de transmisie 178
3.2.1 Protocoale 178
3.2.2 ATR 179
3.2.3 PTS 179
3.3. Norme de acces 180
3.4. Prezentare generală a comenzilor și a codurilor de eroare 183
3.5. Descrierea comenzilor 185
3.5.1 SELECT 186
3.5.2 READ BINARY 187
3.5.3 UPDATE BINARY 194
3.5.4 GET CHALLENGE 200
3.5.5 VERIFY 200
3.5.6 GET RESPONSE 202
3.5.7 PSO: VERIFY CERTIFICATE 202
3.5.8 INTERNAL AUTHENTICATE 204
3.5.9 EXTERNAL AUTHENTICATE 205
3.5.10 GENERAL AUTHENTICATE 206
3.5.11 MANAGE SECURITY ENVIRONMENT 207
3.5.12 PSO: HASH 210
3.5.13 PERFORM HASH OF FILE 211
3.5.14 PSO: COMPUTE DIGITAL SIGNATURE 212
3.5.15 PSO: VERIFY DIGITAL SIGNATURE 213
3.5.16 PROCESS DSRC MESSAGE 214
4. STRUCTURA CARDURILOR DE TAHOGRAF 216
4.1. Fișier *master* MF 216

4.2. Aplicații de card de conducător auto 217
4.2.1 Aplicația de card de conducător auto de generația 1 217
4.2.2 Aplicația de card de conducător auto de generația 2 221
4.3. Aplicații de card de atelier 224
4.3.1 Aplicația de card de atelier de generația 1 224
4.3.2 Aplicația de card de atelier de generația 2 228
4.4. Aplicații de card de control 233
4.4.1 Aplicația de card de control de generația 1 233
4.4.2 Aplicația de card de control de generația 2 235
4.5. Aplicații de card de societate 237
4.5.1 Aplicația de card de societate de generația 1 237
4.5.2 Aplicația de card de societate de generația 2 238

1. INTRODUCERE

1.1. **Abrevieri**

În sensul prezentului apendice, se aplică următoarele abrevieri:

AC	Condiții de acces
AES	Standard de criptare avansată
AID	Identificator de aplicație
ALW	Întotdeauna
APDU	Unitate de date pentru protocolul de aplicație (structura unei comenzi)
ATR	Răspuns la resetare
AUT	Autentificat.
C6, C7	Contactele nr. 6 și 7 de pe card, conform descrierii din ISO/IEC 7816-2
cc	cicluri ceas
CHV	Informații de verificare a titularului cardului
CLA	Octet de clasă al unei comenzi APDU
DSRC	Comunicații specializate cu rază scurtă de acțiune
DF	Fișier dedicat. Un DF poate conține alte fișiere (EF sau DF)
ECC	Criptografie bazată pe curbe eliptice
EF	Fișier elementar
etu	unitate elementară de timp
G1	Generația 1
G2	Generația 2
IC	Circuit integrat
ICC	Card cu circuite integrate
ID	Identificator
IFD	Dispozitiv de interfață
IFS	Dimensiunea câmpului de informații
IFSC	Dimensiunea câmpului de informații pentru card

IFSD	Dimensiunea câmpului de informații pentru dispozitiv (pentru terminal)
INS	Octet de instrucțiuni al unei comenzi APDU
Lc	Lungimea datelor de intrare pentru o comandă APDU
Le	Lungimea datelor așteptate (date de ieșire pentru o comandă)
MF	Fișier *master* (DF rădăcină)
NAD	Adresă nod utilizată în protocolul T=1
NEV	Niciodată
P1-P2	Octeți de parametru
PIN	Număr de identificare personal
PRO SM	Protejat cu mesagerie securizată
PTS	Selectarea protocolului de transmisie
RFU	Rezervat pentru o utilizare viitoare
RST	Resetare (a cardului)
SFID	Identificator de EF scurt
SM	Mesagerie securizată
SW1-SW2	Octeți de stare
TS	Caracter inițial ATR
VPP	Tensiune de programare
VU	Unitate montată pe vehicul
XXh	Valoare XX în notație hexadecimală
'XXh'	Valoare XX în notație hexadecimală
||	Simbol de concatenare 03||04=0304

1.2. **Referințe**

În prezentul apendice se utilizează următoarele referințe:

ISO/IEC 7816-2 *Identification cards – Integrated circuit cards – Part 2: Dimensions and location of the contacts.* ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 *Identification cards – Integrated circuit cards – Part 3: Electrical interface and transmission protocols.* ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 *Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange.* ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 *Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange.* ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 *Identification cards – Integrated circuit cards – Part 8: Commands for security operations.* ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function.* ISO/IEC 9797-2:2011

2. CARACTERISTICI ELECTRICE ȘI FIZICE

TCS_01 Toate semnalele electronice trebuie să fie conforme cu ISO/IEC 7816-3, cu excepția cazului în care se specifică altfel.

TCS_02 Localizarea și dimensiunile contactelor cardului trebuie să fie conforme cu ISO/IEC 7816-2.

2.1. **Tensiunea de alimentare și consumul de curent**

TCS_03 Cardul trebuie să funcționeze conform specificațiilor în limitele de consum prevăzute în ISO/IEC 7816-3.

TCS_04 Cardul trebuie să funcționeze cu Vcc = 3V (± 0,3V) sau cu Vcc = 5V (± 0,5V).

Selectarea tensiunii trebuie să se facă în conformitate cu ISO/IEC 7816-3.

2.2. **Tensiunea de programare V_{pp}**

TCS_05 Cardul trebuie să nu necesite o tensiune de programare la contactul C6. Se prevede ca acest contact C6 să nu fie conectat într-un IFD. Contactul C6 poate fi conectat la V_{cc} în card, dar trebuie să nu fie conectat la masă. Această tensiune nu ar trebui interpretată în niciun caz.

2.3. **Generare și frecvență ceas**

TCS_06 Cardul trebuie să funcționeze într-un interval de frecvență de la 1 la 5 MHz și poate suporta frecvențe mai mari. Într-o sesiune de lucru cu cardul, frecvența ceasului poate varia cu ±2 %. Frecvența ceasului este generată de unitatea montată pe vehicul și nu de cardul în sine. Factorul de utilizare poate varia între 40 și 60 %.

TCS_07 Ceasul extern poate fi oprit în condițiile cuprinse în fișierul de card EF ICC. Primul octet din corpul fișierului EF ICC codează condițiile pentru modul „Clockstop”:

Scăzut	Ridicat		
Bit 3	Bit 2	Bit 1	
0	0	1	*Clockstop* permis, fără nivel preferat
0	1	1	*Clockstop* permis, nivel ridicat preferat
1	0	1	*Clockstop* permis, nivel scăzut preferat
0	0	0	*Clockstop* nepermis
0	1	0	*Clockstop* permis doar la nivel ridicat
1	0	0	*Clockstop* permis doar la nivel scăzut

Biții 4-8 nu sunt utilizați.

2.4. **Contact I/O (intrare/ieșire)**

TCS_08 Contactul I/O C7 este utilizat pentru recepționarea datelor de la IFD și pentru transmiterea datelor către IFD. În cursul funcționării, doar cardul sau doar IFD trebuie să fie în mod de transmisie. Dacă ambele unități sunt în mod de transmisie, cardul trebuie să nu sufere nicio deteriorare. Cu excepția cazului în care transmite, cardul trebuie să intre automat în mod de recepție.

2.5. **Stări ale cardului**

TCS_09 Cardul prezintă două stări atunci când se află sub tensiunea de alimentare:

Starea de funcționare, atunci când execută comenzi sau interfațează cu unitatea digitală,

Starea de repaus, în toate celelalte momente; în această stare, toate datele sunt reținute de card.

3. HARDWARE ȘI COMUNICAȚII

3.1. **Introducere**

Prezentul punct descrie funcționalitatea minimă necesară pentru cardurile de tahograf și VU în vederea asigurării unei funcționări corecte și a interoperabilității.

Cardurile de tahograf sunt conforme, în cea mai mare măsură posibilă, cu standardele disponibile ISO/IEC aplicabile (în special ISO/IEC 7816). Cu toate acestea, comenzile și protocoalele sunt descrise integral pentru a specifica anumite utilizări limitate sau anumite diferențe, dacă acestea există. Comenzile specificate sunt conforme pe deplin cu normele la care se face trimitere, cu excepția cazurilor indicate.

3.2. **Protocolul de transmisie**

TCS_10 Protocolul de transmisie trebuie să fie conform cu ISO/IEC 7816-3 pentru T=0 și T=1. În special, VU trebuie să recunoască prelungirile duratei de așteptare transmise de card.

3.2.1 *Protocoale*

TCS_11 Cardul trebuie să ofere atât protocolul **T=0**, cât și protocolul **T=1**. În plus, cardul poate fi compatibil și cu alte protocoale orientate pe contact.

TCS_12 **T=0** este protocolul implicit, prin urmare este necesară o comandă **PTS** pentru schimbarea protocolului în **T=1**.

TCS_13 Dispozitivele trebuie să fie compatibile cu **convenția directă** în ambele protocoale: prin urmare, convenția directă este obligatorie pentru card.

TCS_14 ATR trebuie să conțină, în caracterul TA3, octetul privind **dimensiunea câmpului de informații pentru card**. Această valoare trebuie să fie de cel puțin 'F0h' (= 240 de octeți).

Protocoalele sunt supuse următoarelor restricții:

TCS_15 **T=0**

— dispozitivul de interfață trebuie să fie compatibil cu un răspuns la intrare/ieșire după partea ascendentă a semnalului în RST plecând de la 400 cc;

— dispozitivul de interfață trebuie să poată citi caractere separate de 12 etu;

— dispozitivul de interfață trebuie să citească un caracter eronat și repetiția acestuia dacă sunt separate de 13 etu. Dacă este detectat un caracter eronat, semnalul de eroare la intrare/ieșire poate apărea între 1 etu și 2 etu. Dispozitivul trebuie să fie compatibil cu o întârziere de 1 etu;

— dispozitivul de interfață trebuie să accepte un ATR de 33 de octeți (TS+32);

— dacă ATR conține TC1, trebuie să fie prezent „Extra Guard Time" (timpul suplimentar de gardă) pentru caracterele transmise de către dispozitivul de interfață, deși caracterele transmise de card pot fi totuși separate de 12 etu. Acest lucru este valabil și pentru caracterul ACK transmis de card după un caracter P3 emis de dispozitivul de interfață;

— dispozitivul de interfață trebuie să țină cont de un caracter NUL emis de card;

— dispozitivul de interfață trebuie să accepte modul complementar pentru ACK;

— comanda „get-response" (obține un răspuns) nu poate fi utilizată în modul de înlănțuire pentru a obține date a căror lungime ar putea depăși 255 de octeți.

TCS_16 **T=1**

— octet NAD: neutilizat (NAD se setează la '00');

— *S-block ABORT*: neutilizat;

— *S-block VPP state error*: neutilizat;

— lungimea totală de înlănțuire pentru un câmp de date nu va depăși 255 de octeți (cerință care trebuie asigurată de IFD);

— dimensiunea câmpului de informații pentru dispozitiv (*Information Field Size Device* – IFSD) trebuie indicată de IFD imediat după ATR: IFD transmite solicitarea *S-Block IFS* după ATR, iar cardul răspunde transmițând *S-Block IFS*. Valoarea recomandată pentru IFSD este de 254 de octeți;

— cardul nu va solicita o reajustare a IFS.

3.2.2 *ATR*

TCS_17 Dispozitivul verifică octeții ATR, în conformitate cu ISO/IEC 7816-3. Nu se face nicio verificare cu privire la caracterele istorice ale ATR.

Exemplu de biprotocol de bază ATR conform ISO/IEC 7816-3

Caracter	Valoare	Observații
TS	'3Bh'	Indică convenție directă.
T0	'85h'	TD1 prezent; 5 octeți istorici sunt prezenți.
TD1	'80h'	TD2 prezent; trebuie folosit T=0
TD2	'11h'	TA3 prezent; trebuie folosit T=1
TA3	'XXh' (cel puțin 'F0h')	Dimensiunea câmpului de informații pentru card (IFSC)
TH1-TH5	'XXh'	Caractere istorice
TCK	'XXh'	Verificare caracter (SAU exclusiv)

TCS_18 După „Answer To Reset" (ATR), fișierul *master* (MF) este selectat implicit și devine directorul curent.

3.2.3 *PTS*

TCS_19 Protocolul implicit este T=0. Pentru a seta protocolul T=1, dispozitivul trebuie să transmită cardului o comandă PTS (cunoscută și ca PPS).

TCS_20 Întrucât protocoalele T=0 și T=1 sunt ambele obligatorii pentru card, PTS de bază pentru schimbarea protocolului este obligatorie pentru card.

PTS poate fi utilizată, conform indicațiilor din ISO/IEC 7816-3, pentru a trece la rate de modulație mai mari decât cea implicită propusă de card în ATR, dacă există o astfel de rată implicită [octetul TA(1)].

Ratele de modulație mai mari sunt opționale pentru card.

TCS_21 În cazul în care cardul nu este compatibil cu alte rate de modulație decât rata implicită (sau dacă nu este compatibil cu rata de modulație selectată), cardul trebuie să răspundă la PTS în mod corect, în conformitate cu ISO/IEC 7816-3, omițând octetul PPS1.

Următoarele sunt exemple de PTS de bază pentru selectarea protocolului:

Caracter	Valoare	Observații
PPSS	'FFh'	Caracterul de inițializare („The Initiate Character").
PPS0	'00h' sau '01h'	PPS1-PPS3 nu sunt prezente; '00h' pentru a selecta T0, '01h' pentru a selecta T1.
PK	'XXh'	Verificare caracter („Check character"): 'XXh' = 'FFh' dacă PPS0 = '00h', 'XXh' = 'FEh' dacă PPS0 = '01h'.

3.3. **Norme de acces**

TCS_22 O normă de acces specifică pentru un mod de acces, și anume o comandă, condițiile de securitate corespunzătoare. Dacă aceste condiții de securitate sunt îndeplinite, comanda corespunzătoare este prelucrată.

TCS_23 Următoarele condiții de securitate sunt utilizate pentru cardul de tahograf:

Abreviere	Sens
ALW	Acțiunea este posibilă întotdeauna și poate fi executată fără nicio restricție. APDU de comandă și de răspuns sunt transmise ca text în clar, adică fără mesagerie securizată.
NEV	Acțiunea nu este posibilă niciodată.
PLAIN-C	APDU de comandă este transmisă ca text în clar, adică fără mesagerie securizată.
PWD	Acțiunea poate fi executată numai dacă PIN-ul cardului de atelier a fost verificat cu succes, și anume dacă este stabilită starea de securitate internă „PIN_Verified" a cardului. Comanda trebuie transmisă fără mesagerie securizată.
EXT-AUT-G1	Acțiunea poate fi executată numai în cazul în care comanda „External Authenticate" (autentificare externă) pentru autentificarea de generația 1 (a se vedea, de asemenea, apendicele 11 partea A) a fost executată cu succes.
SM-MAC-G1	APDU (comandă și răspuns) trebuie să fie aplicată cu mesagerie securizată de generația 1 în mod doar de autentificare (a se vedea apendicele 11 partea A).
SM-C-MAC-G1	APDU de comandă trebuie să fie aplicată cu mesagerie securizată de generația 1 în mod doar de autentificare (a se vedea apendicele 11 partea A).
SM-R-ENC-G1	APDU de răspuns trebuie să fie aplicată cu mesagerie securizată de generația 1 în mod de criptare (a se vedea apendicele 11 partea A), și anume nu se returnează niciun cod de autentificare a mesajului.
SM-R-ENC-MAC-G1	APDU de răspuns trebuie să fie aplicată cu mesagerie securizată de generația 1 în mod de criptare apoi autentificare (a se vedea apendicele 11 partea A).
SM-MAC-G2	APDU (comandă și răspuns) trebuie să fie aplicată cu mesagerie securizată de generația 2 în mod doar de autentificare (a se vedea apendicele 11 partea B).
SM-C-MAC-G2	APDU de comandă trebuie să fie aplicată cu mesagerie securizată de generația 2 în mod doar de autentificare (a se vedea apendicele 11 partea B).
SM-R-ENC-MAC-G2	APDU de răspuns trebuie să fie aplicată cu mesagerie securizată de generația 2 în mod de criptare apoi autentificare (a se vedea apendicele 11 partea B).

TCS_24 Aceste condiții de securitate pot fi conectate în următoarele moduri:

ȘI: Trebuie îndeplinite toate condițiile de securitate

SAU: Trebuie îndeplinită cel puțin o condiție de securitate

Normele de acces pentru sistemul de fișiere, și anume comanda SELECT, READ BINARY și UPDATE BINARY, sunt specificate în capitolul 4. Normele de acces pentru restul comenzilor sunt specificate în tabelele de mai jos.

TCS_25 În aplicația DF Tachograph G1 se utilizează următoarele norme de acces:

Comandă	Card de conducător auto	Card de atelier	Card de control	Card de societate
External Authenticate				
— Pentru autentificarea de generația 1	ALW	ALW	ALW	ALW
— Pentru autentificarea de generația 2	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nu se aplică.	Nu se aplică.	Nu se aplică.	Nu se aplică.
PSO: Compute Digital Signature	ALW SAU SM-MAC-G2	ALW SAU SM-MAC-G2	Nu se aplică.	Nu se aplică.
PSO: Hash	Nu se aplică.	Nu se aplică.	ALW	Nu se aplică.
PSO: Hash of File	ALW SAU SM-MAC-G2	ALW SAU SM-MAC-G2	Nu se aplică.	Nu se aplică.
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nu se aplică.	Nu se aplică.	ALW	Nu se aplică.
Verify	Nu se aplică.	ALW	Nu se aplică.	Nu se aplică.

TCS_26 În aplicația DF Tachograph_G2 se utilizează următoarele norme de acces:

Comandă	Card de conducător auto	Card de atelier	Card de control	Card de societate
External Authenticate				
— Pentru autentificarea de generația 1	Nu se aplică.	Nu se aplică.	Nu se aplică.	Nu se aplică.
— Pentru autentificarea de generația 2	ALW	PWD	ALW	ALW
Internal Authenticate	Nu se aplică.	Nu se aplică.	Nu se aplică.	Nu se aplică.

Comandă	Card de conducător auto	Card de atelier	Card de control	Card de societate
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nu se aplică.	ALW	ALW	Nu se aplică.
PSO: Compute Digital Signature	ALW SAU SM-MAC-G2	ALW SAU SM-MAC-G2	Nu se aplică.	Nu se aplică.
PSO: Hash	Nu se aplică.	Nu se aplică.	ALW	Nu se aplică.
PSO: Hash of File	ALW SAU SM-MAC-G2	ALW SAU SM-MAC-G2	Nu se aplică.	Nu se aplică.
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nu se aplică.	Nu se aplică.	ALW	Nu se aplică.
Verify	Nu se aplică.	ALW	Nu se aplică.	Nu se aplică.

TCS_27 În MF se utilizează următoarele norme de acces:

Comandă	Card de conducător auto	Card de atelier	Card de control	Card de societate
External Authenticate				
— Pentru autentificarea de generația 1	Nu se aplică.	Nu se aplică.	Nu se aplică.	Nu se aplică.
— Pentru autentificarea de generația 2	ALW	PWD	ALW	ALW
Internal Authenticate	Nu se aplică.	Nu se aplică.	Nu se aplică.	Nu se aplică.
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nu se aplică.	Nu se aplică.	Nu se aplică.	Nu se aplică.

Comandă	Card de conducător auto	Card de atelier	Card de control	Card de societate
PSO: Compute Digital Signature	Nu se aplică.	Nu se aplică.	Nu se aplică.	Nu se aplică.
PSO: Hash	Nu se aplică.	Nu se aplică.	Nu se aplică.	Nu se aplică.
PSO: Hash of File	Nu se aplică.	Nu se aplică.	Nu se aplică.	Nu se aplică.
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Nu se aplică.	ALW	Nu se aplică.	Nu se aplică.

TCS_28 Un card de tahograf poate sau nu să accepte o comandă cu un nivel de securitate mai ridicat decât cel specificat în condițiile de securitate. Cu alte cuvinte, în cazul în care condiția de securitate este ALW (sau PLAIN-C) cardul poate accepta o comandă cu mesagerie securizată (mod de criptare și/sau de autentificare). În cazul în care condiția de securitate impune utilizarea de mesagerie securizată cu mod de autentificare, cardul de tahograf poate accepta o comandă cu mesagerie securizată din aceeași generație în mod de autentificare și de criptare.

Notă: descrierile comenzilor oferă mai multe informații cu privire la compatibilitatea comenzilor cu diferitele tipuri de card de tahograf și cu diferitele DF.

3.4. **Prezentare generală a comenzilor și a codurilor de eroare**

Comenzile și organizarea fișierelor sunt derivate din ISO/IEC 7816-4 și sunt conforme cu acest standard.

Prezenta secțiune descrie perechile de comandă-răspuns APDU menționate în cele ce urmează. Variantele de comandă care sunt compatibile cu o aplicație de generația 1 și 2 sunt specificate în descrierile corespunzătoare ale comenzilor.

Comandă	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	

Comandă	INS
INTERNAL AUTHENTICATE	'88h'
EXTERNAL AUTHENTICATE	'82h'
MANAGE SECURITY ENVIRONMENT	'22h'
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	'86h'

TCS_29 Cuvintele de stare SW1 SW2 sunt returnate în orice mesaj de răspuns și indică starea de procesare a comenzii.

SW1	SW2	Sens
90	00	Procesare normală.
61	XX	Procesare normală. XX = numărul de octeți de răspuns disponibili.
62	81	Procesare de avertizare. Este posibil ca o parte din datele returnate să fie corupte
63	00	Autentificare eșuată (avertizare)
63	CX	CHV (PIN) eronat. Numărul încercărilor rămase este dat de 'X'.
64	00	Eroare de execuție – Starea memoriei nevolatile nu s-a modificat. Eroare de integritate.
65	00	Eroare de execuție – Starea memoriei nevolatile s-a modificat.
65	81	Eroare de execuție – Starea memoriei nevolatile s-a modificat – Eroare de memorie
66	88	Eroare de securitate: sumă de verificare criptografică eronată (în cursul mesageriei securizate) sau certificat eronat (în cursul verificării certificatului) sau criptogramă eronată (în cursul autentificării externe) sau semnătură eronată (în cursul verificării semnăturii)
67	00	Lungime eronată (Lc sau Le eronată)
68	82	Incompatibilitate cu mesageria securizată
68	83	Se așteaptă ultima comandă din lanț
69	00	Comandă interzisă (niciun răspuns disponibil în T=0)
69	82	Starea de securitate nu este îndeplinită.
69	83	Metoda de autentificare este blocată.
69	85	Condițiile de utilizare nu sunt satisfăcute.
69	86	Comandă nepermisă (niciun EF curent)

SW1	SW2	Sens
69	87	Obiectele de date așteptate din mesageria securizată lipsesc
69	88	Obiectele de date din mesageria securizată sunt incorecte
6A	80	Parametri incorecți în câmpul de date
6A	82	Fișierul nu poate fi găsit.
6A	86	Parametrii P1-P2 eronați.
6A	88	Datele menționate nu pot fi găsite.
6B	00	Parametri eronați (deplasare în afara EF).
6C	XX	Lungime eronată, SW2 indică lungimea exactă. Nu este returnat niciun câmp de date.
6D	00	Cod de instrucțiuni incompatibil sau invalid.
6E	00	Clasă incompatibilă.
6F	00	Alte erori de verificare.

TCS_30 Dacă într-o APDU de comandă este îndeplinită mai mult de o condiție de eroare, cardul poate returna oricare dintre cuvintele de stare corespunzătoare.

3.5. **Descrierea comenzilor**

Prezentul capitol descrie comenzile obligatorii pentru cardurile de tahograf.

Detalii suplimentare pertinente cu privire la operațiunile criptografice implicate se găsesc în apendicele 11 Mecanisme de securitate comune pentru generația 1 și generația 2 de tahografe.

Toate comenzile sunt descrise independent de protocolul utilizat (T=0 sau T=1). Octeții APDU CLA, INS, P1, P2, Lc și Le sunt întotdeauna indicați. Dacă Lc sau Le nu sunt necesare pentru comanda descrisă, lungimea, valoarea și descrierea aferente sunt vide.

TCS_31 Dacă sunt solicitați ambii octeți de lungime (Lc și Le), comanda descrisă trebuie să fie separată în două părți în cazul în care IFD utilizează protocolul T=0: IFD transmite comanda conform descrierii cu P3=Lc + date și apoi transmite o comandă GET RESPONSE (a se vedea secțiunea 3.5.6) cu P3=Le.

TCS_32 Dacă sunt solicitați ambii octeți de lungime, iar Le=0 (mesagerie securizată):

— atunci când se utilizează protocolul T=1, cardul trebuie să răspundă la Le=0 prin transmiterea tuturor datelor de ieșire disponibile;

— atunci când se utilizează protocolul T=0, IFD trebuie să transmită prima comandă cu P3=Lc + date, iar cardul trebuie să răspundă (la această valoare implicită Le=0) cu octeții de stare '**61La**', unde La este numărul de octeți de răspuns disponibili. IFD trebuie să genereze apoi o comandă GET RESPONSE cu P3 = La, pentru a citi datele.

TCS_33 Un card de tahograf poate fi compatibil cu câmpuri cu lungime extinsă în conformitate cu ISO/IEC 7816-4, ca o caracteristică opțională. Un card de tahograf care este compatibil cu câmpuri cu lungime extinsă trebuie:

— să indice compatibilitatea cu câmpurile cu lungime extinsă în ATR;

— să furnizeze dimensiunile zonei tampon compatibile prin intermediul informației privind lungimea extinsă în EF ATR/INFO, a se vedea TCS_146;

— să indice dacă este compatibil cu câmpuri cu lungime extinsă pentru T = 1 și/sau T = 0 în EF *Extended Length*, a se vedea TCS_147;

— să fie compatibil cu câmpuri cu lungime extinsă pentru generația 1 și 2 de aplicații tahografice.

Note:

Toate comenzile sunt specificate pentru câmpuri cu o lungime redusă. Utilizarea APDU-urilor cu lungime extinsă rezultă clar din ISO/IEC 7816-4.

În general, comenzile sunt specificate pentru scrierea în clar, adică fără mesagerie securizată, nivelul de mesagerie securizată fiind specificat în apendicele 11. Din normele de acces pentru o comandă rezultă în mod clar dacă respectiva comandă trebuie să fie compatibilă cu mesageria securizată sau nu și dacă respectiva comandă trebuie să fie compatibilă cu generația 1 și/sau generația 2 de mesagerie securizată. Unele variante de comandă sunt descrise incluzând mesageria securizată, pentru a ilustra utilizarea mesageriei securizate.

TCS_34 VU trebuie să execute întregul protocol de autentificare reciprocă VU – card de generația 2 pentru o sesiune incluzând verificarea certificatului (dacă este necesar), fie în DF Tachograph, fie în DF Tachograph_G2, fie în MF.

3.5.1 *SELECT*

Această comandă respectă ISO/IEC 7816-4, dar are o utilizare restricționată comparativ cu comanda definită în standard.

Comanda SELECT se utilizează:

— pentru a selecta un DF de aplicație (trebuie utilizată selectarea după denumire);

— pentru a selecta un fișier elementar corespunzător ID-ului fișierului prezentat.

3.5.1.1 Selectare după denumire (AID)

Această comandă permite selectarea unui DF de aplicație din card.

TCS_35 Această comandă poate fi executată din orice parte din structura fișierelor (după ATR sau în orice moment).

TCS_36 Selectarea unei aplicații resetează mediul de securitate curent. După ce s-a efectuat selectarea aplicației, nu mai este selectată nicio cheie publică curentă. De asemenea, se pierde condiția de acces EXT-AUT-G1. În cazul în care comanda a fost executată fără mesagerie securizată, cheile de sesiune anterioare ale mesageriei securizate nu mai sunt disponibile.

TCS_37 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Selectare după denumire (AID)
P2	1	'0Ch'	Nu se așteaptă niciun răspuns
Lc	1	'NNh'	Numărul de octeți transmiși către card (lungimea AID): '06h' pentru aplicația tahografică
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' pentru aplicația tahografică de generația 1 AID: 'FF 53 4D 52 44 54' pentru aplicația tahografică de generația 2

Nu este necesar niciun răspuns la comanda SELECT (Le absentă în T=1 sau nu se solicită niciun răspuns în T=0).

TCS_38 **Mesaj de răspuns (nu se solicită niciun răspuns)**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă aplicația corespunzătoare AID nu este găsită, starea de procesare returnată este '**6A82**'.

— În T=1, dacă este prezent octetul Le, starea returnată este '**6700**'.

— În T=0, dacă se solicită un răspuns după comanda SELECT, starea returnată este '**6900**'.

— Dacă aplicația selectată este considerată coruptă (în atributele fișierului este detectată o eroare de integritate), starea de procesare returnată este '**6400**' sau '**6581**'.

3.5.1.2 Selectarea unui fișier elementar folosind identificatorul de fișier al acestuia

TCS_39 **Mesaj de comandă**

TCS_40 Un card de tahograf trebuie să fie compatibil cu mesageria securizată de generația 2 conform specificațiilor din apendicele 11 partea B pentru această variantă de comandă.

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Selectarea unui EF din DF curent
P2	1	'0Ch'	Nu se așteaptă niciun răspuns
Lc	1	'02h'	Numărul de octeți transmiși către card
#6-#7	2	'XXXXh'	Identificatorul fișierului

Nu este necesar niciun răspuns la comanda SELECT (Le absentă în T=1 sau nu se solicită niciun răspuns în T=0).

TCS_41 **Mesaj de răspuns (nu se solicită niciun răspuns)**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă fișierul corespunzător identificatorului de fișier nu este găsit, starea de procesare returnată este '**6A82**'.

— În T=1, dacă este prezent octetul Le, starea returnată este '**6700**'.

— În T=0, dacă se solicită un răspuns după comanda SELECT, starea returnată este '**6900**'.

— Dacă fișierul selectat este considerat corupt (în atributele fișierului este detectată o eroare de integritate), starea de procesare returnată este '**6400**' sau '**6581**'.

3.5.2 *READ BINARY*

Această comandă respectă ISO/IEC 7816-4, dar are o utilizare restricționată comparativ cu comanda definită în standard.

Comanda READ BINARY se utilizează pentru citirea datelor dintr-un fișier transparent.

Răspunsul cardului constă în returnarea datelor citite, încapsulate opțional într-o structură de mesagerie securizată.

3.5.2.1 Comandă cu deplasare în P1-P2

Această comandă permite IFD să citească datele din EF-ul selectat în momentul respectiv, fără mesagerie securizată.

Notă: Această comandă fără mesagerie securizată poate fi utilizată numai pentru a citi un fișier care este compatibil cu condiția de securitate ALW pentru modul de acces de citire („read").

TCS_42 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'B0h'	Citire date (*Read Binary*)
P1	1	'XXh'	Deplasare octeți de la începutul fișierului: cel mai semnificativ octet
P2	1	'XXh'	Deplasare octeți de la începutul fișierului: cel mai puțin semnificativ octet
Le	1	'XXh'	Lungimea datelor așteptate. Numărul de octeți de citit.

Notă: bitul 8 al P1 trebuie setat la 0.

TCS_43 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
#1-#X	X	'XX..XXh'	Date citite
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă nu este selectat niciun EF, starea de procesare returnată este '**6986**'.

— Dacă nu sunt îndeplinite condițiile de securitate pentru fișierul selectat, comanda este întreruptă cu '**6982**'.

— Dacă deplasarea nu este compatibilă cu dimensiunea EF (Deplasare > dimensiune EF), starea de procesare returnată este '**6B00**'.

— Dacă dimensiunea datelor de citit nu este compatibilă cu dimensiunea EF (Deplasare + Le > dimensiune EF), starea de procesare returnată este '**6700**' sau '**6Cxx**', unde 'xx' indică lungimea exactă.

— Dacă în atributele fișierului este detectată o eroare de integritate, cardul trebuie să considere fișierul ca fiind corupt și irecuperabil, iar starea de procesare returnată este '**6400**' sau '**6581**'.

— Dacă în datele stocate este detectată o eroare de integritate, cardul trebuie să returneze datele solicitate, iar starea de procesare returnată este '**6281**'.

3.5.2.1.1 Comandă cu mesagerie securizată (exemple)

Această comandă permite IFD să citească date din EF-ul selectat în momentul respectiv, cu mesagerie securizată, pentru a verifica integritatea datelor primite și pentru a proteja confidențialitatea datelor în cazul în care este aplicată condiția de securitate SM-R-ENC-MAC-G1 (generația 1) sau SM-R-ENC-MAC-G2 (generația 2).

TCS_44 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'0Ch'	Mesagerie securizată solicitată
INS	1	'B0h'	Citire date (*Read Binary*)
P1	1	'XXh'	P1 (deplasare octeți de la începutul fișierului): cel mai semnificativ octet
P2	1	'XXh'	P2 (deplasare octeți de la începutul fișierului): cel mai puțin semnificativ octet
Lc	1	'XXh'	Lungimea datelor de intrare pentru mesageria securizată
#6	1	'97h'	T_{LE}: etichetă pentru specificația lungimii așteptate.
#7	1	'01h'	L_{LE}: lungimea lungimii așteptate
#8	1	'NNh'	Specificația lungimii așteptate (Le originală): numărul de octeți de citit
#9	1	'8Eh'	T_{CC}: etichetă pentru suma de verificare criptografică
#10	1	'XXh'	L_{CC}: lungimea sumei de verificare criptografice următoare '04h' pentru mesageria securizată de generația 1 (a se vedea apendicele 11 partea A) '08h', '0Ch' sau '10h', în funcție de lungimea cheii AES pentru mesageria securizată de generația 2 (a se vedea apendicele 11 partea B)
#11-#(10 + L)	L	'XX..XXh'	Sumă de verificare criptografică
Le	1	'00h'	Conform specificațiilor din ISO/IEC 7816-4

TCS_45 **Mesaj de răspuns dacă SM-R-ENC-MAC-G1 (generația 1) / SM-R-ENC-MAC-G2 (generația 2) nu este necesară și dacă formatul de intrare pentru mesageria securizată este corect:**

Octet	Lungime	Valoare	Descriere
#1	1	'99h'	Etichetă pentru starea de procesare (SW1-SW2) – opțională pentru mesageria securizată de generația 1
#2	1	'02h'	Lungimea stării de procesare
#3 – #4	2	'XX XXh'	Starea de procesare a APDU de răspuns neprotejate
#5	1	'81h'	T_{PV}: etichetă pentru valoarea datelor în clar
#6	L	'NNh' sau '81 NNh'	L_{PV}: lungimea datelor returnate (= Le originală) L este de 2 octeți dacă L_{PV} > 127 de octeți.

Octet	Lungime	Valoare	Descriere
#(6 + L)-#(5 + L + NN)	NN	'XX..XXh'	Valoarea datelor în clar
#(6 + L + NN)	1	'8Eh'	T_{CC}: etichetă pentru suma de verificare criptografică
#(7 + L + NN)	1	'XXh'	L_{CC}: lungimea sumei de verificare criptografice următoare '04h' pentru mesageria securizată de generația 1 (a se vedea apendicele 11 partea A) '08h', '0Ch' sau '10h', în funcție de lungimea cheii AES pentru mesageria securizată de generația 2 (a se vedea apendicele 11 partea B)
#(8 + L + NN)-#(7 + M + L + NN)	M	'XX..XXh'	Sumă de verificare criptografică
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

TCS_46 **Mesaj de răspuns dacă SM-R-ENC-MAC-G1 (generația 1) / SM-R-ENC-MAC-G2 (generația 2) este necesară și dacă formatul de intrare pentru mesageria securizată este corect:**

Octet	Lungime	Valoare	Descriere
#1	1	'87h'	$T_{PI\ CG}$: etichetă pentru date criptate (criptogramă)
#2	L	'MMh' sau '81 MMh'	$L_{PI\ CG}$: lungimea datelor criptate returnate (diferită de Le originală a comenzii din cauza completării). L este de 2 octeți dacă $L_{PI\ CG}$ > 127 de octeți
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Date criptate: indicator de completare și criptogramă
#(2+L+MM)	1	'99h'	Etichetă pentru starea de procesare (SW1-SW2) – opțională pentru mesageria securizată de generația 1
#(3+L+MM)	1	'02h'	Lungimea stării de procesare
#(4+L+MM) – #(5+L+MM)	2	'XX XXh'	Starea de procesare a APDU de răspuns neprotejate
#(6+L+MM)	1	'8Eh'	T_{CC}: etichetă pentru suma de verificare criptografică
#(7+L+MM)	1	'XXh'	L_{CC}: lungimea sumei de verificare criptografice următoare '04h' pentru mesageria securizată de generația 1 (a se vedea apendicele 11 partea A) '08h', '0Ch' sau '10h', în funcție de lungimea cheii AES pentru mesageria securizată de generația 2 (a se vedea apendicele 11 partea B)
#(8+L+MM)-#(7+N+L+MM)	N	'XX..XXh'	Sumă de verificare criptografică
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

Comanda READ BINARY poate returna stările de procesare normale enumerate în TCS_43 cu eticheta '99h', conform descrierii din TCS_59, folosind structura de răspuns a mesageriei securizate.

În plus, pot apărea unele erori legate în mod specific de mesageria securizată. În acest caz, starea de procesare este returnată pur și simplu, fără a mai implica o structură de mesagerie securizată:

TCS_47 **Mesaj de răspuns dacă formatul de intrare pentru mesageria securizată este incorect**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— Dacă nu este disponibilă nicio cheie de sesiune curentă, se returnează starea de procesare '**6A88**'. Acest lucru se întâmplă fie în cazul în care cheia de sesiune nu a fost generată deja, fie în cazul în care valabilitatea cheii de sesiune a expirat (în acest caz, IFD trebuie să ruleze din nou un proces de autentificare reciprocă pentru a seta o nouă cheie de sesiune).

— Dacă unele dintre obiectele de date așteptate (conform specificațiilor de mai sus) lipsesc din formatul de mesagerie securizată, se returnează starea de procesare '**6987**': această eroare se produce dacă lipsește o etichetă așteptată sau dacă corpul comenzii nu este construit în mod corect.

— Dacă unele obiecte de date sunt incorecte, starea de procesare returnată este '**6988**': această eroare se produce dacă toate etichetele necesare sunt prezente, dar unele lungimi sunt diferite de cele așteptate.

— Dacă verificarea sumei de verificare criptografice eșuează, starea de procesare returnată este '**6688**'.

3.5.2.2 Comandă cu identificator de EF (fișier elementar) scurt

Această variantă de comandă permite IFD să selecteze un EF prin intermediul unui identificator de EF scurt și să citească date din EF-ul respectiv.

TCS_48 Un card de tahograf trebuie să fie compatibil cu această variantă de comandă pentru toate fișierele elementare care au un identificator de EF scurt specificat. Acești identificatori de EF scurți sunt specificați în capitolul 4.

TCS_49 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'B0h'	Citire date (*Read Binary*)
P1	1	'XXh'	Bitul 8 este setat la 1 Biții 7 și 6 sunt setați la 00 Biții 5-1 codează identificatorul de EF scurt al EF-ului corespunzător
P2	1	'XXh'	Codează o deplasare de la 0 la 255 de octeți în EF-ul la care face trimitere P1
Le	1	'XXh'	Lungimea datelor așteptate. Numărul de octeți de citit.

Notă: identificatorii de EF scurți utilizați pentru aplicația tahografică de generația 2 sunt specificați în capitolul 4.

Dacă P1 codează un identificator de EF scurt și comanda este executată cu succes, EF-ul identificat devine EF-ul selectat în momentul respectiv (EF curent).

TCS_50 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
#1-#L	L	'XX..XXh'	Date citite
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă fișierul corespunzător identificatorului de EF scurt nu este găsit, starea de procesare returnată este '**6A82**'.

— Dacă nu sunt îndeplinite condițiile de securitate pentru fișierul selectat, comanda este întreruptă cu '**6982**'.

— Dacă deplasarea nu este compatibilă cu dimensiunea EF (Deplasare > dimensiune EF), starea de procesare returnată este '**6B00**'.

— Dacă dimensiunea datelor de citit nu este compatibilă cu dimensiunea EF (Deplasare + Le > dimensiune EF), starea de procesare returnată este '**6700**' sau '**6Cxx**', unde 'xx' indică lungimea exactă.

— Dacă în atributele fișierului este detectată o eroare de integritate, cardul trebuie să considere fișierul ca fiind corupt și irecuperabil, iar starea de procesare returnată este '**6400**' sau '**6581**'.

— Dacă în datele stocate este detectată o eroare de integritate, cardul trebuie să returneze datele solicitate, iar starea de procesare returnată este '**6281**'.

3.5.2.3 Comandă cu octet de instrucțiuni impar

Această variantă de comandă permite IFD să citească datele dintr-un EF cu 32 768 de octeți sau mai mulți.

TCS_51 Un card de tahograf care este compatibil cu EF-uri cu 32 768 de octeți sau mai mulți trebuie să fie compatibil cu această variantă de comandă pentru EF-urile respective. Un card de tahograf poate să fie sau nu compatibil cu această variantă de comandă pentru alte EF-uri, cu excepția EF *Sensor_Installation_Data*. A se vedea TCS_156 și TCS_160.

TCS_52 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'B1h'	Citire date (*Read Binary*)
P1	1	'00h'	EF curent
P2	1	'00h'	
Lc	1	'NNh'	Lc Lungimea obiectului de date deplasat.
#6-#(5+NN)	NN	'XX..XXh'	Obiect de date deplasat: Etichetă '54h' Lungime '01h' sau '02h' Valoare deplasare
Le	1	'XXh'	Numărul de octeți de citit.

IFD trebuie să codeze lungimea obiectului de date deplasat cu un număr minim posibil de octeți, și anume: utilizând octetul de lungime '01h' IFD codează o deplasare de la 0 la 255 și utilizând octetul de lungime '02h' o deplasare de la '256' până la '65 535' de octeți.

TCS_53 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
#1-#L	L	'XX..XXh'	Date citite încapsulate într-un obiect de date discreționar cu eticheta '53h'.
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă nu este selectat niciun EF, starea de procesare returnată este '**6986**'.

— Dacă nu sunt îndeplinite condițiile de securitate pentru fișierul selectat, comanda este întreruptă cu '**6982**'.

— Dacă deplasarea nu este compatibilă cu dimensiunea EF (Deplasare > dimensiune EF), starea de procesare returnată este '**6B00**'.

— Dacă dimensiunea datelor de citit nu este compatibilă cu dimensiunea EF (Deplasare + Le > dimensiune EF), starea de procesare returnată este '**6700**' sau '**6Cxx**', unde 'xx' indică lungimea exactă.

— Dacă în atributele fișierului este detectată o eroare de integritate, cardul trebuie să considere fișierul ca fiind corupt și irecuperabil, iar starea de procesare returnată este '**6400**' sau '**6581**'.

— Dacă în datele stocate este detectată o eroare de integritate, cardul trebuie să returneze datele solicitate, iar starea de procesare returnată este '**6281**'.

3.5.2.3.1 Comandă cu mesagerie securizată (exemplu)

Următorul exemplu ilustrează utilizarea mesageriei securizate în cazul în care se aplică condiția de securitate SM-MAC-G2.

TCS_54 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'0Ch'	Mesagerie securizată solicitată
INS	1	'B1h'	Citire date (*Read Binary*)
P1	1	'00h'	EF curent
P2	1	'00h'	
Lc	1	'XXh'	Lungimea câmpului de date securizate
#6	1	'B3h'	Etichetă pentru valoarea datelor în clar codate în BER-TLV
#7	1	'NNh'	L_{PV}: lungimea datelor transmise
#(8)-#(7+NN)	NN	'XX..XXh'	Date în clar codate în BER-TLV, și anume obiectul de date deplasat cu eticheta '54'
#(8+NN)	1	'97h'	T_{LE}: etichetă pentru specificația lungimii așteptate.
#(9+NN)	1	'01h'	L_{LE}: lungimea lungimii așteptate
#(10+NN)	1	'XXh'	Specificația lungimii așteptate (Le originală): numărul de octeți de citit
#(11+NN)	1	'8Eh'	T_{CC}: etichetă pentru suma de verificare criptografică
#(12+NN)	1	'XXh'	L_{CC}: lungimea sumei de verificare criptografice următoare '08h', '0Ch' sau '10h', în funcție de lungimea cheii AES pentru mesageria securizată de generația 2 (a se vedea apendicele 11 partea B)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Sumă de verificare criptografică
Le	1	'00h'	Conform specificațiilor din ISO/IEC 7816-4

TCS_55 Mesaj de răspuns în cazul în care comanda este executată cu succes

Octet	Lungime	Valoare	Descriere
#1	1	'B3h'	Date în clar codate în BER-TLV
#2	L	'NNh' sau '81 NNh'	L_{PV}: lungimea datelor returnate (= Le originală) L este de 2 octeți dacă L_{PV} > 127 de octeți
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Valoarea datelor în clar codate în BER-TLV, adică datele citite încapsulate într-un obiect de date discreționar cu eticheta '53h'.
#(2+L+NN)	1	'99h'	Starea de procesare a APDU de răspuns neprotejate
#(3+L+NN)	1	'02h'	Lungimea stării de procesare
#(4+L+NN) – #(5+L+NN)	2	'XX XXh'	Starea de procesare a APDU de răspuns neprotejate
#(6+L+NN)	1	'8Eh'	T_{CC}: etichetă pentru suma de verificare criptografică
#(7+L+NN)	1	'XXh'	L_{CC}: lungimea sumei de verificare criptografice următoare '08h', '0Ch' sau '10h', în funcție de lungimea cheii AES pentru mesageria securizată de generația 2 (a se vedea apendicele 11 partea B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Sumă de verificare criptografică
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

3.5.3 *UPDATE BINARY*

Această comandă respectă ISO/IEC 7816-4, dar are o utilizare restricționată comparativ cu comanda definită în standard.

Mesajul de comandă UPDATE BINARY inițializează actualizarea (ștergere + scriere) biților deja prezenți într-un EF binar cu biții dați în APDU de comandă.

3.5.3.1 Comandă cu deplasare în P1-P2

Această comandă permite IFD să scrie date în EF-ul selectat în momentul respectiv, fără ca integritatea datelor primite să fie verificată de card.

Notă: Această comandă fără mesagerie securizată poate fi utilizată numai pentru a actualiza un fișier care este compatibil cu condiția de securitate ALW pentru modul de acces de actualizare („update").

TCS_56 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'D6h'	Actualizare date (*Update Binary*)

Octet	Lungime	Valoare	Descriere
P1	1	'XXh'	Deplasare octeți de la începutul fișierului: cel mai semnificativ octet
P2	1	'XXh'	Deplasare octeți de la începutul fișierului: cel mai puțin semnificativ octet
Lc	1	'NNh'	Lc Lungimea datelor de actualizat. Numărul de octeți de scris.
#6-#(5+NN)	NN	'XX..XXh'	Date de scris

Notă: bitul 8 al P1 trebuie setat la 0.

TCS_57 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă nu este selectat niciun EF, starea de procesare returnată este '**6986**'.

— Dacă nu sunt îndeplinite condițiile de securitate pentru fișierul selectat, comanda este întreruptă cu '**6982**'.

— Dacă deplasarea nu este compatibilă cu dimensiunea EF (Deplasare > dimensiune EF), starea de procesare returnată este '**6B00**'.

— Dacă dimensiunea datelor de scris nu este compatibilă cu dimensiunea EF (Deplasare + Lc > dimensiunea EF), starea de procesare returnată este '**6700**'.

— Dacă în atributele fișierului este detectată o eroare de integritate, cardul trebuie să considere fișierul ca fiind corupt și irecuperabil, iar starea de procesare returnată este '**6400**' sau '**6500**'.

— Dacă scrierea nu este executată cu succes, starea de procesare returnată este '**6581**'.

3.5.3.1.1 Comandă cu mesagerie securizată (exemple)

Această comandă permite IFD să scrie date în EF-ul selectat în momentul respectiv, integritatea datelor primite fiind verificată de card. Întrucât nu este necesară păstrarea confidențialității, datele nu sunt criptate.

TCS_58 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'0Ch'	Mesagerie securizată solicitată
INS	1	'D6h'	Actualizare date (*Update Binary*)
P1	1	'XXh'	Deplasare octeți de la începutul fișierului: cel mai semnificativ octet
P2	1	'XXh'	Deplasare octeți de la începutul fișierului: cel mai puțin semnificativ octet
Lc	1	'XXh'	Lungimea câmpului de date securizate

Octet	Lungime	Valoare	Descriere
#6	1	'81h'	T_{PV}: etichetă pentru valoarea datelor în clar
#7	L	'NNh' sau '81 NNh'	L_{PV}: lungimea datelor transmise. L este de 2 octeți dacă L_{PV} > 127 de octeți.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Valoarea datelor în clar (date de scris)
#(7+L+NN)	1	'8Eh'	T_{CC}: etichetă pentru suma de verificare criptografică
#(8+L+NN)	1	'XXh'	L_{CC}: lungimea sumei de verificare criptografice următoare '04h' pentru mesageria securizată de generația 1 (a se vedea apendicele 11 partea A) '08h', '0Ch' sau '10h', în funcție de lungimea cheii AES pentru mesageria securizată de generația 2 (a se vedea apendicele 11 partea B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Sumă de verificare criptografică
Le	1	'00h'	Conform specificațiilor din ISO/IEC 7816-4

TCS_59 **Mesaj de răspuns dacă formatul de intrare pentru mesageria securizată este corect**

Octet	Lungime	Valoare	Descriere
#1	1	'99h'	T_{SW}: etichetă pentru cuvinte de stare (de protejat de către CC)
#2	1	'02h'	L_{SW}: lungimea cuvintelor de stare returnate
#3-#4	2	'XXXXh'	Starea de procesare a APDU de răspuns neprotejate
#5	1	'8Eh'	T_{CC}: etichetă pentru suma de verificare criptografică
#6	1	'XXh'	L_{CC}: lungimea sumei de verificare criptografice următoare '04h' pentru mesageria securizată de generația 1 (a se vedea apendicele 11 partea A) '08h', '0Ch' sau '10h', în funcție de lungimea cheii AES pentru mesageria securizată de generația 2 (a se vedea apendicele 11 partea B)
#7-#(6+L)	L	'XX..XXh'	Sumă de verificare criptografică
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

Stările de procesare „normale", descrise pentru comanda UPDATE BINARY fără mesagerie securizată (a se vedea secțiunea 3.5.3.1), pot fi returnate utilizând structura de mesaj de răspuns descrisă anterior.

În plus, pot apărea unele erori legate în mod specific de mesageria securizată. În acest caz, starea de procesare este returnată pur și simplu, fără a mai implica o structură de mesagerie securizată:

TCS_60 **Mesaj de răspuns în caz de eroare în cadrul mesageriei securizate**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— Dacă nu este disponibilă nicio cheie de sesiune curentă, se returnează starea de procesare '**6A88**'.

— Dacă unele dintre obiectele de date așteptate (conform specificațiilor de mai sus) lipsesc din formatul de mesagerie securizată, se returnează starea de procesare '**6987**': această eroare se produce dacă lipsește o etichetă așteptată sau dacă corpul comenzii nu este construit în mod corect.

— Dacă unele obiecte de date sunt incorecte, starea de procesare returnată este '**6988**': această eroare se produce dacă toate etichetele necesare sunt prezente, dar unele lungimi sunt diferite de cele așteptate.

— Dacă verificarea sumei de verificare criptografice eșuează, starea de procesare returnată este '**6688**'.

3.5.3.2 Comandă cu identificator de EF scurt

Această variantă de comandă permite IFD să selecteze un EF prin intermediul unui identificator de EF scurt și să scrie date din EF-ul respectiv.

TCS_61 Un card de tahograf trebuie să fie compatibil cu această variantă de comandă pentru toate fișierele elementare care au un identificator de EF scurt specificat. Acești identificatori de EF scurți sunt specificați în capitolul 4.

TCS_62 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'D6h'	Actualizare date (*Update Binary*)
P1	1	'XXh'	Bitul 8 este setat la 1 Biții 7 și 6 sunt setați la 00 Biții 5-1 codează identificatorul de EF scurt al EF-ului corespunzător
P2	1	'XXh'	Codează o deplasare de la 0 la 255 de octeți în EF-ul la care face trimitere P1
Lc	1	'NNh'	Lc Lungimea datelor de actualizat. Numărul de octeți de scris.
#6-#(5+NN)	NN	'XX..XXh'	Date de scris

TCS_63 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

Notă: Identificatorii de EF scurți utilizați pentru aplicația tahografică de generația 2 sunt specificați în capitolul 4.

Dacă P1 codează un identificator de EF scurt și comanda este executată cu succes, EF-ul identificat devine EF-ul selectat în momentul respectiv (EF curent).

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă fișierul corespunzător identificatorului de EF scurt nu este găsit, starea de procesare returnată este '**6A82**'.

— Dacă nu sunt îndeplinite condițiile de securitate pentru fișierul selectat, comanda este întreruptă cu '**6982**'.

— Dacă deplasarea nu este compatibilă cu dimensiunea EF (Deplasare > dimensiune EF), starea de procesare returnată este '**6B00**'.

— Dacă dimensiunea datelor de scris nu este compatibilă cu dimensiunea EF (Deplasare + Lc > dimensiunea EF), starea de procesare returnată este '**6700**'.

— Dacă în atributele fișierului este detectată o eroare de integritate, cardul trebuie să considere fișierul ca fiind corupt și irecuperabil, iar starea de procesare returnată este '**6400**' sau '**6581**'.

— Dacă scrierea nu este executată cu succes, starea de procesare returnată este '**6581**'.

3.5.3.3 Comandă cu octet de instrucțiuni impar

Această variantă de comandă permite IFD să scrie date într-un EF cu 32 768 de octeți sau mai mulți.

TCS_64 Un card de tahograf care este compatibil cu EF-uri cu 32 768 de octeți sau mai mulți trebuie să fie compatibil cu această variantă de comandă pentru EF-urile respective. Un card de tahograf poate sau nu să fie compatibil cu această variantă de comandă pentru alte EF-uri.

TCS_65 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'D7h'	Actualizare date (*Update Binary*)
P1	1	'00h'	EF curent
P2	1	'00h'	
Lc	1	'NNh'	Lc Lungimea datelor din câmpul de date al comenzii
#6-#(5+NN)	NN	'XX..XXh'	Obiect de date deplasat cu eticheta '54h' || Obiect de date discreționar cu eticheta '53h' care cuprinde datele de scris

IFD trebuie să codeze lungimea obiectului de date deplasat și a obiectului de date discreționar cu numărul minim posibil de octeți, și anume: utilizând octetul de lungime '01h', IFD trebuie să codeze o deplasare / lungime de la 0 la 255 și utilizând octetul de lungime '02h' o deplasare / lungime de la '256' până la '65 535' de octeți.

TCS_66 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă nu este selectat niciun EF, starea de procesare returnată este '**6986**'.

— Dacă nu sunt îndeplinite condițiile de securitate pentru fișierul selectat, comanda este întreruptă cu '**6982**'.

— Dacă deplasarea nu este compatibilă cu dimensiunea EF (Deplasare > dimensiune EF), starea de procesare returnată este '**6B00**'.

— Dacă dimensiunea datelor de scris nu este compatibilă cu dimensiunea EF (Deplasare + Lc > dimensiunea EF), starea de procesare returnată este '**6700**'.

— Dacă în atributele fișierului este detectată o eroare de integritate, cardul trebuie să considere fișierul ca fiind corupt și irecuperabil, iar starea de procesare returnată este '**6400**' sau '**6500**'.

— Dacă scrierea nu este executată cu succes, starea de procesare returnată este '**6581**'.

3.5.3.3.1 Comandă cu mesagerie securizată (exemplu)

Următorul exemplu ilustrează utilizarea mesageriei securizate în cazul în care se aplică condiția de securitate SM-MAC-G2.

TCS_67 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'0Ch'	Mesagerie securizată solicitată
INS	1	'D7h'	Actualizare date (*Update Binary*)
P1	1	'00h'	EF curent
P2	1	'00h'	
Lc	1	'XXh'	Lungimea câmpului de date securizate
#6	1	'B3h'	Etichetă pentru valoarea datelor în clar codate în BER-TLV
#7	L	'NNh' sau '81 NNh'	L_{PV}: lungimea datelor transmise. L este de 2 octeți dacă L_{PV} > 127 de octeți.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Date în clar codate în BER-TLV, și anume obiect de date deplasat cu eticheta '54h' || obiect de date discreționar cu eticheta '53h' care cuprinde datele de scris
#(7+L+NN)	1	'8Eh'	T_{CC}: etichetă pentru suma de verificare criptografică
#(8+L+NN)	1	'XXh'	L_{CC}: lungimea sumei de verificare criptografice următoare '08h', '0Ch' sau '10h', în funcție de lungimea cheii AES pentru mesageria securizată de generația 2 (a se vedea apendicele 11 partea B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Sumă de verificare criptografică
Le	1	'00h'	Conform specificațiilor din ISO/IEC 7816-4

TCS_68 Mesaj de răspuns în cazul în care comanda este executată cu succes

Octet	Lungime	Valoare	Descriere
#1	1	'99h'	T_{SW}: etichetă pentru cuvinte de stare (de protejat de către CC)
#2	1	'02h'	L_{SW}: lungimea cuvintelor de stare returnate
#3-#4	2	'XXXXh'	Starea de procesare a APDU de răspuns neprotejate
#5	1	'8Eh'	T_{CC}: etichetă pentru suma de verificare criptografică

Octet	Lungime	Valoare	Descriere
#6	1	'XXh'	L_{CC}: lungimea sumei de verificare criptografice următoare '08h', '0Ch' sau '10h', în funcție de lungimea cheii AES pentru mesageria securizată de generația 2 (a se vedea apendicele 11 partea B)
#7-#(6+L)	L	'XX..XXh'	Sumă de verificare criptografică
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

3.5.4 *GET CHALLENGE*

Această comandă respectă ISO/IEC 7816-4, dar are o utilizare restricționată comparativ cu comanda definită în standard.

Comanda GET CHALLENGE solicită cardului să emită date de provocare pentru a fi utilizate într-o procedură legată de securitate în cadrul căreia se transmit cardului o criptogramă sau date codificate.

TCS_69 Datele de provocare emise de card sunt valabile doar pentru următoarea comandă, care utilizează date de provocare, transmisă cardului.

TCS_70 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (Lungimea așteptată a datelor de provocare).

TCS_71 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
#1-#8	8	'XX..XXh'	Date de provocare
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă Le este diferită de '08h', starea de procesare este '**6700**'.

— Dacă parametrii P1-P2 sunt incorecți, starea de procesare este '**6A86**'.

3.5.5 *VERIFY*

Această comandă respectă ISO/IEC 7816-4, dar are o utilizare restricționată comparativ cu comanda definită în standard.

Numai cardul de atelier trebuie să fie compatibil cu această comandă.

Alte tipuri de carduri de tahograf pot sau nu să implementeze această comandă, dar pentru cardurile respective nu este personalizată nicio CHV de referință. Prin urmare, cardurile respective nu pot executa cu succes această comandă. Pentru alte tipuri de carduri de tahograf decât cardurile de atelier, comportamentul, și anume codul de eroare returnat, se află în afara domeniului de aplicare al prezentei specificații, dacă această comandă este transmisă.

Comanda „Verify” inițializează în card comparația dintre datele CHV (PIN) transmise prin comandă cu CHV de referință stocate în card.

TCS_72 PIN-ul introdus de utilizator trebuie să fie codat ASCI și completat la dreapta de către IFD cu octeți 'FFh' până la lungimea de 8 octeți; a se vedea, de asemenea, tipul de date *WorkshopCardPIN* din apendicele 1.

TCS_73 Generația 1 și 2 de aplicații tahografice trebuie să utilizeze aceleași CHV de referință.

TCS_74 Cardul de tahograf trebuie să verifice dacă comanda este corect codată. În cazul în care comanda nu este corect codată, cardul trebuie să nu compare valorile CHV, să nu scadă numărul încercărilor CHV rămase și să nu reseteze starea de securitate „PIN_Verified”, ci să anuleze comanda. O comandă este codată corect dacă octeții CLA, INS, P1, P2, Lc au valorile specificate, Le lipsește, iar câmpul de date al comenzii are lungimea corectă.

TCS_75 În cazul în care comanda este executată cu succes, numărul de încercări CHV rămase se reinițializează. Valoarea inițială a numărului de încercări CHV rămase este de 5. În cazul în care comanda este executată cu succes, cardul trebuie să seteze starea de securitate internă „PIN_Verified”. Cardul trebuie să reseteze această stare de securitate în cazul în care cardul este resetat sau în cazul în care codul CHV transmis în cadrul comenzii nu corespunde cu CHV de referință stocate.

Notă: Utilizarea acelorași CHV de referință și a unei stări de securitate globale face să nu mai fie necesar ca un angajat al atelierului să reintroducă PIN-ul după selectarea altui DF de aplicație tahografică.

TCS_76 O comparație nereușită este înregistrată în card, și anume numărul de încercări CHV rămase trebuie scăzut cu una, pentru a limita numărul încercărilor ulterioare de utilizare a CHV de referință.

TCS_77 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (CHV verificate sunt cunoscute implicit)
Lc	1	'08h'	Lungimea codului CHV transmis
#6-#13	8	'XX..XXh'	CHV

TCS_78 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă CHV de referință nu sunt găsite, starea de procesare returnată este '**6A88**'.

— Dacă CHV sunt blocate (numărul de încercări rămase pentru CHV este zero), starea de procesare returnată este '**6983**'. Odată ce se află în această stare, CHV nu mai pot fi niciodată prezentate cu succes.

— În cazul în care comparația nu reușește, numărul de încercări rămase scade și se returnează starea '**63CX**' (X>0, X fiind egal cu numărul de încercări CHV rămase.

— Dacă CHV de referință sunt considerate a fi corupte, starea de procesare returnată este '**6400**' sau '**6581**'.

— Dacă Lc este diferită de '08h', starea de procesare este '**6700**'.

3.5.6 *GET RESPONSE*

Această comandă respectă ISO/IEC 7816-4.

Această comandă (necesară și disponibilă doar pentru protocolul T=0) este utilizată pentru a transmite datele pregătite de la card către dispozitivul de interfață (cazul în care o comandă avea inclusă atât Lc, cât și Le).

Comanda GET RESPONSE trebuie emisă imediat după comanda de pregătire a datelor, altfel datele sunt pierdute. După executarea comenzii GET RESPONSE (cu excepția cazurilor în care se produce eroarea '**61xx**' sau '**6Cxx**', a se vedea mai jos), datele pregătite anterior nu mai sunt disponibile.

TCS_79 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Numărul de octeți așteptați

TCS_80 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
#1-#X	X	'XX..XXh'	Date
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă nu au fost pregătite date de către card, starea de procesare returnată este '**6900**' sau '**6F00**'.

— Dacă Le depășește numărul de octeți disponibili sau dacă Le este egală cu zero, starea de procesare returnată este '**6Cxx**', unde 'xx' reprezintă numărul exact de octeți disponibili. În acest caz, datele pregătite sunt în continuare disponibile pentru o comandă GET RESPONSE ulterioară.

— Dacă Le nu este egală cu zero, dar este mai mică decât numărul de octeți disponibili, datele solicitate sunt transmise în mod normal de către card, iar starea de procesare returnată este '**61xx**', unde 'xx' indică numărul de octeți suplimentari care sunt încă disponibili pentru o comandă GET RESPONSE ulterioară.

— În cazul în care comanda nu este compatibilă (protocol T=1), cardul returnează starea '**6D00**'.

3.5.7 *PSO: VERIFY CERTIFICATE*

Această comandă respectă ISO/IEC 7816-8, dar are o utilizare restricționată comparativ cu comanda definită în standard.

Cardul utilizează comanda VERIFY CERTIFICATE pentru a obține o cheie publică din afară și pentru a verifica valabilitatea acesteia.

3.5.7.1 Pereche de comandă – răspuns pentru generația 1

TCS_81 Această variantă de comandă este compatibilă doar cu o aplicație tahografică de generația 1.

TCS_82 În cazul în care o comandă VERIFY CERTIFICATE este executată cu succes, cheia publică este stocată pentru o utilizare ulterioară în mediul de securitate. Această cheie trebuie să fie setată în mod explicit pentru a fi utilizată de comanda MSE (a se vedea secțiunea 3.5.11) în cadrul comenzilor legate de securitate (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE sau VERIFY CERTIFICATE), folosindu-se identificatorul său de cheie.

TCS_83 În orice caz, comanda VERIFY CERTIFICATE utilizează cheia publică selectată anterior de către comanda MSE pentru a deschide certificatul. Această cheie publică trebuie să aparțină unui stat membru sau Europei.

TCS_84 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'2Ah'	Executarea unei operațiuni de securitate
P1	1	'00h'	P1
P2	1	'AEh'	P2: date necodate BER-TLV (concatenarea elementelor de date)
Lc	1	'C2h'	Lc: lungimea certificatului, 194 de octeți
#6-#199	194	'XX..XXh'	Certificat: concatenarea elementelor de date (conform descrierii din apendicele 11)

TCS_85 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă verificarea certificatului eșuează, starea de procesare returnată este '**6688**'. Procesul de verificare și de deschidere a certificatului este descris în apendicele 11 pentru G1 și G2.

— Dacă în mediul de securitate nu există nicio cheie publică, se returnează starea '**6A88**'.

— Dacă cheia publică selectată (utilizată pentru deschiderea certificatului) este considerată coruptă, starea de procesare returnată este '**6400**' sau '**6581**'.

— Doar generația 1: Dacă cheia publică selectată (utilizată pentru deschiderea certificatului) are un CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) diferit de '00' (adică nu aparține unuia dintre statele membre sau Europei), starea de procesare returnată este '**6985**'.

3.5.7.2 Pereche de comandă – răspuns pentru generația 2

În funcție de dimensiunea curbei, certificatele ECC pot fi atât de lungi încât să nu poată fi transmise într-o singură APDU. În acest caz, trebuie aplicată înlănțuirea comenzilor conform ISO/IEC 7816-4 și certificatul trebuie transmis în două APDU-uri *PSO: Verify Certificate* consecutive.

Structura certificatului și parametrii domeniului sunt definiți în apendicele 11.

TCS_86 Comanda poate fi executată în MF, în DF Tachograph și în DF Tachograph_G2; a se vedea, de asemenea, TCS_ 33.

TCS_87 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'X0h'	Octet CLA care indică înlănțuirea comenzilor: '00h' unica sau ultima comandă din lanț '10h' alte comenzi decât ultima comandă din lanț
INS	1	'2Ah'	Executarea unei operațiuni de securitate
P1	1	'00h'	
P2	1	'BEh'	Verificarea certificatului autodescriptiv
Lc	1	'XXh'	Lungimea câmpului de date al comenzii, a se vedea TCS_88 și TCS_89.
#6-#5+L	L	'XX..XXh'	Date codate DER-TLV: obiectul de date *ECC Certificate Body* ca prim obiect de date, concatenat cu obiectul de date *ECC Certificate Signature* ca al doilea obiect de date, sau o parte a acestei concatenări. Eticheta '7F21' și lungimea corespunzătoare nu se transmit. Ordinea acestor obiecte de date este fixă.

TCS_88 Pentru APDU-urile cu lungime redusă se aplică următoarele dispoziții: IFD trebuie să utilizeze numărul minim de APDU-uri necesar pentru a transmite datele utile ale comenzii și să transmită numărul maxim de octeți în prima APDU de comandă, conform valorii din octetul privind dimensiunea câmpului de informații pentru card, a se vedea TCS_14. Dacă IFD se comportă diferit, comportamentul cardului iese în afara zonei de aplicare.

TCS_89 Pentru APDU-urile cu lungime extinsă se aplică următoarele dispoziții: dacă certificatul nu se încadrează într-o singură APDU, cardul trebuie să fie compatibil cu înlănțuirea comenzilor. IFD trebuie să utilizeze numărul minim de APDU-uri necesar pentru a transmite datele utile ale comenzii și să transmită numărul maxim de octeți în prima APDU de comandă. Dacă IFD se comportă diferit, comportamentul cardului iese în afara zonei de aplicare.

Notă: Conform apendicelui 11, cardul stochează certificatul sau conținutul relevant al certificatului și își actualizează *currentAuthenticatedTime*.

Structura mesajului de răspuns și cuvintele de stare sunt cele definite în TCS_85.

TCS_90 Pe lângă codurile de eroare enumerate în TCS_85, cardul poate returna următoarele coduri de eroare:

— Dacă cheia publică selectată (utilizată pentru deschiderea certificatului) are un CHA.LSB (*CertificateHolderAuthorisation.equipmentType*) care nu este potrivit pentru verificarea certificatului în conformitate cu apendicele 11, starea de procesare returnată este '**6985**'.

— Dacă *currentAuthenticatedTime* al cardului este mai târziu decât data expirării certificatului, starea de procesare returnată este '**6985**'.

— Dacă este așteptată ultima comandă din lanț, cardul returnează starea '**6883**'.

— Dacă în câmpul de date al comenzii sunt transmiși parametri incorecți, cardul returnează starea '**6A80**' (utilizată, de asemenea, în cazul în care obiectele de date nu sunt trimise în ordinea specificată).

3.5.8 *INTERNAL AUTHENTICATE*

Această comandă respectă ISO/IEC 7816-4.

TCS_91 Toate cardurile de tahograf trebuie să fie compatibile cu această comandă în DF Tachograph de generația 1. Comanda poate sau nu să fie accesibilă în MF și/sau în DF Tachograph_G2. În acest caz, comanda se încheie cu un cod de eroare adecvat, deoarece cheia privată a cardului (*Card.SK*) pentru protocolul de autentificare de generația 1 este accesibilă numai în DF_Tachograph de generația 1.

Utilizând comanda INTERNAL AUTHENTICATE, IFD poate să autentifice cardul. Procesul de autentificare este descris în apendicele 11. Acesta include următoarele mențiuni:

TCS_92 Comanda INTERNAL AUTHENTICATE utilizează cheia privată a cardului (selectată implicit) pentru a semna datele de autentificare, inclusiv K1 (primul element pentru înțelegerea asupra cheii de sesiune) și RND1, și utilizează cheia publică selectată în momentul respectiv (prin intermediul ultimei comenzi MSE) pentru a cripta semnătura și a forma tokenul de autentificare (mai multe detalii în apendicele 11).

TCS_93 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Lungimea datelor transmise către card
#6 – #13	8	'XX..XXh'	Date de provocare utilizate pentru autentificarea cardului
#14 -#21	8	'XX..XXh'	VU.CHR (a se vedea apendicele 11)
Le	1	'80h'	Lungimea datelor așteptate de la card

TCS_94 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
#1-#128	128	'XX..XXh'	Token de autentificare a cardului (a se vedea apendicele 11)
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă în mediul de securitate nu există nicio cheie publică, starea de procesare returnată este '**6A88**'.

— Dacă în mediul de securitate nu există nicio cheie privată, starea de procesare returnată este '**6A88**'.

— Dacă VU.CHR nu corespunde identificatorului cheii publice curente, starea de procesare returnată este '**6A88**'.

— Dacă cheia privată selectată este considerată coruptă, starea de procesare returnată este '**6400**' sau '**6581**'.

TCS_95 În cazul în care comanda INTERNAL AUTHENTICATE este executată cu succes, cheia de sesiune curentă, dacă există, este ștearsă și nu mai este disponibilă. Pentru a face disponibilă o nouă cheie de sesiune, trebuie executată cu succes comanda EXTERNAL AUTHENTICATE pentru mecanismul de autentificare de generația 1.

3.5.9 *EXTERNAL AUTHENTICATE*

Această comandă respectă ISO/IEC 7816-4.

Utilizând comanda EXTERNAL AUTHENTICATE, cardul poate autentifica IFD-ul. Procesul de autentificare este descris în apendicele 11 pentru generația 1 și 2 de tahografe (autentificare VU).

TCS_96 Varianta de comandă pentru mecanismul de autentificare reciprocă de generația 1 este compatibilă numai cu o aplicație tahografică de generația 1.

TCS_97 Varianta de comandă pentru autentificarea reciprocă VU-card de a doua generație poate fi executată în MF, în DF Tachograph și în DF Tachograph_G2; a se vedea, de asemenea, TCS_34.

TCS_98 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Cheile și algoritmii cunoscuți implicit
P2	1	'00h'	
Lc	1	'XXh'	Lc (Lungimea datelor transmise către card)
#6-#(5+L)	L	'XX..XXh'	Autentificarea de generația 1: criptogramă (a se vedea apendicele 11 partea A) Autentificarea de generația 2: semnătură generată de IFD (a se vedea apendicele 11 partea B)

TCS_99 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă CHA a cheii publice setate în momentul respectiv nu este reprezentată de concatenarea AID-ului aplicației tahografice și a unui tip de echipament VU, starea de procesare returnată este '**6F00**'.

— În cazul în care comanda nu urmează imediat unei comenzi GET CHALLENGE, starea de procesare returnată este '**6985**'.

Aplicația tahografică de generația 1 poate returna următoarele coduri de eroare suplimentare:

— Dacă în mediul de securitate nu există nicio cheie publică, se returnează starea '**6A88**'.

— Dacă în mediul de securitate nu există nicio cheie privată, starea de procesare returnată este '**6A88**'.

— Dacă verificarea criptogramei este eronată, starea de procesare returnată este '**6688**'.

— Dacă cheia privată selectată este considerată coruptă, starea de procesare returnată este '**6400**' sau '**6581**'.

Varianta de comandă pentru autentificarea de generația 2 poate returna următorul cod de eroare suplimentar:

— Dacă verificarea semnăturii a eșuat, cardul returnează '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Această comandă este utilizată pentru protocolul de autentificare a cipului de generația 2 specificat în apendicele 11 partea B și este conformă cu ISO/IEC 7816-4.

TCS_100 Comanda poate fi executată în MF, în DF Tachograph și în DF Tachograph_G2; a se vedea, de asemenea, TCS_34.

TCS_101 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Protocolul și cheile cunoscute implicit
P2	1	'00h'	
Lc	1	'NNh'	Lc: lungimea câmpului de date subsecvent
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	Valoarea cheii publice efemere codate DER-TLV (a se vedea apendicele 11) VU trebuie să trimită obiectele de date în această ordine.

TCS_102 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	Date dinamice de autentificare codate DER-TLV: *nonce* și token de autentificare (a se vedea apendicele 11)
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Cardul returnează starea '**6A80**' pentru a indica existența unor parametri incorecți în câmpul de date.

— Cardul returnează starea '**6982**' în cazul în care comanda *External Authenticate* nu a fost executată cu succes.

Obiectul de răspuns cu date dinamice de autentificare '7Ch'

— trebuie să fie prezent dacă operațiunea reușește, și anume cuvintele de stare sunt '**9000**',

— trebuie să fie absent în cazul unei erori de execuție sau al unei erori de verificare, și anume în cazul în care cuvintele de stare se înscriu în intervalul '**6400**' – '**6FFF**' și

— poate fi absent în cazul unei avertizări, și anume în cazul în care cuvintele de stare se înscriu în intervalul '**6200**' – '**63FF**'.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Această comandă este utilizată pentru setarea unei chei publice pentru autentificare.

3.5.11.1 Pereche de comandă – răspuns pentru generația 1

Această comandă respectă ISO/IEC 7816-4. Utilizarea acestei comenzi este restricționată față de standardul corespunzător.

TCS_103 Această comandă este compatibilă doar cu o aplicație tahografică de generația 1.

TCS_104 Cheia identificată în câmpul de date MSE rămâne cheia publică curentă până la următoarea comandă MSE corectă, până la selectarea unui DF sau până când cardul este resetat.

TCS_105 Dacă cheia identificată nu este (deja) prezentă în card, mediul de securitate rămâne neschimbat.

TCS_106 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: cheia identificată valabilă pentru toate operațiunile criptografice
P2	1	'B6h'	P2 (date identificate privind semnătura digitală)
Lc	1	'0Ah'	Lc: lungimea câmpului de date subsecvent
#6	1	'83h'	Etichetă pentru identificarea unei chei publice în cazuri asimetrice
#7	1	'08h'	Lungimea identificatorului de cheie (identificator cheie)
#8-#15	8	'XX..XXh'	Identificator cheie conform specificațiilor din apendicele 11

TCS_107 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă cheia identificată nu este prezentă în card, starea de procesare returnată este '**6A88**'.

— Dacă unele dintre obiectele de date așteptate lipsesc din formatul de mesagerie securizată, se returnează starea de procesare '**6987**'. Acest lucru se poate întâmpla dacă lipsește eticheta '83h'.

— Dacă unele obiecte de date sunt incorecte, starea de procesare returnată este '**6988**'. Acest lucru se poate întâmpla dacă lungimea identificatorului cheii nu este '08h'.

— Dacă cheia selectată este considerată coruptă, starea de procesare returnată este '**6400**' sau '**6581**'.

3.5.11.2 Perechi de comandă – răspuns pentru generația 2

Pentru autentificarea de generația 2, cardul de tahograf este compatibil cu următoarele versiuni de comandă *MSE: Set* care respectă ISO/IEC 7816-4. Aceste versiuni de comandă nu sunt compatibile în ceea ce privește autentificarea de generația 1.

3.5.11.2.1 MSE:SET AT pentru autentificarea cipului

Următoarea comandă MSE:SET AT este utilizată pentru a selecta parametrii pentru autentificarea cipului care este efectuată de o comandă *General Authenticate* ulterioară.

TCS_108 Comanda poate fi executată în MF, în DF Tachograph și în DF Tachograph_G2; a se vedea, de asemenea, TCS_34.

TCS_109 **Mesaj de comandă MSE:SET AT pentru autentificarea cipului**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'22h'	

Octet	Lungime	Valoare	Descriere
P1	1	'41h'	Setat pentru autentificare internă
P2	1	'A4h'	Autentificare
Lc	1	'NNh'	Lc: lungimea câmpului de date subsecvent
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Identificatorul mecanismului criptografic codat DER-TLV: identificatorul de obiect al autentificării cipului (doar valoarea, eticheta '06h' este omisă). A se vedea apendicele 1 pentru valorile identificatorilor de obiect; trebuie folosită notația cu octeți. A se vedea apendicele 11 pentru îndrumări cu privire la modul de selectare a unuia dintre acești identificatori de obiect.

3.5.11.2.2 MSE:SET AT pentru autentificarea VU

Următoarea comandă MSE:SET AT este utilizată pentru a selecta parametrii și cheile pentru autentificarea VU care este efectuată de o comandă *External Authenticate* ulterioară.

TCS_110 Comanda poate fi executată în MF, în DF Tachograph și în DF Tachograph_G2; a se vedea, de asemenea, TCS_34.

TCS_111 **Mesaj de comandă MSE:SET AT pentru autentificarea VU**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Setat pentru autentificare externă
P2	1	'A4h'	Autentificare
Lc	1	'NNh'	Lc: lungimea câmpului de date subsecvent
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Identificatorul mecanismului criptografic codat DER-TLV: identificatorul de obiect al autentificării VU (doar valoarea, eticheta '06h' este omisă). A se vedea apendicele 1 pentru valorile identificatorilor de obiect; trebuie folosită notația cu octeți. A se vedea apendicele 11 pentru îndrumări cu privire la modul de selectare a unuia dintre acești identificatori de obiect.
		'83h' + '08h' + 'XX..XXh'	Identificator codat DER-TLV al cheii publice a VU de către identificatorul deținătorului certificatului menționat în certificatul aferent.
		'91h' + L_{91} + 'XX..XXh'	Reprezentare comprimată, codată DER-TLV, a cheii publice efemere a VU care va fi folosită în cursul autentificării cipului (a se vedea apendicele 11)

3.5.11.2.3 MSE:SET DST

Următoarea comandă MSE:SET DST este utilizată pentru a stabili o cheie publică fie

— pentru verificarea unei semnături care este furnizată într-o comandă *PSO: Verify Digital Signature* ulterioară, fie

— pentru verificarea semnăturii unui certificat care este furnizat într-o comandă *PSO: Verify Certificate* ulterioară.

TCS_112 Comanda poate fi executată în MF, în DF Tachograph și în DF Tachograph_G2; a se vedea, de asemenea, TCS_ 33.

TCS_113 **Mesaj de comandă MSE:SET DST**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Setat pentru verificare
P2	1	'B6h'	Semnătură digitală
Lc	1	'NNh'	Lc: lungimea câmpului de date subsecvent
#6-#(5+L)	L	'83h' + '08h' + 'XX...XXh'	Identificator codat DER-TLV al unei chei publice, și anume identificatorul deținătorului certificatului din certificatul cheii publice (a se vedea apendicele 11)

Pentru toate versiunile de comandă, structura mesajului de răspuns și cuvintele de stare sunt date de:

TCS_114 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'. Protocolul a fost selectat și inițializat.

— '**6A80**' indică existența unor parametri incorecți în câmpul de date al comenzii.

— '**6A88**' indică faptul că datele identificate (și anume o cheie identificată) nu sunt disponibile.

3.5.12 *PSO: HASH*

Această comandă este utilizată pentru a transfera pe card rezultatul unui calcul *hash* aplicat anumitor date. Această comandă este utilizată pentru verificarea semnăturilor digitale. Valoarea *hash* este stocată temporar pentru comanda ulterioară *PSO: Verify Digital Signature*

Această comandă respectă ISO/IEC 7816-8. Utilizarea acestei comenzi este restricționată față de standardul corespunzător.

Numai cardul de control trebuie să fie compatibil cu această comandă în DF Tachograph și în DF Tachograph_G2.

Alte tipuri de card de tahograf pot sau nu să implementeze această comandă. Comanda poate sau nu să fie accesibilă în MF.

Aplicația cardului de control de generația 1 este compatibilă numai cu SHA-1.

TCS_115 Valoarea *hash* stocată temporar trebuie ștearsă dacă o nouă valoare *hash* este calculată prin intermediul unei comenzi *PSO: HASH*, dacă este selectat un DF și dacă cardul de tahograf este resetat.

TCS_116 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'2Ah'	Executarea unei operațiuni de securitate
P1	1	'90h'	Returnare cod *hash*
P2	1	'A0h'	Etichetă: câmpul de date conține DO-urile relevante pentru *hashing*
Lc	1	'XXh'	Lungimea Lc a câmpului de date subsecvent
#6	1	'90h'	Etichetă pentru codul *hash*
#7	1	'XXh'	Lungimea L a codului *hash*: '14h' în aplicația de generația 1 (a se vedea apendicele 11 partea A) '20h', '30h' sau '40h' în aplicația de generația 2 (a se vedea apendicele 11 partea B)
#8-#(7+L)	L	'XX..XXh'	Cod *hash*

TCS_117 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă unele dintre obiectele de date așteptate (conform specificațiilor de mai sus) lipsesc, se returnează starea de procesare '**6987**'. Acest lucru se poate întâmpla dacă lipsește una dintre etichetele '90h'.

— Dacă unele obiecte de date sunt incorecte, starea de procesare returnată este '**6988**'. Această eroare apare dacă eticheta necesară este prezentă, dar cu o lungime diferită de '14h' pentru SHA-1, '20h' pentru SHA-256, '30h' pentru SHA-384, '40h' pentru SHA-512 (aplicația de generația 2).

3.5.13 *PERFORM HASH OF FILE*

Această comandă nu respectă ISO/IEC 7816-8. Astfel, octetul CLA al acestei comenzi indică o utilizare exclusivă a comenzii PERFORM SECURITY OPERATION / HASH.

Numai cardul de conducător auto și cardul de control trebuie să fie compatibile cu această comandă în DF Tachograph și în DF Tachograph_G2.

Alte tipuri de card de tahograf pot sau nu să implementeze această comandă. Dacă un card de societate sau de control implementează această comandă, comanda trebuie implementată conform specificațiilor din prezentul capitol.

Comanda poate sau nu să fie accesibilă în MF. În acest caz, comanda trebuie să fie implementată conform specificațiilor din prezentul capitol, și anume să nu permită calcularea unei valori *hash*, ci să se încheie cu un cod de eroare adecvat.

TCS_118 Comanda PERFORM HASH OF FILE este utilizată pentru a executa o operațiune *hash* în zona de date a EF transparent selectat în momentul respectiv.

TCS_119 Un card de tahograf trebuie să fie compatibil cu această comandă numai pentru EF-urile care sunt menționate în capitolul 4 din cadrul DF_Tachograph și DF_Tachograph_G2, cu următoarea excepție. Un card de tahograf nu trebuie să fie compatibil cu această comandă pentru EF *Sensor_Installation_Data* din DF Tachograph_G2.

TCS_120 Rezultatul operațiunii *hash* este stocat temporar în card. Ulterior, acesta poate fi utilizat pentru a obține semnătura digitală a fișierului, utilizând comanda *PSO: COMPUTE DIGITAL SIGNATURE*.

TCS_121 Valoarea *hash* de fișier stocată temporar trebuie ștearsă dacă o nouă valoare *hash* de fișier este calculată prin intermediul comenzii *PSO: Hash of File*, dacă este selectat un DF și dacă cardul de tahograf este resetat.

TCS_122 Aplicația tahografică de generația 1 trebuie să fie compatibilă cu SHA-1.

TCS_123 Aplicația tahografică de generația 2 trebuie să fie compatibilă cu SHA-1 și cu SHA-2 (256, 384 și 512 biți).

TCS_124 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'80h'	CLA
INS	1	'2Ah'	Executarea unei operațiuni de securitate
P1	1	'90h'	Etichetă: *Hash*
P2	1	'XXh'	P2: indică algoritmul care trebuie utilizat pentru *hashing*-ul datelor din fișierul transparent selectat în momentul respectiv: '00h' pentru SHA-1 '01h' pentru SHA-256 '02h' pentru SHA-384 '03h' pentru SHA-512

TCS_125 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă EF-ul curent nu permite această comandă (EF *Sensor_Installation_Data* din DF Tachograph_G2), se returnează starea de procesare '**6985**'.

— Dacă EF-ul selectat este considerat corupt (erori în atributele fișierului sau erori de integritate a datelor stocate), starea de procesare returnată este '**6400**' sau '**6581**'.

— Dacă fișierul selectat nu este un fișier transparent sau dacă nu există un EF curent, starea de procesare returnată este '**6986**'.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Această comandă este utilizată pentru calcularea semnăturii digitale a codului *hash* calculat anterior (a se vedea „PERFORM HASH OF FILE", secțiunea 3.5.13).

Numai cardul de conducător auto și cardul de control trebuie să fie compatibile cu această comandă în DF Tachograph și în DF Tachograph_G2.

Alte tipuri de carduri de tahograf pot sau nu să implementeze această comandă, dar nu trebuie să aibă o cheie de semnătură. Prin urmare, aceste carduri nu pot executa comanda cu succes, ci o încheie cu un cod de eroare adecvat.

Comanda poate sau nu să fie accesibilă în MF. În acest caz, comanda trebuie să se încheie cu un cod de eroare adecvat.

Această comandă respectă ISO/IEC 7816-8. Utilizarea acestei comenzi este restricționată față de standardul corespunzător.

TCS_126 Această comandă nu trebuie să calculeze o semnătură digitală a codului *hash* calculat anterior prin comanda *PSO: HASH*.

TCS_127 Cheia privată a cardului este utilizată pentru a calcula semnătura digitală și este cunoscută implicit de card.

TCS_128 Aplicația tahografică de generația 1 execută o semnătură digitală utilizând o metodă de completare conformă cu PKCS1 (a se vedea apendicele 11 pentru detalii).

TCS_129 Aplicația tahografică de generația 2 calculează o semnătură digitală bazată pe curbe eliptice (a se vedea apendicele 11 pentru detalii).

TCS_130 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'2Ah'	Executarea unei operațiuni de securitate
P1	1	'9Eh'	Semnătură digitală de returnat
P2	1	'9Ah'	Etichetă: câmpul de date conține date de semnat. Întrucât nu este inclus niciun câmp de date, se presupune că datele sunt deja prezente în card (*hash* de fișier)
Le	1	'NNh'	Lungimea semnăturii așteptate

TCS_131 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
#1-#L	L	'XX..XXh'	Semnătura codului *hash* calculat anterior
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă cheia privată selectată implicit este considerată coruptă, starea de procesare returnată este '**6400**' sau '**6581**'.

— În cazul în care codul *hash* care a fost calculat într-o comandă *Perform Hash of File* anterioară nu este disponibil, starea de procesare returnată este '**6985**'.

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Această comandă este utilizată pentru a verifica semnătura digitală, furnizată ca intrare, al cărui cod *hash* este cunoscut de card. Algoritmul semnăturii este cunoscut implicit de card.

Această comandă respectă ISO/IEC 7816-8. Utilizarea acestei comenzi este restricționată față de standardul corespunzător.

Numai cardul de control trebuie să fie compatibil cu această comandă în DF Tachograph și în DF Tachograph_G2.

Alte tipuri de card de tahograf pot sau nu să implementeze această comandă. Comanda poate sau nu să fie accesibilă în MF.

TCS_132 Comanda VERIFY DIGITAL SIGNATURE utilizează întotdeauna cheia publică selectată de comanda anterioară *Manage Security Environment MSE: Set DST* și codul *hash* anterior introdus de o comandă *PSO: HASH*.

TCS_133 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'2Ah'	Executarea unei operațiuni de securitate
P1	1	'00h'	
P2	1	'A8h'	Etichetă: câmpul de date conține DO-urile relevante pentru verificare
Lc	1	'83h'	Lungimea Lc a câmpului de date subsecvent
6	1	'9Eh'	Etichetă pentru semnătura digitală
#7-#8	2	'81 XXh'	Lungimea semnăturii digitale: 128 de octeți codați în conformitate cu apendicele 11 partea A pentru aplicația tahografică de generația 1 În funcție de curba aleasă pentru aplicația tahografică de generația 2 (a se vedea apendicele 11 partea B)
#9-#(8+L)	L	'XX..XXh'	Conținutul semnăturii digitale

TCS_134 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— Dacă verificarea semnăturii eșuează, starea de procesare returnată este '**6688**'. Procesul de verificare este descris în apendicele 11.

— Dacă nu este selectată nicio cheie publică, starea de procesare returnată este '**6A88**'.

— Dacă unele dintre obiectele de date așteptate (conform specificațiilor de mai sus) lipsesc, se returnează starea de procesare '**6987**'. Acest lucru se poate întâmpla dacă una dintre etichetele necesare lipsește.

— Dacă nu este disponibil niciun cod *hash* pentru procesarea comenzii (ca urmare a unei comenzi *PSO: Hash* anterioare), starea de procesare returnată este '**6985**'.

— Dacă unele obiecte de date sunt incorecte, starea de procesare returnată este '**6988**'. Acest lucru se poate întâmpla dacă lungimea unuia dintre obiectele de date necesare este incorectă.

— Dacă cheia publică selectată este considerată coruptă, starea de procesare returnată este '**6400**' sau '**6581**'.

3.5.16 *PROCESS DSRC MESSAGE*

Această comandă este utilizată pentru a verifica integritatea și autenticitatea mesajului DSRC și pentru a descifra datele comunicate de o VU unei autorități de control sau unui atelier prin legătura DSRC. Cardul obține cheia de criptare și cheia MAC folosite pentru a securiza mesajul DSRC conform descrierii din apendicele 11 partea B capitolul 13.

Numai cardul de control și cardul de atelier trebuie să fie compatibile cu această comandă în DF Tachograph_G2.

Alte tipuri de carduri de tahograf pot sau nu să implementeze această comandă, dar nu trebuie să aibă o cheie *master* DSRC. Prin urmare, aceste carduri nu pot executa comanda cu succes, ci o încheie cu un cod de eroare adecvat.

Comanda poate sau nu să fie accesibilă în MF și/sau în DF Tachograph. În acest caz, comanda trebuie să se încheie cu un cod de eroare adecvat.

TCS_135 Cheia *master* DSRC este accesibilă numai în DF Tachograph_G2, și anume cardul de control și cardul de atelier trebuie să permită executarea cu succes a comenzii doar în DF Tachograph_G2.

TCS_136 Comanda decriptează doar datele DSRC și verifică suma de verificare criptografică, dar fără a interpreta datele de intrare.

TCS_137 Ordinea obiectelor de date din câmpul de date al comenzii este fixată de prezenta specificație.

TCS_138 **Mesaj de comandă**

Octet	Lungime	Valoare	Descriere
CLA	1	'80h'	CLA exclusiv
INS	1	'2Ah'	Executarea unei operațiuni de securitate
P1	1	'80h'	Date de răspuns: valoare a datelor în clar
P2	1	'B0h'	Date de comandă: valoare a datelor în clar codată BER-TLV și incluzând DO-uri SM
Lc	1	'NNh'	Lungimea Lc a câmpului de date subsecvent
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	Octet indicator de conținut de completare codat DER-TLV, urmat de datele utile de tahograf criptate. Pentru octetul indicator de conținut de completare trebuie folosită valoarea '00h' („nicio altă indicație" în conformitate cu tabelul 52 din ISO/IEC 7816-4:2013). Pentru mecanismul de criptare, a se vedea apendicele 11 partea B capitolul 13. Valorile permise pentru lungimea L_{87} sunt multiplii lungimii de bloc AES plus 1 pentru octetul indicator de conținut de completare, adică de la 17 octeți până la 193 de octeți, inclusiv. *Notă:* a se vedea tabelul 49 din ISO/IEC 7816-4:2013 pentru obiectul de date SM cu eticheta '87h'.
		'81h' + '10h'	Model de referință de control pentru confidențialitate, codat DER-TLV, care găzduiește concatenarea următoarelor elemente de date (a se vedea apendicele 1, *DSRCSecurityData*, și apendicele 11 partea B capitolul 13): — marcă temporală – 4 octeți — contor – 3 octeți — numărul de serie al VU – 8 octeți — versiunea cheii *master* DSRC – 1 octet *Notă:* a se vedea tabelul 49 din ISO/IEC 7816-4:2013 pentru obiectul de date SM cu eticheta '81h'.
		'8Eh' + L_{8E} + 'XX..XXh'	MAC codat DER-TLV prin mesajul DSRC. Pentru calcularea și algoritmul MAC, a se vedea apendicele 11 partea B capitolul 13. *Notă:* a se vedea tabelul 49 din ISO/IEC 7816-4:2013 pentru obiectul de date SM cu eticheta '8Eh'.

TCS_139 **Mesaj de răspuns**

Octet	Lungime	Valoare	Descriere
#1-#L	L	'XX..XXh'	Lipsește (în cazul unei erori) sau date descifrate (completare eliminată)
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, cardul returnează starea '**9000**'.

— '**6A80**' indică existența unor parametri incorecți în câmpul de date al comenzii (utilizat, de asemenea, în cazul în care obiectele de date nu sunt trimise în ordinea specificată).

— '**6A88**' indică faptul că datele menționate nu sunt disponibile, și anume cheia *master* DSRC identificată nu este disponibilă.

— '**6900**' indică faptul că verificarea sumei de verificare criptografice sau decriptarea datelor a eșuat.

4. STRUCTURA CARDURILOR DE TAHOGRAF

Prezenta secțiune specifică structurile de fișiere ale cardurilor de tahograf pentru stocarea datelor accesibile.

Ea nu specifică structurile interne care depind de producătorul cardului, precum anteturile fișierelor, nici stocarea și procesarea elementelor de date necesare doar pentru uz intern, precum `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` sau `WorkshopCardPin`.

TCS_140 Un card de tahograf de generația 2 trebuie să cuprindă fișierul *master* MF și o aplicație tahografică de generația 1 și una de generația 2 de același tip (de exemplu, aplicațiile cardului de conducător auto).

TCS_141 Un card de tahograf trebuie să fie compatibil cel puțin cu numărul minim de înregistrări specificat pentru aplicațiile corespondente și trebuie să nu permită mai multe înregistrări decât numărul maxim de înregistrări specificat pentru aplicațiile corespondente.

Numărul minim și numărul maxim de înregistrări pentru diferitele aplicații sunt specificate în prezentul capitol.

Pentru condițiile de securitate utilizate în cadrul normelor de acces pe parcursul prezentului capitol, a se consulta capitolul 3.3. În general, modul de acces „read" denotă comanda READ BINARY cu octet INS par și, dacă este compatibil, impar, cu excepția EF *Sensor_Installation_Data* din cardul de atelier, a se vedea TCS_156 și TCS_160. Modul de acces „update" denotă comanda UPDATE BINARY cu octet INS par și, dacă este compatibil, impar, iar modul de acces „select" denotă comanda SELECT.

4.1. Fișier *master* MF

TCS_142 După personalizarea sa, fișierul *master* MF trebuie să aibă următoarea structură permanentă a fișierelor și următoarele norme de accesare a fișierelor:

Notă: identificatorul de EF scurt SFID este dat ca număr zecimal, de exemplu valoarea 30 corespunde lui 11110 în cod binar.

			Norme de acces	
Fișier	**ID fișier**	**SFID**	***Read / Select***	***Update***
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (în anumite condi□ii)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (în anumite condi□ii)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

În acest tabel este folosită următoarea abreviere pentru condiția de securitate:

SC1 ALW SAU SM-MAC-G2

TCS_143 Structura tuturor EF trebuie să fie transparentă.

TCS_144 Fișierul *master* MF trebuie să aibă următoarea structură de date:

Fișier / element de date	Nr. de înregistrări	Dimensiune (octeți) Min	Max	Valori implicite
MF		*63*	*184*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
EF DIR		*20*	*20*	
A se vedea TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
A se vedea TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
A se vedea TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Fișierul elementar EF DIR trebuie să conțină următoarele obiecte de date legate de aplicații: '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'

TCS_146 Fișierul elementar EF ATR/INFO trebuie să fie prezent în cazul în care cardul de tahograf indică, în ATR-ul său, că este compatibil cu câmpuri cu lungime extinsă. În acest caz, EF ATR/INFO conține obiectul de date informativ cu lungime extinsă (DO'7F66'), conform specificațiilor din ISO/IEC 7816-4:2013, clauza 12.7.1.

TCS_147 Fișierul elementar EF *Extended_Length* trebuie să fie prezent în cazul în care cardul de tahograf indică, în ATR-ul său, că este compatibil cu câmpuri cu lungime extinsă. În acest caz, EF-ul trebuie să conțină următorul obiect de date: '02 01 xx', unde valoarea 'xx' indică dacă câmpurile cu lungime extinsă sunt compatibile cu protocolul T = 1 și / sau T = 0.

Valoarea '01' arată compatibilitatea câmpului cu lungime extinsă cu protocolul T = 1.

Valoarea '10' arată compatibilitatea câmpului cu lungime extinsă cu protocolul T = 0.

Valoarea '11' arată compatibilitatea câmpului cu lungime extinsă cu protocolul T = 1 și cu protocolul T = 0.

4.2. Aplicații de card de conducător auto

4.2.1 *Aplicația de card de conducător auto de generația 1*

TCS_148 După personalizarea sa, aplicația de card de conducător auto de generația 1 trebuie să aibă următoarea structură permanentă a fișierelor și următoarele norme de accesare a fișierelor:

		Norme de acces		
Fișier	**ID Fișier**	***Read***	***Select***	***Update***
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'050Eh'	SC2	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

În acest tabel sunt folosite următoarele abrevieri pentru condițiile de securitate:

SC1 ALW SAU SM-MAC-G2

SC2 ALW SAU SM-MAC-G1 SAU SM-MAC-G2

SC3 SM-MAC-G1 SAU SM-MAC-G2

TCS_149 Structura tuturor EF trebuie să fie transparentă.

TCS_150 Aplicația de card de conducător auto de generația 1 trebuie să aibă următoarea structură de date:

Fișier / element de date	Nr. de înregistrări	Dimensiune (octeți) Min	Max	Valori implicite
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
└CardVehiclesUsed		*2606*	*6202*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*2604*	*6200*	
└─CardVehicleRecord	n_3	*31*	*31*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
└CardPlaceDailyWorkPeriod		*841*	*1121*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*840*	*1120*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
└SpecificConditionRecord	56	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_151 Următoarele valori, utilizate pentru a specifica dimensiuni în tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului de conducător auto trebuie să le utilizeze pentru o aplicație de generația 1:

		Min	**Max**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 de octeți (28 de zile * 93 de modificări de activitate)	13 776 de octeți (28 de zile * 240 de modificări de activitate)

4.2.2 *Aplicația de card de conducător auto de generația 2*

TCS_152 După personalizarea sa, aplicația de card de conducător auto de generația 2 trebuie să aibă următoarea structură permanentă a fișierelor și următoarele norme de accesare a fișierelor.

Notă: identificatorul de EF scurt SFID este dat ca număr zecimal, de exemplu valoarea 30 corespunde lui 11110 în cod binar.

			Norme de acces	
Fișier	**ID fișier**	**SFID**	***Read / Select***	***Update***
└─ DF Tachograph_G2			SC1	
├─ EF Application_Identification	'0501h'	1	SC1	NEV
├─ EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─ EF CardSignCertificate	'C101h'	3	SC1	NEV
├─ EF CA_Certificate	'C108h'	4	SC1	NEV
├─ EF Link_Certificate	'C109h'	5	SC1	NEV
├─ EF Identification	'0520h'	6	SC1	NEV
├─ EF Card_Download	'050Eh'	7	SC1	SC1
├─ EF Driving_Licence_Info	'0521h'	10	SC1	NEV
├─ EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
├─ EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
├─ EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
├─ EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
├─ EF Places	'0506h'	16	SC1	SM-MAC-G2
├─ EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
├─ EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
├─ EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
├─ EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
└─ EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

În acest tabel este folosită următoarea abreviere pentru condiția de securitate:

SC1 ALW SAU SM-MAC-G2

TCS_153 Structura tuturor EF trebuie să fie transparentă.

TCS_154 Aplicația de card de conducător auto de generația 2 trebuie să aibă următoarea structură de date:

Fișier / element de date	Nr. de înregistrări	Dimensiune (octeți) Min	Max	Valori implicite
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
CardVehiclesUsed		*4034*	*9602*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*4032*	*9600*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
CardPlaceDailyWorkPeriod		*1766*	*2354*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		*1764*	*2352*	
PlaceRecord	n_4	*21*	*21*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Următoarele valori, utilizate pentru a specifica dimensiuni în tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului de conducător auto trebuie să le utilizeze pentru o aplicație de generația 2:

		Min	**Max**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 de octeți (28 de zile * 93 de modificări de activitate)	13 776 de octeți (28 de zile * 240 de modificări de activitate)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. Aplicații de card de atelier

4.3.1 *Aplicația de card de atelier de generația 1*

TCS_156 După personalizarea sa, aplicația de card de atelier de generația 1 trebuie să aibă următoarea structură permanentă a fișierelor și următoarele norme de accesare a fișierelor:

		Norme de acces		
Fișier	**ID Fișier**	***Read***	***Select***	***Update***
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	SC2	SC1	NEV
├EF Card_Download	'0509h'	SC2	SC1	**SC1**
├EF Calibration	'050Ah'	SC2	SC1	SC3
├EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	NEV
├EF Events_Data	'0502h'	SC2	SC1	SC3
├EF Faults_Data	'0503h'	SC2	SC1	SC3
├EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├EF Places	'0506h'	SC2	SC1	SC3
├EF Current_Usage	'0507h'	SC2	SC1	SC3
├EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└EF Specific_Conditions	'0522h'	SC2	SC1	SC3

În acest tabel sunt folosite următoarele abrevieri pentru condițiile de securitate:

SC1 ALW SAU SM-MAC-G2

SC2 ALW SAU SM-MAC-G1 SAU SM-MAC-G2

SC3 SM-MAC-G1 SAU SM-MAC-G2

SC4 Pentru comanda READ BINARY cu octet INS par:

(PLAIN-C ȘI SM-R-ENC-G1) SAU (SM-C-MAC-G1 ȘI SM-R-ENC-MAC-G1) SAU

(SM-C-MAC-G2 ȘI SM-R-ENC-MAC-G2)

Pentru comanda READ BINARY cu octet INS impar (dacă este compatibil): NEV

TCS_157 Structura tuturor EF trebuie să fie transparentă.

TCS_158 Aplicația de card de atelier de generația 1 trebuie să aibă următoarea structură de date:

Fișier / element de date	Nr. de înregistrări	Dimensiune (octeți) Min	Dimensiune (octeți) Max	Valori implicite
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

EF Sensor_Installation_Data		*16*	*16*	
└SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
└CardEventData		*432*	*432*	
└cardEventRecords	6	*72*	*72*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└CardFaultData		*288*	*288*	
└cardFaultRecords	2	*144*	*144*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└CardDriverActivity		*202*	*496*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
└CardVehiclesUsed		*126*	*250*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*124*	*248*	
└CardVehicleRecord	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
└vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
└CardPlaceDailyWorkPeriod		*61*	*81*	
├placePointerNewestRecord		1	1	{00}
└placeRecords		*60*	*80*	
└PlaceRecord	n_4	*10*	*10*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
└vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Următoarele valori, utilizate pentru a specifica dimensiuni în tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului de atelier trebuie să le utilizeze pentru o aplicație de generația 1:

		Min	**Max**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 de octeți (1 zi * 93 de modificări de activitate)	492 de octeți (1 zi * 240 de modificări de activitate)

4.3.2 *Aplicația de card de atelier de generația 2*

TCS_160 După personalizarea sa, aplicația de card de atelier de generația 2 trebuie să aibă următoarea structură permanentă a fișierelor și următoarele norme de accesare a fișierelor.

Notă: identificatorul de EF scurt SFID este dat ca număr zecimal, de exemplu valoarea 30 corespunde lui 11110 în cod binar.

			Norme de acces		
Fișier	**ID Fișier**	**SFID**	***Read***	***Select***	***Update***
└─DF Tachograph_G2			SC1	SC1	
├─EF Application_Identification	'0501h'	1	SC1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
├─EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
├─EF Identification	'0520h'	6	SC1	SC1	NEV
├─EF Card_Download	'0509h'	7	SC1	SC1	SC1
├─EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
├─EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-G2	NEV
├─EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
├─EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
├─EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
├─EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
├─EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
├─EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
└─EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

În acest tabel sunt folosite următoarele abrevieri pentru condițiile de securitate:

SC1 ALW SAU SM-MAC-G2

SC5 Pentru comanda READ BINARY cu octet INS par: SM-C-MAC-G2 ȘI SM-R-ENC-MAC-G2

Pentru comanda READ BINARY cu octet INS impar (dacă este compatibil): NEV

TCS_161 Structura tuturor EF trebuie să fie transparentă.

TCS_162 Aplicația de card de atelier de generația 2 trebuie să aibă următoarea structură de date:

Fișier / element de date	Nr. de înregistrări	Dimensiune (octeți) Min	Max	Valori implicite
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

├─oldTimeValue		4	4	{00..00}
├─newTimeValue		4	4	{00..00}
├─nextCalibrationDate		4	4	{00..00}
├─vuPartNumber		16	16	{20..20}
├─vuSerialNumber		8	8	{00..00}
├─sensorSerialNumber		8	8	{00..00}
├─sensorGNSSSerialNumber		8	8	{00..00}
├─rcmSerialNumber		8	8	{00..00}
├─vuAbility		1	1	{00}
└─sealDataCard		46	46	
├─noOfSealRecords		1	1	{00}
└─SealRecords		45	45	
└─SealRecord	5	9	9	
├─equipmentType		1	1	{00}
└─extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
└─SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
└─CardEventData		*792*	*792*	
└─cardEventRecords	11	*72*	*72*	
└─CardEventRecord	n_1	*24*	*24*	
├─eventType		1	1	{00}
├─eventBeginTime		4	4	{00..00}
├─eventEndTime		4	4	{00..00}
└─eventVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└─CardFaultData		*288*	*288*	
└─cardFaultRecords	2	*144*	*144*	
└─CardFaultRecord	n_2	*24*	*24*	
├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└─CardDriverActivity		*202*	*496*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
└─CardVehiclesUsed		*194*	*386*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*192*	*384*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

TCS_163 Următoarele valori, utilizate pentru a specifica dimensiuni în tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului de atelier trebuie să le utilizeze pentru o aplicație de generația 2:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 de octeți (1 zi * 93 de modificări de activitate)	492 de octeți (1 zi * 240 de modificări de activitate)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Aplicații de card de control

4.4.1 *Aplicația de card de control de generația 1*

TCS_164 După personalizarea sa, aplicația de card de control de generația 1 trebuie să aibă următoarea structură permanentă a fișierelor și următoarele norme de accesare a fișierelor:

		Norme de acces		
Fișier	**ID Fișier**	***Read***	***Select***	***Update***
└DF Tachograph	'0500h'			
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

În acest tabel sunt folosite următoarele abrevieri pentru condițiile de securitate:

SC1 ALW SAU SM-MAC-G2

SC2 ALW SAU SM-MAC-G1 SAU SM-MAC-G2

SC3 SM-MAC-G1 SAU SM-MAC-G2

SC6 EXT-AUT-G1 SAU SM-MAC-G1 SAU SM-MAC-G2

TCS_165 Structura tuturor EF trebuie să fie transparentă.

TCS_166 Aplicația de card de control de generația 1 trebuie să aibă următoarea structură de date:

Fișier / element de date	Nr. de înregistrări	Dimensiune (octeți) Min	Max	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Următoarele valori, utilizate pentru a specifica dimensiuni în tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului de control trebuie să le utilizeze pentru o aplicație de generația 1:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Aplicația de card de control de generația 2*

TCS_168 După personalizarea sa, aplicația de card de control de generația 2 trebuie să aibă următoarea structură permanentă a fișierelor și următoarele norme de accesare a fișierelor.

Notă: identificatorul de EF scurt SFID este dat ca număr zecimal, de exemplu valoarea 30 corespunde lui 11110 în cod binar.

			Norme de acces	
Fișier	**ID Fișier**	**SFID**	***Read / Select***	***Update***
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	‘0501h’	1	SC1	NEV
├─EF CardMA_Certificate	‘C100h’	2	SC1	NEV
├─EF CA_Certificate	‘C108h’	4	SC1	NEV
├─EF Link_Certificate	‘C109h’	5	SC1	NEV
├─EF Identification	‘0520h’	6	SC1	NEV
└─EF Controller_Activity_Data	‘050Ch’	14	SC1	SM-MAC-G2

În acest tabel este folosită următoarea abreviere pentru condiția de securitate:

SC1 ALW SAU SM-MAC-G2

TCS_169 Structura tuturor EF trebuie să fie transparentă.

TCS_170 Aplicația de card de control de generația 2 trebuie să aibă următoarea structură de date:

Fișier / element de date	Nr. de înregistrări	Dimensiune (octeți) Min	Max	
DF Tachograph_G2		*11410*	*25161*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Următoarele valori, utilizate pentru a specifica dimensiuni în tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului de control trebuie să le utilizeze pentru o aplicație de generația 2:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.5. Aplicații de card de societate

4.5.1 *Aplicația de card de societate de generația 1*

TCS_172 După personalizarea sa, aplicația de card de societate de generația 1 trebuie să aibă următoarea structură permanentă a fișierelor și următoarele norme de accesare a fișierelor:

		Norme de acces		
Fișier	**ID Fișier**	***Read***	***Select***	***Update***
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

În acest tabel sunt folosite următoarele abrevieri pentru condițiile de securitate:

SC1 ALW SAU SM-MAC-G2

SC2 ALW SAU SM-MAC-G1 SAU SM-MAC-G2

SC3 SM-MAC-G1 SAU SM-MAC-G2

SC6 EXT-AUT-G1 SAU SM-MAC-G1 SAU SM-MAC-G2

TCS_173 Structura tuturor EF trebuie să fie transparentă.

TCS_174 Aplicația de card de societate de generația 1 trebuie să aibă următoarea structură de date:

Fișier / element de date	**Nr. de înregistrări**	**Dimensiune (octeți) Min**	**Max**	**Valori implicite**
└DF Tachograph		*11114*	*24454*	
├EF Application_Identification		*5*	*5*	
│└CompanyCardApplicationIdentification		*5*	*5*	
│├typeOfTachographCardId		1	1	{00}
│├cardStructureVersion		2	2	{00 00}
│└noOfCompanyActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
│└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
│└MemberStateCertificate		194	194	{00..00}
├EF Identification		*139*	*139*	
│├CardIdentification		*65*	*65*	
││├cardIssuingMemberState		1	1	{00}
││├cardNumber		16	16	{20..20}
││├cardIssuingAuthorityName		36	36	{00, 20..20}
││├cardIssueDate		4	4	{00..00}
││├cardValidityBegin		4	4	{00..00}
││└cardExpiryDate		4	4	{00..00}
│└CompanyCardHolderIdentification		*74*	*74*	
│├companyName		36	36	{00, 20..20}
│├companyAddress		36	36	{00, 20..20}
│└cardHolderPreferredLanguage		2	2	{20 20}
└EF Company_Activity_Data		*10582*	*23922*	
└CompanyActivityData		*10582*	*23922*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*23920*	
└companyActivityRecord	n_8	*46*	*46*	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├downloadPeriodBegin		4	4	{00..00}
└downloadPeriodEnd		4	4	{00..00}

TCS_175 Următoarele valori, utilizate pentru a specifica dimensiuni în tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului de societate trebuie să le utilizeze pentru o aplicație de generația 1:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Aplicația de card de societate de generația 2*

TCS_176 După personalizarea sa, aplicația de card de societate de generația 2 trebuie să aibă următoarea structură permanentă a fișierelor și următoarele norme de accesare a fișierelor.

Notă: identificatorul de EF scurt SFID este dat ca număr zecimal, de exemplu valoarea 30 corespunde lui 11110 în cod binar.

			Norme de acces	
Fișier	**ID Fișier**	**SFID**	***Read / Select***	***Update***
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

În acest tabel este folosită următoarea abreviere pentru condiția de securitate:

SC1 ALW SAU SM-MAC-G2

TCS_177 Structura tuturor EF trebuie să fie transparentă.

TCS_178 Aplicația de card de societate de generația 2 trebuie să aibă următoarea structură de date:

Fișier / element de date	Nr. de înregistrări	Dimensiune (octeți) Min	Max	Valori implicite
DF Tachograph_G2		*11338*	*25089*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_179 Următoarele valori, utilizate pentru a specifica dimensiuni în tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului de societate trebuie să le utilizeze pentru o aplicație de generația 2:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

Apendicele 3

PICTOGRAME

PIC_001 Tahograful poate folosi opțional următoarele pictograme și combinații de pictograme (sau pictograme și combinații suficient de asemănătoare pentru a fi clar identificabile cu acestea):

1. PICTOGRAME DE BAZĂ

	Persoane	**Acțiuni**	**Moduri de funcționare**
	Societate		Mod societate
	Agent de control	Control	Mod de control
	Conducător auto	Conducere	Mod operațional
	Atelier/stație de testare	Inspecție/etalonare	Mod calibrare
	Producător		
	Activități	**Durată**	
	Disponibil	Perioada de disponibilitate curentă	
	Conducere	Timp de conducere continuă	
	Odihnă	Perioada de odihnă curentă	
	Alte activități	Ziua de lucru curentă	
	Pauză	Durata cumulată a pauzelor	
	Necunoscută		
	Echipament	**Funcții**	
1	Slot pentru cardul de conducător auto		
2	Slot pentru cardul copilotului		
	Card		
	Ceas		
	Afișaj	Afișare	
	Stocare externă	Descărcare	
	Sursă de alimentare (electrică)		
	Imprimantă/document imprimat	Imprimare	
	Senzor		
	Dimensiunea pneurilor		
	Vehicul/unitate montată pe vehicul		
	Echipament GNSS		
	Echipament de detectare la distanță		
	Interfață ITS		
	Condiții specifice		
OUT	În afara zonei de aplicare a reglementărilor		
	Traversare cu feribotul sau cu trenul		

Diverse

!	Evenimente	✕	Anomalii
▮▶	Începutul zilei de lucru	▶▮	Sfârșitul zilei de lucru
●	Loc		
M	Introducere manuală a activităților conducătorului auto		
🔒	Securitate		
>	Viteză		
🕒	Oră		
Σ	Total/rezumat		

Calificative

24h	Zilnic
I	Săptămânal
II	Două săptămâni
+	De la sau până la

2. COMBINAȚII DE PICTOGRAME

Diverse

🏛●	Locul controlului		
●▮▶	Loc de începere a zilei de lucru	▶▮●	Loc de încheiere a zilei de lucru
🕒+	De la ora	+🕒	Până la ora
🚗+	De la vehicul		
OUT+	În afara zonei de aplicare a reglementărilor, început	+OUT	În afara zonei de aplicare a reglementărilor, sfârșit

Carduri

🪪	Card de conducător auto
🏢	Card de societate
🏛	Card de control
🔧	Card de atelier
----	Niciun card

Conducere

🪪🪪	Conducere în echipaj
🪪 I	Timp de conducere pentru o săptămână
🪪 II	Timp de conducere pentru două săptămâni

Documente imprimate

24h 🖨	Document imprimat zilnic privind activitățile conducătorului auto extrase de pe card
24h 🚗🖨	Document imprimat zilnic privind activităților conducătorului auto extrase din VU
! ✕ 🖨	Document imprimat privind evenimentele și anomaliile de pe card
! ✕ 🚗🖨	Document imprimat privind evenimentele și anomaliile din VU
🔧🕒🖨	Document imprimat privind datele tehnice
>>🖨	Document imprimat privind depășirea limitei de viteză

Evenimente

	Introducerea unui card nevalabil
	Conflict de carduri
	Suprapunere a timpului
	Conducere fără un card corespunzător
	Introducerea cardului în timpul conducerii
	Încheiere incorectă a ultimei sesiuni de utilizare a cardului
	Depășire a limitei de viteză
	Întrerupere a alimentării cu energie electrică
	Eroare privind datele de la senzorul de mișcare
	Conflict privind deplasarea vehiculului
	Încălcare a securității
	Reglarea orei (de către atelier)
	Control pentru depășirea limitei de viteză

Anomalii

	Anomalie a cardului (slot pentru cardul de conducător auto)
	Anomalie a cardului (slot pentru cardul copilotului)
	Anomalie a afișajului
	Anomalie la descărcare
	Anomalie a imprimantei
	Anomalie a senzorului
	Anomalie internă a VU
	Anomalie a GNSS
	Anomalie privind detectarea la distanță

Procedură privind introducerea manuală a datelor

	Aceeași zi de lucru în curs?
	Sfârșitul zilei de lucru anterioare?
	Confirmați sau introduceți locul de încheiere a zilei de lucru
	Introduceți ora de pornire
	Introduceți locul de începere a zilei de lucru.

Notă: În apendicele 4 sunt definite combinații suplimentare de pictograme, pentru formarea de blocuri de imprimare sau de identificatori de înregistrare.

Apendicele 4

DOCUMENTE IMPRIMATE

CUPRINS

1. GENERALITĂȚI 243
2. SPECIFICAȚII PRIVIND BLOCURILE DE DATE 243
3. SPECIFICAȚII REFERITOARE LA DOCUMENTELE IMPRIMATE 250
3.1. Document imprimat zilnic privind activitățile conducătorului auto extrase de pe card 250
3.2. Document imprimat zilnic privind activităților conducătorului auto extrase din VU 251
3.3. Document imprimat privind evenimentele și anomaliile de pe card 252
3.4. Document imprimat privind evenimentele și anomaliile din VU 252
3.5. Document imprimat privind datele tehnice 253
3.6. Document imprimat privind depășirea limitei de viteză 253
3.7. Istoricul introducerii cardurilor 254

1. GENERALITĂȚI

Fiecare document imprimat este construit prin înlănțuirea a diverse blocuri de date, identificate, dacă este cazul, prin intermediul unui identificator de bloc.

Un bloc de date conține una sau mai multe înregistrări, identificate, dacă este cazul, cu un identificator de înregistrare.

PRT_001 Când un identificator de înregistrare urmează imediat după un identificator de bloc, identificatorul de înregistrare nu este imprimat.

PRT_002 În cazul în care un element de date este necunoscut sau nu trebuie imprimat din motive legate de drepturile de acces la date, în locul acestuia se imprimă spații.

PRT_003 Dacă întregul conținut al unui rând este necunoscut sau nu trebuie imprimat, se omite întregul rând.

PRT_004 La imprimare, câmpurile de date numerice sunt aliniate la dreapta, cu un spațiu de separare pentru mii și milioane și fără zerouri la început.

PRT_005 La imprimare, câmpurile de date constituite din șiruri de caractere sunt aliniate la stânga și completate cu spații până la lungimea elementului de date sau trunchiate la lungimea elementului de date, atunci când este necesar (nume și adrese).

PRT_006 În cazul trecerii la un nou rând din cauza lungimii textului, la începutul noului rând ar trebui imprimat un caracter special (un punct la jumătatea înălțimii rândului, „•”).

2. SPECIFICAȚII PRIVIND BLOCURILE DE DATE

În acest capitol sunt utilizate următoarele notații convenționale pentru formatare:

— caracterele **aldine** indică faptul că trebuie imprimat un text în clar (textul se imprimă cu caractere normale);

— caracterele normale reprezintă variabile (pictograme sau date) care trebuie înlocuite cu valorile lor în scopul imprimării;

— denumirile variabilelor au fost completate cu liniuțe de subliniere pentru a ilustra lungimea elementului de date disponibil pentru variabila în cauză;

— datele sunt specificate în formatul „zz/ll/aaaa” (zi, lună, an). Se poate utiliza, de asemenea, formatul „zz.ll.aaaa”;

— termenul „identificarea cardului” reprezintă combinația dintre: tipul de card, reprezentat printr-o combinație de pictograme de card, codul statului membru care a emis cardul, o bară oblică orientată spre dreapta și numărul cardului cu indexul de înlocuire și indexul de reînnoire separate de un spațiu:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Combinații de pictograme de card		Codul statului membru emitent				Primele 14 caractere din numărul cardului (care includ, eventual, un indice secvențial)														Indice de înlocuire		Indice de reînnoire

PRT_007 Documentele imprimate utilizează următoarele blocuri de date și/sau înregistrări de date, în conformitate cu următoarele semnificații și formate:

Numărul blocului sau al înregistrării Sens	Data Format
1 ***Data și ora imprimării documentului***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Tipul documentului imprimat*** Identificator de bloc Combinația de pictograme din documentul imprimat (a se vedea apendicele 3), reglajul limitatorului de viteză (imprimare numai în caz de depășire a vitezei)	----------▼---------- Picto xxx **km/h**
3 ***Identificarea titularului cardului*** Identificator de bloc P= pictogramă „persoane” Numele titularului cardului Prenumele titularului (dacă este cazul) Identificarea cardului Data expirării cardului (dacă este cazul) și numărul generației cardului (GEN 1 sau GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

În cazul în care cardul este un card nenominal, pe care nu figurează niciun nume de titular, în locul acestuia se imprimă denumirea societății, a atelierului sau a organismului de control.

(*) Numărul generației cardului poate fi imprimat numai de tahograful inteligent.

4 ***Identificarea vehiculului.*** Identificator de bloc VIN (numărul de identificare al vehiculului) Statul membru de înmatriculare și VRN	----------🚘---------- 🚘 VIN_____ Nat/VRN_____
5 ***Identificarea unității montate pe vehicul (VU)*** Identificator de bloc Denumirea producătorului VU Numărul de componentă a VU Numărul generației VU (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Numărul generației cardului poate fi imprimat numai de tahograful inteligent.

6 ***Ultima etalonare a tahografului*** Identificator de bloc Denumirea atelierului Identificarea cardului de atelier Data etalonării	----------▼---------- ▼ Last_Name_____ Card_Identification_____ ▼ dd/mm/yyyy

7 ***Ultimul control (efectuat de un agent de control)***

Identificator de bloc	----------▣----------
Identificarea cardului de conducător auto	Card_Identification_____
Data, ora și tipul controlului	▣ dd/mm/yyyy hh:mm ppppp

Tipul de control: Maximum cinci pictograme. Tipul de control poate fi (o combinație a următoarelor elemente):
▬: Descărcare de pe card, ↧: Descărcare de pe VU, ↧: Imprimare, □: Afișare, ↾: Verificarea etalonării în trafic

8 ***Activitățile conducătorului auto, stocate pe card în ordine cronologică***

Identificator de bloc	----------⊙----------
Data interogării (ziua calendaristică care face obiectul documentului imprimat) + contorul prezenței zilnice pentru card	dd/mm/yyyy xxx
8a *Condiția „În afara zonei de aplicare a reglementărilor" la începutul zilei respective* (a nu se completa dacă nu este deschisă nicio condiție de tip „În afara zonei de aplicare a reglementărilor")	----------OUT----------
8.1 *Perioadă în care nu a fost introdus cardul*	
8.1a Identificator de înregistrare (începutul perioadei)	----------
8.1b *Perioadă necunoscută*. Ora începerii, durata	? hh:mm hhhmm
8.1c *Activitate introdusă manual*. Pictograma activității, ora începerii, durata	A hh:mm hhhmm
8.2 *Introducerea cardului în slotul S*	
Identificator de înregistrare; S = pictogramă „slot"	---------S---------
Statul membru de înmatriculare al vehiculului și VRN	Nat/VRN_____
Odometrul vehiculului în momentul introducerii cardului	x xxx xxx **km**
8.3 *Activitate (în timp ce cardul era introdus)*	
Pictograma activității, ora începerii, durata, regimul de conducere (pictograma „echipaj" dacă regimul este „ECHIPAJ", spații goale dacă regimul este „SINGUR")	A hh:mm hhhmm ⊙⊙
8.3a *Condiție specifică*. Ora introducerii, pictograma condiției specifice (sau o combinație de pictograme).	hh:mm ---pppp---
8.4 *Retragerea cardului*	
Odometrul vehiculului și distanța parcursă de la ultima introducere a cardului pentru care se cunoaște valoarea indicată de odometru	x xxx xxx **km**; x xxx **km**

9 ***Activitățile conducătorului auto, stocate într-o VU, per slot, în ordine cronologică***

Identificator de bloc	----------⊙----------
Data interogării (ziua calendaristică care face obiectul documentului imprimat)	dd/mm/yyyy
Odometrul la 00.00 și la 24.00	x xxx xxx - x xxx xxx **km**

10 ***Activități desfășurate în slotul S***

Identificator de bloc	----------S----------
10a *Condiția „În afara zonei de aplicare a reglementărilor" la începutul zile respective* (a nu se completa dacă nu este deschisă nicio condiție de tip „În afara zonei de aplicare a reglementărilor")	----------OUT----------
10.1 *Perioadă în care nu este introdus niciun card în slotul S*	
Identificator de înregistrare	----------
Niciun card introdus	⊙▬---
Odometrul vehiculului la începutul perioadei	x xxx xxx **km**
10.2 *Introducerea cardului*	
Identificatorul de înregistrare a introducerii cardului	----------
Numele conducătorului auto	⊙ Last_Name_____

	Prenumele conducătorului auto	First_Name_____
	Identificarea cardului de conducător auto	Card_Identification_____
	Data expirării cardului (dacă este cazul) și numărul generației cardului (GEN 1 sau GEN 2) (*)	dd/mm/yyyy - GEN 2
	Statul membru de înmatriculare și VRN ale vehiculului utilizat anterior	+Nat/VRN_____
	Data și ora retragerii cardului din vehiculul anterior	dd/mm/yyyy hh:mm
	Rând liber	
	Valoarea odometrului în momentul introducerii cardului, indicatorul de stare „Introducerea manuală a activităților conducătorului auto” (M dacă da, spațiu gol dacă nu).	x xxx xxx **km** M
	Dacă nu s-a introdus niciun card de conducător auto în ziua pentru care se imprimă documentul, pentru blocul 10.2 se utilizează datele citite din odometru cu ocazia ultimei introduceri disponibile a cardului din ziua anterioară.	
10.3	*Activitate*	
	Pictograma activității, ora începerii, durata, regimul de conducere (pictograma „echipaj” dacă regimul este „ECHIPAJ”, spații goale dacă regimul este „SINGUR”)	A hh:mm hh**h**mm
10.3a	*Condiții specifice*. Ora introducerii, pictograma condiției specifice (sau o combinație de pictograme)	hh:mm ---pppp---
10.4	*Retragerea cardului sau sfârșitul perioadei în care nu a fost introdus niciun card*	
	Valoarea indicată de odometru în momentul retragerii cardului sau la sfârșitul perioadei în care nu este introdus niciun card și distanța parcursă de la introducerea cardului sau de la începutul perioadei în care nu este introdus niciun card.	x xxx xxx **km**; x xxx **km**

(*) Numărul generației cardului poate fi imprimat numai de tahograful inteligent.

11	***Rezumat zilnic***	
	Identificator de bloc	----------Σ----------
11.1	***Rezumatul VU al perioadelor fără card în slotul pentru cardul de conducător auto***	
	Identificator de bloc	1----
11.2	***Rezumatul VU al perioadelor fără card în slotul pentru cardul copilotului***	
	Identificator de bloc	2----
11.3	***Rezumat zilnic VU pentru fiecare conducător auto***	
	Identificator de înregistrare	----------
	Numele conducătorului auto	Last_Name_____
	Prenumele conducătorului auto	First_Name_____
	Identificarea cardului de conducător auto	Card_Identification_____
11.4	*Introducerea locului în care începe și/sau se încheie ziua de lucru*	
	pi=pictograma locului de începere/încheiere, ora, țara, regiunea,	pihh:mm Cou Reg
	Odometru	x xxx xxx **km**
11.5	*Introducerea locului în care începe și/sau se încheie ziua de lucru*	
	și după un timp de conducere continuă de 3 ore	hh:mm
	Odometru	x xxx xxx **km**
11.6	*Totaluri activități (de pe un card)*	
	Durata totală a perioadei de conducere, distanța parcursă	hh**h**mm x xxx **km**
	Durata totală a perioadei de lucru și de disponibilitate	hh**h**mm hh**h**mm
	Durata totală a perioadei de odihnă și a activităților necunoscute	hh**h**mm hh**h**mm
	Durata totală a activităților desfășurate de echipaj	hh**h**mm
11.7	*Totaluri activități (perioade fără card introdus în slotul pentru cardul conducătorului auto)*	
	Durata totală a perioadei de conducere, distanța parcursă	hh**h**mm x xxx **km**
	Durata totală a perioadei de lucru și de disponibilitate	hh**h**mm hh**h**mm
	Durata totală a perioadei de odihnă	hh**h**mm

11.8	*Totaluri activități (perioade fără card introdus în slotul pentru cardul copilotului)*	
	Durata totală a perioadei de lucru și de disponibilitate	hh**h**mm hh**h**mm
	Durata totală a perioadei de odihnă	hh**h**mm
11.9	*Totaluri activitate (per conducător auto, pentru ambele sloturi)*	
	Durata totală a perioadei de conducere, distanța parcursă	hh**h**mm x xxx **km**
	Durata totală a perioadei de lucru și de disponibilitate	hh**h**mm hh**h**mm
	Durata totală a perioadei de odihnă	hh**h**mm
	Durata totală a activităților desfășurate de echipaj	hh**h**mm

Când este necesară imprimarea unui document zilnic pentru ziua respectivă, rezumatul informațiilor zilnice se calculează cu ajutorul datelor disponibile în momentul imprimării.

12	***Evenimente și/sau anomalii stocate pe un card***	
12.1	Identificator de bloc pentru ultimele 5 „Evenimente și anomalii” înregistrate pe un card	----------!×---------- ----------!×----------
12.2	Identificator de bloc pentru toate „Evenimentele” înregistrate pe un card	----------!----------
12.3	Identificator de bloc pentru toate „Anomaliile” înregistrate pe un card	----------×----------
12.4	*Înregistrarea evenimentului și/sau a anomaliei*	
	Identificator înregistrare	----------
	Pictograma evenimentului/anomaliei, scopul înregistrării, data și ora începerii	Pic (p) dd/mm/yyyy hh:mm
	Cod suplimentar al evenimentului/anomaliei (dacă este cazul), durata	!xx hh**h**mm
	Statul membru de înmatriculare și VRN ale vehiculului în care s-a produs evenimentul sau anomalia	Nat/VRN_____

13	***Evenimente și/sau anomalii stocate sau aflate în desfășurare într-o VU***	
13.1	Identificator de bloc pentru ultimele 5 „Evenimente și anomalii” înregistrate în VU	----------!×---------- ----------!×----------
13.2	Identificator de bloc pentru toate „Evenimentele” înregistrate sau aflate în desfășurare într-o VU	----------!----------
13.3	Identificator de bloc pentru toate „Anomaliile” înregistrate sau aflate în desfășurare într-o VU	----------×----------
13.4	*Înregistrarea evenimentului și/sau a anomaliei*	
	Identificator de înregistrare	----------
	Pictograma evenimentului/anomaliei, scopul înregistrării, data și ora începerii	Pic (p) dd/mm/yyyy hh:mm
	Cod suplimentar al evenimentului/anomaliei (dacă este cazul), numărul evenimentelor similare din ziua respectivă, durata	!xx (xxx) hh**h**mm
	Identificarea cardurilor introduse la începutul sau la sfârșitul evenimentului sau anomaliei (maximum 4 rânduri, fără repetarea numărului de card)	Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____
	Caz în care nu a fost introdus niciun card	--- < Literal><ErrorCode>
	Date specifice producătorului	

Scopul înregistrării (p) este un cod numeric care identifică motivul pentru care evenimentul sau anomalia a fost înregistrată, codat în conformitate cu elementul de date `EventFaultRecordPurpose`.

„`Literal`” este un cod de litere specific producătorului tahografului, compus din maximum 12 caractere.

„`ErrorCode`” este un cod de eroare specific producătorului tahografului, compus din maximum 12 caractere.

14 ***Identificarea VU***

Identificator de bloc	----------B----------
Denumirea producătorului VU	B Name_____
Adresa producătorului VU	Address_____
Numărul de componentă VU	PartNumber_____
Numărul de omologare al VU	Apprv_____
Numărul de serie al VU	S/N_____
Anul de fabricație a VU	yyyy
Versiunea software-ului VU și data instalării acestuia	V xxxx dd/mm/yyyy

15 ***Identificarea senzorului***

Identificator de bloc	----------Л----------
15.1 *Înregistrarea asocierilor*	
Numărul de serie al senzorului	Л S/N_____
Numărul de omologare al senzorului	Apprv_____
Data asocierii senzorului	dd/mm/yyyy hh:mm

16 ***Identificarea GNSS***

Identificator de bloc	----------▚----------
16.1 *Înregistrarea cuplărilor*	
Numărul de serie al echipamentului GNSS extern:	▚ S/N_____
Numărul de omologare al echipamentului GNSS extern:	Apprv_____
Data asocierii echipamentului GNSS extern:	dd/mm/yyyy hh:mm

17 ***Date privind etalonarea***

Identificator de bloc	----------T----------
17.1 *Înregistrarea etalonării*	
Identificator de înregistrare	----------
Denumirea atelierului care a efectuat etalonarea	T Workshop_name_____
Adresa atelierului	Workshop_address_____
Identificarea cardului de atelier	Card_Identification_____
Data expirării cardului de atelier	dd/mm/yyyy
Rând liber	
Data etalonării + scopul etalonării	T dd/mm/yyyy (p)
VIN (numărul de identificare al vehiculului)	A VIN_____
Statul membru de înmatriculare și VRN	Nat/VRN_____
Coeficientul caracteristic al vehiculului	w xx xxx Imp/km
Constanta aparaturii de înregistrare	k xx xxx Imp/km
Effective circumference of wheel tyres	l xx xxx mm
Dimensiunea pneurilor montate	● TyreSize_____
Reglajul limitatorului de viteză	> xxx km/h
Valoarea veche și valoarea nouă a odometrului	x xxx xxx – x xxx xxx km

Scopul etalonării (p) este un cod numeric care indică motivul pentru care au fost înregistrați respectivii parametri de etalonare, codat în conformitate cu elementul de date `CalibrationPurpose`.

18 ***Reglarea orei***

	Identificator de bloc	----------◷----------
18.1	*Înregistrarea reglării orei*	
	Identificator de înregistrare	----------
	Data și ora vechi	!◷ dd/mm/yyyy hh:mm
	Data și ora noi	◷ dd/mm/yyyy hh:mm
	Denumirea atelierului care a efectuat reglarea orei	T Workshop_name_____
	Adresa atelierului	Workshop_address_____
	Identificarea cardului de atelier	Card_Identification_____
	Data de expirare a cardului de atelier	dd/mm/yyyy

19 ***Cel mai recent eveniment și cea mai recentă anomalie înregistrate în VU***

	Identificator de bloc	----------!×🖷----------
	Data și ora celui mai recent eveniment	! dd/mm/yyyy hh:mm
	Data și ora celei mai recente anomalii	× dd/mm/yyyy hh:mm

20 ***Informații privind controalele pentru depășirea limitei de viteză***

	Identificator de bloc	----------►►----------
	data și ora la care s-a efectuat ultimul CONTROL PENTRU DEPĂȘIREA LIMITEI DE VITEZĂ	►▫dd/mm/yyyy hh:mm
	Data/ora primei depășiri a limitei de viteză și numărul de evenimente de tip „depășirea limitei de viteză” survenite ulterior	►►dd/mm/yyyy hh:mm (nnn)

21 ***Înregistrarea depășirilor limitei de viteză***

21.1	Identificator de bloc „Prima depășire a limitei de viteză după ultima etalonare”	--------►►T---------
21.2	Identificator de bloc „Cele mai grave 5 depășiri ale limitei de viteză survenite în ultimele 365 de zile”	-------►►(365)------
21.3	Identificator de bloc „Cea mai gravă depășire a limitei de viteză pentru fiecare din ultimele 10 zile de producere a evenimentului”	-------►►(10)-------
21.4	Identificator de înregistrare	----------
	Data, ora și durata	►►dd/mm/yyyy hh:mm hhhmm
	Viteza maximă, viteza medie și nr. de evenimente similare din ziua respectivă	xxx km/h xxx km/h(xxx)
	Numele conducătorului auto	◙ Last_Name_____
	Prenumele conducătorului auto	First_Name_____
	Identificarea cardului de conducător auto	Card_Identification_____
21.5	Dacă într-un bloc nu există nicio înregistrare a depășirii limitei de viteză	►►---

22 ***Informații scrise de mână***

	Identificator de bloc	----------
22.1	Locul controlului	▫• .....
22.2	Semnătura agentului de control	▫ .....
22.3	De la ora	◷+ .....
22.4	Până la ora	+◷ .....
22.5	Semnătura conducătorului auto	◙ .....

„Informații scrise de mână”; A se introduce suficiente rânduri libere deasupra unui element scris de mână pentru a se putea scrie efectiv informațiile necesare sau pentru a se introduce o semnătură.

23 ***Cele mai recente carduri introduse în VU***
Identificator de bloc
23.1 Card introdus
Identificator de înregistrare
Tip de card, generație, versiune, producător (*)
Identificarea cardului
Numărul de serie al cardului
Data și ora ultimei introduceri a cardului

```
-------- ⊟■⊙ --------

----
⍑ <gen> <version> <MC>
Identificarea cardului
Card Serial Number
dd/mm/yyyy hh:mm
```

(*) (toate informațiile pe un singur rând)
reprezentate astfel:
tip de card: Pictogramă, un caracter + spațiu
gen (generația): GEN1 sau GEN2, 4 caractere + spațiu
version (versiune): până la 10 caractere
MC (producător): codul producătorului, 3 caractere

3. SPECIFICAȚII REFERITOARE LA DOCUMENTELE IMPRIMATE

În prezentul capitol s-au folosit următoarele notații convenționale:

N	A se imprima blocul sau înregistrarea cu numărul N.
N	A se imprima blocul sau înregistrarea cu numărul N, operațiune repetată ori de câte ori este necesar.
X/Y	A se imprima blocurile sau înregistrările X și/sau Y, după caz, cu repetarea operațiunii ori de câte ori este necesar.

3.1. **Document imprimat zilnic privind activitățile conducătorului auto extrase de pe card**

PRT_008 Documentul imprimat zilnic privind activitățile conducătorului auto extrase de pe card respectă următorul format:

1	Data și ora imprimării documentului
2	Tipul de document imprimat
3	Identificarea agentului de control (dacă în VU este introdus un card de control)
3	Identificarea conducătorului auto (de pe cardul care face obiectul imprimării + GEN)
4	Identificarea vehiculului (vehiculul din care se imprimă datele)
5	Identificarea VU (VU din care se imprimă datele + GEN)
6	Ultima etalonare a respectivei VU
7	Ultimul control la care a fost supus conducătorul auto inspectat
8	Delimitator al activităților conducătorului auto
8a	Condiție „În afara zonei de aplicare a reglementărilor” la începutul zilei respective
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Activitățile conducătorului auto în ordine cronologică
11	Delimitator al rezumatului zilnic

11.4	Locurile introduse în ordine cronologică
11.5	Date GNSS
11.6	Totaluri activitate
12.1	Evenimente sau anomalii din delimitatorul cardului
12.4	Înregistrări de evenimente/anomalii (ultimele 5 evenimente sau anomalii înregistrate pe card)
13.1	Evenimente sau anomalii extrase din delimitatorul VU
13.4	Înregistrări de evenimente/anomalii (ultimele 5 evenimente sau anomalii înregistrate sau în curs de desfășurare în VU)
22.1	Locul controlului
22.2	Semnătura agentului de control
22.5	Semnătura conducătorului auto

3.2. **Document imprimat zilnic privind activităților conducătorului auto extrase din VU**

PRT_009 Documentul imprimat zilnic privind activităților conducătorului auto extrase din VU respectă următorul format:

1	Data și ora imprimării documentului
2	Tipul de document imprimat
3	Identificarea titularului cardului (pentru toate cardurile introduse în VU + GEN)
4	Identificarea vehiculului (vehiculul din care se imprimă datele)
5	Identificarea VU (VU din care se imprimă datele + GEN)
6	Ultima etalonare a respectivei VU
7	Ultimul control al tahografului respectiv
9	Delimitator al activităților conducătorului auto
10	Delimitator al slotului pentru cardul de conducător auto (slotul 1)
10a	Condiție „În afara zonei de aplicare a reglementărilor” la începutul zilei respective
10.1 / 10.2 / 10.3 /10.3a / 10.4	Activități în ordine cronologică (slot pentru cardul de conducător auto)
10	Delimitator al slotului pentru cardul copilotului (slotul 2)
10a	Condiție „În afara zonei de aplicare a reglementărilor” la începutul zilei respective
10.1 / 10.2 / 10.3 /10.3a / 10.4	Activități în ordine cronologică (slot pentru cardul copilotului)
11	Delimitator al rezumatului zilnic
11.1	Rezumatul perioadelor fără card în slotul pentru cardul de conducător auto
11.4	Locurile introduse în ordine cronologică
11.5	Date GNSS
11.6	Totaluri activitate
11.2	Rezumatul perioadelor fără card în slotul pentru cardul copilotului
11.4	Locurile introduse în ordine cronologică
11.5	Date GNSS

11.7	Totaluri activitate
11.3	Rezumatul activităților unui conducător auto, pentru ambele sloturi
11.4	Locurile introduse de respectivul conducător auto în ordine cronologică
11.5	Date GNSS
11.8	Totaluri activitate pentru respectivul conducător auto
13.1	Delimitator evenimente/anomalii
12.4	Înregistrări de evenimente/anomalii (ultimele 5 evenimente sau anomalii înregistrate sau în curs de desfășurare în VU)
13.1	Locul controlului
22.2	Semnătura agentului de control
22.3	De la ora (spațiu disponibil pentru ca un conducător auto fără card să indice care perioade sunt relevante pentru el)
22.4	Până la ora
22.5	Semnătura conducătorului auto

3.3. **Document imprimat privind evenimentele și anomaliile de pe card**

PRT_010 Documentul imprimat privind evenimentele și anomaliile de pe card respectă următorul format:

1	Data și ora imprimării documentului
2	Tipul de document imprimat
3	Identificarea agentului de control (dacă în VU este introdus un card de control + GEN)
3	Identificarea conducătorului auto (de pe cardul care face obiectul imprimării)
4	Identificarea vehiculului (vehiculul din care se imprimă datele)
12.2	Delimitator al evenimentelor
12.4	Înregistrări ale evenimentelor (toate evenimentele stocate pe card)
12.3	Delimitator al anomaliilor
12.4	Înregistrări ale anomaliilor (toate anomaliile stocate pe card)
22.1	Locul controlului
22.2	Semnătura agentului de control
22.5	Semnătura conducătorului auto

3.4. **Document imprimat privind evenimentele și anomaliile din VU**

PRT_011 Documentul imprimat privind evenimentele și anomaliile din VU respectă următorul format:

1	Data și ora imprimării documentului
2	Tipul de document imprimat
3	Identificarea titularului cardului (pentru toate cardurile introduse în VU + GEN)
4	Identificarea vehiculului (vehiculul din care se imprimă datele)

13.2	Delimitator al evenimentelor
13.4	Înregistrări ale evenimentelor (toate evenimentele stocate sau în curs de desfășurare în VU)
13.3	Delimitator al anomaliilor
13.4	Înregistrări ale anomaliilor (toate anomaliile stocate sau în curs de desfășurare în VU)
22.1	Locul controlului
22.2	Semnătura agentului de control
22.5	Semnătura conducătorului auto

3.5. **Document imprimat privind datele tehnice**

PRT_012 Documentul imprimat privind datele tehnice respectă următorul format:

1	Data și ora imprimării documentului
2	Tipul de document imprimat
3	Identificarea titularului cardului (pentru toate cardurile introduse în VU + GEN)
4	Identificarea vehiculului (vehiculul din care se imprimă datele)
14	Identificarea VU
15	Identificarea senzorului
15.1	Date privind asocierea senzorului (toate datele disponibile în ordine cronologică)
16	Identificarea GNSS
16.1	Date privind cuplarea echipamentului GNSS extern (toate datele disponibile în ordine cronologică)
17	Delimitator al datelor de etalonare
17.1	Înregistrări ale etalonărilor (toate înregistrările disponibile în ordine cronologică)
18	Delimitator al reglării orei
18.1	Înregistrări ale reglării orei (toate înregistrările disponibile din înregistrările reglării orei și ale datelor de etalonare)
19	Cel mai recent eveniment și cea mai recentă anomalie înregistrate în VU

3.6. **Document imprimat privind depășirea limitei de viteză**

PRT_013 Documentul imprimat privind depășirea limitei de viteză respectă următorul format:

1	Data și ora imprimării documentului
2	Tipul de document imprimat
3	Identificarea titularului cardului (pentru toate cardurile introduse în VU + GEN)
4	Identificarea vehiculului (vehiculul din care se imprimă datele)
20	Informații privind controalele pentru depășirea limitei de viteză
21.1	Identificatorul datelor privind depășirile limitei de viteză
21.4 / 21.5	Prima depășire a limitei de viteză după ultima etalonare

21.2	Identificatorul datelor privind depășirile limitei de viteză
21.4 / 21.5	Cele mai grave 5 depășiri ale limitei de viteză din ultimele 365 de zile
21.3	Identificatorul datelor privind depășirile limitei de viteză
21.4 / 21.5	Cea mai gravă depășire a limitei de viteză pentru fiecare dintre ultimele 10 zile de producere a evenimentului
22.1	Locul controlului
22.2	Semnătura agentului de control
22.5	Semnătura conducătorului auto

3.7. **Istoricul introducerii cardurilor**

PRT_014 Documentul imprimat privind istoricul introducerii cardurilor respectă următorul format:

1	Data și ora imprimării documentului
2	Tipul de document imprimat
3	Identificarea titularului cardului (pentru toate cardurile introduse în VU)
23	Cel mai recent card introdus în VU
23.1	Carduri introduse (până la 88 de înregistrări)
12.3	Delimitator al anomaliilor

Apendicele 5

AFIȘAJUL

În prezentul apendice s-au folosit următoarele notații convenționale de formatare:

— caracterele **aldine** indică textul în clar care urmează să fie afișat (afișajul rămâne în caractere normale);

— caracterele normale indică variabilele (pictograme sau date) care trebuie să fie înlocuite cu valorile lor în scopul afișării:

  — zz ll aaaa: ziua, luna, anul,

  — hh: ore,

  — mm: minute,

  — D: pictograma pentru durată,

  — EF: combinație de pictograme pentru evenimente sau anomalii,

  — O: pictograma modului de funcționare.

DIS_001 Tahograful afișează datele folosind următoarele formate:

Date	Format
Afișaj implicit	
Ora locală	hh:mm
Mod de funcționare	O
Informații privind conducătorul auto	1 Dhh**h**mm ▮▮hh**h**mm
Informații privind copilotul	2 Dhh**h**mm
Condiția „În afara zonei de aplicare a reglementărilor” deschisă	OUT
Afișaj de avertizare	
Depășirea timpului de conducere continuă	1 ⊙ hh**h**mm ▮▮hh**h**mm
Eveniment sau anomalie	EF
Alte afișaje	
Data UTC ora	UTC ⊙ zz/ll/aaaa sau UTC ⊙ zz.ll.aaaa hh:mm
Timpul de conducere continuă și durata cumulată a pauzelor conducătorului auto	1 ⊙ hh**h**mm ▮▮hh**h**mm
Timpul de conducere continuă și durata cumulată a pauzelor copilotului	2 ⊙ hh**h**mm ▮▮hh**h**mm
Timpul de conducere cumulat al conducătorului auto pentru săptămâna anterioară și cea curentă	1 ⊙ ▮ hhh**h**mm
Timpul de conducere cumulat al copilotului pentru săptămâna anterioară și cea curentă	2 ⊙ ▮ hhh**h**mm

Apendicele 6

CONECTOR FRONTAL PENTRU ETALONARE ȘI DESCĂRCARE

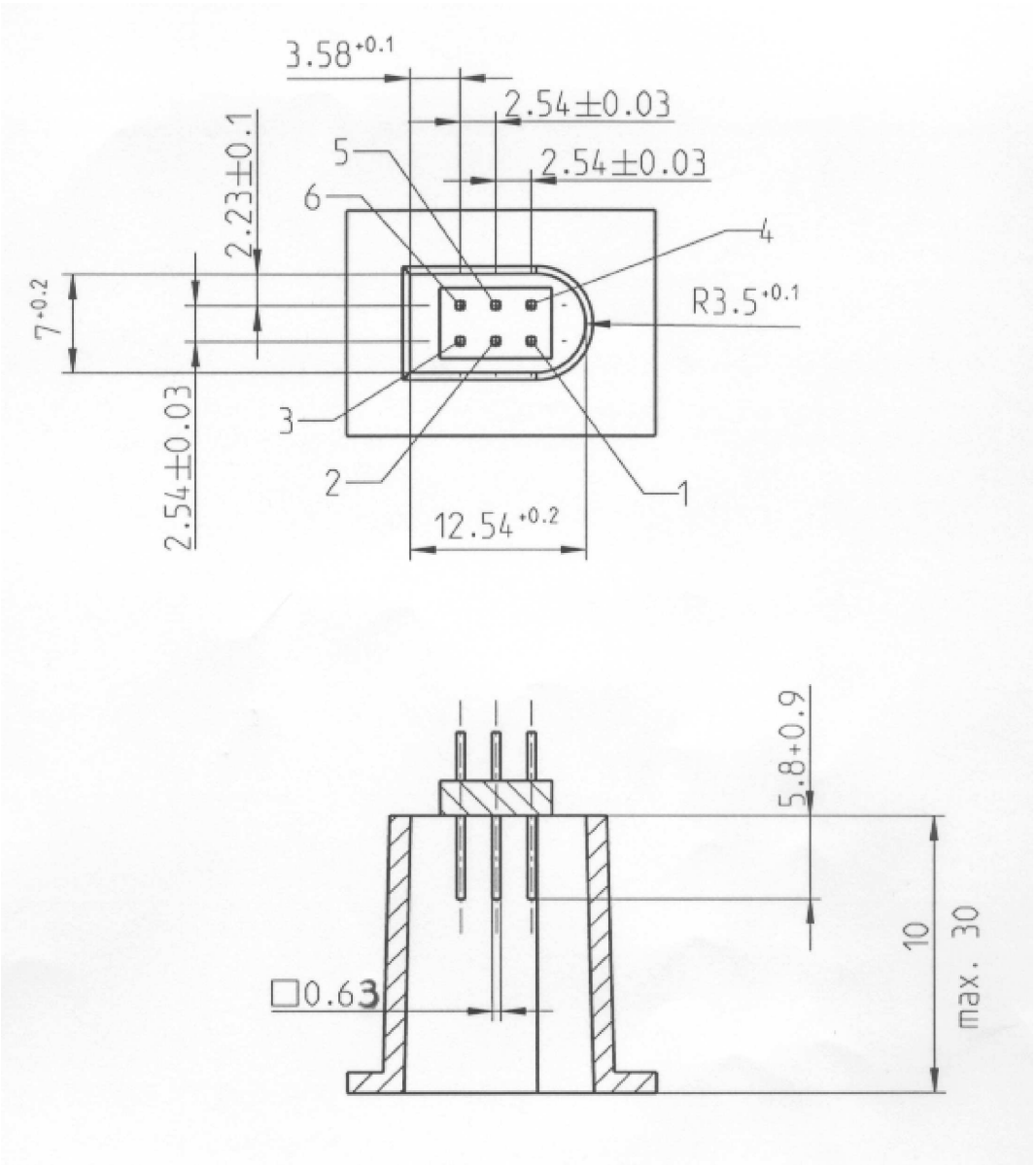
CUPRINS

1. HARDWARE 256
1.1. Conector 256
1.2. Alocarea contactelor 257
1.3. Schema funcțională 258
2. INTERFAȚĂ DE DESCĂRCARE 258
3. INTERFAȚĂ DE ETALONARE 259

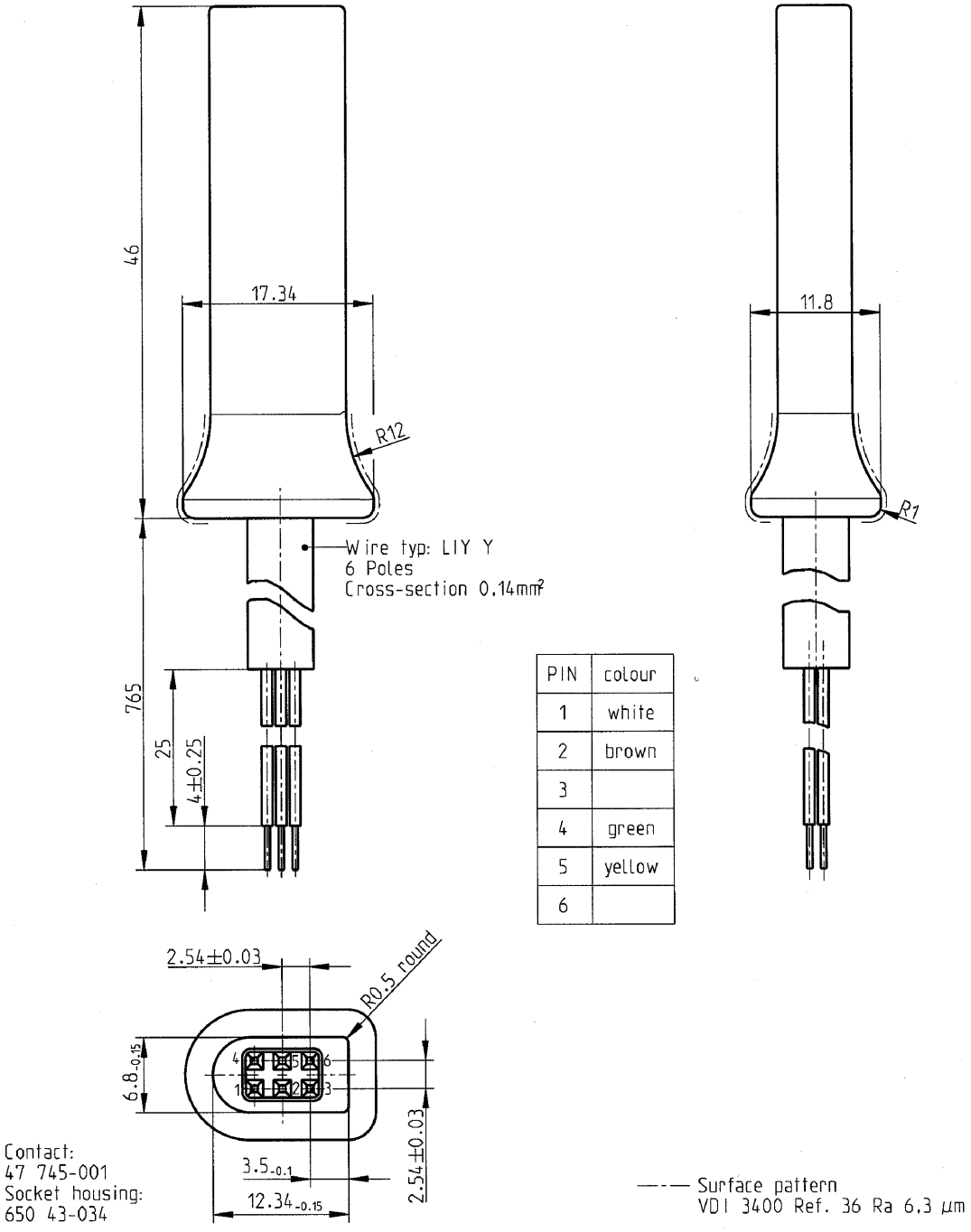
1. HARDWARE

1.1. **Conector**

INT_001 Conectorul pentru descărcare/etalonare trebuie să fie un conector cu 6 contacte, care să poată fi accesat de la panoul frontal, fără a fi necesară deconectarea unei părți a tahografului, și trebuie să respecte detaliile din următoarea schiță (toate dimensiunile sunt în milimetri):



În următoarea diagramă este prezentată o fișă obișnuită de conectare cu 6 contacte:



1.2. **Alocarea contactelor**

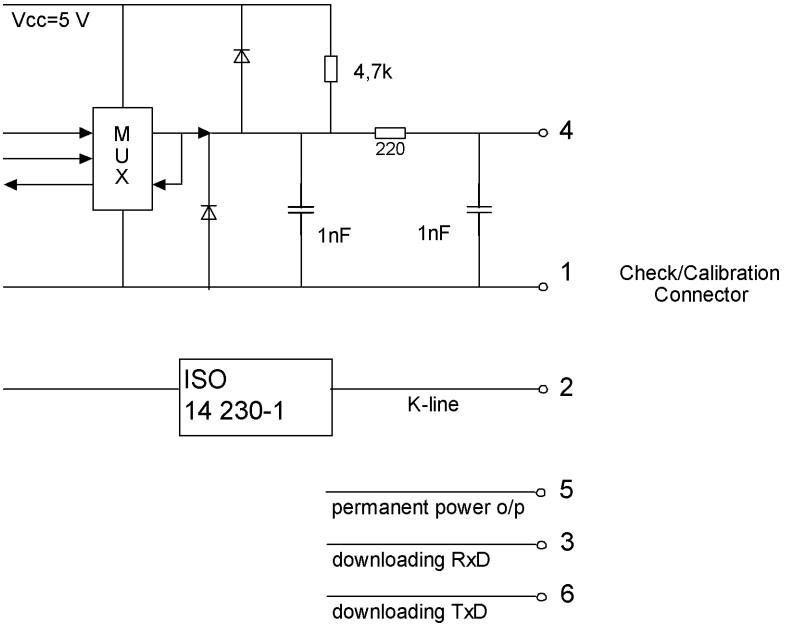
INT_002 Contactele se alocă în conformitate cu tabelul următor:

Contact	Descriere	Observație
1	Pol negativ al bateriei	Conectat la polul negativ al bateriei vehiculului
2	Comunicarea datelor	Linia K (ISO 14230-1)

Contact	Descriere	Observație
3	RxD – Descărcare	Date de intrare în tahograf
4	Semnal de intrare/ieșire	Etalonare
5	Putere de ieșire permanentă	Intervalul de tensiune trebuie să fie identic cu cel pentru alimentarea electrică a vehiculului minus 3 V pentru a lua în calcul căderea de tensiune din circuitele de protecție. Ieșire de 40 mA
6	TxD – Descărcare	Date de ieșire provenite de la tahograf

1.3. **Schema funcțională**

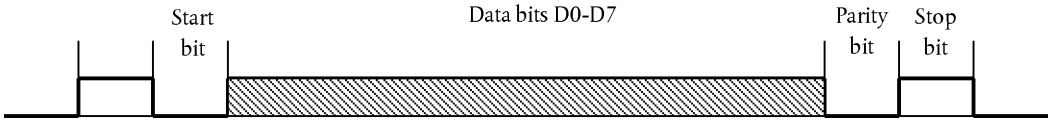
INT_003 Schema funcțională trebuie să respecte următoarele indicații:



2. INTERFAȚĂ DE DESCĂRCARE

INT_004 Interfața de descărcare trebuie să respecte specificațiile RS232.

INT_005 Interfața de descărcare folosește un bit de pornire, 8 biți de date cu un LSB (bitul cel mai puțin semnificativ) la început, un bit de paritate pară și 1 bit de oprire.



Organizarea octeților de informații

Bit de inițiere: un bit cu nivel logic 0;

Biți de date: transmiși cu un LSB la început;

Bit de paritate: paritate pară

Bit de oprire: un bit cu nivel logic 1

La transmisia datelor numerice compuse din mai mult de un octet, octetul cel mai semnificativ este transmis la început și octetul cel mai puțin semnificativ este transmis la sfârșit.

INT_006 Viteza de transmisie a datelor poate fi reglată într-un interval cuprins între 9 600 bps și 115 200 bps. Transmisia se realizează la viteza maximă posibilă, viteza de transmisie inițială după începerea comunicării fiind stabilită la 9 600 bps.

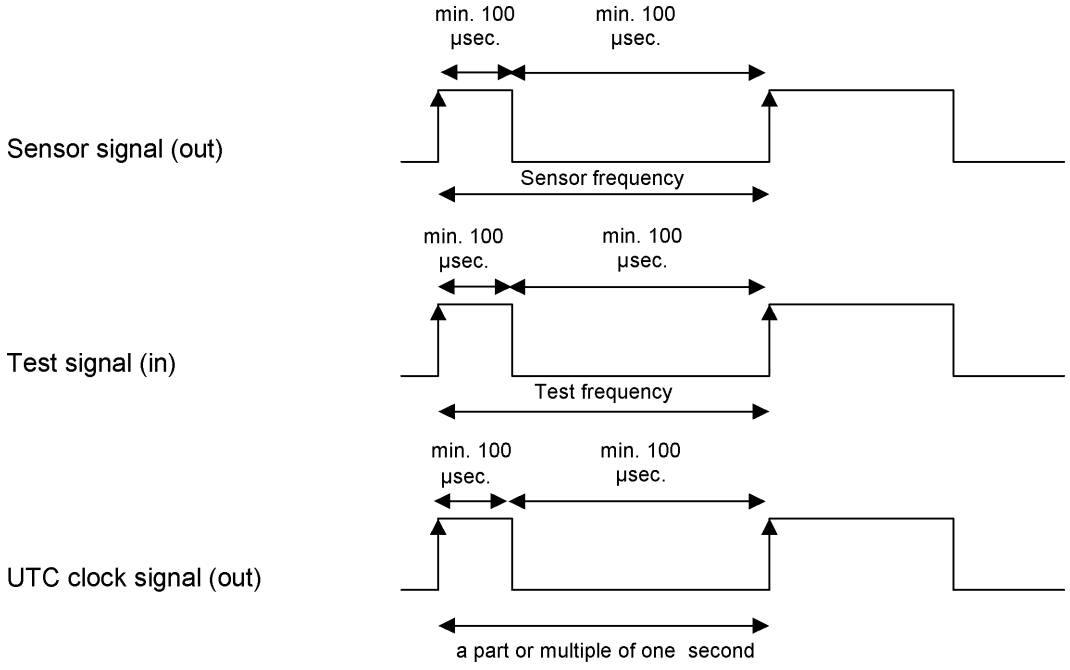
3. INTERFAȚĂ DE ETALONARE

INT_007 Comunicările de date respectă ISO 14230-1 *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 1: Physical layer,* prima ediție: 1999.

INT_008 Semnalul de intrare/ieșire respectă următoarele specificații electrice:

Parametru	Minim	Normal	Maxim	Observație
U_{low} (intrare)			1,0 V	I = 750 µA
U_{high} (intrare)	4 V			I = 200 µA
Frecvență			4 kHz	
U_{low} (ieșire)			1,0 V	I = 1 mA
U_{high} (ieșire)	4 V			I = 1 mA

INT_009 Semnalul de intrare/ieșire trebuie să respecte următoarele diagrame de timp:



Apendicele 7

PROTOCOALE DE DESCĂRCARE A DATELOR

CUPRINS

1.	INTRODUCERE	261
1.1.	Domeniu de aplicare	261
1.2.	Acronime și notații	261
2.	DESCĂRCAREA DATELOR DE PE VU	262
2.1.	Procedura de descărcare	262
2.2.	Protocolul de descărcare a datelor	262
2.2.1	Structura mesajului	262
2.2.2	Tipuri de mesaje	264
2.2.2.1	Solicitare de inițiere a comunicării (*Start Communication Request*)(SID 81)	266
2.2.2.2	Răspuns pozitiv la solicitarea de inițiere a comunicării (*Positive Response Start Communication*)(SID C1)	266
2.2.2.3	Solicitare de începere a sesiunii de diagnosticare (*Start Diagnostic Session Request*) (SID 10)	266
2.2.2.4	Răspuns pozitiv la solicitarea de începere a sesiunii de diagnosticare (*Positive Response Start Diagnostic*) (SID 50)	266
2.2.2.5	Serviciul de control al legăturii (*Link Control Service*) (SID 87)	266
2.2.2.6	Răspuns pozitiv la controlul legăturii (*Link Control Positive Response*) (SID C7)	266
2.2.2.7	Solicitare de încărcare (*Request Upload*)(SID 35)	266
2.2.2.8	Răspuns pozitiv la solicitarea de încărcare (*Positive Response Request Upload*) (SID 75)	266
2.2.2.9	Solicitare de transfer de date (*Transfer Data Request*) (SID 36)	266
2.2.2.10	Răspuns pozitiv la solicitarea de transfer de date (*Positive Response Transfer Data*) (SID 76)	267
2.2.2.11	Solicitare de încheiere a transferului (*Request Transfer Exit*) (SID 37)	267
2.2.2.12	Răspuns pozitiv la solicitarea de încheiere a transferului (SID 77) (*Positive Response Request Transfer Exit*)	267
2.2.2.13	Solicitare de încheiere a comunicării (*Stop Communication Request*) (SID 82)	267
2.2.2.14	Răspuns pozitiv la solicitarea de încheiere a comunicării (*Positive Response Stop Communication*) (SID C2)	267
2.2.2.15	Confirmare de primire a sub-mesajului (*Acknowledge Sub Message*) (SID 83)	267
2.2.2.16	Răspuns negativ (*Negative Response*) (SID 7F)	268
2.2.3	Fluxul mesajelor	268
2.2.4	Sincronizare	269
2.2.5	Gestionarea erorilor	270
2.2.5.1	Etapa de inițiere a comunicării	270
2.2.5.2	Etapa de comunicare	270
2.2.6	Conținutul mesajelor de răspuns	272
2.2.6.1	Răspuns pozitiv la solicitarea de transfer de date de prezentare generală (*Positive Response Transfer Data Overview*)	273
2.2.6.2	Răspuns pozitiv la solicitarea de transfer de date privind activitățile (*Positive Response Transfer Data Activities*)	274
2.2.6.3	Răspuns pozitiv la solicitarea de transfer de date privind evenimentele și anomaliile (*Positive Response Transfer Data Events and Faults*)	275
2.2.6.4	Răspuns pozitiv la solicitarea de transfer de date privind viteza detaliată (*Positive Response Transfer Data Detailed Speed*)	276
2.2.6.5	Răspuns pozitiv la solicitarea de transfer de date tehnice (*Positive Response Transfer Data Technical Data*)	276
2.3.	Stocarea fișierelor în ESM	277

3. PROTOCOL DE DESCĂRCARE DE PE CARDURILE DE TAHOGRAF 277
3.1. Domeniu de aplicare 277
3.2. Definiții 277
3.3. Descărcarea informațiilor de pe card 277
3.3.1 Secvența de inițializare 278
3.3.2 Secvența de descărcare de fișiere de date nesemnate 278
3.3.3 Secvența de descărcare de fișiere de date semnate 279
3.3.4 Secvența de resetare a unui contor de etalonare. 279
3.4. Formatul de stocare a datelor 280
3.4.1 Introducere 280
3.4.2 Formatul fișierului 280
4. DESCĂRCAREA INFORMAȚIILOR DE PE UN CARD DE TAHOGRAF PRIN INTERMEDIUL UNEI UNITĂȚI MONTATE PE VEHICUL 281

1. INTRODUCERE

Prezentul apendice cuprinde procedurile care trebuie urmate pentru a realiza diferite tipuri de descărcare de date pe un mediu de stocare extern, precum și protocoalele care trebuie puse în aplicare pentru a asigura transferul corect de date și compatibilitatea deplină a formatului datelor descărcate, pentru a permite oricărui controlor să inspecteze aceste date și să poată verifica autenticitatea și integritatea acestora înainte de a le analiza.

1.1. **Domeniu de aplicare**

Datele pot fi descărcate pe un ESM:

— de pe o unitate montată pe vehicul, cu ajutorul unui echipament inteligent dedicat (IDE) conectat la VU;

— de pe un card de tahograf, cu ajutorul unui IDE conectat la un dispozitiv de interfață pentru card (IFD);

— de pe un card de tahograf, prin intermediul unei unități montate pe vehicul și cu ajutorul unui IDE conectat la VU.

Pentru a permite verificarea autenticității și integrității datelor descărcate stocate pe un ESM, datele se descarcă însoțite de o semnătură atașată în conformitate cu apendicele 11 „Mecanisme de securitate comune”. Se descarcă, de asemenea, identificarea echipamentului sursă (VU sau card) și certificatele sale de securitate (stat membru și echipament). Persoana care verifică datele trebuie să dețină o cheie publică europeană certificată.

DDP_001 Datele descărcate în cadrul unei sesiuni de descărcare trebuie să fie stocate în ESM într-un fișier unic.

1.2. **Acronime și notații**

În prezentul apendice sunt folosite următoarele acronime:

AID Identificator de aplicație (*Application Identifier*)

ATR Răspuns de resetare (*Answer To Reset*)

CS Octet de sumă de verificare (*Checksum byte*)

FD Fișier dedicat (*Dedicated File*)

DS_ Sesiune de diagnosticare (*Diagnostic Session*)

EF Fișier elementar (*Elementary File*)

ESM Mediu de stocare extern (*External Storage Medium*)

FID Identificatorul fișierului [*File Identifier (File ID)*]

FMT Octet de format (primul octet al antetului mesajului) (*Format Byte*)

ICC Card cu circuite integrate (*Integrated Circuit Card*)

IDE Echipament inteligent dedicat: echipamentul folosit la efectuarea descărcării datelor în ESM (de exemplu, un calculator personal)

IFD Dispozitiv de interfață (*Interface Device*)

KWP Keyword Protocol 2000

LEN Octet de lungime (ultimul octet al antetului mesajului) (*Length Byte*)

PPS Selecția parametrilor protocolului (*Protocol Parameter Selection*)

PSO Executarea unei operațiuni de securitate (*Perform Security Operation*)

SID Identificator de serviciu (*Service Identifier*)

SRC Octet sursă (*Source byte*)

TGT Octet țintă (*Target Byte*)

TLV Valoarea lungimii etichetei (*Tag Length Value*)

TREP Parametru de răspuns la transfer (*Transfer Response Parameter*)

TRTP Parametru de solicitare de transfer (*Transfer Request Parameter*)

VU Unitate montată pe vehicul (*Vehicle Unit*)

2. DESCĂRCAREA DATELOR DE PE VU

2.1. **Procedura de descărcare**

Pentru a efectua o descărcare de date de pe VU, operatorul trebuie să realizeze următoarele operațiuni:

— să insereze cardul său de tahograf într-un slot pentru card al VU (*);

— să conecteze IDE la conectorul de descărcare al VU;

— să stabilească conexiunea dintre IDE și VU;

— să selecteze în IDE datele care trebuie descărcate și să trimită solicitarea la VU;

— să încheie sesiunea de descărcare.

2.2. **Protocolul de descărcare a datelor**

Protocolul este structurat pe baza unei arhitecturi de tip *master/slave*, unde IDE are rolul de *master* și VU are rolul de *slave*.

Structura, tipurile și fluxul mesajelor se bazează în principal pe protocolul *Keyword Protocol 2000* (KWP) (*ISO 14230-2 Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part2: Data link layer*).

Stratul de aplicație se bazează în principal pe proiectul actual de standard ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1: Diagnostic services*, versiunea 6 din 22 februarie 2001).

2.2.1 *Structura mesajului*

DDP_002 Toate mesajele schimbate între IDE și VU sunt formatate cu o structură care constă în trei părți:

— un antet compus dintr-un octet de format (FMT), un octet țintă (TGT), un octet sursă (SRC) și, eventual, un octet de lungime (LEN);

— un câmp de date compus dintr-un octet al identificatorului de serviciu (SID) și un număr variabil de octeți de date, care pot cuprinde un octet opțional de sesiune de diagnosticare (DS_) sau un octet opțional de parametru de transfer (TRTP sau TREP);

— Sumă de verificare compusă dintr-un octet de sumă de verificare (CS).

Antet				Câmp de date					Sumă de verificare
FMT	TGT	SRC	LEN	SID	DATE	…	…	…	CS
4 octeți				Maximum 255 de octeți					1 octet

(*) Cardul introdus va declanșa drepturile corespunzătoare de acces la funcția de descărcare și la date. Datele pot fi totuși descărcate de pe un card de conducător auto introdus într-unul din sloturile VU atunci când în celălalt slot nu este introdus niciun alt tip de card.

Octetul TGT și octetul SRC reprezintă adresa fizică a destinatarului și a inițiatorului mesajului. Valorile sunt F0 Hex pentru IDE și EE Hex pentru VU.

Octetul LEN reprezintă lungimea câmpului de date.

Octetul de sumă de verificare este seria de sume de 8 biți modulo 256 a tuturor octeților din mesaj, cu excepția CS.

Octeții FMT, SID, DS_, TRTP și TREP sunt definiți în continuare în prezentul document.

DDP_003 În cazul în care datele pe care urmează să le transporte mesajul sunt mai lungi decât spațiul disponibil în câmpul de date, mesajul este transmis practic sub forma mai multor sub-mesaje. Fiecare sub-mesaj are un antet, același SID, TREP și un contor de sub-mesaje de 2 octeți care indică numărul de ordine al sub-mesajului în cadrul mesajului integral. Pentru a permite verificarea erorilor și un eventual abandon al schimbului de date, IDE confirmă fiecare sub-mesaj. IDE poate accepta sub-mesajul, poate solicita retransmiterea acestuia și poate solicita VU să reia sau să abandoneze transmisia.

DDP_004 Dacă ultimul sub-mesaj conține exact 255 de octeți în câmpul de date, trebuie să se adauge un sub-mesaj final cu un câmp de date gol (cu excepția SID, TREP și a contorului de sub-mesaje) pentru a indica sfârșitul mesajului.

Exemplu:

Antet	SID	TREP	Mesaj	CS
4 octeți	Cu o lungime de peste 255 de octeți			

Se transmite astfel:

Antet	SID	TREP	00	01	Sub-mesaj 1	CS
4 octeți	255 octeți					

Antet	SID	TREP	00	02	Sub-mesaj 2	CS
4 octeți	255 octeți					

…

Antet	SID	TREP	xx	yy	Sub-mesaj n	CS
4 octeți	Mai puțin de 255 de octeți					

sau astfel:

Antet	SID	TREP	00	01	Sub-mesaj 1	CS
4 octeți	255 octeți					

Antet	SID	TREP	00	02	Sub-mesaj 2	CS
4 octeți	255 octeți					

…

Antet	SID	TREP	xx	yy	Sub-mesaj n	CS
4 octeți	255 octeți					

Antet	SID	TREP	xx	yy + 1	CS
4 octeți	4 octeți				

2.2.2 *Tipuri de mesaje*

Protocolul de comunicare pentru descărcarea de date între VU și IDE impune schimbul a opt tipuri diferite de mesaje.

Aceste mesaje sunt prezentate în tabelul următor.

Structura mesajului	Maximum 4 octeți Antet				Maximum 255 de octeți Date			1 octet Sumă de verificare
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATE	CS
Solicitare de inițiere a comunicării	81	EE	F0		81			E0
Răspuns pozitiv la solicitarea de inițiere a comunicării	80	F0	EE	03	C1		EA, 8F	9B
Solicitare de începere a sesiunii de diagnosticare	80	EE	F0	02	10	81		F1
Răspuns pozitiv la solicitarea de începere a sesiunii de diagnosticare	80	F0	EE	02	50	81		31
Serviciul de control al legăturii Verificarea ratei de modulație (etapa 1)								
9 600 Bd	80	EE	F0	04	87		01,01, 01	EC
19 200 Bd	80	EE	F0	04	87		01,01, 02	ED
38 400 Bd	80	EE	F0	04	87		01,01, 03	EE
57 600 Bd	80	EE	F0	04	87		01,01, 04	EF
115 200 Bd	80	EE	F0	04	87		01,01, 05	F0
Răspuns pozitiv la o solicitare de verificare a ratei de modulație	80	F0	EE	02	C7		01	28
Rata de modulație de tranziție (etapa 2)	80	EE	F0	03	87		02,03	ED
Solicitare de încărcare	80	EE	F0	0 A	35		00,00, 00,00, 00,FF,FF, FF,FF	99
Răspuns pozitiv la solicitarea de încărcare	80	F0	EE	03	75		00,FF	D5

Structura mesajului	Maximum 4 octeți Antet				Maximum 255 de octeți Date			1 octet Sumă de verificare
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATE	CS
Solicitare de transfer de date								
Prezentare generală	80	EE	F0	02	36	01		97
Activități	80	EE	F0	06	36	02	Data	CS
Evenimente și anomalii	80	EE	F0	02	36	03		99
Viteză detaliată	80	EE	F0	02	36	04		9A
Date tehnice	80	EE	F0	02	36	05		9 B
Descărcarea informațiilor de pe card	80	EE	F0	02	36	06	Slot	CS
Răspuns pozitiv la solicitarea de transfer de date	80	F0	EE	Len	76	TREP	Date	CS
Solicitare de încheiere a transferului	80	EE	F0	01	37			96
Răspuns pozitiv la solicitarea de încheiere a transferului	80	F0	EE	01	77			D6
Solicitare de încheiere a comunicării	80	EE	F0	01	82			E1
Răspuns pozitiv la solicitarea de încheiere a comunicării	80	F0	EE	01	C2			21
Confirmare de primire a sub-mesajului	80	EE	F0	Len	83		Date	CS
Răspunsuri negative								
Respingere generală	80	F0	EE	03	7F	Sid Req	10	CS
Serviciu incompatibil	80	F0	EE	03	7F	Sid Req	11	CS
Subfuncție incompatibilă	80	F0	EE	03	7F	Sid Req	12	CS
Lungime incorectă a mesajului	80	F0	EE	03	7F	Sid Req	13	CS
Condiții incorecte sau eroare a secvenței de interogare	80	F0	EE	03	7F	Sid Req	22	CS
Solicitare în afara intervalului	80	F0	EE	03	7F	Sid Req	31	CS
Încărcare refuzată	80	F0	EE	03	7F	Sid Req	50	CS
Răspuns în așteptare	80	F0	EE	03	7F	Sid Req	78	CS
Datele nu sunt disponibile	80	F0	EE	03	7F	Sid Req	FA	CS

Note:

— Sid Req = Sid-ul solicitării corespunzătoare.

— TREP = TRTP-ul solicitării corespunzătoare.

— Rubricile marcate cu negru indică absența unei transmisii.

— Termenul „încărcare” (*upload*) (privit din perspectiva IDE) se folosește pentru a garanta compatibilitatea cu ISO 14229. Are aceeași semnificație ca și termenul „descărcare” (*download*) văzut din perspectiva VU.

— În acest tabel nu se găsește niciun contor potențial de sub-mesaje de 2 octeți.

— Slot este numărul slotului, fie „1” (card în slotul conducătorului auto), fie „2” (card în slotul copilotului)

— În cazul în care slotul nu este specificat, VU trebuie să selecteze slotul 1 dacă se introduce un card în slotul respectiv și să selecteze slotul 2 numai în cazul în care este ales în mod specific de către utilizator.

2.2.2.1 Solicitare de inițiere a comunicării (*Start Communication Request*)(SID 81)

DDP_005 Acest mesaj este emis de IDE în vederea inițierii legăturii de comunicare cu VU. Comunicările inițiale sunt efectuate întotdeauna la 9 600 de bauzi (până la eventuala schimbare a ratei de modulație cu ajutorul serviciilor adecvate de control al legăturii).

2.2.2.2 Răspuns pozitiv la solicitarea de inițiere a comunicării (*Positive Response Start Communication*)(SID C1)

DDP_006 Acest mesaj este emis de VU ca răspuns pozitiv la un mesaj de solicitare de inițiere a comunicării. Este compus din cei doi octeți cheie „EA" „8F" care indică faptul că unitatea este compatibilă cu protocolul în cauză și are un antet care include informații privind sursa, ținta și lungimea.

2.2.2.3 Solicitare de începere a sesiunii de diagnosticare (*Start Diagnostic Session Request*) (SID 10)

DDP_007 IDE emite un mesaj de solicitare de începere a sesiunii de diagnosticare (*Start Diagnostic Session request*) pentru a solicita o nouă sesiune de diagnosticare cu VU. Subfuncția „sesiune implicită" (81 Hex) indică faptul că urmează să înceapă o sesiune de diagnosticare standard.

2.2.2.4 Răspuns pozitiv la solicitarea de începere a sesiunii de diagnosticare (*Positive Response Start Diagnostic*)(SID 50)

DDP_008 Mesajul de răspuns pozitiv la solicitarea de începere a sesiunii de diagnosticare (*Positive Response Start Diagnostic*) este trimis de VU ca răspuns pozitiv la solicitarea de începere a sesiunii de diagnosticare (*Diagnostic Session Request*).

2.2.2.5 Serviciul de control al legăturii (*Link Control Service*) (SID 87)

DDP_052 Serviciul de control al legăturii este folosit de IDE pentru a iniția o schimbare a ratei de modulație. Acest lucru se realizează în două etape. În prima etapă, IDE propune schimbarea ratei de modulație, indicând rata nouă. La primirea mesajului cu răspuns pozitiv de la VU, IDE trimite confirmarea privind modificarea ratei de modulație la VU (etapa a doua). EID trece apoi la noua rată de modulație. După primirea confirmării, VU trece la noua rată de modulație.

2.2.2.6 Răspuns pozitiv la controlul legăturii (*Link Control Positive Response*) (SID C7)

DDP_053 Răspunsul pozitiv la controlul legăturii este emis de VU ca răspuns pozitiv la solicitarea serviciului de control al legăturii. A se remarca faptul că solicitarea de confirmare nu primește niciun răspuns (etapa a doua).

2.2.2.7 Solicitare de încărcare (*Request Upload*)(SID 35)

DDP_009 Mesajul de solicitare de încărcare (*Request Upload*) este emis de IDE pentru a indica VU faptul că s-a solicitat o operațiune de descărcare. Pentru a respecta cerințele standardului ISO 14229, sunt incluse date care se referă la adresă și la detalii privind dimensiunea și formatul datelor solicitate. Deoarece IDE nu cunoaște aceste date înainte de descărcare, adresa memoriei este setată la 0, formatul este necriptat și necomprimat, iar dimensiunea memoriei este setată la valoarea maximă.

2.2.2.8 Răspuns pozitiv la solicitarea de încărcare (*Positive Response Request Upload*) (SID 75)

DDP_010 Mesajul de răspuns pozitiv la solicitarea de încărcare este trimis de VU pentru a indica IDE faptul că VU este pregătită pentru descărcarea datelor. Pentru a respecta cerințele standardului ISO 14229, în acest mesaj privind răspunsul pozitiv sunt incluse date care indică IDE că următoarele mesaje de răspuns pozitiv la solicitarea de transfer de date (*Positive Response Transfer Data*) vor fi compuse din maximum 00FF hex octeți.

2.2.2.9 Solicitare de transfer de date (*Transfer Data Request*) (SID 36)

DDP_011 Solicitarea de transfer de date (*Transfer Data Request*) este trimisă de EID pentru a indica VU tipul de date care urmează să fie descărcate. Un parametru de solicitare de transfer (TRTP) de un octet indică tipul transferului.

Există șase tipuri de transfer de date:

— Prezentare generală (*Overview*) (TRTP 01),

— Activitățile de la o anumită dată (*Activities of a specified date*) (TRTP 02),

— Evenimente și anomalii (*Events and faults*) (TRTP 03),

— Viteza detaliată (*Detailed speed*) (TRTP 04),

— Date tehnice (*Technical data*) (TRTP 05),

— Descărcarea informațiilor de pe card (*Card download*) (TRTP 06).

DDP_054 Este obligatoriu pentru IDE să solicite un transfer de date de prezentare generală (TRTP 01) în timpul unei sesiuni de descărcare, deoarece este singurul lucru care garantează înregistrarea certificatelor VU în fișierul descărcat (și permite verificarea semnăturii digitale).

În al doilea caz (TRTP 02) mesajul de solicitare de transfer de date (*Transfer Data Request*) include indicația zilei calendaristice (format `TimeReal`) care urmează să fie descărcată.

2.2.2.10 Răspuns pozitiv la solicitarea de transfer de date (*Positive Response Transfer Data*) (SID 76)

DDP_012 Mesajul de răspuns pozitiv la solicitarea de transfer de date (*Positive Response Transfer Data*) este trimis de VU ca răspuns la solicitarea de transfer de date (*Transfer Data Request*). Mesajul conține datele solicitate, cu un *Transfer Response Parameter* (TREP) corespunzător TRTP-ului solicitării.

DDP055 În primul caz (TREP 01), VU trimite datele care să poată ajuta operatorul IDE în alegerea datelor pe care dorește să le descarce în continuare. Informațiile incluse în acest mesaj sunt reprezentate de:

— certificate de securitate,

— identificarea vehiculului,

— data și ora actuale pentru VU,

— data de descărcare minimă și maximă (date VU),

— indicații privind prezența cardurilor în VU,

— descărcarea precedentă către o societate,

— blocări executate de societăți,

— controale anterioare.

2.2.2.11 Solicitare de încheiere a transferului (*Request Transfer Exit*) (SID 37)

DDP_013 Mesajul de solicitare de încheiere a transferului este trimis de IDE pentru a informa VU că sesiunea de descărcare s-a încheiat.

2.2.2.12 Răspuns pozitiv la solicitarea de încheiere a transferului (SID 77) (*Positive Response Request Transfer Exit*)

DDP_014 Mesajul de răspuns pozitiv la solicitarea de încheiere a transferului (*Positive Response Request Transfer Exit)* este trimis de VU pentru a confirma primirea mesajului de solicitare de încheiere a transferului.

2.2.2.13 Solicitare de încheiere a comunicării (*Stop Communication Request*) (SID 82)

DDP_015 Mesajul de solicitare de încheiere a comunicării *(Stop Communication Request)* este trimis de IDE cu scopul de a întrerupe legătura de comunicare cu VU.

2.2.2.14 Răspuns pozitiv la solicitarea de încheiere a comunicării (*Positive Response Stop Communication*) (SID C2)

DDP_016 Mesajul de răspuns pozitiv la solicitarea de încheiere a comunicării *(Positive Response Stop Communication)* este trimis de VU pentru a confirma primirea mesajului *Stop Communication Request*.

2.2.2.15 Confirmare de primire a sub-mesajului (*Acknowledge Sub Message*) (SID 83)

DDP_017 Confirmarea de primire a sub-mesajului *(Acknowledge Sub Message)* este trimis de IDE pentru a confirma primirea fiecărei părți a unui mesaj care este transmis prin intermediul mai multor sub-mesaje. Câmpul de date conține SID primit de la VU și un cod de 2 octeți după cum urmează:

— MsgC + 1 Confirmă primirea corectă a sub-mesajului cu numărul MsgC.

Solicitare din partea IDE către VU pentru a transmite sub-mesajul următor

— MsgC indică apariția unei probleme la primirea sub-mesajului cu numărul MsgC.

Solicitare din partea IDE către VU de a transmite sub-mesajul din nou

— FFFF solicită întreruperea mesajului aflat în curs de transmitere.

IDE poate folosi acest cod pentru a întrerupe transmiterea mesajului VU, indiferent de motiv.

Primirea ultimului sub-mesaj al unui mesaj (octetul LEN < 255) poate fi confirmată cu ajutorul unuia dintre aceste coduri sau poate să nu fie confirmată.

Răspunsurile din partea VU compuse din câteva sub-mesaje sunt:

— Răspuns pozitiv la solicitarea de transfer de date (*Positive Response Transfer Data*) (SID 76)

2.2.2.16 Răspuns negativ (*Negative Response*) (SID 7F)

DDP_018 Mesajul de răspund negativ (*Negative Response)* este trimis de VU ca răspuns la mesajele de solicitare menționate anterior în cazul în care VU nu poate da curs solicitării. Câmpurile de date ale mesajului conțin SID-ul răspunsului (7F), SID-ul solicitării și un cod care precizează motivul răspunsului negativ. Sunt disponibile următoarele coduri:

— 10 respingere generală

Acțiunea nu poate fi realizată dintr-un motiv care nu este menționat în continuare.

— 11 serviciu incompatibil

SID-ul solicitării nu poate fi înțeles.

— 12 subfuncție incompatibilă

DS_ sau TRTP al solicitării nu poate fi înțeles sau nu mai există alte sub-mesaje de transmis.

— 13 lungime incorectă a mesajului

Lungimea mesajului primit este incorectă.

— 22 condiții incorecte sau eroare a secvenței de interogare

Serviciul solicitat nu este activ sau secvența mesajelor de solicitare nu este corectă.

— 31 solicitare în afara intervalului

Înregistrarea parametrului solicitării (câmpul de date) nu este valabilă.

— 50 încărcare refuzată

Solicitarea nu poate fi executată (VU nu se află în modul de funcționare corespunzător sau există o anomalie internă a VU).

— 78 răspuns în așteptare

Acțiunea solicitată nu poate fi finalizată în timp util și VU nu este pregătită să accepte o nouă solicitare.

— FA datele nu sunt disponibile

Obiectul de date al unei solicitări de transfer de date nu este disponibil în VU (de exemplu, cardul nu este inserat, …)

2.2.3 *Fluxul mesajelor*

Pe parcursul unei proceduri normale de descărcare de date, un flux de mesaje tipic se efectuează de obicei astfel:

IDE		VU
Solicitare de inițiere a comunicării	⇨	
	⇦	Răspuns pozitiv
Solicitare de inițiere a serviciului de diagnosticare	⇨	
	⇦	Răspuns pozitiv
Solicitare de încărcare	⇨	
	⇦	Răspuns pozitiv

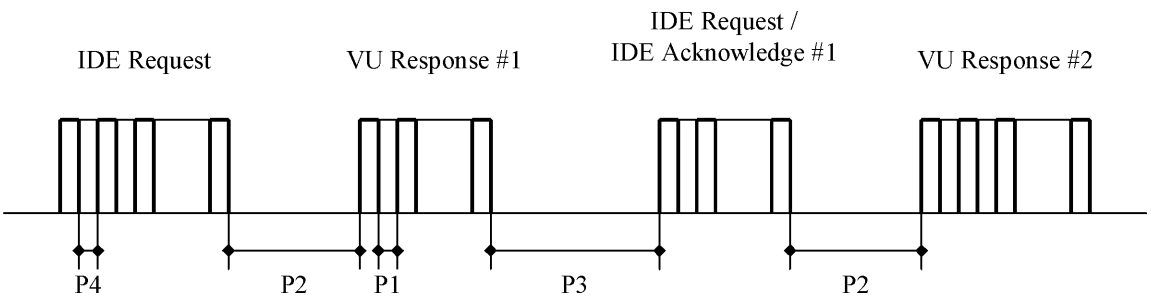
IDE		VU
Solicitare de transfer de date de prezentare generală	⇨	
	⇦	Răspuns pozitiv
Solicitare de transfer de date #2	⇨	
	⇦	Răspuns pozitiv #1
Confirmare de primire a sub-mesajului #1	⇨	
	⇦	Răspuns pozitiv #2
Confirmare de primire a sub-mesajului #2	⇨	
	⇦	Răspuns pozitiv #m
Confirmare de primire a sub-mesajului #m	⇨	
	⇦	Răspuns pozitiv (Câmp de date <255 de octeți)
Confirmare de primire a sub-mesajului (opțional)	⇨	
…		
Solicitare de transfer de date #n	⇨	
	⇦	Răspuns pozitiv
Solicitare de încheiere a transferului	⇨	
	⇦	Răspuns pozitiv
Solicitare de încheiere a comunicării	⇨	
	⇦	Răspuns pozitiv

2.2.4 *Sincronizare*

DDP_019 În condiții de funcționare normale, se aplică parametrii de sincronizare indicați în figura următoare:

Figura 1

Fluxul mesajelor, sincronizare



Unde:

P1 = Timp interoctet pentru răspunsul VU.

P2 = Interval de timp între încheierea solicitării IDE și începerea răspunsului VU sau între încheierea confirmării de primire a IDE și începerea următorului răspuns al VU.

P3 = Interval de timp între încheierea răspunsului VU și începerea noii solicitări a IDE sau între încheierea răspunsului VU și începerea confirmării de primire a IDE sau între încheierea solicitării IDE și începerea noii solicitări a IDE dacă VU nu reușește să răspundă.

P4 = Interval de timp interoctet pentru solicitarea IDE.

P5 = Valoarea extinsă a P3 pentru descărcarea informațiilor de pe card.

Valorile permise pentru parametrii de sincronizare sunt indicate în tabelul următor (setul de parametri de sincronizare extinși KWP folosiți în caz de adresare fizică pentru o comunicare mai rapidă).

Parametru sincronizare	Limita inferioară Valoare (ms)	Limita superioară Valoare (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 de minute

(*) dacă VU răspunde cu un răspuns negativ (*Negative Response*) care conține un cod cu sensul de „solicitare primită corect, răspuns în așteptare”, această valoare este extinsă până la aceeași valoare a limitei superioare a P3.

2.2.5 *Gestionarea erorilor*

Dacă o eroare intervine în timpul schimbului de mesaje, schema fluxului de mesaje se modifică în funcție de echipamentul care a detectat eroarea și de mesajul care a generat eroarea.

În figura 2 și în figura 3 sunt prezentate procedurile de gestionare a erorilor folosite de VU și, respectiv, de IDE.

2.2.5.1 Etapa de inițiere a comunicării

DDP_020 Dacă IDE detectează o eroare în timpul etapei de inițiere a comunicării, fie la nivelul sincronizării, fie la nivelul fluxului de biți, așteaptă o perioadă de P3min înainte de a emite din nou solicitarea.

DDP_021 Dacă VU detectează o eroare în secvența primită de la IDE, nu trimite niciun răspuns și așteaptă un alt mesaj de solicitare de inițiere a comunicării (*Start Communication Request*) timp de P3 max.

2.2.5.2 Etapa de comunicare

Pot fi definite două proceduri diferite de gestionare a erorilor:

1. **VU detectează o eroare de transmisie a IDE**

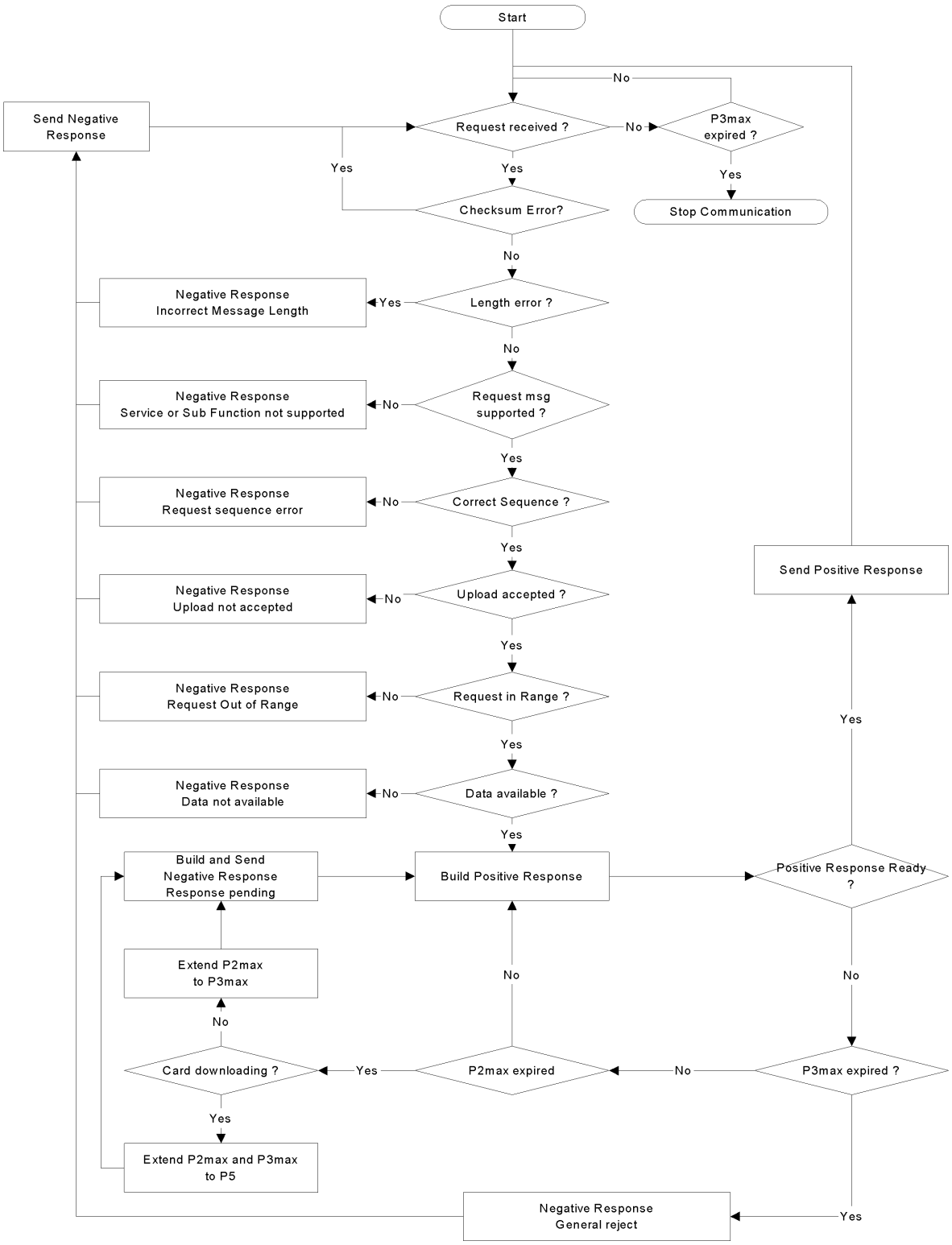
DDP_022 VU analizează fiecare mesaj primit pentru a detecta erori de sincronizare, erori de format al octeților (de exemplu, încălcări ce afectează biții de pornire și oprire) și erori de cadru (primirea unui număr greșit de octeți, octet de sumă de verificare eronat).

DDP_023 Dacă VU detectează una dintre erorile menționate anterior, nu trimite niciun răspuns și ignoră mesajul primit.

DDP_024 VU poate detecta alte erori ale formatului sau conținutului mesajului primit (de exemplu, mesaj incompatibil) chiar dacă mesajul respectă cerințele de lungime și de sumă de verificare; în acest caz, VU răspunde IDE cu un mesaj de răspuns negativ (*Negative Response*), indicând tipul erorii.

Figura 2

Gestionarea erorilor de către VU



2. **IDE detectează o eroare de transmisie a VU**

DDP_025 IDE analizează fiecare mesaj primit pentru a detecta erori de sincronizare, erori de format al octeților (de exemplu, încălcări ce afectează biții de pornire și oprire) și erori de cadru (primirea unui număr greșit de octeți, octet de sumă de verificare eronat).

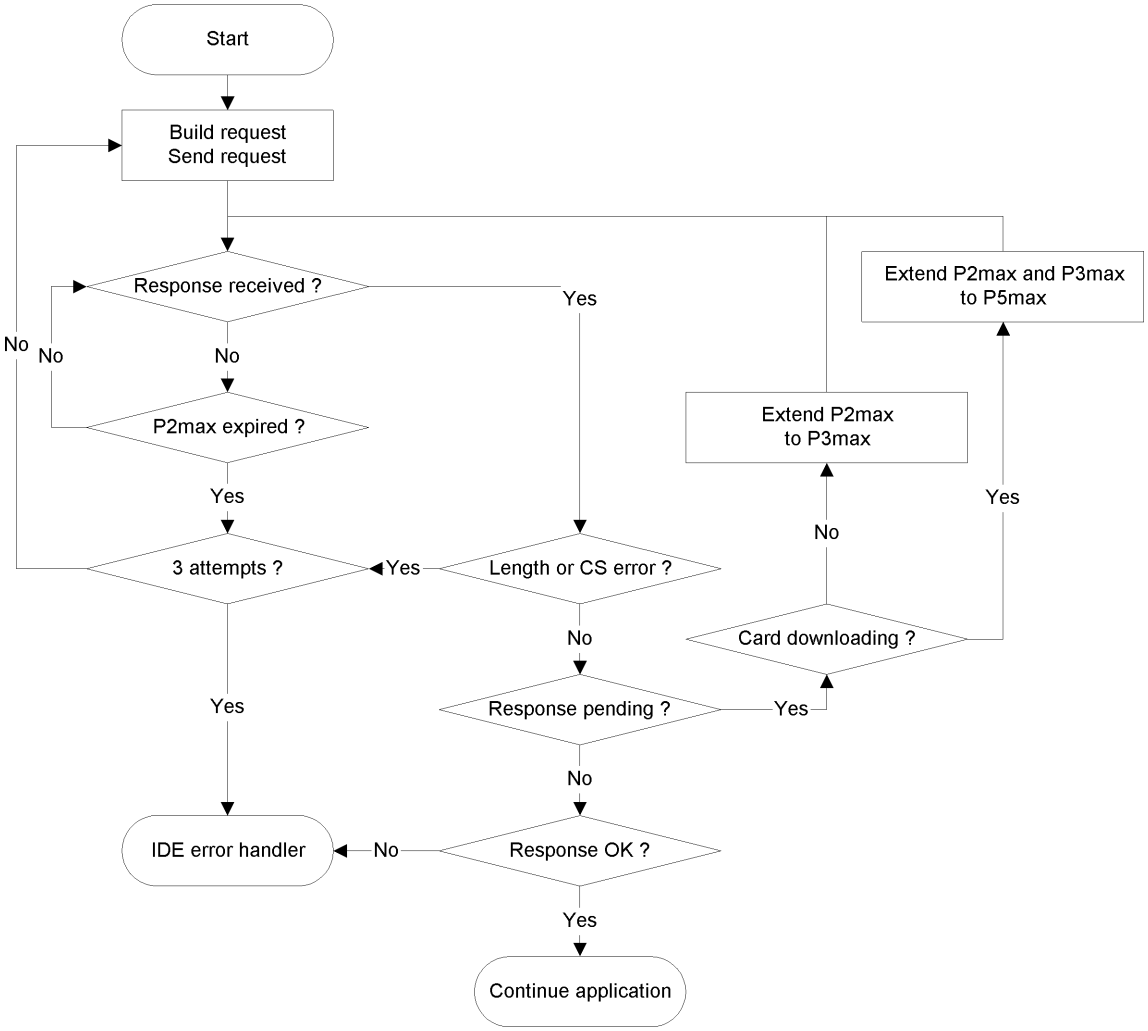
DDP_026 IDE detectează erorile de secvență, de exemplu incrementări greșite ale contorului de sub-mesaje în mesajele succesive primite.

DDP_027 Dacă IDE detectează o eroare sau dacă nu primește niciun răspuns de la VU într-o perioadă P2max, mesajul de solicitare este transmis din nou de cel mult trei ori. În scopul detectării acestei erori, o confirmare de primire a sub-mesajului este considerată a fi o solicitare adresată VU.

DDP_028 IDE așteaptă o perioadă de P3min înainte de începerea fiecărei transmisii; perioada de așteptare se măsoară de la ultima apariție calculată a unui bit de oprire după detectarea erorii în cauză.

Figura 3

Gestionarea erorilor de către IDE



2.2.6 *Conținutul mesajelor de răspuns*

La acest punct este prezentat conținutul câmpurilor de date ale diferitelor mesaje de răspuns pozitiv.

Elementele de date sunt definite în dicționarul de date din apendicele 1.

Observație: Pentru descărcări de generația 2, fiecare element de date de nivel superior este reprezentat de o colecție de înregistrări, chiar și în cazul în care aceasta conține numai o singură înregistrare. O colecție de înregistrări începe cu un antet; acest antet conține tipul de înregistrări, dimensiunea înregistrărilor și numărul de înregistrări. Colecțiile de înregistrări sunt denumite „... *RecordArray*” (cu antet) în următoarele tabele.

2.2.6.1 Răspuns pozitiv la solicitarea de transfer de date de prezentare generală (*Positive Response Transfer Data Overview*)

DDP_029 Câmpul de date al mesajului de răspuns pozitiv la solicitarea de transfer de date de prezentare generală („*Positive Response Transfer Data Overview*") furnizează următoarele date în ordinea prezentată mai jos în conformitate cu SID 76 Hex, TREP 01 Hex și criteriile adecvate de separare și numărare a sub-mesajelor:

Structura datelor generația 1

Element de date	Observații
MemberStateCertificate VUCertificate	Certificate de securitate VU
VehicleIdentificationNumber VehicleRegistrationIdentification	Identificarea vehiculului
CurrentDateTime	Data și ora actuale pentru VU
VuDownloadablePeriod	Perioada care poate fi descărcată
CardSlotsStatus	Tipuri de carduri introduse în VU
VuDownloadActivityData	Descărcare anterioară VU
VuCompanyLocksData	Toate blocările executate de societăți și stocate. Dacă secțiunea nu conține date, se trimite numai noOfLocks = 0.
VuControlActivityData	Toate înregistrările activităților de control stocate în VU. Dacă secțiunea nu conține date, se trimite numai noOfControls = 0.
Signature	Semnătura RSA a tuturor datelor (cu excepția certificatelor), începând cu VehicleIdentificationNumber până la ultimul octet din ultima VuControlActivityData.

Structura datelor generația 2

Element de date	Observații
MemberStateCertificateRecordArray	Certificatul statului membru
VUCertificateRecordArray	Certificatul VU
VehicleIdentificationNumberRecordArray	Identificarea vehiculului
VehicleRegistrationNumberRecordArray	Numărul de înmatriculare al vehiculului
CurrentDateTimeRecordArray	Data și ora actuale pentru VU
VuDownloadablePeriodRecordArray	Perioada care poate fi descărcată
CardSlotsStatusRecordArray	Tipuri de carduri introduse în VU
VuDownloadActivityDataRecordArray	Descărcare anterioară VU
VuCompanyLocksRecordArray	Toate blocările executate de societăți și stocate. Dacă secțiunea nu conține date, se trimite un antet cu noOfRecords = 0.
VuControlActivityRecordArray	Toate înregistrările activităților de control stocate în VU. Dacă secțiunea nu conține date, se trimite un antet cu noOfRecords = 0.
SignatureRecordArray	Semnătura ECC a tuturor datelor precedente, cu excepția certificatelor.

2.2.6.2 Răspuns pozitiv la solicitarea de transfer de date privind activitățile (*Positive Response Transfer Data Activities*)

DDP_030 Câmpul de date al mesajului de răspuns pozitiv la solicitarea de transfer de date privind activitățile („*Positive Response Transfer Data Activities*") furnizează următoarele date în ordinea prezentată mai jos în conformitate cu SID 76 Hex, TREP 02 Hex și criteriile adecvate de separare și numărare a sub-mesajelor:

Structura datelor generația 1

Element de date	Observații
TimeReal	Data zilei descărcate
OdometerValueMidnight	Odometrul la sfârșitul zilei descărcate
VuCardIWData	Date privind ciclurile de introducere și de retragere a cardurilor. — Dacă această secțiune nu conține date disponibile, se trimite numai noOfVuCardIWRecords = 0. — Atunci când VuCardIWRecord conține date înregistrate înainte de ora 00.00 (introducerea cardului în ziua anterioară) sau după ora 24.00 (retragerea cardului în ziua următoare), aceste înregistrări apar integral în cele două zile implicate.
VuActivityDailyData	Starea sloturilor la 00:00 și modificările de activitate înregistrate pentru ziua descărcată.
VuPlaceDailyWorkPeriodData	Date privind locurile, înregistrate pentru ziua descărcată. Dacă secțiunea nu conține date, se trimite numai noOfPlaceRecords = 0.
VuSpecificConditionData	Date privind condițiile specifice, înregistrate pentru ziua descărcată. Dacă secțiunea nu conține date, se trimite numai noOfSpecificConditionRecords = 0.
Signature	Semnătura RSA a tuturor datelor, începând de la TimeReal până la ultimul octet din ultima înregistrare privind condițiile specifice.

Structura datelor generația 2:

Element de date	Observații
DateOfDayDownloadedRecordArray	Data zilei descărcate
OdometerValueMidnightRecordArray	Odometrul la sfârșitul zilei descărcate
VuCardIWRecordArray	Date privind ciclurile de introducere și de retragere a cardurilor. — Dacă această secțiune nu conține date disponibile, se trimite un antet al colecției cu noOfRecords = 0. — Atunci când VuCardIWRecord conține date înregistrate înainte de ora 00.00 (introducerea cardului în ziua anterioară) sau după ora 24.00 (retragerea cardului în ziua următoare), aceste înregistrări apar integral în cele două zile implicate.
VuActivityDailyRecordArray	Starea sloturilor la 00:00 și modificările de activitate înregistrate pentru ziua descărcată.
VuPlaceDailyWorkPeriodRecordArray	Date privind locurile, înregistrate pentru ziua descărcată. Dacă secțiunea nu conține date, se trimite un antet al colecției cu noOfRecords = 0.
VuGNSSCDRecordArray	Pozițiile GNSS ale vehiculului dacă timpul de conducere continuă al conducătorului auto atinge un multiplu de trei ore. Dacă secțiunea nu conține date, se trimite un antet al colecției cu noOfRecords = 0.
VuSpecificConditionRecordArray	Date privind condițiile specifice, înregistrate pentru ziua descărcată. Dacă secțiunea nu conține date, se trimite un antet al colecției cu noOfRecords = 0.
SignatureRecordArray	Semnătura ECC a tuturor datelor precedente.

2.2.6.3 Răspuns pozitiv la solicitarea de transfer de date privind evenimentele și anomaliile (*Positive Response Transfer Data Events and Faults*)

DDP_031 Câmpul de date al mesajului de răspuns pozitiv la solicitarea de transfer de date privind evenimentele și anomaliile („*Positive Response Transfer Data Events and Faults*") furnizează următoarele date în ordinea prezentată mai jos în conformitate cu SID 76 Hex, TREP 03 Hex și criteriile adecvate de separare și numărare a sub-mesajelor:

Structura datelor generația 1

Element de date	Observații
VuFaultData	Toate anomaliile stocate sau curente în VU. Dacă secțiunea nu conține date, se trimite numai noOfVuFaults = 0.
VuEventData	Toate evenimentele (cu excepția depășirii limitei de viteză) stocate sau în curs în VU. Dacă secțiunea nu conține date, se trimite numai noOfVuEvents = 0.
VuOverSpeedingControlData	Date referitoare la ultimul control privind depășirea limitei de viteză (valoare implicită în lipsa datelor).
VuOverSpeedingEventData	Toate evenimentele de depășire a limitei de viteză stocate în VU. Dacă secțiunea nu conține date, se trimite numai noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Toate evenimentele de reglare a orei stocate în VU (în afara cadrului unei etalonări complete). Dacă secțiunea nu conține date, se trimite numai noOfVuTimeAdjRecords = 0.
Signature	Semnătura RSA a tuturor datelor, începând cu noOfVuFaults până la ultimul octet din ultima înregistrare privind reglarea orei.

Structura datelor generația 2:

Element de date	Observații
VuFaultRecordArray	Toate anomaliile stocate sau curente în VU. Dacă secțiunea nu conține date, se trimite un antet al colecției cu noOfRecords = 0.
VuEventRecordArray	Toate evenimentele (cu excepția depășirii limitei de viteză) stocate sau în curs în VU. Dacă secțiunea nu conține date, se trimite un antet al colecției cu noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Date referitoare la ultimul control privind depășirea limitei de viteză (valoare implicită în lipsa datelor).
VuOverSpeedingEventRecordArray	Toate evenimentele de depășire a limitei de viteză stocate în VU. Dacă secțiunea nu conține date, se trimite un antet al colecției cu noOfRecords = 0.
VuTimeAdjustmentRecordArray	Toate evenimentele de reglare a orei stocate în VU (în afara cadrului unei etalonări complete). Dacă secțiunea nu conține date, se trimite un antet al colecției cu noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Semnătura ECC a tuturor datelor precedente.

2.2.6.4 Răspuns pozitiv la solicitarea de transfer de date privind viteza detaliată (*Positive Response Transfer Data Detailed Speed*)

DDP_032 Câmpul de date al mesajului de răspuns pozitiv la solicitarea de transfer de date privind viteza detaliată („*Positive Response Transfer Data Detailed Speed*") furnizează următoarele date în ordinea prezentată mai jos în conformitate cu SID 76 Hex, TREP 04 Hex și criteriile adecvate de separare și numărare a sub-mesajelor:

Structura datelor generația 1

Element de date	Observații
VuDetailedSpeedData	Toate datele privind viteza detaliată stocate în VU (un bloc de viteze pentru fiecare minut în timpul căruia vehiculul a fost în mișcare) 60 valori ale vitezei pe minut (una pe secundă).
Signature	Semnătura RSA a tuturor datelor, începând cu noOfSpeedBlocks până la ultimul octet din ultimul bloc de viteze.

Structura datelor generația 2:

Element de date	Observații
VuDetailedSpeedBlockRecordArray	Toate datele privind viteza detaliată stocate în VU (un bloc de viteze pentru fiecare minut în timpul căruia vehiculul a fost în mișcare) 60 valori ale vitezei pe minut (una pe secundă).
SignatureRecordArray	Semnătura ECC a tuturor datelor precedente.

2.2.6.5 Răspuns pozitiv la solicitarea de transfer de date tehnice (*Positive Response Transfer Data Technical Data*)

DDP_033 Câmpul de date al mesajului de răspuns pozitiv la solicitarea de transfer de date tehnice („*Positive Response Transfer Data Technical Data*") furnizează următoarele date în ordinea prezentată mai jos în conformitate cu SID 76 Hex, TREP 05 Hex și criteriile adecvate de separare și numărare a sub-mesajelor:

Structura datelor generația 1

Element de date	Observații
VuIdentification	
SensorPaired	
VuCalibrationData	Toate înregistrările activităților de etalonare stocate în VU.
Signature	Semnătura RSA a tuturor datelor, începând cu vuManufacturerName până la ultimul octet din ultimul VuCalibrationRecord.

Structura datelor generația 2:

Element de date	Observații
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Toate asocierile MS stocate în VU.
VuSensorExternalGNSSCoupledRecordArray	Toate cuplările echipamentului GNSS extern stocate în VU.
VuCalibrationRecordArray	Toate înregistrările activităților de etalonare stocate în VU.
VuCardRecordArray	Toate datele referitoare la introducerea cardurilor stocate în VU.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Semnătura ECC a tuturor datelor precedente.

2.3. **Stocarea fișierelor în ESM**

DDP_034 Dacă o sesiune de descărcare a inclus un transfer de date de pe VU, IDE stochează într-un singur fișier fizic toate datele primite de la VU în timpul sesiunii de descărcare în mesajele de răspuns pozitiv la solicitarea de transfer de date. Datele stocate nu includ anteturi de mesaje, contoare de sub-mesaje, sub-mesaje fără date și sume de verificare, dar includ SID și TREP (din primul sub-mesaj, numai dacă există mai multe sub-mesaje).

3. PROTOCOL DE DESCĂRCARE DE PE CARDURILE DE TAHOGRAF

3.1. **Domeniu de aplicare**

Acest punct cuprinde o descriere a descărcării datelor de pe un card de tahograf pe un IDE. IDE nu face parte din mediul securizat; prin urmare, nu se realizează nicio procedură de autentificare între card și IDE.

3.2. **Definiții**

Sesiune de descărcare: De fiecare dată când se efectuează o operațiune de descărcare de date de pe ICC. Sesiunea include întreaga procedură, de la resetarea ICC cu ajutorul unui IFD până la dezactivarea ICC (retragerea cardului sau următoarea resetare).

Fișier de date semnat: Un fișier din ICC. Fișierul este transferat în IFD sub formă de text în clar. Pe ICC fișierul este supus funcției hash și semnat, iar semnătura este transferată la IFD.

3.3. **Descărcarea informațiilor de pe card**

DDP_035 Descărcarea de pe un card de tahograf include următoarele etape:

— Descărcarea informațiilor comune stocate pe card în fișierele elementare (EF) `ICC` și `IC`. Aceste informații sunt opționale și nu sunt protejate de o semnătură digitală.

— Descărcarea fișierelor elementare (EF) `Card_Certificate` (ori `CardSignCertificate`) și `CA_Certificate`. Aceste informații nu sunt protejate de o semnătură digitală.

Descărcarea acestor fișiere este obligatorie în cadrul fiecărei sesiuni de descărcare.

— Descărcarea celorlalte EF de date privind aplicația (în `Tachograph DF` și `Tachograph_G2 DF` dacă este relevant), cu excepția EF `Card_Download`. Aceste informații sunt protejate de o semnătură digitală.

— Este obligatoriu să se descarce cel puțin EF `Application_Identification` și `ID` pentru fiecare sesiune de descărcare.

— La descărcarea de pe cardul de conducător auto, descărcarea următoarelor EF este obligatorie:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- GNSS_Places (if relevant),
- Control_Activity_Data,
- Specific_Conditions.

— La descărcarea de pe un card al conducătorului auto, se impune actualizarea datei LastCardDownload în EF Card_Download.

— La descărcarea de pe un card de atelier, se impune resetarea contorului de etalonare în EF Card_Download.

— La descărcarea de pe un card de atelier, nu se descarcă EF Sensor_Installation_Data.

3.3.1 *Secvența de inițializare*

DDP_036 IDE inițiază secvența după cum urmează:

Card	Direcție	IDE/IFD	Semnificație/Observații
	⇦	Resetare hardware	
ATR	⇨		

Opțional, se poate folosi PPS pentru a trece la o rată de modulație mai mare dacă ICC este compatibil.

3.3.2 *Secvența de descărcare de fișiere de date nesemnate*

DDP_037 Secvența de descărcare a EF ICC, IC, Card_Certificate (sau CardSignCertificate) și CA_Certificate este următoarea:

Card	Direcție	IDE/IFD	Semnificație/Observații
	⇦	**Select file**	Selectează în funcție de identificatorii fișierelor
OK	⇨		
	⇦	**Read Binary**	Dacă fișierul conține mai multe date decât dimensiunea zonei tampon a cititorului sau a cardului, comanda trebuie repetată până la citirea integrală a datelor din fișier.
Arhivare date (*File Data*) **OK**	⇨	Stocarea datelor în ESM	în conformitate cu **3.4** Formatul de stocare a datelor

Nota 1: Înainte de a selecta *Card_Certificate* (ori *CardSignCertificate) EF*, trebuie să selectați aplicația de tahograf (selecție cu AID).

Nota 2: Selectarea și citirea unui fișier poate fi efectuată, de asemenea, într-o singură etapă cu ajutorul unei comenzi de citire a datelor (*Read Binary*) cu un identificator EF scurt.

3.3.3 *Secvența de descărcare de fișiere de date semnate*

DDP_038 Următoarea secvență se folosește pentru fiecare dintre fișierele următoare care trebuie descărcate împreună cu semnătura lor:

Card	Dir	IDE/IFD	Semnificație/Observații
	⇦	**Selecționează fișierul**	
OK	⇨		
	⇦	**Efectuează *Hash of File***	Calculează valoarea hash în raport cu conținutul de date al fișierului selectat cu ajutorul algoritmului de *hashing* indicat în conformitate cu apendicele 11. Această comandă nu este o comandă conform *ISO*.
Se calculează *Hash of File* și se stochează temporar valoarea hash			
OK	⇨		
	⇦	**Read Binary**	Dacă fișierul conține mai multe date decât poate să stocheze zona tampon a cititorului sau a cardului, comanda trebuie repetată până la citirea integrală a datelor din fișier.
Arhivare date (*File Data*) **OK**	⇨	Stochează datele primite în ESM	în conformitate cu **3.4** Formatul de stocare a datelor
	⇦	**PSO: Compute Digital Signature**	
Execută operațiunea de securitate „Calcularea semnăturii digitale” cu ajutorul valorii hash stocate temporar			
Semnătură **OK**	⇨	Adaugă date la datele stocate anterior în ESM	în conformitate cu **3.4** Formatul de stocare a datelor

Notă: Selectarea și citirea unui fișier poate fi efectuată, de asemenea, într-o singură etapă cu ajutorul unei comenzi de citire a datelor (*Read Binary*) cu un identificator EF scurt. În acest caz, EF poate fi selectat și citit înainte de a fi aplicată comanda Efectuează *Hash of File*.

3.3.4 *Secvența de resetare a unui contor de etalonare.*

DDP_039 Secvența de resetare a contorului `NoOfCalibrationsSinceDownload` din EF `Card_Download` al unui card de atelier se prezintă după cum urmează:

Card	Dir	IDE/IFD	Semnificație/Observații
	⇦	**Select File** EF Card_Download	Selectează în funcție de identificatorii fișierelor
OK	⇨		

Card	Dir	IDE/IFD	Semnificație/Observații
	⇦	**Update Binary** NoOfCalibrationsSince-Download = '00 00'	
Resetează numărul de descărcări de pe card			
OK	⇨		

Notă: Selectarea și actualizarea unui fișier poate fi efectuată, de asemenea, într-o singură etapă cu ajutorul unei comenzi *Update Binary* cu un identificator EF scurt.

3.4. Formatul de stocare a datelor

3.4.1 *Introducere*

DDP_040 Datele descărcate trebuie stocate în conformitate cu următoarele condiții:

— Stocarea datelor trebuie să fie transparentă. Acest lucru înseamnă că, pe parcursul stocării, trebuie să se mențină ordinea octeților, precum și ordinea biților din interiorul octeților care sunt transferați de pe card.

— Toate fișierele de pe card descărcate în cadrul unei sesiuni de descărcare sunt stocate într-un singur fișier în ESM.

3.4.2 *Formatul fișierului*

DDP_041 Formatul fișierului este o concatenare a mai multor obiecte TLV.

DDP_042 Eticheta pentru un EF este FID însoțit de apendicele „00”.

DDP_043 Eticheta pentru o semnătură a EF este FID al fișierului însoțit de apendicele „01”.

DDP_044 Lungimea este o valoare de 2 octeți. Valoarea definește numărul de octeți din câmpul de valori. Valoarea „FF FF” din câmpul de lungime este rezervată pentru o utilizare viitoare.

DDP_045 Dacă un fișier nu este descărcat, nu se stochează nicio informație privind fișierul (nicio etichetă și nicio lungime zero).

DDP_046 O semnătură trebuie salvată drept următorul obiect TLV imediat după obiectul TLV care conține datele fișierului.

Definiție	Sens	Lungime
FID (2 octeți) || '00'	Eticheta pentru EF (FID)	3 octeți
FID (2 octeți) || '01'	Eticheta pentru semnătura EF (FID)	3 octeți
xx xx	Lungimea câmpului de valori	2 octeți

Exemplu de date dintr-un fișier de descărcare de pe o ESM:

Etichetă	Lungime	Valoare
00 02 00	00 11	Date din EF ICC
C1 00 00	00 C2	Date din EF Card_Certificate
		…
05 05 00	0A 2E	Date din EF Vehicles_Used
05 05 01	00 80	Semnătura EF Vehicles_Used

4. DESCĂRCAREA INFORMAȚIILOR DE PE UN CARD DE TAHOGRAF PRIN INTERMEDIUL UNEI UNITĂȚI MONTATE PE VEHICUL

DDP_047 VU trebuie să permită descărcarea conținutului unui card de conducător auto introdus într-un IDE conectat.

DDP_048 IDE trimite un mesaj de solicitare de transfer de date privind descărcarea informațiilor de pe card („*Transfer Data Request Card Download*") către VU pentru a iniția acest mod (a se vedea 2.2.2.9).

DDP_049 VU descarcă apoi integral cardul, fișier cu fișier, în conformitate cu protocolul de descărcare definit la punctul 3, și trimite toate datele primite de pe card către IDE în formatul de fișier TLV adecvat (a se vedea 3.4.2) și încapsulate într-un mesaj de răspuns pozitiv la solicitarea de transfer de date („*Positive Response Transfer Data*").

DDP_050 IDE preia datele de pe card din mesajul de răspuns pozitiv la solicitarea de transfer de date („*Positive Response Transfer Data*") (eliminând toate anteturile, SID-urile, TREP-urile contoarele de sub-mesaje și sumele de verificare) și le stochează într-un singur fișier fizic conform descrierii de la punctul 2.3.

DDP_051 În continuare, VU actualizează, dacă este cazul, fișierul `Control_Activity_Data` sau `Card_Download` de pe cardul conducătorului auto.

Apendicele 8

PROTOCOL DE ETALONARE

CUPRINS

1. INTRODUCERE 283

2. TERMENI, DEFINIȚII ȘI REFERINȚE 283

3. PREZENTARE GENERALĂ A SERVICIILOR 284

3.1. Servicii disponibile 284

3.2. Coduri de răspuns 285

4. SERVICII DE COMUNICARE 285

4.1. Serviciul StartCommunication 285

4.2. Serviciul StopCommunication 287

4.2.1 Descrierea mesajului 287

4.2.2 Formatul mesajului 288

4.2.3 Definirea parametrilor 289

4.3. Serviciul TesterPresent 289

4.3.1 Descrierea mesajului 289

4.3.2 Formatul mesajului 289

5. SERVICII DE GESTIONARE 291

5.1. Serviciul StartDiagnosticSession 291

5.1.1 Descrierea mesajului 291

5.1.2 Formatul mesajului 292

5.1.3 Definirea parametrilor 293

5.2. Serviciul SecurityAccess 294

5.2.1 Descrierea mesajului 294

5.2.2 Formatul mesajului – SecurityAccess – requestSeed 295

5.2.3 Formatul mesajului – SecurityAccess – sendKey 296

6. SERVICII DE TRANSMISIE A DATELOR 297

6.1. Serviciul ReadDataByIdentifier 298

6.1.1 Descrierea mesajului 298

6.1.2 Formatul mesajului 298

6.1.3 Definirea parametrilor 299

6.2. Serviciul WriteDataByIdentifier 300

6.2.1 Descrierea mesajului 300

6.2.2 Formatul mesajului 300

6.2.3 Definirea parametrilor 302

7. CONTROLUL IMPULSURILOR DE TEST – UNITATEA FUNCȚIONALĂ DE CONTROL AL INTRĂRILOR/IEȘIRILOR 302

7.1. Serviciul InputOutputControlByIdentifier 302

7.1.1 Descrierea mesajului 302

7.1.2 Formatul mesajului 303

7.1.3 Definirea parametrilor 304

8. FORMATE DATARECORDS 305

8.1. Intervalele parametrilor transmiși 305

8.2. Formate dataRecords 306

1. INTRODUCERE

Prezentul apendice descrie modul în care are loc schimbul de date între o unitate montată pe vehicul și un aparat de testare prin intermediul liniei K care face parte din interfața de etalonare descrisă în apendicele 6. De asemenea, în prezentul apendice este descris controlul liniei de semnalizare I/O efectuat asupra conectorului de etalonare.

Modul de stabilire a comunicărilor pe linia K este descris în secțiunea 4, „Communication Services”.

În prezentul apendice se folosește ideea de „sesiuni” de diagnosticare pentru a determina sfera controlului liniei K în diferite condiții. Sesiunea implicită este „StandardDiagnosticSession”, în cadrul căreia pot fi citite toate datele de pe o unitate montată pe vehicul, dar nu pot fi înregistrate date pe o unitate montată pe vehicul.

Selectarea sesiunii de diagnosticare este descrisă în secțiunea 5, „Management Services”.

Prezentul apendice trebuie să fie considerat relevant pentru ambele generații de VU și de carduri de atelier, în conformitate cu cerințele de interoperabilitate prevăzute în prezentul regulament.

CPR_001 Sesiunea „ECUProgrammingSession” permite introducerea datelor în unitatea montată pe vehicul. În cazul introducerii datelor de etalonare, unitatea montată pe vehicul trebuie să se afle în modul de funcționare ETALONARE.

Transferul de date prin intermediul liniei K este descris în secțiunea 6, „Data Transmission Services”. Formatele pentru datele transferate sunt descrise în detaliu în secțiunea 8, „dataRecords formats”.

CPR_002 Sesiunea „ECUAdjustmentSession” permite selectarea modului I/O al liniei de semnalizare I/O de etalonare, prin interfața liniei K. Controlul liniei de semnalizare I/O de etalonare este descris în secțiunea 7, „Control of Test Pulses – Input/Output Control functional unit”.

CPR_003 În cadrul prezentului document, adresa aparatului de testare este notată cu ‘tt’. Cu toate că este posibil să existe adrese privilegiate pentru aparatele de testare, VU trebuie să răspundă corect la orice adresă a aparatului de testare. Adresa fizică a VU este 0xEE.

2. TERMENI, DEFINIȚII ȘI REFERINȚE

Protocoalele, mesajele și codurile de eroare se bazează în principal pe un proiect al standardului ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1: Diagnostic services*, versiunea 6 din 22 februarie 2001).

Codificările octeților și alte valori hexazecimale sunt folosite la definirea identificatorilor de servicii, la elaborarea solicitărilor și a răspunsurilor de servicii și la configurarea parametrilor standard.

Termenul „aparat de testare” se referă la echipamentul folosit la introducerea datelor de programare/etalonare în VU.

Termenii „client” și „server” se referă la aparatul de testare, respectiv la VU.

Termenul ECU înseamnă „Unitate electronică de control” și se referă la VU.

Referințe:

ISO 14230-2: Road Vehicles -Diagnostic Systems – Keyword Protocol 2000- Part 2: Data Link Layer.

Prima ediție: 1999.

Vehicles – Diagnostic.

3. PREZENTARE GENERALĂ A SERVICIILOR

3.1. **Servicii disponibile**

Următorul tabel cuprinde o prezentare generală a serviciilor care vor fi disponibile în tahograf și sunt definite în prezentul document.

CPR_004 Tabelul prezintă serviciile disponibile în cadrul unei sesiuni de diagnosticare active.

— **Prima coloană** cuprinde serviciile disponibile.

— A **doua coloană** include numărul secțiunii din prezentul apendice unde serviciul este definit mai detaliat.

— A **treia coloană** indică valorile atribuite identificatorului de serviciu pentru mesajele de solicitare.

— A **patra coloană** precizează serviciile sesiunii **„StandardDiagnosticSession" (SD)** care trebuie implementate în fiecare VU.

— A **cincea coloană** precizează serviciile sesiunii **„ECUAdjustmentSession" (ECUAS)** care trebuie implementate pentru a permite controlul liniei de semnalizare I/O în conectorul de etalonare din panoul frontal al VU.

— A **șasea coloană** precizează serviciile sesiunii **„ECUProgrammingSession" (ECUPS)** care trebuie implementate pentru a permite programarea parametrilor în VU.

Tabelul 1

Tabel de prezentare a valorilor identificatorilor de serviciu

			Sesiuni de diagnosticare		
Denumirea serviciului de diagnosticare	Secțiunea Nr.	SID Valoarea solicitată	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Acest simbol indică faptul că serviciul este obligatoriu în această sesiune de diagnosticare.

Absența oricărui simbol indică faptul că acest serviciu nu este permis în această sesiune de diagnosticare.

3.2. **Coduri de răspuns**

Codurile de răspuns sunt definite pentru fiecare serviciu în parte.

4. Servicii de comunicare

Există anumite servicii care sunt necesare pentru inițierea și menținerea comunicării. Acestea nu apar în stratul aplicațiilor. Serviciile disponibile sunt prezentate în detaliu în tabelul următor:

Tabelul 2

Servicii de comunicare

Denumirea serviciului	Descriere
StartCommunication	Clientul solicită inițierea unei sesiuni de comunicare cu unul sau mai multe servere.
StopCommunication	Clientul solicită încheierea sesiunii de comunicare în curs de desfășurare.
TesterPresent	Clientul semnalează serverului faptul că este încă prezent.

CPR_005 Serviciul StartCommunication este folosit pentru inițierea unei comunicări. Pentru a efectua un serviciu, trebuie să se inițializeze comunicarea, iar parametrii de comunicare trebuie să fie adaptați modului dorit.

4.1. **Serviciul StartCommunication**

CPR_006 La primirea unei primitive de indicare StartCommunication, VU verifică dacă legătura de comunicare solicitată poate fi inițializată în condițiile existente. Condițiile necesare inițializării unei legături de comunicare sunt descrise în documentul ISO 14230-2.

CPR_007 În continuare, VU realizează toate acțiunile necesare pentru a inițializa o legătură de comunicare și trimite o primitivă de răspuns StartCommunication cu parametrii de răspuns pozitiv selectați.

CPR_008 Dacă o VU deja inițializată (și care a început o sesiune de diagnosticare) primește o nouă solicitare StartCommunication (de exemplu, datorită unei remedieri a erorii în aparatul de testare), solicitarea este acceptată și VU este reinițializată.

CPR_009 Dacă legătura de comunicare nu poate fi inițializată, indiferent de motiv, VU continuă să funcționeze în aceleași condiții care existau imediat înainte de încercarea de inițializare a legăturii de comunicare.

CPR_010 Mesajului de solicitare StartCommunication trebuie să i se aloce o adresă fizică.

CPR_011 Inițializarea VU pentru servicii se realizează cu ajutorul unei metode de „inițializare rapidă”;

— Anterior oricărei activități există o perioadă de inactivitate a magistralei.

— În continuare, aparatul de testare trimite o configurare de inițializare.

— Toate informațiile necesare inițializării comunicării sunt incluse în răspunsul VU.

CPR_012 După finalizarea inițializării,

— Tuturor parametrilor de comunicare le sunt atribuite valorile definite în tabelul 4 în funcție de octeții cheie.

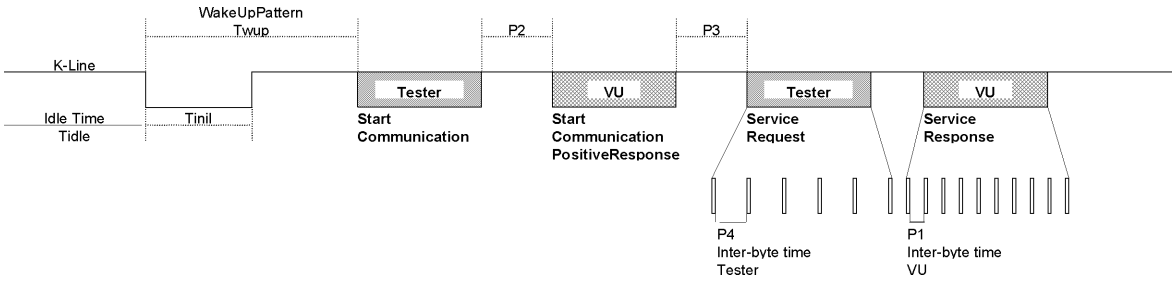
— VU așteaptă prima solicitare din partea aparatului de testare.

— VU se află în modul de diagnosticare implicit, adică StandardDiagnosticSession.

— Linia de semnalizare I/O de etalonare este în starea implicită, adică inactivă.

CPR_014 Viteza de transmisie a datelor pe linia K este de 10 400 bauzi.

CPR_016 Inițializarea rapidă este lansată de aparatul de testare prin transmiterea unei secvențe de ieșire din starea inactivă (Wup) pe linia K. Secvența începe după perioada inactivă pe linia K, cu o perioadă scurtă Tinil. Aparatul de testare transmite primul bit al serviciului StartCommunication după un timp Twup, după prima linie descendentă.



CPR_017 Valorile de sincronizare pentru inițializarea rapidă și comunicare în general sunt descrise în detaliu în tabelele prezentate în continuare. Pentru perioada de inactivitate există diferite posibilități:

— Prima transmisie după conectarea la alimentare, Tidle = 300 ms.

— După finalizarea unui serviciu StopCommunication, Tidle = P3 min.

— După încheierea comunicării prin depășirea timpului alocat P3 max, Tidle = 0.

Tabelul 3

Valori de sincronizare pentru inițializarea rapidă

Parametru		valoare minimă	valoare maximă
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabelul 4

Valorile de sincronizare pentru comunicare

Parametru de sincronizare	Descrierea parametrului	valori minime admise (ms)	valori maxime admise (ms)
		min.	max.
P1	Timpul între octeți pentru răspunsul VU	0	20
P2	Timpul dintre solicitarea aparatului de testare și răspunsul VU sau dintre două răspunsuri VU	25	250
P3	Timpul dintre sfârșitul răspunsurilor VU și începutul noii solicitări a aparatului de testare	55	5 000
P4	Timpul între octeți pentru solicitarea aparatului de testare	5	20

CPR_018 Formatul mesajului pentru inițializarea rapidă este prezentat în detaliu în tabelele următoare. (NOTĂ: Hex înseamnă hexazecimal)

Tabelul 5

Mesaj StartCommunication Request

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	81	FMT
#2	Octet al adresei țintă	EE	TGT
#3	Octet al adresei sursă	tt	SRC
#4	**StartCommunication Request Service Id**	**81**	**SCR**
#5	Sumă de verificare	00-FF	CS

Tabelul 6

Mesaj StartCommunication Positive Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	03	LEN
#5	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
#6	Octet cheie 1	EA	KB1
#7	Octet cheie 2	8F	KB2
#8	Sumă de verificare	00-FF	CS

CPR_019 Nu există niciun răspuns negativ la mesajul StartCommunication Request; dacă nu există un mesaj de răspuns pozitiv de transmis, VU nu este inițializată, nu se transmite niciun mesaj și aceasta rămâne în modul său normal de funcționare.

4.2. **Serviciul StopCommunication**

4.2.1 *Descrierea mesajului*

Scopul acestui serviciu al stratului de comunicare este de a încheia o sesiune de comunicare.

CPR_020 La primirea unei primitive de indicare StopCommunication, VU verifică dacă condițiile din momentul respectiv permit încheierea comunicării în cauză. În acest caz, VU realizează toate acțiunile necesare pentru a încheia comunicarea în cauză.

CPR_021 Dacă încheierea comunicării este posibilă, VU emite o primitivă de răspuns StopCommunication cu parametrii de răspuns pozitiv selectați, înainte de încheierea comunicării.

CPR_022 Dacă încheierea comunicării nu este posibilă, indiferent de motiv, VU emite o primitivă de răspuns StopCommunication împreună cu parametrul de răspuns negativ selectat.

CPR_023 Dacă VU detectează depășirea timpului alocat P3max, comunicarea este încheiată fără a se emite o primitivă de răspuns.

4.2.2 *Formatul mesajului*

CPR_024 Formatele mesajelor pentru primitivele StopCommunication sunt prezentate în detaliu în tabelele următoare:

Tabelul 7

Mesaj StopCommunication Request

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	EE	TGT
#3	Octet al adresei sursă	tt	SRC
#4	Octet de lungime suplimentar	01	LEN
#5	**StopCommunication Request Service Id**	**82**	**SPR**
#6	Sumă de verificare	00-FF	CS

Tabelul 8

Mesaj StopCommunication Positive Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Sumă de verificare	00-FF	CS

Tabelul 9

Mesaj StopCommunication Negative Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	StopCommunication Request Service Identification	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Sumă de verificare	00-FF	CS

4.2.3 *Definirea parametrilor*

Acest serviciu nu necesită definirea niciunui parametru.

4.3. **Serviciul TesterPresent**

4.3.1 *Descrierea mesajului*

Serviciul TesterPresent este folosit de aparatul de testare pentru a indica serverului că este încă prezent, în scopul de a preveni astfel revenirea automată a serverului la modul de funcționare normal și posibila întrerupere a comunicării de către acesta. Acest serviciu, trimis periodic, menține sesiunea de diagnosticare/comunicarea activă prin resetarea contorului P3 de fiecare dată când se primește o solicitare pentru acest serviciu.

4.3.2 *Formatul mesajului*

CPR_079 Formatele mesajelor pentru primitivele TesterPresent sunt prezentate în detaliu în tabelele următoare.

Tabelul 10

Mesaj TesterPresent Request

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	EE	TGT
#3	Octet al adresei sursă	tt	SRC
#4	Octet de lungime suplimentar	02	LEN
#5	**TesterPresent Request Service Id**	**3E**	**TP**

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#6	Subfuncție = responseRequired = [da	01	RESPREQ_Y
	nu]	02	RESPREQ_NO
#7	Sumă de verificare	00-FF	CS

CPR_080 Dacă parametrul responseRequired are valoarea „da”, serverul răspunde cu următorul mesaj de răspuns pozitiv. Dacă valoarea este „nu”, serverul nu trimite niciun răspuns.

Tabelul 11

Mesaj TesterPresent Positive Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Sumă de verificare	00-FF	CS

CPR_081 Serviciul este compatibil cu următoarele coduri de răspuns negativ:

Tabelul 12

Mesaj TesterPresent Negative Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	TesterPresent Request Service Identification	3E	TP

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
#8	Sumă de verificare	00-FF	CS

5. SERVICII DE GESTIONARE

Serviciile disponibile sunt prezentate în detaliu în tabelul următor:

Tabelul 13

Servicii de gestionare

Denumirea serviciului	Descriere
StartDiagnosticSession	Clientul solicită inițierea unei sesiuni de diagnosticare cu o VU.
SecurityAccess	Clientul solicită accesul la funcții rezervate utilizatorilor autorizați.

5.1. **Serviciul StartDiagnosticSession**

5.1.1 *Descrierea mesajului*

CPR_025 Serviciul StartDiagnosticSession este utilizat pentru activarea unor diferite sesiuni de diagnosticare în server. O sesiune de diagnosticare activează un set specific de servicii în conformitate cu tabelul 17. O sesiune poate activa servicii specifice ale producătorului vehiculului care nu fac parte din prezentul document. Normele de implementare respectă următoarele cerințe:

— Întotdeauna există doar o sesiune de diagnosticare activă în VU,

— VU lansează întotdeauna StandardDiagnosticSession când este conectată la o sursă de alimentare. Dacă nu este lansată o altă sesiune de diagnosticare, StandardDiagnosticSession rămâne deschisă atâta timp cât VU este conectată la o sursă de alimentare,

— Dacă o sesiune de diagnosticare în curs de desfășurare a fost solicitată de un aparat de testare, VU trimite un mesaj de răspuns pozitiv,

— De fiecare dată când un aparat de testare solicită o sesiune de diagnosticare nouă, VU trimite mai întâi un mesaj de răspuns pozitiv la solicitarea StartDiagnosticSession, înainte ca noua sesiune să devină activă în VU. Dacă VU nu poate lansa noua sesiune de diagnosticare solicitată, aceasta răspunde cu un mesaj de răspuns negativ la solicitarea StartDiagnosticSession, iar sesiunea aflată în desfășurare continuă.

CPR_026 O sesiune de diagnosticare poate fi lansată numai în cazul în care comunicarea a fost stabilită între client și VU.

CPR_027 Parametrii de sincronizare definiți în tabelul 4 devin activi după efectuarea cu succes a StartDiagnosticSession, parametrul diagnosticSession fiind stabilit la valoarea „StandardDiagnosticSession” în mesajul de solicitare în cazul în care o altă sesiune de diagnosticare a fost activă anterior.

5.1.2 *Formatul mesajului*

CPR_028 Formatele mesajelor pentru primitivele StartDiagnosticSession sunt prezentate în detaliu în tabelele următoare.

Tabelul 14

Mesaj StartDiagnosticSession Request

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	EE	TGT
#3	Octet al adresei sursă	tt	SRC
#4	Octet de lungime suplimentar	02	LEN
#5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
#6	diagnosticSession = [o valoare din tabelul 17]	xx	DS_…
#7	Sumă de verificare	00-FF	CS

Tabelul 15

Mesaj StartDiagnosticSession Positive Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	diagnosticSession = [aceeași valoare ca la octetul #6 din tabelul 14]	xx	DS_…
#7	Sumă de verificare	00-FF	CS

Tabelul 16

Mesaj StartDiagnosticSession Negative Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT

Octet #	Denumirea parametrului		Valoarea Hex	Cod mnemonic
#3	Octet al adresei sursă		EE	SRC
#4	Octet de lungime suplimentar		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	StartDiagnosticSession Request Service Id		10	STDS
#7	ResponseCode =	[subFunctionNotSupported ([a])	12	RC_SFNS
		incorrectMessageLength ([b])	13	RC_IML
		conditionsNotCorrect ([c])	22	RC_CNC
#8	Sumă de verificare		00-FF	CS

([a]) – valoarea introdusă la octetul # 6 din mesajul de solicitare nu este compatibilă, adică nu se află în tabelul 17,
([b]) – lungimea mesajului nu este corectă,
([c]) – criteriile pentru solicitarea StartDiagnosticSession nu sunt îndeplinite.

5.1.3 *Definirea parametrilor*

CPR_029 Parametrul ***diagnosticSession (DS_)*** este folosit de serviciul StartDiagnosticSession pentru a selecta comportamentul specific al serverului (serverelor). În prezentul document sunt precizate următoarele sesiuni de diagnosticare:

Tabelul 17

Definiția valorilor diagnosticSession

Hex	Descriere	Cod mnemonic
81	**StandardDiagnosticSession** Această sesiune de diagnosticare activează toate serviciile specificate în **coloana 4 "SD"** din **tabelul 1**. Aceste servicii permit citirea datelor de pe un server (VU). Această sesiune de diagnosticare este activă după finalizarea cu succes a inițializării între client (aparatul de testare) și server (VU). Această sesiune de diagnosticare poate fi suprascrisă de alte sesiuni de diagnosticare specificate în prezenta secțiune.	**SD**
85	**ECUProgrammingSession** Această sesiune de diagnosticare activează toate serviciile specificate în **coloana 6 "ECUPS"** din **tabelul 1**. Serviciile respective sunt compatibile cu programarea memoriei unui server (VU). Această sesiune de diagnosticare poate fi suprascrisă de alte sesiuni de diagnosticare specificate în prezenta secțiune.	**ECUPS**
87	**ECUAdjustmentSession** Această sesiune de diagnosticare activează toate serviciile specificate în **coloana 5 "ECUAS"** din **tabelul 1**. Aceste servicii sunt compatibile cu controlul intrărilor/ieșirilor unui server (VU). Această sesiune de diagnosticare poate fi suprascrisă de alte sesiuni de diagnosticare specificate în prezenta secțiune.	**ECUAS**

5.2. **Serviciul SecurityAccess**

Scrierea datelor de etalonare este posibilă doar dacă VU se află în mod ETALONARE. Pe lângă introducerea unui card de atelier în VU, este necesară și introducerea PIN-ului corespunzător în VU înainte de acordarea accesului la modul ETALONARE.

În cazul în care VU se află în modul ETALONARE sau CONTROL, este posibilă, de asemenea, accesarea liniei I/O de etalonare.

Serviciul SecurityAccess oferă o modalitate de introducere a PIN-ului și de a semnala aparatului de testare dacă VU se află sau nu în mod ETALONARE.

Se permite introducerea PIN-ului și prin intermediul altor metode.

5.2.1 *Descrierea mesajului*

Serviciul SecurityAccess constă într-un mesaj SecurityAccess „requestSeed", urmat eventual de un mesaj SecurityAccess „sendKey". Serviciul SecurityAccess trebuie să fie executat după serviciul StartDiagnosticSession.

CPR_033 Aparatul de testare folosește mesajul SecurityAccess „requestSeed" pentru a verifica dacă unitatea montată pe vehicul este pregătită să accepte un PIN.

CPR_034 Dacă unitatea montată pe vehicul este deja în mod ETALONARE, aceasta răspunde solicitării prin trimiterea unei „valori inițiale (*seed*)" de 0x0000 cu ajutorul serviciului SecurityAccess Positive Response.

CPR_035 Dacă unitatea montată pe vehicul este pregătită să accepte un PIN pentru verificarea cu un card de atelier, aceasta răspunde solicitării prin trimiterea unei „valori inițiale" mai mari de 0x0000 cu ajutorul serviciului SecurityAccess Positive Response.

CPR_036 Dacă unitatea montată pe vehicul nu este pregătită să accepte un PIN de la aparatul de testare, întrucât fie cardul de atelier introdus nu este valabil, fie nu a fost introdus niciun card de atelier, fie unitatea montată pe vehicul așteaptă transmiterea PIN-ului printr-o altă metodă, aceasta răspunde solicitării cu un răspuns negativ având un cod de răspuns setat pe conditionsNotCorrectOrRequestSequenceError.

CPR_037 Apoi, aparatul de testare folosește în cele din urmă mesajul SecurityAccess „sendKey" pentru a transmite un PIN unității montate pe vehicul. Pentru a aloca timpul necesar realizării procesului de autentificare a cardului, VU folosește codul de răspuns negativ requestCorrectlyReceived-ResponsePending pentru a prelungi timpul de răspuns. Totuși, timpul maxim de răspuns nu trebuie să depășească 5 minute. După finalizarea serviciului solicitat, VU trimite un mesaj de răspuns pozitiv sau un mesaj de răspuns negativ cu un cod de răspuns diferit de acesta. Codul de răspuns negativ requestCorrectlyReceived-ResponsePending poate fi repetat de VU până la finalizarea serviciului solicitat și trimiterea mesajului de răspuns final.

CPR_038 Unitatea montată pe vehicul răspunde acestei solicitări folosind serviciul SecurityAccess Positive Response numai când este în modul ETALONARE.

CPR_039 În următoarele cazuri, unitatea montată pe vehicul răspunde acestei solicitări cu un răspuns negativ însoțit de un cod de răspuns cu valoarea:

— subFunctionNot supported: format nevalabil pentru parametrul subfuncției (accessType);

— conditionsNotCorrectOrRequestSequenceError: unitatea montată pe vehicul nu este pregătită să accepte introducerea unui PIN,

— invalidKey: PIN nevalabil și numărul de încercări permise de verificare a PIN-ului nedepășit,

— exceededNumberOfAttempts: PIN nevalabil și numărul de încercări permise de verificare a PIN-ului depășit,

— generalReject: PIN corect, dar tentativă nereușită de autentificare reciprocă cu cardul de atelier.

5.2.2 *Formatul mesajului – SecurityAccess – requestSeed*

CPR_040 Formatele mesajelor pentru primitivele SecurityAccess „requestSeed" sunt prezentate în detaliu în tabelele următoare.

Tabelul 18

Mesaj SecurityAccess Request- requestSeed

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	EE	TGT
#3	Octet al adresei sursă	tt	SRC
#4	Octet de lungime suplimentar	02	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Sumă de verificare	00-FF	CS

Tabelul 19

Mesaj SecurityAccess – requestSeed Positive Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	04	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	Valoare inițială superioară	00-FF	SEEDH
#8	Valoare inițială inferioară	00-FF	SEEDL
#9	Sumă de verificare	00-FF	CS

Tabelul 20

Mesaj SecurityAccess Negative Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#4	Octet de lungime suplimentar	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	SecurityAccess Request Service Id	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Sumă de verificare	00-FF	CS

5.2.3 *Formatul mesajului – SecurityAccess – sendKey*

CPR_041 Formatele mesajelor pentru primitivele SecurityAccess „sendKey" sunt prezentate în detaliu în tabelele următoare.

Tabelul 21

Mesaj SecurityAccess Request – sendKey

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	EE	TGT
#3	Octet al adresei sursă	tt	SRC
#4	Octet de lungime suplimentar	m+2	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
de la #7 până la #m+6	Cheia #1 (superioară)	xx	KEY
	…	…	
	Cheia #m (inferioară, m trebuie să fie minim 4 și maxim 8)	xx	
#m+7	Sumă de verificare	00-FF	CS

Tabelul 22

Mesaj SecurityAccess – sendKey Positive Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#4	Octet de lungime suplimentar	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Sumă de verificare	00-FF	CS

Tabelul 23

Mesaj SecurityAccess Negative Response

Octet #	Denumirea parametrului		Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică		80	FMT
#2	Octet al adresei țintă		tt	TGT
#3	Octet al adresei sursă		EE	SRC
#4	Octet de lungime suplimentar		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	SecurityAccess Request Service Id		27	SA
#7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Sumă de verificare		00-FF	CS

6. SERVICII DE TRANSMISIE A DATELOR

Serviciile disponibile sunt prezentate în detaliu în tabelul următor:

Tabelul 24

Servicii de transmisie de date

Denumirea serviciului	Descriere
ReadDataByIdentifier	Clientul solicită transmisia valorii curente a unei înregistrări care poate fi accesată prin recordDataIdentifier.
WriteDataByIdentifier	Clientul solicită scrierea unei înregistrări care poate fi accesată prin recordDataIdentifier.

6.1. **Serviciul ReadDataByIdentifier**

6.1.1 *Descrierea mesajului*

CPR_050 Serviciul ReadDataByIdentifier este folosit de client pentru a solicita valorile datelor înregistrate de la un server. Datele sunt identificate de un recordDataIdentifier. Producătorul VU trebuie să se asigure că, la efectuarea acestui serviciu, condițiile privind serverul sunt îndeplinite.

6.1.2 *Formatul mesajului*

CPR_051 Formatele mesajelor pentru primitivele ReadDataByIdentifier sunt prezentate în detaliu în tabelele următoare.

Tabelul 25

Mesaj ReadDataByIdentifier Request

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	EE	TGT
#3	Octet al adresei sursă	tt	SRC
#4	Octet de lungime suplimentar	03	LEN
#5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
de la #6 la #7	recordDataIdentifier = [o valoare din tabelul 28]	xxxx	RDI_…
#8	Sumă de verificare	00-FF	CS

Tabelul 26

Mesaj ReadDataByIdentifier Positive Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	m+3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 și #7	recordDataIdentifier = [aceeași valoare ca octeții #6 și #7 din tabelul 25]	xxxx	RDI_…
de la #8 până la #m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Sumă de verificare	00-FF	CS

Tabelul 27

Mesaj ReadDataByIdentifier Negative Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	ReadDataByIdentifier Request Service Id	22	RDBI
#7	ResponseCode = [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Sumă de verificare	00-FF	CS

6.1.3 *Definirea parametrilor*

CPR_052 Parametrul ***recordDataIdentifier (RDI_)*** din mesajul de solicitare ReadDataByIdentifier identifică o înregistrare de date.

CPR_053 Valorile recordDataIdentifier definite în prezentul document sunt indicate în tabelul de mai jos.

Tabelul recordDataIdentifier este format din patru coloane și mai multe rânduri.

— **Prima coloană (Hex)** cuprinde „valoarea Hex” atribuită recordDataIdentifier specificat în coloana a treia.

— A **doua coloană (element de date)** precizează elementul de date din apendicele 1 pe care se bazează recordDataIdentifier (uneori este necesară transcodarea).

— A **treia coloană (descriere)** specifică denumirea recordDataIdentifier corespunzătoare.

— A **patra coloană (cod mnemonic)** indică codul mnemonic al recordDataIdentifier în cauză.

Tabelul 28

Definiția valorilor recordDataIdentifier

Hex	Element de date	Denumirea recordDataIdentifier (a se vedea formatul în secțiunea 8.2)	Cod mnemonic
F90B	`CurrentDateTime`	TimeDate	RDI_TD
F912	`HighResOdometer`	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	`K-ConstantOfRecordingEquipment`	Kfactor	RDI_KF

Hex	Element de date	Denumirea recordDataIdentifier (a se vedea formatul în secțiunea 8.2)	Cod mnemonic
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 Parametrul ***dataRecord (DREC_)*** este folosit de mesajul de răspuns pozitiv ReadDataByIdentifier pentru a furniza clientului (aparatul de testare) valoarea înregistrării de date identificată de recordDataIdentifier. Formatele datelor sunt specificate în secțiunea 8. Se pot implementa dataRecords suplimentare ca opțiune a utilizatorului, precum date de intrare, interne și de ieșire specifice pentru VU, dar acestea nu sunt definite în prezentul document.

6.2. **Serviciul WriteDataByIdentifier**

6.2.1 *Descrierea mesajului*

CPR_056 Serviciul WriteDataByIdentifier este folosit de client pentru a scrie valorile înregistrării de date pe un server. Datele sunt identificate de un recordDataIdentifier. Producătorul VU trebuie să se asigure că, la efectuarea acestui serviciu, condițiile privind serverul sunt îndeplinite. Pentru a actualiza parametrii enumerați în tabelul 28, VU trebuie să se afle în modul ETALONARE.

6.2.2 *Formatul mesajului*

CPR_057 Formatele mesajelor pentru primitivele WriteDataByIdentifier sunt prezentate în detaliu în tabelele următoare.

Tabelul 29

Mesaj WriteDataByIdentifier Request

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	EE	TGT
#3	Octet al adresei sursă	tt	SRC
#4	Octet de lungime suplimentar	m+3	LEN
#5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
de la #6 până la #7	recordDataIdentifier = [o valoare din tabelul 28]	xxxx	RDI_…

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
de la #8 până la m +7	dataRecord[] = [data#1	xx	DREC_DATA1
	:	:	:
	data#m]	xx	DREC_DATAm
#m+8	Sumă de verificare	00-FF	CS

Tabelul 30

Mesaj WriteDataByIdentifier Positive Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
de la #6 până la #7	recordDataIdentifier = [aceeași valoare ca octeții #6 și #7 din tabelul 29]	xxxx	RDI_…
#8	Sumă de verificare	00-FF	CS

Tabelul 31

Mesaj WriteDataByIdentifier Negative Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	WriteDataByIdentifier Request Service Id	2E	WDBI

Octet #	Denumirea parametrului		Valoarea Hex	Cod mnemonic
#7	ResponseCode =	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Sumă de verificare		00-FF	CS

6.2.3 *Definirea parametrilor*

Parametrul ***recordDataIdentifier (RDI_)*** este definit în tabelul 28.

Parametrul ***dataRecord (DREC_)*** este folosit de mesajul de solicitare WriteDataByIdentifier pentru a furniza serverului (VU) valorile înregistrărilor de date identificate de recordDataIdentifier. Formatele datelor sunt specificate în secțiunea 8.

7. CONTROLUL IMPULSURILOR DE TEST – UNITATEA FUNCȚIONALĂ DE CONTROL AL INTRĂRILOR/IEȘIRILOR

Serviciile disponibile sunt prezentate în detaliu în tabelul următor:

Tabelul 32

Unitatea funcțională de control al intrărilor/ieșirilor

Denumirea serviciului	Descriere
InputOutputControlByIdentifier	Clientul solicită controlul unei intrări/ieșiri specifice serverului.

7.1. Serviciul InputOutputControlByIdentifier

7.1.1 *Descrierea mesajului*

Conexiunea realizată cu ajutorul conectorului frontal permite controlul sau monitorizarea impulsurilor de test folosind un aparat de testare corespunzător.

CPR_058 Linia de semnalizare I/O de etalonare poate fi configurată cu ajutorul comenzii lansate pe linia K folosind serviciul InputOutputControlByIdentifier pentru a selecta funcția de intrare sau ieșire solicitată pentru linie. Stările disponibile ale liniei sunt următoarele:

— dezactivată,

— speedSignalInput, caz în care linia de semnalizare I/O de etalonare este utilizată pentru a introduce un semnal de viteză (semnal de test) care să înlocuiască semnalul de viteză al senzorului de mișcare; această funcție nu este disponibilă în modul CONTROL,

— realTimeSpeedSignalOutputSensor, caz în care linia de semnalizare I/O de etalonare este utilizată pentru ieșirea unui semnal de viteză de la senzorul de mișcare,

— RTCOutput, caz în care linia de semnalizare I/O de etalonare este utilizată pentru ieșirea unui semnal de ceas UTC; această funcție nu este disponibilă în modul CONTROL.

CPR_059 Pentru a configura starea liniei, unitatea montată pe vehicul trebuie să fi intrat într-o sesiune de reglare și să se afle în modul ETALONARE sau CONTROL. Dacă VU se află în mod ETALONARE, cele patru stări ale liniei pot fi selectate (dezactivată, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Dacă VU se află în modul CONTROL, numai două stări ale liniilor pot fi selectate (dezactivată, realTimeSpeedOutputSensor). La ieșirea din sesiunea de reglare sau din modul ETALONARE sau CONTROL, unitatea montată pe vehicul trebuie să se asigure că linia de semnalizare I/O de etalonare a revenit la starea „dezactivată” (stare implicită).

CPR_060 În cazul în care impulsurile de viteză sunt primite pe linia de intrare a semnalului de viteză în timp real a VU, iar linia de semnalizare I/O de etalonare este setată în modul intrare, linia de semnalizare I/O de etalonare este setată pe ieșire sau este readusă la starea dezactivată.

CPR_061 Ordinea operațiunilor este următoarea:

— Stabilirea comunicărilor cu ajutorul serviciului StartCommunication

— Intrarea într-o sesiune de reglare cu ajutorul serviciului StartDiagnosticSession și trecerea în modul de funcționare ETALONARE sau CONTROL (ordinea de efectuare a acestor două operațiuni nu este importantă).

— Modificarea stării ieșirii cu ajutorul serviciului InputOutputControlByIdentifier.

7.1.2 *Formatul mesajului*

CPR_062 Formatele mesajelor pentru primitivele InputOutputControlByIdentifier sunt prezentate în detaliu în tabelele următoare.

Tabelul 33

Mesaj InputOutputControlByIdentifier Request

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	EE	TGT
#3	Octet al adresei sursă	tt	SRC
#4	Octet de lungime suplimentar	xx	LEN
#5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
#6 și #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 sau	ControlOptionRecord = [		COR_…
de la #8 până la #9	InputOutputControlParameter – o valoare din tabelul 36	xx	IOCP_…
	controlState – o valoare din tabelul 37 (a se vedea nota de mai jos)]	xx	CS_…
#9 sau #10	Sumă de verificare	00-FF	CS

Notă: Parametrul controlState este prezent numai în anumite cazuri (a se vedea 7.1.3).

Tabelul 34

Mesaj InputOutputControlByIdentifier Positive Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	xx	LEN
#5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 și #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 sau de la #8 până la #9	controlStatusRecord =[		CSR_
	inputOutputControlParameter (aceeași valoare ca cea a octetului #8 din tabelul 33)	xx	IOCP_…
	controlState (aceeași valoare ca cea a octetului #9 tabelul 33)] (dacă este cazul)	xx	CS_…
#9 sau #10	Sumă de verificare	00-FF	CS

Tabelul 35

Mesaj InputOutputControlByIdentifier Negative Response

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
#1	Octet de format – adresare fizică	80	FMT
#2	Octet al adresei țintă	tt	TGT
#3	Octet al adresei sursă	EE	SRC
#4	Octet de lungime suplimentar	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	inputOutputControlByIdentifier Request SId	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Sumă de verificare	00-FF	CS

7.1.3 *Definirea parametrilor*

CPR_064 Parametrul ***inputOutputControlParameter (IOCP_)*** este definit în tabelul următor.

Tabelul 36

Definiția valorilor inputOutputControlParameter

Hex	Descriere	Cod mnemonic
00	**ReturnControlToECU** Această valoare indică serverului (VU) faptul că aparatul de testare nu mai are controlul asupra liniei de semnalizare I/O de etalonare.	RCTECU
01	**ResetToDefault** Această valoare indică serverului (VU) faptul că s-a solicitat resetarea liniei de semnalizare I/O de etalonare la starea implicită.	RTD
03	**ShortTermAdjustment** Această valoare indică serverului (VU) faptul că s-a solicitat ajustarea liniei de semnalizare I/O de etalonare la valoarea inclusă în parametrul controlState.	STA

CPR_065 Parametrul ***controlState*** este prezent numai în cazul în care inputOutputControlParameter este setat la ShortTermAdjustment și este definit în tabelul următor:

Tabelul 37

Definiția valorilor controlState

Mod	Valoarea Hex	Descriere
Dezactivare	00	Linia I/O este dezactivată (stare implicită)
Activare	01	Se activează linia I/O de etalonare ca speedSignalInput
Activare	02	Se activează linia I/O de etalonare ca realTimeSpeedSignalOutputSensor
Activare	03	Se activează linia I/O de etalonare ca RTCOutput

8. FORMATE DATARECORDS

Această secțiune prezintă în detaliu:

— normele generale care se aplică intervalelor de parametri transmiși de unitatea montată pe vehicul către aparatul de testare,

— formatele care se folosesc pentru datele transferate cu ajutorul serviciilor de transmisie de date descrise în secțiunea 6.

CPR_067 Toți parametrii identificați sunt compatibili cu VU.

CPR_068 Datele transmise de VU către aparatul de testare ca răspuns la un mesaj de solicitare sunt de tip cuantificabil (și anume, valoarea activă a parametrului solicitat, astfel cum a fost măsurată sau observată de VU).

8.1. **Intervalele parametrilor transmiși**

CPR_069 Tabelul 38 definește intervalele folosite la determinarea valabilității unui parametru transmis.

CPR_070 Valorile din intervalul „indicator de eroare" (*error indicator*) permit unității montate pe vehicul să indice imediat faptul că nicio dată parametrică valabilă nu este disponibilă pentru moment din cauza unui anumit tip de eroare la nivelul tahografului.

CPR_071 Valorile din intervalul „indisponibil" (*not available*) permit unității montate pe vehicul să transmită un mesaj care conține un parametru indisponibil sau incompatibil cu modulul în cauză. Valorile din intervalul „nesolicitat" (*not requested*) permit transmiterea de către un dispozitiv a unui mesaj de comandă și identifică acei parametri în cazul cărora nu se așteaptă niciun răspuns de la dispozitivul de recepție.

CPR_072 Dacă defecțiunea unei componente împiedică transmisia de date valabile pentru un parametru, în locul datelor parametrice respective ar trebui folosiți indicatorii de eroare descriși în tabelul 38. Cu toate acestea, dacă datele măsurate sau calculate au ca rezultat o valoare valabilă care depășește totuși intervalul definit al parametrului respectiv, indicatorul de eroare nu ar trebui folosit. Datele trebuie să fie transmise folosind valoarea minimă sau maximă adecvată a parametrului.

Tabelul 38

Intervalele dataRecords

Denumirea intervalului	1 octet (valoarea Hex)	2 octeți (valoarea Hex)	4 octeți (valoarea Hex)	ASCII
Semnal valabil	00-FA	0000-FAFF	00000000-FAFFFFFF	de la 1 la 254
Indicator specific parametrului	FB	FB00-FBFF	FB000000-FBFFFFFF	nu există
Interval rezervat pentru viitorii biți ai indicatorului	FC-FD	FC00-FDFF	FC000000-FDFFFFFF	nu există
Indicator de eroare	FE	FE00-FEFF	FE000000-FEFFFFFF	0
Nu sunt disponibile sau nu sunt solicitate	FF	FF00-FFFF	FF000000-FFFFFFFF	FF

CPR_073 Pentru parametrii codați în ASCII, caracterul ASCII „*" este rezervat ca delimitator.

8.2. **Formate dataRecords**

În tabelele 39 – 42 de mai jos sunt prezentate în detaliu formatele care trebuie folosite prin intermediul serviciilor ReadDataByIdentifier și WriteDataByIdentifier.

CPR_074 În tabelul 39 sunt indicate lungimea, rezoluția și domeniul de valori ale fiecărui parametru identificat de recordDataIdentifier:

Tabelul 39

Formatul dataRecords

Denumirea parametrului	Lungimea datelor (octeți)	Rezoluția	Domeniul de valori
TimeDate	8	A se vedea detaliile din tabelul 40	
HighResolutionTotalVehicleDistance	4	amplificare 5 m/bit, deplasare 0 m	de la 0 până la + 21 055 406 km
Kfactor	2	amplificare 0,001 impulsuri/m/bit, deplasare 0	0-64,255 impulsuri/m
LfactorTyreCircumference	2	amplificare 0,125 10^{-3} m/bit, deplasare 0	de la 0 la 8,031 m
WvehicleCharacteristicFactor	2	amplificare 0,001 impulsuri/m/bit, deplasare 0	0-64,255 impulsuri/m
TyreSize	15	ASCII	ASCII

Denumirea parametrului	Lungimea datelor (octeți)	Rezoluția	Domeniul de valori
NextCalibrationDate	3	A se vedea detaliile din tabelul 41	
SpeedAuthorised	2	amplificare 1/256 km/h/bit, deplasare 0	0-250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	A se vedea detaliile din tabelul 42	
VIN	17	ASCII	ASCII

CPR_075 În tabelul 40 sunt prezentate în detaliu formatele diferiților octeți ai parametrului TimeDate:

Tabelul 40

Formatul detaliat al TimeDate (valoarea recordDataIdentifier # F90B)

Octet	Definirea parametrilor	Rezoluția	Domeniul de valori
1	Secunde	amplificare 0,25 s/bit, deplasare 0 s	de la 0 la 59,75 s
2	Minute	amplificare 1 min/bit, deplasare 0 min	0-59 min
3	Ore	amplificare 1 h/bit, deplasare 0 h	0-23 h
4	Luna	amplificare 1 lună/bit, deplasare 0 luni	1-12 luni
5	Ziua	amplificare 0,25 zile/bit, deplasare 0 zile (a se vedea NOTA de sub tabelul 41)	0,25-31,75 zile
6	Anul	amplificare 1 lună/bit, deplasare an + 1985 (a se vedea NOTA de sub tabelul 41)	anul 1985-anul 2235
7	Deplasare locală minute	amplificare 1 min/bit, deplasare – 125 min	de la – 59 la + 59 min
8	Deplasare locală ore	amplificare 1 h/bit, deplasare -125 h	de la – 23 la + 23 h

CPR_076 În tabelul 41 sunt prezentate în detaliu formatele diferiților octeți ai parametrului NextCalibrationDate.

Tabelul 41

Formatul detaliat al NextCalibrationDate (valoarea recordDataIdentifier # F922)

Octet	Definirea parametrilor	Rezoluția	Domeniul de valori
1	Luna	amplificare 1 lună/bit, deplasare 0 luni	1-12 luni
2	Ziua	amplificare 0,25 zile/bit, deplasare 0 zile (a se vedea NOTA de mai jos)	0,25-31,75 zile
3	Anul	amplificare 1 lună/bit, deplasare an + 1985 (a se vedea NOTA de mai jos)	anul 1985-anul 2235

NOTĂ privind folosirea parametrului „Zi”:

1) O valoare 0 pentru dată este o valoare nulă. Valorile 1, 2, 3 și 4 sunt folosite pentru a identifica prima zi a lunii; valorile 5, 6, 7 și 8 identifică a doua zi a lunii etc.

2) Acest parametru nu influențează și nici nu modifică parametrul pentru oră menționat anterior.

NOTĂ privind folosirea octetului parametrului „An”:

Valoarea 0 pentru an corespunde anului 1985; valoarea 1 indică anul 1986 etc.

CPR_078 În tabelul 42 sunt prezentate în detaliu formatele diferiților octeți ai parametrului VehicleRegistration-Number:

Tabelul 42

Formatul detaliat al VehicleRegistrationNumber (valoarea recordDataIdentifier # F97E)

Octet	Definirea parametrilor	Rezoluția	Domeniul de valori
1	Pagină de cod (conform definiției din apendicele 1)	ASCII	de la 01 la 0A
2-14	Numărul de înmatriculare al vehiculului (conform definiției din apendicele 1)	ASCII	ASCII

Apendicele 9.

OMOLOGAREA DE TIP LISTA TESTELOR MINIME OBLIGATORII

CUPRINS

1. INTRODUCERE 309

2. TESTE DE FUNCȚIONARE A UNITĂȚII MONTATE PE VEHICUL 311

3. TESTE DE FUNCȚIONARE A SENZORULUI DE MIȘCARE 315

4. TESTE DE FUNCȚIONARE A CARDURILOR DE TAHOGRAF 318

5. TESTE PRIVIND ECHIPAMENTUL GNSS EXTERN 328

6. TESTE PRIVIND ECHIPAMENTUL DE COMUNICARE LA DISTANȚĂ 331

7. TESTE DE FUNCȚIONARE PRIVIND HÂRTIA 333

8. TESTE DE INTEROPERABILITATE 335

1. INTRODUCERE

1.1. **Omologarea de tip**

Omologarea CE de tip pentru aparatura de înregistrare (sau o componentă a acesteia) sau pentru un card de tahograf se bazează pe:

— o **certificare a securității**, pe baza specificațiilor prevăzute în criteriile comune, în raport cu un obiectiv de securitate care respectă în totalitate apendicele 10 la prezenta anexă (de completat/modificat);

— o **certificare a funcționării**, efectuată de o autoritate a unui stat membru, care certifică faptul că articolul testat respectă cerințele prezentei anexe din punctul de vedere al funcțiilor îndeplinite, al preciziei măsurătorilor și al caracteristicilor de mediu;

— o **certificare a interoperabilității**, efectuată de un organism competent, care certifică faptul că aparatura de înregistrare (sau cardul de tahograf) este în întregime interoperabilă(interoperabil) cu modelele necesare de card de tahograf (sau de aparatură de înregistrare) (a se vedea capitolul 8 din prezenta anexă).

Prezentul apendice enumeră testele minime care trebuie efectuate de către o autoritate a unui stat membru în cadrul testelor de funcționare, precum și testele minime care trebuie efectuate de organismul competent în cadrul testelor de interoperabilitate. Procedurile care trebuie urmate în vederea efectuării testelor sau tipul de teste nu sunt specificate în cuprinsul prezentului document.

Prezentul apendice nu se vizează aspecte legate de certificarea securității. Dacă unele teste necesare pentru omologarea de tip sunt efectuate în cadrul procesului de evaluare și de certificare a securității, ele nu mai trebuie repetate. Într-un asemenea caz, este suficientă inspectarea rezultatelor acestor teste de securitate. În scop informativ, cerințele care ar urma să fie testate (sau cele strâns legate de testele care ar urma să fie efectuate) în cadrul certificării securității sunt marcate cu un „*” în cuprinsul prezentului apendice.

Cerințele numerotate se referă la corpusul anexei, în timp ce celelalte cerințe se referă la celelalte apendice (de exemplu, PIC_001 se referă la cerința PIC_001 din apendicele 3, „Pictograme”).

Prezentul apendice tratează separat omologarea de tip a senzorului de mișcare, a unității montate pe vehicul și a echipamentului GNSS extern în calitate de componente ale aparaturii de înregistrare. Fiecare componentă va primi propriul certificat de omologare de tip în care vor fi indicate celelalte componente compatibile. Testul de funcționare a senzorului de mișcare (sau a echipamentului GNSS extern) se efectuează împreună cu testul de funcționare a unității montate pe vehicul și viceversa.

Interoperabilitatea dintre fiecare model de senzor de mișcare (respectiv echipament GNSS extern) și fiecare model de unitate montată pe vehicul nu este necesară. În acest caz, omologarea de tip a unui senzor de mișcare (respectiv, echipament GNSS extern) poate fi acordată numai în combinație cu omologarea de tip a unității montate pe vehicul corespunzătoare și viceversa.

1.2. **Referințe**

În prezentul apendice se utilizează următoarele referințe:

IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Rece

IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat (sinusoidal).

IEC 60068-2-6: Environmental testing – Part 2: Tests – Test Fc: Vibration

IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature

IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock

IEC 60068-2-30: Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)

IEC 60068-2-64: Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance

IEC 60068-2-78 Environmental testing – Part 2-78: Tests – Test Cab: Damp heat, steady state

ISO 16750-3 – Mechanical loads (2012-12)

ISO 16750-4 – Climatic loads(2010-04).

ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access

ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014 Road vehicles – Test methods for electrical disturbances from electrostatic discharge

ISO 7637-1:2002 + AMD1: 2008 Road vehicles – Electrical disturbances from conduction and coupling – Part 1: Definitions and general considerations.

ISO 7637-2 Road vehicles – Electrical disturbances from conduction and coupling – Part 2: Electrical transient conduction along supply lines only.

ISO 7637-3 Road vehicles – Electrical disturbances from conduction and coupling – Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines.

ISO/IEC 7816-1 Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics..

ISO/IEC 7816-2 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts.

ISO/IEC 7816-3 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Semnale electronice și protocol de transmisie.

ISO/IEC 10373-1:2006 + AMD1:2012 Identification cards – Test methods – Part 1: Caracteristici generale

ISO/IEC 10373-3:2010 + Technical Corrigendum:2013 Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices

ISO 16844-3:2004, Cor 1:2006 Road vehicles – Tachograph systems – Part 3: Motion sensor interface (with vehicle units).

ISO 16844-4 Road vehicles – Tachograph systems – Part 4: CAN interface

ISO 16844-6 Road vehicles – Tachograph systems – Part 6: Diagnostics

ISO 16844-7 Road vehicles – Tachograph systems – Part 7: Parameters

ISO 534 Paper and board – Determination of thickness, density and specific volume

UN ECE R10 Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility (United Nation Economic Commission for Europe)

2. TESTE DE FUNCȚIONARE A UNITĂȚII MONTATE PE VEHICUL

Nr.	Test	Descriere	Cerințe asociate
1	**Examinare administrativă**		
1.1	Documentație	Corectitudinea documentației	
1.2	Rezultatele testelor efectuate de producător	Rezultatele testului efectuat de producător în cursul integrării. Documente pentru demonstrarea testelor efectuate.	88, 89, 91
2	**Inspecție vizuală**		
2.1	Conformitatea cu documentația		
2.2	Identificare/inscripții		224 – 226
2.3	Materiale		219 – 223
2.4	Sigilare		398, 401 – 405
2.5	Interfețe externe		
3	**Teste de funcționare**		
3.1	Funcții oferite		03, 04, 05, 07, 382,
3.2	Moduri de funcționare		09 – 11*, 132, 133
3.3	Funcții și drepturi de acces la date		12*, 13*, 382, 383, 386 – 389
3.4	Monitorizarea introducerii și retragerii cardurilor		15, 16, 17, 18, 19*, 20*, 132
3.5	Măsurarea vitezei și a distanței		21 – 31
3.6	Măsurarea timpului (teste efectuate la 20 °C)		38 – 43
3.7	Monitorizarea activităților conducătorului auto		44 – 53, 132
3.8	Monitorizarea regimului de conducere		54, 55, 132

Nr.	Test	Descriere	Cerințe asociate
3.9	Introducerea manuală a datelor		56 – 62
3.10	Gestionarea blocărilor efectuate de societate		63 – 68
3.11	Monitorizarea activităților de control		69, 70
3.12	Detectarea de evenimente și/sau anomalii		71 – 88 132
3.13	Date de identificare a echipamentelor		93*, 94*, 97, 100
3.14	Date privind introducerea și retragerea cardului de conducător auto		102* – 104*
3.15	Date privind activitatea conducătorului auto		105* – 107*
3.16	Date privind locurile și pozițiile		108* – 112*
3.17	Date privind odometrul		113* – 115*
3.18	Date privind viteza detaliată		116*
3.19	Date privind evenimentele		117*
3.20	Date privind anomaliile		118*
3.21	Date privind etalonarea		119* – 121*
3.22	Date privind reglarea orei		124*, 125*
3.23	Date privind activitățile de control		126*, 127*
3.24	Date privind blocările efectuate de societate		128*
3.25	Date privind activitatea de descărcare		129*
3.26	Date privind condițiile specifice		130*, 131*
3.27	Înregistrarea și stocarea informațiilor pe cardurile de tahograf		134, 135,, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Afișare		90, 132, 149 – 166, PIC_001, DIS_001
3.29	Imprimare		90, 132, 167 – 179, PIC_001, PRT_001 – PRT_014
3.30	Avertizare		132, 180 – 189, PIC_001

Nr.	Test	Descriere	Cerințe asociate
3.31	Descărcarea datelor pe suporturi externe		90, 132, 190 – 194
3.32	Comunicarea la distanță pentru controalele selective în trafic		195 – 197
3.33	Date de ieșire transmise unor dispozitive externe suplimentare		198, 199
3.34	Etalonare		202 – 206*, 383, 384, 386 – 391
3.35	Verificarea etalonării în trafic		207 – 209
3.36	Reglarea orei		210 – 212*
3.37	Neinterferența cu funcțiile suplimentare		06, 425
3.38	Interfața senzorului de mișcare		02, 122
3.39	Echipamentul GNSS extern		03, 123
3.40	Se verifică dacă VU detectează, înregistrează și stochează evenimentul (evenimentele) și/sau anomalia (anomaliile) definite de producătorul VU atunci când un senzor de mișcare asociat reacționează la câmpurile magnetice care perturbă detectarea deplasării vehiculului.		217
3.41	Suite cifru și parametri de domeniu standardizați		CSM_48, CSM_50
4	**Teste de mediu**		
4.1	Temperatură	Verificarea funcționalității prin: Test în conformitate cu ISO 16750-4, Chapter 5.1.1.2: Low temperature operation test (72 h @ – 20 °C) Acest test se referă la IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold Test în conformitate cu ISO 16750-4: Chapter 5.1.2.2: High temperature operation test (72 h at 70 °C) Acest test se referă la IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Test în conformitate cu ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 cycles, dwell time 2h at each temperature) Un număr redus de teste (dintre cele definite în secțiunea 3 din prezentul tabel) pot fi efectuate la temperatura cea mai scăzută, la temperatura cea mai ridicată și pe parcursul ciclurilor de temperatură	213

Nr.	Test	Descriere	Cerințe asociate
4.2	Umiditate	Se verifică, prin intermediul testului Db IEC 60068-2-30, dacă unitatea montată pe vehicul poate suporta un ciclu de căldură umedă (test de căldură), prin șase cicluri de câte 24 de ore fiecare, cu temperaturi variind între + 25 °C și + 55 °C la o umiditate relativă de 97 % la + 25 °C și egală cu 93 % la + 55 °C	214
4.3	Teste mecanice	1. Vibrații sinusoidale. Se verifică dacă unitatea montată pe vehicul poate suporta vibrații sinusoidale cu următoarele caracteristici: deplasare constantă la frecvențe între 5 și 11 Hz: valoare maximă 10 mm accelerație constantă între 11 și 300 Hz: 5 g Această cerință este verificată prin intermediul testului Fc IEC 60068-2-6, cu o durată minimă a testului de 3 × 12 ore (12 ore per axă) ISO 16750-3 nu prevede un test de vibrații sinusoidale pentru dispozitivele situate în cabina decuplată a vehiculului. 2. Vibrații aleatorii: Test în conformitate cu ISO 16750-3: Chapter 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab Test de vibrații aleatorii, 10…2 000 Hz, RMS vertical 21,3 m/s^2, RMS longitudinal 11,8 m/s^2, RMS lateral 13,1 m/s^2, 3 axe, 32 de ore per axă, inclusiv ciclul de temperatură – 20…70 °C. Acest test se referă la IEC 60068-2-64: Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance 3. Șocuri: șoc mecanic semisinusoidal 3 g în conformitate cu ISO 16750. Testele descrise anterior se efectuează pe mostre diferite ale tipului de echipament testat.	219
4.4	Protecție împotriva apei și corpurilor străine	Test în conformitate cu ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (No change in parameters); Valoare minimă IP 40	220, 221
4.5	Protecție împotriva supratensiunii	Se verifică dacă unitatea montată pe vehicul poate suporta o sursă de alimentare de: Pentru versiunile de 24 V: 34 V la + 40 °C 1 oră Pentru versiunile de 12 V: 17 V la + 40 °C 1 oră (ISO 16750-2)	216
4.6	Protecție împotriva polarității inverse	Se verifică dacă unitatea montată pe vehicul poate suporta o inversare a polarității la sursa de alimentare (ISO 16750-2)	216

Nr.	Test	Descriere	Cerințe asociate
4.7	Protecție împotriva scurtcircuitelor	Se verifică dacă semnalele de intrare/ieșire sunt protejate împotriva scurtcircuitelor la sursa de alimentare și la masă (ISO 16750-2)	216
5	**Teste CEM**		
5.1	Emisii de radiații și susceptibilitate de radiații	Conformitate cu Regulamentul R10 al CEE	218
5.2	Descărcări electrostatice	Conformitate cu ISO 10605:2008 + Rectificare tehnică:2010 + AMD1:2014: +/– 4kV pentru contact și +/– 8kV pentru evacuarea aerului	218
5.3	Susceptibilitate de conducție tranzitorie la sursa de alimentare	Pentru versiunile de 24 V: conformitate cu ISO 7637-2 + Regulamentul nr. 10 al CEE Rev. 3: puls 1a: Vs = – 450 V Ri = 50 ohmi puls 2a: Vs = + 37 V Ri = 2 ohmi puls 2b: Vs = + 20 V Ri = 0,05 ohmi puls 3a: Vs = – 150 V Ri = 50 ohmi puls 3b: Vs = + 150 V Ri = 50 ohmi puls 4: Vs = – 16 V Va = – 12 V t6 = 100ms puls 5: Vs = + 120 V Ri = 2,2 ohmi td = 250ms Pentru versiunile de 12 V: conformitate cu ISO 7637-1 + Regulamentul nr. 10 al CEE Rev. 3: puls 1: Vs = – 75 V Ri = 10 ohmi puls 2a: Vs = + 37 V Ri = 2 ohmi puls 2b: Vs = + 10 V R i= 0,05 ohmi puls 3a: Vs = – 112 V Ri = 50 ohmi puls 3b: Vs = + 75 V Ri = 50 ohmi puls 4: Vs = –6 V Va = – 5 V t6 = 15ms puls 5: Vs = + 65 V Ri = 3 ohmi td = 100ms Pulsul 5 se testează numai pentru unitățile montate pe vehicule care sunt proiectate pentru a fi instalate în vehicule care nu dispun de o protecție externă obișnuită împotriva întreruperii alimentării Pentru propunerea privind întreruperea alimentării, a se vedea ISO 16750-2, a 4-a ediție, capitolul 4.6.4.	218

3. TESTE DE FUNCȚIONARE A SENZORULUI DE MIȘCARE

Nr.	Test	Descriere	Cerințe asociate
1.	**Examinare administrativă**		
1.1	Documentație	Corectitudinea documentației	

Nr.	Test	Descriere	Cerințe asociate
2.	**Inspecție vizuală**		
2.1.	Conformitatea cu documentația		
2.2.	Identificare/inscripții		225, 226,
2.3	Materiale		219 – 223
2.4.	Sigilare		398, 401 – 405
3.	**Teste de funcționare**		
3.1	Date de identificare a senzorului		95 – 97*
3.2	Asociere senzor de mișcare – unitate montată pe vehicul		122*, 204
3.3	Detectarea mișcării Precizia măsurării mișcării		30 – 35
3.4	Interfața unității montate pe vehicul		02
3.5	Se verifică dacă senzorul de mișcare este imun la un câmp magnetic constant. Alternativ, se verifică dacă senzorul de mișcare reacționează la câmpurile magnetice constante care perturbă detectarea deplasării vehiculului astfel încât o VU conectată să poată detecta, înregistra și stoca anomaliile senzorului		217
4.	**Teste de mediu**		
4.1	Temperatura de funcționare	Se verifică funcționalitatea (conform definiției din testul nr. 3.3) pentru intervalul de temperatură [– 40 °C; + 135 °C] prin: testul Ad, IEC 60068-2-1, cu o durată de 96 de ore a testului la temperatura minimă To_{min} testul Bd, IEC 60068-2-2, cu o durată a testului de 96 de ore la temperatura maximă To_{max} Test în conformitate cu ISO 16750-4: Chapter 5.1.1.2: Low temperature operation test (24 h @ – 40 °C) Acest test se referă la IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold IEC 68-2-2 test Bd, with a test duration of 96 hours at the lowest temperature of – 40 °C. Test în conformitate cu ISO 16750-4: Chapter 5.1.2.2: Low temperature operation test (96 h @ 135 °C) Acest test se referă la IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat	213

Nr.	Test	Descriere	Cerințe asociate
4.2	Cicluri de temperatură	Test în conformitate cu ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (– 40 °C/135 °C, 20 cycles, dwell time 30 min at each temperature) IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature	213
4.3	Cicluri de umiditate	Se verifică funcționalitatea (conform definiției din testul nr. 3.3) prin testul Db, IEC 60068-2-30, prin șase cicluri de câte 24 de ore fiecare, temperatura variind în cadrul fiecărui ciclu între + 25 °C și + 55 °C, la o umiditate relativă de 97 % la + 25 °C și egală cu 93 % la + 55 °C	214
4.4	Vibrații	ISO 16750-3: Chapter 4.1.2.6: Test VI: Commercial vehicle, engine, gearbox Test de vibrații în mod mixt, care include: a) Test de vibrații sinusoidale, 20...520 Hz, 11,4 ... 120 m/s^2, <= 0,5 oct/min b) Test de vibrații aleatorii, 10...2 000 Hz, RMS 177 m/s^2 94 de ore pe axă, inclusiv ciclul de temperatură -20...70 °C) Acest test se referă la IEC 60068-2-80: Environmental testing – Part 2-80: Tests – Test Fi: Vibration – Mixed mode	219
4.5	Șoc mecanic	ISO 16750-3: Chapter 4.2.3: Test VI: Test for devices in or on the gearbox șoc semisinusoidal, accelerație de stabilit în intervalul 3 000...15 000 m/s^2, durata pulsului de stabilit, dar < 1 ms, număr de șocuri: de stabilit Acest test se referă la IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock	219
4.6	Protecție împotriva apei și corpurilor străine	Test în conformitate cu ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (Valoare țintă IP 64)	220, 221
4.7	Protecție împotriva polarității inverse	Se verifică dacă senzorul de mișcare poate suporta o inversare a polarității la sursa de alimentare	216
4.8	Protecție împotriva scurtcircuitelor	Se verifică dacă semnalele de intrare/ieșire sunt protejate împotriva scurtcircuitelor la sursa de alimentare și la masă	216

Nr.	Test	Descriere	Cerințe asociate
5.	**CEM**		
5.1	Emisii de radiații și susceptibilitate de radiații	Se verifică conformitatea cu Regulamentul R10 al CEE	218
5.2	Descărcări electrostatice	Conformitate cu ISO 10605:2008 + Rectificare tehnică:2010 + AMD1:2014: +/- 4kV pentru contact și +/- 8kV pentru evacuarea aerului	218
5.3	Susceptibilitate de conducție tranzitorie la sursa de alimentare)	Pentru versiunile de 24 V: conformitate cu ISO 7637-2 + Regulamentul nr. 10 al CEE Rev. 3: puls 1a: Vs=-450 V Ri=50 ohmi puls 2a: Vs=+37 V Ri=2 ohmi puls 2b: Vs=+20 V Ri=0,05 ohmi puls 3a: Vs=-150 V Ri=50 ohmi puls 3b: Vs=+150 V Ri=50 ohmi puls 4: Vs=-16 V Va=-12 V t6=100ms puls 5: Vs=+120 V Ri=2,2 ohmi td=250ms Pentru versiunile de 12 V: conformitate cu ISO 7637-1 + Regulamentul nr. 10 al CEE Rev. 3: puls 1: Vs=-75 V Ri=10 ohmi puls 2a: Vs=+37 V Ri=2 ohmi puls 2b: Vs=+10 V Ri=0,05 ohmi puls 3a: Vs=-112 V Ri=50 ohmi puls 3b: Vs=+75 V Ri=50 ohmi puls 4: Vs=-6 V Va=-5 V t6=15ms puls 5: Vs=+65 V Ri=3 ohmi td=100ms Pulsul 5 se testează numai pentru unitățile montate pe vehicule care sunt proiectate pentru a fi instalate în vehicule care nu dispun de o protecție externă obișnuită împotriva întreruperii alimentării Pentru propunerea privind întreruperea alimentării, a se vedea ISO 16750-2, a 4-a ediție, capitolul 4.6.4.	218

4. TESTE DE FUNCȚIONARE A CARDURILOR DE TAHOGRAF

Testele în conformitate cu prezenta secțiune 4, numerele

5 „Teste privind protocoalele";

6 „Structura cardului" și

7 „Teste de funcționare"

pot fi efectuate de evaluator sau de certificator în cursul procesului de certificare a securității modulul cipului în conformitate cu criteriile comune (CC).

Testele cu numerele 2.3 și 4.2 sunt identice. Este vorba despre testele mecanice efectuate asupra ansamblului format din corpul cardului și modulul cipului. Aceste teste sunt necesare dacă una dintre aceste componente (corpul cardului, modulul cipului) este modificată.

Nr.	Test	Descriere	Cerințe asociate
1.	**Examinare administrativă**		
1.1	Documentație	Corectitudinea documentației	
2	**Corpul cardului**		
2.1	Elementele imprimate	Se verifică dacă toate elementele de protecție și toate datele vizibile sunt imprimate corect pe card și sunt conforme. [Identificator] Anexa 1C capitolul 4.1 „Date vizibile”, punctul 227) Pe recto figurează: cuvintele „Card de conducător auto” sau „Card de control” sau „Card de atelier” sau „Card de societate”, tipărite cu majuscule în limba sau limbile oficiale ale statului membru emitent, în funcție de tipul cardului. [Denumirea statului membru] Anexa 1C capitolul 4.1 „Date vizibile”, punctul 228) Pe recto figurează: denumirea statului membru emitent al cardului (opțional). [Indicativ] Anexa 1C capitolul 4.1 „Date vizibile”, punctul 229) Pe recto figurează: indicativul statului membru emitent al cardului, tipărit în negativ într-un dreptunghi albastru și înconjurat de 12 stele galbene. [Enumerare] Anexa 1C capitolul 4.1 „Date vizibile”, punctul 232) Pe verso figurează: explicații pentru elementele numerotate de pe recto-ul cardului. [Culoare] Anexa 1C capitolul 4.1 „Date vizibile”, punctul 234) Cardurile de tahograf se imprimă pe fonduri având următoarele culori predominante: — cardul de conducător auto: alb; — cardul de atelier: roșu; — cardul de control: albastru; — cardul de societate: galben.	227 – 229, 232, 234 – 236

Nr.	Test	Descriere	Cerințe asociate
		[Securitate] Anexa 1C capitolul 4.1 „Date vizibile”, punctul 235) Cardurile de tahograf trebuie să aibă cel puțin următoarele caracteristici pentru protecția corpului cardului împotriva falsificării și a manipulării frauduloase: — un fond de securitate cu ghioșe și irizat; — cel puțin o linie bicoloră microimprimată.	
		[Inscripții] Anexa 1C capitolul 4.1 „Date vizibile”, punctul 236) Statele membre pot adăuga culori sau inscripții cum ar fi simboluri naționale sau caracteristici de securitate.	
		[Marca de omologare] Cardurile de tahograf conțin o marcă de omologare. Marca de omologare constă în următoarele: — un dreptunghi în interiorul căruia se plasează litera „e” urmată de un număr sau de o literă distinctiv(ă) pentru țara care a emis omologarea; — un număr de omologare corespunzător numărului certificatului de omologare acordat unui card de tahograf, plasat oriunde în imediata apropiere a dreptunghiului susmenționat.	
2.2	Teste mecanice	[Mărimea cardului] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [5] Dimensiunea cardului; [5.1] Mărimea cardului; [5.1.1] Dimensiunile cardului și toleranțe; Card de tip ID-1 Card neutilizat	240, 243 ISO/IEC 7810
		[Marginile cardului] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [5] Dimensiunea cardului; [5.1] Mărimea cardului; [5.1.2] Marginile cardului	

Nr.	Test	Descriere	Cerințe asociate
		[Construcția cardului] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [6] Construcția cardului	
		[Materiale utilizate pentru fabricarea cardului] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [7] Materiale utilizate pentru fabricarea cardului	
		[Rigiditatea de îndoire] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.1] Rigiditate de îndoire	
		[Toxicitate] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.3] Toxicitate	
		[Rezistența la substanțe chimice] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.4] Rezistența la substanțe chimice	
		[Stabilitatea cardului] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.5] Stabilitatea dimensională a cardului și capacitatea de deformare sub efectul temperaturii și al umidității	

Nr.	Test	Descriere	Cerințe asociate
		[Lumină] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.6] Lumină	
		[Durabilitate] Anexa 1C capitolul 4.4, „Specificații de mediu și electrice”, punctul 241) Cardurile de tahograf trebuie să poată funcționa corect timp de cinci ani dacă sunt folosite conform specificațiilor de mediu și electrice.	
		[Rezistența stratului exterior] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.8] Rezistența stratului exterior	
		[Aderență sau blocare] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.9] Aderență sau blocare	
		[Capacitate de deformare] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.11] Capacitatea de deformare globală a cardului	
		[Rezistența la căldură] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.12] Rezistența la căldură	

Nr.	Test	Descriere	Cerințe asociate
		[Distorsiuni ale suprafeței] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.13] Distorsiuni ale suprafeței	
		[Contaminare] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810, Identification cards – Physical characteristics, [8] Caracteristicile cardului, [8.14] Contaminarea și interacțiunea componentelor cardului	
2.3	Teste mecanice cu modulul cipului integrat	[Îndoire] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Tensiune de îndoire dinamică Numărul total de cicluri de îndoire: 4 000.	ISO/IEC 7810
		[Torsiune] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Tensiune de torsiune dinamică Numărul total de cicluri de torsiune: 4 000.	
3	**Modul**		
3.1	Modul	Modulul este alcătuit din capsula ermetică și plotul cipului. [Profil de suprafață] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.2] Profilul de suprafață al contactelor	ISO/IEC 7816

Nr.	Test	Descriere	Cerințe asociate
		[Rezistență mecanică] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.3] Rezistență mecanică (a unui card și a contactelor)	
		[Rezistență electrică] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.4] Rezistență electrică (a contactelor)	
		[Dimensiune] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7816-2:2007, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts [3] Dimensiunea contactelor	
		[Locație] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7816-2:2007, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts [4] Numărul și locația contactelor În cazul modulelor cu șase contacte, contactele „C4” și „C8” nu fac obiectul acestei cerințe de testare.	
4	**Cip**		
4.1	Cip	[Temperatura de funcționare] Cipul cardului de tahograf funcționează în intervalul de temperatură ambientală dintre – 25 °C și + 85 °C.	241 – 244 R10 al CEE ISO/IEC 7810 ISO/IEC 10373

Nr.	Test	Descriere	Cerințe asociate
		[Temperatură și umiditate] Anexa 1C capitolul 4.4, „Specificații de mediu și electrice”, punctul 241) Cardurile de tahograf trebuie să poată funcționa corect în toate condițiile climatice întâlnite în mod normal pe teritoriul Uniunii și cel puțin în intervalul de temperatură cuprins între – 25 °C și + 70 °C, cu creșteri ocazionale ale temperaturii de până la + 85 °C; „ocazional” înseamnă timp de cel mult 4 ore o dată și de cel mult 100 de ori pe întreaga durată de viață a cardului. Cardurile de tahograf sunt expuse, în etape consecutive, la următoarele temperaturi și niveluri de umiditate, pe durata indicată. După fiecare etapă, se testează funcționalitatea electrică a cardurilor de tahograf. 1. Temperatură de – 20 °C timp de 2 h. 2. Temperatură de +/– 0 °C timp de 2 h. 3. Temperatură de + 20 °C, umiditate relativă de 50 %, timp de 2 h. 4. Temperatură de + 50 °C, umiditate relativă de 50 %, timp de 2 h. 5. Temperatură de + 70 °C, umiditate relativă de 50 %, timp de 2 h. Temperatura este mărită intermitent la + 85 °C, umiditate relativă de 50 %, timp de 60 min. 6. Temperatură de + 70 °C, umiditate relativă de 85 %, timp de 2 h. Temperatura este mărită intermitent la + 85 °C, umiditate relativă de 85 %, timp de 30 min.	
		[Umiditate] Anexa 1C capitolul 4.4, „Specificații de mediu și electrice”, punctul 242) Cardurile de tahograf trebuie să poată funcționa corect în intervalul de umiditate cuprins între 10 % și 90 %.	
		[Compatibilitate electromagnetică – CEM] Anexa 1C capitolul 4.4, „Specificații de mediu și electrice”, punctul 244) În cursul funcționării, cardurile de tahograf respectă R10 al CEE, referitor la compatibilitatea electromagnetică.	

Nr.	Test	Descriere	Cerințe asociate
		[Electricitate statică] Anexa 1C capitolul 4.4, „Specificații de mediu și electrice”, punctul 244) În timpul funcționării, cardurile de tahograf sunt protejate împotriva descărcărilor electrostatice. Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.4] Electricitate statică [9.4.1] Carduri IC cu contacte Tensiune de testare: 4 000 V.	
		[raze X] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.1] Raze X	
		[Lumină ultravioletă] ISO/IEC 10373-1:2006, Identification cards – Test methods – Part 1: General characteristics [5.11] Lumină ultravioletă	
		[cu 3 roți] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 10373-1:2006/Amd. 1:2012, Identification cards – Test methods – Part 1: General characteristics, Amendment 1 [5.22] Carduri IC – Rezistență mecanică: test cu 3 roți pentru carduri IC cu contacte	
		[Învelișul] Cardurile de tahograf trebuie să respecte standardul MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Testarea rezistenței învelișului [13.2.1.32] TM-422: Fiabilitate mecanică: Test privind ambalajul	

Nr.	Test	Descriere	Cerințe asociate
4.2	Teste mecanice cu modulul cipului integrat în corpul cardului-> identic cu 2.3	[Îndoire] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Tensiune de îndoire dinamică Numărul total de cicluri de îndoire: 4 000. [Torsiune] Cardurile de tahograf trebuie să respecte standardul ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Tensiune de torsiune dinamică Numărul total de cicluri de torsiune: 4 000.	ISO/IEC 7810
5	**Teste privind protocoalele**		
5.1	ATR	Se verifică dacă ATR este conform	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T = 0	Se verifică dacă protocolul T = 0 este conform	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Se verifică conformitatea comenzii PTS prin schimbarea protocolului T = 0 în T = 1	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T = 1	Se verifică dacă protocolul T = 1 este conform	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Structura cardului**		
6.1		Se testează conformitatea structurii de fișiere a cardului, verificându-se prezența pe card a fișierelor obligatorii și condițiile de acces ale acestora	TCS_22 – TCS_28 TCS_140 – TCS_179
7	**Teste de funcționare**		
7.1	Procesare normală	Se testează cel puțin o dată fiecare utilizare permisă a fiecărei comenzi (de ex.: se testează comanda UPDATE BINARY cu CLA = '00', CLA = '0C' și cu parametri P1, P2 și Lc diferiți) Se verifică dacă operațiunile au fost efectiv efectuate pe card (de ex.: prin citirea fișierului pe care s-a executat comanda)	TCS_29 – TCS_139

Nr.	Test	Descriere	Cerințe asociate
7.2	Mesaje de eroare	Se testează cel puțin o dată fiecare mesaj de eroare (conform apendicelui 2) pentru fiecare comandă. Se testează cel puțin o dată fiecare eroare generică (cu excepția erorilor de integritate '**6400**' verificate în cadrul certificării de securitate)	
7.3	Suite cifru și parametri de domeniu standardizați		CSM_48, CSM_50
8	**Personalizare**		
8.1	Personalizare optică	Anexa 1C capitolul 4.1 „Date vizibile", punctul 230) Pe recto figurează: informații specifice pentru cardul emis. Anexa 1C capitolul 4.1 „Date vizibile", punctul 231) Pe recto figurează: datele în format „zz/ll/aaaa" sau „zz.ll.aaaa" (zi, lună, an). Anexa 1C capitolul 4.1 „Date vizibile", punctul 235) Cardurile de tahograf trebuie să aibă cel puțin următoarele caracteristici pentru protecția corpului cardului împotriva falsificării și a manipulării frauduloase: — în zona fotografiei, fondul de securitate și fotografia se suprapun.	230, 231, 235

5. TESTE PRIVIND ECHIPAMENTUL GNSS EXTERN

Nr.	Test	Descriere	Cerințe asociate
1.	**Examinare administrativă**		
1.1	Documentație	Corectitudinea documentației	
2.	**Inspecție vizuală a echipamentului GNSS extern**		
2.1.	Conformitatea cu documentația		
2.2.	Identificare/inscripții		224 – 226
2.3	Materiale		219 – 223
3.	**Teste de funcționare**		
3.1	Date de identificare a senzorului		98,99
3.2	Cuplare între echipamentul GNSS extern și unitatea montată pe vehicul		123, 205

Nr.	Test	Descriere	Cerințe asociate
3.3	Poziție GNSS		36, 37
3.4	Interfața unității montate pe vehicul atunci când receptorul GNSS este exterior unității montate pe vehicul		03
3.5	Suite cifru și parametri de domeniu standardizați		CSM_48, CSM_50
4.	**Teste de mediu**		
4.1	Temperatură	Verificarea funcționalității prin: Test în conformitate cu ISO 16750-4, Chapter 5.1.1.2: Low temperature operation test (72 h @ – 20 °C) Acest test se referă la IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold Test în conformitate cu ISO 16750-4: Chapter 5.1.2.2: High temperature operation test (72 h @ 70 °C) Acest test se referă la IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Test în conformitate cu ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (-20°C/70 °C, 20 cycles, dwell time 1h at each temperature) Un număr redus de teste (dintre cele definite în secțiunea 3 din prezentul tabel) pot fi efectuate la temperatura cea mai scăzută, la temperatura cea mai ridicată și pe parcursul ciclurilor de temperatură	213
4.2	Umiditate	Se verifică, prin intermediul testului Db, IEC 60068-2-30, dacă unitatea montată pe vehicul poate suporta un ciclu de căldură umedă (testul de căldură), prin șase cicluri de câte 24 de ore fiecare, cu temperaturi variind între + 25 °C și + 55 °C la o umiditate relativă de 97 % la + 25 °C și egală cu 93 % la + 55 °C	214
4.3	Teste mecanice	1. Vibrații sinusoidale. Se verifică dacă unitatea montată pe vehicul poate suporta vibrații sinusoidale cu următoarele caracteristici: deplasare constantă la frecvențe între 5 și 11 Hz: valoare maximă 10 mm accelerație constantă între 11 și 300 Hz: 5 g Această cerință este verificată prin intermediul testului Fc, IEC 60068-2-6, cu o durată minimă a testului de 3 × 12 ore (12 ore per axă) ISO 16750-3 nu prevede un test de vibrații sinusoidale pentru dispozitivele situate în cabina decuplată a vehiculului.	219

Nr.	Test	Descriere	Cerințe asociate
		2. Vibrații aleatorii: Test în conformitate cu ISO 16750-3: Chapter 4.1.2.8: Testul VIII: Commercial vehicle, decoupled vehicle cab Test de vibrații aleatorii, 10…2 000 Hz, RMS vertical 21,3 m/s^2, RMS longitudinal 11,8 m/s^2, RMS lateral 13,1 m/s^2, 3 axe, 32 de ore per axă, inclusiv ciclul de temperatură – 20…70 °C. Acest test se referă la IEC 60068-2-64: Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broad-band random and guidance 3. Șocuri: șoc mecanic semisinusoidal 3 g în conformitate cu ISO 16750. Testele descrise anterior se efectuează pe mostre diferite ale tipului de echipament testat.	
4.4	Protecție împotriva apei și corpurilor străine	Test în conformitate cu ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (No change in parameters)	220, 221
4.5	Protecție împotriva supratensiunii	Se verifică dacă unitatea montată pe vehicul poate suporta o sursă de alimentare de: Pentru versiunile de 24 V: 34 V la + 40 °C 1 oră Pentru versiunile de 12 V: 17 V la + 40 °C 1 oră (ISO 16750-2, capitolul 4.3)	216
4.6	Protecție împotriva polarității inverse	Se verifică dacă unitatea montată pe vehicul poate suporta o inversare a polarității la sursa de alimentare (ISO 16750-2, capitolul 4.7)	216
4.7	Protecție împotriva scurtcircuitelor	Se verifică dacă semnalele de intrare/ieșire sunt protejate împotriva scurtcircuitelor la sursa de alimentare și la masă (ISO 16750-2, capitolul 4.10)	216
5	**Teste CEM**		
5.1	Emisii de radiații și susceptibilitate de radiații	Conformitate cu Regulamentul R10 al CEE	218

Nr.	Test	Descriere	Cerințe asociate
5.2	Descărcări electrostatice	Conformitate cu ISO 10605:2008 + Rectificare tehnică:2010 + AMD1:2014: +/– 4kV pentru contact și +/– 8kV pentru evacuarea aerului	218
5.3	Susceptibilitate de conducție tranzitorie la sursa de alimentare	Pentru versiunile de 24 V: conformitate cu ISO 7637-2 + Regulamentul nr. 10 al CEE Rev. 3: puls 1a: Vs = – 450 V Ri = 50 ohmi puls 2a: Vs = + 37 V Ri = 2 ohmi puls 2b: Vs = + 20 V Ri = 0,05 ohmi puls 3a: Vs = – 150 V Ri = 50 ohmi puls 3b: Vs = + 150 V Ri = 50 ohmi puls 4: Vs = –16 V Va = –12 V t6 = 100ms puls 5: Vs = + 120 V Ri = 2,2 ohmi td = 250ms Pentru versiunile de 12 V: conformitate cu ISO 7637-1 + Regulamentul nr. 10 al CEE Rev. 3: puls 1: Vs = – 75 V Ri = 10 ohmi puls 2a: Vs = + 37 V Ri = 2 ohmi puls 2b: Vs = + 10 V Ri = 0,05 ohmi puls 3a: Vs = – 112 V Ri = 50 ohmi puls 3b: Vs = + 75 V Ri = 50 ohmi puls 4: Vs = – 6 V Va = – 5 V t6 = 15ms puls 5: Vs = + 65 V Ri = 3 ohmi td = 100ms Pulsul 5 se testează numai pentru unitățile montate pe vehicule care sunt proiectate pentru a fi instalate în vehicule care nu dispun de o protecție externă obișnuită împotriva întreruperii alimentării Pentru propunerea privind întreruperea alimentării, a se vedea ISO 16750-2, a 4-a ediție, capitolul 4.6.4.	218

6. TESTE PRIVIND ECHIPAMENTUL DE COMUNICARE LA DISTANȚĂ

Nr.	Test	Descriere	Cerințe asociate
1.	**Examinare administrativă**		
1.1	Documentație	Corectitudinea documentației	
2.	**Inspecție vizuală**		
2.1.	Conformitatea cu documentația		
2.2.	Identificare/inscripții		225, 226
2.3	Materiale		219 – 223

Nr.	Test	Descriere	Cerințe asociate
4.	**Teste de mediu**		
4.1	Temperatură	Verificarea funcționalității prin: Test în conformitate cu ISO 16750-4, Chapter 5.1.1.2: Low temperature operation test (72 h @ -20 °C) Acest test se referă la IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold Test în conformitate cu ISO 16750-4: Chapter 5.1.2.2: High temperature operation test (72 h @ 70 °C) Acest test se referă la IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Test în conformitate cu ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 cycles, dwell time 1 h (?) at each temperature) Un număr redus de teste (dintre cele definite în secțiunea 3 din prezentul tabel) pot fi efectuate la temperatura cea mai scăzută, la temperatura cea mai ridicată și pe parcursul ciclurilor de temperatură	213
4.4	Protecție împotriva apei și corpurilor străine	Test în conformitate cu ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (targeted value IP40)	220, 221
5	**Teste CEM**		
5.1	Emisii de radiații și susceptibilitate de radiații	Conformitate cu Regulamentul R10 al CEE	218
5.2	Descărcări electrostatice	Conformitate cu ISO 10605:2008 + Rectificare tehnică:2010 + AMD1:2014: +/– 4kV pentru contact și +/– 8kV pentru evacuarea aerului	218
5.3	Susceptibilitate de conducție tranzitorie la sursa de alimentare	Pentru versiunile de 24 V: conformitate cu ISO 7637-2 + Regulamentul nr. 10 al CEE Rev. 3: puls 1a: Vs = – 450 V Ri = 50 ohmi puls 2a: Vs = + 37 V Ri = 2 ohmi puls 2b: Vs = + 20 V Ri = 0,05 ohmi puls 3a: Vs = – 150 V Ri = 50 ohmi puls 3b: Vs = + 150 V Ri = 50 ohmi puls 4: Vs = – 16 V Va = – 12 V t6=100ms puls 5: Vs = + 120 V Ri = 2,2 ohmi td = 250ms	218

Nr.	Test	Descriere	Cerințe asociate
		Pentru versiunile de 12 V: conformitate cu ISO 7637-1 + Regulamentul nr. 10 al CEE Rev. 3: puls 1: Vs = – 75 V Ri = 10 ohmi puls 2a: Vs = + 37 V Ri = 2 ohmi puls 2b: Vs = + 10 V Ri = 0,05 ohmi puls 3a: Vs = – 112 V Ri = 50 ohmi puls 3b: Vs = + 75 V Ri = 50 ohmi puls 4: Vs = – 6 V Va = – 5 V t6 = 15ms puls 5: Vs = + 65 V Ri = 3 ohmi td = 100ms Pulsul 5 se testează numai pentru unitățile montate pe vehicule care sunt proiectate pentru a fi instalate în vehicule care nu dispun de o protecție externă obișnuită împotriva întreruperii alimentării Pentru propunerea privind întreruperea alimentării, a se vedea ISO 16750-2, a 4-a ediție, capitolul 4.6.4.	

7. TESTE DE FUNCȚIONARE PRIVIND HÂRTIA

Nr.	Test	Descriere	Cerințe asociate
1.	**Examinare administrativă**		
1.1	Documentație	Corectitudinea documentației	
2	**Teste generale**		
2.1	Număr de caractere pe fiecare rând	Inspecție vizuală a documentelor imprimate.	172
2.2	Dimensiunea minimă a caracterelor	Inspecție vizuală a documentului imprimat și verificarea caracterelor.	173
2.3	Seturi de caractere compatibile	Imprimanta trebuie să fie compatibilă cu caracterele specificate în apendicele 1 capitolul 4, „Seturi de caractere”.	174
2.4	Definiția documentelor imprimate	Verificarea omologării de tip a tahografului și inspecția vizuală a documentelor imprimate	174
2.5	Lizibilitatea și identificarea documentelor imprimate	Inspectarea documentelor imprimate Demonstrate prin rapoarte de testare și protocoale de testare de către producător. Toate numerele de omologare ale tahografelor cu care poate fi utilizată imprimanta sunt imprimate pe hârtie.	175, 177, 178
2.6	Adăugarea de mențiuni scrise de mână	Inspecție vizuală: Este disponibil un câmp pentru semnătura conducătorului auto. Sunt disponibile câmpuri pentru alte mențiuni scrise de mână.	180

Nr.	Test	Descriere	Cerințe asociate
2.7	Detalii suplimentare privind fețele hârtiei.	Pe ambele fețe ale hârtiei pot figura detalii și informații suplimentare. Aceste detalii și informații suplimentare nu trebuie să afecteze lizibilitatea documentelor imprimate. Inspecție vizuală.	177, 178
3	**Teste privind stocarea**		
3.1	Căldură uscată	Condiții prealabile: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ±3 % Mediul de testare: 72 ore la + 70 °C ± 2 °C Recuperare: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 %	176, 178 IEC 60068-2-2-Bb
2.2	Căldură umedă	Condiții prealabile: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 % Mediul de testare: 144 ore la + 55 °C ± 2 °C și umiditate relativă de 93 % ± 3 % Recuperare: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 %	176, 178 IEC 60068-2-78-Cab
4	**Teste privind utilizarea hârtiei**		
4.1	Rezistența la umiditate a fundalului (hârtie neimprimată)	Condiții prealabile: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 % Mediul de testare: 144 ore la + 55 °C ± 2 °C și umiditate relativă de 93 % ± 3 % Recuperare: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 %	176, 178 IEC 60068-2-78-Cab
4.2	Capacitatea de imprimare	Condiții prealabile: 24 ore la + 40 °C ± 2 °C/umiditate relativă de 93 % ±3 % Mediul de testare: document imprimat la + 23 °C ± 2 °C Recuperare: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 %	176, 178
4.3	Rezistența la căldură	Condiții prealabile: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 % Mediul de testare: 2 ore la + 70 °C ± 2 °C, căldură uscată Recuperare: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 %	176, 178 IEC 60068-2-2-Bb
4.4	Rezistența la temperatură scăzută	Condiții prealabile: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ±3 % Mediul de testare: 24 de ore la -20 °C ± 3 °C, căldură umedă Recuperare: 16 ore la +23 °C ± 2 °C/umiditate relativă de 55 % ± 3 %	176, 178 ISO 60068-2-1-Ab

Nr.	Test	Descriere	Cerințe asociate
4.5	Rezistența la lumină	Condiții prealabile: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 % Mediu de testare: 100 ore, la o iluminare de 5 000 de lucși, la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 % Recuperare: 16 ore la + 23 °C ± 2 °C/umiditate relativă de 55 % ± 3 %	176, 178

Criterii de lizibilitate pentru testele 3.x și 4.x:

Lizibilitatea documentelor imprimate este asigurată dacă densitățile optice respectă următoarele limite:

Caractere imprimate: min. 1,0

Fundal (hârtie neimprimată): max. 0,2

Densitățile optice ale documentelor imprimate rezultate se măsoară conform standardului DIN EN ISO 534.

Documentele imprimate trebuie să nu prezinte modificări ale dimensiunilor și să rămână perfect lizibile.

8. TESTE DE INTEROPERABILITATE

Nr.	Test	Descriere
9.1 Teste de interoperabilitate între unități montate pe vehicule și carduri de tahograf		
1	Autentificare reciprocă	Se verifică dacă autentificarea reciprocă dintre unitatea montată pe vehicul și cardul de tahograf se produce normal
2	Teste de scriere/citire	Se execută un scenariu tipic de activitate asupra unității montate pe vehicul. Scenariul trebuie adaptat tipului de card supus testării și implică scrierea pe card într-un număr cât mai mare de fișiere elementare. Se verifică, prin descărcarea datelor din unitatea montată pe vehicul, dacă toate înregistrările corespunzătoare au fost efectuate corect. Se verifică, prin descărcarea datelor de pe card, dacă toate înregistrările corespunzătoare au fost efectuate corect. Se verifică, prin documente imprimate zilnice, dacă toate înregistrările corespunzătoare pot fi citite în mod adecvat.
9.2 Teste de interoperabilitate între unități montate pe vehicule și senzori de mișcare		
1	Asociere	Se verifică dacă asocierea dintre unitățile montate pe vehicule și senzorii de mișcare se desfășoară normal
2	Teste privind activitățile	Se execută un scenariu tipic de activitate asupra senzorului de mișcare. Scenariul implică o activitate normală și crearea cât mai multor evenimente sau anomalii. Se verifică, prin descărcarea datelor din unitatea montată pe vehicul, dacă toate înregistrările corespunzătoare au fost efectuate corect. Se verifică, prin descărcarea datelor de pe card, dacă toate înregistrările corespunzătoare au fost efectuate corect. Se verifică, printr-un document imprimat zilnic, dacă toate înregistrările corespunzătoare pot fi citite în mod adecvat.

Nr.	Test	Descriere
9.3 Teste de interoperabilitate între unități montate pe vehicule și echipamente GNSS externe (acolo unde este cazul)		
1	Autentificare reciprocă	Se verifică dacă autentificarea reciprocă (cuplarea) dintre unitatea montată pe vehicul și echipamentul GNSS extern se desfășoară normal.
2	Teste privind activitățile	Se execută un scenariu tipic de activitate asupra echipamentului GNSS extern. Scenariul implică o activitate normală și crearea de cât mai multe evenimente sau anomalii. Se verifică, prin descărcarea datelor din unitatea montată pe vehicul, dacă toate înregistrările corespunzătoare au fost efectuate corect. Se verifică, prin descărcarea datelor de pe card, dacă toate înregistrările corespunzătoare au fost efectuate corect. Se verifică, printr-un document imprimat zilnic, dacă toate înregistrările corespunzătoare pot fi citite în mod adecvat.

Apendicele 10

CERINȚE DE SECURITATE

Prezentul apendice specifică cerințele de securitate informatică pentru componentele sistemului tahografic inteligent (tahograf de a doua generație).

SEC_001 Următoarele componente ale sistemului tahografic inteligent trebuie să fie certificate din punctul de vedere al securității în conformitate cu criteriile comune:

— unitatea montată pe vehicul;

— cardul de tahograf;

— senzorul de mișcare;

— echipamentul GNSS extern.

SEC_002 Cerințele minime de securitate informatică pe care trebuie să le respecte fiecare componentă care trebuie să fie certificată din punctul de vedere al securității sunt definite într-un profil de protecție al componentei, în conformitate cu criteriile comune.

SEC_003 Comisia Europeană se asigură că patru profile de protecție conforme cu prezenta anexă sunt sponsorizate, dezvoltate, aprobate de organismele guvernamentale de certificare în domeniul securității informatice, create în cadrul Grupului de lucru mixt privind interpretarea (JIWG – *Joint Interpretation Working Group*), care sprijină recunoașterea reciprocă a certificatelor în cadrul MRA (Acordul de recunoaștere reciprocă a certificatelor de evaluare a securității informatice) al grupului european SOGIS, și înregistrate:

— profilul de protecție pentru unitatea montată pe vehicul;

— profilul de protecție pentru cardul de tahograf;

— profilul de protecție pentru senzorul de mișcare;

— profilul de protecție pentru echipamentul GNSS extern.

Profilul de protecție pentru unitatea montată pe vehicul trebuie să abordeze cazurile în care VU este proiectată pentru a fi sau nu utilizată cu un echipament GNSS extern. În primul caz, cerințele de securitate aplicabile echipamentului GNSS extern sunt specificate în profilul de protecție aferent.

SEC_004 Producătorii componentelor ameliorează și completează, după necesități, profilul de protecție corespunzător al componentei, fără a modifica sau a șterge amenințările, obiectivele, mijloacele procedurale și specificațiile funcțiilor de asigurare a securității existente, pentru a crea un obiectiv de securitate în raport cu care să solicite certificarea de securitate a componentei respective.

SEC_005 În cursul procesului de evaluare, trebuie declarată conformitatea strictă a acestui obiectiv de securitate specific cu profilul de protecție corespunzător.

SEC_006 Nivelul de siguranță al fiecărui profil de protecție trebuie să fie EAL4, amplificat de componentele de siguranță ATE_DPT.2 și AVA_VAN.5.

Apendicele 11

MECANISME DE SECURITATE COMUNE

CUPRINS

PREAMBUL		340
PARTEA A	SISTEMUL TAHOGRAFIC DE PRIMA GENERAȚIE	341
1.	INTRODUCERE	341
1.1.	Referințe	341
1.2.	Notații și termeni abreviați	341
2.	SISTEME ȘI ALGORITMI CRIPTOGRAFICI	343
2.1.	Sisteme criptografice	343
2.2.	Algoritmi criptografici	343
2.2.1	Algoritmul RSA	343
2.2.2	Algoritmul de hash	343
2.2.3	Algoritmul de criptare a datelor	343
3.	CHEI ȘI CERTIFICATE	343
3.1.	Generarea și distribuirea cheilor	343
3.1.1	Generarea și distribuirea cheilor RSA	343
3.1.2	Chei de testare RSA	345
3.1.3	Cheile senzorului de mișcare	345
3.1.4	Generarea și distribuția cheilor de sesiune T-DES	345
3.2.	Chei	345
3.3.	Certificate	345
3.3.1	Conținutul certificatelor	346
3.3.2	Certificate emise	348
3.3.3	Verificarea și deschiderea certificatelor	349
4.	MECANISMUL DE AUTENTIFICARE RECIPROCĂ	349
5.	CONFIDENȚIALITATEA, INTEGRITATEA ȘI MECANISMUL DE AUTENTIFICARE ALE TRANSFERULUI DE DATE DINTRE VU ȘI CARDURI	352
5.1.	Mesagerie securizată	352
5.2.	Tratarea erorilor mesageriei securizate	354
5.3.	Algoritmul de calcul al sumelor de verificare criptografice	354
5.4.	Algoritmul de calcul al criptogramelor pentru obiecte de date (DO) confidențiale	355
6.	MECANISMELE DE SEMNARE DIGITALĂ A DATELOR DESCĂRCATE	355
6.1.	Generarea semnăturilor	355
6.2.	Verificarea semnăturilor	356

PARTEA B	SISTEMUL TAHOGRAFIC DE A DOUA GENERAȚIE	357
7.	INTRODUCERE	357
7.1.	Referințe	357
7.2.	Notații și abrevieri	357
7.3.	Definiții	359
8.	SISTEME ȘI ALGORITMI CRIPTOGRAFICI	359
8.1.	Sisteme criptografice	359
8.2.	Algoritmi criptografici	360
8.2.1	Algoritmi simetrici	360
8.2.2	Algoritmi asimetrici și parametri de domeniu standardizați	360
8.2.3	Algoritmi de hashing	361
8.2.4	Suite cifru	361
9.	CHEI ȘI CERTIFICATE	361
9.1.	Perechi de chei asimetrice și certificate de cheie publică	361
9.1.1	Considerații generale	361
9.1.2	Nivelul european	362
9.1.3	Nivelul statului membru	362
9.1.4	Nivelul echipamentului: Unități montate pe vehicule	363
9.1.5	Nivelul echipamentului: Carduri de tahograf	365
9.1.6	Nivelul echipamentului: Echipamente GNSS externe	366
9.1.7	Prezentare generală: Înlocuirea certificatelor	367
9.2.	Chei simetrice	368
9.2.1	Chei pentru siguranța comunicațiilor dintre VU și senzorul de mișcare	368
9.2.2	Chei pentru securizarea comunicațiilor specializate cu rază scurtă de acțiune (DSRC)	372
9.3.	Certificate	375
9.3.1	Considerații generale	375
9.3.2	Conținutul certificatelor	375
9.3.3	Solicitarea de certificate	377
10.	AUTENTIFICAREA RECIPROCĂ ȘI MESAGERIA SECURIZATĂ ÎNTRE VU ȘI CARDURI	378
10.1.	Considerații generale	378
10.2.	Verificarea reciprocă a lanțului de certificate	379
10.2.1	Verificarea lanțului de certificate de către VU	379
10.2.2	Verificarea lanțului de certificate ale VU de către card	381
10.3.	Autentificarea VU	384
10.4.	Autentificarea cipului și înțelegerea asupra cheilor de sesiune	385

10.5. Mesagerie securizată 387

10.5.1 Considerații generale 387

10.5.2 Structura mesageriei securizate 388

10.5.3 Abandonarea sesiunii de mesagerie securizată 391

11. CUPLAREA, AUTENTIFICAREA RECIPROCĂ ȘI MESAGERIA SECURIZATĂ ÎNTRE VU ȘI ECHIPAMENTUL GNSS EXTERN 392

11.1. Considerații generale 392

11.2. Cuplarea dintre VU și echipamentul GNSS extern 393

11.3. Verificarea reciprocă a lanțului de certificate 393

11.3.1 Considerații generale 393

11.3.2 În timpul cuplării VU – EGF 393

11.3.3 În timpul funcționării normale 394

11.4. Autentificarea VU, autentificarea cipului și înțelegerea asupra cheilor de sesiune 395

11.5. Mesageria securizată 395

12. ASOCIEREA ȘI COMUNICAREA DINTRE O VU ȘI UN SENZOR DE MIȘCARE 396

12.1. Considerații generale 396

12.2. Asocierea VU – senzor de mișcare folosind generații diferite de chei 396

12.3. Comunicarea și asocierea dintre o VU și un senzor de mișcare folosind AES 397

12.4. Asocierea VU – senzor de mișcare pentru echipamente de diferite generații 399

13. SECURITATEA COMUNICĂRII LA DISTANȚĂ PRIN DSRC 399

13.1. Considerații generale 399

13.2. Criptarea datelor utile ale tahografului și generarea MAC 400

13.3. Verificarea și decriptarea datelor utile ale tahografului 401

14. SEMNAREA DESCĂRCĂRII DE DATE ȘI VERIFICAREA SEMNĂTURILOR 401

14.1. Considerații generale 401

14.2. Generarea semnăturilor 402

14.3. Verificarea semnăturilor 402

PREAMBUL

Prezentul apendice precizează mecanismele de securitate care asigură

— autentificarea reciprocă între diferitele componente ale sistemului tahografic,

— confidențialitatea, integritatea, autenticitatea și/sau evitarea respingerii datelor transferate între diferitele componente ale sistemului tahografic sau descărcate pe suporturi de stocare externe.

Prezentul apendice cuprinde două părți. Partea A definește mecanismele de securitate pentru sistemul tahografic de prima generație (tahograful digital). Partea B definește mecanismele de securitate pentru sistemul tahografic de a doua generație (tahograful inteligent).

Mecanismele menționate în partea A din prezentul apendice se aplică în cazul în care cel puțin una dintre componentele sistemului tahografic implicate într-un proces de autentificare reciprocă și/sau de transfer de date este de prima generație.

Mecanismele menționate în partea B din prezentul apendice se aplică în cazul în care ambele componente ale sistemului tahografic implicate într-un proces de autentificare reciprocă și/sau de transfer de date sunt de a doua generație.

Apendicele 15 oferă mai multe informații privind utilizarea componentelor de prima generație în combinație cu componente de a doua generație.

PARTEA A

SISTEMUL TAHOGRAFIC DE PRIMA GENERAȚIE

1. INTRODUCERE

1.1. **Referințe**

În prezentul apendice se face trimitere la următoarele standarde:

SHA-1	*National Institute of Standards and Technology* (NIST). *Publication* FIPS 180-1: *Secure Hash Standard*. Aprilie 1995.
PKCS1	*RSA Laboratories*. PKCS # 1: *RSA Encryption Standard* Versiunea 2.0. Octombrie 1998
TDES	*National Institute of Standards and Technology* (NIST). *FIPS Publication 46-3: Data Encryption Standard* Proiect 1999.
TDES-OP	ANSI X9.52, *Triple Data Encryption Algorithm Modes of Operation* 1998.
ISO/IEC 7816-4	*Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interexchange*. Prima ediție: 1995 + Amendamentul 1: 1997.
ISO/IEC 7816-6	*Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements*. Prima ediție: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	*Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands*. Prima ediție 1999.
ISO/IEC 9796-2	*Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function*. Prima ediție: 1997.
ISO/IEC 9798-3	*Information Technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm*. Ediția a doua 1998.
ISO 16844-3	Road vehicles – Tachograph systems – Part 3: Motion sensor interface.

1.2. **Notații și termeni abreviați**

În prezentul apendice sunt folosite următoarele notații și termeni abreviați:

(K_a, K_b, K_c)	un grup de chei utilizat de algoritmul de criptare triplă a datelor,
CA	autoritate de certificare,
CAR	identificator al autorității de certificare,
CC	sumă de verificare criptografică,
CG	criptogramă,
CH	antet de comandă,
CHA	autorizația deținătorului certificatului,
CHR	identificator al deținătorului certificatului,
D()	decriptare cu DES (*Data Encryption Standard*),

DE	element de date,
DO	obiect de date,
d	cheie privată RSA, exponent privat,
e	cheie publică RSA, exponent public,
E()	criptare cu DES,
EQT	echipament,
Hash()	valoare *hash*, un rezultat al funcției *hash*,
Hash	funcție *hash*,
KID	identificator de cheie,
Km	cheie TDES. Cheie master definită în ISO 16844-3.
Km_{VU}	cheie TDES introdusă în unitățile montate pe vehicule,
Km_{WC}	cheie TDES introdusă în cardurile de atelier.
m	reprezentant de mesaj, număr întreg cuprins între 0 și *n*-1,
n	chei RSA, modul,
PB	octeți de completare,
PI	Octet indicator de completare (utilizat în criptograme pentru confidențialitatea DO),
PV	Valoare a datelor în clar,
s	reprezentant de semnătură, număr întreg cuprins între 0 și *n*-1,
SSC	Contor de secvențe trimise,
SM	Mesagerie securizată,
TCBC	Mod de funcționare prin înlănțuirea blocurilor cifrate TDEA,
TDEA	Algoritm de criptare triplă a datelor,
TLV	Valoarea unei lungimi de etichetă,
VU	Unitate montată pe vehicul,
X.C	Certificatul utilizatorului X emis de o autoritate de certificare,
X.CA	o autoritate de certificare a utilizatorului X,
X.CA.PK $_{o}$ X.C	Operația de dezvăluire a unui certificat pentru a extrage o cheie publică. Este un operator infix, al cărui operand stâng este cheia publică a unei autorități de certificare, iar operandul drept este certificatul emis de acea autoritate de certificare. Rezultatul este cheia publică a utilizatorului X al cărui certificat este operandul drept,
X.PK	Cheia privată RSA a utilizatorului X,
X.PK[I]	Cifrarea RSA a unor informații I, folosind cheia publică a utilizatorului X
X.SK	Cheia privată RSA a utilizatorului X,
X.SK[I]	Cifrarea RSA a unor informații I, folosind cheia privată a utilizatorului X,
'xx'	o valoare hexazecimală,
||	Operatorul de concatenare.

2. SISTEME ȘI ALGORITMI CRIPTOGRAFICI

2.1. **Sisteme criptografice**

CSM_001 Unitățile montate pe vehicule și cardurile de tahograf utilizează un sistem criptografic cu cheie publică RSA clasic pentru a oferi următoarele mecanisme de securitate:

— autentificarea între unitățile montate pe vehicule și carduri,

— transportul cheilor de sesiune de tip DES triplu între unitățile montate pe vehicule și cardurile de tahograf,

— semnătura digitală a datelor descărcate din unitățile montate pe vehicule și din cardurile de tahograf pe suporturi externe.

CSM_002 Unitățile montate pe vehicule și cardurile de tahograf utilizează un sistem criptografic simetric DES triplu în scopul de a asigura un mecanism pentru integritatea datelor în timpul schimburilor de date privind utilizatorul dintre unitățile montate pe vehicule și cardurile de tahograf și pentru a garanta, unde este cazul, confidențialitatea schimburilor de date dintre unitățile montate pe vehicule și cardurile de tahograf.

2.2. **Algoritmi criptografici**

2.2.1 *Algoritmul RSA*

CSM_003 Algoritmul RSA este definit în întregime de următoarele relații:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

O descriere mai completă a funcției RSA poate fi găsită în referința [PKCS1]. Exponentul public, e, pentru calculul funcției RSA este un număr întreg cuprins între 3 și n-1 care satisface gcd[e, lcm(p-1, q-1)] = 1.

2.2.2 *Algoritmul de hash*

CSM_004 Mecanismele de semnătură digitală utilizează algoritmul de *hash* SHA-1 astfel cum este definit în referința [SHA-1].

2.2.3 *Algoritmul de criptare a datelor*

CSM_005 Algoritmii bazați pe DES sunt utilizați în modul de funcționare prin înlănțuirea blocurilor cifrate.

3. CHEI ȘI CERTIFICATE

3.1. **Generarea și distribuirea cheilor**

3.1.1 *Generarea și distribuirea cheilor RSA*

CSM_006 Cheile RSA sunt generate prin trei niveluri ierarhice funcționale:

— nivelul european,

— nivelul statului membru,

— nivelul echipamentului.

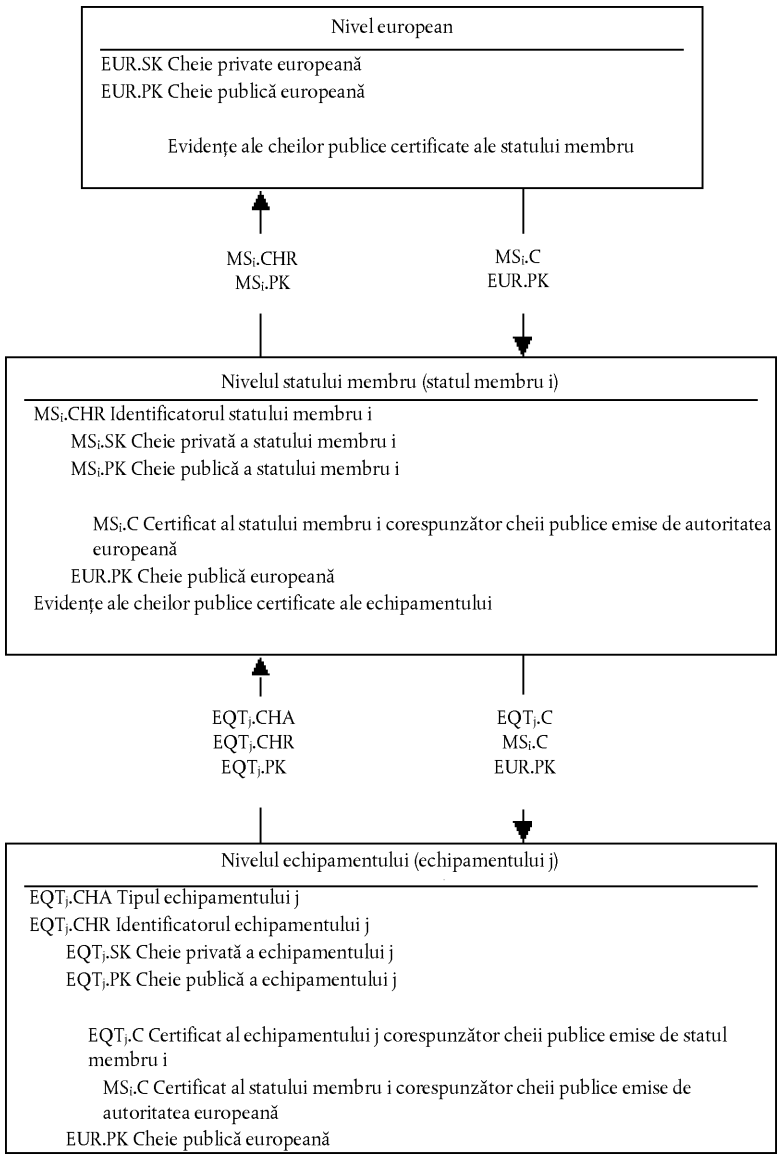
CSM_007 La nivelul european se generează o pereche unică de chei europene (EUR.SK și EUR.PK). Cheia privată europeană se utilizează pentru certificarea cheilor publice ale statelor membre. Se ține evidența tuturor cheilor certificate. Aceste sarcini sunt îndeplinite de o autoritate de certificare europeană, sub autoritatea și responsabilitatea Comisiei Europene.

CSM_008 La nivelul statului membru se generează o pereche de chei ale statului membru (MS.SK și MS.PK). Cheile publice ale statelor membre sunt certificate de autoritatea de certificare europeană. Cheile private ale statelor membre se utilizează pentru certificarea cheilor publice care se introduc în echipament (unitatea montată pe vehicul sau cardul de tahograf). Se ține evidența tuturor cheilor publice certificate, împreună cu datele de identificare a echipamentului căruia îi sunt destinate. Aceste sarcini sunt îndeplinite de autoritatea de certificare a unui stat membru. Un stat membru își poate schimba periodic perechea de chei.

CSM_009 La nivelul echipamentului se generează o singură pereche de chei (EQT.SK și EQT.PK), care se introduce în fiecare echipament. Cheile publice ale echipamentelor sunt certificate de autoritatea de certificare a unui stat membru. Aceste sarcini pot fi îndeplinite de producătorii de echipamente, de serviciile de personalizare a echipamentelor sau de autoritățile statelor membre. Această pereche de chei se folosește pentru serviciile de autentificare, de semnătură digitală și de cifrare.

CSM_010 Confidențialitatea cheilor private trebuie menținută în timpul generării, transportului (dacă este cazul) și stocării.

Ilustrația următoare sintetizează fluxul de date al acestui proces:



3.1.2 *Chei de testare RSA*

CSM_011 Pentru testarea echipamentelor (inclusiv pentru testele de interoperabilitate), autoritatea de certificare europeană generează o pereche unică diferită de chei de testare europene și cel puțin două perechi de chei de testare ale statului membru, ale cărui chei publice sunt certificate cu cheia de testare privată europeană. Producătorii introduc, în echipamentele supuse testelor pentru omologarea de tip, chei de testare certificate cu una dintre aceste chei de testare ale statului membru.

3.1.3 *Cheile senzorului de mișcare*

Confidențialitatea celor trei chei TDES descrise mai jos trebuie asigurată în mod corespunzător în timpul generării, transportului (dacă este cazul) și stocării.

În scopul de a asigura compatibilitatea componentelor tahografului cu ISO 16844, autoritatea de certificare europeană și autoritățile de certificare din statele membre asigură, în plus, următoarele:

CSM_036 Autoritatea de certificare europeană generează KmVU și KmWC, două chei DES triple independente și unice, și generează Km ca fiind: $Km = Km_{VU}$ XOR Km_{WC} . Autoritatea de certificare europeană transmite aceste chei, prin proceduri securizate corespunzător, autorităților de certificare ale statelor membre, la cererea acestora.

CSM_037 Autoritățile de certificare ale statelor membre:

— folosesc Km pentru a cripta datele de la senzorul de mișcare solicitate de producătorii de senzori de mișcare (datele care trebuie criptate cu Km sunt definite în ISO 16844-3),

— transmit Km_{VU} producătorilor de unități montate pe vehicule, prin proceduri securizate corespunzător, pentru a fi introdusă în unitățile montate pe vehicule,

— se asigură că Km_{WC} va fi introdusă în toate cardurile de atelier (`SensorInstallationSecData` din fișierul elementar `Sensor_Installation_Data`) în timpul personalizării cardului.

3.1.4 *Generarea și distribuția cheilor de sesiune T-DES*

CSM_012 Unitățile montate pe vehicule și cardurile de tahograf generează și își transmit reciproc datele necesare pentru elaborarea unei chei de sesiune comune de tip DES triplu, ca parte a procesului de autentificare reciprocă. Confidențialitatea acestui schimb de date trebuie să fie protejată printr-un mecanism de criptare RSA.

CSM_013 Această cheie se utilizează pentru toate operațiunile criptografice ulterioare folosind mesageria securizată. Valabilitatea ei expiră la terminarea sesiunii (retragerea cardului sau reinițializarea cardului) și/sau după 240 de utilizări (o utilizare a cheii = o comandă trimisă cardului folosind mesageria securizată și răspunsul asociat).

3.2. **Chei**

CSM_014 Cheile RSA au următoarele lungimi (indiferent de nivel): modul *n* 1 024 de biți, exponentul public *e* maxim 64 de biți, exponentul privat *d* 1 024 de biți.

CSM_015 Cheile de tip DES triplu au forma (K_a, K_b, K_a), unde K_a și K_b sunt chei independente cu o lungime de 64 de biți. Nu se configurează niciun bit pentru detectarea erorilor de paritate.

3.3. **Certificate**

CSM_016 Certificatele cheilor publice RSA sunt certificate de tip „non self-descriptive” (nu se pot autodescrie) și „Card Verifiable” (verificabile cu ajutorul cardului) (ref.: ISO/IEC 7816-8)

3.3.1 *Conținutul certificatelor*

CSM_017 Certificatele cheilor publice RSA sunt alcătuite din următoarele date, în ordinea indicată:

Date	Format	Octeți	Observații
CPI	ÎNTREG	1	Identificator de profil al certificatului ('01' pentru prezenta versiune)
CAR	ȘIR DE OCTEȚI	8	Identificatorul autorității de certificare
CHA	ȘIR DE OCTEȚI	7	Autorizația deținătorului certificatului
EOV	TimeReal	4	Data expirării valabilității certificatului. Opțional, completat cu 'FF' dacă nu este folosit
CHR	ȘIR DE OCTEȚI	8	Identificatorul deținătorului certificatului
n	ȘIR DE OCTEȚI	128	Cheie publică (modul)
e	ȘIR DE OCTEȚI	8	Cheie publică (exponent public)
		164	

Note:

1. „Identificatorul de profil al certificatului" (CPI) determină structura precisă a unui certificat de autentificare. El poate fi folosit ca identificator intern al echipamentului pentru o listă antet relevantă care descrie concatenarea elementelor de date în cadrul certificatului.

   Lista antet asociată cu acest conținut al certificatului este următoarea:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Eticheta listei antet extinse	Lungimea listei antet	Eticheta CPI	Lungimea CPI	Eticheta CAR	Lungimea CAR	Eticheta CAR	Lungimea CHA	Eticheta CAR	Lungimea EOV	Eticheta CHR	Lungimea CHR	Etichetă cheie publică (construită)	Lungimea DO-urilor ulterioare	Etichetă modul	Lungime modul	Etichetă exponent public	Lungime exponent public

2. „Identificatorul autorității de certificare" (CAR) are scopul de a identifica autoritatea de certificare care a emis certificatul, astfel încât elementul de date să poată fi folosit în același timp și ca un identificator al cheii de autoritate pentru a face trimitere la cheia publică a autorității de certificare (pentru codificare, a se vedea mai jos identificatorul de cheie).

3. „Autorizația deținătorului certificatului” (CHA) este folosită pentru a identifica drepturile deținătorului certificatului. Aceasta se compune din ID-ul aplicației tahografice și din tipul de echipament căruia îi este destinat certificatul (în conformitate cu elementul de date `EquipmentType`, ‘00’ pentru un stat membru).

4. „Identificatorul deținătorului certificatului” (CHR) are scopul de a identifica în mod unic deținătorul certificatului, astfel încât elementul de date să poată fi folosit în același timp ca identificator al cheii subiect pentru a face trimitere la cheia publică a deținătorului certificatului.

5. Identificatoarele cheii identifică în mod unic deținătorul certificatului sau autoritățile de certificare. Acestea sunt codificate după cum urmează:

5.1. Echipament (VU sau card):

Date	Numărul de serie al echipamentului	Data	Tip	Producător
Lungime	4 octeți	2 octeți	1 octet	1 octet
Valoare	Întreg	ll aa codare BCD	Specific producătorului	Codul producătorului

În cazul unei unități montate pe vehicul, atunci când producătorul solicită certificate, el poate sau nu să cunoască identificatorul echipamentului în care vor fi introduse cheile.

În primul caz, producătorul trimite identificatorul echipamentului împreună cu cheia publică la autoritatea statului membru respectiv pentru certificare. Certificatul va conține în acest caz identificatorul echipamentului, iar producătorul trebuie să se asigure că cheile și certificatele sunt introduse în echipamentele prevăzute. Identificatorul cheii are forma indicată mai sus.

În al doilea caz, producătorul trebuie să identifice în mod unic fiecare cerere de certificat și să trimită acest identificator împreună cu cheia publică la autoritatea statului membru respectiv pentru certificare. Certificatul conține identificatorul cererii. Producătorul trebuie să informeze autoritatea statului său membru cu privire la atribuirea cheii pentru echipament (și anume, identificatorul cererii de certificat, identificatorul echipamentului) după instalarea cheii în echipament. Identificatorul cheii are forma următoare:

Date	Numărul de serie al cererii de certificat	Data	Tip	Producător
Lungime	4 octeți	2 octeți	1 octet	1 octet
Valoare	Întreg	ll aa codare BCD	‘FF’	Codul producătorului

5.2. Autoritatea de certificare:

Date	Identificatorul autorității	Numărul de serie al cheii	Informații suplimentare	Identificator
Lungime	4 octeți	1 octet	2 octeți	1 octet

Valoare	Codul numeric național 1 octet Codul alfanumeric național 3 octeți	Întreg	codificare suplimentară (specific CA) 'FF FF' dacă nu este folosit	'01'

Numărul de serie al cheii este folosit pentru a distinge cheile diferite ale unui stat membru, în cazul în care cheia este schimbată.

6. Verificatorii certificatelor știu implicit că cheia publică certificată este o cheie RSA relevantă pentru autentificare, pentru verificarea semnăturii digitale și pentru cifrarea în scopul serviciilor de confidențialitate (certificatul nu conține niciun identificator de obiect care să specifice acest lucru).

3.3.2 *Certificate emise*

CSM_018 Certificatul emis este o semnătură digitală cu recuperarea parțială a conținutului certificatului în conformitate cu ISO/IEC 9796-2 (cu excepția anexei A4 a acestuia), cu „identificatorul autorității de certificare" adăugat.

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Cu conținutul certificatului = Cc = C_r || C_n

106 octeți 58 de octeți

Note:

1. Acest certificat are o lungime de 194 de octeți.

2. CAR, fiind ascuns de semnătură, este în același timp adăugat la semnătură, astfel încât cheia publică a autorității de certificare să poată fi selectată pentru verificarea certificatului.

3. Verificatorul certificatului cunoaște implicit algoritmul folosit de autoritatea de certificare pentru semnarea certificatului.

4. Lista antet asociată cu acest certificat emis este următoarea:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Eticheta certificatului CV (construită)	Lungimea DO-urilor ulterioare	Eticheta semnăturii	Lungimea semnăturii	Eticheta restului	Lungimea restului	Eticheta CAR	Lungimea CAR

3.3.3 *Verificarea și deschiderea certificatelor*

Verificarea și deschiderea certificatelor constă în verificarea semnăturii în conformitate cu ISO/IEC 9796-2, extrăgând conținutul certificatului și cheia publică conținută: X.PK = X.CA.PK $_o$ X.C și în verificarea valabilității certificatului.

CSM_019 Aceasta implică următoarele etape:

Verificarea semnăturii și extragerea conținutului:

— din X.C se extrage semnătura, C_n' și CAR': X.C = Semnare || C_n' || CAR'

	Semnare	||	C_n'	||	CAR'
	128 de octeți		58 de octeți		8 octeți

— din CAR' se selectează cheia publică a autorității de certificare corespunzătoare (dacă nu s-a selecționat anterior prin alte metode)

— se deschide semnătura cu cheia publică a CA: Sr'= X.CA.PK [Sign],

— se verifică dacă Sr' începe cu '6A' și se termină cu 'BC'

— se calculează C_r' și H' cu formula: Sr' = '6 A' || C_r' || H' || 'BC'

	'6 A'	||	C_r'	||	H'	|| 'BC'
			106 octeți		20 de octeți		

— se recuperează conținutul certificatului C' = C_r' || C_n',

— se verifică faptul că *Hash*(C') = H'

Dacă verificările sunt în regulă, certificatul este original, având conținutul C'.

Se verifică valabilitatea. Din C':

— dacă este cazul, se verifică data de expirare a valabilității

Se extrage și se stochează cheia publică, identificatorul cheii, autorizația deținătorului certificatului și data de expirare a valabilității din C':

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECANISMUL DE AUTENTIFICARE RECIPROCĂ

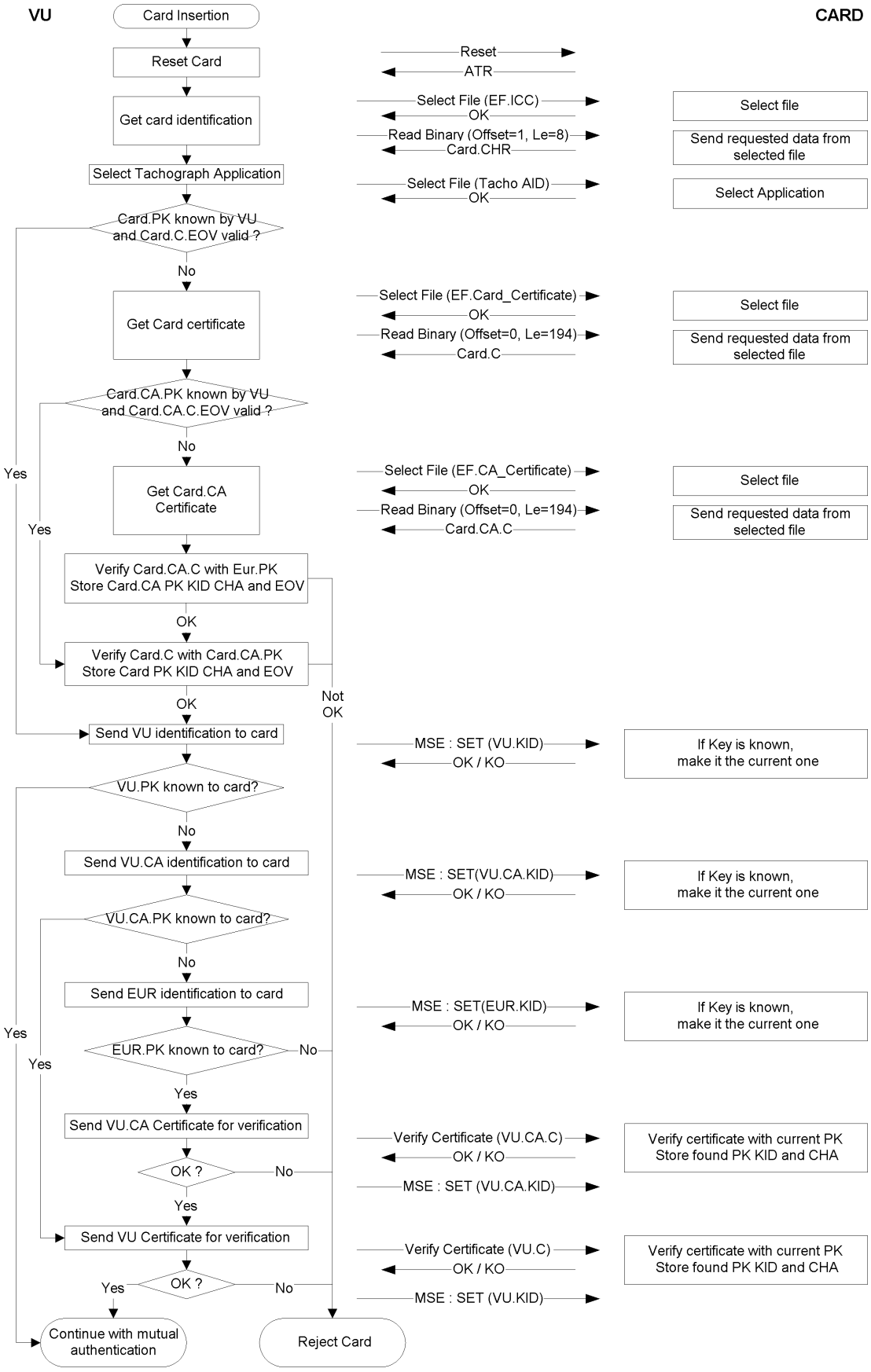
Autentificarea reciprocă între carduri și VU se bazează pe principiul următor:

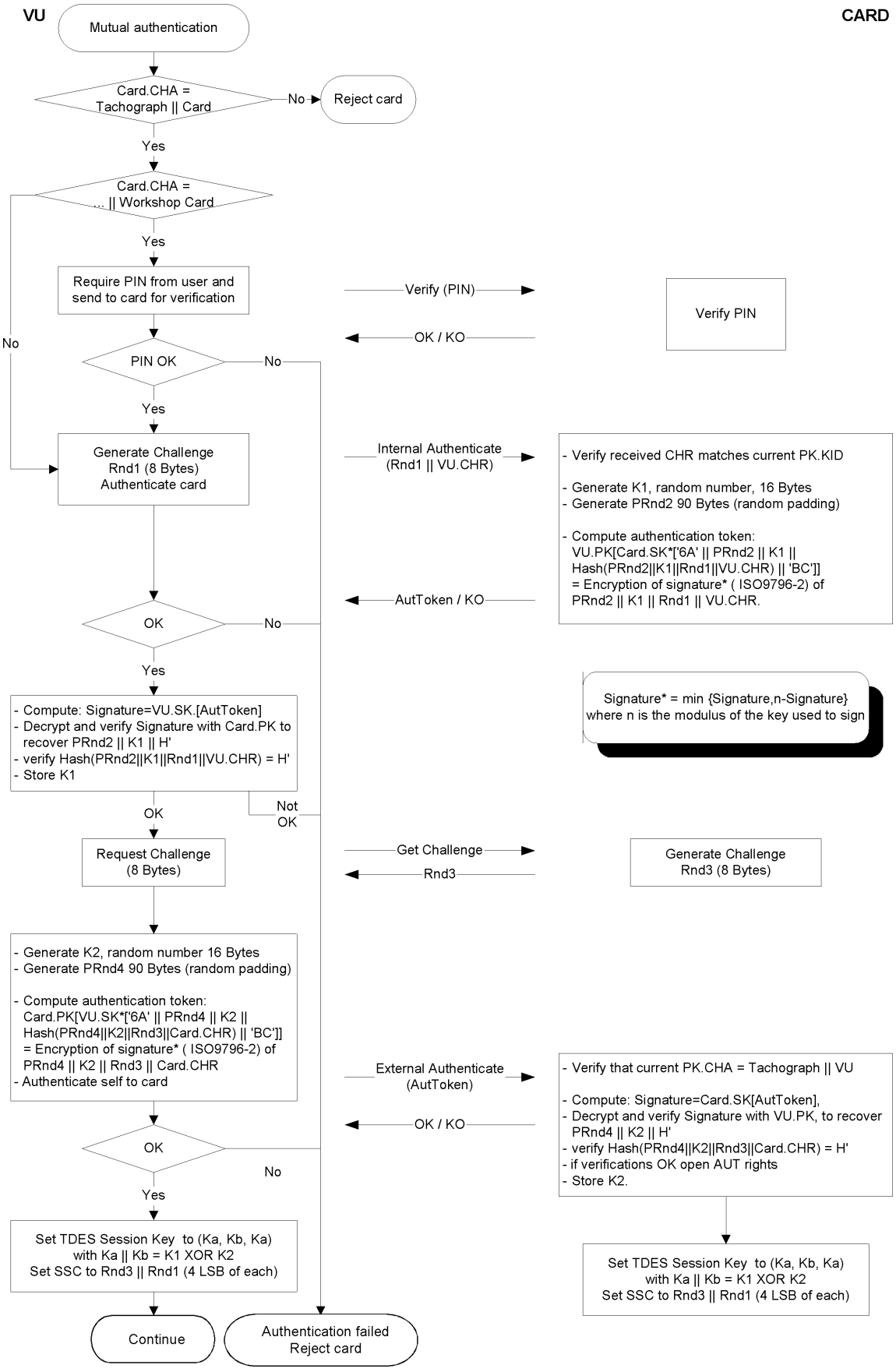
Fiecare parte îi demonstrează celeilalte că deține o pereche valabilă de chei, a cărei cheie publică a fost certificată de autoritatea de certificare a unui stat membru, care la rândul ei a fost certificată de autoritatea de certificare europeană.

Demonstrația se face prin semnarea cu cheia privată a unui număr aleatoriu trimis de cealaltă parte, care trebuie să recupereze numărul aleatoriu trimis în momentul verificării acestei semnături.

Mecanismul este declanșat de către VU la introducerea cardului. Acesta începe cu schimbul de certificate și deschiderea cheilor publice și se termină cu stabilirea unei chei de sesiune.

CSM_020 Trebuie utilizat următorul protocol [săgețile indică comenzile și datele schimbate (a se vedea apendicele 2)]:




VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. CONFIDENȚIALITATEA, INTEGRITATEA ȘI MECANISMUL DE AUTENTIFICARE ALE TRANSFERULUI DE DATE DINTRE VU ȘI CARDURI

5.1. **Mesagerie securizată**

CSM_021 Integritatea transferurilor de date dintre VU și carduri trebuie protejată printr-o mesagerie securizată în conformitate cu referințele (ISO/IEC 7816-4) și (ISO/IEC 7816-8).

CSM_022 Atunci când datele trebuie să fie protejate în timpul transferului, se adaugă un obiect de date de tip sumă de verificare criptografică la obiectele de date trimise în cadrul comenzii sau al răspunsului. Suma de verificare criptografică este verificată de receptor.

CSM_023 Suma de verificare criptografică a datelor trimise în cadrul unei comenzi integrează antetul comenzii și toate obiectele de date trimise (=>CLA = '0C', iar toate obiectele de date sunt încapsulate cu etichete în care b1 = 1).

CSM_024 Octeții de stare-informații transmiși ca răspuns sunt protejați printr-o sumă de verificare criptografică atunci când răspunsul nu conține niciun câmp de date.

CSM_025 Sumele de verificare criptografice au o lungime de 4 octeți.

Structura comenzilor și răspunsurilor când se utilizează mesageria securizată este următoarea:

Obiectele de date utilizate sunt un set parțial din obiectele de date de mesagerie securizată descrise în ISO/IEC 7816-4:

Etichetă	Cod mnemonic	Sens
'81'	T_{PV}	Valoare a datelor în clar necodată prin BER-TLV (a se proteja prin CC)
'97'	$\mathbf{T_{LE}}$	Valoarea Le din comanda nesecurizată (a se proteja prin CC)
'99'	T_{SW}	Informații de stare (a se proteja prin CC)
'8E'	T_{CC}	Sumă de verificare criptografică
'87'	$T_{PI\ CG}$	Octet indicator de completare || Criptogramă (valoare a datelor în clar necodată prin BER-TLV)

Fiind dată o pereche comandă-răspuns nesecurizată:

Antet de comandă				Corpul comenzii		
CLA	INS	P1	P2	[Câmp L_c]	[Câmp de date]	[Câmp L_e]
patru octeți				L octeți, indicați cu identificatori de la B_1 la B_L		

Corpul răspunsului	Coada răspunsului	
[Câmp de date]	SW1	SW2
Octeți de date L_r	doi octeți	

Perechea corespunzătoare comandă-răspuns securizată este:

Comanda securizată:

Antetul comenzii (CH)				Corpul comenzii										
CLA	INS	P1	P2	[Câmp nou L_c]	[Câmp de date nou]									[Câmp nou L_e]
'OC'				Lungimea Câmp de date nou	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
					'81'	L_c	Câmp de date	'97'	'01'	L_e	'8E'	'04'	CC	

Datele care trebuie integrate în suma de verificare = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Octeți de completare (80 .. 00) în conformitate cu ISO-IEC 7816-4 și cu ISO 9797 metoda 2.

Obiectele de date PV și LE sunt prezente numai dacă există anumite date corespondente în comanda nesecurizată.

Răspunsul securizat:

1. Cazul în care câmpul de date răspuns nu este gol și nu este nevoie să fie protejat pentru confidențialitate:

Corpul răspunsului						Coada răspunsului
[Câmp de date nou]						SW1 SW2 noi
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Câmp de date	'8E'	'04'	CC	

Datele care trebuie integrate în suma de verificare = T_{PV} || L_{PV} || PV || PB

2. Cazul în care câmpul de date răspuns nu este gol și este nevoie să fie protejat pentru confidențialitate:

Corpul răspunsului						Coada răspunsului
[Câmp de date nou]						SW1 SW2 noi
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Datele care sunt transportate prin CG: date necodate prin BER-TLV și octeți de completare.

Datele care trebuie integrate în suma de verificare = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Cazul în care câmpul de date răspuns este gol:

Corpul răspunsului						Coada răspunsului
[Câmp de date nou]						SW1 SW2 noi
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	SW1 SW2 noi	'8E'	'04'	CC	

Datele care trebuie integrate în suma de verificare = T_{SW} || L_{SW} || SW || PB

5.2. **Tratarea erorilor mesageriei securizate**

CSM_026 Atunci când cardul de tahograf recunoaște o eroare de SM (mesagerie securizată) în timpul interpretării unei comenzi, octeții de stare trebuie să fie returnați fără SM. În conformitate cu standardul ISO/IEC 7816-4, următorii octeți de stare sunt definiți pentru a indica erori de SM:

'66 88': verificarea sumei de verificare criptografice a eșuat,

'69 87': obiectele de date așteptate ale SM lipsesc,

'69 88': obiectele de date ale SM sunt incorecte.

CSM_027 Atunci când cardul de tahograf returnează octeții de stare fără obiectele de date ale SM sau cu un obiect de date al SM eronat, sesiunea trebuie să fie terminată de VU.

5.3. **Algoritmul de calcul al sumelor de verificare criptografice**

CSM_028 Sumele de verificare criptografice sunt construite folosind un MAC (cod de autentificare a mesajelor) detaliat, conform standardului ANSI X9.19, cu criptarea DES:

— Etapa inițială: blocul de verificare inițial y0 este E(Ka, SSC).

— Etapa secvențială: blocurile de verificare y1,…, yn sunt calculate folosind Ka.

— Etapa finală: suma de verificare criptografică este calculată din ultimul bloc de control yn după cum urmează: E[Ka, D(Kb, yn)].

unde E() este criptarea cu DES, iar D() este decriptarea cu DES.

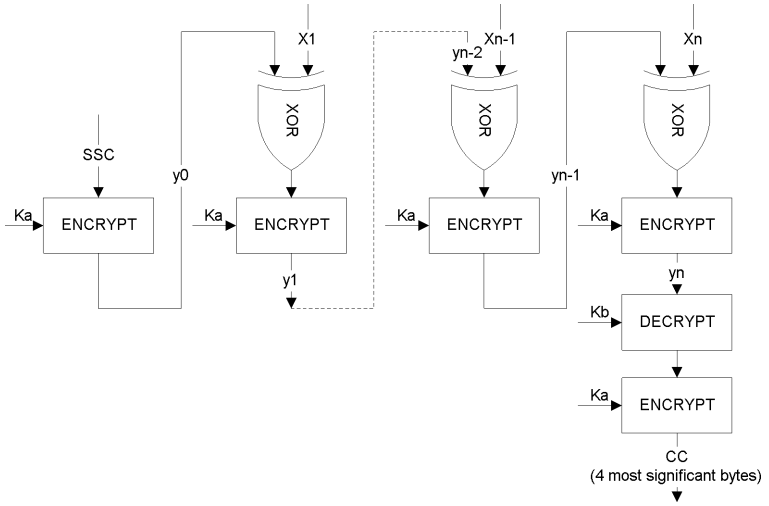
Cei mai relevanți patru octeți ai sumei de verificare criptografice sunt transferați.

CSM_029 Contorul de secvențe trimise (SSC) este inițializat în timpul procedurii de înțelegere asupra cheii la:

SSC inițial: Rnd3 (cei 4 octeți cel mai puțin semnificativi) || Rnd1 (cei 4 octeți cel mai puțin semnificativi) ||

CSM_030 Contorul de secvențe trimise este incrementat cu 1 de fiecare dată înainte de calcularea unui MAC (și anume, SSC pentru prima comandă este SSC inițial + 1, SSC pentru primul răspuns este SSC inițial + 2).

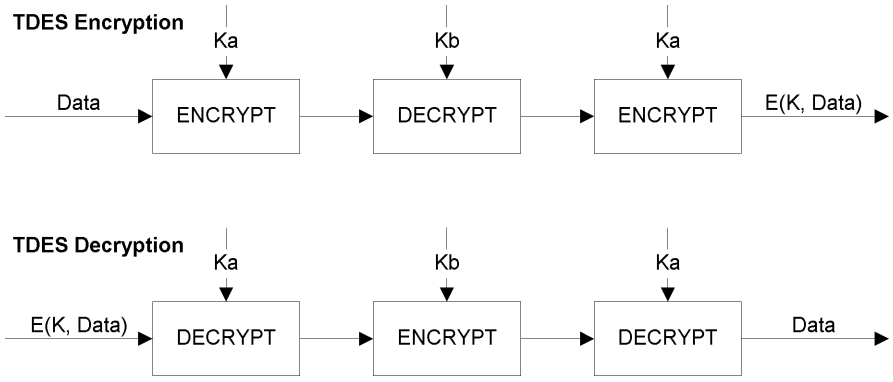
Figura următoare ilustrează calcularea MAC detaliat:



5.4. Algoritmul de calcul al criptogramelor pentru obiecte de date (DO) confidențiale

CSM_031 Criptogramele sunt calculate folosind TDEA în modul de funcționare TCBC, în conformitate cu referințele [TDES] și [TDES-OP], și utilizând vectorul nul ca bloc de valoare inițială.

Figura următoare ilustrează aplicarea cheilor în TDES:



6. MECANISMELE DE SEMNARE DIGITALĂ A DATELOR DESCĂRCATE

CSM_032 Echipamentul inteligent dedicat (IDE) stochează într-un singur fișier fizic de date datele recepționate de la un echipament (VU sau card) în timpul unei sesiuni de descărcare. Acest fișier trebuie să conțină certificatele MS_i.C și EQT.C. Fișierul conține semnăturile digitale ale blocurilor de date așa cum se specifică în apendicele 7, „Protocoale de descărcare a datelor”.

CSM_033 Semnăturile digitale ale datelor descărcate utilizează o schemă de semnătură digitală cu apendice astfel încât datele descărcate să poată fi citite fără nicio descifrare dacă se dorește.

6.1. Generarea semnăturilor

CSM_034 Generarea semnăturilor de date de către echipament trebuie să respecte schema de semnătură cu apendice definită în referința [PKCS1] cu funcția *hash* SHA-1:

Semnătura = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = șir de octeți de completare cu valoarea 'FF', astfel încât lungimea să fie 128.

DER(SHA-1(*M*)) este codificarea ID-ului algoritmului pentru funcția *hash* și pentru valoarea *hash* într-o valoare ASN.1 de tip DigestInfo (reguli de codare distincte):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||valoare *hash*.

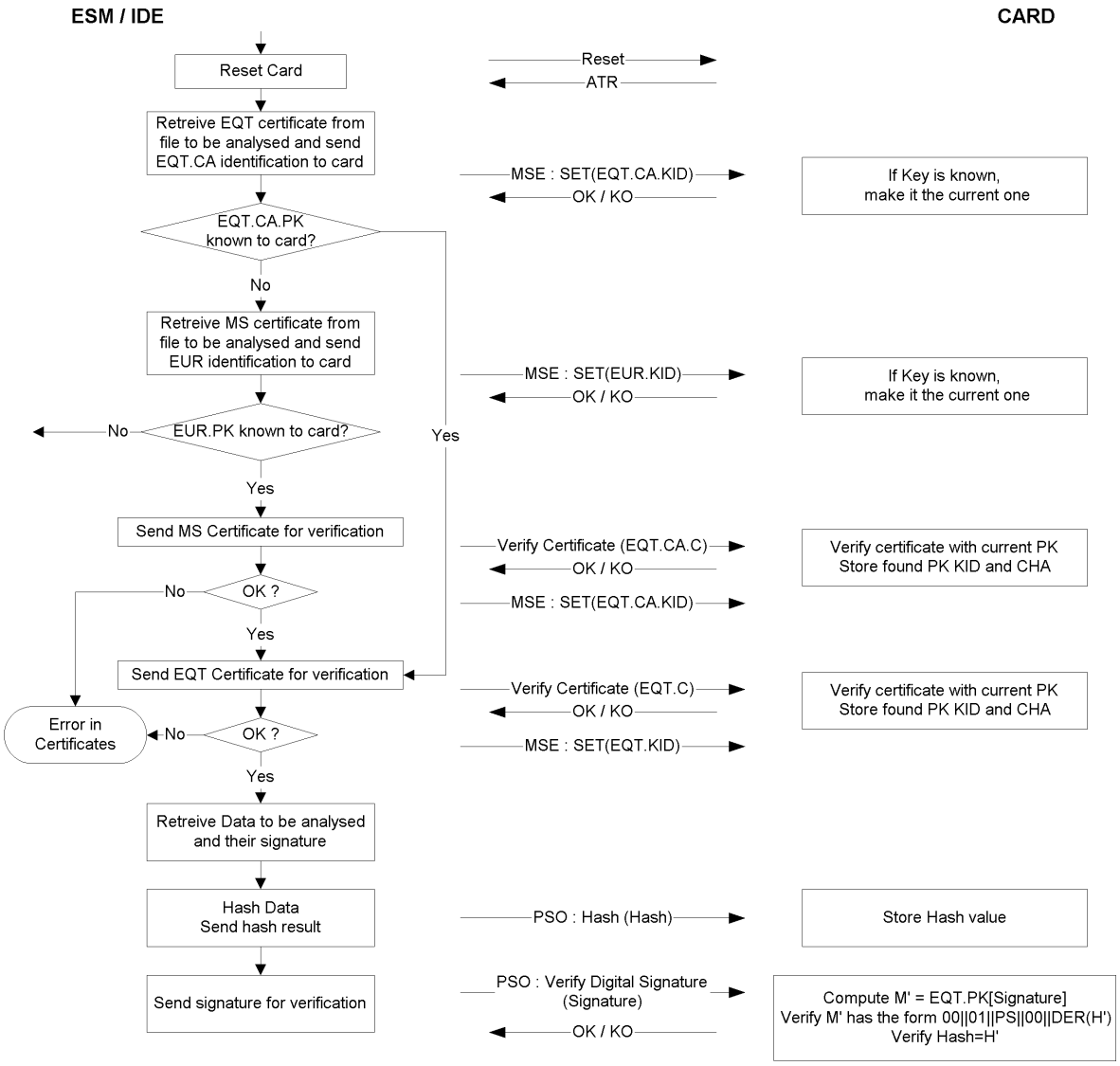
6.2. Verificarea semnăturilor

CSM_035 Verificarea semnăturilor datelor la datele descărcate este efectuată conform schemei de semnătură cu apendice definită în referința [PKCS1] cu funcția *hash* SHA-1.

Cheia publică europeană EUR.PK trebuie să fie cunoscută independent (și aprobată) de verificator.

Tabelul următor ilustrează protocolul pe care îl poate urma un IDE dotat cu un card de control pentru a verifica integritatea datelor descărcate și stocate pe ESM (suport de memorie extern). Cardul de control este folosit pentru a efectua descifrarea semnăturilor digitale. În acest caz, această funcție nu trebuie neapărat să fie implementată în IDE.

Echipamentul care a descărcat și semnat datele de analizat este denumit EQT.



PARTEA B

SISTEMUL TAHOGRAFIC DE A DOUA GENERAȚIE

7. INTRODUCERE

7.1. **Referințe**

În această parte a prezentului apendice se face trimitere la următoarele standarde:

AES	*National Institute of Standards and Technology* (NIST), FIPS PUB 197: *Advanced Encryption Standard* (AES), 26 noiembrie 2001
DSS	*National Institute of Standards and Technology* (NIST), FIPS PUB 186-4: *Digital Signature Standard* (DSS), iulie 2013
ISO 7816-4	ISO/IEC 7816-4, *Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*. Ediția a treia, 15.4.2013
ISO 7816-8	ISO/IEC 7816-8, *Identification cards – Integrated circuit cards – Part 8: Commands for security operations*. Ediția a doua, 1.6.2004
ISO 8825-1	ISO/IEC 8825-1 *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*. Ediția a patra, 15.12.2008
ISO 9797-1	ISO/IEC 9797-1, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*. Ediția a doua, 1.3.2011
ISO 10116	ISO/IEC 10116, *Information technology – Security techniques – Modes of operation of an n-bit block cipher*. Ediția a treia, 1.2.2006
ISO 16844-3	ISO16844-3 *Road vehicles – Tachograph systems – Part 3: Motion sensor interface*. Prima ediție 2004, inclusiv rectificarea tehnică 1, 2006
RFC 5480	*Elliptic Curve Cryptography Subject Public Key Information*, martie 2009
RFC 5639	*Elliptic Curve Cryptography (ECC) – Brainpool Standard Curves and Curve Generation*, 2010
RFC 5869	*HMAC-based Extract-and-Expand Key Derivation Function* (HKDF), mai 2010
SHS	*National Institute of Standards and Technology* (NIST), FIPS PUB 180-4: *Secure Hash Standard*, martie 2012
SP 800-38B	*National Institute of Standards and Technology* (NIST), Special Publication 800-38B: *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, 2005
TR-03111	*BSI Technical Guideline TR-03111, Elliptic Curve Cryptography*, versiunea 2.00, 28.6.2012

7.2. **Notații și abrevieri**

În prezentul apendice sunt folosite următoarele notații și abrevieri:

AES	Standard de criptare avansată
CA	Autoritate pentru certificate
CAR	Identificatorul autorității pentru certificate
CBC	Înlănțuirea blocurilor cifrate (mod de funcționare)

CH	Antet de comandă
CHA	Autorizația deținătorului certificatului
CHR	Identificatorul deținătorului certificatului
CV	Vector constant
DER	Reguli de codificare distincte
DO	Obiect de date
DSRC	Comunicații specializate cu rază scurtă de acțiune
ECC	Criptografie bazată pe curbe eliptice
ECDSA	Algoritm pentru semnătura digitală bazat pe curbe eliptice
ECDH	(Algoritm de înțelegere asupra cheii bazat pe) curba eliptică Diffie-Hellman
EGF	echipament GNSS extern
EQT	Echipament
IDE	Echipament inteligent dedicat
K_M	Cheie master a senzorului de mișcare, care permite o asociere a unei unități montate pe vehicul cu un senzor de mișcare
K_{M-VU}	Cheie introdusă în unitățile montate pe vehicule, permițând unei VU să deriveze cheia master a senzorului de mișcare în cazul în care un card de atelier este introdus în respectiva VU
K_{M-WC}	Cheie introdusă în cardurile de atelier, permițând unei VU să deriveze cheia master a senzorului de mișcare în cazul în care un card de atelier este introdus în respectiva VU
MAC	Cod de autentificare a mesajelor
MoS	Senzor de mișcare
MSB	Bitul cel mai semnificativ
PKI	Infrastructură pentru chei publice
RCF	Echipament de comunicare la distanță
SSC	Contor de secvențe trimise
SM	Mesagerie securizată
TDES	Standard de criptare triplă a datelor
TLV	Valoarea lungimii etichetei
VU	Unitate montată pe vehicul
X.C	certificatul de cheie publică al utilizatorului X
X.CA	autoritatea pentru certificate care a emis certificatul utilizatorului X
X.CAR	identificatorul autorității pentru certificate menționat în certificatul utilizatorului X
X.CHR	identificatorul deținătorului certificatului menționat în certificatul utilizatorului X
X.PK	cheia publică a utilizatorului X
X.SK	cheia privată a utilizatorului X
$X.PK_{eph}$	cheia publică efemeră a utilizatorului X
$X.SK_{eph}$	cheia privată efemeră a utilizatorului X
‘xx’	o valoare hexazecimală
||	operator de concatenare

7.3. **Definiții**

Definițiile termenilor utilizați în prezentul apendice sunt incluse în secțiunea I a anexei 1C.

8. SISTEME ȘI ALGORITMI CRIPTOGRAFICI

8.1. **Sisteme criptografice**

CSM_38 Unitățile montate pe vehicule și cardurile de tahograf utilizează un sistem criptografic cu chei publice bazat pe curbe eliptice pentru a oferi următoarele servicii de securitate:

— autentificarea reciprocă între o unitate montată pe vehicul și un card,

— înțelegerea asupra cheilor de sesiune AES între o unitate montată pe vehicul și un card,

— asigurarea autenticității, integrității și nerepudierii datelor descărcate din unitățile montate pe vehicule sau din cardurile de tahograf pe suporturi externe.

CSM_39 Unitățile montate pe vehicule și echipamentele GNSS externe utilizează un sistem criptografic cu chei publice bazat pe curbe eliptice pentru a oferi următoarele servicii de securitate:

— cuplarea unei unități montate pe vehicul cu un echipament GNSS extern,

— autentificarea reciprocă între o unitate montată pe vehicul și un dispozitiv GNSS extern,

— înțelegerea asupra unei chei de sesiune AES între o unitate montată pe vehicul și un echipament GNSS extern,

CSM_40 Unitățile montate pe vehicule și cardurile de tahograf utilizează un sistem criptografic simetric bazat pe AES pentru a oferi următoarele servicii de securitate:

— asigurarea autenticității și integrității datelor schimbate între o unitate montată pe vehicul și un card de tahograf,

— după caz, asigurarea confidențialității datelor schimbate între o unitate montată pe vehicul și un card de tahograf,

CSM_41 Unitățile montate pe vehicule și echipamentele GNSS externe utilizează un sistem criptografic simetric bazat pe AES pentru a oferi următoarele servicii de securitate:

— asigurarea autenticității și integrității datelor schimbate între o unitate montată pe vehicul și un echipament GNSS extern.

CSM_42 Unitățile montate pe vehicule și senzorii de mișcare utilizează un sistem criptografic simetric bazat pe AES pentru a oferi următoarele servicii de securitate:

— asocierea dintre o unitate montată pe vehicul și un senzor de mișcare,

— autentificarea reciprocă între o unitate montată pe vehicul și un senzor de mișcare,

— asigurarea confidențialității datelor schimbate între o unitate montată pe vehicul și un senzor de mișcare.

CSM_43 Unitățile montate pe vehicule și cardurile de tahograf utilizează un sistem criptografic simetric bazat pe AES pentru a oferi următoarele servicii de securitate la nivelul interfeței de comunicare la distanță:

— asigurarea confidențialității, autenticității și integrității datelor transmise de la o unitate montată pe vehicul la un card de control.

Note:

— În mod concret, datele sunt transmise de la o unitate montată pe vehicul la un echipament de interogare la distanță, sub controlul unui agent de control, folosind un echipament de comunicare la distanță care poate fi intern sau extern în raport cu VU (a se vedea apendicele 14). Cu toate acestea, echipamentul de interogare la distanță trimite datele primite unui card de control pentru decriptare și validarea autenticității. Din punctul de vedere al securității, echipamentul de comunicare la distanță și echipamentul de interogare la distanță sunt pe deplin transparente.

— Un card de atelier oferă aceleași servicii de securitate pentru interfața DSRC ca un card de control. Aceasta permite unui atelier să valideze funcționarea corectă a interfeței de comunicare la distanță a unei VU, inclusiv a sistemului de asigurare a securității acesteia. A se vedea secțiunea 9.2.2 pentru informații suplimentare.

8.2. Algoritmi criptografici

8.2.1 *Algoritmi simetrici*

CSM_44 Unitățile montate pe vehicule, cardurile de tahograf, senzorii de mișcare și echipamentele GNSS externe sunt compatibile cu algoritmul AES, astfel cum este definit în [AES], cu lungimi ale cheilor de 128, 192 și 256 de biți.

8.2.2 *Algoritmi asimetrici și parametri de domeniu standardizați*

CSM_45 Unitățile montate pe vehicule, cardurile de tahograf și echipamentele GNSS externe sunt compatibile cu criptografia bazată pe curbe eliptice, cu lungimi ale cheii de 256, 384 și 512/521 biți.

CSM_46 Unitățile montate pe vehicule, cardurile de tahograf și echipamentele GNSS externe sunt compatibile cu algoritmul de semnare ECDSA, astfel cum este precizat în [DSS].

CSM_47 Unitățile montate pe vehicule, cardurile de tahograf și echipamentele GNSS externe sunt compatibile cu algoritmul de înțelegere asupra cheii ECKA-EG, astfel cum este precizat în [TR03111].

CSM_48 Unitățile montate pe vehicule, cardurile de tahograf și echipamentele GNSS externe sunt compatibile cu toți parametrii de domeniu standardizați precizați în tabelul 1 de mai jos pentru criptografia bazată pe curbe eliptice.

Tabelul 1

Parametri de domeniu standardizați

Denumire	Dimensiune (biți)	Referință	Identificatorul de obiect
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

Notă: identificatorii de obiecte menționați în ultima coloană a tabelul 1 sunt specificați în [RFC 5639] pentru curbele Brainpool, respectiv în [RFC 5480] pentru curbele NIST.

Exemplul 1: identificatorul de obiect al curbei BrainpoolP256r1 este `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

Sau în notația cu puncte: `1.3.36.3.3.2.8.1.1.7`.

Exemplul 2: identificatorul de obiect al curbei NIST P-384 este

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

Sau în notația cu puncte: `1.3.132.0.34`.

8.2.3 *Algoritmi de hashing*

CSM_49 Unitățile montate pe vehicule și cardurile de tahograf sunt compatibile cu algoritmii SHA-256, SHA-384 și SHA-512 specificați în [SHS].

8.2.4 *Suite cifru*

CSM_50 În cazul în care un algoritm simetric, un algoritm asimetric și/sau un algoritm de *hashing* sunt utilizați împreună pentru a forma un protocol de securitate, lungimile cheilor lor respective și dimensiunile lor *hash* respective trebuie să aibă (aproximativ) aceeași putere. În tabelul 2 sunt indicate suitele cifru permise:

Tabelul 2

Suite cifru permise

Identificatorul suitei cifru	Lungimea cheii ECC (biți)	Lungimea cheii AES (biți)	Algoritm de *hashing*	Lungimea MAC (octeți)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Notă: Dimensiunile de 512 biți și de 521 de biți ale cheilor sunt considerate a avea puteri egale pentru toate scopurile în cadrul prezentului apendice.

9. CHEI ȘI CERTIFICATE

9.1. **Perechi de chei asimetrice și certificate de cheie publică**

9.1.1 *Considerații generale*

Notă: cheile descrise în această secțiune sunt utilizate pentru autentificarea reciprocă și mesageria securizată între unitățile montate pe vehicule și cardurile de tahograf și între unitățile montate pe vehicule și echipamentele GNSS externe. Aceste procese sunt descrise în detaliu în capitolele 10 și 11 din prezentul apendice.

CSM_51 În cadrul sistemului tahografic inteligent european, perechile de chei ECC și certificatele aferente sunt generate și administrate prin trei niveluri ierarhice funcționale:

— nivelul european,

— nivelul statului membru,

— nivelul echipamentului.

CSM_52 În cadrul întregului sistem tahografic digital european, cheile și certificatele publice și private sunt generate, administrate și comunicate folosind metode standardizate și sigure.

9.1.2 *Nivelul european*

CSM_53 La nivel european se generează o pereche unică de chei ECC denumită EUR. Ea este formată dintr-o cheie privată (EUR.SK) și o cheie publică (EUR.PK). Această pereche de chei reprezintă perechea de chei rădăcină a întregii PKI pentru tahograful digital european. Această sarcină este îndeplinită de o Autoritate europeană pentru certificatele rădăcină (ERCA), sub autoritatea și responsabilitatea Comisiei Europene.

CSM_54 ERCA utilizează cheia privată europeană pentru a semna un certificat rădăcină (autosemnat) al cheii publice europene și comunică acest certificat rădăcină european tuturor statelor membre.

CSM_55 ERCA utilizează cheia privată europeană pentru a semna certificatele cheilor publice ale statelor membre, la cerere. ERCA ține evidențe ale tuturor certificatelor de cheie publică semnate ale statelor membre.

CSM_56 După cum se arată în figura 1 din secțiunea 9.1.7, ERCA generează o nouă pereche de chei rădăcină europene o dată la 17 ani. Ori de câte ori ERCA generează o nouă pereche de chei rădăcină europene, aceasta creează un nou certificat rădăcină autosemnat pentru noua cheie publică europeană. Perioada de valabilitate a unui certificat rădăcină european este de 34 de ani și 3 luni.

Notă: Introducerea unei noi perechi de chei rădăcină implică de asemenea faptul că ERCA va genera o nouă cheie master pentru senzorul de mișcare și o nouă cheie master pentru DSRC (a se vedea secțiunile 9.2.1.2 și 9.2.2.2.)

CSM_57 Înainte de a genera o nouă pereche de chei rădăcină europene, ERCA va efectua o analiză a puterii criptografice necesare pentru noua pereche de chei, ținând cont de faptul că aceasta din urmă ar trebui să fie sigură pentru următorii 34 de ani. Dacă se va considera necesar, ERCA va alege o suită cifru mai puternică decât actuala suită, astfel cum este precizat în CSM_50.

CSM_58 Ori de câte ori generează o nouă pereche de chei rădăcină, ERCA creează un certificat de legătură pentru noua cheie publică europeană și îl semnează cu cheia privată europeană anterioară. Perioada de valabilitate a certificatului de legătură este de 17 ani. Acest proces este prezentat și în figura 1 din secțiunea 9.1.7.

Notă: Întrucât un certificat de legătură conține cheia publică din generația *X* generată de ERCA și este semnat cu cheia privată din generația *X-1* generată de ERCA, un certificat de legătură oferă echipamentului produs în cadrul generației *X-1* o metodă de a avea încredere în echipamentele produse în cadrul generației *X*.

CSM_59 ERCA nu mai utilizează cheia privată a unei perechi de chei rădăcină în niciun scop după momentul în care a fost validat un nou certificat de cheie rădăcină.

CSM_60 În orice moment, ERCA dispune de una dintre următoarele chei criptografice și certificate:

— Perechea de chei EUR actuală și certificatul aferent

— Toate certificatele EUR anterioare care urmează să fie utilizate pentru verificarea certificatelor MSCA încă valabile

— Certificate de legătură pentru toate generațiile de certificate EUR, cu excepția primei generații.

9.1.3 *Nivelul statului membru*

CSM_61 La nivel de stat membru, toate statele membre cărora li se solicită să semneze certificate de card de tahograf generează una sau mai multe perechi de chei ECC unice desemnate ca fiind MSCA_Card. Toate statele membre cărora li se solicită să semneze certificate pentru unități montate pe vehicul sau pentru echipamente GNSS externe generează în plus una sau mai multe perechi de chei ECC desemnate ca fiind MSCA_VU-EGF.

CSM_62 Sarcina de a genera perechi de chei pentru statul membru este îndeplinită de autoritatea pentru certificate a unui stat membru (MSCA). Ori de câte ori o MSCA generează o pereche de chei pentru statul membru, aceasta trimite cheia publică la ERCA în vederea obținerii unui certificat aferent al statului membru, semnat de ERCA.

CSM_63 O MSCA alege puterea unei perechi de chei a unui stat membru astfel încât să fie egală cu puterea perechii de chei rădăcină europene utilizate pentru semnarea certificatului aferent al statului membru.

CSM_64 O pereche de chei MSCA_VU-EGF, dacă există, este formată din cheia privată MSCA_VU-EGF.SK și din cheia publică MSCA_VU-EGF.SK. O MSCA utilizează cheia privată MSCA_VU-EGF.SK exclusiv pentru semnarea certificatelor de cheie publică ale unităților montate pe vehicule și ale echipamentelor GNSS externe.

CSM_65 O pereche de chei MSCA_Card este formată din cheia privată MSCA_Card.SK și din cheia publică MSCA_Card.PK. O MSCA utilizează cheia privată MSCA_Card.SK exclusiv pentru semnarea certificatelor de cheie publică ale cardurilor de tahograf.

CSM_66 O MSCA ține evidențe privind toate certificatele semnate ale unităților montate pe vehicule, ale echipamentelor GNSS externe și ale certificatelor de card, cât și privind identificarea echipamentului căruia îi este destinat fiecare certificat în parte.

CSM_67 Perioada de valabilitate a unui certificat MSCA_VU-EGF este de 17 ani și 3 luni. Perioada de valabilitate a unui certificat MSCA_Card este de 7 ani și 1 lună.

CSM_68 Astfel cum este indicat în figura 1 din secțiunea 9.1.7, cheia privată a unei perechi de chei MSCA_VU-EGF și cheia privată a unei perechi de chei MSCA_Card au o perioadă de utilizare de doi ani.

CSM_69 O MSCA nu mai utilizează cheia privată a unei perechi de chei MSCA_VU-EGF în niciun scop după momentul în care perioada sa de utilizare a expirat. De asemenea, o MSCA nu mai utilizează cheia privată a unei perechi de chei MSCA_Card key în niciun scop după momentul la care perioada sa de utilizare a expirat.

CSM_70 În orice moment, o MSCA dispune de una dintre următoarele chei criptografice și certificate:

— Perechea de chei MSCA_Card actuală și certificatul aferent

— Toate certificatele MSCA_Card anterioare care urmează să fie utilizate pentru verificarea certificatelor cardurilor de tahograf încă valabile

— Certificatul EUR actual necesar pentru verificarea certificatului MSCA actual

— Toate certificatele EUR anterioare necesare pentru verificarea certificatelor MSCA încă valabile

CSM_71 În cazul în care o MSCA este solicitată să semneze certificate pentru unități montate pe vehicule sau pentru echipamente GNSS externe, aceasta trebuie, în plus, să aibă la dispoziție următoarele chei și certificate:

— Perechea de chei MSCA_VU-EGF actuală și certificatul aferent

— Toate cheile publice MSCA_VU-EGF anterioare care urmează să fie utilizate pentru verificarea certificatelor încă valabile ale VU-urilor sau ale echipamentelor GNSS externe

9.1.4 *Nivelul echipamentului: Unități montate pe vehicule*

CSM_72 Pentru fiecare unitate montată pe vehicul sunt generate două perechi de chei ECC unice, desemnate ca fiind VU_MA și VU_Sign. Această sarcină este îndeplinită de producătorii de VU-uri. Ori de câte ori este generată o pereche de chei pentru VU, partea care generează cheia transmite cheia publică către MSCA a țării în care își are reședința, în scopul de a obține un certificat aferent al VU semnat de MSCA. Cheia privată este utilizată doar de către unitatea montată pe vehicul.

CSM_73 Certificatele VU_MA și VU_Sign ale unui anumit vehicul au aceeași dată de începere a valabilității certificatului.

CSM_74 Un producător de VU alege puterea unei perechi de chei pentru VU astfel încât să fie egală cu puterea perechii de chei MSCA utilizate pentru semnarea certificatului aferent al VU.

CSM_75 O unitate montată pe vehicul utilizează perechea sa de chei VU_MA, formată din cheia privată VU_MA.SK și din cheia publică VU_MA.PK, exclusiv pentru procedura de autentificare a VU în raport cu cardurile de tahograf și cu echipamentele GNSS externe, astfel cum este specificat în secțiunile 10.3 și 11.4 din prezentul apendice.

CSM_76 O unitate montată pe vehicul este capabilă să genereze perechi de chei ECC efemere și utilizează o pereche de chei efemere exclusiv pentru a efectua înțelegerea asupra cheilor de sesiune cu un card de tahograf sau cu un echipament GNSS extern, astfel cum este specificat în secțiunile 10.4 și 11.4 din prezentul apendice.

CSM_77 O unitate montată pe vehicul utilizează cheia privată VU_Sign.SK a perechii sale de chei VU_Sign exclusiv pentru a semna fișiere de date descărcate, astfel cum este specificat la capitolul 14 din prezentul apendice. Cheia publică aferentă VU_Sign.PK este utilizată exclusiv pentru a verifica semnăturile create de unitatea montată pe vehicul.

CSM_78 Astfel cum se arată în figura 1 din secțiunea 9.1.7, perioada de valabilitate a unui certificat VU_MA este de 15 ani și 3 luni. Perioada de valabilitate a unui certificat VU_Sign este de asemenea de 15 ani și 3 luni.

Note:

— Perioada prelungită de valabilitate a unui certificat VU_Sign permite unei unități montate pe vehicul să creeze semnături valabile pentru datele descărcate în primele trei luni de la data la care certificatul respectiv a expirat, astfel cum se prevede în Regulamentul (UE) nr. 581/2010.

— Perioada prelungită de valabilitate a unui certificat VU_MA este necesară pentru a permite VU să se autentifice în raport cu un card de control sau cu un card de societate în cursul primelor trei luni de la data la care certificatul respectiv a expirat, astfel încât să fie posibilă descărcarea de date.

CSM_79 O unitate montată pe vehicul nu mai utilizează în niciun scop cheia privată a unei perechi de chei a VU după expirarea valabilității certificatului aferent.

CSM_80 Perechile de chei ale VU (cu excepția perechilor de chei efemere) și certificatele aferente ale unui anumit vehicul nu sunt înlocuite sau reînnoite pe teren odată ce unitatea de vehicul a fost pusă în funcțiune.

Note:

— Perechile de chei efemere nu fac obiectul dispoziției de mai sus, întrucât o pereche nouă de chei efemere este generată de o VU de fiecare dată când se efectuează autentificarea cipului și înțelegerea asupra cheilor de sesiune (a se vedea secțiunea 10.4). A se nota faptul că perechile de chei efemere nu au certificate aferente.

— Această cerință nu exclude posibilitatea de a înlocui perechile de chei ale VU-urilor statice în timpul unei renovări sau reparații efectuate într-un mediu sigur controlat de producător.

CSM_81 Atunci când sunt puse în funcțiune, unitățile montate pe vehicule trebuie să conțină următoarele chei criptografice și certificate:

— Cheia privată VU_MA și certificatul aferent

— Cheia privată VU_Sign și certificatul aferent

— Certificatul MSCA_VU-EGF care conține cheia publică MSCA_VU-EGF.PK destinată verificării certificatului VU_MA și certificatului VU_Sign

— Certificatul EUR care conține cheia publică EUR.PK destinată verificării certificatului MSCA_VU-EGF

— Certificatul EUR a cărui perioadă de valabilitate precede imediat perioada de valabilitate a certificatului EUR destinat verificării certificatului MSCA_VU-EGF, dacă există

— Certificatul de legătură care face conexiunea între aceste două certificate de mai sus, dacă există

CSM_82 Pe lângă cheile criptografice și certificatele enumerate în CSM_81, unitățile montate pe vehicule conțin, de asemenea, chei și certificate specificate în partea A din prezentul apendice, permițând unei unități montate pe vehicul să interacționeze cu cardurile de tahograf de prima generație.

9.1.5 *Nivelul echipamentului: Carduri de tahograf*

CSM_83 Pentru fiecare card de tahograf este generată o unică pereche de chei ECC, desemnată ca fiind Card_MA. O a doua pereche unică de chei ECC, desemnată ca fiind Card_Sign, este generată suplimentar pentru fiecare card de conducător auto și pentru fiecare card de atelier. Această sarcină poate fi îndeplinită de producătorii de carduri sau de serviciile de personalizare a cardurilor. Ori de câte ori este generată o pereche de chei pentru carduri, partea care generează cheia transmite cheia publică către MSCA a țării în care își are reședința, în scopul de a obține un certificat aferent de card semnat de MSCA. Cheia privată este utilizată doar de către cardul de tahograf.

CSM_84 Certificatele Card_MA și Card_Sign ale unui anumit card de conducător auto au aceeași dată de începere a valabilității certificatului.

CSM_85 Un producător de carduri sau un serviciu de personalizare a cardurilor alege puterea unei perechi de chei pentru carduri astfel încât aceasta să fie egală cu puterea perechii de chei MSCA utilizate pentru semnarea certificatului aferent de card.

CSM_86 Un card de tahograf utilizează perechea sa de chei Card_MA, formată din cheia privată Card_MA.SK și din cheia publică Card_MA.PK, exclusiv pentru procedurile de autentificare reciprocă și de înțelegere asupra cheilor de sesiune în raport cu unitățile montate pe vehicul, astfel cum este precizat în secțiunile 10.3 și 10.4 din prezentul apendice.

CSM_87 Un card de conducător auto sau un card de atelier utilizează cheia privată Card_Sign.SK a perechii sale de chei Card_Sign exclusiv pentru a semna fișierele de date descărcate, astfel cum este specificat la capitolul 14 din prezentul apendice. Cheia publică aferentă Card_Sign.PK este utilizată exclusiv pentru a verifica semnăturile create de card.

CSM_88 Perioada de valabilitate a unui certificat Card_MA este după cum urmează:

— Pentru carduri de conducător auto: 5 ani

— Pentru carduri de societate: 2 ani

— Pentru carduri de control: 2 ani

— Pentru carduri de atelier: 1 an

CSM_89 Perioada de valabilitate a unui certificat Card_Sign este după cum urmează:

— Pentru carduri de conducător auto: 5 ani si o lună

— Pentru carduri de atelier: 1 an si o lună

Notă: perioada prelungită de valabilitate a unui certificat Card_Sign permite unui card de conducător auto să creeze semnături valabile pentru datele descărcate în prima lună de la data la care certificatul respectiv a expirat. Acest lucru este necesar având în vedere Regulamentul (UE) nr. 581/2010, care prevede că o descărcare de date de pe un card de conducător auto trebuie să fie posibilă într-un interval de cel mult 28 de zile de la data la care au fost înregistrate ultimele date.

CSM_90 Odată ce cardul a fost emis, perechile de chei și certificatele aferente ale unui anumit tahograf nu sunt înlocuite sau reînnoite.

CSM_91 Atunci când sunt emise, cardurile de tahograf conțin următoarele chei criptografice și certificate:

— cheia privată Card_MA și certificatul aferent

— Pentru cardurile de conducător auto și cardurile de atelier, în plus: cheia privată Card_Sign și certificatul aferent

— certificatul MSCA_Card care conține cheia publică MSCA_Card.PK destinată verificării certificatului Card_MA și certificatului Card_Sign

— certificatul EUR care conține cheia publică EUR.PK destinată verificării certificatului MSCA_Card.

— Certificatul EUR a cărui perioadă de valabilitate precede imediat perioada de valabilitate a certificatului EUR destinat verificării certificatului MSCA_Card, dacă există.

— Certificatul de legătură care face conexiunea între aceste două certificate de mai sus, dacă există.

CSM_92 Pe lângă cheile criptografice și certificatele enumerate în CSM_91, cardurile de tahograf conțin, de asemenea, chei și certificate specificate în partea A din prezentul apendice, permițând acestor carduri să interacționeze cu VU-urile de prima generație.

9.1.6 *Nivelul echipamentului: Echipamente GNSS externe*

CSM_93 O pereche unică de chei ECC este generată pentru fiecare echipament GNSS extern, desemnată ca fiind EGF_MA. Această sarcină este îndeplinită de producătorii de echipamente GNSS externe. Ori de câte ori este generată o pereche de chei EGF_MA, cheia publică este trimisă către MSCA a țării în care aceasta își are reședința, în scopul de a obține un certificat EGF_MA aferent semnat de MSCA. Cheia privată este utilizată doar de către echipamentul GNSS extern.

CSM_94 Un producător de EGF alege puterea unei perechi de chei EGF_MA astfel încât să fie egală cu puterea perechii de chei MSCA utilizate pentru semnarea certificatului aferent EGF_MA.

CSM_95 Un echipament GNSS extern își utilizează perechea de chei EGF_MA, formată din cheia privată EGF_MA.SK și din cheia publică EGF_MA.PK, exclusiv pentru procedurile de autentificare reciprocă și de înțelegere asupra cheilor de sesiune în raport cu unitățile montate pe vehicule, astfel cum este precizat în secțiunile 11.4 și 11.4 din prezentul apendice.

CSM_96 Perioada de valabilitate a certificatului EGF_MA este de 15 ani.

CSM_97 Un echipament GNSS extern nu mai utilizează în niciun scop cheia privată a perechii sale de chei EGF_MA după expirarea valabilității certificatului aferent.

Notă: astfel cum s-a explicat în secțiunea 11.3.3, un EGF ar putea folosi cheia sa privată pentru autentificarea reciprocă în raport cu VU-ul la care este deja cuplat, chiar și după expirarea certificatului aferent.

CSM_98 Odată ce EGF a fost pus în funcțiune, perechea de chei EGF_MA și certificatul aferent ale unui anumit echipament GNSS extern nu sunt înlocuite sau reînnoite pe teren.

Notă: Această cerință nu exclude posibilitatea de a înlocui perechile de chei EGF în timpul unei renovări sau reparații efectuate într-un mediu sigur controlat de producătorul EGF-ului.

CSM_99 Atunci când sunt puse în funcțiune, echipamentele GNSS externe trebuie să conțină următoarele chei criptografice și certificate:

— cheia privată EGF_MA și certificatul aferent

— certificatul MSCA_VU-EGF care conține cheia publică MSCA_VU-EGF.PK destinată verificării certificatului EGF_MA

— Certificatul EUR care conține cheia publică EUR.PK destinată verificării certificatului MSCA_VU-EGF

— Certificatul EUR a cărui perioadă de valabilitate precede imediat perioada de valabilitate a certificatului EUR destinat verificării certificatului MSCA_VU-EGF, dacă există

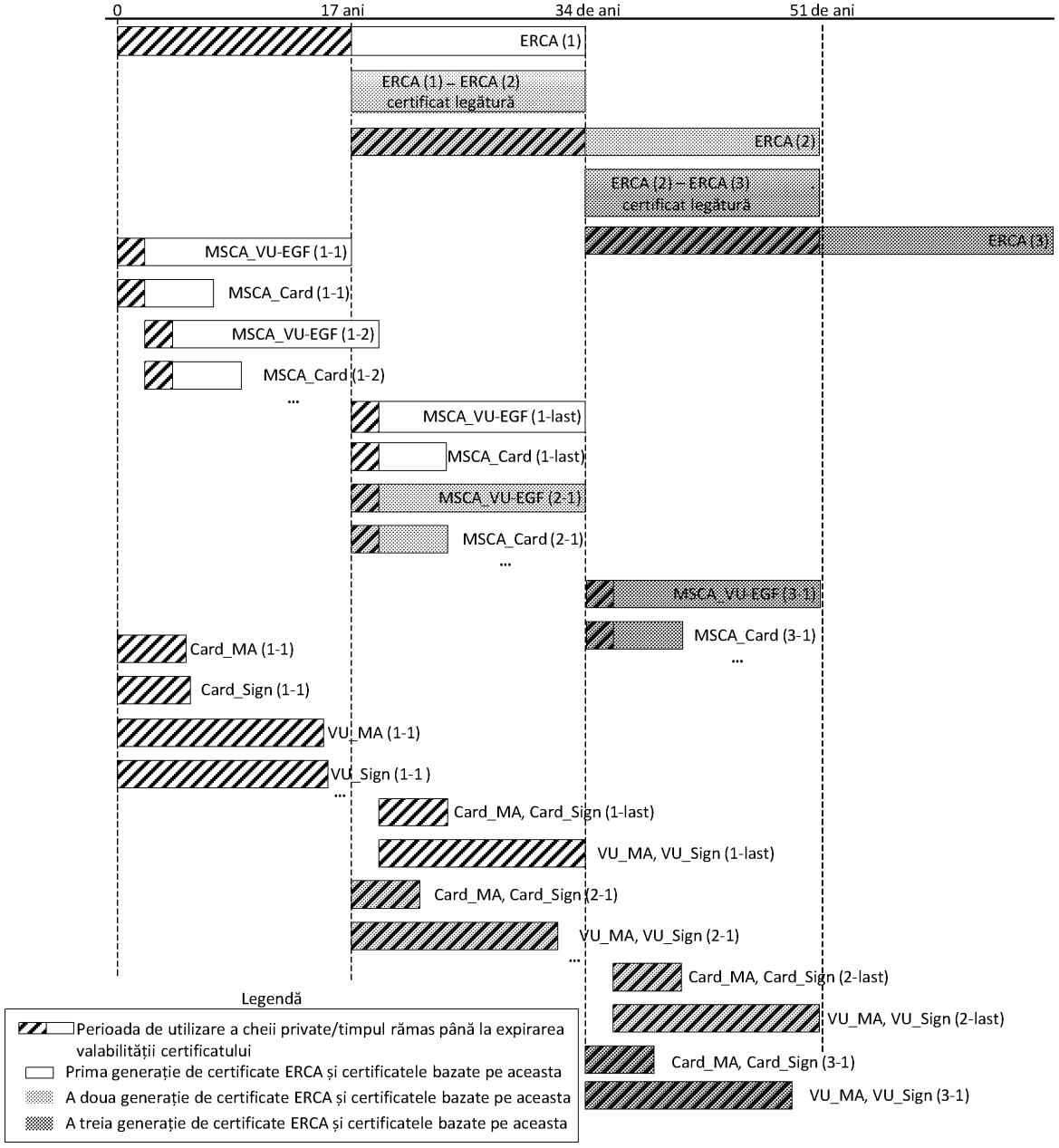
— Certificatul de legătură care face conexiunea între aceste două certificate de mai sus, dacă există

9.1.7 *Prezentare generală: Înlocuirea certificatelor*

În figura 1 de mai jos este prezentat modul în care sunt emise și utilizate de-a lungul timpului diferitele generații de certificate rădăcină ERCA, de certificate de legătură ERCA, de certificate MSCA și de certificate de echipament (VU și card).

Figura 1

Eliberarea și utilizarea diferitelor generații de certificate rădăcină ERCA, de certificate de legătură ERCA, de certificate MSCA și de certificate de echipament



Note la figura 1:

1. Diferitele generații ale certificatului rădăcină sunt indicate de un număr între paranteze. De exemplu, ERCA (1) este prima generație a certificatului rădăcină ERCA; ERCA (2) este a doua generație etc.

2. Alte certificate sunt marcate cu două cifre între paranteze, prima cifră indicând generația certificatului rădăcină în cadrul căreia acestea sunt emise, iar a doua cifră indicând generația certificatului în sine. De exemplu, MSCA_Card (1-1) este primul certificat MSCA_Card emis în cadrul generației ERCA (1); MSCA_Card (2-1) este primul certificat MSCA_Card emis în cadrul generației ERCA (2); MSCA_Card (2-last) este ultimul certificat MSCA_Card emis în cadrul generației ERCA (2); Card_MA (2-1) este primul certificat de card pentru autentificare reciprocă emis în cadrul generației ERCA (2) etc.

3. Certificatele MSCA_Card (2-1) și MSCA_Card (1-last) sunt emise aproape la aceeași dată, dar nu exact la aceeași dată. MSCA_Card (2-1) este primul certificat MSCA_Card emis în cadrul generației ERCA (2) și va fi emis puțin mai târziu decât MSCA_Card (1-last), acesta din urmă fiind ultimul certificat MSCA_Card emis în cadrul generației ERCA (1).

4. Astfel cum este indicat în figură, primele certificate VU și de card emise în cadrul ERCA (2) vor apărea cu aproape doi ani înaintea apariției ultimelor certificate VU și de card emise în cadrul generației ERCA (1). Această situație este o consecință a faptului că certificatele VU și de card nu sunt emise în mod direct în cadrul certificatului ERCA, ci în cadrul unui certificat MSCA. Certificatul MSCA (2-1) va fi emis direct după începerea valabilității ERCA (2), dar certificatul MSCA (1-ultimul) va fi emis cu puțin timp înaintea momentului respectiv, și anume în ultimul moment în care certificatul ERCA (1) este încă valabil. Prin urmare, aceste două certificate MSCA vor avea aproape aceeași perioadă de valabilitate, cu toate că sunt din generații diferite.

5. Perioada de valabilitate indicată pentru carduri este cea pentru cardurile de conducător auto (5 ani).

6. Pentru a economisi spațiu, diferența dintre perioadele de valabilitate ale certificatelor CARD_MA și Card_Sign și diferența dintre perioadele de valabilitate ale certificatelor VU_MA și VU_Sign este indicată numai pentru prima generație.

9.2. **Chei simetrice**

9.2.1 *Chei pentru siguranța comunicațiilor dintre VU și senzorul de mișcare*

9.2.1.1 *Considerații generale*

Notă: se consideră că cititorii prezentei secțiuni sunt familiarizați cu conținutul standardului (ISO 16844-3), care descrie interfața dintre o unitate montată pe vehicul și un senzor de mișcare. Procesul de asociere dintre o VU și un senzor de mișcare este descris în mod detaliat la capitolul 12 din prezentul apendice.

CSM_100 Sunt necesare mai multe chei simetrice pentru asocierea dintre unitățile montate pe vehicule și senzorii de mișcare, pentru autentificarea reciprocă între unitățile montate pe vehicule și senzorii de mișcare și pentru criptarea comunicațiilor dintre unitățile montate pe vehicule și senzorii de mișcare, astfel cum se arată în tabelul 3. Toate aceste chei sunt chei AES cu o lungime egală cu lungimea cheii master a senzorului de mișcare, care este legată de lungimea (preconizată) a perechii de chei rădăcină europene, astfel cum este precizat în CSM_50.

Tabelul 3

Chei pentru securizarea comunicațiilor dintre unitatea montată pe vehicul și senzorul de mișcare

Cheie	Simbol	Generată de	Metodă de generare	Stocată de
Cheie master a senzorului de mișcare – componentă a VU	$K_{M\text{-}VU}$	ERCA	Aleatoriu	ERCA, MSCA-uri implicate în eliberarea certificatelor VU, producători de VU, unități montate pe vehicul

Cheie	Simbol	Generată de	Metodă de generare	Stocată de
Cheie master a senzorului de mișcare – componentă a atelierului	K_{M-WC}	ERCA	Aleatoriu	ERCA, MSCA-uri, producătorii de carduri, cardurile de atelier
Cheie master a senzorului de mișcare	K_M	Nu este generată în mod independent	Calculată astfel: $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, MSCA-uri implicate în emiterea de chei pentru senzorii de mișcare (opțional) (*)
Cheie de identificare	K_{ID}	Nu este generată în mod independent	Calculată astfel: $K_{ID} = K_M$ XOR CV, unde CV este precizat în CSM_106	ERCA, MSCA-uri implicate în emiterea de chei pentru senzorii de mișcare (opțional) (*)
Cheie de asociere	K_P	Producător de senzori de mișcare	Aleatoriu	Un senzor de mișcare
Cheie de sesiune	K_S	VU (în timpul asocierii dintre VU și senzorul de mișcare)	Aleatoriu	O VU și un senzor de mișcare

(*) Stocarea cheilor K_M și K_{ID} este opțională, întrucât aceste chei pot fi derivate din K_{M-VU}, K_{M-WC} și CV.

CSM_101 Autoritatea europeană pentru certificatele rădăcină generează K_{M-VU} și K_{M-WC}, două chei AES unice și aleatorii, pe baza cărora poate fi calculată cheia master a senzorului de mișcare, K_M, ca fiind K_{M-VU} XOR K_{M-WC}. ERCA comunică K_M, K_{M-VU} și K_{M-WC} autorităților pentru certificate ale statelor membre, la cererea acestora.

CSM_102 ERCA atribuie fiecărei chei master K_M a senzorului de mișcare un număr unic de versiune, ceea ce este aplicabil și pentru constituirea cheilor K_{M-VU} și K_{M-WC}, precum și pentru cheia de identificare aferentă K_{ID}. ERCA informează MSCA-urile cu privire la numărul versiunii în momentul în care le trimite acestora cheile K_{M-VU} și K_{M-WC}.

Notă: Numărul versiunii este utilizat pentru a face distincția între diferitele generații ale acestor chei, astfel cum se explică în detaliu în secțiunea 9.2.1.2.

CSM_103 O autoritate pentru certificate a unui stat membru transmite cheia K_{M-VU}, împreună cu numărul versiunii sale, producătorilor de unități montate pe vehicule, la cererea acestora. Producătorii de VU introduc K_{M-VU} și numărul versiunii acesteia în toate VU produse.

CSM_104 O autoritate pentru certificate a unui stat membru se asigură că cheia K_{M-WC}, împreună cu numărul versiunii sale, sunt introduse în toate cardurile de atelier emise sub responsabilitatea acesteia.

Note:

— A se vedea descrierea tipului de date `SensorInstallationSecData` din apendicele 2.

— astfel cum se explică în secțiunea 9.2.1.2, poate fi necesar ca mai multe generații de chei K_{M-WC} să fie introduse în același card de atelier.

CSM_105 Pe lângă cheia AES menționată în CSM_104, o MSCA se asigură că cheia TDES Km_{WC}, specificată în cerința CSM_037 din partea A din prezentul apendice, este introdusă în fiecare card emis sub responsabilitatea acesteia.

Note:

— Aceasta permite utilizarea unui card de atelier de a doua generație pentru cuplarea cu o VU de prima generație.

— Un card de atelier de a doua generație va conține două aplicații diferite, și anume una care îndeplinește cerințele din partea B din prezentul apendice și una care îndeplinește cerințele din partea A. Cea din urmă aplicație va conține cheia TDES Km_{WC}.

CSM_106 O MSCA implicată în emiterea de senzori de mișcare derivă cheia de identificare pornind de la cheia master a senzorului de mișcare căreia i se aplică operația logică XOR (disjuncție exclusivă) cu un vector constant CV. Valoarea CV este după cum urmează:

— Pentru cheile master de 128 de biți ale senzorilor de mișcare: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83'

— Pentru cheile master de 192 de biți ale senzorilor de mișcare: CV = '72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25'

— Pentru cheile master de 256 de biți ale senzorilor de mișcare: CV = '1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60'

Notă: vectorii constanți au fost generați după cum urmează:

Pi_10 = primii 10 octeți ai porțiunii zecimale a constantei matematice π = '24 3F 6A 88 85 A3 08 D3 13 19'

CV_ 128-bits = primii 16 octeți ai SHA-256(Pi_10)

CV_ 192-bits = primii 24 de octeți ai SHA-384(Pi_10)

CV_ 256-bits = primii 32 de octeți ai SHA-512(Pi_10)

CSM_107 Producătorii senzorilor de mișcare generează o cheie de asociere K_P aleatorie și unică pentru fiecare senzor de mișcare și trimite fiecare cheie de asociere autorității pentru certificate a unui stat membru. MSCA criptează fiecare cheie de asociere în mod separat, cu cheia master K_M a senzorului de mișcare, și returnează cheia criptată producătorului senzorului de mișcare. Pentru fiecare cheie criptată, MSCA notifică producătorului senzorului de mișcare numărul versiunii cheii K_M asociate.

Notă: astfel cum s-a explicat în secțiunea 9.2.1.2, poate fi necesar ca un producător de senzori de mișcare să genereze mai multe chei de asociere unice pentru un singur senzor de mișcare.

CSM_108 Producătorii de senzori de mișcare generează un număr de serie unic pentru fiecare senzor de mișcare și trimit toate numerele de serie autorității pentru certificate a unui stat membru. MSCA criptează fiecare număr de serie în mod separat, cu cheia de identificare K_{ID}, și returnează numărul de serie criptat producătorului senzorului de mișcare. Pentru fiecare număr de serie criptat, MSCA notifică producătorul senzorului de mișcare numărul versiunii cheii K_{ID} asociate.

CSM_109 Pentru cerințele CSM_107 și CSM_108, MSCA utilizează algoritmul AES în modul de operare cu înlănțuirea blocurilor cifrate, astfel cum este definit în standardul (ISO 10116), cu un parametru intermediar m = 1 și un vector de inițializare SV = '00' {16}, adică 16 octeți cu valoarea binară 0. După caz, MSCA utilizează metoda de completare 2 definită în (ISO 9797-1).

CSM_110 Producătorul senzorului de mișcare stochează cheia de asociere criptată și numărul de serie criptat în senzorul de mișcare destinat, împreună cu valorile de text în clar și cu numerele versiunilor cheilor K_M și K_{ID} utilizate pentru criptare.

Notă: astfel cum s-a explicat în secțiunea 9.2.1.2, poate fi necesar ca un producător de senzori de mișcare să introducă mai multe chei de asociere criptate și mai multe numere de serie criptate într-un singur senzor de mișcare.

CSM_111 Pe lângă materialul criptografic bazat pe AES specificat în CSM_110, un producător de senzori de mișcare poate stoca, de asemenea, în fiecare senzor de mișcare materialul criptografic bazat pe TDES specificat în cerința CSM_037 din partea A din prezentul apendice.

Notă: acest lucru va permite cuplarea unui senzor de mișcare de a doua generație la o VU de prima generație.

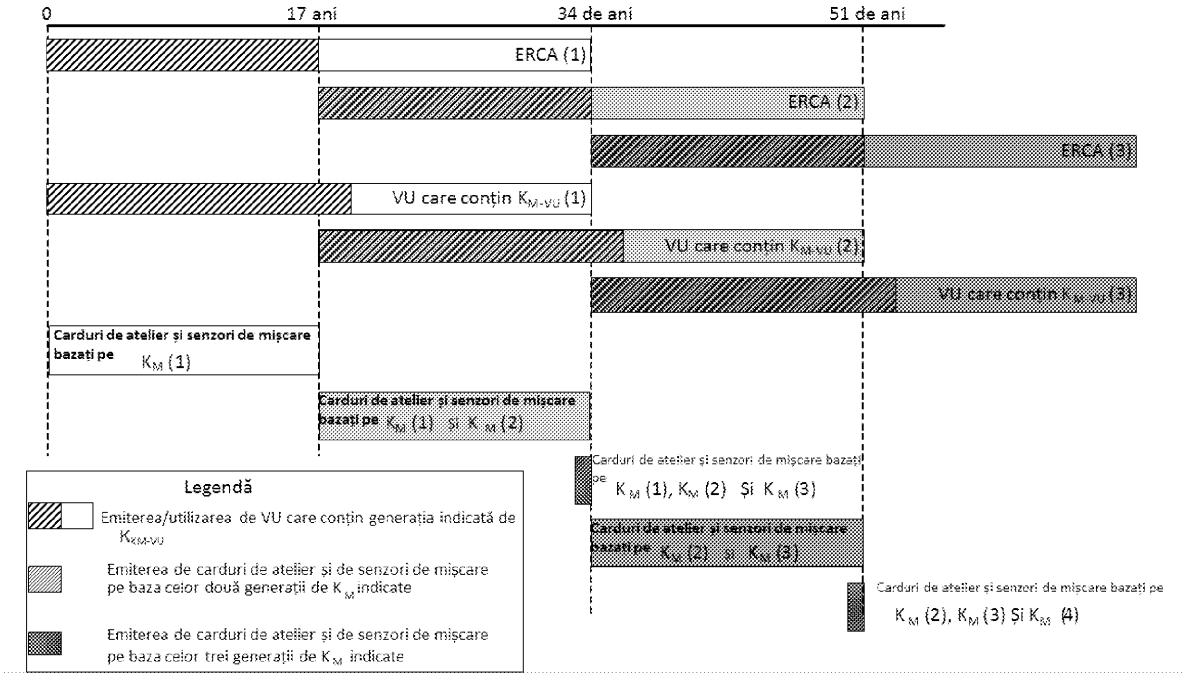
CSM_112 Lungimea cheii de sesiune K_S generate de o VU în timpul asocierii cu un senzor de mișcare depinde de lungimea cheii sale K_{M-VU}, astfel cum este precizat în CSM_50.

9.2.1.2 *Înlocuirea cheii master a senzorului de mișcare din echipamentul de a doua generație.*

CSM_113 Fiecare cheie master a senzorului de mișcare și toate cheile aferente (a se vedea tabelul 3) sunt asociate cu o generație specifică a perechii de chei rădăcină a ERCA. Prin urmare, aceste chei se înlocuiesc o dată la 17 ani. Perioada de valabilitate a fiecărei generații a cheii master a senzorului de mișcare începe cu un an înaintea începerii valabilității perechii de chei rădăcină asociate a ERCA și se termină atunci când perechea de chei rădăcină asociată a ERCA expiră. Acest fapt este descris în figura 2.

Figura 2

Emiterea și utilizarea diferitelor generații ale cheii master a senzorului de mișcare din unitățile montate pe vehicule, din senzorii de mișcare și din cardurile de atelier



CSM_114 Cu cel puțin un an înainte de generarea unei noi perechi de chei rădăcină europene, astfel cum este descris în CSM_56, ERCA generează o nouă cheie master K_M a senzorului de mișcare prin generarea unor noi chei K_{M-VU} și K_{M-WC}. Lungimea cheii master a senzorului de mișcare este legată de puterea prevăzută a noii perechi de chei rădăcină europene, în conformitate cu CSM_50. ERCA comunică noile chei K_M, K_{M-VU} și K_{M-WC} MSCA-urilor, la cererea acestora, împreună cu numărul lor de versiune respectiv.

CSM_115 O MSCA se asigură că toate generațiile valabile de chei K_{M-WC} sunt stocate pe fiecare card de atelier emis sub autoritatea acesteia, împreună cu numerele lor de versiune, astfel cum este prezentat în figura 2.

Notă: aceasta implică faptul că, în ultimul an al perioadei de valabilitate a unui certificat ERCA, cardurile de atelier vor fi emise cu trei generații diferite de K_{M-WC}, astfel cum este indicat în figura 2.

CSM_116 În ceea ce privește procesul descris în CSM_107 și CSM_108 de mai sus: O MSCA criptează fiecare pereche de chei de asociere K_P pe care o primește de la un producător de senzori de mișcare în mod separat cu fiecare generație valabilă a cheii master K_M a senzorului de mișcare. O MSCA criptează de asemenea fiecare număr de serie pe care îl primește de la un producător de senzori de mișcare în mod separat cu fiecare generație valabilă a cheii de identificare K_{ID}. Un producător de senzori de mișcare stochează toate criptările cheii de asociere și toate criptările numărului de serie în senzorul de mișcare destinat, împreună cu valorile de text în clar aferente și cu numărul (numerele) de versiune ale cheilor K_M și K_{ID} utilizate pentru criptare.

Notă: aceasta implică faptul că, în ultimul an al perioadei de valabilitate a unui certificat ERCA, senzorii de mișcare vor fi livrați cu date criptate bazate pe trei generații diferite de K_M, astfel cum este indicat în figura 2.

CSM_117 În ceea ce privește procesul descris în CSM_107 de mai sus: Întrucât lungimea cheii de asociere K_P este legată de lungimea cheii K_M (a se vedea CSM_100), poate fi necesar ca un producător de senzori de mișcare să genereze până la trei perechi diferite de chei de asociere (de lungimi diferite) pentru un senzor de mișcare, în cazul în care generațiile ulterioare de chei K_M au lungimi diferite. În acest caz, producătorul trimite fiecare pereche de chei de asociere către MSCA. MSCA se asigură că fiecare cheie de asociere este criptată cu generația corectă a cheii master a senzorului de mișcare, adică cu cea care are aceeași lungime.

Notă: În cazul în care producătorul senzorului de mișcare decide să genereze o cheie de asociere bazată pe TDES pentru un senzor de mișcare de a doua generație (a se vedea CSM_111), producătorul îi indică MSCA-ului faptul că pentru criptarea acestei chei de asociere trebuie să fie utilizată cheia master bazată pe TDES a senzorului de mișcare. Acest lucru se datorează faptului că lungimea unei chei TDES poate să nu fie egală cu cea a unei chei AES și, prin urmare, MSCA nu poate trage o concluzie exclusiv pe baza lungimii cheii.

CSM_118 Producătorii de unități montate pe vehicule introduc doar o generație de K_{M-VU} în fiecare unitate montată pe vehicul, împreună cu numărul versiunii acesteia. Această generație de K_{M-VU} este legată de certificatul ERCA pe care sunt bazate certificatele unităților montate pe vehicule.

Note:

— O unitate montată pe vehicul bazată pe certificatul ERCA din generația *X* conține doar cheia K_{M-VU} din generația *X*, chiar dacă a fost produsă după începutul perioadei de valabilitate a certificatului ERCA din generația *X+1*. Această situație este ilustrată în figura 2.

— O VU din generația *X* nu poate fi asociată cu un senzor de mișcare din generația *X-1*

— Întrucât cardurile de atelier au o perioadă de valabilitate de un an, rezultatul CSM_113 – CSM_118 este că toate cardurile de atelier vor conține noua cheie K_{M-WC} la momentul producerii primei VU care conține noua cheie K_{M-VU}. Prin urmare, o astfel de VU va fi întotdeauna în măsură să calculeze noua cheie K_M. În plus, până la momentul respectiv, majoritatea noilor senzori de mișcare vor conține date criptate bazate inclusiv pe noua cheie K_M.

9.2.2 *Chei pentru securizarea comunicațiilor specializate cu rază scurtă de acțiune (DSRC)*

9.2.2.1 *Considerații generale*

CSM_119 Autenticitatea și confidențialitatea datelor comunicate de la o unitate montată pe vehicul la o autoritate de control printr-un canal de comunicare la distanță DSRC este asigurată prin intermediul unui set de chei AES specifice ale VU derivate dintr-o singură cheie master DSRC, și anume din cheia KM_{DSRC}.

CSM_120 Cheia master DSRC, KM_{DSRC}, este o cheie AES generată, stocată și distribuită de ERCA în mod securizat. Lungimea cheii poate fi de 128,192 sau 256 de biți și este legată de lungimea perechii de chei rădăcină europene, astfel cum este descris în CSM_50.

CSM_121 ERCA comunică în mod securizat cheia master DSRC autorităților pentru certificate ale statelor membre, la cererea acestora, pentru a le permite să deriveze cheile DSRC specifice ale VU și pentru a se asigura că cheia master DSRC este introdusă în toate cardurile de control și în toate cardurile de atelier emise sub responsabilitatea lor.

CSM_122 ERCA atribuie fiecărei chei master DSRC un număr unic de versiune. ERCA informează MSCA-urile cu privire la numărul versiunii în momentul în care le trimite cheia master DSRC.

Notă: Numărul versiunii este utilizat pentru a face distincția între diferitele generații ale cheii master DSRC, astfel cum se explică în detaliu în secțiunea 9.2.2.2.

CSM_123 Pentru fiecare unitate montată pe vehicul, producătorul unității montate pe vehicul creează un număr de serie unic al VU și trimite acest număr autorității pentru certificate a statului său membru într-o cerere de obținere a unui set de două chei DSRC specifice pentru VU. Numărul de serie al VU are tipul de date `VuSerialNumber`, iar pentru codificare se utilizează regulile de codificare distincte (DER), în conformitate cu (ISO 8825-1).

CSM_124 La primirea unei cereri de chei DSRC specifice pentru VU, MSCA derivează două chei AES pentru unitatea montată pe vehicul, denumite K_VU_{DSRC}_ENC și K_VU_{DSRC}_MAC. Aceste chei specifice pentru VU trebuie să aibă lungimea egală cu cea a cheii master DSRC. MSCA utilizează funcția de derivare a cheilor definită în [RFC 5869]. Funcția *hash* necesară pentru a instanția funcția HMAC-hash este legată de lungimea cheii master DSRC, astfel cum este precizat în CSM_50. Funcția de derivare a cheilor din standardul [RFC 5869] este după cum urmează:

Etapa 1 (extragere)

— *PRK* = HMAC-Hash (*salt, IKM*), unde *salt* este un șir vid ‘ ’, iar *IKM* este KM_{DSRC}.

Etapa 2 (extindere)

— *OKM* = *T(1)*, unde

T(1) = HMAC-Hash (*PRK, T(0)* || *info* || ‘01’), cu

— *T (0)* = un șir vid (‘ ’),

— *info* = numărul de serie al VU, astfel cum este specificat în CSM_123

— K_VU_{DSRC}_ENC = primii *L* octeți ai *OKM* și

K_VU_{DSRC}_MAC = ultimii *L* octeți ai *OKM,*

unde *L* este lungimea necesară a K_VU_{DSRC}_ENC și a K_VU_{DSRC}_MAC în octeți.

CSM_125 MSCA distribuie K_VU_{DSRC}_ENC și K_VU_{DSRC}_MAC producătorilor de VU într-un mod securizat pentru a fi introduse în unitatea montată pe vehicul căreia îi sunt destinate.

CSM_126 La momentul producerii, o unitate montată pe vehicul are stocate în memoria sa securizată cheile K_VU_{DSRC}_ENC și K_VU_{DSRC}_MAC, pentru a putea asigura integritatea, autenticitatea și confidențialitatea datelor trimise prin canalul de comunicare la distanță. O unitate montată pe vehicul stochează de asemenea cheia master DSRC utilizată pentru a deriva aceste chei specifice pentru VU.

CSM_127 La momentul emiterii, cardurile de control și cardurile de atelier au stocate în memoria lor securizată cheia KM_{DSRC}, pentru a putea verifica astfel integritatea și autenticitatea datelor trimise de o VU printr-un canal de comunicare la distanță și pentru a putea decripta datele respective. Cardurile de control și cardurile de atelier stochează de asemenea numărul versiunii cheii master DSRC.

Notă: astfel cum se explică în secțiunea 9.2.2.2, poate fi necesar ca mai multe generații de chei KM_{DSRC} să fie introduse în același card de atelier sau în același card de control.

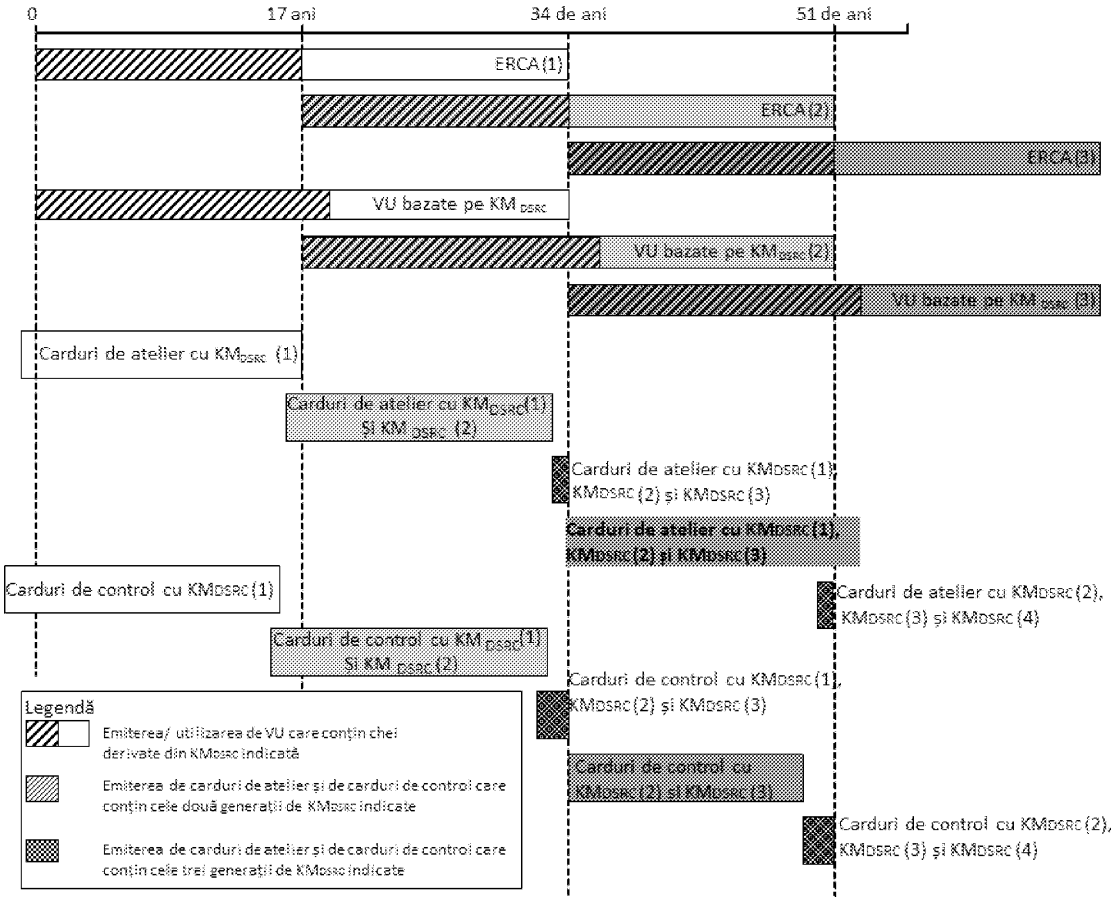
CSM_128 MSCA ține evidența tuturor cheilor DSRC specifice pentru VU pe care le-a generat, a numărului versiunii acestora și a detaliilor de identificare a VU cărora le este destinat fiecare set de chei.

9.2.2.2 *Înlocuirea cheii master DSRC*

CSM_129 Fiecare cheie master DSRC este asociată cu o generație specifică a perechii de chei rădăcină a ERCA. Prin urmare, ERCA înlocuiește cheia master DSRC o dată la 17 ani. Perioada de valabilitate a fiecărei generații a cheii master DSRC începe cu doi ani înaintea începerii valabilității perechii de chei rădăcină asociate a ERCA și se termină atunci când perechea de chei rădăcină asociată a ERCA expiră. Acest fapt este descris în figura 3.

Figura 3

Emiterea și utilizarea diferitelor generații ale cheii master DSRC în unitățile montate pe vehicule, în cardurile de atelier și în cardurile de control



CSM_130 Cu cel puțin doi ani înainte de generarea unei noi perechi de chei rădăcină europene, astfel cum este descris în CSM_56, ERCA generează o nouă cheie master DSRC. Lungimea cheii master DSRC este legată de puterea prevăzută a noii perechi de chei rădăcină europene, în conformitate cu CSM_50. ERCA comunică noua cheie master DSRC MSCA-urilor, la cererea acestora, împreună cu numărul versiunii sale.

CSM_131 O MSCA se asigură că toate generațiile valabile ale cheii KM_{DSRC} sunt stocate pe fiecare card de control emis sub autoritatea acesteia, împreună cu numerele versiunilor acestora, astfel cum este ilustrat în figura 3.

Notă: aceasta implică faptul că, în ultimii doi ani ai perioadei de valabilitate a unui certificat ERCA, cardurile de control vor fi emise cu trei generații diferite ale cheii KM_{DSRC}, astfel cum este indicat în figura 3.

CSM_132 O MSCA se asigură că toate generațiile cheii KM_{DSRC} care au fost valabile pentru cel puțin un an și sunt în continuare valabile sunt stocate pe fiecare card de atelier emis sub autoritatea acesteia, împreună cu numerele versiunilor acestora, astfel cum este ilustrat în figura 3.

Notă: aceasta implică faptul că, în ultimul an al perioadei de valabilitate a unui certificat ERCA, cardurile de atelier vor fi emise cu trei generații diferite ale KM_{DSRC}, astfel cum este indicat în figura 3.

CSM_133 Producătorii de unități montate pe vehicule introduc doar un set de chei DSRC specifice pentru VU în fiecare unitate montată pe vehicul, împreună cu numărul versiunii acestora. Acest set de chei este derivat din generația KM_{DSRC} legată de certificatul ERCA pe care se bazează certificatele unităților montate pe vehicule.

Note:

— Acest lucru implică faptul că o unitate montată pe vehicul bazată pe certificatul ERCA din generația *X* conține doar cheile K_VU_{DSRC}_ENC și K_VU_{DSRC}_MAC din generația *X*, chiar dacă VU a fost produsă după începutul perioadei de valabilitate a certificatului ERCA din generația *X +1*. Această situație este ilustrată în figura 3.

— Deoarece perioada de valabilitate a cardurilor de atelier este de un an, iar a cardurilor de control este de doi ani, rezultatul CSM_131 – CSM_133 este că toate cardurile de atelier și toate cardurile de control vor conține noua cheie master DSRC la momentul în care va fi emisă prima VU conținând chei specifice pentru VU bazate pe cheia master respectivă.

9.3. **Certificate**

9.3.1 *Considerații generale*

CSM_134 Toate certificatele din sistemul european de tahografe inteligente se pot autodescrie și sunt verificabile cu ajutorul cardurilor (CV), în conformitate cu (ISO 7816-4) și (ISO 7816-8).

CSM_135 Regulile de codificare distincte (DER), în conformitate cu (ISO 8825-1), sunt utilizate atât pentru codificarea structurilor de date ASN.1, cât și pentru codificarea obiectelor de date (specifice aplicațiilor) în cadrul certificatelor.

Notă: această codificare are ca rezultat o structură de tip „valoarea lungimii etichetei” (TLV) după cum urmează:

Etichetă: Eticheta este codificată în unul sau doi octeți și indică conținutul.

Lungime: Lungimea este codificată ca un întreg nesemnat în unul, doi sau trei octeți, ducând la o lungime maximă de 65 535 de octeți. Se utilizează numărul minim de octeți.

Valoare: Valoarea este codificată în zero sau mai mulți octeți.

9.3.2 *Conținutul certificatelor*

CSM_136 Toate certificatele au structura prezentată în profilul de certificat din tabelul 4.

Tabelul 4

Profil de certificat versiunea 1

Câmp	ID-ul câmpului	Etichetă	Lungime (octeți)	Tip de date ASN. 1 (a se vedea apendicele 1)
Certificat ECC	C	‘7F 21‘	var	
Corpul certificatului ECC	B	‘7F 4E‘	var	

Câmp	ID-ul câmpului	Etichetă	Lungime (octeți)	Tip de date ASN. 1 (a se vedea apendicele 1)
Identificator de profil al certificatului	CPI	'5F 29'	'01'	INTEGER(0..255)
Identificatorul autorității pentru certificate	CAR	'42'	'08'	KeyIdentifier
Autorizația deținătorului certificatului	CHA	'5F 4C'	'07'	CertificateHolder Authorisation
Cheie publică	PK	'7F 49'	var	
Parametrii de domeniu	DP	'06'	var	OBJECT IDENTIFIER
Punct public	PP	'86'	var	OCTET STRING
Identificatorul deținătorului certificatului	CHR	'5F 20'	'08'	KeyIdentifier
Data de începere a valabilității certificatului	CEfD	'5F 25'	'04'	TimeReal
Data expirării certificatului	CExD	'5F 24'	'04'	TimeReal
Semnătura certificatului ECC	S	'5F 37'	var	OCTET STRING

Notă: ID-ul câmpului va fi utilizat în secțiuni ulterioare ale prezentului apendice pentru a indica câmpurile individuale ale unui certificat; de exemplu, X.CAR este identificatorul autorității pentru certificate menționat în certificatul utilizatorului X.

9.3.2.1 Identificator de profil al certificatului

CSM_137 Certificatele utilizează un identificator de profil al certificatului pentru a indica profilul certificatului utilizat. Versiunea 1, astfel cum este specificat în tabelul 4, este identificată de o valoare '00'.

9.3.2.2 Identificatorul autorității pentru certificate

CSM_138 Identificatorul autorității pentru certificate se folosește pentru identificarea cheii publice care trebuie utilizată pentru verificarea semnăturii unui certificat. Prin urmare, identificatorul autorității pentru certificate este egal cu identificatorul deținătorului certificatului în certificatul autorității aferente pentru certificate.

CSM_139 Un certificat rădăcină al ERCA este autosemnat, adică identificatorul autorității pentru certificate este egal cu identificatorul deținătorului certificatului în certificat.

CSM_140 În cazul unui certificat de legătură al ERCA, identificatorul deținătorului certificatului (CHR) este egal cu CHR al noului certificat rădăcină al ERCA. Identificatorul autorității pentru certificate în cazul unui certificat de legătură este egal cu CHR al certificatului rădăcină anterior al ERCA.

9.3.2.3 Autorizația deținătorului certificatului

CSM_141 Autorizația deținătorului certificatului este folosită pentru a identifica tipul de certificat. Aceasta este formată din cei mai semnificativi șase octeți ai ID-ului aplicației tahografice, concatenați cu tipul de echipament căruia îi este destinat certificatul.

9.3.2.4 Cheie publică

Cheia publică imbrică două elemente de date: parametrii de domeniu standardizați care urmează să fie utilizați cu cheia publică în certificat și valoarea punctului public.

CSM_142 Elementul de date *Domain Parameters* conține unul dintre identificatorii de obiect specificați în tabelul 1 pentru a face trimitere la un set de parametri de domeniu standardizați.

CSM_143 Elementul de date *Public Point* conține punctul public. Punctele publice pe bază de curbe eliptice sunt transformate în șiruri de octeți, astfel cum este precizat în (TR-03111). Se utilizează formatul de codificare necomprimat. La recuperarea unui punct bazat pe curbe eliptice din formatul său codificat, se efectuează întotdeauna validările descrise în (TR-03111).

9.3.2.5 Identificatorul deținătorului certificatului

CSM_144 Identificatorul deținătorului certificatului este un identificator pentru cheia publică furnizată în certificat. El este utilizat pentru a face trimitere la această cheie publică în alte certificate.

CSM_145 În cazul certificatelor de card și al certificatelor de echipament GNSS extern, identificatorul deținătorului certificatului are tipul de date `ExtendedSerialNumber` specificat în apendicele 1.

CSM_146 În cazul unităților montate pe vehicul, în momentul în care producătorul solicită un certificat, acesta poate să știe sau poate să nu știe numărul de serie, specific producătorului, al VU căreia îi sunt destinate certificatul respectiv și cheia privată asociată. În primul caz, identificatorul deținătorului certificatului are tipul de date `ExtendedSerialNumber` specificat în apendicele 1. În al doilea caz, identificatorul deținătorului certificatului are tipul de date `CertificateRequestID` specificat în apendicele 1.

CSM_147 În cazul certificatelor ERCA și MSCA, identificatorul deținătorului certificatului are tipul de date `CertificationAuthorityKID` specificat în apendicele 1.

9.3.2.6 Data de începere a valabilității certificatului

CSM_148 Data de începere a valabilității certificatului indică data și ora la care certificatul intră în perioada de valabilitate. Data de începere a valabilității certificatului este data la care certificatul a fost generat.

9.3.2.7 Data expirării certificatului

CSM_149 Data expirării certificatului indică data și ora de la care certificatul nu mai este valabil.

9.3.2.8 Semnătura de pe certificat

CSM_150 Semnătura de pe certificat este creată prin intermediul corpului codificat al certificatului, inclusiv eticheta și lungimea corpului certificatului. Algoritmul semnăturii este ECDSA, astfel cum este precizat în [DSS], folosindu-se algoritmul de *hashing* legat de mărimea cheii autorității cu drept de semnătură, astfel cum este specificat în CSM_50. Formatul semnăturii este simplu, astfel cum este precizat în (TR-03111).

9.3.3 *Solicitarea de certificate*

CSM_151 Atunci când solicită un certificat, un solicitant trebuie să transmită următoarele date autorității sale pentru certificate:

— Identificatorul de profil al certificatului solicitat

— Referința autorității pentru certificate care se preconizează a fi utilizată pentru semnarea certificatului.

— Cheia publică care urmează să fie semnată

CSM_152 Pe lângă datele din CSM_151, o MSCA trimite către ERCA următoarele date în cadrul unei cereri de certificat, permițând ERCA să creeze identificatorul deținătorului certificatului pentru noul certificat MSCA:

— Codul numeric național al autorității de certificare (tip de date `NationNumeric` definit în apendicele 1)

— Codul alfanumeric național al autorității de certificare (tip de date `NationAlpha` definit în apendicele 1)

— Numărul de serie de 1 octet pentru a face distincția între diferitele chei ale autorității de certificare în cazul în care aceste chei sunt modificate.

— Câmpul de doi octeți care conține informații suplimentare specifice privind autoritatea de certificare.

CSM_153 Pe lângă datele din CSM_151, un producător de echipamente trimite către MSCA următoarele date în cadrul unei cereri de certificat, permițând MSCA să creeze identificatorul deținătorului certificatului pentru noul certificat de echipament:

— Un identificator al tipului de echipament, specific producătorului

— Dacă este cunoscut (a se vedea CSM_154), un număr de serie al echipamentului, asociat în mod unic producătorului, precum și tipul echipamentului și luna în care acesta a fost produs. În caz contrar, un identificator unic asociat cererii de certificat.

— Luna și anul de producție a echipamentelor sau ale cererii de certificat.

Producătorul trebuie să se asigure că aceste date sunt corecte și că certificatul transmis înapoi de către MSCA este introdus în echipamentul căruia îi este destinat.

CSM_154 În cazul unei VU, în momentul în care producătorul solicită un certificat, acesta poate să știe sau poate să nu știe numărul de serie, specific producătorului, al VU căreia îi sunt destinate certificatul respectiv și cheia privată asociată. În primul caz, producătorul unității montate pe vehicul trimite acest număr de serie către MSCA. În cel de al doilea caz, producătorul trebuie să identifice în mod unic fiecare cerere de certificat și să trimită către MSCA numărul de serie al acestei cereri de certificat. Certificatul astfel obținut va conține prin urmare numărul de serie al cererii de certificat. După introducerea certificatului într-o VU specifică, producătorul îi comunică MSCA legătura dintre numărul de serie al cererii de certificat și identificarea VU.

10. AUTENTIFICAREA RECIPROCĂ ȘI MESAGERIA SECURIZATĂ ÎNTRE VU ȘI CARDURI

10.1. **Considerații generale**

CSM_155 La un nivel înalt, comunicarea securizată între o unitate montată pe vehicul și un card de tahograf se bazează pe următoarele etape:

— În prima etapă, fiecare parte îi demonstrează celeilalte părți că deține un certificat de cheie publică, semnat de către autoritatea pentru certificate a unui stat membru. La rândul său, certificatul de cheie publică al MSCA trebuie să fie semnat de Autoritatea europeană pentru certificatele rădăcină. Această etapă se numește verificarea lanțului de certificate și este descrisă în detaliu în secțiunea 10.2.

— În a doua etapă, unitatea montată pe vehicul îi demonstrează cardului că este în posesia cheii private aferente cheii publice din certificatul prezentat. Acest lucru se realizează prin semnarea unui număr aleatoriu trimis de card. Cardul verifică semnătura prin intermediul numărului aleatoriu. În cazul în care această verificare are un rezultat pozitiv, VU este autentificată. Această etapă se numește autentificarea VU și este descrisă în detaliu în secțiunea 10.3.

— În a treia etapă, ambele părți, în mod independent, calculează două chei de sesiune AES utilizând un algoritm asimetric de înțelegere asupra cheii. Utilizând una dintre aceste chei de sesiune, cardul creează un cod de autentificare a mesajelor (MAC) prin intermediul unor date trimise de VU. VU verifică MAC. În cazul în care această verificare are un rezultat pozitiv, cardul este autentificat. Această etapă se numește autentificarea cardului și este descrisă în detaliu în secțiunea 10.4.

— În a patra etapă, VU și cardul utilizează cheile de sesiune convenite pentru a asigura confidențialitatea, integritatea și autenticitatea tuturor mesajelor schimbate. Aceasta se numește mesageria securizată și este descrisă în detaliu în secțiunea 10.5.

CSM_156 Mecanismul descris în CSM_155 este declanșat de unitatea montată pe vehicul ori de câte ori se introduce un card într-unul dintre sloturile sale pentru carduri.

10.2. **Verificarea reciprocă a lanțului de certificate**

10.2.1 *Verificarea lanțului de certificate de către VU*

CSM_157 Unitățile montate pe vehicul utilizează protocolul descris în figura 4 pentru a verifica lanțul de certificate al unui card de tahograf.

Note la figura 4:

— Certificatele de card și cheile publice menționate în figură sunt cele utilizate pentru autentificarea reciprocă. Acestea sunt indicate în secțiunea 9.1.5 ca fiind Card_MA.

— Certificatele și cheile publice Card.CA menționate în figură sunt cele utilizate pentru semnarea certificatelor de card și sunt indicate în CAR al certificatului de card. Acestea sunt indicate în secțiunea 9.1.3 ca fiind MSCA_Card.

— Certificatul Card.CA.EUR menționat în figură este certificatul rădăcină european precizat în CAR al certificatului Card.CA.

— Certificatul Card.Link menționat în figură este certificatul de legătură al cardului, dacă acesta există. Astfel cum este specificat în secțiunea 9.1.2, acesta este un certificat de legătură pentru o nouă pereche de chei rădăcină europene create de ERCA și semnate de cheia privată europeană anterioară.

— Certificatul Card.Link.EUR este certificatul rădăcină european precizat în CAR al certificatului Card.Link.

CSM_158 Așa cum se arată în figura 4, verificarea lanțului de certificate al cardului începe la introducerea cardului. Unitatea montată pe vehicul citește identificatorul titularului cardului (`cardExtendedSerialNumber`) din EF ICC VU verifică dacă cunoaște cardul, și anume, dacă verificarea lanțului de certificate efectuată anterior de către VU respectivă a avut un rezultat pozitiv și dacă lanțul în cauză a fost stocat pentru consultare viitoare. Dacă rezultatul verificării a fost pozitiv și dacă certificatul de card este încă valabil, procesul continuă cu verificarea lanțului de certificate ale VU. În caz contrar, VU citește de pe card, în mod succesiv, certificatul MSCA_Card necesar pentru a verifica certificatul de card (certificatul Card_CA). Certificatul EUR necesar pentru a verifica certificatul MSCA_Card, precum și, eventual, certificatul de legătură, până ce găsește un certificat pe care îl cunoaște sau pe care îl poate verifica. În cazul în care este găsit un certificat, VU utilizează certificatul respectiv pentru a verifica certificatele de card subiacente pe care le-a citit de pe card. În cazul în care rezultatele sunt pozitive, procesul continuă cu verificarea lanțului de certificate ale VU. În cazul în care rezultatele sunt negative, VU ignoră cardul.

Notă: Există trei moduri în care VU poate cunoaște certificatul Card.CA.EUR:

— certificatul Card.CA.EUR este același certificat ca certificatul EUR al VU;

— certificatul Card.CA.EUR precede certificatul EUR al VU, iar VU conținea deja acest certificat la emitere (a se vedea CSM_81);

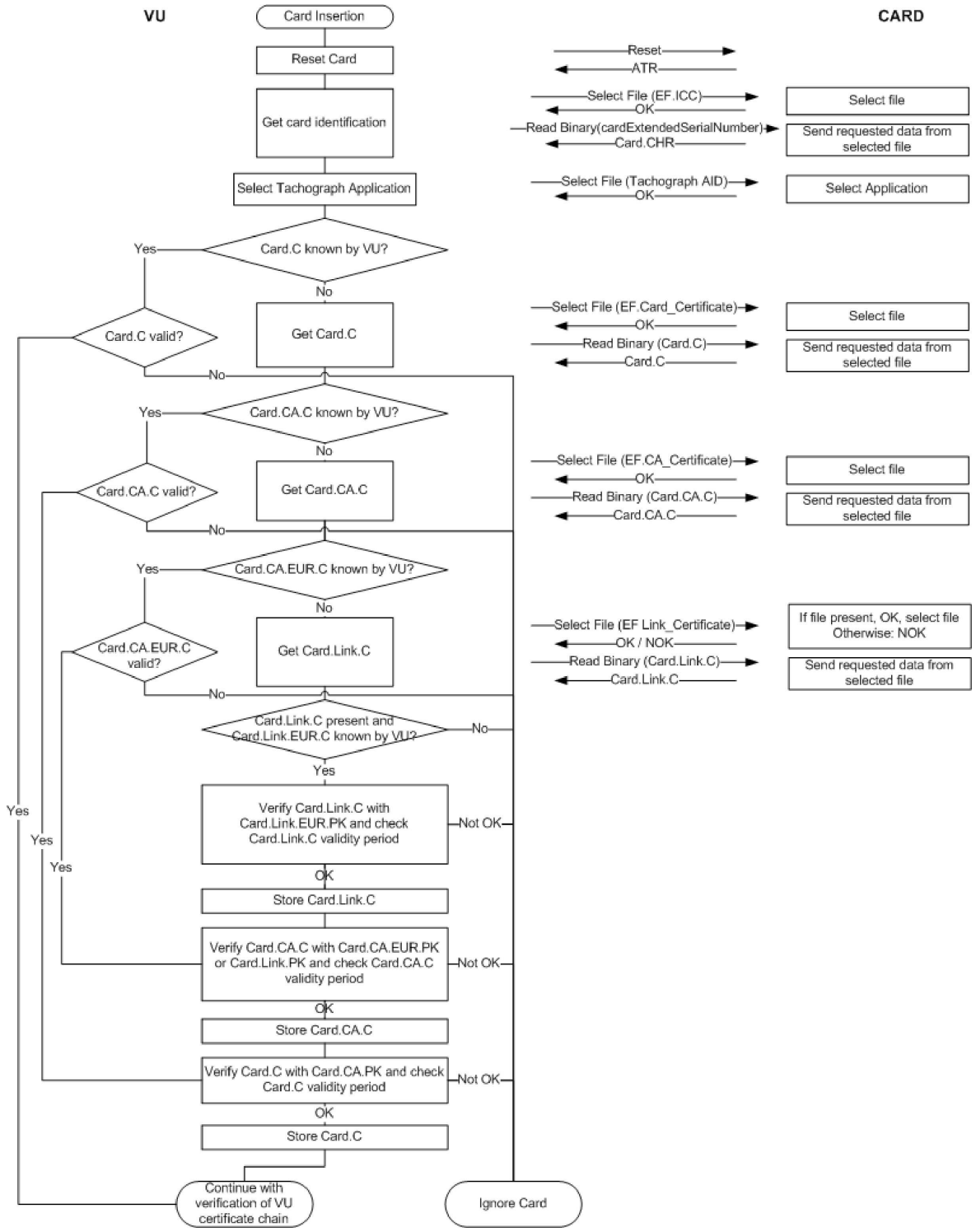
— certificatul Card.CA.EUR este emis ulterior certificatului EUR al VU, iar VU a primit anterior un certificat de legătură de la un alt card de tahograf, l-a verificat și l-a stocat pentru consultare viitoare.

CSM_159 Astfel cum este indicat în figura 4, după ce VU a verificat autenticitatea și valabilitatea unui certificat care era necunoscut anterior, aceasta poate stoca certificatul respectiv pentru consultare viitoare nemaifiind necesar, prin urmare, ca VU să verifice încă o dată autenticitatea certificatului respectiv dacă acesta este prezentat din nou unității montate pe vehicul. În loc de a stoca întregul certificat, o VU poate alege să stocheze numai conținuturile corpului certificatului, astfel cum se specifică în secțiunea 9.3.2.

CSM_160 VU verifică valabilitatea temporală a oricărui certificat, citită de pe card sau stocată în memoria sa, și respinge certificatele expirate. Pentru a verifica valabilitatea temporală a unui certificat prezentat de card, o VU își utilizează ceasul intern.

Figura 4

Protocol pentru verificarea lanțului de certificate de card de către VU

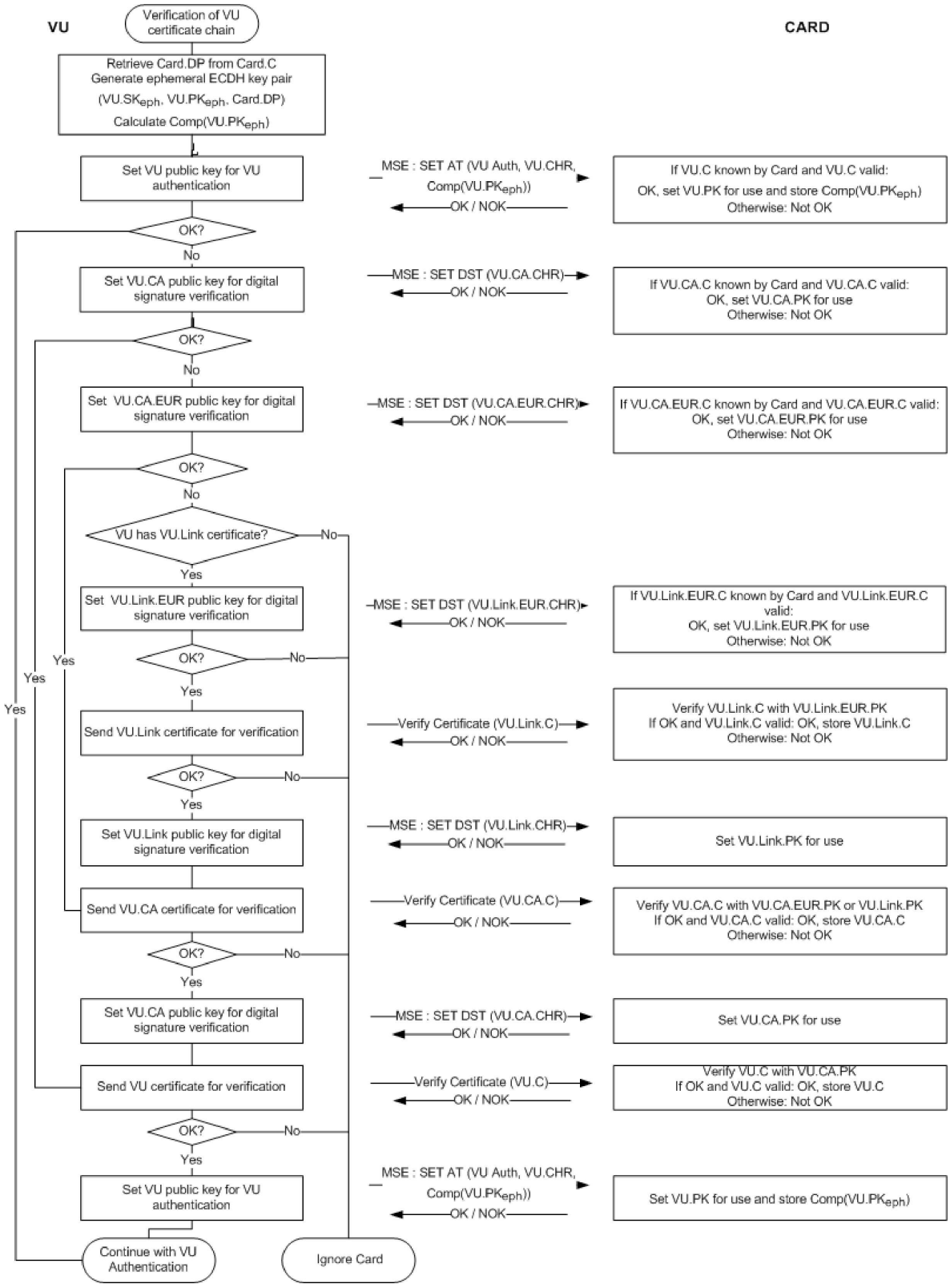


10.2.2 *Verificarea lanțului de certificate ale VU de către card*

CSM_161 Cardurile de tahograf utilizează protocolul descris în figura 5 pentru a verifica lanțul de certificate al unei VU.

Figura 5

Protocol pentru verificarea lanțului de certificate ale VU de către card



Note la figura 5:

— Certificatele VU și cheile publice menționate în figură sunt cele utilizate pentru autentificarea reciprocă. Acestea sunt indicate în secțiunea 9.1.4 ca fiind VU_Card.

— Certificatele și cheile publice VU.CA menționate în figură sunt cele utilizate pentru semnarea certificatelor VU și ale echipamentelor GNSS externe. Acestea sunt indicate în secțiunea 9.1.3 ca fiind MSCA_VU-EGF.

— Certificatul VU.CA.EUR menționat în figură este certificatul rădăcină european precizat în CAR al certificatului VU.CA.

— Certificatul VU.Link menționat în figură este certificatul de legătură al VU, dacă acesta există. Astfel cum este specificat în secțiunea 9.1.2, acesta este un certificat de legătură pentru o nouă pereche de chei rădăcină europene create de ERCA și semnate de cheia europeană anterioară.

— Certificatul VU.Link.EUR este certificatul rădăcină european precizat în CAR al certificatului VU.Link.

CSM_162 Astfel cum se indică în figura 5, verificarea lanțului de certificate ale unității montate pe vehicul începe cu încercarea unității montate pe vehicul de a-și stabili propria cheie publică pentru a fi utilizată în cardul de tahograf. Dacă această încercare se concretizează, înseamnă că lanțul de certificate ale VU a fost verificat cu succes de către card, acesta din urmă stocând certificatul VU pentru consultare ulterioară. În acest caz, certificatul VU este pregătit pentru utilizare, iar procesul continuă cu autentificarea VU. În cazul în care cardul nu cunoaște certificatul VU, VU prezintă în mod succesiv certificatul VU.CA care trebuie folosit pentru verificarea certificatului său VU, certificatul VU.CA.EUR care trebuie folosit pentru verificarea certificatului VU.CA, precum și, eventual, certificatul de legătură, în scopul de a găsi un certificat cunoscut sau verificabil de către card. În cazul în care este găsit un astfel de certificat, cardul utilizează certificatul respectiv pentru a verifica certificatele VU subiacente care i-au fost prezentate. Dacă verificarea are un rezultat pozitiv, VU își stabilește în final cheia publică necesară pentru utilizarea în cardul de tahograf. În cazul în care rezultatele verificării sunt negative, VU ignoră cardul.

Notă: Există trei moduri prin care cardul poate cunoaște certificatul VU.CA.EUR:

— certificatul VU.CA.EUR este același certificat ca certificatul EUR al cardului;

— certificatul VU.CA.EUR precede certificatul EUR al cardului, iar cardul conținea deja acest certificat la emitere (a se vedea CSM_91);

— certificatul VU.CAR.EUR este emis ulterior emiterii certificatului EUR al cardului, iar cardul a primit anterior un certificat de legătură de la o altă unitate montată pe vehicul, l-a verificat și l-a stocat pentru consultare viitoare.

CSM_163 VU folosește comanda MSE: Set AT pentru a-și stabili cheia publică care urmează a fi utilizată în cardul de tahograf. Astfel cum se specifică în apendicele 2, această comandă conține o indicație a mecanismului criptografic care va fi utilizat cu cheia stabilită. Acest mecanism este denumit în continuare „Autentificarea VU utilizând algoritmul ECDSA, în combinație cu algoritmul de *hashing* legat de mărimea cheilor din perechea de chei VU_MA a VU, astfel cum este specificat în CSM_50".

CSM_164 Comanda MSE: Set AT conține de asemenea o indicație privind perechea de chei efemere pe care le va utiliza VU în timpul înțelegerii asupra cheilor de sesiune (a se vedea secțiunea 10.4). Prin urmare, înainte de a lansa comanda MSE: Set AT, VU generează o pereche de chei ECC efemere. Pentru generarea perechii de chei efemere, VU utilizează parametrii de domeniu standardizați indicați în certificatul de card. Perechea de chei efemeră se notează astfel: ($VU.SK_{eph}$, $VU.PK_{eph}$, Card. DP). VU utilizează coordonata x a punctului public efemer ECDH ca identificator al cheii; aceasta este denumită reprezentarea comprimată a cheii publice și este notată astfel: Comp($VU.PK_{eph}$).

CSM_165 În cazul în care comanda MSE: Set AT funcționează corect, cardul stabilește cheia VU.PK indicată pentru a o utiliza ulterior în timpul autentificării vehiculului și stochează temporar Comp($VU.PK_{eph}$). În cazul în care două sau mai mult comenzi MSE: Set AT sunt lansate cu succes înaintea efectuării înțelegerii asupra cheilor de sesiune, cardul stochează doar ultima Comp($VU.PK_{eph}$) primită.

CSM_166 Cardul verifică valabilitatea temporală a oricărui certificat prezentat de VU sau menționat de VU la momentul stocării în memoria cardului și respinge certificatele expirate.

CSM_167 Pentru a verifica valabilitatea temporală a unui certificat prezentat de VU, fiecare card de tahograf stochează intern anumite date care reprezintă ora curentă. Aceste date nu sunt actualizate direct de către o VU. La momentul emiterii, ora curentă a cardului este reglată pentru a fi egală cu momentul la care începe valabilitatea certificatului Card_MA al cardului. Un card își actualizează ora curentă dacă momentul la care începe valabilitatea unui certificat autentic de tip „sursă valabilă de indicare a orei" prezentat de o VU este mai recent decât ora curentă a cardului. În acest caz, cardul își reglează ora curentă pentru a fi identică cu momentul la care începe valabilitatea certificatului respectiv. Cardul acceptă doar următoarele certificate ca sursă valabilă de indicare a orei:

— Certificatele de legătură ERCA de a doua generație

— Certificatele MSCA de a doua generație

— Certificatele VU de a doua generație emise de aceeași țară care a emis certificatul (certificatele) de card al(e) cardului.

Notă: ultima cerință implică faptul că un card este în măsură să recunoască CAR al certificatului VU, adică certificatul MSCA_VU-EGF. CAR recunoscut nu va fi același precum CAR al propriului certificat, care este certificatul MSCA_Card.

CSM_168 Astfel cum este indicat în figura 5, după ce cardul a verificat autenticitatea și valabilitatea unui certificat care era necunoscut anterior, acesta poate stoca certificatul respectiv pentru consultare viitoare, astfel încât cardul nu mai trebuie să verifice încă o dată autenticitatea certificatului respectiv dacă acesta este prezentat din nou cardului. În loc de a stoca întregul certificat, un card poate alege să stocheze numai conținuturile corpului certificatului, astfel cum se specifică în secțiunea 9.3.2.

10.3. **Autentificarea VU**

CSM_169 Unitățile montate pe vehicule și cardurile utilizează protocolul de autentificare descris în figura 6 pentru a autentifica VU în raport cu cardul. Autentificarea VU permite cardului de tahograf să verifice în mod explicit că VU este autentică. În acest sens, VU își utilizează cheia privată pentru a semna date de provocare generate de card.

CSM_170 Alături de datele de provocare de pe card / ale cardului, VU include în semnătură referința titularului cardului obținută din certificatul de card.

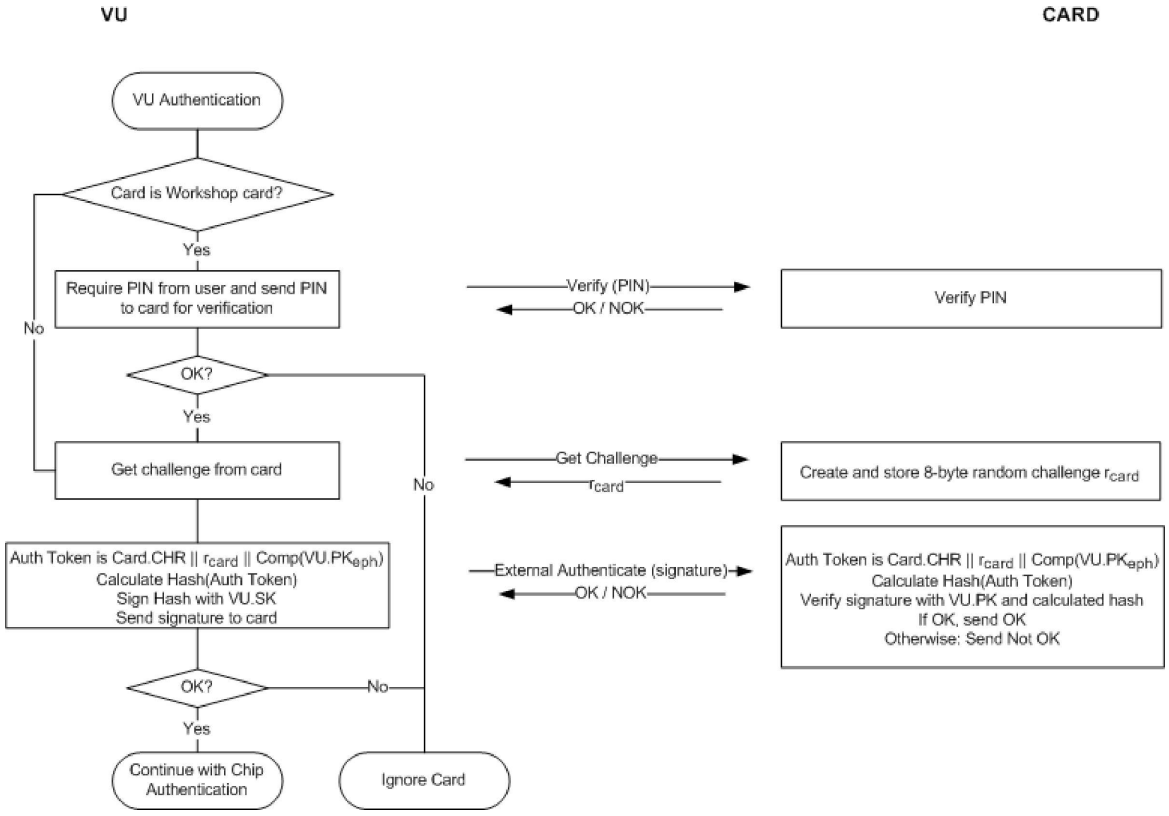
Notă: Astfel este garantat faptul că acest card în raport cu care se autentifică VU este același card al cărui lanț de certificate a fost verificat anterior de către VU.

CSM_171 VU include, de asemenea, în semnătură, identificatorul cheii publice efemere Comp(VU.PK_{eph}), utilizate de VU pentru a stabili mesageria securizată în timpul procesului de autentificare a cipului, specificată în secțiunea 10.4.

Notă: Acest lucru asigură faptul că VU cu care comunică un card în timpul sesiunii de mesagerie securizată este aceeași VU care a fost autentificată de card.

Figura 6

Protocolul de autentificare a VU



CSM_172 În cazul în care mai multe comenzi GET CHALLENGE sunt trimise de VU în timpul autentificării VU, cardul trimite de fiecare dată înapoi noi date de provocare aleatorii de 8 octeți, dar stochează doar ultimele date de provocare.

CSM_173 Algoritmul de semnare utilizat de VU pentru autentificarea VU este ECDSA, astfel cum este precizat în [DSS], folosindu-se algoritmul de *hashing* legat de mărimea cheilor din perechea de chei VU_MA a VU, astfel cum este specificat în CSM_50. Formatul semnăturii este simplu, astfel cum este precizat în (TR-03111). VU trimite cardului semnătura rezultată.

CSM_174 La primirea semnăturii VU într-o comandă EXTERNAL AUTHENTICATE, cardul

— calculează tokenul de autentificare prin concatenarea Card.CHR, a datelor de provocare r_{card} a cardului și a identificatorului cheii publice efemere a VU, Comp($VU.PK_{eph}$),

— calculează valoarea *hash* prin intermediul tokenului de autentificare, utilizând algoritmul de *hashing* legat de mărimea cheilor din perechea de chei VU_MA a VU, astfel cum este specificat în CSM_50,

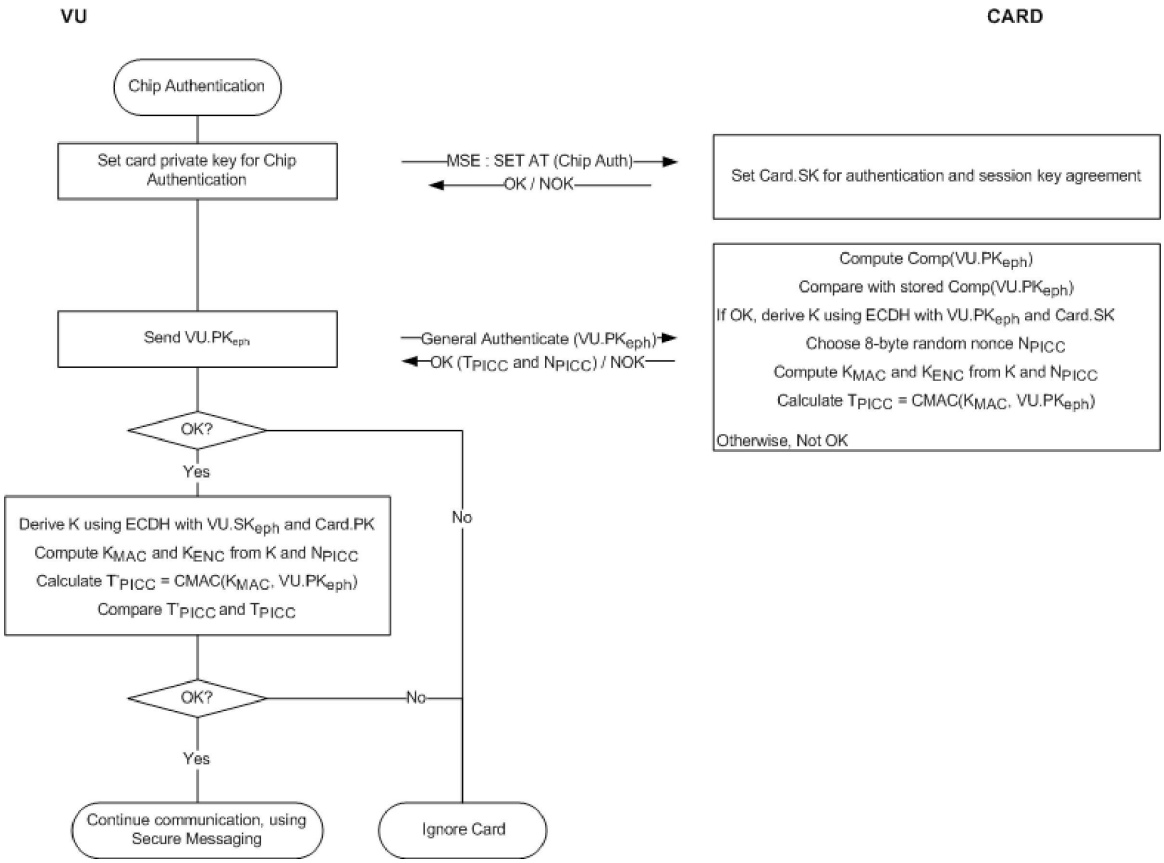
— verifică semnătura VU utilizând algoritmul ECDSA în combinație cu VU.PK și cu valoarea *hash* calculată.

10.4. **Autentificarea cipului și înțelegerea asupra cheilor de sesiune**

CSM_175 Unitățile montate pe vehicule și cardurile utilizează protocolul de autentificare a cipului descris în **figura 7** pentru a autentifica cardul în raport cu VU. Autentificarea cipului permite unității montate pe vehicul să verifice în mod explicit autenticitatea cardului.

Figura 7

Autentificarea cipului și înțelegerea asupra cheilor de sesiune



CSM_176 VU și cardul parcurg următoarele etape:

1. Unitatea montată pe vehicul inițiază procesul de autentificare a cipului prin lansarea comenzii MSE: Set AT, care indică „Autentificare a cipului utilizând algoritmul ECDH rezultând într-o lungime a cheii de sesiune legată de mărimea cheilor din perechea de chei Card_MA a cardului, astfel cum este specificat în CSM_50”. VU determină mărimea cheilor din perechea de chei a cardului pe baza certificatului de card.

2. VU trimite cardului punctul public $VU.PK_{eph}$ al perechii sale de chei efemere. Astfel cum a fost explicat în CSM_164, VU a generat această pereche de chei efemere anterior verificării lanțului de certificate ale VU. VU a trimis cardului identificatorul cheii publice efemere $Comp(VU.PK_{eph})$, iar cardul l-a stocat.

3. Cardul calculează $Comp(VU.PK_{eph})$ pe baza $VU.PK_{eph}$ și îl compară cu valoarea stocată a $Comp(VU.PK_{eph})$.

4. Utilizând algoritmul ECDH în combinație cu cheia privată statică a cardului și cu cheia publică efemeră a VU, cardul calculează o cheie K secretă.

5. Cardul alege o cheie de unică folosință aleatorie de 8 octeți, N_{PICC}, și o utilizează pentru a deriva două chei de sesiune AES, K_{MAC} și K_{ENC}, pe baza cheii K. A se vedea CSM_179.

6. Utilizând K_{MAC}, cardul calculează un token de autentificare prin intermediul identificatorului cheii publice efemere a VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Cardul trimite N_{PICC} și T_{PICC} unității montate pe vehicul.

7. Utilizând algoritmul ECDH în combinație cu cheia privată statică a cardului și cu cheia publică efemeră a VU, VU calculează aceeași cheie secretă K calculată de card în etapa 4.

8. VU derivează cheile de sesiune K_{MAC} și K_{ENC} pe baza cheilor K și N_{PICC}; A se vedea CSM_179.

9. VU verifică autenticitatea tokenului T_{PICC}.

CSM_177 În etapa 3 de mai sus, cardul calculează Comp(VU.PKeph) drept coordonata x a punctului public în VU.PKeph.

CSM_178 În etapele 4 și 7 de mai sus, cardul și unitatea montată pe vehicul utilizează algoritmul ECKA-EG astfel cum este definit în (TR-03111).

CSM_179 În etapele 5 și 8 de mai sus, cardul și unitatea montată pe vehicul utilizează funcția de derivare a cheilor pentru cheile de sesiune AES definite în (TR-03111), cu următoarele precizii și modificări:

— Valoarea contorului este '00 00 00 01' pentru K_{ENC} și '00 00 00 02' pentru $K_{MAC.}$

— Cheia opțională de unică folosință *r* este utilizată și este egală cu N_{PICC}.

— Pentru cheile AES derivate de 128 de biți, algoritmul de *hashing* care trebuie utilizat este SHA-256.

— Pentru cheile AES derivate de 192 de biți, algoritmul de *hashing* care trebuie utilizat este SHA-384.

— Pentru cheile AES derivate de 256 de biți, algoritmul de *hashing* care trebuie utilizat este SHA-512.

Lungimea cheilor de sesiune (adică lungimea la care valoarea *hash* este trunchiată) este legată de mărimea perechii de chei Card_MA, astfel cum este specificat în CSM_50.

CSM_180 În etapele 6 și 9 de mai sus, cardul și unitatea montată pe vehicul utilizează algoritmul AES în modul CMAC, astfel cum este definit în [SP 800-38B]. Lungimea T_{PIC} este legată de lungimea cheilor de sesiune AES, astfel cum este specificat în CSM_50.

10.5. **Mesagerie securizată**

10.5.1 *Considerații generale*

CSM_181 Toate comenzile și toate răspunsurile schimbate între o unitate montată pe vehicul și un card de tahograf după confirmarea autenticității cipului și până la sfârșitul sesiunii sunt protejate prin mesageria securizată.

CSM_182 Cu excepția situației în care se efectuează citirea de pe un fișier cu condiții de acces SM-R-ENC-MAC-G2 (a se vedea secțiunea 4 din apendicele 2), mesageria securizată este utilizată în modul exclusiv cu autentificare. În acest mod, o sumă de verificare criptografică (cunoscută și sub denumirea de MAC) se adaugă la toate comenzile și răspunsurile pentru a asigura autenticitatea și integritatea mesajului.

CSM_183 În cazul în care se efectuează citirea datelor dintr-un fișier cu condiția de acces SM-R-ENC-MAC-G2, mesageria securizată este utilizată în modul criptare urmată de autentificare, iar apoi, prin intermediul datelor criptate formatate se calculează o MAC pentru a asigura autenticitatea și integritatea.

CSM_184 Mesageria securizată utilizează AES, astfel cum este definită în [AES], cu cheile de sesiune K_{MAC} și K_{ENC} care au fost stabilite în timpul autentificării cipului.

CSM_185 Un întreg nesemnat se utilizează drept contor de secvențe trimise (SSC) pentru a preveni atacurile prin reluare. Mărimea SSC este egală cu mărimea blocului AES, și anume 128 de biți. SSC este în format *MSB-first* (cel mai semnificativ octet la început). Contorul de secvențe trimise începe cu zero (și anume, '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00') atunci când este lansată mesageria securizată. SSC este mărit de fiecare dată înaintea generării unei comenzi sau a unui răspuns APDU, ceea ce înseamnă că, întrucât valoarea de început a SSC într-o sesiune SM este 0, în prima comandă valoarea SSC va fi 1. Valoarea SSC pentru primul răspuns va fi 2.

CSM_186 Pentru criptarea unui mesaj, cheia K_{ENC} este utilizată cu AES în modul de operare cu înlănțuirea blocurilor cifrate (CBC), astfel cum este definit în (ISO 10116), cu un parametru intermediar $m = 1$ și un vector de inițializare SV = E(K_{ENC}, SSC), adică valoarea curentă a contorului de secvențe trimise criptată cu cheia K_{ENC}.

CSM_187 Pentru autentificarea mesajelor, cheia K_{MAC} este utilizată cu AES în modul CMAC, astfel cum este specificat în (SP 800-38B). Lungimea MAC este legată de lungimea cheilor de sesiune AES, astfel cum este specificat în CSM_50. Contorul de secvențe trimise este inclus în MAC prin adăugarea acestuia la începutul datagramei care trebuie autentificată.

10.5.2 *Structura mesageriei securizate*

CSM_188 Mesageria securizată utilizează numai obiectele de date din mesageria securizată [a se vedea (ISO 7816-4)] enumerate în tabelul 5. În orice mesaj, aceste obiecte de date sunt utilizate în ordinea precizată în tabelul menționat mai sus.

Tabelul 5

Obiecte de date ale mesageriei securizate

Denumirea obiectului de date	Etichetă	Prezență obligatorie (M), condițională (C) sau interzisă (F) în	
		Comenzi	Răspunsuri
Valoarea datelor în clar necodificată în BER-TLV	'81'	C	C
Valoarea a datelor în clar codată în BER-TLV, dar care nu include obiecte de date (DO) ale SM	'B3'	C	C
Indicator al conținutului de completare urmat de criptogramă, valoare a datelor în clar necodată în BER-TLV	'87'	C	C
Le protejată	'97'	C	F
Starea de procesare	'99'	F	M
Sumă de verificare criptografică	'8E'	M	M

Notă: Astfel cum este specificat în apendicele 2, cardurile de tahograf pot trata comenzile READ BINARY și UPDATE BINARY cu un octet INS impar ('B1', respectiv 'D7'). Aceste variante de comenzi trebuie să citească și să actualizeze fișiere cu mai mult de 32 768 de octeți. În cazul în care este utilizată o astfel de variantă, un obiect de date cu eticheta 'B3' este utilizat în locul unui obiect cu eticheta '81'. A se vedea apendicele 2 pentru mai multe informații.

CSM_189 Toate obiectele de date ale SM sunt codificate în DER TLV, astfel cum este specificat în (ISO 8825-1). Rezultatele codificării într-o structură de tip „valoarea lungimii etichetei" (TLV) sunt după cum urmează:

Etichetă: Eticheta este codificată în unul sau doi octeți și indică conținutul.

Lungime: Lungimea este codificată ca un întreg nesemnat în unul, doi sau trei octeți, ducând la o lungime maximă de 65 535 de octeți. Se utilizează numărul minim de octeți.

Valoare: Valoarea este codificată în zero sau mai mulți octeți.

CSM_190 APDU (unitățile de date pentru protocolul de aplicație) care sunt protejate prin mesageria securizată sunt create astfel:

— Antetul comenzii este inclus în calcularea MAC; prin urmare, pentru octetul de clasă CLA este utilizată valoarea '0C'.

— Astfel cum se specifică în apendicele 2, toți octeții INS trebuie să fie pari, cu posibila excepție a octeților impari INS utilizați pentru comenzile READ BINARY și UPDATE BINARY.

— Valoarea curentă a Lc va fi modificată în Lc' după aplicarea mesageriei securizate.

— Câmpul de date constă în obiectele de date ale SM.

— În comanda protejată APDU, noul octet Le se setează la '00'. Dacă este necesar, în câmpul de date este inclus un obiect de date '97' pentru a indica valoarea inițială a Le.

CSM_191 Orice obiect de date care urmează să fie criptat este completat în conformitate cu (ISO 7816-4), utilizând indicatorul '01' al conținutului de completare. Pentru calcularea MAC, fiecare obiect de date din APDU este de asemenea completat separat în conformitate cu (ISO 7816-4).

Notă: Completarea pentru mesageria securizată este efectuată întotdeauna de stratul de mesagerie securizată, nu de algoritmii CMAC sau CBC.

Rezumat și exemple

O comandă APDU cu mesageria securizată aplicată va avea următoarea structură, în funcție de cazul comenzii nesecurizate respective (DO înseamnă obiect de date):

Cazul 1:	CLA INS P1 P2 || Lc' || DO '8E' || Le
Cazul 2:	CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le
Cazul 3 (octet INS par):	CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le
Cazul 3 (octet INS impar):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le
Cazul 4 (octet INS par):	CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le
Cazul 4 (octet INS impar):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

unde Le = '00' sau '00 00', aceasta depinzând de lungimea câmpurilor utilizate, și anume câmpuri de lungime scurtă sau câmpuri de lungime extinsă; a se vedea (ISO 7816-4).

Un răspuns APDU cu mesageria securizată aplicată va avea următoarea structură, în funcție de cazul răspunsului nesecurizat respectiv:

Cazul 1 sau 3:	DO '99' || DO '8E' || SW1SW2
Cazul 2 sau 4 (octet INS par) cu criptare:	DO '81' || DO '99' || DO '8E' || SW1SW2
Cazul 2 sau 4 (octet INS par) fără criptare:	DO '87' || DO '99' || DO '8E' || SW1SW2
Cazul 2 sau 4 (octet INS impar) fără criptare:	DO 'B3' || DO '99' || DO '8E' || SW1SW2

Notă: Cazul 2 sau 4 (octet INS impar) cu criptare nu este niciodată utilizat în comunicarea dintre o VU și un card.

Mai jos sunt prezentate trei exemple de transformări APDU pentru comenzi cu cod INS par. În figura 8 este prezentată o comandă APDU autentificată din cazul 4, în figura 9 este prezentat un răspuns APDU autentificat din cazul 2/cazul 4, iar în figura 10 este prezentat un răspuns APDU criptat și autentificat din cazul 2/cazul 4.

Figura 8

Transformarea unei comenzi APDU autentificate din cazul 4

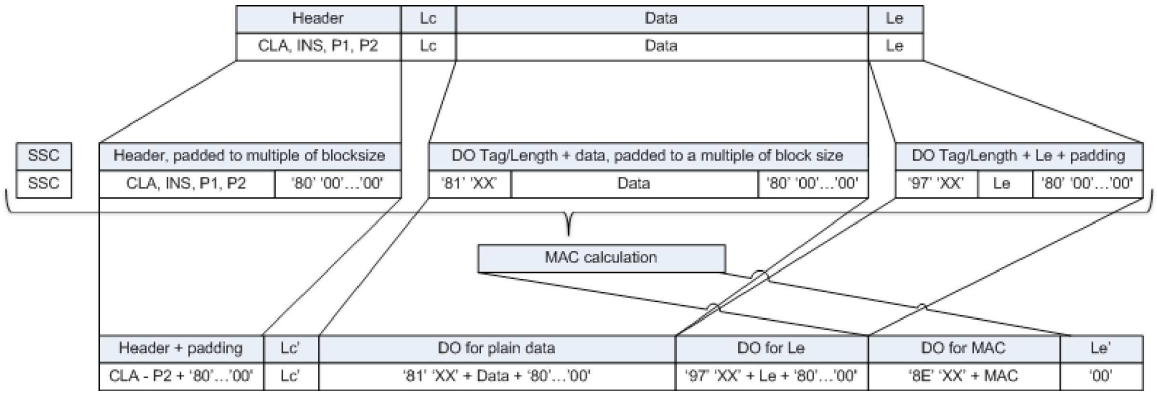


Figura 9

Transformarea unui răspuns APDU autentificat din cazul 1/cazul 3

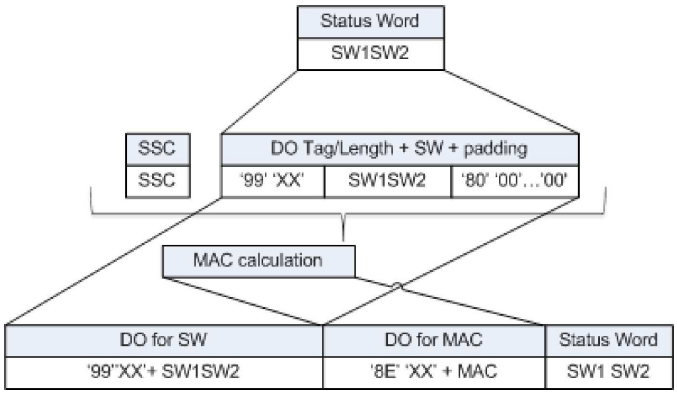
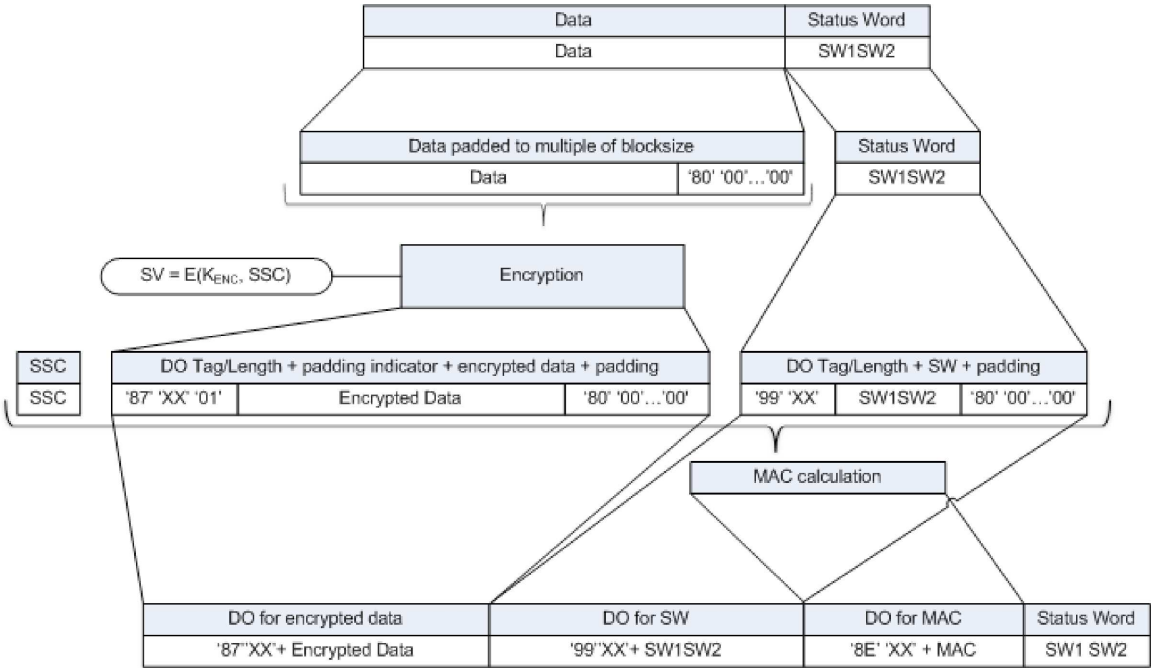


Figura 10

Transformarea unui răspuns APDU criptat și autentificat din cazul 2/cazul 4



10.5.3 *Abandonarea sesiunii de mesagerie securizată*

CSM_192 O unitate montată pe vehicul abandonează o sesiune de mesagerie securizată în curs de desfășurare dacă și numai dacă are loc unul dintre următoarele evenimente:

— unitatea primește un răspuns simplu APDU,

— unitatea detectează o eroare a mesageriei securizate într-un răspuns APDU:

— un obiect de date preconizat lipsește din mesageria securizată, ordinea obiectelor de date este incorectă sau este inclus un obiect de date necunoscut.

— Un obiect de date din mesageria securizată este incorect, de exemplu valoarea MAC este incorectă, structura TLV este incorectă sau indicatorul de completare din eticheta '87' nu este egal cu '01'.

— cardul trimite un octet de stare care indică faptul că acesta a detectat o eroare SM (a se vedea CSM_194),

— a fost atinsă limita numărului de comenzi și de răspunsuri aferente din sesiunea curentă. Pentru o anumită VU, această limită este definită de producătorul său, luând în considerare cerințele de securitate ale hardware-ului utilizat, cu o valoare maximă de 240 de comenzi și de răspunsuri aferente SM pe sesiune.

CSM_193 Un card de tahograf abandonează o sesiune de mesagerie securizată în curs de desfășurare dacă și numai dacă are loc unul dintre următoarele evenimente:

— cardul primește un răspuns simplu APDU,

— cardul detectează o eroare a mesageriei securizate într-o comandă APDU:

— un obiect de date preconizat lipsește din mesageria securizată, ordinea obiectelor de date este incorectă sau este inclus un obiect de date necunoscut.

— Un obiect de date din mesageria securizată este incorect, de exemplu valoarea MAC este incorectă sau structura TLV este incorectă.

— cardul este deconectat de la alimentarea cu energie electrică sau este resetat,

— VU selectează o aplicație pe card,

— VU începe procesul de autentificare al VU,

— a fost atinsă limita numărului de comenzi și de răspunsuri aferente din sesiunea curentă. Pentru un anumit card, această limită este definită de producătorul său, luând în considerare cerințele de securitate ale hardware-ului utilizat, cu o valoare maximă de 240 de comenzi și de răspunsuri aferente SM pe sesiune.

CSM_194 În ceea ce privește gestionarea erorilor SM de către cardul de tahograf:

— În cazul în care într-o comandă APDU lipsesc anumite obiecte de date preconizate ale mesageriei securizate, ordinea obiectelor de date este incorectă sau sunt incluse obiecte de date necunoscute, cardul de tahograf răspunde cu octeții de stare '69 87'.

— În cazul în care un obiect de date din mesageria securizată într-o comandă APDU este incorect, un card de tahograf răspunde cu octeții de stare '69 88'.

Într-un astfel de caz, octeții de stare sunt returnați fără utilizarea SM.

CSM_195 Dacă o sesiune de mesagerie securizată între o VU și un card de tahograf este abandonată, VU și cardul de tahograf

— distrug în mod securizat cheile de sesiune stocate

— stabilesc imediat o nouă sesiune de mesagerie securizată, astfel cum este descris în secțiunile 10.2 – 10.5.

CSM_196 În cazul în care, din orice motiv, VU decide să reînceapă procedura de autentificare reciprocă în raport cu un card introdus, procesul se reia cu verificarea lanțului de certificate de card, astfel cum este descris în secțiunea 10.2, și continuă astfel cum este descris în secțiunile 10.2 – 10.5.

11. CUPLAREA, AUTENTIFICAREA RECIPROCĂ ȘI MESAGERIA SECURIZATĂ ÎNTRE VU ȘI ECHIPAMENTUL GNSS EXTERN

11.1. **Considerații generale**

CSM_197 Echipamentul GNSS utilizat de o VU pentru a-și determina poziția poate fi intern (adică poate fi montat în interiorul carcasei VU, fără a fi detașabil) sau poate fi un modul extern. În primul caz, nu este necesar să se standardizeze comunicarea internă dintre echipamentul GNSS și VU, iar cerințele din prezentul capitol nu se aplică. În al doilea caz, comunicarea dintre VU și echipamentul GNSS extern este standardizată și protejată astfel cum este descris în prezentul capitol.

CSM_198 Comunicarea securizată între o unitate montată pe vehicul și un echipament GNSS extern are loc în același mod ca o comunicare securizată între o unitate montată pe vehicul și un card de tahograf, echipamentul GNSS extern (EGF) având rolul cardului. Un EGF îndeplinește toate cerințele menționate în capitolul 10 referitoare la cardurile de tahograf, ținând seama de deviațiile, clarificările și adăugirile menționate în prezentul capitol. În special, verificarea reciprocă a lanțurilor de certificate, autentificarea VU și autentificarea cipurilor sunt efectuate astfel cum este descris în secțiunile 11.3 și 11.4.

CSM_199 Comunicarea dintre o unitate montată pe vehicul și un EGF este diferită față de comunicarea dintre o unitate montată pe vehicul și un card prin faptul că o unitate montată pe vehicul și un EGF trebuie să fie cuplate mai întâi într-un atelier pentru a putea schimba ulterior date bazate pe GNSS în timpul funcționării normale. Procesul de cuplare este descris în secțiunea 11.2.

CSM_200 Pentru comunicarea dintre o unitate montată pe vehicul și un EGF se utilizează comenzile și răspunsurile bazate pe (ISO 7816-4) și (ISO 7816-8). Structura precisă a acestor APDU este definită în apendicele 2 la prezenta anexă.

11.2. **Cuplarea dintre VU și echipamentul GNSS extern**

CSM_201 O unitate montată pe vehicul și un EGF sunt cuplate de un atelier. În timpul funcționării normale, numai o unitate montată pe vehicul și un EGF cuplate vor putea comunica între ele.

CSM_202 Cuplarea unei unități montate pe vehicul cu un EGF este posibilă numai dacă unitatea montată pe vehicul este în modul etalonare. Cuplarea este inițiată de unitatea montată pe vehicul.

CSM_203 Un atelier poate recupla o unitate montată pe vehicul la un alt EGF sau la același EGF în orice moment. În timpul recuplării, VU distruge în mod securizat certificatul EGF_MA existent din memoria sa și stochează certificatul EGF_MA al EGF la care este în curs de a fi cuplată.

CSM_204 Un atelier poate recupla un echipament GNSS extern la o altă VU sau la aceeași VU în orice moment. În timpul recuplării, EGF distruge în mod securizat certificatul VU_MA existent din memoria sa și stochează certificatul VU_MA al VU la care este în curs de a fi cuplat.

11.3. **Verificarea reciprocă a lanțului de certificate**

11.3.1 *Considerații generale*

CSM_205 Verificarea reciprocă a lanțului de certificate dintre o VU și un EGF are loc în timpul cuplării VU și a EGF de către un atelier. În timpul funcționării normale a unei VU și a unui EGF cuplate între ele, nu este verificat niciun certificat. În locul acestei verificări, VU și EGF au încredere în certificatele pe care le-au stocat în timpul cuplării, după ce au verificat valabilitatea temporală a acestor certificate. VU și EGF nu au încredere în niciun alt certificat pentru protejarea comunicării VU – EGF în timpul funcționării normale.

11.3.2 *În timpul cuplării VU – EGF*

CSM_206 În timpul cuplării la un EGF, o unitate montată pe vehicul utilizează protocolul descris în figura 4 (secțiunea 10.2.1) pentru verificarea lanțului de certificate ale echipamentului GNSS extern.

Note la figura 4 în acest context:

— Controlul comunicărilor este în afara domeniului de aplicare al prezentului apendice. Cu toate acestea, un EGF nu este un card inteligent și, prin urmare, VU nu va trimite, probabil, o comandă de resetare pentru a iniția comunicarea și nici nu va primi un ATR.

— Certificatele și cheile publice ale cardurilor menționate în figură sunt interpretate ca fiind certificatele și cheile publice EGF pentru identificarea reciprocă. Acestea sunt indicate în secțiunea 9.1.6 ca fiind EGF_MA.

— Certificatele Card.CA și cheile publice menționate în figură sunt interpretate ca fiind certificatele și cheile publice MSCA pentru semnarea certificatelor EGF. Acestea sunt indicate în secțiunea 9.1.3 ca fiind MSCA_VU-EGF.

— Certificatul Card.CA.EUR menționat în figură este interpretat ca fiind certificatul rădăcină european precizat în CAR al certificatului MSCA_VU-EGF.

— Certificatul Card.Link menționat în figură este interpretat ca fiind certificatul de legătură al EGF, dacă acesta există. Astfel cum este specificat în secțiunea 9.1.2, acesta este un certificat de legătură pentru o nouă pereche de chei rădăcină europene create de ERCA și semnate de cheia privată europeană anterioară.

— Certificatul Card.Link.EUR este certificatul rădăcină european precizat în CAR al certificatului Card.Link.

— În loc de a citi `cardExtendedSerialNumber`, VU citește `sensorGNSSserialNumber` din EF ICC.

— În loc de a selecta AID al tahografului, VU selectează AID al EGF.

— „Ignore Card" se interpretează ca „Ignore EGF".

CSM_207 După ce a verificat certificatul EGF_MA, unitatea montată pe vehicul stochează acest certificat pentru utilizarea sa în timpul funcționării normale; a se vedea secțiunea 11.3.3.

CSM_208 În timpul cuplării la o VU, un echipament GNSS extern utilizează protocolul descris în figura 5 (secțiunea 10.2.2) pentru verificarea lanțului de certificate ale VU.

Note la figura 5 în acest context:

— VU generează o nouă pereche de chei efemere utilizând parametrii de domeniu din certificatul EGF.

— Certificatele și cheile publice ale VU menționate în figură sunt cele utilizate pentru autentificarea reciprocă. Acestea sunt indicate în secțiunea 9.1.4 ca fiind VU_MA.

— Certificatele și cheile publice VU.CA menționate în figură sunt cele utilizate pentru semnarea certificatelor VU și ale echipamentului GNSS extern. Acestea sunt indicate în secțiunea 9.1.3 ca fiind MSCA_VU-EGF.

— Certificatul VU.CA.EUR menționat în figură este certificatul rădăcină european precizat în CAR al certificatului VU.CA.

— Certificatul VU.Link menționat în figură este certificatul de legătură al VU, dacă acesta există. Astfel cum este specificat în secțiunea 9.1.2, acesta este un certificat de legătură pentru o nouă pereche de chei rădăcină europene create de ERCA și semnate de cheia privată europeană anterioară.

— Certificatul VU.Link.EUR este certificatul rădăcină european precizat în CAR al certificatului VU.Link.

CSM_209 Ca o excepție de la cerința CSM_167, un EGF utilizează ora indicată de GNSS pentru a verifica valabilitatea temporală a oricărui certificat prezentat.

CSM_210 După ce a verificat certificatul VU_MA, unitatea GNSS externă stochează acest certificat pentru a-l utiliza în timpul funcționării normale; a se vedea secțiunea 11.3.3.

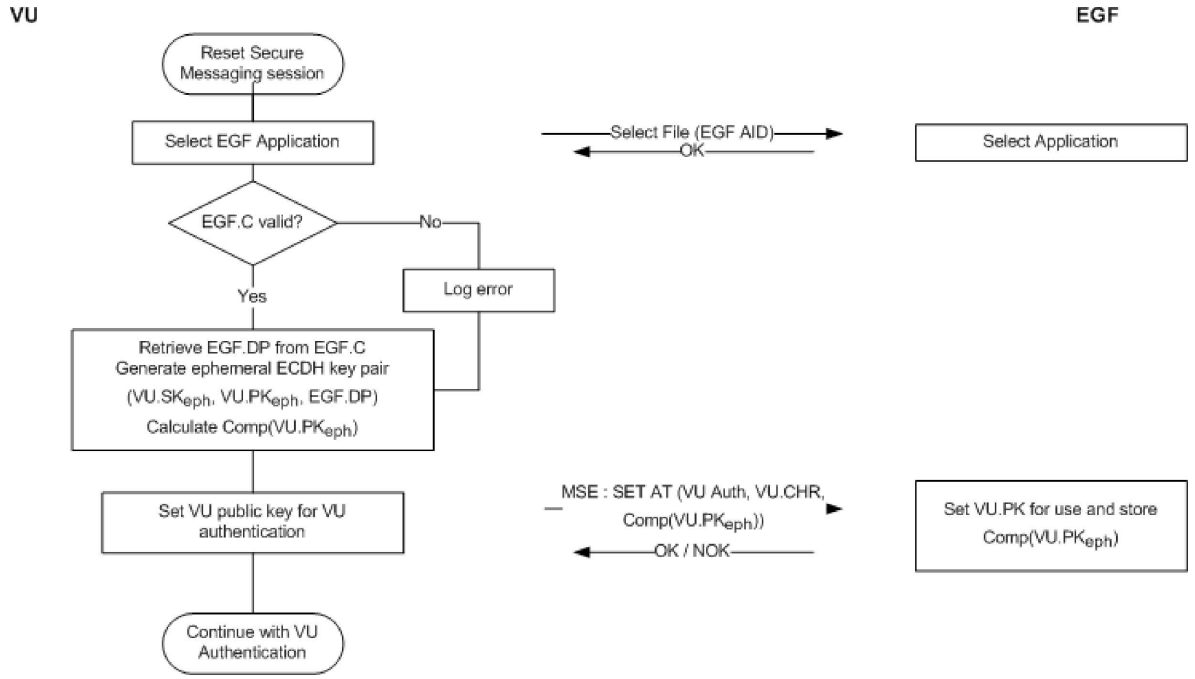
11.3.3 *În timpul funcționării normale*

CSM_211 În timpul funcționării normale, o unitate montată pe vehicul și un EGF utilizează protocolul descris în figura 11 pentru a verifica valabilitatea temporală a certificatelor stocate EGF_MA și VU_MA și pentru a configura cheia publică VU_MA în scopul autentificării ulterioare a VU. Nicio altă verificare reciprocă a lanțurilor de certificate nu este efectuată în timpul funcționării normale.

A se remarca faptul că figura 11 este compusă în esență din primele etape prezentate în figura 4 și în figura 5. A se remarca încă o dată faptul că, întrucât EGF nu este un card inteligent, VU nu va trimite, probabil, o comandă de resetare pentru a iniția comunicarea și nici nu va primi un ATR. În orice caz, acest aspect este în afara domeniului de aplicare al prezentului apendice.

Figura 11

Verificarea reciprocă a valabilității temporale a certificatului în timpul funcționării normale VU – EGF



CSM_212 Astfel cum reiese din figura 11, unitatea montată pe vehicul înregistrează o eroare în cazul în care certificatul EGF_MA nu mai este valabil. Cu toate acestea, autentificarea reciprocă, înțelegerea asupra cheilor și comunicarea ulterioară prin mesageria securizată continuă în mod normal.

11.4. Autentificarea VU, autentificarea cipului și înțelegerea asupra cheilor de sesiune

CSM_213 Autentificarea VU, autentificarea cipului și înțelegerea asupra cheilor de sesiune între o VU și un EGF sunt efectuate în timpul cuplării și ori de câte ori este restabilită o sesiune de mesagerie securizată în timpul funcționării normale. VU și EGF efectuează procesele descrise în secțiunile 10.3 și 10.4. Se aplică toate cerințele din aceste secțiuni.

11.5. Mesageria securizată

CSM_214 Toate comenzile și toate răspunsurile schimbate între o unitate montată pe vehicul și un echipament GNSS extern după confirmarea autenticității cipului și până la sfârșitul sesiunii sunt protejate prin mesageria securizată în modul exclusiv cu autentificare. Se aplică toate cerințele din secțiunea 10.5.

CSM_215 Dacă o sesiune de mesagerie securizată dintre o VU și un EGF este abandonată, VU trebuie să stabilească imediat o nouă sesiune de mesagerie securizată, astfel cum este descris în secțiunile 11.3.3 și 11.4.

12. ASOCIEREA ȘI COMUNICAREA DINTRE O VU ȘI UN SENZOR DE MIȘCARE

12.1. **Considerații generale**

CSM_216 O unitate montată pe vehicul comunică cu un senzor de mișcare utilizând protocolul de interfață specificat în (ISO 16844-3) în timpul asocierii și al funcționării normale, cu schimbările descrise în prezentul capitol și în secțiunea 9.2.1.

Notă: se presupune că cititorii prezentului capitol sunt familiarizați cu conținutul standardului (ISO 16844-3).

12.2. **Asocierea VU – senzor de mișcare folosind generații diferite de chei**

Astfel cum s-a explicat în secțiunea 9.2.1, cheia master a senzorului de mișcare și toate cheile asociate sunt înlocuite în mod periodic. Acest fapt duce la prezența în cardurile de atelier a până la trei chei K_{M-WC} AES legate de senzorul de mișcare (din generații consecutive de chei). În mod similar, în senzorii de mișcare pot fi prezente până la trei criptări diferite de date bazate pe AES (care au la bază generații consecutive ale cheii master K_M a senzorului de mișcare). O unitate montată pe vehicul conține o singură cheie K_{M-VU} legată de senzorul de mișcare.

CSM_217 O VU din a doua generație și un senzor de mișcare din a doua generație sunt asociate după cum urmează [a se compara cu tabelul 6 din (ISO 16844-3)]:

1. Un card de atelier din a doua generație este introdus în VU, iar VU este conectat la senzorul de mișcare.

2. VU citește toate cheile K_{M-WC} disponibile din cardul de atelier, inspectează numerele de versiune ale acestora și alege cheia al cărei număr de versiune corespunde numărului de versiune al cheii K_{M-VU} a VU. În cazul în care cheia K_{M-WC} corespunzătoare nu este prezentă pe cardul de atelier, VU abandonează procesul de asociere și afișează un mesaj adecvat de eroare pentru titularul cardului de atelier.

3. VU calculează cheia master K_M a senzorului de mișcare pe baza cheilor K_{M-VU} și K_{M-WC}, precum și cheia de identificare K_{ID} pe baza cheii K_M, astfel cum este specificat în secțiunea 9.2.1.

4. VU trimite instrucțiunea pentru a iniția procesul de asociere în raport cu senzorul de mișcare, astfel cum este descris în (ISO 16844-3), și criptează numărul de serie pe care îl primește de la senzorul de mișcare cu cheia de identificare K_{ID}. VU trimite înapoi senzorului de mișcare numărul de serie criptat.

5. Senzorul de mișcare compară consecutiv numărul de serie criptat cu fiecare dintre criptările numărului de serie pe care îl conține intern. În cazul în care găsește o corespondență, VU este autentificată. Senzorul de mișcare notează generația cheii K_{ID} utilizate de VU și returnează versiunea criptată corespondentă a cheii sale de asociere, și anume criptarea care a fost creată folosind aceeași generație a K_M.

6. VU decriptează cheia de asociere utilizând K_M, generează o cheie de sesiune K_S, o criptează cu cheia de asociere și trimite rezultatul senzorului de mișcare. Senzorul de mișcare decriptează K_S.

7. VU reunește informațiile de asociere astfel cum sunt definite în (ISO 16844-3), criptează informațiile cu cheia de asociere și trimite rezultatul senzorului de mișcare. Senzorul de mișcare decriptează informațiile de asociere.

8. Senzorul de mișcare criptează informațiile de asociere primite, cu ajutorul cheii K_S, și le transmite înapoi către VU. VU verifică dacă informațiile de asociere sunt identice cu informațiile pe care VU le-a trimis senzorului de mișcare în etapa anterioară. Dacă acest lucru se confirmă, înseamnă că senzorul de mișcare a utilizat aceeași cheie K_S ca VU și, prin urmare, în etapa 5, acesta și-a trimis cheia de asociere criptată cu generația corectă a cheii K_M. În consecință, senzorul de mișcare este autentificat.

A se nota faptul că etapele 2 și 5 sunt diferite față de procesul standard din (ISO 16844-3); celelalte etape sunt standard.

Exemplu: Să presupunem că are loc o asociere în primul an de valabilitate a certificatului ERCA (3); a se vedea figura 2 din secțiunea 9.2.1.2. În plus,

— să presupunem că senzorul de mișcare a fost produs în ultimul an de valabilitate a certificatului ERCA (1). Prin urmare, aceasta va conține următoarele chei și date:

  — $N_s[1]$: numărul de serie criptat cu generația 1 a K_{ID},

  — $N_s[2]$: numărul său de serie criptat cu generația 2 a K_{ID},

  — $N_s[3]$: numărul său de serie criptat cu generația 3 a K_{ID},

  — $K_P[1]$: generația 1 a cheii sale de asociere ([1]), criptată cu generația 1 a cheii K_M,

  — $K_P[2]$: generația 2 a cheii sale de asociere, criptată cu generația 2 a cheii K_M,

  — $K_P[3]$: generația 3 a cheii sale de asociere, criptată cu generația 3 a cheii K_M,

— Să presupunem că livrarea cardului de atelier a fost efectuată în ultimul an de valabilitate a certificatului ERCA (3). Acesta va conține, prin urmare, generația 2 și generația 3 ale cheii $K_{M\text{-}WC}$.

— Să presupunem că VU este din generația 2 de VU, conținând generația 2 a cheii $K_{M\text{-}VU}$.

În acest caz, în etapele 2-5 vor avea loc următoarele evenimente:

— Etapa 2: VU citește generația 2 și generația 3 ale cheii $K_{M\text{-}WC}$ din cardul de atelier și inspectează numerele de versiune ale acestora.

— Etapa 3: VU combină generația 2 a cheii $K_{M\text{-}WC}$ cu cheia sa $K_{M\text{-}VU}$ pentru a calcula K_M și K_{ID}.

— Etapa 4: VU criptează numărul de serie pe care îl primește de la senzorul de mișcare cu cheia K_{ID}.

— Etapa 5: Senzorul de mișcare compară datele primite cu $N_s[1]$ și nu găsește nicio corespondență. Apoi, acesta compară datele cu $N_s[2]$ și găsește o corespondență. Senzorul de mișcare trage concluzia că VU este din generația 2 de VU și, prin urmare, trimite înapoi $K_P[2]$.

12.3. **Comunicarea și asocierea dintre o VU și un senzor de mișcare folosind AES**

CSM_218 Astfel cum este precizat în tabelul 3 din secțiunea 9.2.1, toate cheile implicate în asocierea unei unități (de a doua generație) montate pe vehicul și a unui senzor de mișcare, precum și în comunicarea lor ulterioară, sunt mai curând chei AES decât chei de lungime dublă TDES, astfel cum este specificat în (ISO 16844-3). Aceste chei AES pot avea o lungime de 128, 192 sau 256 de biți. Întrucât mărimea blocurilor AES este de 16 octeți, lungimea unui mesaj criptat trebuie să fie un multiplu de 16 octeți, în comparație cu lungimea de 8 octeți din cazul TDES. În plus, unele dintre aceste mesaje vor fi utilizate pentru a transporta chei AES, a căror lungime poate fi de 128, 192 sau 256 de biți. Prin urmare, numărul de octeți de date per instrucțiune în tabelul 5 din (ISO 16844-3) se modifică după cum este indicat în tabelul 6:

Tabelul 6

Numărul de octeți de date cu text simplu și criptate per instrucțiune definit în (ISO 16844-3)

Instrucțiune	Solicitare/răspuns	Descrierea datelor	Nr. de octeți de date cu text simplu în conformitate cu (ISO 16844-3)	Nr. de octeți de date cu text simplu folosind chei AES	Nr. de octeți de date criptate folosind chei AES cu lungimea de (în biți):		
					128	192	256
10	solicitare	Datele de autentificare + numărul fișierului	8	8	16	16	16

([1]) A se nota faptul că generația 1, generația 2 și generația 3 de chei de asociere pot reprezenta de fapt aceeași cheie sau pot fi trei chei diferite cu lungimi diferite, astfel cum este explicat în CSM_117.

Instrucțiune	Solicitare/ răspuns	Descrierea datelor	Nr. de octeți de date cu text simplu în conformitate cu (ISO 16844-3)	Nr. de octeți de date cu text simplu folosind chei AES	Nr. de octeți de date criptate folosind chei AES cu lungimea de (în biți):		
					128	192	256
11	răspuns	Datele de autentificare + conținuturile fișierelor	16 sau 32, depinde de fișier	16 sau 32, depinde de fișier	16/32	16/32	16/32
41	solicitare	Numărul de serie al MoS (senzorul de mișcare)	8	8	16	16	16
41	răspuns	Cheie de asociere	16	16/24/32	16	32	32
42	solicitare	Cheie de sesiune	16	16/24/32	16	32	32
43	solicitare	Informații de asociere	24	24	32	32	32
50	răspuns	Informații de asociere	24	24	32	32	32
70	solicitare	Date de autentificare	8	8	16	16	16
80	răspuns	Valoarea contorului MoS + date de autentificare	8	8	16	16	16

CSM_219 Informațiile de asociere trimise în instrucțiunile 43 (solicitarea VU) și 50 (răspunsul MoS) sunt reunite astfel cum este precizat în secțiunea 7.6.10 din (ISO 16844-3), cu excepția faptului că se utilizează algoritmul AES în locul algoritmului TDES în schema de criptare a datelor de asociere, ceea ce duce, prin urmare, la folosirea a două criptări AES și la adoptarea completării specificate în CSM_220 pentru a corespunde mărimii blocului AES. Cheia K'_P utilizată pentru această criptare este generată în modul următor:

— În cazul în care cheia de asociere K_P are o lungime de 16 octeți: $K'_P = K_P \text{ XOR } (N_s||N_s)$

— În cazul în care cheia de asociere K_P are o lungime de 24 de octeți: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s)$

— În cazul în care cheia de asociere K_P are o lungime de 32 de octeți: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s||N_s)$

unde N_s este numărul de serie de 8 octeți al senzorului de mișcare.

CSM_220 În cazul în care lungimea datelor de text simplu (utilizând chei AES) nu este un multiplu de 16 octeți, se folosește metoda 2 de completare definită în (ISO 9797-1).

Notă: în (ISO 16844-3), numărul de octeți de date cu text simplu este întotdeauna un multiplu de 8, astfel încât completarea nu este necesară atunci când se folosește TDES. Definiția datelor și mesajelor în ISO (16844-3) nu este modificată prin prezenta parte din prezentul apendice, fiind necesară, prin urmare, aplicarea completării.

CSM_221 Pentru instrucțiunea 11 și în cazul în care trebuie încriptate cel puțin două blocuri de date, se utilizează modul de funcționare cu înlănțuirea blocurilor cifrate, astfel cum se precizează în (ISO 10116), cu un parametru intermediar $m = 1$. Vectorul de inițializare (IV) care trebuie utilizat este:

— Pentru instrucțiunea 11: blocul de autentificare de 8 octeți specificat în secțiunea 7.6.3.3. din (ISO 16844-3), completat utilizând metoda de completare 2 definită în (ISO 9797-1); a se vedea, de asemenea, secțiunile 7.6.5 și 7.6.6 din ISO (16844-3).

— Pentru toate celelalte secțiuni în care sunt transferați mai mult de 16 octeți, astfel cum este precizat în tabelul 6: '00' {16}, adică șaisprezece octeți cu valoarea binară 0.

Notă: Așa cum se arată în secțiunile 7.6.5 și 7.6.6 din (ISO 16844-3), atunci când MoS criptează fișierele de date pentru a fi incluse în instrucțiunea 11, blocul de autentificare este

— atât utilizat ca vector de inițializare pentru modul CBC de criptare a fișierelor de date,

— cât și criptat și inclus ca prim bloc în datele trimise către VU.

12.4. **Asocierea VU – senzor de mișcare pentru echipamente de diferite generații**

CSM_222 Astfel cum s-a explicat în secțiunea 9.2.1, un senzor de mișcare din a doua generație poate conține criptarea bazată pe TDES a datelor de asociere (astfel cum este definit în partea A a prezentului apendice), ceea ce permite asocierea senzorului de mișcare cu o VU de prima generație. În acest caz, o VU de prima generație și un senzor de mișcare de a doua generație sunt asociați conform descrierii din partea A a prezentului apendice și din (ISO 16844-3). Pentru procesul de asociere poate fi folosit un card de atelier de prima generație sau de a doua generație.

Note:

— Nu este posibilă asocierea unei VU de a doua generație cu un senzor de mișcare de prima generație.

— Nu este posibilă utilizarea unui card de atelier de prima generație pentru a cupla o VU de a doua generație la un senzor de mișcare.

13. SECURITATEA COMUNICĂRII LA DISTANȚĂ PRIN DSRC

13.1. **Considerații generale**

Astfel cum se specifică în apendicele 14, o VU generează periodic date de monitorizare de la distanță a tahografelor (RTM) și trimite aceste date echipamentului (intern sau extern) de comunicare la distanță (RCF). Echipamentul de monitorizare la distanță este responsabil pentru trimiterea datelor, prin interfața DSRC descrisă în apendicele 14, către echipamentul de interogare la distanță. În apendicele 1 se precizează că datele RTM sunt concatenarea următoarelor elemente:

Datele utile criptate ale tahografului criptarea datelor utile cu text simplu ale tahografului

Datele de securitate DSRC descrise mai jos

Formatul datelor utile cu text simplu ale tahografului este precizat în apendicele 1 și descris în detaliu în apendicele 14. În această secțiune este descrisă structura datelor de securitate DSRC; specificația formală este descrisă în apendicele 1.

CSM_223 Datele cu text în clar `tachographPayload` comunicate de o VU unui echipament de comunicare la distanță (dacă RCF este instalat în afara VU) sau de la VU către un echipament de interogare la distanță prin intermediul interfeței DSRC (dacă RCF este instalat în interiorul VU) sunt protejate în modul criptare urmată de autentificare, ceea ce înseamnă că mai întâi se criptează datele utile ale tahografului pentru a asigura confidențialitatea mesajului, iar apoi se calculează un MAC pentru a asigura autenticitatea și integritatea datelor.

CSM_224 Datele de securitate DSRC constau în concatenarea elementelor de date de mai jos, în următoarea ordine; a se vedea, de asemenea figura 12:

Data și ora curente	data și ora curente ale VU (tip de date `TimeReal`)
Contor	un contor de 3 octeți, a se vedea CSM_225

Numărul de serie al VU	numărul de serie al VU (tip de date `VuSerialNumber`)
Numărul de versiune al cheii master DSRC	numărul de versiune de 1 octet al cheii master DSRC din care au fost derivate cheile DSRC specifice pentru VU (a se vedea secțiunea 9.2.2).
MAC	MAC calculat prin intermediul tuturor octeților anteriori din datele RTM.

CSM_225 Contorul de 3 octeți din datele de securitate DSRC sunt în formatul MSB (cel mai semnificativ octet) la început. Prima dată când o VU calculează un set de date RTM după ce este pusă în producție, aceasta reglează valoarea contorului la 0. De fiecare dată înainte de a calcula următorul set de date RTM, VU mărește cu 1 valoarea datelor contorului.

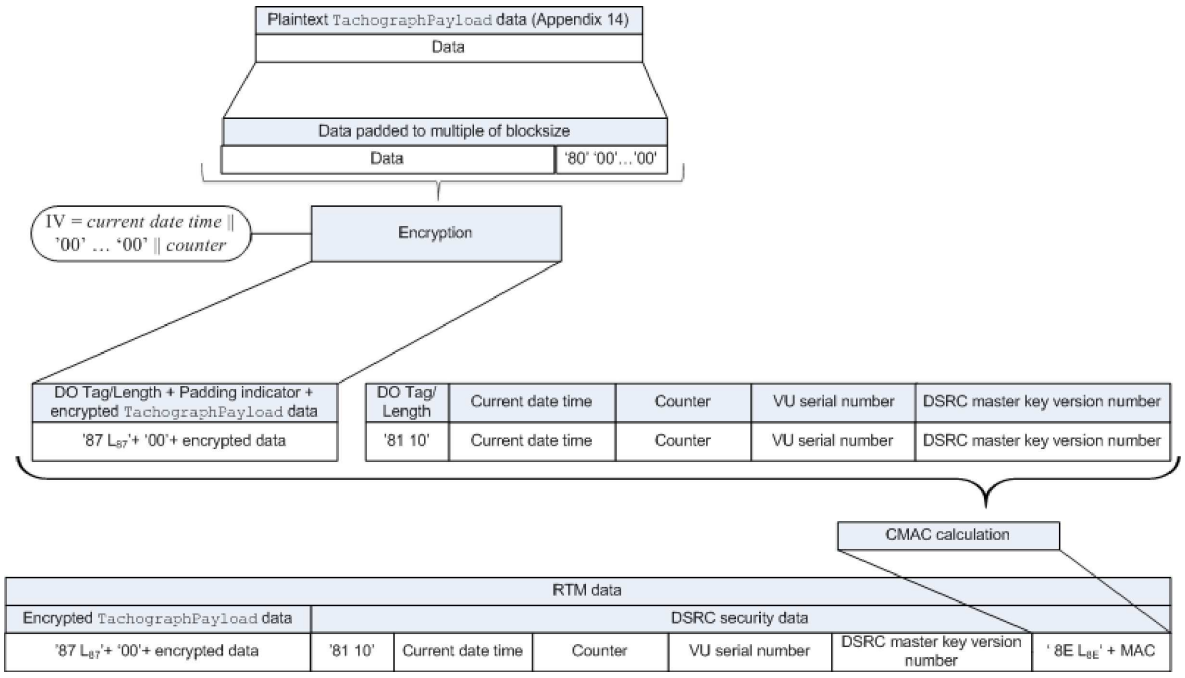
13.2. Criptarea datelor utile ale tahografului și generarea MAC

CSM_226 Fiind dat un element de date cu text simplu având tipul de date `TachographPayload` astfel cum este descris în apendicele 14, o VU criptează aceste date după cum este indicat în figura 12: Cheia DSRC a VU folosită pentru criptare, $K_VU_{DSRC}_ENC$ (a se vedea secțiunea 9.2.2), este utilizată cu AES în modul de funcționare cu înlănțuirea blocurilor cifrate, astfel cum este definit în (ISO 10116), cu un parametru intermediar m = 1. Vectorul de inițializare este: IV = *data și ora curentă* || '*00 00 00 00 00 00 00 00*' || *contor,* unde *data și ora curentă* și *contorul* sunt specificate în CSM_224. Datele care trebuie criptate sunt completate folosind metoda 2 definită în (ISO 9797-1)

CSM_227 O VU calculează MAC din datele de securitate DSRC astfel cum este indicat în figura 12: MAC este calculat pe baza tuturor octeților precedenți din datele RTM, până la numărul de versiune al cheii master DSRC (inclusiv acest număr) și incluzând etichetele și lungimile obiectelor de date. VU își utilizează cheia DSRC pentru a verifica autenticitatea $K_VU_{DSRC}_MAC$ (a se vedea secțiunea 9.2.2) cu algoritmul AES în modul CMAC, astfel cum este specificat în (SP 800-38B). Lungimea MAC este legată de lungimea cheilor DSRC specifice pentru VU, astfel cum este specificat în CSM_50.

Figura 12

Criptarea datelor utile ale tahografului și generarea MAC



13.3. **Verificarea și decriptarea datelor utile ale tahografului**

CSM_228 Atunci când un echipament de interogare la distanță primește date RTM de la o VU, acesta trimite toate datele RTM la un card de control în câmpul de date al unei comenzi PROCESS DSRC MESSAGE, astfel cum este descris în apendicele 2. În acest caz:

1. Cardul de control inspectează numărul de versiune al cheii master DSRC din datele de securitate DSRC. În cazul în care cardul de control nu cunoaște cheia master DSRC indicată, acesta trimite înapoi un mesaj de eroare specificat în anexa 2 și abandonează procesul.

2. Cardul de control utilizează cheia master DSRC indicată în combinație cu numărul de serie al VU din datele de securitate DSRC pentru a deriva cheile DSRC specifice pentru VU, și anume K_VU_{DSRC}_ENC și K_VU_{DSRC}_MAC, astfel cum este specificat în CSM_124.

3. Cardul de control utilizează K_VU_{DSRC}_MAC pentru a verifica MAC în datele de securitate DSRC, astfel cum este specificat în CSM_227. Dacă MAC este incorect, cardul de control trimite înapoi un mesaj de eroare specificat în apendicele 2 și abandonează procesul.

4. Cardul de control utilizează K_VU_{DSRC}_ENC pentru a decripta datele utile criptate ale tahografului, astfel cum este specificat în CSM_226. Cardul de control elimină completarea și trimite datele utile decriptate ale tahografului către echipamentul de interogare la distanță.

CSM_229 Pentru a preveni atacurile prin reluare, echipamentul de interogare la distanță verifică dacă datele RTM sunt reînnoite verificând faptul că *data și ora curente* din datele de securitate DSRC nu se abat prea mult de la ora curentă a echipamentului de interogare la distanță.

Note:

— Pentru această verificare este necesar ca echipamentul de interogare la distanță să dispună de o sursă de indicare a orei exactă și fiabilă.

— Întrucât conform cerințelor din apendicele 14, VU trebuie să calculeze un nou set de date RTM la fiecare 60 de secunde, iar ceasul VU poate avea o abatere de 1 minut de la ora reală, o limită mai acceptabilă pentru reînnoirea datelor RTM este de 2 minute. Reînnoirea reală a datelor care trebuie prevăzută depinde, de asemenea, de exactitatea ceasului echipamentului de interogare la distanță.

CSM_230 Atunci când un atelier verifică funcționarea corectă a funcționalității DSRC a unei VU, acesta trimite totalitatea datelor RTM primite de la VU unui card de atelier în câmpul de date al unei comenzi PROCESS DSRC MESSAGE, astfel cum este descris în apendicele 2. Cardul de atelier efectuează toate verificările și acțiunile specificate în CSM_228.

14. SEMNAREA DESCĂRCĂRII DE DATE ȘI VERIFICAREA SEMNĂTURILOR

14.1. **Considerații generale**

CSM_231 Echipamentul inteligent dedicat (IDE) stochează într-un singur fișier fizic de date datele primite de la o VU sau de la un card în timpul unei sesiuni de descărcare. Datele pot fi stocate pe un suport de memorie extern (ESM). Acest fișier conține semnături digitale de blocuri de date, astfel cum este specificat în apendicele 7. Fișierul menționat mai sus conține, de asemenea, următoarele certificate (a se vedea secțiunea 9.1):

— În cazul unei descărcări de pe o VU:

— Certificatul VU_Sign

— Certificatul MSCA_VU-EGF care conține cheia publică destinată utilizării pentru verificarea certificatului VU_Sign

— În cazul unei descărcări de pe un card:

— Certificatul Card_Sign

— Certificatul MSCA_Card care conține cheia publică destinată verificării certificatului Card_Sign

CSM_232 IDE dispune, de asemenea, de:

— În cazul în care acesta utilizează un card de control pentru verificarea semnăturii, astfel cum este indicat în figura 13: Certificatul de legătură care leagă cel mai recent certificat EUR de certificatul EUR a cărui perioadă de valabilitate este imediat anterioară acestui celui mai recent certificat EUR, dacă acesta există.

— În cazul în care verifică chiar el semnătura: toate certificatele rădăcină europene valabile.

Notă: metoda folosită de IDE pentru a obține aceste certificate nu este specificată în prezentul apendice.

14.2. **Generarea semnăturilor**

CSM_233 Algoritmul de semnare utilizat pentru a crea semnături prin intermediul datelor descărcate este ECDSA, astfel cum este precizat în [DSS], folosindu-se algoritmul de *hashing* legat de mărimea cheilor VU sau ale cardului, astfel cum este specificat în CSM_50. Formatul semnăturii este simplu, astfel cum este precizat în (TR-03111).

14.3. **Verificarea semnăturilor**

CSM_234 Un IDE poate efectua verificarea unei semnături pe baza datelor descărcate în mod nemijlocit sau poate utiliza un card de control în acest scop. În cazul în care IDE utilizează un card de control, verificarea semnăturii se efectuează astfel cum este indicat în figura 13. În cazul în care IDE efectuează nemijlocit verificarea semnăturii, acesta verifică autenticitatea și valabilitatea tuturor certificatelor din lanțul de certificate din fișierul de date și verifică semnătura prin intermediul datelor, urmând schema de semnătură definită în [DSS].

Note la figura 13:

— Echipamentul care a semnat datele de analizat este denumit EQT.

— Certificatele EQT și cheile publice menționate în figură sunt cele utilizate pentru semnare, și anume VU_Sign sau Card_Sign.

— Certificatele și cheile publice EQT.CA menționate în figură sunt cele utilizate pentru semnarea certificatelor VU sau a celor de card, după caz.

— Certificatul EQT.CA.EUR menționat în figură este certificatul rădăcină european precizat în CAR al certificatului EQT.CA.

— Certificatul EQT.Link menționat în figură este certificatul de legătură al EQT, dacă acesta există. Astfel cum este specificat în secțiunea 9.1.2, acesta este un certificat de legătură pentru o nouă pereche de chei rădăcină europene create de ERCA și semnate cu cheia privată europeană anterioară.

— Certificatul EQT.Link.EUR este certificatul rădăcină european precizat în CAR al certificatului EQT.Link.

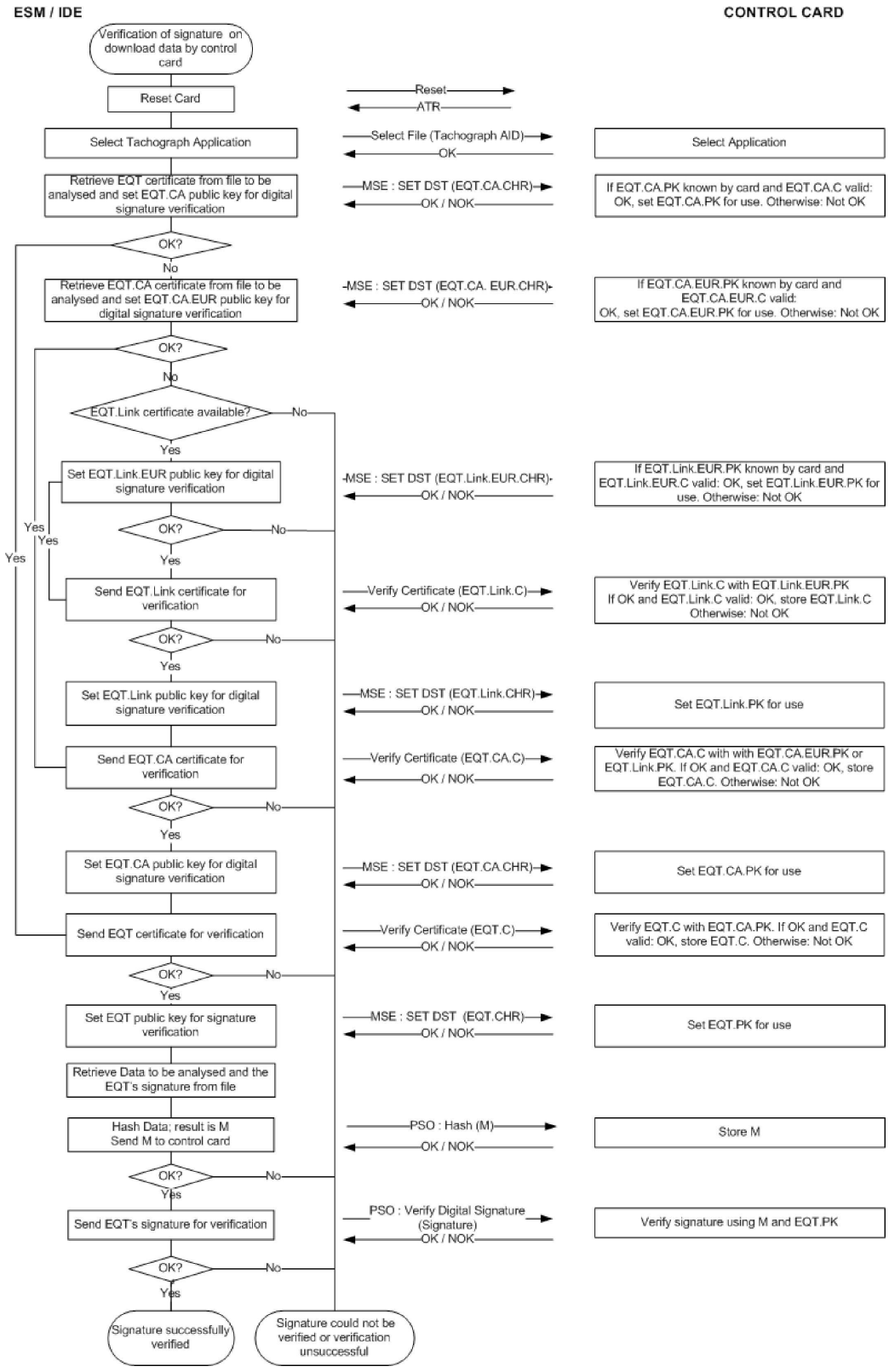
CSM_235 Pentru a calcula funcția *hash* a mesajului M trimis către cardul de control în comanda PSO:Hash, IDE utilizează algoritmul de *hashing* legat de mărimea cheii VU sau a cardului de pe care se descarcă datele, astfel cum este specificat în CSM_50.

CSM_236 Pentru a verifica semnătura EQT, cardul de control trebuie să respecte schema de semnătură definită în [DSS].

Notă: Prezentul document nu precizează nicio acțiune care să fie întreprinsă în cazul în care o semnătură prin intermediul unui fișier de date descărcat nu poate fi verificată sau dacă verificarea are un rezultat negativ.

Figura 13

Protocol pentru verificarea semnăturii prin intermediul unui fișier de date descărcate



Apendicele 12

POZIȚIONAREA BAZATĂ PE SISTEMUL GLOBAL DE NAVIGAȚIE PRIN SATELIT (GNSS)

CUPRINS

1. INTRODUCERE 405

1.1. Domeniu de aplicare 405

1.2. Acronime și notații 405

2. SPECIFICAȚIA RECEPTORULUI GNSS 406

3. PROPOZIȚIILE NMEA 406

4. UNITATE MONTATĂ PE VEHICUL CU UN ECHIPAMENT GNSS EXTERN 408

4.1. Configurație 408

4.1.1 Componente principale și interfețe 408

4.1.2 Starea echipamentului GNSS extern la finalul procesului de producție 408

4.2. Comunicarea între echipamentul GNSS extern și unitatea montată pe vehicul 409

4.2.1 Protocolul de comunicare 409

4.2.2 Transferul securizat de date GNSS 411

4.2.3 Structura comenzii de citire a înregistrării (Read Record) 412

4.3. Cuplarea, autentificarea reciprocă și înțelegerea asupra cheii de sesiune a echipamentului GNSS extern cu unitatea montată pe vehicul 413

4.4. Gestionarea erorilor 413

4.4.1 Eroare de comunicare cu echipamentul GNSS extern 413

4.4.2 Încălcarea integrității fizice a echipamentului GNSS extern 413

4.4.3 Absența informațiilor de poziționare de la receptorul GNSS 413

4.4.4 Certificatul echipamentului GNSS extern a expirat 414

5. UNITATE MONTATĂ PE VEHICUL FĂRĂ UN ECHIPAMENT GNSS EXTERN 414

5.1. Configurație 414

5.2. Gestionarea erorilor 414

5.2.1 Absența informațiilor de poziționare de la receptorul GNSS 414

6. CONFLICT ORĂ GNSS 414

7. CONFLICT PRIVIND DEPLASAREA VEHICULULUI 415

1. INTRODUCERE

Prezentul apendice prevede cerințele tehnice pentru datele GNSS utilizate de unitatea montată pe vehicul, inclusiv protocoalele care trebuie implementate pentru a asigura transferul de date corect și în siguranță al informațiilor de poziționare.

Principalele articole din Regulamentul (UE) nr. 165/2014 care impun aceste cerințe sunt: „Articolul 8 Înregistrarea poziției vehiculului în anumite puncte în timpul zilei de lucru”, „Articolul 10 Interfața cu sistemele de transport inteligente” și „Articolul 11 Dispoziții detaliate pentru tahograful inteligent”.

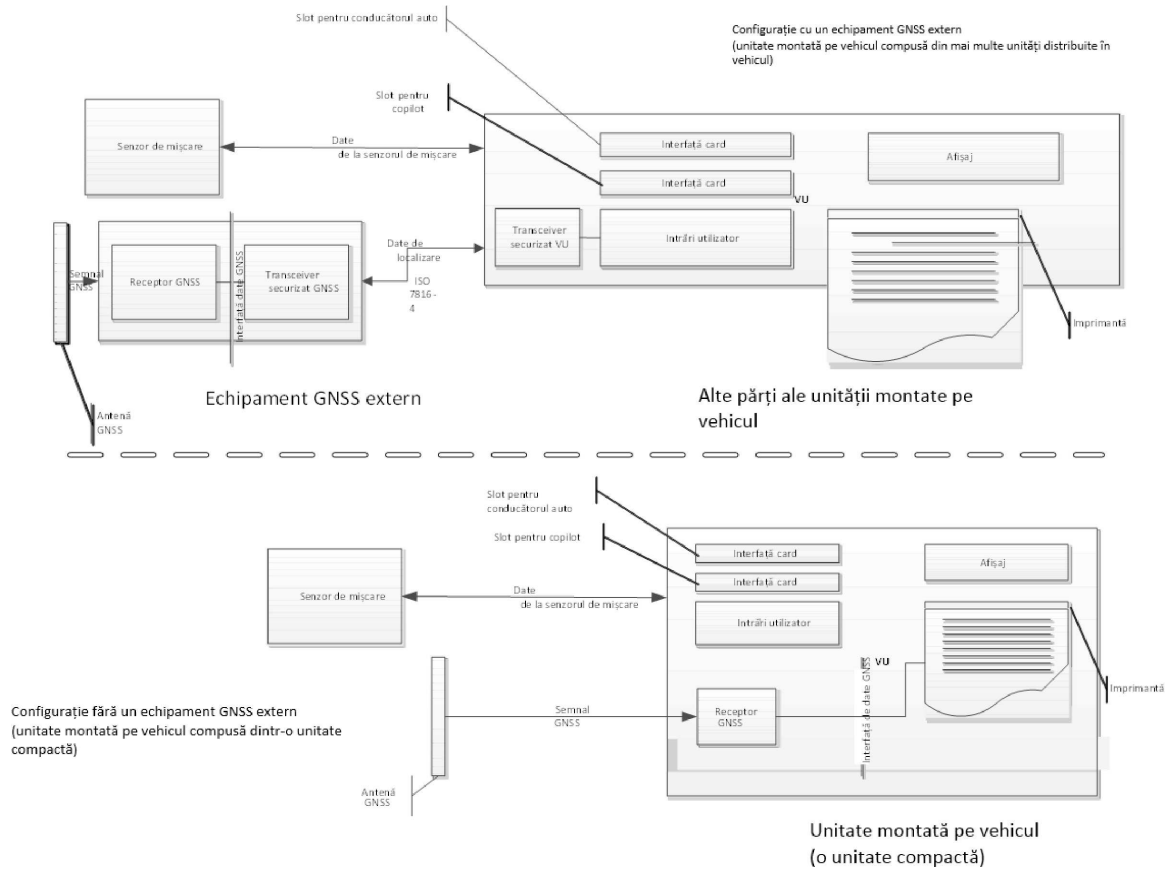
1.1. **Domeniu de aplicare**

GNS_1 Unitatea montată pe vehicul colectează date de localizare cel puțin de la un GNSS pentru a sprijini punerea în aplicare a articolului 8.

Unitatea montată pe vehicul poate fi dotată sau nu cu un echipament GNSS extern, astfel cum este descris în Figura 1:

Figura 1

Diferite configurații pentru receptorul GNSS.



1.2. **Acronime și notații**

În prezentul apendice sunt folosite următoarele acronime:

DOP *Dilution of Precision* (Scădere a preciziei)

EGF Fișier elementar Dispozitiv GNSS (*Elementary file GNSS Facility*)

EGNOS Serviciul european geostaționar mixt de navigare (*European Geostationary Navigation Overlay Service*)

GNSS Sistem global de navigație prin satelit (*Global Navigation Satellite System*)

GSA GPS DOP și sateliți activi

HDOP *Horizontal Dilution of Precision* (Scădere a preciziei în plan orizontal)

ICD Document de control al interfeței

NMEA National Marine Electronics Association

PDOP *Position Dilution of Precision* (Diminuare a preciziei ca urmare a poziționării sateliților)

RMC Recommended Minimum Specific

SIS Semnal în spațiu (*Signal in Space*)

VDOP *Vertical Dilution of Precision* (Scădere a preciziei în plan vertical)

VU Unitate montată pe vehicul (*Vehicle Unit*)

2. SPECIFICAȚIA RECEPTORULUI GNSS

Indiferent de configurația tahografului inteligent, cu sau fără un echipament GNSS extern, furnizarea de informații de poziționare exacte și fiabile reprezintă un element esențial pentru funcționarea eficientă a tahografului inteligent. Prin urmare, este oportun să se solicite compatibilitatea acestuia cu serviciile furnizate de programele Galileo și Serviciul european geostaționar mixt de navigare (EGNOS), astfel cum sunt prevăzute în Regulamentul (UE) nr. 1285/2013 al Parlamentului European și al Consiliului ([1]). Sistemul constituit în cadrul programului Galileo este un sistem global de navigație prin satelit independent, iar cel constituit în cadrul programului EGNOS este un sistem regional de navigație prin satelit, care îmbunătățește calitatea semnalului sistemului de poziționare globală.

GNS_2 Producătorii garantează că receptoarele GNSS din tahografele inteligente sunt compatibile cu serviciile de poziționare furnizate de sistemele Galileo și EGNOS. De asemenea, producătorii pot alege, în plus, compatibilitatea cu alte sisteme de navigație prin satelit.

GNS_3 Receptorul GNSS trebuie să fie compatibil cu autentificarea pe serviciul deschis al Galileo atunci când acest serviciu va fi furnizat de sistemul Galileo și integrat de producătorii de receptoare GNSS. Totuși, pentru tahografele inteligente introduse pe piață înainte de a fi îndeplinite condițiile susmenționate și care nu sunt compatibile cu autentificarea pe serviciul deschis al Galileo, reabilitarea nu va fi obligatorie.

3. PROPOZIȚIILE NMEA

Această secțiune descrie propozițiile NMEA utilizate în funcționarea tahografului inteligent. Această secțiune este valabilă atât pentru configurația tahografului inteligent cu echipament GNSS extern, cât și a celui fără echipament GNSS extern.

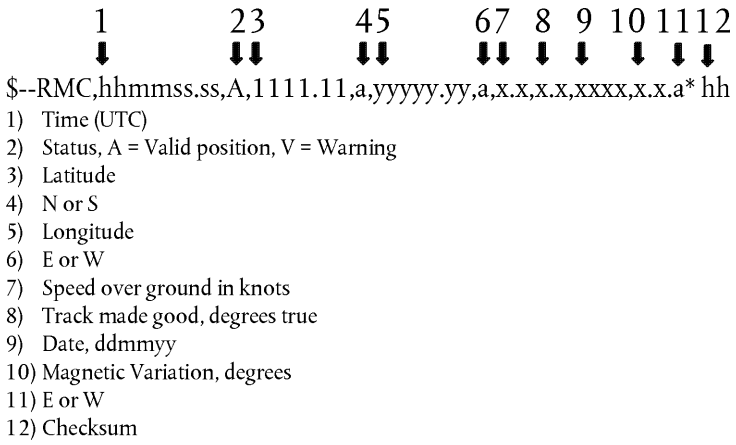
GNS_4 Datele de localizare se bazează pe propoziția NMEA *Recommended Minimum Specific (RMC) GNSS Data*, care conține informații de poziționare (latitudine, longitudine), ora în format UTC (hhmmss.ss), viteza față de sol în noduri plus valori suplimentare.

Formatul propoziției RMC este următorul (conform standardului NMEA V4.1):

([1]) Regulamentul (UE) nr. 1285/2013 al Parlamentului European și al Consiliului din 11 decembrie 2013 privind punerea în aplicare și exploatarea sistemelor europene de radionavigație prin satelit și de abrogare a Regulamentului (CE) nr. 876/2002 al Consiliului și a Regulamentului (CE) nr. 683/2008 al Parlamentului European și al Consiliului (JO L 347, 20.12.2013, p. 1).

Figura 2

Structura propoziției RMC



Statutul (*Status*) indică dacă semnalul GNSS este disponibil. Până când valoarea statutului nu este setată la A, datele primite (de exemplu, referitoare la oră sau latitudine/longitudine) nu pot fi utilizate pentru înregistrarea poziției vehiculului în VU.

Rezoluția poziției se bazează pe formatul propoziției RMC descris mai sus. Prima parte din câmpurile 3) și 5) (primele două cifre) se utilizează pentru a reprezenta gradele. Restul se utilizează pentru a reprezenta minutele cu trei zecimale. Astfel, rezoluția este 1/1000 de minut sau 1/60000 de grad (deoarece un minut este 1/60 dintr-un grad).

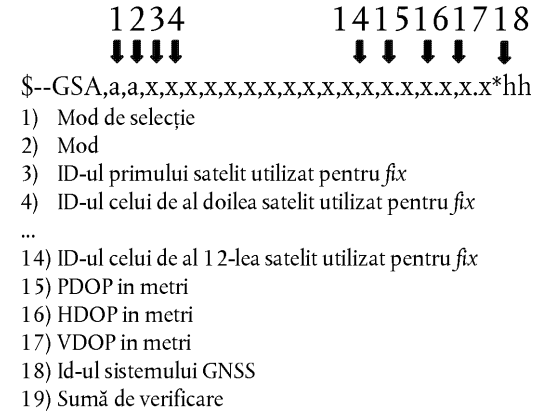
GNS_5 Unitatea montată pe vehicul stochează în baza de date a VU informațiile de poziționare pentru latitudine și longitudine cu o rezoluție de 1/10 de minut sau 1/600 de grad, astfel cum este descris în apendicele 1 pentru tipul GeoCoordinates.

Comanda GPS DOP și sateliți activi (GSA) poate fi utilizată de VU pentru a determina și a înregistra disponibilitatea și precizia semnalului. În special HDOP este utilizată pentru a furniza o indicație cu privire la gradul de precizie a datelor de localizare înregistrate (a se vedea 4.2.2). VU va înregistra valoarea *Horizontal Dilution of Precision* (HDOP), calculată ca cea mai mică dintre valorile HDOP colectate de la sistemele GNSS disponibile.

Id-ul sistemului GNSS indică GPS, Glonass, Galileo, Beidou sau sistem de augmentare cu ajutorul sateliților (*Satellite-Based Augmentation System*, SBAS).

Figura 3

Structura propoziției GSA



Unde modul (2) indică dacă un *fix* nu este disponibil (Mode = 1) sau un *fix* este disponibil pentru 2D (Mode = 2) ori 3D (Mode = 3).

GNS_6 Propoziția *GSA* este stocată cu număr de înregistrare '06'.

GNS_7 Dimensiunea maximă a propozițiilor NMEA (de exemplu, RMC, GSA sau altele), care poate fi utilizată pentru dimensionarea comenzii de citire a înregistrării (*Read Record*) este de 85 de octeți (a se vedea Tabelul 1).

4. UNITATE MONTATĂ PE VEHICUL CU UN ECHIPAMENT GNSS EXTERN

4.1. **Configurație**

4.1.1 *Componente principale și interfețe*

În această configurație, receptorul GNSS face parte din echipamentul GNSS extern.

GNS_8 Echipamentul GNSS extern trebuie să fie alimentat cu o interfață specifică a vehiculului.

GNS_9 Echipamentul GNSS extern constă în următoarele componente (a se vedea Figura 4):

a) Un receptor GNSS comercial care să furnizeze datele de poziționare prin interfața de date GNSS. De exemplu, interfața de date GNSS poate fi standardul NMEA V4.10, unde receptorul GNSS acționează ca un emițător și transmite propoziții NMEA către transceiverul securizat GNSS cu o frecvență de 1 Hz pentru setul predefinit de propoziții NMEA, care trebuie să cuprindă cel puțin propozițiile RMC și GSA. Implementarea interfeței de date GNSS este la alegerea producătorilor de echipament GNSS extern.

b) O unitate de emisie-recepție (transceiver securizat GNSS), compatibilă cu standardul ISO/IEC 7816-4:2013 (a se vedea 4.2.1) pentru a comunica cu unitatea montată pe vehicul și compatibilă cu interfața de date GNSS pentru receptorul GNSS. Unitatea este prevăzută cu o memorie pentru stocarea datelor de identificare ale receptorului GNSS și ale echipamentului GNSS extern.

c) Un sistem de încapsulare cu funcție de detectare a manipulărilor frauduloase, care încapsulează atât receptorul GNSS, cât și transceiverul securizat GNSS. Funcția de detectare a manipulărilor frauduloase implementează măsurile de protecție a securității conform cerințelor din profilul de protecție al tahografului inteligent.

d) O antenă GNSS instalată pe vehicul și conectată la receptorul GNSS prin sistemul de încapsulare.

GNS_10 Echipamentul GNSS extern are cel puțin următoarele interfețe externe:

a) interfața cu antena GNSS instalată pe remorca vehiculului, dacă se utilizează o antenă externă;

b) interfața cu unitatea montată pe vehicul.

GNS_11 În VU, transceiverul securizat VU este celălalt capăt al comunicării securizate cu transceiverul securizat GNSS și trebuie să fie compatibil cu ISO/IEC 7816-4:2013 pentru conectarea la echipamentul GNSS extern.

GNS_12 Pentru nivelul fizic al comunicării cu echipamentul GNSS extern, unitatea montată pe vehicul trebuie să fie compatibilă cu ISO/IEC 7816-12: 2005 sau cu un alt standard compatibil cu ISO/IEC 7816-4: 2013. (a se vedea 4.2.1).

4.1.2 *Starea echipamentului GNSS extern la finalul procesului de producție*

GNS_13 Echipamentul GNSS extern stochează următoarele valori în memoria nevolatilă a transceiverului securizat GNSS atunci când părăsește fabrica:

— perechea de chei EGF_MA și certificatul corespunzător,

— certificatul MSCA_VU-EGF care conține cheia publică MSCA_VU-EGF.PK care trebuie utilizată pentru verificarea certificatului EGF_MA,

— certificatul EUR care conține cheia publică EUR.PK care trebuie utilizată pentru verificarea certificatului MSCA_VU-EGF,

— certificatul EUR a cărui perioadă de valabilitate precede direct perioada de valabilitate a certificatului EUR care trebuie utilizat pentru verificarea certificatului MSCA_VU-EGF, dacă există,

— certificatul legătură care leagă aceste două certificate EUR, dacă există,

— numărul de serie lung al echipamentului GNSS extern,

— identificatorul sistemului de operare al echipamentului GNSS,

— numărul de omologare de tip al echipamentului GNSS extern,

— identificatorul componentei de securitate a modulului GNSS extern.

4.2. **Comunicarea între echipamentul GNSS extern și unitatea montată pe vehicul**

4.2.1 *Protocolul de comunicare*

GNS_14 Protocolul de comunicare între echipamentul GNSS extern și unitatea montată pe vehicul asigură trei funcții:

1. Colectarea și distribuirea datelor GNSS (de exemplu, poziția, ora, viteza),

2. Colectarea datelor de configurație ale echipamentului GNSS extern,

3. Protocolul de gestionare pentru a asigura cuplarea, autentificarea reciprocă și înțelegerea asupra cheii de sesiune între echipamentul GNSS extern și VU.

GNS_15 Protocolul de comunicare se bazează pe standardul ISO/IEC 7816-4: 2013 unde transceiverul securizat VU deține rolul de *master*, iar transceiverul securizat GNSS deține rolul de *slave*. Conexiunea fizică între echipamentul GNSS extern și unitatea montată pe vehicul se bazează pe ISO/IEC 7816-12:2005 sau pe un alt standard compatibil cu ISO/IEC 7816-4:2013.

GNS_16 Protocolul de comunicare nu este necesar să fie compatibil cu câmpuri cu lungime extinsă.

GNS_17 Protocolul de comunicare din ISO 7816 (atât *-4:2013, cât și *-12:2005) dintre echipamentul GNSS extern și VU se setează la T=1.

GNS_18 În ceea ce privește funcțiile 1) colectarea și distribuirea datelor GNSS, 2) colectarea datelor de configurație ale echipamentului GNSS extern și 3) protocolul de gestionare, transceiverul securizat GNSS simulează un card inteligent cu o arhitectură a sistemului de fișiere compusă dintr-un fișier *master* (MF), un fișier director (DF) cu identificatorul aplicației specificat în apendicele 1 capitolul 6.2 ('FF 44 54 45 47 4D') și cu 3 EF care conțin certificate și un singur fișier elementar (EF.EGF) cu identificatorul fișierului egal cu '2F2F' conform descrierii de la Tabelul 1.

GNS_19 Transceiverul securizat GNSS stochează datele care provin de la receptorul GNSS și configurația în EF. EGF. Acesta este un fișier de înregistrare liniar de lungime variabilă cu un identificator egal cu '2F2F' în format hexadecimal.

GNS_20 Transceiverul securizat GNSS utilizează o memorie pentru stocarea datelor și are o capacitate de cel puțin 20 de milioane de cicluri de scriere/citire. În afară de acest aspect, proiectarea internă și implementarea transceiverului securizat GNSS rămân la latitudinea producătorilor.

Maparea numerelor înregistrărilor și a datelor este furnizată în Tabelul 1. Se menționează faptul că există patru propoziții GSA pentru cele patru sisteme prin satelit și sistemul de augmentare cu ajutorul sateliților (SBAS).

GNS_21 Structura fișierelor este furnizată în Tabelul 1. Pentru condițiile de acces (ALW, NEV, SM-MAC) a se vedea apendicele 2 capitolul 3.5.

Tabelul 1

Structura fișierelor

		Condiții de acces		
Fișier	ID fișier	Citire	Actualizare	Criptat
MF	3F00			
EF.ICC	0002	ALW	NEV (de VU)	Nu
DF Echipament GNSS	0501	ALW	NEV	Nu
EF EGF_MACertificate	C100	ALW	NEV	Nu
EF CA_Certificate	C108	ALW	NEV	Nu
EF Link_Certificate	C109	ALW	NEV	Nu
EF.EGF	2F2F	SM-MAC	NEV (de VU)	Nu

Fișier / element de date	Numărul înregistrării	Dimensiune (octeți)		Valori implicite
		Min	Max	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF Echipament GNSS		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
Propoziție RMC NMEA	‘01’	85	85	
Prima propoziție GSA NMEA	‘02’	85	85	
A 2-a propoziție GSA NMEA	‘03’	85	85	

Fișier / element de date	Numărul înregistrării	Dimensiune (octeți)		Valori implicite
		Min	Max	
A 3-a propoziție GSA NMEA	'04'	85	85	
A 4-a propoziție GSA NMEA	'05'	85	85	
A 5-a propoziție GSA NMEA	'06'	85	85	
Numărul de serie lung al echipamentului GNSS extern definit în apendicele 1 ca SensorGNSSSerialNumber.	'07'	8	8	
Identificatorul sistemului de operare al transceiverului securizat GNSS definit în apendicele 1 ca SensorOSIdentifier.	'08'	2	2	
Numărul de omologare de tip al echipamentului GNSS extern definit în apendicele 1 ca SensorExternalGNSSApprovalNumber.	'09'	16	16	
Identificatorul componentei de securitate a echipamentului GNSS extern definit în apendicele 1 ca SensorExternalGNSSSCIdentifier.	'10'	8	8	
RFU – Rezervat pentru o utilizare viitoare	De la '11' la 'FD'			

4.2.2 *Transferul securizat de date GNSS*

GNS_22 Transferul securizat de date de poziționare GNSS este permis numai în următoarele condiții:

1. Procesul de cuplare a fost încheiat, astfel cum este descris în apendicele 11. „Mecanisme de securitate comune".

2. Autentificarea reciprocă periodică și înțelegerea asupra cheii de sesiune dintre VU și echipamentul GNSS extern descrisă, de asemenea, în apendicele 11. „Mecanisme de securitate comune" a fost executată cu frecvența indicată.

GNS_23 La fiecare T secunde, unde T reprezintă o valoare mai mică sau egală cu 10, cu excepția cazului în care are loc cuplarea sau autentificarea reciprocă și înțelegerea asupra cheii de sesiune, VU solicită de la echipamentul GNSS extern informațiile de poziționare pe baza următorului flux:

1. VU solicită date de localizare de la echipamentul GNSS extern, împreună cu date *Dilution of Precision* (de la propoziția GSA NMEA). Transceiverul securizat VU utilizează comenzile SELECT și READ RECORD(S) în conformitate cu standardul ISO/IEC 7816-4:2013 în modul doar de autentificare al mesageriei securizate, conform descrierii din apendicele 11 secțiunea 11.5 cu identificatorul fișierului „2F2F" și numărul RECORD egal cu „01" pentru propoziția RMC NMEA și '02','03','04','05','06' pentru propoziția GSA NMEA.

2. Ultimele date de localizare primite sunt stocate în EF cu identificatorul '2F2F' și înregistrările descrise în Tabelul 1 în transceiverul securizat GNSS deoarece transceiverul securizat GNSS recepționează date NMEA cu o frecvență de cel puțin 1 Hz de la receptorul GNSS prin interfața de date GNSS.

3. Transceiverul securizat GNSS trimite răspunsul la transceiverul securizat VU folosind mesajul de răspuns APDU în modul doar de autentificare al mesageriei securizate, conform descrierii din apendicele 11 secțiunea 11.5.

4. Transceiverul securizat VU verifică autenticitatea și integritatea răspunsului primit. În cazul unui rezultat pozitiv, datele de localizare sunt transferate către procesorul VU prin interfața de date GNSS.

5. Procesorul VU verifică datele primite și extrage informațiile (de exemplu, latitudinea, longitudinea, ora) din propoziția RMC NMEA. Propoziția RMC NMEA include informații privind valabilitatea poziției. În cazul în care poziția nu este valabilă, datele de localizare nu sunt încă disponibile și nu pot fi utilizate pentru înregistrarea poziției vehiculului. Dacă poziția este valabilă, procesorul VU extrage, de asemenea,valorile HDOP din propozițiile GSA NMEA și calculează valoarea medie pe baza sistemelor prin satelit disponibile (de ex., când *fix* este disponibil).

6. Procesorul VU stochează informațiile primite și prelucrate, cum ar fi latitudinea, longitudinea, ora și viteza, în formatul definit în apendicele 1 „Dicționar de date" ca GeoCoordinates, împreună cu valoarea HDOP calculată ca valoarea minimă a valorilor HDOP colectate pe baza sistemelor GNSS disponibile.

4.2.3 *Structura comenzii de citire a înregistrării (Read Record)*

Această secțiune descrie în detaliu structura comenzii de citire a înregistrării (*Read Record*). Mesageria securizată (modul doar de autentificare) este adăugată conform descrierii din apendicele 11 „Mecanisme de securitate comune".

GNS_24 Comanda trebuie să fie compatibilă cu modul doar autentificare al mesageriei securizate, cf. apendicele 11.

GNS_25 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'0Ch'	Mesagerie securizată solicitată.
INS	1	'B2h'	Citește înregistrarea
P1	1	'XXh'	Numărul înregistrării ('00' indică înregistrarea curentă)
P2	1	'04h'	Citește înregistrarea cu numărul înregistrării indicat în P1
Le	1	'XXh'	Lungimea datelor așteptate. Numărul de octeți de citit.

GNS_26 Înregistrarea indicată în P1 devine înregistrarea curentă.

Octet	Lungime	Valoare	Descriere
#1-#X	X	'XX..XXh'	Date citite
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— În cazul în care comanda este executată cu succes, transceiverul securizat GNSS returnează '**9000**'.

— În cazul în care fișierul curent nu este orientat pe înregistrare, transceiverul securizat GNSS returnează '**6981**'.

— În cazul în care comanda este utilizată cu P1 = '00', dar nu există niciun EF curent, transceiverul securizat GNSS returnează '**6986**' (comandă nepermisă).

— În cazul în care înregistrarea nu este găsită, transceiverul securizat GNSS returnează '**6A 83**'.

— În cazul în care echipamentul GNSS extern a detectat manipulare frauduloasă, returnează cuvintele de stare '**66 90**'.

GNS_27 Transceiverul securizat GNSS trebuie să fie compatibil cu următoarele comenzi de tahograf de generația 2 specificate în apendicele 2:

Comandă	Referință
Select	Apendicele 2 capitolul 3.5.1
Read Binary	Apendicele 2 capitolul 3.5.2
Get Challenge	Apendicele 2 capitolul 3.5.4
PSO: Verify Certificate	Apendicele 2 capitolul 3.5.7
External Authenticate	Apendicele 2 capitolul 3.5.9
General Authenticate	Apendicele 2 capitolul 3.5.10
MSE:SET	Apendicele 2 capitolul 3.5.11

4.3. **Cuplarea, autentificarea reciprocă și înțelegerea asupra cheii de sesiune a echipamentului GNSS extern cu unitatea montată pe vehicul**

Cuplarea, autentificarea reciprocă și înțelegerea asupra cheii de sesiune a echipamentului GNSS extern cu unitatea montată pe vehicul este descrisă în apendicele 11 – „Mecanisme de securitate comune”, capitolul 11.

4.4. **Gestionarea erorilor**

Prezenta secțiune descrie modul în care condițiile de eroare potențiale ale echipamentului GNSS extern sunt tratate și înregistrate în VU.

4.4.1 *Eroare de comunicare cu echipamentul GNSS extern*

GNS_28 În cazul în care VU nu reușește să comunice cu echipamentul GNSS extern cuplat timp de mai mult de 20 de minute consecutive, VU generează și înregistrează în VU un eveniment de tipul EventFaultType cu valoarea de enumerare ‘53’H *Anomalie a comunicării GNSS externe* și cu marca temporală setată la ora curentă. Acest eveniment va fi generat numai dacă sunt îndeplinite următoarele două condiții: a) tahograful inteligent nu este în modul etalonare și b) vehiculul este în mișcare. În acest context, este declanșată o eroare de comunicare atunci când transceiverul securizat VU nu primește un mesaj de răspuns după un mesaj de solicitare, conform descrierii din 4.2.

4.4.2 *Încălcarea integrității fizice a echipamentului GNSS extern*

GNS_29 În cazul în care echipamentul GNSS extern a fost manipulat fraudulos, transceiverul securizat GNSS șterge integral memoria acestuia, inclusiv materialul criptografic. Astfel cum este descris în GNS_25 și GNS_26, VU detectează manipulare frauduloasă dacă răspunsul are starea ‘6690’. VU generează apoi un eveniment de tipul EventFaultType cu valoarea de enumerare *‘55’H Detectare a manipulării frauduloase a GNSS*.

4.4.3 *Absența informațiilor de poziționare de la receptorul GNSS*

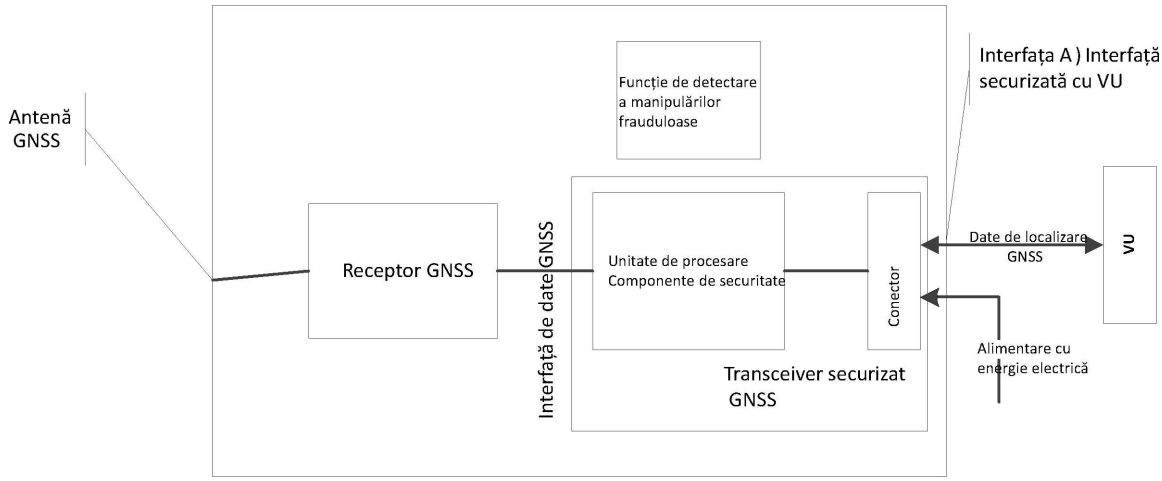
GNS_30 În cazul în care transceiverul securizat GNSS nu primește date de la receptorul GNSS timp de mai mult de 3 ore consecutive, transceiverul securizat GNSS va genera un mesaj de răspuns pentru comanda READ RECORD cu numărul RECORD egal cu ‘01’ cu un câmp de date de 12 octeți setați toți la 0xFF. La primirea mesajului de răspuns cu această valoare a câmpului de date, VU generează și înregistrează un eveniment de tipul EventFaultType cu valoarea de enumerare ‘52’H *Anomalie a receptorului GNSS extern*, cu o marcă temporală egală cu valoarea curentă a orei numai dacă sunt îndeplinite următoarele două condiții: a) tahograful inteligent nu este în modul etalonare și b) vehiculul este în mișcare.

4.4.4 *Certificatul echipamentului GNSS extern a expirat*

GNS_31 Dacă VU detectează că certificatul EGF utilizat pentru autentificarea reciprocă nu mai este valabil, VU generează și înregistrează o anomalie a aparaturii de înregistrare de tipul EventFaultType cu valoarea de enumerare *'56'H Certificatul echipamentului GNSS extern expirat* cu o marcă temporală egală cu valoarea curentă a orei. VU utilizează în continuare datele de poziționare GNSS primite.

Figura 4

Schema echipamentului GNSS extern



5. UNITATE MONTATĂ PE VEHICUL FĂRĂ UN ECHIPAMENT GNSS EXTERN

5.1. **Configurație**

În această configurație, receptorul GNSS se află în interiorul unității montate pe vehicul, conform descrierii din Figura 1.

GNS_32 Receptorul GNSS acționează ca emițător și transmite propoziții NMEA procesorului VU, care acționează ca receptor cu o frecvență de 1/10 Hz sau mai rapid pentru setul prestabilit de propoziții NMEA, care include cel puțin propozițiile RMC și GSA.

GNS_33 O antenă GNSS externă instalată pe vehicul sau o antenă GNSS internă trebuie să fie conectată la VU.

5.2. **Gestionarea erorilor**

5.2.1 *Absența informațiilor de poziționare de la receptorul GNSS*

GNS_34 În cazul în care VU nu primește date de la receptorul GNSS timp de mai mult de 3 ore consecutive, VU generează și înregistrează un eveniment de tipul EventFaultType cu valoarea de enumerare '51'H *Anomalie a receptorului GNSS intern* cu o marcă temporală egală cu valoarea curentă a orei numai dacă sunt îndeplinite următoarele două condiții: a) tahograful inteligent nu este în modul etalonare și b) vehiculul este în mișcare.

6. CONFLICT ORĂ GNSS

Dacă VU detectează o discrepanță de peste 1 minut între ora indicată de funcția de măsurare a timpului a unității montate pe vehicul și ora indicată de receptorul GNSS, VU va înregistra un eveniment de tipul EventFaultType cu valoarea de enumerare *'0B'H Conflict oră (GNSS versus ceasul intern al VU)*. Acest eveniment este înregistrat împreună cu valoarea indicată de ceasul intern al unității montate pe vehicul și este însoțit de o reglare automată a orei. După declanșarea unui eveniment de tip „Conflict oră", VU nu mai va verifica discrepanța de ore în următoarele 12 ore. Acest eveniment nu se declanșează în cazul în care receptorul GNSS nu a putut detecta niciun semnal GNSS valabil în cursul ultimelor 30 de zile. Cu toate acestea, după ce informațiile de poziționare de la receptorul GNSS devin din nou disponibile, se efectuează reglarea automată a orei.

7. CONFLICT PRIVIND DEPLASAREA VEHICULULUI

GNS_35 VU declanșează și înregistrează un eveniment „Conflict privind deplasarea vehiculului” (a se vedea cerința 84 din prezenta anexă) cu o marcă temporală egală cu valoarea curentă a orei, în cazul în care informațiile privind deplasarea calculate de senzorul de mișcare sunt contrazise de informațiile privind deplasarea calculate de receptorul GNSS intern sau de echipamentul GNSS extern. În scopul detectării unor astfel de contradicții, se utilizează valoarea mediană a diferențelor de viteză între aceste surse, după cum se precizează în continuare:

— la fiecare maximum 10 secunde, se calculează valoarea absolută a diferenței dintre viteza vehiculului estimată de GNSS și cea estimată de senzorul de mișcare.

— toate valorile calculate într-o fereastră orară care conține ultimele cinci minute de deplasare se utilizează pentru a calcula valoarea mediană.

— valoarea mediană se calculează ca media a 80 % din valorile rămase, după ce s-au eliminat valorile cele mai mari în valori absolute.

Evenimentul „Conflict privind deplasarea vehiculului” se declanșează dacă valoarea mediană depășește 10 km/h timp de cinci minute neîntrerupte de deplasare a vehiculului. Opțional, pot fi utilizate alte surse independente de detectare a deplasării vehiculului, pentru a se pune la dispoziție o detectare mai fiabilă a manipulărilor tahografului. (Notă: Utilizarea medianei ultimelor 5 minute se aplică pentru a atenua riscul de măsurători aberante și valori tranzitorii). Acest eveniment nu se declanșează în următoarele condiții: a) în timpul unei traversări cu feribotul sau cu trenul, b) atunci când informațiile de poziționare de la receptorul GNSS nu sunt disponibile și c) în modul etalonare.

Apendicele 13

INTERFAȚA ITS

CUPRINS

1. INTRODUCERE 416

2. OBIECT 416

2.1. Acronime, definiții și notații 417

3. REGULAMENTE ȘI STANDARDE MENȚIONATE 418

4. PRINCIPIILE DE FUNCȚIONARE A INTERFEȚEI 418

4.1. Condiții prealabile pentru transferul de date prin interfața ITS 418

4.1.1 Datele furnizate prin interfața ITS 418

4.1.2 Conținutul datelor 418

4.1.3 Aplicații ITS 418

4.2. Tehnologia comunicațiilor 419

4.3. Autorizare prin PIN 419

4.4. Formatul mesajelor 421

4.5. Acordul conducătorului auto 425

4.6. Extragerea de date standard 426

4.7. Extragerea de date cu caracter personal 426

4.8. Extragerea de date privind evenimentele și anomaliile 426

1. INTRODUCERE

Prezentul apendice prezintă detaliile privind concepția și procedurile care trebuie urmate pentru a implementa interfața cu sisteme de transport inteligente (ITS), astfel cum este prevăzut la articolul 10 din Regulamentul (UE) nr. 165/2014 (denumit în continuare *regulamentul*).

Regulamentul prevede că tahografele vehiculelor pot fi echipate cu interfețe standardizate care permit utilizarea în modul operațional, de către un dispozitiv extern, a datelor înregistrate sau produse de tahograf, dacă sunt îndeplinite următoarele condiții:

(a) interfața nu trebuie să afecteze autenticitatea și integritatea datelor tahografului;

(b) interfața trebuie să respecte dispozițiile detaliate de la articolul 11 din *regulament*;

(c) dispozitivul extern conectat la interfață poate accesa datele cu caracter personal, inclusiv datele de geopoziționare, numai după acordul verificabil al conducătorului auto la care se referă datele.

2. OBIECT

Scopul prezentului apendice este să precizeze modul în care aplicațiile instalate pe dispozitive externe pot să extragă date (denumite în continuare *datele*) dintr-un tahograf prin intermediul unei conexiuni Bluetooth®.

Datele disponibile prin intermediul acestei interfețe sunt descrise în anexa 1 la prezentul document. Această interfață nu exclude implementarea altor interfețe (de exemplu, prin intermediul magistralei CAN) în vederea transmiterii datelor din unitatea montată pe vehicul (VU) către alte unități de procesare montate pe vehicul.

Prezentul apendice specifică:

— *datele* disponibile prin interfața ITS;

— profilul Bluetooth® care este utilizat pentru transferul de date;

— procedurile de interogare și de descărcare și secvența de operațiuni;

— mecanismul de asociere dintre tahograf și dispozitivul extern;

— mecanismul de confirmare aflat la dispoziția conducătorului auto.

Pentru clarificare, prezenta anexă nu specifică:

— colectarea *datelor* și gestionarea acestora în cadrul VU (care trebuie să fie specificate în altă secțiune a *regulamentului* sau să depindă de concepția produsului);

— forma de prezentare a datelor colectate către aplicația instalată pe dispozitivul extern;

— dispozițiile de securitate a datelor care depășesc securitatea oferită de Bluetooth® (cum ar fi criptarea) în ceea ce privește conținutul *datelor* [care trebuie să fie specificate în altă secțiune a *regulamentului* (apendicele 10 – Mecanisme de securitate comune)];

— protocoalele Bluetooth® utilizate de interfața ITS.

2.1. **Acronime, definiții și notații**

În prezentul apendice sunt utilizate următoarele acronime și definiții specifice prezentului apendice:

comunicarea schimbul de informații/date între o unitate *master* (și anume, tahografele) și o unitate externă, prin intermediul interfeței ITS și folosind sistemul Bluetooth®.

datele seturile de date precizate în anexa 1.

regulamentul Regulamentul (UE) nr. 165/2014 al Parlamentului European și al Consiliului din 4 februarie 2014 privind tahografele în transportul rutier, de abrogare a Regulamentului (CEE) nr. 3821/85 al Consiliului privind aparatura de înregistrare în transportul rutier și de modificare a Regulamentului (CE) nr. 561/2006 al Parlamentului European și al Consiliului privind armonizarea anumitor dispoziții ale legislației sociale în domeniul transporturilor rutiere.

BR rata de bază (*basic rate*)

EDR rata îmbunătățită de transfer al datelor (*enhanced data rate*)

GNSS sistem global de navigație prin satelit (*Global navigation satellite system*)

IRK cheie de rezolvare a identității (*identity resolution key*)

ITS sistem de transport inteligent (*intelligent transport system*)

LE nivel redus de energie (*low energy*)

PIN număr de identificare personal (*personal identification number*)

PUC cod de deblocare personal (*personal unblocking code*)

SID identificator de serviciu (*service identifier*)

SPP profilul portului serial (*serial port profile*)

SSP asociere simplă securizată (*secure simple pairing*)

TRTP parametru de solicitare de transfer (*transfer request parameter*)

PRT parametru de răspuns la transfer (*transfer response parameter*)

VU unitate montată pe vehicul (*vehicle unit*)

3. REGULAMENTE ȘI STANDARDE MENȚIONATE

Specificația definită în prezentul apendice se referă la toate sau la o parte din următoarele regulamente și standarde și depinde de acestea. În cadrul clauzelor din prezentul apendice sunt specificate standardele relevante sau clauzele relevante ale standardelor. În cazul oricărei situații contradictorii, clauzele din prezentul apendice prevalează.

Regulamentele și standardele la care se face trimitere în prezentul apendice sunt următoarele:

— Regulamentul (UE) nr. 165/2014 al Parlamentului European și al Consiliului din 4 februarie 2014 privind tahografele în transportul rutier, de abrogare a Regulamentului (CEE) nr. 3821/85 al Consiliului privind aparatura de înregistrare în transportul rutier și de modificare a Regulamentului (CE) nr. 561/2006 al Parlamentului European și al Consiliului privind armonizarea anumitor dispoziții ale legislației sociale în domeniul transporturilor rutiere.

— Regulamentul (CE) nr. 561/2006 al Parlamentului European și al Consiliului din 15 martie 2006 privind armonizarea anumitor dispoziții ale legislației sociale în domeniul transporturilor rutiere, de modificare a Regulamentelor (CEE) nr. 3821/85 și (CE) nr. 2135/98 ale Consiliului și de abrogare a Regulamentului (CEE) nr. 3820/85 al Consiliului.

— ISO 16844 – 4: *Road vehicles – Tachograph systems – Part 4: Can interface*

— ISO 16844 – 7: *Road vehicles – Tachograph systems – Part 7: Parameters*

— Bluetooth® – *Serial Port Profile* – V1.2

— Bluetooth® – Versiunea principală 4.2

— Protocolul NMEA 0183 V4.1

4. PRINCIPIILE DE FUNCȚIONARE A INTERFEȚEI

4.1. **Condiții prealabile pentru transferul de date prin interfața ITS**

Unitatea montată pe vehicul are rolul de a actualiza și de a păstra datele care urmează să fie stocate în VU, fără implicarea interfeței ITS. Acest rol este îndeplinit de unitatea montată pe vehicul printr-o modalitate internă, care este specificată în altă secțiune a regulamentului și nu este specificată în prezentul apendice.

4.1.1 *Datele furnizate prin interfața ITS*

Unitatea montată pe vehicul este responsabilă cu actualizarea datelor care vor fi disponibile prin interfața ITS, cu o frecvență stabilită în cadrul procedurilor VU, fără implicarea interfeței ITS. Datele furnizate de unitatea montată pe vehicul sunt utilizate ca bază pentru a completa și a actualiza *datele*; modalitatea prin care se realizează acest lucru este specificată în altă secțiune din *regulament* sau, în cazul în care nu există o astfel de specificație, această modalitate depinde de concepția produsului și nu este specificată în prezentul apendice.

4.1.2 *Conținutul datelor*

Conținutul *datelor* este specificat în anexa 1 la prezentul apendice.

4.1.3 *Aplicații ITS*

Aplicațiile ITS vor folosi datele puse la dispoziție prin interfața ITS, de exemplu pentru a optimiza gestionarea activităților conducătorului auto, respectând în același timp dispozițiile regulamentului, pentru a detecta posibilele anomalii ale tahografului sau pentru utilizarea datelor GNSS. Specificarea aplicațiilor nu face obiectul prezentului apendice.

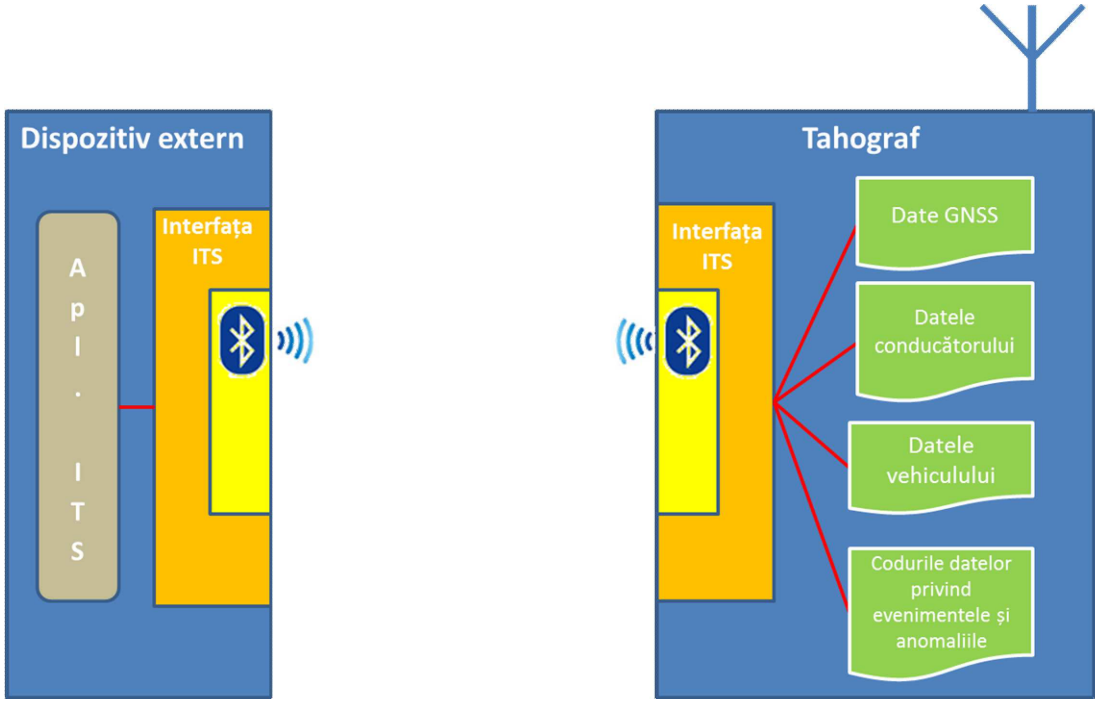
4.2. **Tehnologia comunicațiilor**

Schimbul de *date* prin interfața ITS se efectuează printr-o interfață Bluetooth® compatibilă folosind versiunea 4.2 sau o versiune mai recentă. Bluetooth® funcționează în banda de unde industrială, științifică și medicală (ISM) cu frecvențe cuprinse între 2,4 și 2,485 GHz; această bandă nu face obiectul unei licențe. Bluetooth® 4.2 oferă mecanisme îmbunătățite de confidențialitate și de securitate și este caracterizat de o viteză și o fiabilitate sporite ale transferurilor de date. În scopul prezentei specificații este utilizat sistemul radio Bluetooth® de clasa 2 cu o rază de acțiune de cel mult 10 m. Informații suplimentare cu privire la Bluetooth® 4.2 sunt disponibile la adresa: www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Comunicarea se stabilește cu echipamentele de comunicare după finalizarea unui proces de asociere de către un dispozitiv autorizat. Întrucât Bluetooth® folosește o arhitectură de tip *master/slave* pentru a controla atât momentul în care dispozitivele pot transmite date, cât și destinația acestor date, tahograful va îndeplini funcția de *master*, iar dispozitivul extern va avea rolul de *slave*.

Atunci când un dispozitiv extern intră pentru prima dată în raza de acțiune a VU, procesul de asociere Bluetooth® poate fi inițiat (a se vedea, de asemenea, anexa 2). Dispozitivele își transmit reciproc adresele, numele și profilurile, precum și cheia secretă comună, ceea ce le permite să se lege unul la altul ori de câte ori intră în contact ulterior. După finalizarea acestui pas, dispozitivul extern este „certificat” și este în măsură să lanseze solicitări de descărcare a datelor din tahograf. Nu se preconizează folosirea de mecanisme de criptare suplimentare pe lângă cele deja existente în sistemul Bluetooth®. Cu toate acestea, în cazul în care sunt necesare mecanisme suplimentare de securitate, acestea vor fi implementate în conformitate cu apendicele 10 – Mecanisme de securitate comune.

Figura de mai jos prezintă principiul general de comunicare.



SPP (profilul portului serial) al sistemului Bluetooth® este utilizat pentru a transfera date de la VU la dispozitivul extern.

4.3. **Autorizare prin PIN**

Din motive de securitate, VU trebuie să impună un sistem de autorizare bazat pe un cod PIN, separat de sistemul de asociere Bluetooth. În scopuri de autentificare, fiecare VU trebuie să poată genera coduri PIN formate din cel puțin 4 cifre. De fiecare dată când un dispozitiv extern se asociază cu o VU, dispozitivul respectiv trebuie să furnizeze codul PIN corect înainte de a primi eventualele date.

Introducerea corectă a PIN-ului implică plasarea dispozitivului pe lista dispozitivelor validate. Lista dispozitivelor validate trebuie să cuprindă cel puțin 64 de dispozitive asociate cu o anume VU.

Furnizarea unui cod PIN incorect de trei ori la rând duce la plasarea provizorie a dispozitivului pe lista neagră. Câtă vreme dispozitivul se află pe lista neagră, orice nouă încercare de accesare din partea dispozitivului este respinsă. Furnizarea în continuare a unui cod PIN incorect, de trei ori la rând, duce la plasarea pentru o perioadă din ce în ce mai lungă a dispozitivului pe lista neagră (a se vedea tabelul 1). Furnizarea corectă a codului PIN permite resetarea duratei de interdicție și a numărului de încercări. În figura 1 din anexa 2 este prezentată schema etapelor unei încercări de validare folosind codul PIN.

Tabelul 1

Durata interdicției în funcție de numărul de introduceri consecutive ale unui cod PIN incorect

Numărul de încercări eronate consecutive	Durata interdicției
3	30 de secunde
6	5 minute
9	1 oră
12	24 de ore
15	Permanent

Furnizarea unui cod PIN incorect de cincisprezece ori la rând (5 × 3) duce la plasarea permanentă a dispozitivului pe lista neagră a unității ITS. Această interdicție permanentă se anulează numai prin furnizarea codului PUC corect.

Codul PUC este compus din 8 cifre și este furnizat de producător împreună cu VU. Furnizarea unui cod PUC incorect de zece ori la rând va duce la plasarea definitivă a unității ITS pe lista neagră.

Cu toate că producătorul poate oferi opțiunea schimbării directe a codului PIN prin intermediul VU, codul PUC trebuie să nu poată fi modificat. Dacă există posibilitatea schimbării codului PIN, aceasta se efectuează prin introducerea actualului cod PIN direct în VU.

De asemenea, orice dispozitive stocate în lista dispozitivelor validate rămân incluse în listă până la înlăturarea manuală (a acestora) de către utilizator (de exemplu, prin intermediul interfeței dispozitiv-utilizator a VU sau prin alte mijloace). Prin această procedură pot fi eliminate de pe lista dispozitivelor validate unitățile ITS care au fost pierdute sau furate. În plus, orice unitate ITS care nu se mai află în raza de acțiune a conexiunii Bluetooth timp de peste 24 de ore este eliminată automat din lista dispozitivelor validate a VU și trebuie să furnizeze din nou codul PIN corect la restabilirea conexiunii.

Formatul mesajelor dintre interfața VU și VU nu este furnizat, alegerea acestuia fiind lăsată la latitudinea producătorului. Cu toate acestea, producătorul în cauză trebuie să se asigure că formatul mesajului transmis între unitatea ITS și interfața VU este respectat (a se vedea specificațiile ASN.1).

Prin urmare, toate solicitările de date trebuie să facă obiectul verificării corespunzătoare a acreditărilor expeditorului, înainte de a iniția orice formă de tratare a datelor respective. În figura 2 din anexa 2 este prezentată schema etapelor pentru această procedură. Orice dispozitiv aflat pe lista neagră este respins automat, iar orice dispozitiv care nu se află nici pe lista neagră, nici pe lista dispozitivelor validate primește o cerere de furnizare a PIN-ului pe care trebuie să o îndeplinească înainte de a trimite din nou solicitarea sa de date.

4.4. **Formatul mesajelor**

Toate mesajele transmise între unitatea ITS și VU trebuie să fie formatate într-o structură alcătuită din trei părți: un antet compus dintr-un octet țintă (TGT), un octet sursă (SRC) și un octet de lungime (LEN);

câmpul de date compus dintr-un octet de identificare a serviciului (SID) și dintr-un număr variabil de octeți de date (cel mult 255);

octetul de sumă de verificare (*checksum byte*) corespunde unei serii de sume de câte 1 bit modul 256 care reprezintă toți octeții din mesaj cu excepția octetului de sumă de verificare (CS).

Mesajul este în sistemul *Big Endian*.

Tabelul 2

Formatul general al mesajelor

Antet			Câmp de date					Sumă de verificare
TGT	SRC	LEN	SID	TRTP	CC	CM	DATE	CS
3 octeți			maximum 255 de octeți					1 octet

Antet

TGT și SRC: ID-ul dispozitivului țintă (TGT) și ID-ul dispozitivului sursă (SRC) ale mesajului. Interfața VU trebuie să aibă codul de identificare implicit „EE”. Acest cod de identificare nu poate fi schimbat. Unitatea ITS trebuie să utilizeze codul de identificare implicit „A0” pentru primul său mesaj din sesiunea de comunicare. Interfața VU atribuie apoi un cod de identificare unic unității ITS și îl transmite spre informare unității ITS pentru viitoarele mesaje din timpul sesiunii.

Octetul LEN trebuie să țină seama numai de rubrica „DATE” din câmpul de date (a se vedea tabelul 2); primii 4 octeți sunt impliciți.

Interfața VU trebuie să confirme autenticitatea expeditorului mesajului prin verificări încrucișate ale propriei liste de ID-uri (*IDList*) cu datele obținute prin sistemul Bluetooth, verificând faptul că unitatea ITS corespunzătoare codului de identificare furnizat se află în acel moment în raza de acțiune a conexiunii Bluetooh.

Câmpul de date

Pe lângă SID, câmpul de date trebuie să conțină și alți parametri: un parametru de solicitare de transfer (TRTP) și octeți de numărare.

În cazul în care datele care trebuie transportate sunt mai voluminoase decât spațiul disponibil într-un singur mesaj, ele vor fi separate în mai multe submesaje. Fiecare submesaj trebuie să aibă același antet și același SID, dar va conține un contor cu doi octeți, contorul curent (CC) și contorul maxim (CM), pentru a indica numărul de ordine al submesajului. Pentru a permite verificarea erorilor și o eventuală încetare a schimbului de date, dispozitivul receptor confirmă primirea fiecărui submesaj. Dispozitivul receptor poate accepta submesajul, poate solicita retransmiterea acestuia și poate solicita dispozitivului emițător să reia sau să abandoneze transmisia.

Dacă nu sunt utilizate, CC și CM primesc valoarea 0xFF.

De exemplu, următorul mesaj

ANTET	SID	TRTP	CC	CM	DATE	CS
3 octeți	mai lung de 255 de octeți					1 octet

Se transmite astfel:

ANTET	SID	TRTP	01	n	DATE	CS
3 octeți	255 de octeți					1 octet

ANTET	SID	TRTP	02	n	DATE	CS
3 octeți	255 de octeți					1 octet

...

ANTET	SID	TRTP	N	N	DATE	CS
3 octeți	maximum 255 de octeți					1 octet

Tabelul 3 conține mesajele care pot fi schimbate între VU și unitatea ITS. Conținutul fiecărui parametru este dat în valori hexazecimale. Din motive de claritate, în tabel nu sunt indicați CC și CM; a se vedea mai sus formatul complet.

Tabelul 3

Conținutul detaliat al mesajelor

Mesaj	Antet			DATE			Sumă de control
	TGT	SRC	LEN	SID	TRTP	DATE	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*NUMĂR ÎNTREG (0..9)	
Pairingresult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Timp	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		

Mesaj	Antet			DATE			Sumă de control
	TGT	SRC	LEN	SID	TRTP	DATE	
ResquestAccepted	*ITSID*	EE	Len	09	PRT	Date	
DataUnavailable							
Nu sunt disponibile date	*ITSID*	EE	02	0A	PRT	10	
Datele cu caracter personal nu sunt făcute publice	*ITSID*	EE	02	0A	PRT	11	
NegativeAnswer							
Respingere generală	*ITSID*	EE	02	0B	SID Req	10	
Serviciu incompatibil	*ITSID*	EE	02	0 B	SID Req	11	
Subfuncție incompatibilă	*ITSID*	EE	02	0 B	SID Req	12	
Lungime incorectă a mesajului	*ITSID*	EE	02	0 B	SID Req	13	
Condiții incorecte sau eroare a secvenței de solicitare	*ITSID*	EE	02	0 B	SID Req	22	
Solicitare în afara intervalului	*ITSID*	EE	02	0 B	SID Req	31	
Răspuns în așteptare	*ITSID*	EE	02	0 B	SID Req	78	
Neconcordanță ITSID	*ITSID*	EE	02	0 B	SID Req	FC	
ITSID nu poate fi găsit	*ITSID*	EE	02	0 B	SID Req	FB	

RequestPIN (SID 01)

Acest mesaj este emis de interfața VU în cazul în care o unitate ITS care nu este pe lista neagră, dar nici pe lista dispozitivelor validate trimite o solicitare de date.

SendITSID (SID 02)

Acest mesaj este emis de interfața VU ori de câte ori un nou dispozitiv emite o solicitare. Acest dispozitiv utilizează codul de identificare implicit „A0” înainte de a îi fi atribuit un cod de identificare unic pentru sesiunea de comunicare.

SendPIN (SID 03)

Acest mesaj este emis de unitatea ITS care urmează să fie înscrisă pe lista de dispozitive validate de către interfața VU. Conținutul acestui mesaj este un număr întreg 4 („4 INTEGER”) cuprins între 0 și 9.

PairingResult (SID 04)

Acest mesaj este emis de interfața VU pentru a informa unitatea ITS că aceasta din urmă a trimis un cod PIN corect. Conținutul acestui mesaj este un element BOOLEAN cu valoarea „True” în cazul în care codul PIN este corect, respectiv „False” în caz contrar.

SendPUC (SID 05)

Acest mesaj este emis de unitatea ITS pentru o scoatere de pe lista neagră de către interfața VU. Conținutul acestui mesaj este un număr întreg 8 („8 INTEGER”) cuprins între 0 și 9.

BanLiftingResult (SID 06)

Acest mesaj este emis de interfața VU pentru a informa unitatea ITS că aceasta din urmă a trimis un cod PUC corect. Conținutul acestui mesaj este un element BOOLEAN cu valoarea „True” în cazul în care codul PUC este corect, respectiv „False” în caz contrar.

RequestRejected (SID 07)

Acest mesaj este emis de interfața VU ca răspuns la orice mesaj trimis de o unitate ITS aflată pe lista neagră, cu excepția mesajului „SendPUC”. Mesajul precizează timpul rămas până la scoaterea unității ITS de pe lista neagră, conform formatului secvenței „Timp” astfel cum este definit în anexa 3.

RequestData (SID 08)

Acest mesaj pentru accesarea datelor este emis de unitatea ITS. Un parametru de solicitare de transfer de un octet (TRTP) indică tipul datelor solicitate. Există mai multe tipuri de date:

— standardTachData (TRTP 01): date puse la dispoziție de tahograf și clasificate ca fiind publice.

— personalTachData (TRTP 02): date puse la dispoziție de tahograf și clasificate ca având caracter personal.

— gnssData (TRTP 03): datele referitoare la GNSS, care au întotdeauna un caracter personal.

— standardEventData (TRTP 04): date privind evenimentele înregistrate, clasificate ca fiind publice.

— personalEventData (TRTP 05): date privind evenimentele înregistrate, clasificate ca având caracter personal.

— standardFaultData (TRTP 06): anomalii înregistrate, clasificate ca fiind publice.

— manufacturerData (TRTP 07): date puse la dispoziție de către producător.

A se vedea anexa 3 din prezentul apendice pentru mai multe informații referitoare la conținutul fiecărui tip de date.

A se vedea apendicele 12 pentru mai multe informații cu privire la formatul și conținutul datelor GNSS.

A se vedea anexele IB și IC pentru mai multe informații referitoare la datele privind evenimentele și la anomalii.

ResquestAccepted (SID 09)

Acest mesaj este emis de interfața VU dacă un mesaj „RequestData” transmis de o unitate ITS a fost acceptat. Acest mesaj conține un PRT de un 1 octet, care reprezintă octetul TRTP al mesajului *RequestData* asociat și al tuturor datelor de tipul solicitat.

DataUnavailable (SID 0A)

Acest mesaj este emis de interfața VU dacă, dintr-un motiv oarecare, informațiile solicitate nu sunt disponibile pentru a fi transmise unei unități ITS aflate pe o listă de dispozitive validate. Mesajul conține un PRT de 1 octet, care reprezintă TRTP-ul datelor solicitate, și un cod de eroare de 1 octet, specificat în tabelul 3. Se aplică următoarele coduri:

— Nu sunt disponibile informații (10): Interfața VU nu poate avea acces la datele VU dacă motivele cererii de accesare nu sunt precizate.

— Datele cu caracter personal nu sunt public accesibile (11): Unitatea ITS încearcă să extragă date cu caracter personal în situații în care acestea nu sunt public accesibile.

NegativeAnswer (SID 0B)

Aceste mesaje sunt emise de interfața VU dacă o solicitare nu poate fi finalizată din orice alte motive decât indisponibilitatea datelor. Mesajele respective sunt în general rezultatul utilizării unui format eronat al solicitării (lungime, SID, ITSID...), dar pot avea și alte cauze. TRTP-ul din câmpul de date conține SID-ul solicitării. Câmpul de date conține un cod prin care este identificat motivul răspunsului negativ. Se aplică următoarele coduri:

— Respingere generală (cod: 10)

— Acțiunea nu poate fi realizată dintr-un motiv care nu este menționat nici mai jos, nici în secțiunea (a se introduce numărul secțiunii *DataUnavailable*).

— Serviciu incompatibil (cod: 11)

— SID-ul solicitării nu este comprehensibil.

— Subfuncție incompatibilă (cod: 12)

— TRTP-ul solicitării nu este comprehensibil. Acesta poate fi, de exemplu, absent sau se poate situa în afara intervalului de valori acceptate.

— Lungime incorectă a mesajului (cod: 13)

— Lungimea mesajului primit este incorectă (neconcordanță între octetul LEN și lungimea efectivă a mesajului).

— Condiții incorecte sau eroare a secvenței de solicitare (cod: 22)

— Serviciul solicitat nu este disponibil sau secvența mesajelor de solicitare nu este corectă

— Solicitare în afara intervalului (cod: 33)

— Înregistrarea parametrului solicitării (câmp de date) nu este valabilă

— Răspuns în așteptare (cod: 78)

— Acțiunea solicitată nu poate fi finalizată în timp util și VU nu este pregătită să accepte o nouă solicitare.

— Neconcordanță *ITSID* (cod: FB)

— În urma comparării cu informațiile Bluetooh, rezultă că ITSID-ul SRC-ului nu corespunde dispozitivului asociat.

— *ITSID* absent (cod: FC)

— *ITSID*-ul SRC-ului nu este asociat cu niciun dispozitiv.

Rândurile 1-72 (**FormatMessageModule**) din codul ASN.1 din anexa 3 precizează formatul mesajelor, astfel cum este descris în tabelul 3. Mai jos sunt oferite detalii suplimentare cu privire la conținutul mesajelor.

4.5. **Acordul conducătorului auto**

Toate datele disponibile sunt clasificate fie ca date standard, fie ca date cu caracter personal. Datele cu caracter personal sunt accesibile numai în cazul în care conducătorul auto și-a dat acordul în acest sens, acceptând ca datele sale cu caracter personal referitoare la tahograf să fie transmise în afara rețelei vehiculului pentru a fi utilizate în aplicații ale unor părți terțe.

Acordul conducătorului auto este dat atunci când, la prima introducere a unui anumit card de conducător auto sau a unui card de atelier necunoscut de unitatea montată pe vehicul până la momentul respectiv, titularul cardului este invitat să își exprime acordul pentru transmiterea în exterior, prin intermediul interfeței opționale ITS, a datelor cu caracter personal care se referă la tahograf (a se vedea, de asemenea, anexa I C punctul 3.6.2).

Starea acordului (activat/dezactivat) se înregistrează în memoria tahografului.

În cazul în care există mai mulți conducători auto, numai datele cu caracter personal referitoare la conducătorii auto care și-au dat acordul în acest sens sunt transmise interfeței ITS. De exemplu, în cazul în care există doi conducători auto la bordul vehiculului, dar numai unul dintre aceștia a acceptat să permită accesul la datele sale cu caracter personal, datele referitoare la celălalt conducător auto nu pot fi transmise unei terțe părți.

4.6. **Extragerea de date standard**

În figura 3 din anexa 2 este prezentată diagrama secvențelor unei cereri valabile trimise de unitatea ITS pentru a solicita accesul la date standard. Unitatea ITS este inclusă în mod corespunzător pe lista dispozitivelor validate și nu solicită accesul la date cu caracter personal; prin urmare, nu este necesară nicio verificare suplimentară. În diagramele menționate se consideră că a fost deja urmată procedura corespunzătoare ilustrată în figura 2 din anexa 2. Acestea pot fi considerate echivalente cu dreptunghiul gri purtând mențiunea *REQUEST TREATMENT* din figura 2.

Dintre datele disponibile, următoarele sunt considerate a fi date standard:

— standardTachData (TRTP 01)

— standardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Extragerea de date cu caracter personal**

În figura 4 din anexa 2 este prezentată diagrama secvențelor pentru prelucrarea solicitărilor de date cu caracter personal. După cum s-a menționat anterior, interfața VU transmite date cu caracter personal numai în cazul în care conducătorul auto și-a dat acordul explicit în acest sens (a se vedea, de asemenea, punctul 4.5). În caz contrar, solicitarea trebuie respinsă în mod automat.

Dintre datele disponibile, următoarele sunt considerate a fi date cu caracter personal:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Extragerea de date privind evenimentele și anomaliile**

Unitățile ITS trebuie să aibă capacitatea de a solicita date privind evenimentele, care conțin lista tuturor evenimentelor neprevăzute. Aceste date sunt considerate fie standard, fie date cu caracter personal (a se vedea anexa 3). Conținutul fiecărui eveniment este în conformitate cu documentația furnizată în anexa 1 la prezentul apendice.

ANEXA 1

LISTA DATELOR DISPONIBILE PRIN INTERFAȚA ITS

Date	Sursa	Clasificare recomandată
VehicleIdentificationNumber	Unitatea montată pe vehicul	**publice**
CalibrationDate	Unitatea montată pe vehicul	**publice**
TachographVehicleSpeed speed instant t	Unitatea montată pe vehicul	cu caracter personal
Driver1WorkingState Selector driver	Unitatea montată pe vehicul	cu caracter personal
Driver2WorkingState	Unitatea montată pe vehicul	cu caracter personal
DriveRecognize Speed Threshold detected	Unitatea montată pe vehicul	**publice**
Driver1TimeRelatedStates Weekly day time	Cardul conducătorului auto	cu caracter personal
Driver2TimeRelatedStates	Cardul conducătorului auto	cu caracter personal
DriverCardDriver1	Unitatea montată pe vehicul	**publice**
DriverCardDriver2	Unitatea montată pe vehicul	**publice**
OverSpeed	Unitatea montată pe vehicul	cu caracter personal
TimeDate	Unitatea montată pe vehicul	**publice**
HighResolutionTotalVehicleDistance	Unitatea montată pe vehicul	**publice**
ServiceComponentIdentification	Unitatea montată pe vehicul	**publice**
ServiceDelayCalendarTimeBased	Unitatea montată pe vehicul	**publice**
Driver1Identification	Cardul conducătorului auto	cu caracter personal
Driver2Identification	Cardul conducătorului auto	cu caracter personal
NextCalibrationDate	Unitatea montată pe vehicul	**publice**
Driver1ContinuousDrivingTime	Cardul conducătorului auto	cu caracter personal
Driver2ContinuousDrivingTime	Cardul conducătorului auto	cu caracter personal
Driver1CumulativeBreakTime	Cardul conducătorului auto	cu caracter personal
Driver2CumulativeBreakTime	Cardul conducătorului auto	cu caracter personal
Driver1CurrentDurationOfSelectedActivity	Cardul conducătorului auto	cu caracter personal
Driver2CurrentDurationOfSelectedActivity	Cardul conducătorului auto	cu caracter personal

Date	Sursa	Clasificare recomandată
SpeedAuthorised	Unitatea montată pe vehicul	**publice**
TachographCardSlot1	Cardul conducătorului auto	**publice**
TachographCardSlot2	Cardul conducătorului auto	**publice**
Driver1Name	Cardul conducătorului auto	cu caracter personal
Driver2Name	Cardul conducătorului auto	cu caracter personal
OutOfScopeCondition	Unitatea montată pe vehicul	**publice**
ModeOfOperation	Unitatea montată pe vehicul	**publice**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Cardul conducătorului auto	cu caracter personal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Cardul conducătorului auto	cu caracter personal
EngineSpeed	Unitatea montată pe vehicul	cu caracter personal
RegisteringMemberState	Unitatea montată pe vehicul	**publice**
VehicleRegistrationNumber	Unitatea montată pe vehicul	**publice**
Driver1EndOfLastDailyRestPeriod	Cardul conducătorului auto	cu caracter personal
Driver2EndOfLastDailyRestPeriod	Cardul conducătorului auto	cu caracter personal
Driver1EndOfLastWeeklyRestPeriod	Cardul conducătorului auto	cu caracter personal
Driver2EndOfLastWeeklyRestPeriod	Cardul conducătorului auto	cu caracter personal
Driver1EndOfSecondLastWeeklyRestPeriod	Cardul conducătorului auto	cu caracter personal
Driver2EndOfSecondLastWeeklyRestPeriod	Cardul conducătorului auto	cu caracter personal
Driver1CurrentDailyDrivingTime	Cardul conducătorului auto	cu caracter personal
Driver2CurrentDailyDrivingTime	Cardul conducătorului auto	cu caracter personal
Driver1CurrentWeeklyDrivingTime	Cardul conducătorului auto	cu caracter personal
Driver2CurrentWeeklyDrivingTime	Cardul conducătorului auto	cu caracter personal
Driver1TimeLeftUntilNewDailyRestPeriod	Cardul conducătorului auto	cu caracter personal
Driver2TimeLeftUntilNewDailyRestPeriod	Cardul conducătorului auto	cu caracter personal
Driver1CardExpiryDate	Cardul conducătorului auto	cu caracter personal

Date	Sursa	Clasificare recomandată
Driver2CardExpiryDate	Cardul conducătorului auto	cu caracter personal
Driver1CardNextMandatoryDownloadDate	Cardul conducătorului auto	cu caracter personal
Driver2CardNextMandatoryDownloadDate	Cardul conducătorului auto	cu caracter personal
TachographNextMandatoryDownloadDate	Unitatea montată pe vehicul	**publice**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Cardul conducătorului auto	cu caracter personal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Cardul conducătorului auto	cu caracter personal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Cardul conducătorului auto	cu caracter personal
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Cardul conducătorului auto	cu caracter personal
Driver1CumulativeUninterruptedRestTime	Cardul conducătorului auto	cu caracter personal
Driver2CumulativeUninterruptedRestTime	Cardul conducătorului auto	cu caracter personal
Driver1MinimumDailyRest	Cardul conducătorului auto	cu caracter personal
Driver2MinimumDailyRest	Cardul conducătorului auto	cu caracter personal
Driver1MinimumWeeklyRest	Cardul conducătorului auto	cu caracter personal
Driver2MinimumWeeklyRest	Cardul conducătorului auto	cu caracter personal
Driver1MaximumDailyPeriod	Cardul conducătorului auto	cu caracter personal
Driver2MaximumDailyPeriod	Cardul conducătorului auto	cu caracter personal
Driver1MaximumDailyDrivingTime	Cardul conducătorului auto	cu caracter personal
Driver2MaximumDailyDrivingTime	Cardul conducătorului auto	cu caracter personal
Driver1NumberOfUsedReducedDailyRestPeriods	Cardul conducătorului auto	cu caracter personal
Driver2NumberOfUsedReducedDailyRestPeriods	Cardul conducătorului auto	cu caracter personal
Driver1RemainingCurrentDrivingTime	Cardul conducătorului auto	cu caracter personal
Driver2RemainingCurrentDrivingTime	Cardul conducătorului auto	cu caracter personal
GNSS position	Unitatea montată pe vehicul	cu caracter personal

2) DATE GNSS FURNIZATE ÎN FLUX CONTINUU DISPONIBILE CU ACORDUL CONDUCĂTORULUI AUTO

A se vedea apendicele 12 – GNSS.

3) CODURI ALE EVENIMENTELOR DISPONIBILE FĂRĂ ACORDUL PREALABIL AL CONDUCĂTORULUI AUTO

Eveniment	Reguli de stocare	Date care trebuie înregistrate pentru fiecare eveniment
Introducerea unui card nevalabil	— cele mai recente 10 evenimente.	— data și ora evenimentului, — tipul și numărul cardului (cardurilor), statul membru emitent și generația cardului care a creat evenimentul, — numărul de evenimente similare care au survenit în ziua respectivă.
Conflict de carduri	— cele mai recente 10 evenimente.	— data și ora începerii evenimentului, — data și ora încheierii evenimentului, — tipul și numărul cardului (cardurilor), statul membru emitent și generația celor două carduri care au creat conflictul.
Încheierea incorectă a ultimei sesiuni	— cele mai recente 10 evenimente.	— data și ora introducerii cardului, — tipul, numărul, statul membru emitent și generația cardului (cardurilor), — datele din ultima sesiune, așa cum au fost citite de pe card: — data și ora introducerii cardului, — VRN, statul membru de înmatriculare și generația VU.
Întreruperea alimentării cu energie electrică (2)	— evenimentul care a durat cel mai mult în fiecare din ultimele 10 zile de producere a unui eveniment, — cele mai de durată 5 evenimente din ultimele 365 de zile.	— data și ora începerii evenimentului, — data și ora încheierii evenimentului, — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului, — numărul de evenimente similare care au survenit în ziua respectivă.
Eroare de comunicare cu dispozitivul de comunicare la distanță	— evenimentul care a durat cel mai mult în fiecare din ultimele 10 zile de producere a unui eveniment, — cele mai de durată 5 evenimente din ultimele 365 de zile.	— data și ora începerii evenimentului, — data și ora încheierii evenimentului, — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului, — numărul de evenimente similare care au survenit în ziua respectivă.
Absența informațiilor privind poziția din receptorul GNSS	— evenimentul care a durat cel mai mult în fiecare din ultimele 10 zile în care s-a produs, — cele mai de durată 5 evenimente din ultimele 365 de zile.	— data și ora începerii evenimentului, — data și ora încheierii evenimentului, — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului, — numărul de evenimente similare care au survenit în ziua respectivă.
Eroare privind datele de deplasare	— evenimentul care a durat cel mai mult în fiecare din ultimele 10 zile în care s-a produs, — cele mai de durată 5 evenimente din ultimele 365 de zile.	— data și ora începerii evenimentului, — data și ora încheierii evenimentului, — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului, — numărul de evenimente similare care au survenit în ziua respectivă.

Eveniment	Reguli de stocare	Date care trebuie înregistrate pentru fiecare eveniment
Conflict privind deplasarea vehiculului	— evenimentul care a durat cel mai mult în fiecare din ultimele 10 zile în care s-a produs, — cele mai de durată 5 evenimente din ultimele 365 de zile.	— data și ora începerii evenimentului, — data și ora încheierii evenimentului, — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului, — numărul de evenimente similare care au survenit în ziua respectivă.
Tentativă de încălcare a securității	cele mai recente 10 evenimente, pe tipuri de evenimente.	— data și ora începerii evenimentului, — data și ora încheierii evenimentului (dacă sunt relevante), — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului, — tipul evenimentului.
Conflict temporal	— evenimentul care a durat cel mai mult în fiecare din ultimele 10 zile în care s-a produs, — cele mai de durată 5 evenimente din ultimele 365 de zile.	— data și ora indicate de aparatura de înregistrare — data și ora GNSS, — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului, — numărul de evenimente similare care au survenit în ziua respectivă.

4) CODURI ALE EVENIMENTELOR DISPONIBILE FĂRĂ ACORDUL PREALABIL AL CONDUCĂTORULUI AUTO

Eveniment	Reguli de stocare	Date care trebuie înregistrate pentru fiecare eveniment
Conducere fără un card adecvat	— evenimentul care a durat cel mai mult în fiecare din ultimele 10 zile în care s-a produs, — cele mai de durată 5 evenimente din ultimele 365 de zile.	— data și ora începerii evenimentului, — data și ora încheierii evenimentului, — tipul și numărul cardului (cardurilor), statul membru emitent și generația oricărui card introdus la începutul și/sau la încheierea evenimentului, — numărul de evenimente similare care au survenit în ziua respectivă.
Introducerea cardului în timpul conducerii	— ultimul eveniment survenit în fiecare dintre ultimele 10 zile de producere a unui eveniment,	— data și ora evenimentului, — tipul, numărul, statul membru emitent și generația cardului (cardurilor), — numărul de evenimente similare care au survenit în ziua respectivă
Depășirea limitei de viteză (1)	— cel mai grav eveniment survenit în fiecare dintre ultimele 10 zile în care acesta s-a produs (adică cel în care s-a înregistrat cea mai mare viteză medie), — cele mai grave cinci evenimente survenite în ultimele 365 de zile. — primul eveniment survenit după ultima etalonare,	— data și ora începerii evenimentului, — data și ora încheierii evenimentului, — viteza maximă măsurată pe parcursul evenimentului, — media aritmetică a vitezei măsurate în timpul evenimentului, — tipul și numărul cardului (cardurilor), statul membru emitent și generația cardului de conducător auto (dacă este cazul), — numărul de evenimente similare care au survenit în ziua respectivă.

5) CODURI ALE DATELOR PRIVIND ANOMALIILE DISPONIBILE FĂRĂ ACORDUL PREALABIL AL CONDUCĂTORULUI AUTO

Anomalie	Reguli de stocare	Date care trebuie înregistrate pentru fiecare anomalie
Anomalie a cardului	— cele mai recente 10 anomalii ale cardului de conducător auto.	— data și ora începerii anomaliei, — data și ora încheierii anomaliei, — tipul, numărul, statul membru emitent și generația cardului (cardurilor).
Anomalii ale aparaturii de înregistrare	— cele mai recente 10 anomalii pentru fiecare tip de anomalie, — prima anomalie survenită după ultima etalonare.	— data și ora începerii anomaliei, — data și ora încheierii anomaliei, — tipul de anomalie, — tipul, numărul și statul membru emitent al cardului (cardurilor), precum și generația oricărui card introdus la începutul și/sau la încheierea anomaliei.

Această anomalie este declanșată în cazul survenirii oricăreia dintre următoarele anomalii în celelalte moduri decât modul de etalonare:

— Anomalie internă a VU

— Anomalie a imprimantei

— Anomalie a afișajului

— Anomalie la descărcare

— Anomalie a senzorului

— Anomalie a receptorului GNSS sau a echipamentului GNSS extern

— Anomalie a dispozitivului de comunicare la distanță

6) EVENIMENTE ȘI ANOMALII SPECIFICE PRODUCĂTORULUI, DISPONIBILE FĂRĂ ACORDUL PREALABIL AL CONDUCĂTORULUI AUTO

Eveniment sau anomalie	Reguli de stocare	Date care trebuie înregistrate pentru fiecare eveniment
Se specifică de către producător	Se specifică de către producător	Se specifică de către producător

ANEXA 2

DIAGRAMELE SECVENȚELOR PENTRU SCHIMBURILE DE MESAJE CU UNITATEA ITS.

Figura 1

Diagrama secvențelor pentru încercarea de validare a PIN-ului

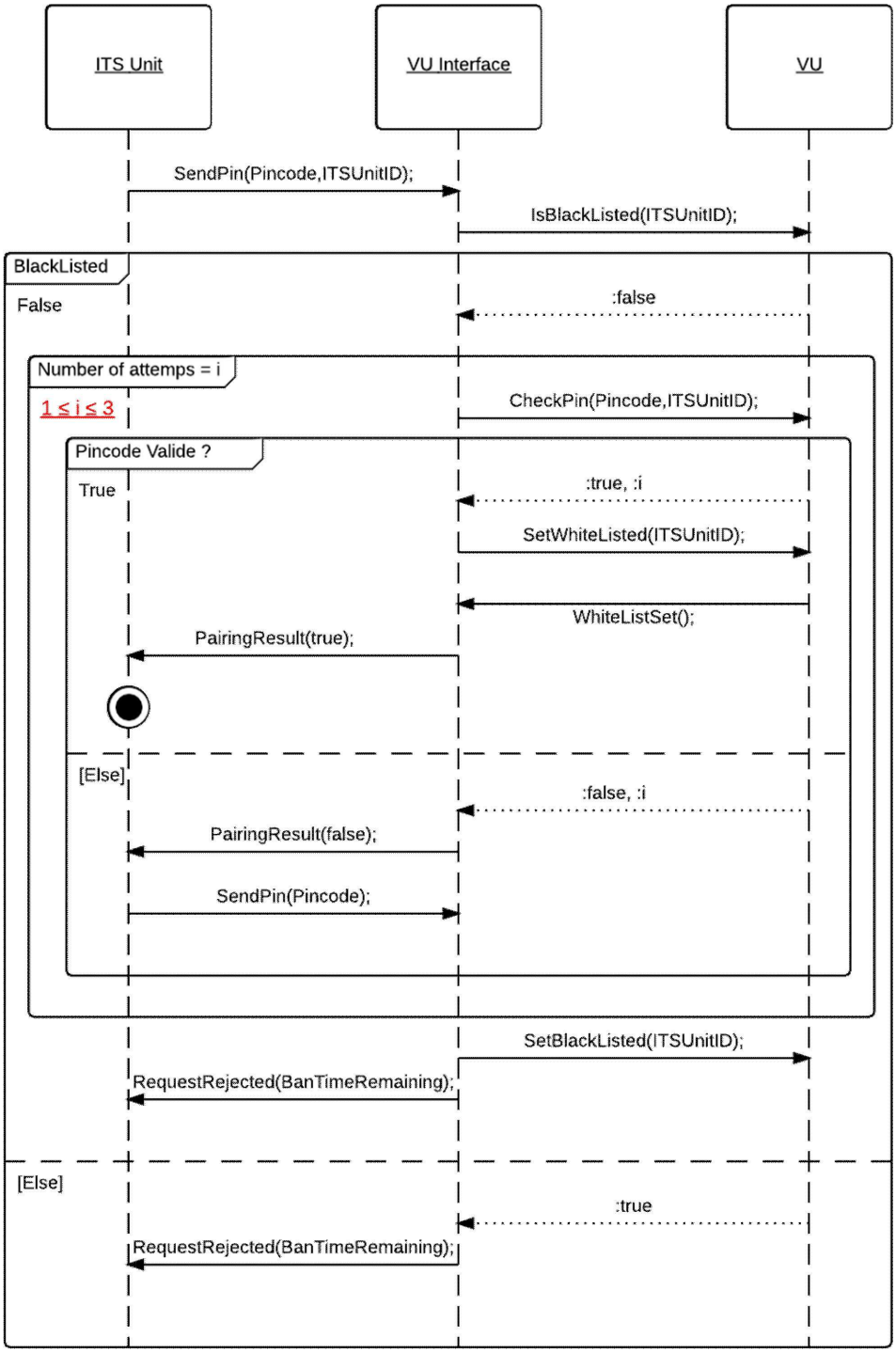


Figura 2

Diagrama secvențelor pentru verificarea autorizării unității ITS

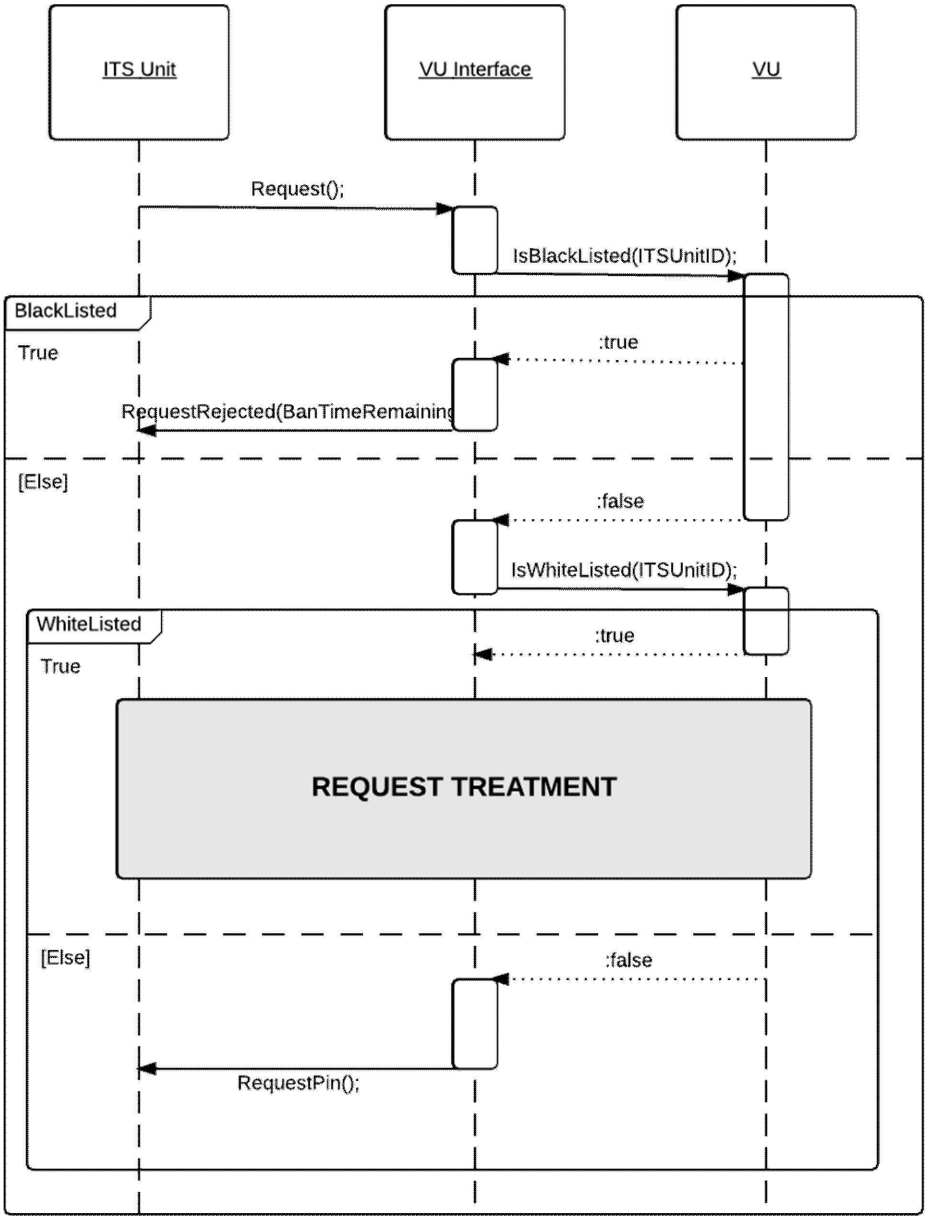


Figura 3

Diagrama secvențelor pentru prelucrarea unei solicitări de date clasificate ca fiind publice (după introducerea corectă a PIN-ului)

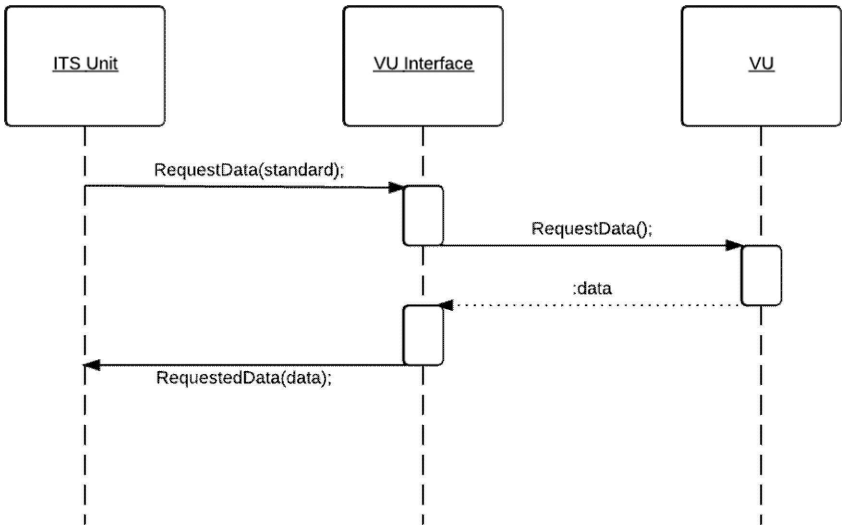


Figura 4

Diagrama secvențelor pentru prelucrarea unei solicitări de date clasificate ca având caracter personal (după introducerea corectă a PIN-ului)

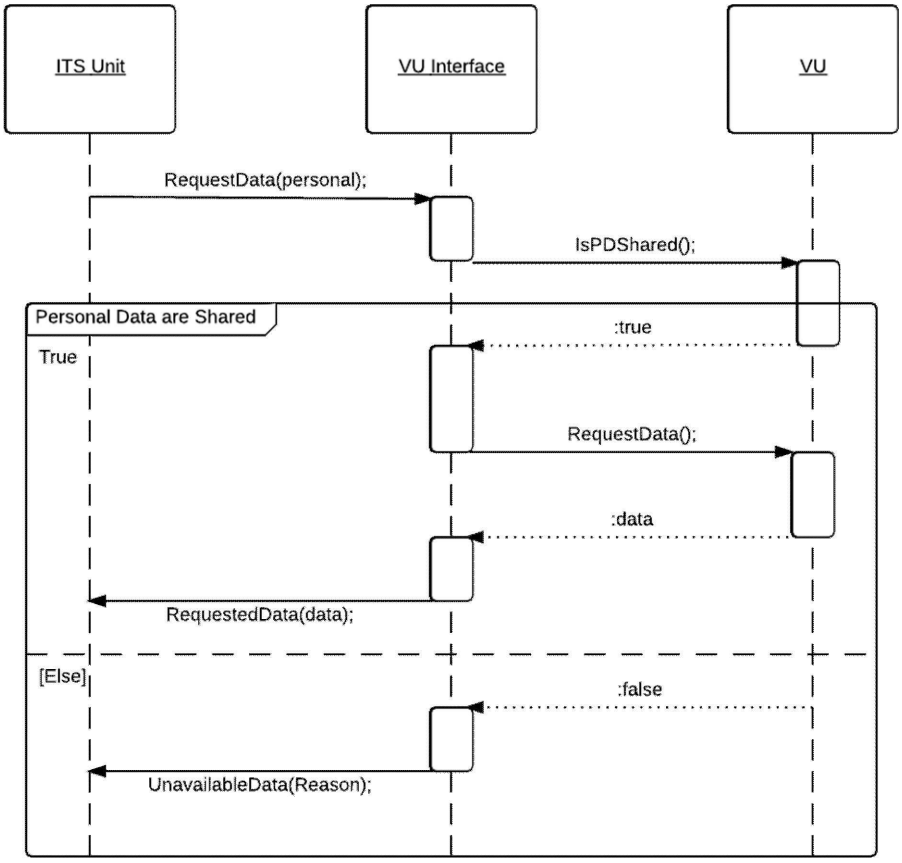
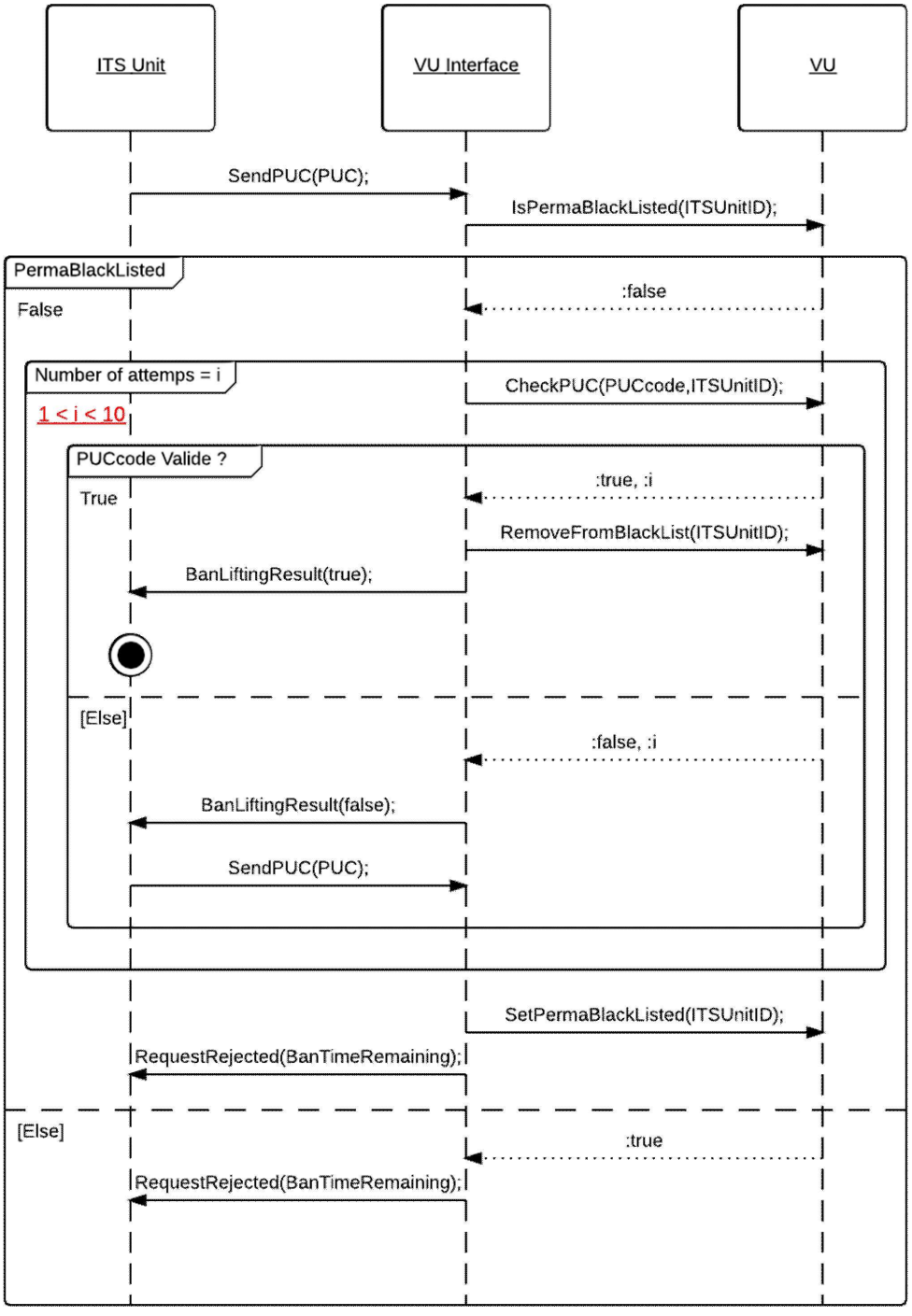


Figura 5

Diagrama secvențelor pentru încercarea de validare a PUC-ului



ANEXA 3

SPECIFICAȚII ASN. 1

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

       CompleteMessage ::=SEQUENCE{
              header Header,
              data DataField,
              checksum Checksum
       }

       ----------------
       --HEADER TYPES--
       ----------------


       Header::=SEQUENCE{
              tgt IDList,
              src IDList,
              len BIT STRING (1..255)
       }

       vuID BIT STRING ::= 'EE'H
       IDList ::=CHOICE{
              vu BIT STRING (vuID),
              itsUnits SEQUENCE OF BIT STRING,
                     --Default hex Value:A0, redefined after first message exchange--
                     --Each ID will be linked to the Bluetooth ID of the device--
              ...
       }

       --------------------
       --DATAFIELDS TYPES--
       --------------------
       DataField ::=SEQUENCE{
              sid BIT STRING,
              trtp BIT STRING,
              subMBytes SubMessageBytes,
              dataField Content,
              ...
       }

       SubMessageBytes ::= SEQUENCE{
              currentSubM BIT STRING,
              totalSubM BIT STRING
       }

       Content ::= CHOICE{
              requestPIN RequestPIN,
              sendITSID SendITSID,
              sendPin SendPIN,
```

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

	----------
	---Utils--
	----------

	PUC ::= SEQUENCE (SIZE(8)) OF
	INTEGER (SIZE(0..9))

	PIN ::=	SEQUENCE (SIZE(4)) OF
		INTEGER (SIZE(0..9))

	--------------------------
	--Messages From ITS Unit--
	--------------------------

	SendPIN {PIN:pin} ::= SEQUENCE {
		sid BIT STRING ('03'H),
		pin PIN (pin)
	}

	SendPUC {PUC:puc} ::= SEQUENCE {
		sid BIT STRING ('05'H),
		puc PUC (puc)
	}
	--------------------
	--Messages From VU--
	--------------------

	PairingResult ::= SEQUENCE{
		sid BIT STRING ('04'H),
		result BOOLEAN
	}

	RequestPIN {MType:receivedRequest}::= SEQUENCE{
		sid BIT STRING ('01'H)
	}

	RequestRejected ::= SEQUENCE{
		sid BIT STRING ('07'H),
		banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

	BanLiftingResult ::= SEQUENCE{
		sid BIT STRING ('06'H),
		result BOOLEAN
	}
END
```

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	---------------------------
	--Complete Tachograph Data--
	---------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document–

```

```
Time ::= SEQUENCE{
	seconds INTEGER (0..59.75), --increment: 0.25s--
	minutes INTEGER (0..59), --increment: 1min--
	hours INTEGER (0..23), --increment: 1h--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	month INTEGER (1..12), --increment: 1month--
	year INTEGER (1985..2235), --increment: 1year--
	locMinOffset INTEGER (-59..59), --increment: 1min--
	locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
	month INTEGER (1..12), --increment: 1month--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
	codePageSurname UTF8String, --See ISO/IEC 8859--
	surname UTF8String,
	codePageFirstname UTF8String, --See ISO/IEC 8859--
	firstname UTF8String,
}

--------------------
--Message Content--
--------------------

StandardTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardTachData),
	personal BOOLEAN (FALSE),
	data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalTachData),
	personal BOOLEAN (TRUE),
	data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&gnssData),
	personal BOOLEAN (TRUE),
	data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardEventData),
	personal BOOLEAN (FALSE),
	data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalEventData),
	personal BOOLEAN (TRUE),
	data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

```
243                 trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                 personal BOOLEAN (FALSE),
245                 data StandardFault
246           }
247
248           ManufacturerDataContent ::= SEQUENCE{
249                 trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                 personal BOOLEAN (TRUE),
251                 ...
252           }
253
254           ---------------
255           --DATA SHEETS--
256           ---------------
257
258           --Data sheet format follows ISO 16844-7.--
259           StandardTachyDataSheet ::= SEQUENCE{
260                 vin UTF8String (SIZE(17)),
261                 calibrationDate Date,
262                 driveRecognize INTEGER (2 UNION 12),
263                 driverCardDriver1 INTEGER (2 UNION 12),
264                 driverCardDriver2 INTEGER (2 UNION 12),
265                 timeDate Time,
266                 highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267     5m--
268                 serviceComponentIdentification INTEGER (0..255),
269                 serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270     -
271                 nextCalibrationDate Date,
272                 speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                 tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                 tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                 outOfScopeCondition INTEGER(2 UNION 12),
276                 modeOfOperation INTEGER (0..4...), --Maximum 250--
277                 registeringMemberState UTF8String,
278           vehicleRegistrationNumber SEQUENCE {
279                       codePageVRN INTEGER (0..255),
280                       vrn OCTET STRING (SIZE(13)),
281                 },
282                 tachographNextMandatoryDownloadDate Date,
283                 ...
284           }
285
286           PersonalTachyDataSheet ::= SEQUENCE{
287                 tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                 driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289     UNION 1012...),
290                 driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291     UNION 1012...),
292
293                 driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294     1002 UNION
295                                                   1012 UNION 1102 UNION 1112 UNION
296     10002 UNION 10012 UNION
297                                                   10102 UNION 10112 UNION 11002 UNION
298     11012...),
299                 driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300     1002 UNION
```

```
                                                    1012 UNION 1102 UNION 1112 UNION
    10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
    11012...),

                overSpeed INTEGER (2 UNION 12),
                driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
    FROM TACHO REGULATION--
                driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
    FROM TACHO REGULATION--
                driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
                driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
                driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
    increment: 1min--
                driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
    increment: 1min--
                driver1Name DriverName,
                driver2Name DriverName,
                driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
    --increment: 1min--
                driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
    --increment: 1min--
                engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
                driver1EndOfLastDailyRestPeriod Time,
                driver2EndOfLastDailyRestPeriod Time,
                driver1EndOfLastWeeklyRestPeriod Time,
                driver2EndOfLastWeeklyRestPeriod Time,
                driver1EndOfSecondLastWeeklyRestPeriod Time,
                driver2EndOfSecondLastWeeklyRestPeriod Time,
                driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
    -
                driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
    -
                driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
    1min--
                driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
    1min--
                driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
    increment: 1min--
                driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
    increment: 1min--
                driver1CardExpiryDate Date,
                driver2CardExpiryDate Date,
                driver1CardNextMandatoryDownloadDate Date,
                driver2CardNextMandatoryDownloadDate Date,
                driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
    increment: 1min--
                driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
    increment: 1min--
                driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
                driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
                driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
    increment: 1min--
                driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
    increment: 1min--
                driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
                driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
                driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
                driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367   1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369   1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385   END
386
387   EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390   about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408   CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410   AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

```
PersonalEvent ::= CHOICE{
	lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
	cardInsertionWhileDriving CardInsertionWhileDriving,
	overSpeeding OverSpeeding,
	...
}

StandardFault ::= CHOICE{
	cardFault CardFault,
	recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
	date GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
```

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

```
537                     numberOfSimilarEvent INTEGER
538             }
539
540             PositionDataError ::= SEQUENCE{
541                     beginDate GeneralizedTime,
542                     endDate GeneralizedTime,
543                     carsdType SEQUENCE OF UTF8String,
544                     cardsNumber SEQUENCE OF INTEGER,
545                     issuingMemberState SEQUENCE OF NationAlpha,
546                     cardsGeneration SEQUENCE OF INTEGER,
547                     numberOfSimilarEvent INTEGER
548             }
549
550             MotionDataError ::= SEQUENCE{
551                     beginDate GeneralizedTime,
552                     endDate GeneralizedTime,
553                     carsdType SEQUENCE OF UTF8String,
554                     cardsNumber SEQUENCE OF INTEGER,
555                     issuingMemberState SEQUENCE OF NationAlpha,
556                     cardsGeneration SEQUENCE OF INTEGER,
557                     numberOfSimilarEvent INTEGER
558             }
559
560             VehicleMotionConflict ::= SEQUENCE{
561                     beginDate GeneralizedTime,
562                     endDate GeneralizedTime,
563                     carsdType SEQUENCE OF UTF8String,
564                     cardsNumber SEQUENCE OF INTEGER,
565                     issuingMemberState SEQUENCE OF NationAlpha,
566                     cardsGeneration SEQUENCE OF INTEGER,
567                     numberOfSimilarEvent INTEGER
568             }
569
570             SecurityBreachAttempt ::= SEQUENCE{
571                     beginDate GeneralizedTime,
572                     endDate GeneralizedTime OPTIONAL,
573                     carsdType SEQUENCE OF UTF8String,
574                     cardsNumber SEQUENCE OF INTEGER,
575                     issuingMemberState SEQUENCE OF NationAlpha,
576                     numberOfSimilarEvent INTEGER,
577                     typeOfEvent SecurityBreachEvent
578             }
579
580
581             TimeConflict ::= SEQUENCE{
582                     beginDate GeneralizedTime,
583                     endDate GeneralizedTime,
584                     carsdType SEQUENCE OF UTF8String,
585                     cardsNumber SEQUENCE OF INTEGER,
586                     issuingMemberState SEQUENCE OF NationAlpha,
587                     cardsGeneration SEQUENCE OF INTEGER,
588                     numberOfSimilarEvent INTEGER
589             }
590
591             ---------------
592             --FAULTS LIST--
593             ---------------
594
595             CardFault ::= SEQUENCE{
```

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

Apendicele 14.

FUNCȚIA DE COMUNICARE LA DISTANȚĂ

CUPRINS

1 INTRODUCERE 450

2 DOMENIU DE APLICARE 451

3 ACRONIME, DEFINIȚII ȘI NOTAȚII 452

4 SCENARII OPERAȚIONALE 454

4.1 Prezentare generală 454

4.1.1 Condiții prealabile pentru transferul de date prin interfața DSRC de 5,8 GHz 454

4.1.2 Profilul 1a: prin intermediul unui cititor pentru comunicarea în scopul detectării timpurii la distanță orientat manual sau montat temporar în afara părții carosabile și orientat 455

4.1.3 Profilul 1b: prin intermediul unui cititor pentru comunicarea în scopul detectării timpurii la distanță (REDCR) montat pe vehicul și direcționat 456

4.2 Securitate/integritate 456

5 CONCEPȚIA ȘI PROTOCOALELE COMUNICĂRII LA DISTANȚĂ 456

5.1 Concepție 456

5.2 Fluxul de lucru 459

5.2.1 Operațiuni 459

5.2.2 Interpretarea datelor primite prin comunicarea DSRC 461

5.3 Parametri ai interfeței fizice DSRC pentru comunicarea la distanță 461

5.3.1 Constrângeri legate de amplasament 461

5.3.2 Parametri ai legăturii descendente și ai legăturii ascendente 461

5.3.3 Concepția antenei 466

5.4 Cerințe de protocol DSRC pentru RTM 466

5.4.1 Prezentare generală 466

5.4.2 Comenzi 469

5.4.3 Secvența comenzilor de interogare 469

5.4.4 Structuri de date 470

5.4.5 Elementele *RtmData*, acțiunile realizate și definiții 472

5.4.6 Mecanismul de transfer al datelor 476

5.4.7 Descriere detaliată a tranzacției DSRC 476

5.4.8 Descrierea tranzacției de testare DRSC 486

5.5 Compatibilitate cu Directiva 2015/71/CE 490

5.5.1 Prezentare generală 490

5.5.2 Comenzi 490

5.5.3 Secvența comenzilor de interogare 490

5.5.4 Structuri de date 490

5.5.5 Modulul ASN. 1 pentru tranzacția DRSC OWS 491

5.5.6 Elementele *OwsData*, acțiunile realizate și definiții 492

5.5.7 Mecanismele de transfer al datelor 492

5.6 Transferul de date între DSRC-VU și VU 492

5.6.1 Conexiunea fizică și interfețele 492

5.6.2 Protocolul de aplicație 493

5.7 Gestionarea erorilor 494

5.7.1 Înregistrarea și comunicarea datelor în DSRC-VU 494

5.7.2 Erori de comunicare fără fir 494

6 TESTELE DE OPERAȚIONALITATE ȘI DE VERIFICARE PERIODICĂ PENTRU FUNCȚIA DE COMUNICARE LA DISTANȚĂ 496

6.1 Generalități 496

6.2 ECHO 496

6.3 Testele de validare a conținutului de date securizate 496

1 INTRODUCERE

Prezentul apendice specifică detaliile privind proiectarea și procedurile care trebuie urmate pentru a utiliza funcția de comunicare la distanță („comunicarea”), astfel cum se prevede la articolul 9 din Regulamentul (UE) nr. 165/2014 („regulamentul”).

DSC_1 Regulamentul (UE) nr. 165/2014 stabilește faptul că tahograful trebuie să fie dotat cu o funcție de comunicare la distanță care să permită agenților autorităților de control competente să citească informații din tahografele vehiculelor care trec pe lângă ei, prin utilizarea unui echipament de interogare la distanță [cititorul pentru comunicarea în scopul detectării timpurii la distanță (*Remote early detection communication reader* – REDCR)], mai precis un echipament de interogare care se conectează fără fir folosind interfețe DSRC (*Dedicated Short Range Communication*) de 5,8 GHz conforme cu CEN.

Este important să se înțeleagă faptul că această funcție are ca unic scop să servească drept prefiltru pentru selectarea vehiculelor în vederea unei inspecții mai amănunțite și că nu înlocuiește procesul de inspecție formal stabilit în dispozițiile Regulamentului (UE) nr. 165/2014. A se vedea considerentul 9 din preambulul prezentului regulament, conform căruia comunicarea dintre tahograf și autoritățile de control în scopul controlului în trafic facilitează controalele selective în trafic.

DSC_2 *Datele* trebuie comunicate prin intermediul *comunicării,* care trebuie să constea într-o interacțiune fără fir folosind comunicații fără fir DSRC de 5,8 GHz în conformitate cu prezentul apendice, și testate pe baza parametrilor corespunzători din EN 300 674-1 [*Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)*].

DSC_3 *Comunicarea* cu echipamentul de comunicare trebuie stabilită doar atunci când este solicitată de echipamentul autorității de control competente care utilizează mijloace de radiocomunicație conforme [*cititorul pentru comunicarea în scopul detectării timpurii la distanță (REDCR)*].

DSC_4 *Datele* trebuie securizate, pentru a se asigura integritatea.

DSC_5 Accesul la *datele* comunicate trebuie limitat la autoritățile de control competente care sunt autorizate să verifice încălcările Regulamentului (CE) nr. 561/2006 și ale Regulamentului (UE) nr. 165/2014 și la ateliere, în măsura în care acest acces este necesar pentru a se verifica funcționarea corectă a tahografului.

DSC_6 *Datele* transmise în timpul *comunicării* trebuie limitate la datele necesare pentru efectuarea de controale selective în trafic ale vehiculelor al căror tahograf este posibil să fi fost manipulat sau utilizat abuziv.

DSC_7 Integritatea și securitatea datelor trebuie obținute prin securizarea *datelor* din cadrul unității montate pe vehicul (VU) și transmiterea doar a datelor utile securizate și a datelor legate de securitate (a se vedea 5.4.4) prin mediul de comunicare fără fir DSRC de 5,8 GHz, ceea ce înseamnă că doar persoanele autorizate din cadrul autorităților de control competente dispun de mijloacele necesare pentru înțelegerea datelor transmise prin *comunicare* și pentru verificarea autenticității acestora. A se vedea apendicele 11 – Mecanisme de securitate comune.

DSC_8 *Datele* trebuie să conțină o marcă temporală care să indice când au fost actualizate ultima dată.

DSC_9 Conținutul datelor de securitate trebuie să fie cunoscut și controlat doar de autoritățile de control competente și de părțile cărora acestea le împărtășesc informațiile respective și nu intră sub incidența prevederilor *comunicării* care face obiectul prezentului apendice, cu excepția cazului în care *comunicarea* prevede transferarea unui pachet de date de securitate împreună cu fiecare pachet de date utile.

DSC_10 Aceeași arhitectură și același echipament trebuie să poată fi folosite pentru a obține alte concepte de date (precum „cântărire–la-bord") utilizând arhitectura specificată.

DSC_11 Pentru clarificare, în conformitate cu dispozițiile Regulamentului (UE) nr. 165/2014 (articolul 7), datele referitoare la identitatea conducătorului auto nu sunt comunicate prin intermediul *comunicării*.

2 DOMENIU DE APLICARE

Scopul prezentului apendice este să precizeze modul în care agenții autorităților de control competente utilizează o comunicare DSRC fără fir de 5,8 GHz specificată pentru a obține de la distanță date (*datele*) de la un vehicul vizat, care identifică faptul că este posibil ca vehiculul vizat să încalce Regulamentul (UE) nr. 165/2014 și că ar trebui să fie avut în vedere pentru oprirea în scopul unei investigații mai amănunțite.

Regulamentul (UE) nr. 165/2014 impune ca datele colectate să se limiteze la sau să țină de date care identifică o potențială încălcare, conform definiției de la articolul 9 din Regulamentul (UE) nr. 165/2014.

În acest scenariu, timpul disponibil pentru comunicare este limitat, deoarece *comunicarea* este selectivă și concepută să fie cu rază scurtă de acțiune. În plus, aceleași mijloace de comunicare ca pentru monitorizarea de la distanță a tahografelor (RTM) pot fi de asemenea utilizate de autoritățile de control competente pentru alte aplicații (precum greutățile și dimensiunile maxime ale vehiculelor grele de marfă definite în Directiva 2015/719/CE), iar aceste operațiuni pot fi separate sau secvențiale, la discreția autorităților de control competente.

Prezentul apendice precizează:

— Echipamentele, procedurile și protocoalele de comunicare care trebuie folosite pentru realizarea *comunicării*.

— Standardele și regulamentele cu care trebuie să fie conform echipamentul radio.

— Prezentarea *datelor* către echipamentul de *comunicare*.

— Procedurile de interogare și de descărcare și secvența de operațiuni.

— *Datele* de transferat.

— Potențiala interpretare a *datelor* transferate prin intermediul *comunicării*.

— Prevederile referitoare la datele de securitate legate de *comunicare*.

— Disponibilitatea *datelor* pentru autoritățile de control competente.

— Modul în care *cititorul pentru comunicarea în scopul detectării timpurii la distanță* poate solicita concepte diferite de date privind mărfurile și parcul auto („freight and fleet").

Pentru clarificare, prezentul apendice nu precizează:

— Colectarea *datelor* și gestionarea acestora în cadrul VU [care trebuie să depindă de concepția produsului, în afara cazului în care sunt specificate în altă parte a Regulamentului (UE) nr. 165/2014].

— Forma de prezentare a datelor colectate către agentul autorităților de control competente, și nici criteriile care trebuie folosite de autoritățile de control competente pentru a decide ce vehicule să fie oprite [care trebuie să depindă de concepția produsului, în afara cazului în care sunt specificate în altă parte a Regulamentului (UE) nr. 165/2014 sau într-o decizie de politică a autorităților de control competente]. Pentru clarificare: *comunicarea* doar pune *datele* la dispoziția autorităților de control competente pentru ca acestea să poată lua decizii în cunoștință de cauză.

— Prevederi referitoare la securitatea datelor (precum criptarea) pentru conținutul *datelor* (care sunt specificate în apendicele 11 – Mecanisme de securitate comune).

— Detalii privind orice alte concepte de date în afara RTM care ar putea fi obținute utilizând aceeași arhitectură și același echipament.

— Detalii privind comportamentul și gestionarea dintre VU-uri și DSRC-VU, și nici privind comportamentul în cadrul DSRC-VU (în afara furnizării *datelor* atunci când sunt solicitate de un REDCR).

3 ACRONIME, DEFINIȚII ȘI NOTAȚII

În prezentul apendice sunt utilizate următoarele acronime și definiții specifice prezentului apendice:

Antena	dispozitiv electric care transformă puterea electrică în unde radio și invers, utilizat în combinație cu un transmițător radio sau cu un receptor radio. Atunci când se află în funcțiune, un transmițător radio furnizează un curent electric care oscilează la frecvența radio a terminalelor antenei, iar antena radiază energia din curent sub formă de unde electromagnetice (unde radio). La recepție, o antenă interceptează o parte din puterea unei unde electromagnetice pentru a produce o foarte mică tensiune la terminalele sale, care este aplicată receptorului pentru a fi amplificată.
Comunicarea	schimb de informații/date între un DSRC-REDCR și o DSRC-VU în conformitate cu secțiunea 5, într-o relație *master-slave*, pentru a obține datele.
Datele	date securizate într-un format definit (a se vedea 5.4.4) solicitate de *DSRC-REDCR* și furnizate *DSRC-REDCR* de către *DSRC-VU* printr-o legătură DSRC de 5,8 GHz, definită la punctul 5 de mai jos.
Regulamentul (UE) nr. 165/2014	Regulamentul (UE) nr. 165/2014 al Parlamentului European și al Consiliului din 4 februarie 2014 privind tahografele în transportul rutier, de abrogare a Regulamentului (CEE) nr. 3821/85 al Consiliului privind aparatura de înregistrare în transportul rutier și de modificare a Regulamentului (CE) nr. 561/2006 al Parlamentului European și al Consiliului privind armonizarea anumitor dispoziții ale legislației sociale în domeniul transporturilor rutiere.
AID	Identificator de aplicație
BLE	Bluetooth de energie redusă (*Bluetooth Low Energy*)
BST	Tabel de serviciu al radiobalizei

CIWD	Introducerea cardului în timpul conducerii
CRC	Verificare redundantă ciclică
DSC (n)	Identificator al unei cerințe privind un apendice DSRC specific
DSRC	Comunicații specializate cu rază scurtă de acțiune
DSRC-REDCR	DSRC – cititor pentru comunicarea în scopul detectării timpurii la distanță.
DSRC-VU	DSRC – unitate montată pe vehicul. Acesta este „echipamentul de comunicare la distanță" definit în anexa 1C.
DWVC	Conducere fără un card valabil
EID	Identificator de element
LLC	Controlul legăturii logice
LPDU	Unitate de date a protocolului LLC
OWS	Sistem de cântărire la bord
PDU	Unitate de date pentru protocol
REDCR	Cititor pentru comunicarea în scopul detectării timpurii la distanță. Acesta este „cititorul pentru comunicarea în scopul detectării timpurii la distanță" definit în anexa 1C.
RTM	Monitorizarea de la distanță a tahografelor
SM-REDCR	Modul de securitate-Cititor pentru comunicarea în scopul detectării timpurii la distanță
TARV	Aplicații telematice pentru vehicule reglementate (seria de standarde ISO 15638)
VU	Unitate montată pe vehicul
VUPM	Memoria utilă a unității montate pe vehicul
VUSM	Modulul de securitate al unității montate pe vehicul
VST	Tabel de serviciu al vehiculului
WIM	Cântărire în mers
WOB	Cântărire la bord

Specificația definită în prezentul apendice se referă la toate sau la o parte din următoarele regulamente și standarde și depinde de acestea. În cadrul clauzelor din prezentul apendice sunt specificate standardele relevante sau clauzele relevante ale standardelor. În cazul oricărei contradicții, clauzele din prezentul apendice prevalează. În cazul oricărei contradicții privind un aspect pentru care nu este stabilită nicio specificație clară în prezentul apendice, prevalează operarea conform ERC 70-03 (cu testare pe baza parametrilor corespunzători din EN 300 674-1), urmată în ordine descrescătoare a preferinței de EN 12795, EN 12253, EN 12834 și EN 13372, 6.2, 6.3, 6.4 și 7.1.

Regulamentele și standardele la care se face trimitere în prezentul apendice sunt următoarele:

[1] Regulamentul (UE) nr. 165/2014 al Parlamentului European și al Consiliului din 4 februarie 2014 privind tahografele în transportul rutier, de abrogare a Regulamentului (CEE) nr. 3821/85 al Consiliului privind aparatura de înregistrare în transportul rutier și de modificare a Regulamentului (CE) nr. 561/2006 al Parlamentului European și al Consiliului privind armonizarea anumitor dispoziții ale legislației sociale în domeniul transporturilor rutiere.

[2] Regulamentul (CE) nr. 561/2006 al Parlamentului European și al Consiliului din 15 martie 2006 privind armonizarea anumitor dispoziții ale legislației sociale în domeniul transporturilor rutiere, de modificare a Regulamentelor (CEE) nr. 3821/85 și (CE) nr. 2135/98 ale Consiliului și de abrogare a Regulamentului (CEE) nr. 3820/85 al Consiliului (Text cu relevanță pentru SEE).

[3] ERC 70-03 CEPT: Recomandarea ECC 70-03: *Relating to the Use of Short Range Devices (SRD)*

[4] ISO 15638 *Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).*

[5] EN 300 674-1 *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU).*

[6] EN 12253 *Road transport and traffic telematics – Dedicated short-range communication – Physical layer using microwave at 5.8 GHz.*

[7] EN 12795 *Road transport and traffic telematics – Dedicated short-range communication – Data link layer: medium access and logical link control.*

[8] EN 12834 *Road transport and traffic telematics – Dedicated short-range communication – Application layer.*

[9] EN 13372 *Road transport and traffic telematics – Dedicated short-range communication – Profiles for RTTT applications*

[10] ISO 14906 *Electronic fee collection — Application interface definition for dedicated short- range communication*

4 SCENARII OPERAȚIONALE

4.1 **Prezentare generală**

Regulamentul (UE) nr. 165/2014 prevede scenarii specifice și controlate în cadrul cărora trebuie utilizată *comunicarea*.

Scenariile compatibile sunt:

„Profilul de comunicare 1: Inspecție în afara părții carosabile folosind un cititor pentru comunicarea în scopul detectării timpurii la distanță, care comunică fără fir pe o rază scurtă de acțiune și care instigă o inspecție fizică în afara părții carosabile (master-:-slave).

Profil cititor 1a: prin intermediul unui cititor pentru comunicarea în scopul detectării timpurii la distanță orientat manual sau montat temporar în afara părții carosabile și orientat

Profil cititor 1b: prin intermediul unui cititor pentru comunicarea în scopul detectării timpurii la distanță montat pe vehicul și direcționat”.

4.1.1 *Condiții prealabile pentru transferul de date prin interfața DSRC de 5,8 GHz*

NOTĂ: pentru a înțelege contextul condițiilor prealabile, cititorul este rugat să consulte figura 14.3 de mai jos.

4.1.1.1 Datele stocate în VU

DSC_12 VU are responsabilitatea de a actualiza la fiecare 60 de secunde și de a menține datele care urmează să fie stocate în VU, fără nicio implicare a funcției de comunicare DSRC. Mijloacele prin care se realizează acest lucru sunt integrate în VU, specificate în Regulamentul (UE) nr. 165/2014, în anexa 1C secțiunea 3.19 „*Comunicare la distanță pentru controalele selective în trafic*” și nu sunt specificate în prezentul apendice.

4.1.1.2 Datele furnizate echipamentului DSRC-VU

DSC_13 VU are responsabilitatea de a actualiza datele tahografice DSRC (*datele*) ori de câte ori datele stocate în VU sunt actualizate, la intervalul stabilit în secțiunea 4.1.1.1 (DSC_12), fără nicio implicare a funcției de comunicare DSRC.

DSC_14 Datele furnizate de VU sunt utilizate ca bază pentru a completa și a actualiza *datele*; mijloacele prin care se realizează acest lucru sunt specificate în anexa 1C secțiunea 3.19 „*Comunicare la distanță pentru controalele selective în trafic*" sau, dacă nu există o astfel de specificație, depind de concepția produsului și nu sunt specificate în prezentul apendice. Pentru concepția conexiunii dintre echipamentul DSRC-VU și VU, vă rugăm să consultați secțiunea 5.6.

4.1.1.3 Conținutul datelor

DSC_15 Conținutul și formatul *datelor* trebuie să fie de așa natură încât, odată decriptate, să fie structurate și puse la dispoziție sub forma și în formatul specificate în secțiunea 5.4.4 din prezentul apendice (Structuri de date).

4.1.1.4 Prezentarea datelor

DSC_16 *Datele*, actualizate frecvent în conformitate cu procedurile stabilite în secțiunea 4.1.1.1, trebuie să fie securizate înainte de a fi prezentate către *DSRC-VU* și trebuie prezentate ca o valoare a conceptului de date securizate, pentru a fi stocate temporar în *DSRC-VU* ca versiunea curentă a *datelor*. Aceste date sunt transferate de la *VUSM* la funcția *VUPM* pentru DSRC. *VUSM* și *VUPM* sunt funcții, nu neapărat entități fizice. Forma instanțierii fizice pentru realizarea acestor funcții ține de concepția produsului, în afara cazului în care este specificată în altă parte a Regulamentului (UE) nr. 165/2014.

4.1.1.5 Datele de securitate

DSC_17 Datele de securitate (*securityData*), care cuprind datele necesare *REDCR* pentru a-și îndeplini funcția de decriptare a *datelor,* trebuie furnizate conform definiției din apendicele 11 (Mecanisme de securitate comune) și prezentate ca o valoare a conceptului de date, pentru stocarea temporară în *DSRC-VU* ca versiunea curentă a *securityData,* sub forma definită în secțiunea 5.4.4 din prezentul apendice.

4.1.1.6 Date VUPM disponibile pentru transfer prin interfața DSRC

DSC_18 Conceptul de date care trebuie să fie mereu disponibil în funcția VUPM pentru DSRC în vederea transferului imediat în urma solicitării *REDCR* este definit în secțiunea 5.4.4 pentru specificațiile complete privind modulul ASN.1.

Prezentare generală a profilului de comunicare 1

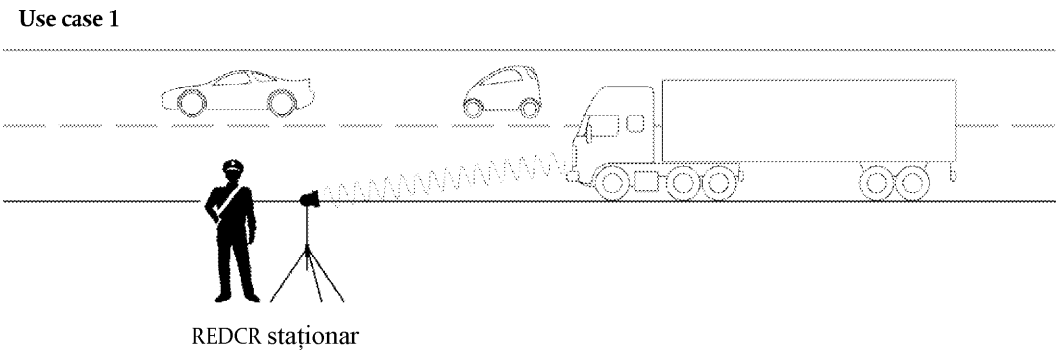
Acest profil se referă la cazul de utilizare în care un agent al autorităților de control competente folosește un cititor pentru comunicarea în scopul detectării timpurii la distanță ce comunică pe o rază scurtă de acțiune (interfețe DSRC de 5,8 GHz care funcționează conform ERC 70-03 și sunt testate pe baza parametrilor corespunzători din EN 300 674-1, conform descrierii din secțiunea 5) (*REDCR*) pentru a identifica de la distanță un vehicul care este posibil să încalce Regulamentul (UE) nr. 165/2014. Odată identificat, agentul autorităților de control competente care controlează interogarea decide dacă vehiculul ar trebui să fie oprit.

4.1.2 *Profilul 1a: prin intermediul unui cititor pentru comunicarea în scopul detectării timpurii la distanță orientat manual sau montat temporar în afara părții carosabile și orientat*

În acest caz de utilizare, agentul autorităților de control competente se află în afara părții carosabile și orientează un *REDCR* portabil ținut în mână ori montat pe un tripod sau un *REDCR* portabil similar dinspre marginea drumului către centrul parbrizului vehiculului vizat. Interogarea se realizează folosind interfețe DSRC de 5,8 GHz care funcționează conform ERC 70-03 și sunt testate pe baza parametrilor corespunzători din EN 300 674-1, conform descrierii din secțiunea 5. A se vedea figura 14.1 (cazul de utilizare 1).

Figura 14.1

Interogare cu REDCR staționar folosind DSRC de 5,8 GHz

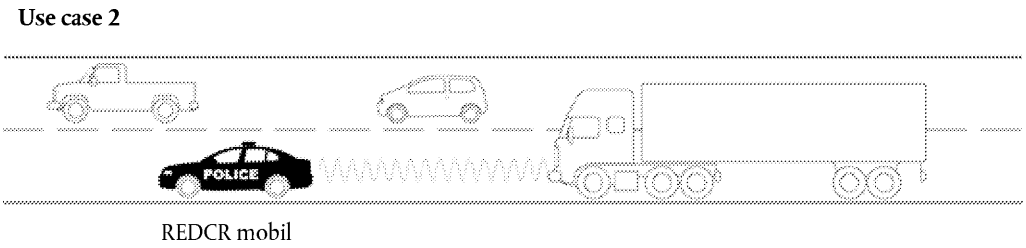


4.1.3 *Profilul 1b: prin intermediul unui cititor pentru comunicarea în scopul detectării timpurii la distanță (REDCR) montat pe vehicul și direcționat*

În acest caz de utilizare, agentul autorităților de control competente se află într-un vehicul în mișcare și fie orientează un *REDCR* portabil ținut în mână dinspre vehicul către centrul parbrizului vehiculului vizat, fie *REDCR-ul* este montat în sau pe vehicul astfel încât să țintească centrul parbrizului vehiculului vizat atunci când vehiculul pe sau în care este situat cititorul pentru comunicarea în scopul detectării timpurii la distanță se află într-o anumită poziție relevantă față de vehiculul vizat (de exemplu direct în fața acestuia în cadrul unui flux de trafic). Interogarea se realizează folosind interfețe DSRC de 5,8 GHz care funcționează conform ERC 70-03 și sunt testate pe baza parametrilor corespunzători din EN 300 674-1, conform descrierii din secțiunea 5. A se vedea figura 14.2. (Cazul de utilizare 2).

Figura 14.2

Interogare cu REDCR mobil folosind DSRC de 5,8 GHz



4.2 **Securitate/integritate**

Pentru a da posibilitatea de verificare a autenticității și integrității datelor descărcate prin comunicarea la distanță, *datele* securizate sunt verificate și decriptate în conformitate cu apendicele 11 – Mecanisme de securitate comune.

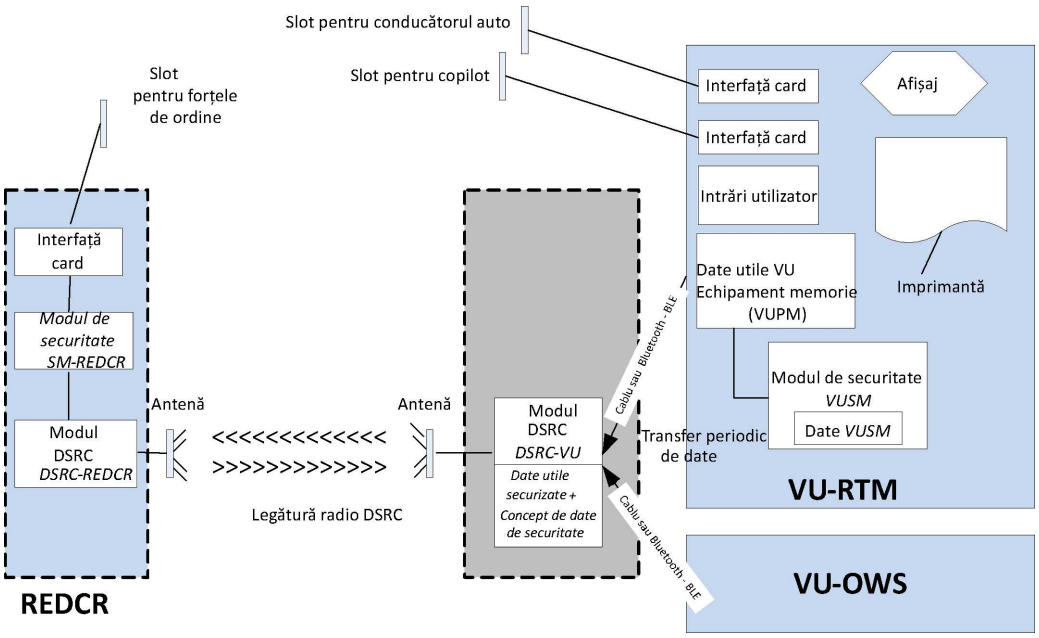
5 CONCEPȚIA ȘI PROTOCOALELE COMUNICĂRII LA DISTANȚĂ

5.1 **Concepție**

Concepția funcției de comunicare la distanță în cadrul tahografului inteligent este prezentată în figura 14.3.

Figura 14.3

Concepția funcției de comunicare la distanță



DSC_19 Următoarele funcții se află în VU:

— Modulul de securitate (*VUSM*). Această funcție prezentă în VU este responsabilă pentru securizarea *datelor* care urmează să fie transmise de la *DSRC-VU* către agentul autorităților de control competente prin comunicarea la distanță.

— Datele securizate sunt stocate în memoria VUSM. La intervalele de timp stabilite în secțiunea 4.1.1.1 (DSC_12), VU criptează și completează conceptul *RTMdata* (care cuprinde valorile conceptelor de date de securitate și de date utile stabilite mai jos în prezentul apendice) aflat în memoria DSRC-VU. Funcționarea modulului de securitate este definită în apendicele 11 (Mecanisme de securitate comune) și nu intră sub incidența prezentului apendice, cu excepția faptului că va trebui să furnizeze actualizări echipamentului de comunicare al VU de fiecare dată când se modifică datele din VUSM.

— Comunicarea dintre VU și DSRC-VU poate fi o comunicare prin cablu sau o comunicare prin Bluetooth de energie redusă (BLE), iar amplasarea fizică a DSRC-VU poate fi împreună cu antena de pe parbrizul vehiculului, în cadrul VU sau undeva între acestea.

— DSRC-VU trebuie să dispună de o sursă de energie electrică fiabilă, disponibilă în orice moment. Mijloacele prin care este alimentată cu energie electrică țin de deciziile de concepție.

— Memoria DSRC-VU trebuie să fie nevolatilă, pentru a menține datele în DSRC-VU chiar și atunci când contactul vehiculului este în poziția „oprit”.

— În cazul în care comunicarea dintre VU și DSRC-VU se face prin BLE și sursa de energie electrică este o baterie nereîncărcabilă, sursa de energie electrică a DSRC-VU trebuie înlocuită cu ocazia fiecărei inspecții periodice, iar producătorul DSRC-VU trebuie să fie responsabil pentru asigurarea faptului că sursa de energie electrică este adecvată pentru a rezista de la o inspecție periodică până la următoarea menținând accesul normal la date printr-un REDCR de-a lungul întregii perioade, fără defectări sau întreruperi.

— Echipamentul de „memorie utilă” al RTM VU (*VUPM*). Această funcție prezentă în VU este responsabilă pentru furnizarea și actualizarea *datelor*. Conținutul *datelor* („TachographPayload”) este definit în secțiunea 5.4.4/5.4.5 de mai jos și este actualizat la intervalul stabilit în secțiunea 4.1.1.1 (DSC_12).

— DSRC-VU. Această funcție, aflată în cadrul antenei sau conectată la antenă și în comunicare cu VU printr-o conexiune prin cablu sau fără fir (BLE), este cea care deține datele curente (*datele VUPM*) și gestionează răspunsul la o interogare transmisă prin mediul DSRC de 5,8 GHz. Deconectarea echipamentului DSRC sau apariția unor interferențe, în timpul utilizării normale a vehiculului, cu funcționarea echipamentului DSRC este considerată o încălcare a Regulamentului (UE) nr. 165/2014.

— Modulul de securitate (REDCR) (*SM-REDCR*) este funcția utilizată pentru a decripta datele care provin de la VU și a verifica integritatea acestora. Mijloacele prin care se realizează acest lucru sunt stabilite în apendicele 11 (Mecanisme de securitate comune) și nu sunt definite în prezentul apendice.

— Funcția echipamentului DSRC (REDCR) (*DSRC-REDCR*) cuprinde un transceiver de 5,8 GHz și programele asociate de firmware și de software, care gestionează *comunicarea* cu *DSRC-VU* în conformitate cu prezentul apendice.

— *DSRC-REDCR* interoghează *DSRC-VU* a vehiculului vizat și obține *datele* (*datele VUPM* curente ale vehiculului vizat) prin legătura DSRC și procesează și stochează datele primite în *SM-REDCR-ul* său.

— Antena *DSRC-VU* („antena”) trebuie poziționată astfel încât să optimizeze comunicarea DSRC dintre vehicul și antena aflată în afara părții carosabile (în general în sau aproape de centrul parbrizului vehiculului). Pentru vehiculele ușoare, este adecvată o instalare care corespunde părții superioare a parbrizului.

— În fața antenei sau aproape de antenă trebuie să nu existe obiecte metalice [de exemplu ecusoane, autocolante, benzi de folie antireflectorizantă (colorate), parasolare, ștergătorul de parbriz în poziția „oprit”] care pot interfera cu comunicarea.

— Antena trebuie montată în așa fel încât linia sa de vizare directă să fie aproximativ paralelă cu suprafața carosabilului.

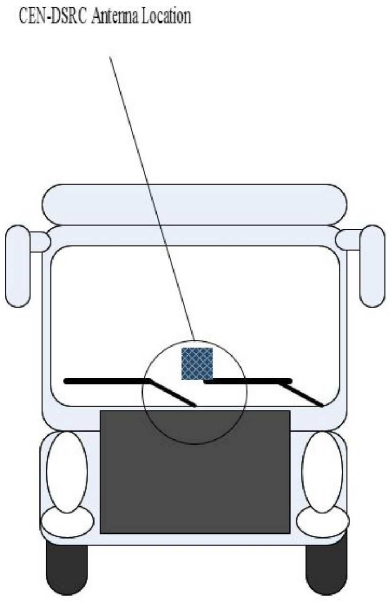
DSC_20 Antena și comunicarea trebuie să funcționeze conform ERC 70-03 și să fie testate pe baza parametrilor corespunzători din EN 300 674-1, conform descrierii din secțiunea 5. Antena și comunicarea pot utiliza tehnici de atenuare a riscului de interferențe radio, conform descrierii din raportul 228 al ECC, folosind de exemplu filtre în cadrul comunicării DSRC de 5,8 GHz conforme cu CEN.

DSC_21 Antena DSRC trebuie să fie conectată la echipamentul DSRC-VU fie direct în cadrul modulului montat pe sau aproape de parbriz, fie printr-un cablu special construit în așa fel încât să facă dificilă deconectarea ilegală. Deconectarea sau interferența cu funcționarea antenei reprezintă o încălcare a Regulamentului (UE) nr. 165/2014. Mascarea sau modificarea prejudiciabilă în alt fel, în mod intenționat, a performanței operaționale a antenei este considerată o încălcare a Regulamentului (UE) nr. 165/2014.

DSC_22 Formatul antenei nu este definit și reprezintă o decizie comercială, atât timp cât DSRC-VU montată îndeplinește cerințele de conformitate definite în secțiunea 5 de mai jos. Antena trebuie poziționată conform celor stabilite la punctul DSC_19 și conform figurii 14.4 (linia ovală) și trebuie să fie compatibilă în mod eficient cu cazurile de utilizare descrise în 4.1.2 și 4.1.3.

Figura 14.4

Exemplu de poziționare a antenei DSRC de 5,8 GHz pe parbrizul vehiculelor reglementate



Formatul *REDCR* și al antenei sale poate varia în funcție de circumstanțele cititorului (montat pe tripod, ținut în mână, montat pe vehicul etc.) și de modul de utilizare folosit de agentul autorităților de control competente.

O funcție de afișare și/sau de notificare este utilizată pentru a prezenta agentului autorităților de control competente rezultatele funcției de comunicare la distanță. Afișarea poate apărea pe un ecran, sub forma unui document imprimat, sub forma unui semnal audio sau ca o combinație a acestor tipuri de notificări. Forma acestei afișări și/sau notificări ține de cerințele agenților autorităților de control competente și de concepția echipamentului și nu este specificată în prezentul apendice.

DSC_23 Formatul și concepția *REDCR* depind de concepția comercială, conform ERC 70-03, și de specificațiile privind concepția și performanța definite în prezentul apendice (secțiunea 5.3.2), oferind astfel pieței flexbilitatea maximă pentru a proiecta și a furniza echipamente care să servească scenariilor specifice de interogare ale oricărei autorități de control competente date.

DSC_24 Formatul și concepția *DSRC-VU* și poziționarea acesteia înăuntrul sau în afara VU depind de concepția comercială, conform ERC 70-03, și de specificațiile privind concepția și performanța definite în prezentul apendice (secțiunea 5.3.2) și în prezenta secțiune (5.1).

DSC_25 Cu toate acestea, *DSRC-VU* trebuie să fie în mod rezonabil capabilă să accepte valori ale conceptelor de date de la alte echipamente inteligente de vehicule prin intermediul unei conexiuni și al unor protocoale conforme cu standarde deschise din domeniu (de exemplu de la echipamente de cântărire la bord), atât timp cât aceste concepte de date sunt identificate prin denumiri de fișier/identificatori de aplicație unici și cunoscuți; instrucțiunile de utilizare a unor astfel de protocoale trebuie puse la dispoziția Comisiei Europene, precum și, în mod gratuit, la dispoziția producătorilor de echipamente relevante.

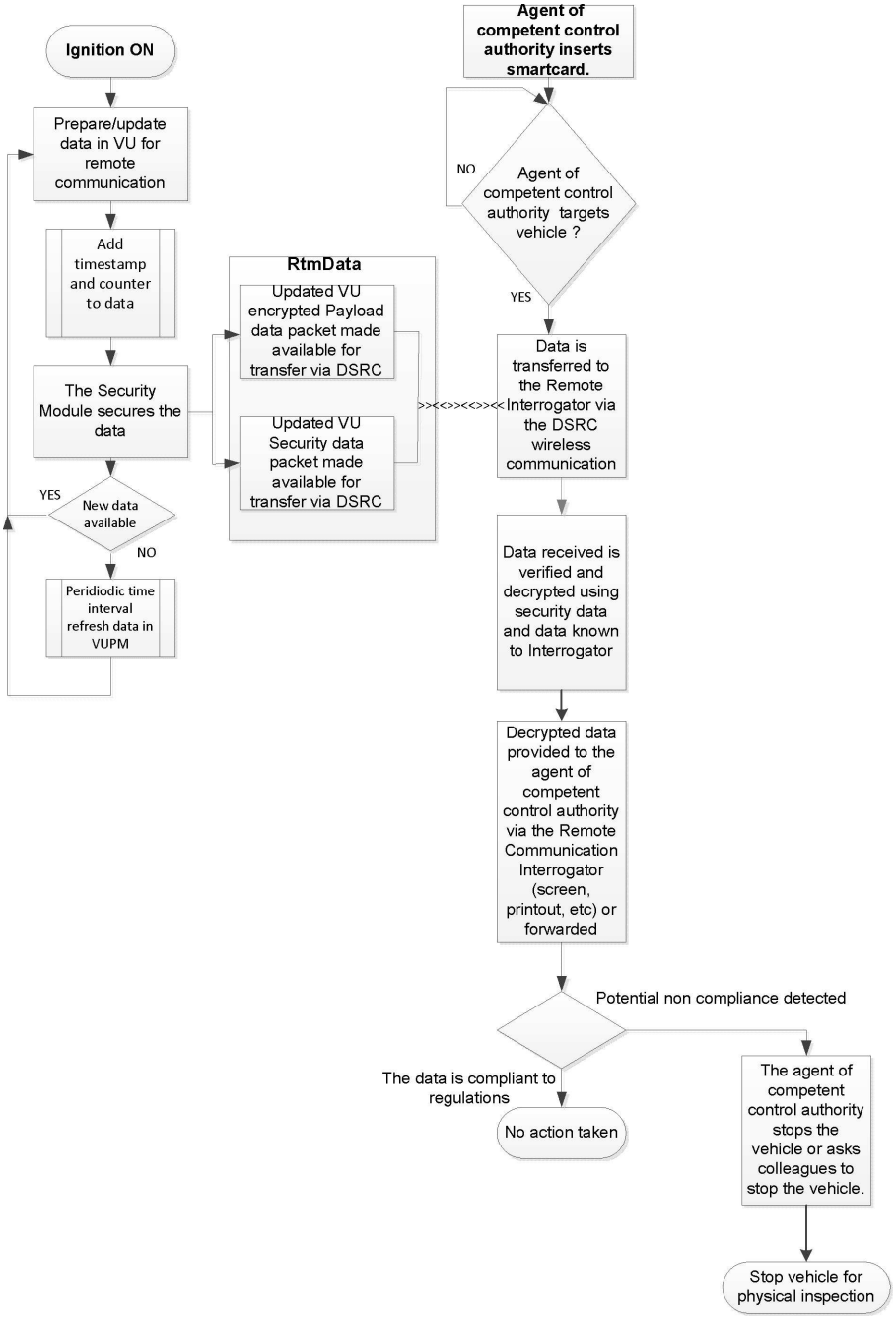
5.2 **Fluxul de lucru**

5.2.1 *Operațiuni*

Fluxul de operațiuni este reprezentat în figura 14.5.

Figura 14.5

Fluxul de lucru pentru funcția de comunicare la distanță



Etapele sunt descrise mai jos:

a. Ori de câte ori un vehicul se află în funcțiune (contactul este în poziția „PORNIT”), tahograful furnizează date funcției VU. Funcția VU pregătește *datele* pentru funcția de comunicare la distanță (criptare) și actualizează VUPM deținute în memoria *DSRC-VU* (conform definiției din secțiunile 4.1.1.1-4.1.1.2). *Datele* colectate trebuie formatate conform celor stabilite în secțiunile 5.4.4-5.4.5 de mai jos.

b. Cu fiecare ocazie în care *datele* sunt actualizate, marca temporală definită în conceptul de date de securitate trebuie actualizată.

c. Funcția *VUSM* securizează datele în conformitate cu procedurile stabilite în apendicele 11.

d. Cu fiecare ocazie în care *datele* sunt actualizate (a se vedea 4.1.1.1-4.1.1.2), *datele* trebuie transferate către *DSRC-VU*, unde înlocuiesc orice date anterioare, pentru ca datele curente actualizate (*datele)* să fie întotdeauna disponibile pentru a fi furnizate în cazul interogării de către un *REDCR*. Atunci când sunt transmise de VU către DSRC-VU, *datele* trebuie să poată fi identificate prin numele de fișier *RTMData* sau prin identificatori „ApplicationID" și „Attribute".

e. Dacă un agent al autorităților de control competente dorește să vizeze un vehicul și să colecteze *datele* de la vehiculul vizat, agentul autorităților de control competente trebuie întâi să își introducă propriul card inteligent (*smartcard*) în *REDCR*, pentru a face posibilă *comunicarea* și pentru a permite *SM-REDCR* să verifice autenticitatea acestuia și să decripteze datele.

f. Apoi, agentul autorității de control competente vizează un vehicul și solicită datele prin comunicare la distanță. *REDCR-ul* deschide o sesiune prin interfața DSRC de 5,8 GHz cu *DSRC-VU* a vehiculului vizat și solicită *datele*. *Datele* sunt transferate către *REDCR* prin sistemul de comunicare fără fir, ca atribut DSRC, folosind serviciul de aplicație GET definit în secțiunea 5.4. Atributul conține valorile datelor utile criptate și datele de securitate DSRC.

g. Datele sunt analizate de echipamentul *REDCR* și prezentate agentului autorității de control competente.

h. Agentul autorității de control competente utilizează datele pentru a lua decizia dacă să oprească sau nu vehiculul pentru o inspecție detaliată sau dacă să ceară altui agent al autorității de control competente să oprească vehiculul.

5.2.2 *Interpretarea datelor primite prin comunicarea DSRC*

DSC_26 Datele primite prin interfața de 5,8 GHz trebuie să prezinte sensul și formatul definite în secțiunile 5.4.4 și 5.4.5 de mai jos, și numai sensul și formatul respective, și trebuie înțelese în contextul obiectivelor definite în acestea. În conformitate cu dispozițiile Regulamentului (UE) nr. 165/2014, *datele* trebuie utilizate numai pentru a furniza informații relevante unei autorități de control competente, pentru ca aceasta să poată stabili ce vehicul ar trebui oprit în vederea efectuării unei inspecții fizice, și trebuie distruse ulterior în conformitate cu articolul 9 din Regulamentul (UE) nr. 165/2014.

5.3 **Parametri ai interfeței fizice DSRC pentru comunicarea la distanță**

5.3.1 *Constrângeri legate de amplasament*

DSC_27 Interogarea la distanță a vehiculelor printr-o interfață DSRC de 5,8GHz nu ar trebui utilizată la o distanță mai mică de 200 de metri de un suport DSRC de 5,8 GHz aflat în funcțiune.

5.3.2 *Parametri ai legăturii descendente și ai legăturii ascendente*

DSC_28 Echipamentul utilizat pentru monitorizarea de la distanță a tahografelor trebuie să fie conform și să funcționeze în conformitate cu ERC70-03 și cu parametrii definiți în tabelele 14.1 și 14.2 de mai jos.

DSC_29 În plus, pentru a asigura compatibilitatea cu parametrii operaționali ai altor sisteme DSRC de 5,8 GHz standardizate, echipamentul folosit pentru monitorizarea de la distanță a tahografelor trebuie să fie conform cu parametrii din EN 12253 și din EN 13372.

Și anume:

Tabelul 14.1

Parametrii legăturii descendente

Nr. crt.	Parametru	Valoare (valori)	Observație
D1	Frecvențe purtătoare pentru legătura descendentă	Există patru alternative care pot fi folosite de un REDCR: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Conform ERC 70-03. Frecvențele purtătoare pot fi selectate de cel care implementează sistemul staționar de monitorizare în trafic și nu este necesar să fie cunoscute în cadrul DSRC-VU (În conformitate cu EN 12253, EN 13372)
D1a (*)	Toleranța frecvențelor purtătoare	în limita a ± 5 ppm	(În conformitate cu EN 12253)
D2 (*)	Masca spectrală a emițătorului RSU (REDCR)	Conform ERC 70-03. REDCR trebuie să fie conform cu clasele B,C definite în EN 12253. În prezenta anexă nu există nicio altă cerință specifică	Parametru utilizat pentru controlarea interferențelor dintre echipamentele de interogare din apropiere (conform definiției din EN 12253 și EN 13372).
D3	Interval de frecvență minim pentru OBU (DSRC-VU)	5,795-5,815 GHz	(În conformitate cu EN 12253)
D4 (*)	E.I.R.P. maximă	Conform ERC 70-03 (fără licență) și reglementărilor naționale maximum + 33 dBm	(În conformitate cu EN 12253)
D4a	Masca E.I.R.P. unghiulară	În conformitate cu specificațiile declarate și publicate ale proiectantului echipamentului de interogare	(În conformitate cu EN 12253)
D5	Polarizare	Circulară levogiră	(În conformitate cu EN 12253)
D5a	Polarizare ortogonală	XPD: În linia de vizare directă: (REDCR) RSU t ≥ 15 dB (DSRC-VU) OBU r ≥ 10 dB În zona de − 3 dB: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(În conformitate cu EN 12253)
D6 (*)	Modulație	Modulație de amplitudine în două trepte.	(În conformitate cu EN 12253)
D6a (*)	Indice de modulație	0,5 … 0,9	(În conformitate cu EN 12253)

Nr. crt.	Parametru	Valoare (valori)	Observație
D6b	Diagramă ochi	≥ 90 % (timp) / ≥ 85 % (amplitudine)	
D7 (*)	Codarea datelor	FM0 Bitul '1' are tranziții doar la începutul și la sfârșitul intervalului de biți. Bitul '0' are o tranziție suplimentară în mijlocul intervalului de biți față de bitul '1'.	(În conformitate cu EN 12253)
D8 (*)	Viteza biților	500 kBit/s	(În conformitate cu EN 12253)
D8a	Toleranța tactului de bit	mai bună decât ± 100 ppm	(În conformitate cu EN 12253)
D9 (*)	Rata de eroare a biților (B.E.R.) pentru comunicare	≤ 10^{-6} când puterea de intrare la OBU (DSRC-VU) se situează în intervalul dat de [D11a – D11b].	(În conformitate cu EN 12253)
D10	Declanșator pentru ieșirea din starea inactivă pentru OBU (DSRC-VU)	OBU (DSRC-VU) se reactivează la primirea oricărui cadru cu 11 sau mai mulți octeți (inclusiv preambul)	Nu este necesară nicio schemă specială de reactivare. DSRC-VU se poate reactiva la primirea unui cadru cu mai puțin de 11 octeți (În conformitate cu EN 12253)
D10a	Timp de pornire maxim	≤ 5 ms	(În conformitate cu EN 12253)
D11	Zonă de comunicare	Ansamblu spațial în cadrul căruia se atinge o B.E.R. conform D9a	(În conformitate cu EN 12253)
D11a (*)	Limita de putere pentru comunicare (superioară).	– 24dBm	(În conformitate cu EN 12253)
D11b (*)	Limita de putere pentru comunicare (inferioară).	Puterea de intrare: – 43 dBm (linia de vizare directă) – 41 dBm [în intervalul de – 45 ° – + 45°Corespunzând planului paralel cu suprafața carosabilului atunci când DSRC-VU este instalată ulterior în vehicul (azimut)]	(În conformitate cu EN 12253) Cerință extinsă pentru unghiurile orizontale până la ± 45°, datorită cazurilor de utilizare definite în prezenta anexă.
D12 (*)	Nivelul puterii de întrerupere al (DSRC-VU)	-60 dBm	(În conformitate cu EN 12253)
D13	Preambul	Preambulul este obligatoriu.	(În conformitate cu EN 12253)
D13a	Preambul – lungime și tipar	16 biți ± 1 bit de biți '1' codați FM0	(În conformitate cu EN 12253)

Nr. crt.	Parametru	Valoare (valori)	Observație
D13b	Forma de undă a preambulului	O secvență alternantă de nivel scăzut și nivel ridicat cu o durată a impulsului de 2 μs. Toleranța este dată de D8a	(În conformitate cu EN 12253)
D13c	Biți de final	RSU (REDCR) poate transmite maximum 8 biți după indicatorul de final. O OBU (DSRC-VU) nu este obligată să țină seama de acești biți suplimentari.	(În conformitate cu EN 12253)

(*) – Parametri ai legăturii descendente care fac obiectul testării conformității pe baza testului de parametru relevant din EN 300 674-1

Tabelul 14.2

Parametrii legăturii ascendente

Nr. crt.	Parametru	Valoare (valori)	Observație
U1 (*)	Frecvențe subpurtătoare	O OBU (DSRC-VU) trebuie să fie compatibilă cu 1,5 MHz și cu 2,0 MHz O RSU (REDCR) trebuie să fie compatibilă cu 1,5 MHz sau cu 2,0 MHz sau cu ambele. U1-0: 1,5 MHz U1-1: 2,0 MHz	Selectarea frecvenței subpurtătoare (1,5 MHz sau 2,0 MHz) depinde de profilul EN 13372 selectat.
U1a (*)	Toleranța frecvențelor subpurtătoare	în limita a ± 0,1 %	(În conformitate cu EN 12253)
U1b	Utilizarea de benzi laterale	Aceleași date de ambele părți	(În conformitate cu EN 12253)
U2 (*)	Masca spectrală a emițătorului OBU (DSRC-VU)	În conformitate cu EN12253 1) Putere în afara benzii: a se vedea ETSI EN 300674-1 2) Putere în bandă: [U4a] dBm în 500 kHz 3) Emisie în orice alt canal de legătură ascendentă: U2(3)-1 = – 35 dBm în 500 kHz	(În conformitate cu EN 12253)
U4a (*)	E.I.R.P. maximă în bandă laterală unică (linia de vizare directă)	Două opțiuni: U4a-0: – 14 dBm U4a-1: – 21 dBm	În conformitate cu specificațiile declarate și publicate ale proiectantului echipamentului
U4b (*)	E.I.R.P. maximă în bandă laterală unică (35°)	Două opțiuni: — Nu se aplică — – 17dBm	În conformitate cu specificațiile declarate și publicate ale proiectantului echipamentului
U5	Polarizare	Circulară levogiră	(În conformitate cu EN 12253)

Nr. crt.	Parametru	Valoare (valori)	Observație
U5a	Polarizare ortogonală	XPD: În linia de vizare directă: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB La – 3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(În conformitate cu EN 12253)
U6	Modulația subpurtătoarei	2-PSK Date codate sincronizate cu subpurtătoarea: tranzițiile datelor codate coincid cu tranzițiile subpurtătoarei.	(În conformitate cu EN 12253)
U6b	Ciclu de funcționare	Ciclu de funcționare: 50 % ± α, α ≤ 5 %	(În conformitate cu EN 12253)
U6c	Modulație pe purtătoare	Multiplicarea subpurtătoarei modulate cu purtătoarea.	(În conformitate cu EN 12253)
U7 (*)	Codarea datelor	NRZI (Nicio tranziție la începutul bitului '1', tranziție la începutul bitului '0', nicio tranziție în cadrul biților)	(În conformitate cu EN 12253)
U8 (*)	Viteza biților	250 kbit/s	(În conformitate cu EN 12253)
U8a	Toleranța tactului de bit	în limita a ± 1 000 ppm	(În conformitate cu EN 12253)
U9	Rata de eroare a biților (B.E.R.) pentru comunicare	$\leq 10^{-6}$	(În conformitate cu EN 12253)
U11	Zonă de comunicare	Ansamblul spațial în cadrul căruia este situată DSRC-VU astfel încât transmisiile sale să fie primite de REDCR cu o B.E.R. mai mică decât cea dată de U9a.	(În conformitate cu EN 12253)
U12a (*)	Amplificare a etajului de amestec (limita inferioară)	1 dB pentru fiecare bandă laterală Intervalul unghiului: Simetric circular între linia de vizare directă și ± 35° și	
		în intervalul de – 45 ° – + 45 °Corespunzând planului paralel cu suprafața carosabilului atunci când DSRC-VU este instalată ulterior în vehicul (azimut)	Mai mare decât intervalul de valori specificat pentru unghiurile orizontale până la ± 45 °, datorită cazurilor de utilizare definite în prezenta anexă.
U12b (*)	Amplificare a etajului de amestec (limita superioară)	10 dB pentru fiecare bandă laterală	Mai mică decât intervalul de valori specificat pentru fiecare bandă laterală într-un con circular în jurul liniei de vizare directă cu unghi de deschidere de ± 45 °
U13	Preambul	Preambulul este obligatoriu.	(În conformitate cu EN 12253)

Nr. crt.	Parametru	Valoare (valori)	Observație
U13a	Preambul Lungime și tipar	32-36 µs, modulate doar cu subpurtătoare, apoi 8 biți de biți '0' codați NRZI.	(În conformitate cu EN 12253)
U13b	Biți de final	DSRC-VU poate transmite maximum 8 biți după indicatorul de final. O RSU (REDCR) nu este obligată să țină seama de acești biți suplimentari.	(În conformitate cu EN 12253)

(*) — Parametri ai legăturii ascendente care fac obiectul testării conformității pe baza testului de parametru relevant din EN 300 674-1

5.3.3 *Concepția antenei*

5.3.3.1 Antena REDCR

DSC_30 Concepția antenei *REDCR* depinde de concepția comercială, în conformitate cu limitele definite în secțiunea 5.3.2, care este adaptată pentru a optimiza performanța de citire a *DSRC-REDCR* în scopul specific și în circumstanțele de citire în care *REDCR* a fost proiectat să funcționeze.

5.3.3.2 Antena VU

DSC_31 Concepția antenei *DSRC-VU* depinde de concepția comercială, în conformitate cu limitele definite în secțiunea 5.3.2, care este adaptată pentru a optimiza performanța de citire a *DSRC-REDCR* în scopul specific și în circumstanțele de citire în care *REDCR* a fost proiectat să funcționeze.

DSC_32 Antena VU trebuie să fie fixată pe sau aproape de parbrizul vehiculului, conform specificațiilor din secțiunea 5.1 de mai sus.

DSC_33 În mediul de testare dintr-un atelier (a se vedea secțiunea 6.3), o antenă DSRC-VU, fixată conform secțiunii 5.1 de mai sus, trebuie să se conecteze cu succes la o comunicare de testare standard și trebuie să realizeze cu succes o tranzacție RTM conform definiției din prezentul apendice, la o distanță cuprinsă între 2 și 10 metri, mai mult de 99 % din timp, potrivit unei medii calculate pe baza a 1 000 de interogări de citire.

5.4 **Cerințe de protocol DSRC pentru RTM**

5.4.1 *Prezentare generală*

DSC_34 Protocolul de tranzacție pentru descărcarea *datelor* prin legătura de interfață DSRC de 5,8 GHz trebuie să corespundă etapelor descrise în cele ce urmează. Prezenta secțiune descrie un flux de tranzacție în condiții ideale fără retransmiteri sau întreruperi ale comunicării.

NOTĂ Scopul fazei de inițializare (etapa 1) este de a stabili comunicarea între *REDCR* și DSRC-VU-urile care au intrat în zona de tranzacție DSRC de 5,8 GHz (*master-slave*), dar care nu au stabilit încă o comunicare cu *REDCR*, și să notifice procesele de aplicație.

— **Etapa 1** Inițializare. *REDCR* transmite un cadru conținând un „tabel de serviciu al radiobalizei" (BST) care include identificatorii de aplicație (AID) din lista de serviciu cu care este compatibil. În aplicația RTM, acesta va fi pur și simplu serviciul cu valoarea AID = 2 (*Freight&Fleet*). *DSRC-VU* evaluează BST primit și răspunde (a se vedea mai jos) cu o listă a aplicațiilor cu care este compatibilă din domeniul *Freight&Fleet* sau nu răspunde dacă nu este compatibilă cu niciuna. Dacă *REDCR* nu oferă AID=2, DSRC-VU nu răspunde REDCR.

— **Etapa 2** *DSRC-VU* transmite un cadru conținând o cerere de alocare a unei ferestre private.

— **Etapa 3** *REDCR* transmite un cadru conținând o alocare a unei ferestre private.

— **Etapa 4** *DSRC-VU* utilizează fereastra privată alocată pentru a transmite un cadru conținând tabelul său de serviciu al vehiculului (VST). Acest VST include o listă a tuturor instanțierilor diferite de aplicații cu care *DSRC-VU* respectivă este compatibilă în cadrul AID=2. Diferitele instanțieri trebuie identificate prin intermediul unor EID-uri unic generate, fiecare asociat cu o valoare de parametru pentru marca contextuală de aplicație (*Application Context Mark*), care indică aplicația și standardul compatibil.

— **Etapa 5** Apoi, *REDCR* analizează VST prezentat și fie întrerupe conexiunea (RELEASE) dacă nu este interesat de nimic din ceea ce VST are de oferit (adică primește de la o *DSRC-VU* un VST care nu este compatibil cu tranzacția RTM), fie, dacă primește un VST corespunzător, pornește o instanțiere de aplicație.

— **Etapa 6** Pentru a realiza acest lucru, REDCR transmite un cadru conținând o comandă de obținere a datelor RTM, identificând instanțierea de aplicație RTM prin precizarea identificatorului care corespunde instanțierii de aplicație RTM (conform celor specificate de DSRC-VU în VST), și alocă o fereastră privată.

— **Etapa 7** *DSRC-VU* utilizează fereastra privată nou-alocată pentru a transmite un cadru conținând identificatorul adresat care corespunde instanțierii de aplicație RTM furnizate în VST, urmat de atributul *RtmData* (element util + element de securitate).

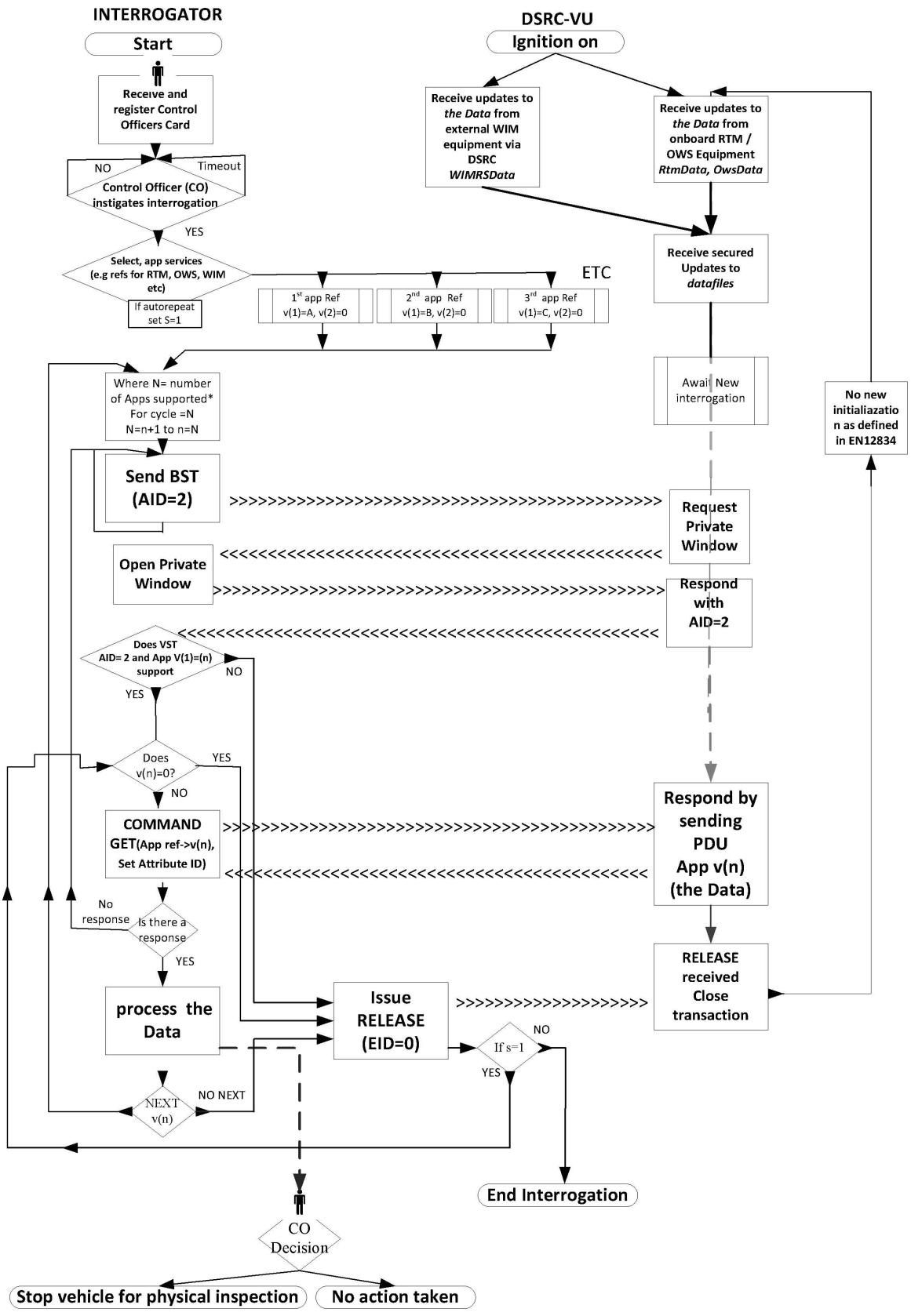
— **Etapa 8** Dacă sunt solicitate mai multe servicii, valoarea „n” se modifică în numărul de referință al serviciului următor și procesul este repetat.

— **Etapa 9** *REDCR* confirmă primirea datelor prin transmiterea unui cadru care conține o comandă RELEASE către *DSRC-VU* pentru a încheia sesiunea SAU, dacă nu a reușit să valideze primirea cu succes a LDPU, revine la etapa 6.

A se vedea figura 14.6 pentru o descriere în imagini a protocolului de tranzacție.

Figura 14.6

Flux de proces RTM prin DSRC de 5,8 GHz



5.4.2 *Comenzi*

DSC_35 Următoarele comenzi sunt singurele funcții utilizate într-o etapă de tranzacție RTM

— **INITIALISATION.request**: o comandă, emisă de REDCR sub forma unei transmisii cu definirea aplicațiilor cu care este compatibil REDCR.

— **INITIALISATION.response**: un răspuns din partea DSRC-VU care confirmă conexiunea și conține o listă a instanțelor de aplicație compatibile, precum și caracteristicile și informațiile privind modul de adresare a acestora (EID).

— **GET.request**: o comandă, emisă de *REDCR* către *DSRC-VU*, care precizează instanțierea de aplicație ce trebuie adresată prin intermediul unui EID definit, conform VST primit, indicându-i *DSRC-VU* să transmită atributul (atributele) ales(e) împreună cu *datele*. Obiectivul comenzii GET este ca *REDCR* să obțină *datele* de la *DSRC-VU*.

— **GET.response**: un răspuns din partea DSRC-VU, care conține *datele* solicitate.

— **ACTION.request ECHO**: o comandă care îi indică *DSRC-VU* să răspundă transmițând date de la *DSRC-VU* la *REDCR*. Obiectivul comenzii ECHO este de a permite atelierelor sau unităților de testare pentru omologarea de tip să verifice dacă legătura DSRC funcționează fără a avea nevoie de acces la elementele de securitate.

— **ACTION**.response ECHO: Un răspuns din partea DSRC VU la comanda ECHO.

— **EVENT_REPORT.request** RELEASE: o comandă care îi indică *DSRC-VU* faptul că tranzacția s-a încheiat. Obiectivul comenzii RELEASE este de a încheia sesiunea cu *DSRC-VU*. La primirea comenzii RELEASE, *DSRC-VU* trebuie să nu răspundă la nicio altă interogare în cadrul conexiunii curente. Trebuie luat act de faptul că, potrivit EN 12834, o DSRC-VU nu se va conecta de două ori la același interogator, cu excepția cazului în care s-a aflat în afara zonei de comunicare timp de 255 de secunde sau dacă ID-ul *Beacon* (radiobaliză) al interogatorului s-a modificat.

5.4.3 *Secvența comenzilor de interogare*

DSC_36 Din perspectiva secvenței de comenzi și de răspunsuri, tranzacția este descrisă după cum urmează:

Secvență	Expeditor		Destinatar	Descriere	Acțiune
1	REDCR	>	DSRC-VU	Inițializarea legăturii de comunicare Solicitare	REDCR transmite BST
2	*DSRC-VU*	>	*REDCR*	*Inițializarea legăturii de comunicare Răspuns*	*Dacă BST este compatibil cu AID = 2, atunci DSRC-VU solicită o fereastră privată*
3	REDCR	>	DSRC-VU	Acordă o fereastră privată	Transmite cadrul care conține alocarea ferestrei private
4	*DSRC-VU*	>	*REDCR*	*Transmite VST*	*Transmite cadrul care conține VST*
5	REDCR	>	DSRC-VU	Transmite *GET.request* privind datele din atributul pentru un EID specific	
6	*DSRC-VU*	>	*REDCR*	*Transmite GET.response cu atributul solicitat pentru EID-ul specific*	*Transmite atributul (RTMData, OWSData etc.) cu datele pentru EID-ul specific*

Secvență	Expeditor		Destinatar	Descriere	Acțiune
7	REDCR	>	DSRC-VU	Transmite *GET.request* privind date din alt atribut (dacă este cazul)	
8	*DSRC-VU*	>	*REDCR*	*Transmite GET.response cu atributul solicitat*	*Transmite atributul cu datele pentru EID-ul specific*
9	REDCR	>	DSRC-VU	Confirmă primirea cu succes a datelor	Transmite comanda RELEASE care încheie tranzacția
10	*DSRC-VU*			*Încheie tranzacția*	

Un exemplu al secvenței de tranzacție și al conținutului cadrelor comunicate este prezentat în secțiunile 5.4.7 și 5.4.8.

5.4.4 *Structuri de date*

DSC_37 Structura semantică a *datelor* atunci când sunt transmise prin interfața DSRC de 5,8 GHz DSRC trebuie să fie în concordanță cu cele descrise în prezentul apendice. Modul în care sunt structurate aceste date este specificat în cadrul prezentei secțiuni.

DSC_38 Datele utile (datele RTM) constau în concatenarea

1. datelor *EncryptedTachographPayload*, care reprezintă varianta criptată a *TachographPayload* definită la punctul ASN.1 din secțiunea 5.4.5. Metoda de criptare este descrisă în apendicele 11;

2. datelor *DSRCSecurityData*, specificate în apendicele 11.

DSC_39 Datele RTM sunt adresate ca atribut RTM =1 și transferate în containerul RTM =10.

DSC_40 Marca contextuală RTM (*RTM Context Mark*) trebuie să identifice partea de standard compatibilă din seria de standarde TARV (RTM corespunde părții 9).

Definiția din modulul ASN.1 pentru datele DSRC din cadrul aplicației RTM este după cum urmează:

```
   TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
   DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for RTM
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


   -- Definitions of the RTM functions:
   RTM-InitialiseComm-Request ::= BST
   RTM-InitialiseComm-Response::= VST
   RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
   ABSENT,  attrIdList})
   RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})

   RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})

   RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the RTM attributes:
   RtmData ::= SEQUENCE {
        encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
   TachographPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   TachographPayload ::= SEQUENCE {
              tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
              tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
              tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
              tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
              tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
              tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
              tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
              tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
              tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                        -- 0= driving selected
              tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
              tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
              tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
   -- All subsequent time related types as defined in Annex 1C.
              tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
              tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
              tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
              tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
              tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
              tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
              tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
              }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                  Ok (1),
                  NoK (2)
                  } SIZE (1..255)
```

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                         [0]    INTEGER,
        bitstring                       [1]    BIT STRING,
        octetstring                     [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString                 [3]    UniversalString,
        beaconId                        [4]    BeaconID,
        t-apdu                          [5]    T-APDUs,
        dsrcApplicationEntityId         [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                     [7]    Dsrc-EID,
        attrIdList                      [8]    AttributeIdList,
        attrList                        [9]    AttributeList{RtmContainer},
        rtmData                         [10]   RtmData,
        rtmContextmark                  [11]   Rtm-ContextMark,
        reserved12                      [12]   NULL,
        reserved13                     [13]   NULL,
        reserved14                      [14]   NULL,
        time                            [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Elementele RtmData, acțiunile realizate și definiții*

DSC_41 Valorile de date care trebuie calculate de VU și utilizate pentru actualizarea datelor securizate din DSRC-VU se calculează în conformitate cu regulile definite în tabelul 14.3:

Tabelul 14.3

Elementele *RtmData*, acțiunile realizate și definiții

(1) Element RTM Data	(2) Acțiune realizată de VU		(3) Definiția datelor din ASN.1
RTM1 **Numărul de înmatriculare al vehiculului**	VU setează valoarea elementului de date RTM1 *tp15638VehicleRegistrationPlate* pe baza valorii înregistrate a tipului de date VehicleRegistrationIdentification definit în apendicele 1 *VehicleRegistrationIdentification*	Numărul de înmatriculare al vehiculului exprimat ca șir de caractere	tp15638VehicleRegstrationPlate LPN, --Numărul de înmatriculare al vehiculului importat din ISO 14906 cu limitarea specificată în EN 15509, care reprezintă o SECVENȚĂ cuprinzând codul de țară urmat de un indicator alfabetic, urmat de numărul de înmatriculare în sine, care este întotdeauna de 14 octeți (completat cu zerouri), astfel încât lungimea de tip EN 15509 LPN este întotdeauna de 17 octeți, din care 14 reprezintă numărul "real" de înmatriculare.

(1) Element RTM Data	(2) Acțiune realizată de VU		(3) Definiția datelor din ASN.1
RTM2 **Eveniment de depășire a limitei de viteză**	VU generează o valoare booleană pentru elementul de date RTM2 *tp15638SpeedingEvent*. Valoarea *tp15638SpeedingEvent* se calculează de VU pe baza numărului evenimentelor de depășire a limitei de viteză (*Over Speeding Events*) înregistrate în VU în ultimele 10 zile de producere a unui eveniment, conform definiției din anexa 1C. Dacă în ultimele 10 zile de producere a unui eveniment a survenit cel puțin un *tp15638SpeedingEvent*, valoarea *tp15638SpeedingEvent* se setează la TRUE. Altfel (ELSE), dacă în ultimele 10 zile de producere a unui eveniment nu s-a produs niciun eveniment, *tp15638SpeedingEvent* se setează la FALSE.	1 (TRUE) – Indică nereguli de viteză în ultimele 10 zile de producere a unui eveniment	`tp15638speedingEvent BOOLEAN,`
RTM3 **Conducere fără un card valabil**	VU generează o valoare booleană pentru elementul de date RTM3 *tp15638DrivingWithoutValidCard*. VU atribuie o valoare de „True" variabilei *tp15638DrivingWithoutValidCard* dacă datele VU au înregistrat, în ultimele 10 zile de producere a unui eveniment, cel puțin un eveniment de tipul „Conducere fără un card adecvat", conform definiției din anexa 1C. Altfel (ELSE), dacă nu există evenimente în ultimele 10 zile de producere a unui eveniment, variabila *tp15638DrivingWithoutValidCard* se setează la FALSE.	1 (TRUE) = Indică utilizarea unui card care nu este valabil	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Card de conducător auto valabil**	VU generează o valoare booleană pentru elementul de date RTM4 *tp15638DriverCard*, pe baza datelor stocate în VU și definite în apendicele 1. Dacă nu este prezent niciun card de conducător auto valabil, VU setează variabila la TRUE Altfel (ELSE), dacă este prezent un card de conducător auto valabil, VU setează variabila la FALSE	0 (FALSE) = Indică un card de conducător auto valabil	`tp15638DriverCard BOOLEAN,`
RTM5 **Introducerea cardului în timpul conducerii**	VU generează o valoare booleană pentru elementul de date RTM5. VU atribuie o valoare de TRUE variabilei *tp15638CardInsertion* dacă datele VU au înregistrat, în ultimele 10 zile de producere a unui eveniment, cel puțin un eveniment de tipul „Introducerea cardului în timpul conducerii", conform definiției din anexa 1C. Altfel (ELSE), dacă nu există astfel de evenimente în ultimele 10 zile de producere a unui eveniment, variabila *tp15638CardInsertion* se setează la FALSE.	1 (TRUE) = indică introducerea cardului în timpul conducerii în ultimele 10 zile de producere a unui eveniment	`tp15638CardInsertion BOOLEAN,`
RTM6 **Eroare privind datele de la senzorul de mișcare**	VU generează o valoare booleană pentru elementul de date RTM6 VU atribuie o valoare de TRUE variabilei *tp15638MotionDataError* dacă datele VU au înregistrat, în ultimele 10 zile de producere a unui eveniment, cel puțin un eveniment de tipul „Eroare privind datele de la senzorul de mișcare", conform definiției din anexa 1C. Altfel (ELSE), dacă nu există astfel de evenimente în ultimele 10 zile de producere a unui eveniment, variabila *tp15638MotionDataError* se setează la FALSE.	1 (TRUE) = Indică o eroare privind datele de la senzorul de mișcare în ultimele 10 zile de producere a unui eveniment	`tp15638motionDataError BOOLEAN,`

(1) Element RTM Data	(2) Acțiune realizată de VU		(3) Definiția datelor din ASN.1
RTM7 **Conflict privind deplasarea vehiculului**	VU generează o valoare booleană pentru elementul de date RTM7 VU atribuie o valoare de TRUE variabilei *tp15638vehicleMotionConflict* dacă datele VU au înregistrat în ultimele 10 zile cel puțin un eveniment de tipul „Conflict privind deplasarea vehiculului" (valoare '0A'H). Altfel (ELSE), dacă nu există evenimente în ultimele 10 zile de producere a unui eveniment, variabila *tp15638vehicleMotionConflict* se setează la FALSE.	1 (TRUE) = Indică un conflict privind deplasarea în ultimele 10 zile de producere a unui eveniment	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Al doilea card de conducător auto**	VU generează o valoare booleană pentru elementul de date RTM8 pe baza anexei 1C („activitatea conducătorului auto" CREW și CO-DRIVER). Dacă este prezent un al doilea card de conducător auto valabil, VU setează variabila la TRUE Altfel (ELSE), dacă nu este prezent un al doilea card de conducător auto valabil, VU setează variabila la FALSE	1 (TRUE) = Indică existența unui al doilea card de conducător auto introdus	`tp156382ndDriverCard` `BOOLEAN,`
RTM9 **Activitate curentă**	VU generează o valoare booleană pentru elementul de date RTM9 Dacă activitatea curentă este înregistrată în VU ca orice altă activitate în afară de „CONDUCERE", conform definiției din anexa 1C, VU setează variabila la TRUE Altfel (ELSE), dacă activitatea curentă este înregistrată în VU drept „CONDUCERE", VU setează variabila la FALSE	1 (TRUE) = altă activitate selectată; 0 (FALSE) = „conducere" selectată	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Ultima sesiune încheiată**	VU generează o valoare booleană pentru elementul de date RTM10. Dacă ultima sesiune de utilizare a cardului nu a fost încheiată corect, conform definiției din anexa 1C, VU setează variabila la TRUE. Altfel (ELSE), dacă ultima sesiune de utilizare a cardului a fost încheiată corect, VU setează variabila la FALSE.	1 (TRUE) = încheiată incorect 0 (FALSE) = încheiată corect	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Întreruperea alimentării cu energie electrică**	VU generează o valoare de număr întreg pentru elementul de date RTM11. VU atribuie pentru variabila *tp15638PowerSupplyInterruption* o valoare egală cu cea mai lungă întrerupere a alimentării cu energie electrică, conform articolului 9 din Regulamentul (UE) nr. 165/2014, de tip „Întreruperea alimentării cu energie electrică", conform definiției din anexa 1C. Altfel (ELSE), dacă în ultimele 10 zile de producere a unui eveniment nu au survenit evenimente de întrerupere a alimentării cu energie electrică, valoarea numărului întreg se setează la 0.	— Numărul întreruperilor de alimentare cu energie electrică în ultimele 10 zile de producere a unui eveniment	`tp15638powerSupplyInterruption` `NUMĂR ÎNTREG (0..127),`

(1) Element RTM Data	(2) Acțiune realizată de VU		(3) Definiția datelor din ASN.1
RTM12 **Anomalie a senzorului**	VU generează o valoare de număr întreg pentru elementul de date RTM12. VU atribuie variabilei *sensorFault* o valoare de: — 1 dacă un eveniment de tipul „anomalie a senzorului '35'H" a fost înregistrat în ultimele 10 zile. — 2 dacă un eveniment de tipul „anomalie a receptorului GNSS" (fie intern, fie extern, cu valorile de enumerare '51'H sau '52'H) a fost înregistrat în ultimele 10 zile. — 3 dacă un eveniment de tipul „anomalie a comunicării GNSS externe" '53'H a fost înregistrat în ultimele 10 zile de producere a unui eveniment. — 4 Dacă atât o „anomalie a sezorului", cât și o „anomalie a receptorului GNSS" au fost înregistrate în ultimele 10 zile de producere a unui eveniment — 5 Dacă atât o „anomalie a sezorului", cât și o „anomalie a comunicării GNSS externe" au fost înregistrate în ultimele 10 zile de producere a unui eveniment — 6 Dacă atât o „anomalie a receptorului GNSS", cât și o „anomalie a comunicării GNSS externe" au fost înregistrate în ultimele 10 zile de producere a unui eveniment — 7 Dacă toate cele trei anomalii de senzor au fost înregistrate în ultimele 10 zile de producere a unui eveniment Altfel (ELSE), atribuie o valoare de 0 dacă nu s-a înregistrat niciun eveniment în ultimele 10 zile de producere a unui eveniment	— anomalie senzor un octet conform dicționarului de date	`tp15638SensorFault NUMĂR ÎNTREG (0..255),`
RTM13 **Reglarea orei**	VU generează o valoare de număr întreg (*timeReal* din apendicele 1) pentru elementul de date RTM13 pe baza prezenței datelor privind reglarea orei, conform definiției din anexa 1C. VU atribuie valoarea orei la care s-a produs ultimul eveniment de date privind reglarea orei. Altfel (ELSE), dacă în datele VU nu este prezent niciun eveniment de tip „reglarea orei", conform definiției din anexa 1C, VU setează o valoare de 0	Ora ultimei reglări a orei	`tp15638TimeAdjustment` `NUMĂR ÎNTREG (0..4294967295),`
RTM14 **Tentativă de încălcare a securității**	VU generează o valoare de număr întreg (*timeReal* din apendicele 1) pentru elementul de date RTM14 pe baza prezenței unei tentative de încălcare a securității, conform definiției din anexa 1C. VU setează valoarea orei la care a fost înregistrată de către VU ultima tentativă de încălcare a securității. Altfel (ELSE), dacă în datele VU nu este prezent niciun eveniment de tip „tentativă de încălcare a securității", conform definiției din anexa 1C, VU setează o valoare de 0x00FF.	Ora ultimei tentative de încălcare — Valoare implicită =0x00FF	`tp15638LatestBreachAttempt` `NUMĂR ÎNTREG (0..4294967295),`
RTM15 **Ultima etalonare**	VU generează o valoare de număr întreg (*timeReal* din apendicele 1) pentru elementul de date RTM15 pe baza prezenței datelor privind ultima etalonare, conform definiției din anexa 1C. VU setează valoarea orei la care au avut loc ultimele două etalonări (RTM15 și RTM16), care sunt stabilite în *VuCalibrationData* definite în apendicele 1. VU setează valoarea pentru RTM 15 la ora reală (*timeReal*) a ultimei înregistrări de etalonare.	Ora ultimelor date de etalonare	`tp15638LastCalibrationData` `NUMĂR ÎNTREG (0..4294967295),`

(1) Element RTM Data	(2) Acțiune realizată de VU		(3) Definiția datelor din ASN.1
RTM16 **Etalonare anterioară**	VU generează o valoare de număr întreg (*timeReal* din apendicele 1) pentru elementul de date RTM16 al înregistrării de etalonare care o precedă pe cea a ultimei etalonări Altfel (ELSE), dacă nu a existat nicio etalonare anterioară, VU setează valoarea RTM16 la 0.	Ora datelor privind etalonarea anterioară	`tp15638PrevCalibrationData` `NUMĂR ÎNTREG (0..4294967295),`
RTM17 **Data conectării tahografului**	Pentru elementul de date RTM17, VU generează o valoare de număr întreg (*timeReal* din apendicele 1). VU setează valoarea orei la care a fost instalată inițial VU. VU extrage aceste date din *VuCalibrationData* (apendicele1) din *vuCalibrationRecords*, *CalibrationPurpose* fiind egal cu: '03'H	Data conectării tahografului	`tp15638DateTachoConnected` `NUMĂR ÎNTREG (0..4294967295),`
RTM18 **Viteza curentă**	VU generează o valoare de număr întreg pentru elementul de date RTM18. VU setează valoarea pentru RTM16 la ultima viteză curentă înregistrată în momentul celei mai recente actualizări a *RtmData*.	Ultima viteză curentă înregistrată	`tp15638CurrentSpeed NUMĂR ÎNTREG (0..255),`
RTM19 **Marcă temporală (*Timestamp*)**	Pentru elementul de date RTM19, VU generează o valoare de număr întreg (*timeReal* din apendicele 1). VU setează valoarea pentru RTM19 la ora ultimei actualizări a *RtmData*.	Marca temporală a înregistrării *TachographPayload* curente	`tp15638Timestamp` `NUMĂR ÎNTREG (0..4294967295),`

5.4.6 *Mecanismul de transfer al datelor*

DSC_42 Datele utile definite anterior sunt solicitate de REDCR după etapa de inițializare și transmise în consecință de către *DSRC-VU* în fereastra alocată. Comanda GET este utilizată de REDCR pentru a obține date.

DSC_43 Pentru toate transmisiile DSRC, datele trebuie să fie codate folosind PER (*Packed Encoding Rules*).

5.4.7 *Descriere detaliată a tranzacției DSRC*

DSC_44 Inițializarea se realizează în conformitate cu DSC_44 – DSC_48 și cu tabelele 14.4 – 14.9. În etapa de inițializare, REDCR începe să transmită un cadru care conține un BST (tabel de serviciu al radiobalizei) în conformitate cu EN 12834 și cu EN 13372, 6.2, 6.3, 6.4 și 7.1, cu setările specificate în următorul tabel 14.4.

Tabelul 14.4

Inițializare – setări cadru BST

Câmp	Setări
Link Identifier	Adresa de transmisie
BeaconId	Conform EN 12834
Time	Conform EN 12834
Profile	Nicio extensie, a se folosi 0 sau 1
MandApplications	Nicio extensie, EID nu este prezent, parametrul nu este prezent, AID= 2 Freight&Fleet
NonMandApplications	Nu este prezent
ProfileList	Nicio extensie, numărul de profiluri din listă = 0
Fragmentation header	Nicio fragmentare
Layer 2 settings	PDU de comandă, comandă UI

Un exemplu practic al setărilor specificate în tabelul 14.4, cu indicarea codării biților, este dat în următorul tabel 14.5.

Tabelul 14.5

Inițializare – exemplu de conținut cadru BST

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
1	FLAG	0111 1110	Indicator de început
2	Broadcast ID	1111 1111	Adresa de transmisie
3	MAC Control Field	1010 0000	PDU de comandă
4	LLC Control field	0000 0011	Comandă UI
5	Fragmentation header	1xxx x001	Nicio fragmentare

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
6	BST	1000	Solicitare de inițializare
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	Aplicațiile neobligatorii (*NonMand*) nu sunt prezente
		xxx	Identificator producător
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	ID de 27 de biți disponibil pentru producător
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	Timp real UNIX de 32 de biți
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,…)	0000 0000	Nicio extensie. Profil de exemplu 0
17	MandApplications SEQUENCE (SIZE(0..127, …)) OF {	0000 0001	Nicio extensie, numărul aplicațiilor obligatorii (*mandApplications*) = 1
18	SEQUENCE {		
	OPTION indicator	0	EID nu este prezent
	OPTION indicator	0	Parametrul nu este prezent
	AID DSRCApplicationEntityID } }	00 0010	Nicio extensie. AID= 2 Freight&Fleet

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
19	ProfileList SEQUENCE (0..127,…) OF Profile }	0000 0000	Nicio extensie, numărul de profiluri din listă = 0
20	FCS	xxxx xxxx	Secvență de verificare a cadrului
21		xxxx xxxx	
22	Flag	0111 1110	Indicator de final

DSC_45 Atunci când primește un BST, o *DSRC-VU* solicită alocarea unei ferestre private, conform specificațiilor din EN 12795 și EN 13372, 7.1.1, fără nicio setare RTM specifică. Tabelul 14.6 oferă un exemplu de codare a biților.

Tabelul 14.6

Inițializare – Conținutul cadrului de solicitare de alocare a unei ferestre private

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
1	FLAG	0111 1110	Indicator de început
2	Private LID	xxxx xxxx	Adresa de legătură a DSRC-VU specifice
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Solicitare de fereastră privată
7	FCS	xxxx xxxx	Secvență de verificare a cadrului
8		xxxx xxxx	
9	Flag	0111 1110	Indicator de final

DSC_45 REDCR răspunde apoi prin alocarea unei ferestre private, conform specificațiilor din EN 12795 și EN 13372, 7.1.1, fără nicio setare RTM specifică.

Tabelul 14.7 oferă un exemplu de codare a biților.

Tabelul 14.7

Inițializare – Conținutul cadrului de alocare a unei ferestre private

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
1	FLAG	0111 1110	Indicator de început
2	Private LID	xxxx xxxx	Adresa de legătură a DSRC-VU specifice
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Alocarea ferestrei private
7	FCS	xxxx xxxx	Secvență de verificare a cadrului
8		xxxx xxxx	
9	Flag	0111 1110	Indicator de final

DSC_47 Atunci când primește alocarea ferestrei private, *DSRC-VU* transmite VST-ul său (tabelul de serviciu al vehiculului), conform definiției din EN 12834 și din EN 13372, 6.2, 6.3, 6.4 și 7.1, cu setările specificate în tabelul 14.8, folosind fereastra de transmisie alocată.

Tabelul 14.8

Inițializare – setări cadru VST

Câmp	Setări
Private LID	Conform EN 12834
VST parameters	Fill = 0, apoi pentru fiecare aplicație compatibilă: EID prezent, parametru prezent, AID = 2, EID generat de OBU
Parameter	Nicio extensie, conține marca contextuală RTM
ObeConfiguration	Câmpul opțional *ObeStatus* poate fi prezent, dar nu trebuie folosit de REDCR
Fragmentation header	Nicio fragmentare
Layer 2 settings	PDU de comandă, comandă UI

DSC_48 *DSRC-VU* trebuie să fie compatibilă cu aplicația „Freight and Fleet”, identificată prin identificatorul de aplicație „2”. Și alți identificatori de aplicație pot fi compatibili, dar nu trebuie să fie prezenți în acest VST, deoarece BST necesită numai AID=2. Câmpul „Applications” conține o listă a instanțelor de aplicații compatibile din *DSRC-VU*. Pentru fiecare instanțiere de aplicație compatibilă este dată o trimitere la standardul corespunzător, formată dintr-o marcă contextuală Rtm, care este compusă dintr-un OBJECT IDENTIFIER reprezentând standardul aferent, partea acestuia (9 pentru RTM) și posibil versiunea sa, plus un EID care este generat de DSRC-VU și asociat instanțierii de aplicație respective.

Un exemplu practic al setărilor specificate în tabelul 14.8, cu indicarea codării biților, este dat în tabelul 14.9.

Tabelul 14.9

Inițializare – exemplu de conținut cadru VST

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
1	FLAG	0111 1110	Indicator de început
2	Private LID	xxxx xxxx	Adresa de legătură a DSRC-VU specifice
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	PDU de comandă
7	LLC Control field	0000 0011	Comandă UI
8	Fragmentation header	1xxx x001	Nicio fragmentare
9	VST SEQUENCE {	1001	Răspuns la inițializare
	Fill BIT STRING (SIZE(4))	0000	Neutilizat și setat la 0
10	Profile INTEGER (0..127,...) Applications SEQUENCE OF {	0000 0000	Nicio extensie. Profil de exemplu 0
11		0000 0001	Nicio extensie, 1 aplicație
12	SEQUENCE {		
	OPTION indicator	1	EID prezent
	OPTION indicator	1	Parametru prezent
	AID DSRCApplicationEntityID	00 0010	Nicio extensie. AID = 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Definit în cadrul OBU și identificând instanța de aplicație

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
14	Parameter Container {	0000 0010	Nicio extensie, opțiune container = 02, șir de octeți
15		0000 1000	Nicio extensie, lungimea mărcii contextuale Rtm = 8
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	Identificator de obiect al standardului compatibil, cu partea si versiunea sa. Exemplu: „ISO (1) Standard (0) TARV (15638) part9(9) Version1 (1)”. Primul octet este 06H, care reprezintă identificatorul de obiect. Al doilea octet este 06H, care reprezintă lungimea acestuia. Următorii 6 octeți codează identificatorul de obiect dat ca exemplu A se lua notă de faptul că doar un element al secvenței este prezent (elementul *RtmCommProfile* opțional este omis)
17		0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence { OPTION indicator	0	ObeStatus nu este prezent
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Identificator al producătorului pentru DSRC-VU, conform descrierii din registrul ISO 14816
27		xxxx xxxx	
28	FCS	xxxx xxxx	Secvență de verificare a cadrului
29		xxxx xxxx	
30	Flag	0111 1110	Indicator de final

DCS_49 REDCR citește apoi datele prin emiterea unei comenzi GET, conformă cu comanda GET definită în EN 13372, 6.2, 6.3, 6.4 și în EN 12834, cu setările specificate în tabelul 14.10.

Tabelul 14.10

Prezentare – setări cadru *GET.request*

Câmp	Setări
Invoker Identifier (IID)	Nu este prezent
Link Identifier (LID)	Adresa de legătură a DSRC-VU specifice
Chaining	Nu

Câmp	Setări
Element Identifier (EID)	Astfel cum este specificat în VST. Nicio extensie
Access Credentials	Nu
AttributeIdList	Nicio extensie, 1 atribut, AttributeID = 1 (RtmData)
Fragmentation	Nu
Layer2 settings	PDU de comandă, comandă ACn cu interogare prealabilă

Tabelul 14.11 prezintă un exemplu de citire a datelor RTM

Tabelul 14.11

Prezentare – exemplu de cadru GET.request

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
1	FLAG	0111 1110	Indicator de început
2	Private LID	xxxx xxxx	Adresa de legătură a DSRC-VU specifice
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU de comandă
7	LLC Control field	n111 0111	Comandă ACn cu interogare prealabilă, bit n
8	Fragmentation header	1xxx x001	Nicio fragmentare
9	Get.request SEQUENCE {	0110	Solicitare de obținere a datelor
	OPTION indicator	0	Acreditările de acces (Access Credentials) nu sunt prezente
	OPTION indicator	0	IID nu este prezent
	OPTION indicator	1	AttributeIdList prezentă
	Fill BIT STRING(SIZE(1))	0	Setată la 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	EID al instanței de aplicație RTM, astfel cum este specificat în VST. Nicio extensie
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Nicio extensie, numărul de atribute = 1
12		0000 0001	*AttributeId*=1, *RtmData*. Nicio extensie

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
13	FCS	xxxx xxxx	Secvență de verificare a cadrului
14		xxxx xxxx	
15	Flag	0111 1110	Indicator de final

DCS_50 Când primește solicitarea GET (*GET.request*), *DSRC-VU* transmite un răspuns GET (*GET.response*) cu datele solicitate, conform cu răspunsul GET definit în EN 13372, 6.2, 6.3, 6.4 și în EN 12834, cu setările specificate în tabelul 14.12.

Tabelul 14.12

Prezentare – setări cadru GET.response

Câmp	Setări
Invoker Identifier (IID)	Nu este prezent
Link Identifier (LID)	Conform EN 12834
Chaining	Nu
Element Identifier (EID)	Astfel cum este specificat în VST.
Access Credentials	Nu
Fragmentation	Nu
Layer2 settings	PDU de răspuns, răspuns disponibil și comandă acceptată, comandă ACn

Tabelul 14.13 prezintă un exemplu de citire a datelor RTM

Tabelul 14.13

Prezentare – exemplu de conținut cadru răspuns

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
1	FLAG	0111 1110	Indicator de început
2	Private LID	xxxx xxxx	Adresa de legătură a DSRC-VU specifice
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
6	MAC Control field	1101 0000	PDU de răspuns
7	LLC Control field	n111 0111	Răspuns disponibil, comandă ACn bit n
8	LLC Status field	0000 0000	Răspuns disponibil și comandă acceptată
9	Fragmentation header	1xxx x001	Nicio fragmentare
10	Get.response SEQUENCE {	0111	Obținere răspuns
	OPTION indicator	0	IID nu este prezent
	OPTION indicator	1	Lista atributelor (Attribute List) prezentă
	OPTION indicator	0	Starea de retur nu este prezentă
	Fill BIT STRING(SIZE(1))	0	Neutilizat
11	EID INTEGER(0..127,…)	xxxx xxxx	Răspuns din partea instanței de aplicație RTM. Nicio extensie,
12	AttributeList SEQUENCE OF {	0000 0001	Nicio extensie, numărul de atribute = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Nicio extensie, AttributeID = 1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Nicio extensie, opțiune container = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Secvență de verificare a cadrului
n+2		xxxx xxxx	
n+3	Flag	0111 1110	Indicator de final

DSC_51 Apoi REDCR închide conexiunea prin emiterea unei comenzi EVENT_REPORT, RELEASE conforme cu EN 13372, 6.2, 6.3, 6.4 și cu EN 12834, 7.3.8, fără nicio setare RTM specifică. Tabelul 14.14 arată un exemplu de codare a biților pentru comanda RELEASE.

Tabelul 14.14

Încheiere. Conținut cadru EVENT_REPORT RELEASE

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
1	FLAG	0111 1110	Indicator de început
2	Private LID	xxxx xxxx	Adresa de legătură a DSRC-VU specifice
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1000 s000	Cadrul conține o LPDU de comandă
7	LLC Control field	0000 0011	Comandă UI
8	Fragmentation header	1xxx x001	Nicio fragmentare
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Acreditările de acces (Access Credentials) nu sunt prezente
	OPTION indicator	0	Parametrul de eveniment nu este prezent
	OPTION indicator	0	IID nu este prezent
	Mode BOOLEAN	0	Nu se așteaptă niciun răspuns
10	EID INTEGER (0..127,…)	0000 0000	Nicio extensie, EID = 0 (sistem)
11	EventType INTEGER (0..127,…) }	0000 0000	Tip de eveniment 0 = Release
12	FCS	xxxx xxxx	Secvență de verificare a cadrului
13		xxxx xxxx	
14	Flag	0111 1110	Indicator de final

DSC_52 Nu se așteaptă ca *DSRC-VU* să răspundă la comanda *Release*. Comunicarea este apoi închisă.

5.4.8 *Descrierea tranzacției de testare DRSC*

DSC_53 Testele complete, care includ securizarea datelor, trebuie realizate conform definiției din apendicele 11 (Mecanisme de securitate comune), de către persoane autorizate care au acces la procedurile de securitate, folosind comanda GET normală definită mai sus.

DSC_54 Testele de operaționalitate și de inspecție (verificare) periodică ce necesită decriptarea și înțelegerea conținutului de date decriptat trebuie realizate conform specificațiilor din apendicele 11 (Mecanisme de securitate comune) și din apendicele 9 (Omologarea de tip – lista testelor minime obligatorii).

Cu toate acestea, comunicarea DSRC de bază poată fi testată prin comanda ECHO. Aceste teste pot fi necesare la verificarea operaționalității, cu ocazia inspecției periodice sau la cererea autorității de control competente sau dacă sunt impuse de Regulamentul (UE) nr. 165/2014 (a se vedea secțiunea 6 de mai jos)

DSC_55 Pentru a realiza această testare a comunicării de bază, comanda ECHO este emisă de REDCR în cursul unei sesiuni, și anume după finalizarea cu succes a unei etape de inițializare. Astfel, secvența de interacțiuni este similară celei a unei interogări:

— Etapa 1 *REDCR* transmite un „tabel de serviciu al radiobalizei" (BST) care include identificatorii de aplicație (AID) din lista de serviciu cu care este compatibil. În aplicațiile RTM, acesta va fi pur și simplu serviciul cu valoarea AID = 2.

DSRC-VU evaluează BST-ul primit și, în cazul în care identifică faptul că BST solicită *Freight&Fleet* (AID = 2), *DSRC-VU* răspunde. Dacă *REDCR* nu oferă AID=2, *DSRC-VU* închide tranzacția sa cu *REDCR*.

— Etapa 2 *DSRC-VU* transmite o cerere de alocare a unei ferestre private.

— Etapa 3 REDCR transmite o alocare de fereastră privată.

— Etapa 4 *DSRC-VU* utilizează fereastra privată alocată pentru a transmite tabelul său de serviciu al vehiculului (VST). Acest VST include o listă a tuturor instanțierilor diferite de aplicații cu care *DSRC-VU* respectivă este compatibilă în cadrul AID=2. Diferitele instanțieri trebuie identificate prin intermediul unor EID-uri unice, fiecare asociat cu o valoare de parametru indicând instanțierea de aplicație compatibilă.

— Etapa 5 Apoi, *REDCR* analizează VST prezentat și fie întrerupe conexiunea (RELEASE) dacă nu este interesat de nimic din ceea ce VST are de oferit (adică primește un VST de la o *DSRC-VU* care nu este o RTM VU), fie, dacă primește un VST corespunzător, pornește o instanțiere de aplicație.

— Etapa 6 *REDCR* emite o comandă (ECHO) către *DSRC-VU* specifică și alocă o fereastră privată.

— Etapa 7 *DSRC-VU* utilizează fereastra privată nou alocată pentru a transmite un cadru de răspuns ECHO.

Tabelele de mai jos oferă un exemplu practic de sesiune de comunicare ECHO.

DSC_56 Inițializarea se realizează în conformitate cu secțiunea 5.4.7 (DSC_44-DSC_48) și cu tabelele 14.4-14.9.

DSC_57 REDCR emite apoi o comandă ACTION, ECHO conformă cu ISO 14906, care conține 100 de octeți de date și nicio setare specifică pentru RTM. Tabelul 14.15 prezintă conținutul cadrului transmis de REDCR.

Tabelul 14.15

Exemplu de cadru de solicitare ACTION, ECHO

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
1	FLAG	0111 1110	Indicator de început
2	Private LID	xxxx xxxx	Adresa de legătură a DSRC-VU specifice
3		xxxx xxxx	

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU de comandă
7	LLC Control field	n111 0111	Comandă ACn cu interogare prealabilă, bit n
8	Fragmentation header	1xxx x001	Nicio fragmentare
9	ACTION.request SEQUENCE {	0000	Solicitare de acțiune (ECHO)
	OPTION indicator	0	Acreditările de acces (Access Credentials) nu sunt prezente
	OPTION indicator	1	Parametru de acțiune prezent
	OPTION indicator	0	IID nu este prezent
	Mode BOOLEAN	1	Răspuns așteptat
10	EID INTEGER (0..127,…)	0000 0000	Nicio extensie, EID = 0 (sistem)
11	ActionType INTEGER (0..127,…)	0000 1111	Nicio extensie, solicitare ECHO de tip acțiune
12	ActionParameter CONTAINER {	0000 0010	Nicio extensie, opțiune container = 2.
13		0110 0100	Nicio extensie. Lungimea șirului = 100 de octeți
14		xxxx xxxx	Datele care trebuie transmise (echoed)
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Secvență de verificare a cadrului
115		xxxx xxxx	
116	Flag	0111 1110	Indicator de final

DSC_58 Când primește solicitarea ECHO, *DSRC-VU* transmite un răspuns ECHO cu 100 de octeți de date, prin reflectarea comenzii primite, conform ISO 14906, fără nicio setare specifică pentru RTM. Tabelul 14.16 prezintă un exemplu de codare la nivelul biților.

Tabelul 14.16

Exemplu de cadru de răspuns ACTION, ECHO

Nr. octet	Atribut/Câmp	Biți în octet	Descriere
1	FLAG	0111 1110	Indicator de început
2	Private LID	xxxx xxxx	Adresa de legătură a VU specifice
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU de răspuns
7	LLC Control field	n111 0111	Comandă ACn, bit n
8	LLC status field	0000 0000	Răspuns disponibil
9	Fragmentation header	1xxx x001	Nicio fragmentare
10	ACTION.response SEQUENCE {	0001	răspuns ACTION (ECHO)
	OPTION indicator	0	IID nu este prezent
	OPTION indicator	1	Parametru de răspuns prezent
	OPTION indicator	0	Starea de retur nu este prezentă
	Fill BIT STRING (SIZE (1))	0	Neutilizat
11	EID INTEGER (0..127,…)	0000 0000	Nicio extensie, EID = 0 (sistem)
12	ResponseParameter CONTAINER {	0000 0010	Nicio extensie, opțiune container = 2.
13		0110 0100	Nicio extensie. Lungimea șirului = 100 de octeți
14		xxxx xxxx	Date transmise (echoed)
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Secvență de verificare a cadrului
115		xxxx xxxx	
116	Flag	0111 1110	Indicator de final

5.5 **Compatibilitate cu Directiva 2015/71/CE**

5.5.1 *Prezentare generală*

DSC_59 Pentru a fi compatibil cu Directiva 2015/719/CE privind greutățile și dimensiunile maxime pentru vehiculele grele de marfă, protocolul de tranzacție pentru descărcarea datelor OWS prin legătura de interfață DSRC de 5,8 GHz va fi același ca cel utilizat pentru datele RTM (a se vedea 5.4.1), singura diferență fiind că identificatorul de obiect legat de standardul TARV se va referi la standardul ISO 15638 (TARV), partea 20 privind WOB/OWS.

5.5.2 *Comenzi*

DSC_60 Comenzile utilizate pentru o tranzacție OWS vor fi aceleași ca cele utilizate pentru o tranzacție RTM.

5.5.3 *Secvența comenzilor de interogare*

DSC_61 Secvența comenzilor de interogare pentru datele OWS va fi aceeași ca cea pentru datele RTM.

5.5.4 *Structuri de date*

DSC_62 Datele utile (datele OWS) constau în concatenarea

1. datelor *EncryptedOwsPayload*, care reprezintă varianta criptată a *OwsPayload* definită la punctul ASN.1 din secțiunea 5.5.5. Metoda de criptare trebuie să fie aceeași ca cea adoptată pentru *RtmData*, care este specificată în apendicele 11;

2. datelor *DSRCSecurityData*, calculate cu aceiași algoritmi ca cei adoptați pentru *RtmData*, specificate în apendicele 11.

5.5.5 *Modulul ASN. 1 pentru tranzacția DRSC OWS*

DSC_63. Definiția din modulul ASN.1 pentru datele DSRC din cadrul aplicației RTM este după cum urmează:

```
   TarvOws {iso(1) standard(0) 15638 part20(20)
   version1(1)} DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for OWS
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

   -- Definitions of the OWS functions:
   OWS-InitialiseComm-Request ::= BST
   OWS-InitialiseComm-Response::= VST
   OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
   ABSENT, iid ABSENT, attrIdList})
   OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})
   OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})
   OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the OWS attributes:
   OwsData :: = SEQUENCE {
        encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
   OwsPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   OwsPayload :: = SEQUENCE {
              tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
              recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
   goods vehicle                                                          -- with 10 Kg
   resolution.
              axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                  -- of axles for 10 axles.
              axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                                -- with 10 Kg resolution.
              tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
        }

Ows-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
        }

StandardIdentifier ::= OBJECT IDENTIFIER
  OwsContainer ::= CHOICE {
        integer                       [0]    INTEGER,
        bitstring                     [1]    BIT STRING,
        octetstring                   [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString               [3]    UniversalString,
        beaconId                      [4]    BeaconID,
        t-apdu                        [5]    T-APDUs,
        dsrcApplicationEntityId       [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                   [7]    Dsrc-EID,
        attrIdList                    [8]    AttributeIdList,
        attrList                      [9]    AttributeList{RtmContainer},
        reserved10                    [10]   NULL,
        OwsContextmark                [11]   Ows-ContextMark,
        OwsData                       [12]   OwsData,
        reserved13                    [13]   NULL,
        reserved14                    [14]   NULL,
        time                          [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.5.6 *Elementele OwsData, acțiunile realizate și definiții*

Elementele *OwsData* sunt definite pentru compatibilitatea cu Directiva 2015/719/CE privind greutățile și dimensiunile maxime pentru vehiculele grele de marfă. Sensul lor este:

— *recordedWeight* reprezintă greutatea totală măsurată a vehiculului greu de marfă cu o rezoluție de 10 kg conform definiției din EN ISO 14906. De exemplu, o valoare de 2 500 reprezintă o greutate de 25 de tone.

— *axlesConfiguration* reprezintă configurația vehiculului greu de marfă în ceea ce privește numărul de axe. Configurația este definită cu masca binară de 20 de biți (extinsă conform EN ISO 14906).

O mască binară de 2 biți reprezintă configurația unei axe cu următorul format:

— Valoarea 00B înseamnă că valoarea este „indisponibilă” pentru că vehiculul nu deține echipament pentru colectarea greutății pe axă.

— Valoarea 01B înseamnă că axa nu este prezentă.

— Value 10B înseamnă că axa este prezentă și că greutatea a fost calculată și colectată și este prezentată în câmpul *axlesRecordedWeight*.

— Valoarea 11B este rezervată pentru utilizări viitoare.

Ultimii 4 biți sunt rezervați pentru utilizări viitoare.

Numărul de axe										
Numărul de axe pe autotractor			Numărul de axe pe remorcă							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 biți)

— *axlesRecordedWeight* reprezintă greutatea specifică înregistrată pentru fiecare axă cu o rezoluție de 10 kg. Pentru fiecare axă se utilizează doi octeți. De exemplu, o valoare de 150 reprezintă o greutate de 1 500 de kg.

Celelalte tipuri de date sunt definite în 5.4.5.

5.5.7 *Mecanismele de transfer al datelor*

DSC_64 Mecanismul pentru transferul datelor OWS între interogator și echipamentul DSRC din vehicul trebuie să fie același ca pentru datele RTM (a se vedea 5.4.6).

DSC_65 Transferul de date între platforma care colectează datele privind greutățile maxime și echipamentul DSRC din vehicul trebuie să se bazeze pe conexiunea fizică și pe interfețele și protocolul definite în secțiunea 5.6.

5.6 **Transferul de date între DSRC-VU și VU**

5.6.1 *Conexiunea fizică și interfețele*

DSC_66 Conexiunea dintre *VU* și *DSRC-VU* se poate realiza fie prin cablu fizic, fie prin comunicare fără fir cu rază scurtă de acțiune bazată pe BLE Bluetooth v4.0.

DSC_67 Indiferent de interfața și de conexiunea fizică selectate, trebuie satisfăcute următoarele cerințe:

DSC_68 (a) Pentru ca furnizori diferiți să poată fi contactați pentru a pune la dispoziție VU și DSRC-VU, inclusiv loturi diferite de DSRC-VU, conexiunea dintre VU și DSRC-VU trebuie să fie o conexiune conformă unui standard disponbil în mod public. VU trebuie să se conecteze la DSRC-VU fie

i) folosind un cablu fix de cel puțin 2 metri, cu un conector DIN 41612 H11 drept – un conector cu fișă cu 11 pini aprobat de la DSRC-VU, care se potrivește cu un conector de recepție DIN/ISO similar aprobat de la dispozitivul VU, fie

ii) folosind Bluetooth de energie redusă (BLE), fie

iii) folosind o conexiune standard ISO 11898 sau SAE J1939

DSC_69 (b) definiția interfețelor și a conexiunii dintre VU și DSRC-VU trebuie să fie compatibilă cu comenzile de protocol de aplicație definite în secțiunea 5.6.2. și

DSC_70 (c) VU și DSRC-VU trebuie să fie compatibile cu realizarea transferului de date prin conexiune în ceea ce privește performanța și alimentarea cu energie electrică.

5.6.2 *Protocolul de aplicație*

DSC_71 Protocolul de aplicație dintre echipamentul de comunicare la distanță al VU și DSRC-VU este responsabil cu transferul periodic al datelor pentru comunicarea la distanță de la VU către DSRC.

DSC_72 Sunt identificate următoarele comenzi principale:

1. Inițializarea legăturii de comunicare – solicitare
2. Inițializarea legăturii de comunicare – răspuns
3. Transmiterea datelor cu identificatorul aplicației RTM și datele utile definite de *RTM Data*
4. Confirmarea primirii datelor
5. Încheierea legăturii de comunicare – solicitare
6. Încheierea legăturii de comunicare – răspuns

DSC_73 În ASN1.0, comenzile anterioare pot fi definite ca:

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 Descrierea comenzilor și a parametrilor este următoarea:

— `RCDT-Communication Link Initialization – Request` este folosită pentru a inițializa legătura de comunicare. Comanda este transmisă de către VU la DSRC-VU. *LinkIdentifier* este setat de VU și comunicat DSRC-VU pentru a urmări o anumită legătură de comunicare.

(Notă: aceasta are ca scop compatibilitatea cu legături viitoare și cu alte aplicații/module, precum cântărirea la bord).

— `RCDT-Communication Link Initialization – Response` este utilizată de DSRC-VU pentru a furniza răspunsul la solicitarea de inițializare a legăturii de comunicare. Comanda este transmisă de DSRC-VU către VU. Comanda dă rezultatul inițializării ca răspuns = 1 (reușită) sau =0 (eșec).

DSC_75 Inițializarea legăturii de comunicare trebuie făcută doar după instalarea, etalonarea și pornirea motorului/VU este pornită.

— `RCDT-Send Data` este utilizată de VU pentru a transmite datele *RCDTData* (și anume *the remote communication Data*, datele pentru comunicarea la distanță) semnate către DSRC-VU. Datele vor fi transmise la fiecare 60 de secunde. Parametrul *DataTransactionId* identifică transmisiunea specifică de date. *LinkIdentifier* este de asemenea folosit pentru a se asigura că legătura corespunzătoare este corectă.

— `RCDT-Data Acknowledgment` este transmisă de DSRC-VU ca *feedback* pentru VU în ceea ce privește primirea datelor dintr-o comandă `RCDT-Send Data` identificată de parametrul *DataTransactionId*. Parametrul de răspuns este 1 (reușită) sau =0 (eșec). Dacă o VU primește mai mult de trei răspunsuri egale cu 0 sau dacă VU nu primește o *RCDT Data Acknowledgment* pentru o anumită *RCDT- Send Data* transmisă anterior cu un *DataTransactionId* specific, VU va genera și înregistra un eveniment.

— `RCDT-Communication Link Termination request` este transmisă de VU către DSRC-VU pentru a încheia o legătură aferentă unui anumit *LinkIdentifier*.

DSC_76 La repornirea DSRC-VU sau a unei VU, toate legăturile de comunicare existente ar trebui eliminate, deoarece ar putea exista legături „rupte” rămase în urma închiderii bruște a unei VU.

— `RCDT-Communication Link Termination – Response` este transmis de DSRC-VU către VU pentru a confirma solicitarea de încheiere a legăturii de către VU pentru *LinkIdentifier*-ul specific.

5.7 **Gestionarea erorilor**

5.7.1 *Înregistrarea și comunicarea datelor în DSRC-VU*

DSC_77 *Datele* trebuie furnizate *DSRC-VU*, deja securizate, de către funcția *VUSM*. *VUSM* trebuie să verifice că datele înregistrate în *DSRC-VU* au fost înregistrate corect. Înregistrarea și raportarea oricăror erori în transferul datelor de la *VU* către memoria *DSRC-VU* trebuie înregistrate cu tipul *EventFaultType* și valoarea de enumerare stabilită la ‘62’H (anomalie a echipamentului de comunicare la distanță), împreună cu marca temporală.

DSC_78 *VU* păstrează un fișier identificat printr-un nume unic, care este ușor identificabil de către inspectori, în scopul înregistrării „eșecurilor de comunicare internă ale VU”.

DSC_79 Dacă VUPM încearcă să obțină date VU de la modulul de securitate (pentru a le transmite către VU-DSRC), dar nu reușește, ea trebuie să înregistreze eșecul respectiv cu tipul *EventFaultType* și valoarea de enumerare stabilită la *‘62’H* (anomalie a echipamentului de comunicare la distanță), împreună cu marca temporală. Eșecul comunicării este detectat atunci când, timp de trei ori consecutiv, nu se primește un mesaj `RCDT Data Acknowledgment` Pentru `RCDT Send Data` aferentă (și anume cu același *DataTransactionId* în mesajele `Send Data și Acknowledgment`).

5.7.2 *Erori de comunicare fără fir*

DSC_80 Gestionarea erorilor de comunicare trebuie să fie în concordanță cu standardele DSRC aferente, și anume EN 300 674-1, EN 12253, EN 12795, EN 12834 și parametrii corespunzători din EN 13372.

5.7.2.1 *Erori de criptare și de semnătură*

DSC_81 Erorile de criptare și de semnătură trebuie gestionate conform definiției din apendicele 11 (Mecanisme de securitate comune) și nu sunt prezente în niciun mesaj de eroare asociat cu transferul DSRC de date.

5.7.2.2 *Înregistrarea erorilor*

Mediul DSRC este o comunicare fără fir dinamică într-un mediu de condiții de interferență și atmosferice nesigure, în special în combinațiile „REDCR portabil" și „vehicul în mișcare" implicate de această aplicație. Prin urmare, este necesar să se stabilească diferența dintre o „eroare de citire" și o condiție de „eroare". În cadrul unei tranzacții printr-o interfață fără fir, eșecul de citire este ceva obișnuit și consecința este de obicei că trebuie reîncercat, și anume BST trebuie retransmis și secvența trebuie încercată din nou, ceea ce, în majoritatea circumstanțelor, va duce la o conexiune de comunicare reușită și la transferul cu succes al datelor, cu excepția cazului în care vehiculul vizat iese din raza de acțiune în decursul perioadei necesare pentru retransmitere. (Este posibil ca o instanță „reușită" a unei operațiuni de „citire" să fi presupus mai multe încercări și reîncercări).

Eșecul de citire se poate produce din cauză că antenele nu au fost asociate în mod corespunzător (eșec de „țintire"); din cauză că una dintre antene este ecranată – în mod deliberat sau din cauza prezenței fizice a altui vehicul, a interferențelor radio, în special de la WIFI de circa 5,8 GHz sau de la alte comunicații fără fir cu acces public, sau din cauza interferențelor radar sau a condițiilor atmosferice dificile (de exemplu în timpul unei furtuni) ori pur și simplu din cauza ieșirii din raza de acțiune a comunicării DSRC. Instanțele individuale de eșecuri de citire, prin natura lor, nu pot fi înregistrate, pur și simplu deoarece comunicarea nu a avut loc.

Cu toate acestea, dacă agentul autorității de control competente vizează un vehicul și încearcă să interogheze *DSRC-VU* a acestuia, dar nu are loc niciun transfer de date reușit, este posibil ca acest eșec să se fi produs din cauza unei manipulări deliberate și, prin urmare, agentul autorității de control competente are nevoie de o modalitate de a înregistra eșecul și de a alerta colegii din aval că este posibil să existe o încălcare a normelor. Aceștia din urmă pot apoi opri vehiculul și realiza o inspecție fizică. Însă dat fiind faptul că nu a avut loc nicio comunicare reușită, DSRC-VU nu poate furniza date privind eșecul. Prin urmare, astfel de raportări depind de concepția echipamentului REDCR.

„Eșecul de citire" este diferit din punct de vedere tehnic de o „eroare". În acest context, o „eroare" reprezintă obținerea unei valori eronate.

Datele transferate către *DSRC-VU* sunt furnizate deja securizate, prin urmare trebuie verificate de către furnizorul datelor (a se vedea 5.4).

Datele transferate ulterior prin interfața aeriană sunt verificate prin verificări redundante ciclice la nivelul comunicațiilor. Dacă CRC le validează, atunci datele sunt corecte. Dacă CRC nu le validează, datele sunt transmise din nou. Probabilitatea ca date incorecte să poată trece cu succes printr-o CRC este atât de scăzută din punct de vedere statistic încât poate să nu fie luată în considerare.

Dacă CRC nu validează datele și nu este timp pentru retransmiterea și primirea datelor corecte, atunci rezultatul nu va fi o eroare, ci o instanțiere a unui tip specific de eșec de citire.

Singurele date de „eșec" semnificative care pot fi înregistrate sunt cele privind numărul inițierilor reușite de tranzacții care au loc, dar care nu duc la un transfer reușit al datelor către REDCR.

DSC_82 Prin urmare, *REDCR* înregistrează, cu marcă temporală, numărul ocaziilor în care etapa de „inițializare" a unei interogări DSRC a reușit, însă tranzacția s-a încheiat înainte ca *datele* să fie obținute cu succes de REDCR. Aceste date trebuie să fie disponibile pentru agentul autorității de control competente și trebuie stocate în memoria echipamentului REDCR. Mijloacele prin care se realizează acest lucru depind de concepția produsului sau de specificațiile unei autorități de control competente.

Singurele date de „eroare" semnificative care pot fi înregistrate sunt cele privind numărul ocaziilor în care REDCR nu reușește să decripteze *datele* primite. Însă trebuie luat notă de faptul că aceasta se va referi numai la eficiența software-ului REDCR. Datele pot fi decriptate tehnic, dar nu au sens din punct de vedere semantic.

DSC_83 Prin urmare, *REDCR* trebuie să înregistreze, cu marcă temporală, numărul ocaziilor în care a încercat, fără succes, să descifreze datele primite prin interfața DSRC.

6 TESTELE DE OPERAȚIONALITATE ȘI DE VERIFICARE PERIODICĂ PENTRU FUNCȚIA DE COMUNICARE LA DISTANȚĂ

6.1 **Generalități**

DSC_84 Pentru funcția de comunicare la distanță sunt prevăzute două tipuri de teste:

1. Un test ECHO pentru a valida canalul de comunicare fără fir *DSRC-REDCR* >>-:-<*DSRC-VU*.
2. Un test de securitate „end-to-end” (de la un capăt la altul) pentru a se asigura faptul că un card de atelier este capabil să acceseze conținutul de date criptate și semnate creat de VU și transmis prin canalul de comunicare fără fir.

6.2 **ECHO**

Prezenta clauză conține dispozițiile specifice pentru a testa numai dacă *DSRC-REDCR* >>-:-<*DSRC-VU* este activ din punct de vedere funcțional.

Obiectivul comenzii ECHO este de a permite atelierelor sau unităților de testare pentru omologarea de tip să verifice dacă legătura DSRC funcționează fără a avea nevoie de acces la elementele de securitate. Prin urmare, echipamentele de testare trebuie doar să poată inițializa o comunicare DSRC (transmițând un BST cu AID=2) și să poată apoi trimite comanda ECHO și, presupunând că DSRC funcționează, vor primi răspunsul ECHO. A se vedea secțiunea 5.4.8 pentru detalii. Presupunând că primește acest răspuns în mod corect, legătura DSRC (*DSRC-REDCR* >>-:-<*DSRC-VU*) poate fi validată ca funcționând corect.

6.3 **Testele de validare a conținutului de date securizate**

DSC_85 Acest test este realizat pentru a valida fluxul de securitate „end-to-end” al datelor. Pentru un astfel de test este necesar un cititor de testare DSRC. Cititorul de testare DSRC îndeplinește aceeași funcție și este implementat cu aceleași specificații ca cititorul folosit de forțele de ordine, cu diferența că pentru autentificarea utilizatorului cititorului de testare DSRC trebuie folosit un card de atelier și nu un card de control. Testul poate fi executat după activarea inițială a unui tahograf inteligent sau la sfârșitul procedurii de etalonare. După activare, unitatea montată pe vehicul trebuie să genereze și să comunice către DSRC-VU datele securizate pentru detectarea timpurie.

DSC_86 Personalul atelierului trebuie să poziționeze cititorul de testare DSRC la o distanță de 2-10 metri în fața vehiculului.

DSC_87 Apoi, personalul atelierului introduce un card de atelier în cititorul de testare DSRC pentru a solicita interogarea datelor pentru detectarea timpurie de la unitatea montată pe vehicul. După o interogare reușită, personalul atelierului va accesa datele primite pentru a se asigura ca au fost validate cu succes în ceea ce privește integritatea și decriptate.

Apendicele 15

MIGRAȚIE: GESTIONAREA COEXISTENȚEI MAI MULTOR GENERAȚII DE ECHIPAMENTE

CUPRINS

1. DEFINIȚII 497

2. DISPOZIȚII GENERALE 497

2.1. Prezentare generală a tranziției 497

2.2. Interoperabilitatea dintre VU și carduri 498

2.3. Interoperabilitatea dintre VU și MS 498

2.4. Interoperabilitatea dintre unitățile montate pe vehicule, cardurile de tahograf și echipamentele pentru descărcarea datelor 498

2.4.1 Descărcare directă de pe card de către IDE 498

2.4.2 Descărcare de pe card prin intermediul unei unități montate pe vehicul 499

2.4.3 Descărcarea din unitatea montată pe vehicul 499

2.5. Interoperabilitatea dintre VU și echipamentele de etalonare 499

3. PRINCIPALELE ETAPE ÎN PERIOADA ANTERIOARĂ DATEI INTRODUCERII 499

4. DISPOZIȚII PENTRU PERIOADA POSTERIOARĂ DATEI INTRODUCERII 499

1. DEFINIȚII

În sensul prezentului apendice, se folosesc următoarele definiții:

sistem tahografic inteligent: conform definiției din prezenta anexă [capitolul 1: definiția (bbb)];

sistem tahografic de prima generație: conform definiției din prezentul regulament (articolul 2: definiția 1);

sistem tahografic de a doua generație: conform definiției din prezentul regulament (articolul 2: definiția 7);

data introducerii: conform definiției din prezenta anexă [capitolul 1: definiția (ccc)];

echipament inteligent dedicat (IDE): echipament utilizat la descărcarea de date, conform definiției din apendicele 7 la prezenta anexă.

2. DISPOZIȚII GENERALE

2.1. **Prezentare generală a tranziției**

Preambulul la prezenta anexă oferă o prezentare generală a tranziției de la prima la a doua generație de sisteme tahografice.

În plus față de cele prevăzute în prezentul preambul:

— prima generație de senzori de mișcare nu va fi interoperabilă cu a doua generație de unități montate pe vehicule;

— a doua generație de senzori de mișcare va începe să fie instalată în vehicule în același timp cu a doua generație de unități montate pe vehicule;

— echipamentele de etalonare și de descărcare a datelor vor trebui să evolueze pentru a fi compatibile cu utilizarea ambelor generații de aparatură de înregistrare și de carduri de tahograf.

2.2. **Interoperabilitatea dintre VU și carduri**

Este de la sine înțeles că prima generație de carduri de tahograf este interoperabilă cu prima generație de unități montate pe vehicule (în conformitate cu anexa 1B la prezentul regulament), în timp ce a doua generație de carduri de tahograf este interoperabilă cu a doua generație de unități montate pe vehicule (în conformitate cu anexa 1C la prezentul regulament). În plus, se aplică cerințele de mai jos.

MIG_001 Cu excepția cazurilor prevăzute în cerința MIG_004 și în MIG_005, cardurile de tahograf de prima generație pot fi utilizate în continuare cu a doua generație de unități montate pe vehicule, până la data de expirare a valabilității lor. Deținătorii acestora pot însă solicita înlocuirea lor cu carduri de tahograf de a doua generație, de îndată ce acestea din urmă sunt disponibile.

MIG_002 A doua generație de unități montate pe vehicule trebuie să poată utiliza orice card valabil de conducător auto, de control și de societate de prima generație introdus.

MIG_003 Această capacitate poate fi suprimată definitiv în aceste unități montate pe vehicule, în cadrul atelierelor, astfel încât să nu mai poată fi acceptate cardurile de tahograf de prima generație. Aceasta se poate face numai după ce Comisia Europeană a lansat o procedură pentru a solicita atelierelor să acționeze în acest sens, de exemplu cu ocazia fiecărei inspecții periodice a tahografului.

MIG_004 A doua generație de unități montate pe vehicule trebuie să poată utiliza numai carduri de atelier de a doua generație.

MIG_005 Pentru stabilirea modului de funcționare, a doua generație de unități montate pe vehicule trebuie să ia în considerare numai tipurile cardurilor valabile introduse, indiferent de generația acestora.

MIG_006 Orice card de tahograf de a doua generație valabil trebuie să poată fi utilizat cu prima generație de unități montate pe vehicule exact în același mod ca un card de tahograf de prima generație de același tip.

2.3. **Interoperabilitatea dintre VU și MS**

Este de la sine înțeles că prima generație de senzori de mișcare este interoperabilă cu prima generație de unități montate pe vehicule, iar a doua generație de senzori de mișcare este interoperabilă cu a doua generație de unități montate pe vehicule. În plus, se aplică cerințele de mai jos.

MIG_007 A doua generație de unități montate pe vehicule nu va putea fi asociată și utilizată cu senzori de mișcare de prima generație.

MIG_008 Senzorii de mișcare de a doua generație pot fi asociați și utilizați numai cu a doua generație de unități montate pe vehicule sau cu ambele generații de unități montate pe vehicule.

2.4. **Interoperabilitatea dintre unitățile montate pe vehicule, cardurile de tahograf și echipamentele pentru descărcarea datelor**

MIG_009 Echipamentele pentru descărcarea datelor pot fi utilizate cu o singură generație de unități montate pe vehicule și de carduri de tahograf sau cu ambele.

2.4.1 *Descărcare directă de pe card de către IDE*

MIG_010 Datele sunt descărcate de către IDE de pe cardurile de tahograf de o anumită generație introduse în cititoarele lor de carduri, cu utilizarea mecanismelor de securitate și a protocolului de descărcare a datelor aferente generației respective, iar datele descărcate trebuie să aibă formatul definit pentru generația respectivă.

MIG_011 Pentru a permite controlarea conducătorilor auto de către autorități de control care nu aparțin de UE, trebuie să fie de asemenea posibilă descărcarea cardurilor de conducător auto (și de atelier) de a doua generație exact în același mod ca și cardurile de conducător autor (și de atelier) de prima generație. Această descărcare trebuie să includă:

— EF nesemnate `IC` și `ICC`,

— EF nesemnate (prima generație) `Card_Certificate` și `CA_Certificate`,

— celelalte EF cu date de aplicație (din cadrul TACHO DF) impuse de protocolul de descărcare pentru cardurile de prima generație. Aceste informații trebuie să fie protejate de o semnătură digitală, în conformitate cu mecanismele de securitate aferente primei generații.

Această descărcare trebuie să nu includă EF cu date de aplicație care sunt prezente doar în cardurile de conducător auto (și de atelier) de a doua generație (EF cu date de aplicație din cadrul TACHO_G2 DF).

2.4.2 *Descărcare de pe card prin intermediul unei unități montate pe vehicul*

MIG_012 Datele de pe un card de a doua generație introdus într-o unitate montată pe vehicul de prima generație se descarcă folosind protocolul de descărcare a datelor aferent primei generații. Cardul trebuie să răspundă comenzilor date de unitatea montată pe vehicul exact în același mod ca un card de prima generație, iar datele descărcate trebuie să aibă același format ca datele descărcate de pe un card de prima generație.

MIG_013 Datele de pe un card de prima generație introdus într-o unitate montată pe vehicul de a doua generație se descarcă folosind protocolul de descărcare a datelor definit în apendicele 7 la prezenta anexă. Unitatea montată pe vehicul trebuie să transmită comenzi cardului exact în același mod ca o unitate montată pe vehicul de prima generație, iar datele descărcate trebuie să respecte formatul definit pentru cardurile de prima generație.

2.4.3 *Descărcarea din unitatea montată pe vehicul*

MIG_014 Datele din a doua generație de unități montate pe vehicule se descarcă folosind mecanismele de securitate aferente celei de-a doua generații și protocolul de descărcare a datelor specificat în apendicele 7 la prezenta anexă.

MIG_015 Pentru a permite controlarea conducătorilor auto de către autorități de control care nu aparțin de UE, precum și descărcarea de către ateliere din afara UE a datelor din unitatea montată pe vehicul, poate exista opțiunea descărcării datelor din a doua generație de unități montate pe vehicule cu utilizarea mecanismelor de securitate aferente primei generații și a protocolului de descărcare a datelor aferent primei generații. Datele descărcate trebuie să aibă același format ca datele descărcate dintr-o unitate montată pe vehicul de prima generație. Această opțiune poate fi selectată cu ajutorul comenzilor din meniu.

2.5. **Interoperabilitatea dintre VU și echipamentele de etalonare**

MIG_016 Echipamentele de etalonare trebuie să poată efectua etalonarea fiecărei generații de tahografe, utilizând protocolul de etalonare aferent generației respective. Echipamentele de etalonare pot fi utilizate cu o singură generație de tahografe sau cu ambele.

3. PRINCIPALELE ETAPE ÎN PERIOADA ANTERIOARĂ DATEI INTRODUCERII

MIG_017 Certificatele și cheile de testare trebuie să se afle la dispoziția producătorilor cel târziu cu **30 de luni** înainte de data introducerii.

MIG_018 Testele de interoperabilitate trebuie să fie gata de demarare, dacă sunt solicitate de producători, cel târziu cu **15 luni** înainte de data introducerii.

MIG_017 Certificatele și cheile oficiale trebuie să se afle la dispoziția producătorilor cel târziu cu **12 luni** înainte de data introducerii.

MIG_020 Statele membre trebuie să fie în măsură să emită carduri de atelier de a doua generație cel târziu cu **3 luni** înainte de data introducerii.

MIG_021 Statele membre trebuie să fie în măsură să emită toate tipurile de carduri de tahograf de a doua generație cel târziu cu **1 lună înainte de data introducerii**.

4. DISPOZIȚII PENTRU PERIOADA POSTERIOARĂ DATEI INTRODUCERII

MIG_022 După data introducerii, statele membre trebuie să emită numai carduri de tahograf de a doua generație.

MIG_023 Producătorilor de unități montate pe vehicule / senzori de mișcare li se permite să producă unități montate pe vehicule / senzori de mișcare de prima generație atât timp cât acestea / aceștia sunt utilizate / utilizați în practică, astfel încât componentele defecte să poată fi înlocuite.

MIG_024 Producătorilor de unități montate pe vehicule / senzori de mișcare li se permite să solicite și să obțină menținerea omologării de tip pentru tipurile deja omologate de unități montate pe vehicule / senzori de mișcare de prima generație.

Apendicele 16.

ADAPTOR PENTRU VEHICULELE DIN CATEGORIILE M1 ȘI N1

CUPRINS

1. ABREVIERI ȘI DOCUMENTE DE REFERINȚĂ 501

1.1. Abrevieri 501

1.2. Standarde de referință 501

2. CARACTERISTICILE GENERALE ȘI FUNCȚIILE ADAPTORULUI 502

2.1. Descriere generală a adaptorului 502

2.2. Funcții 502

2.3. Securitate 502

3. CERINȚE PENTRU APARATURA DE ÎNREGISTRARE ÎN CAZUL INSTALĂRII UNUI ADAPTOR 502

4. CERINȚE FUNCȚIONALE ȘI DE CONSTRUCȚIE PENTRU ADAPTOR 503

4.1. Interfațare și adaptarea impulsurilor de viteză de intrare 503

4.2. Orientarea impulsurilor de intrare către senzorul de mișcare integrat 503

4.3. Senzorul de mișcare integrat 503

4.4. Cerințe de securitate 503

4.5. Caracteristici de performanță 504

4.6. Materiale 504

4.7. Marcaje 504

5. INSTALAREA APARATURII DE ÎNREGISTRARE ÎN CAZUL UTILIZĂRII UNUI ADAPTOR 504

5.1. Instalarea 504

5.2. Sigilarea 505

6. CONTROALE, INSPECȚII ȘI REPARAȚII 505

6.1. Inspecții periodice 505

7. OMOLOGAREA DE TIP A APARATURII DE ÎNREGISTRARE ÎN CAZUL UTILIZĂRII UNUI ADAPTOR 505

7.1. Considerații generale 505

7.2. Certificat de funcționare 506

1. ABREVIERI ȘI DOCUMENTE DE REFERINȚĂ

1.1. **Abrevieri**

TBD de precizat

VU Unitate montată pe vehicul

1.2. **Standarde de referință**

ISO16844-3 *Road vehicles – Tachograph systems – Part 3: Motion sensor interface*

2. CARACTERISTICILE GENERALE ȘI FUNCȚIILE ADAPTORULUI

2.1. **Descriere generală a adaptorului**

ADA_001 Adaptorul furnizează unei unități montate pe vehicul conectate date de mișcare securizate, care sunt în mod permanent reprezentative pentru viteza vehiculului și pentru distanța parcursă de acesta.

Adaptorul este destinat numai vehiculelor care, conform prezentului regulament, trebuie să fie echipate cu aparatură de înregistrare.

Acesta se instalează și se utilizează numai la tipurile de vehicule definite la definiția (yy), „adaptor", acolo unde este imposibil din punct de vedere mecanic să se instaleze orice alt tip de senzor de mișcare existent care respectă dispozițiile prezentei anexe și ale apendicelor 1-16 la prezenta anexă.

Adaptorul nu se conectează mecanic la un element mobil al vehiculului, ci se conectează la impulsurile de viteză/distanță generate de senzori integrați sau de interfețe alternative.

ADA_002 Un senzor de mișcare omologat de tip (conform dispozițiilor din secțiunea 8 a prezentei anexe IC, Omologarea de tip a aparaturii de înregistrare și a cardurilor de tahograf) este montat în carcasa adaptorului, care conține de asemenea un dispozitiv de convertire a impulsurilor al cărui rol este să orienteze impulsurile de intrare către senzorul de mișcare integrat. Senzorul de mișcare integrat este conectat la VU, astfel încât interfața dintre VU și adaptor să respecte cerințele stabilite în standardul ISO16844-3.

2.2. **Funcții**

ADA_003 Adaptorul are următoarele funcții:

— interfațare și adaptarea impulsurilor de viteză de intrare,

— orientarea impulsurilor de intrare către senzorul de mișcare integrat,

— toate funcțiile senzorului de mișcare integrat, care furnizează VU date de mișcare securizate.

2.3. **Securitate**

ADA_004 Securitatea adaptorului nu se certifică conform obiectivului general de securitate pentru senzorii de mișcare definit în apendicele 10 la prezenta anexă. În locul acestuia, se aplică cerințele de securitate specificate în secțiunea 4.4 din prezentul apendice.

3. CERINȚE PENTRU APARATURA DE ÎNREGISTRARE ÎN CAZUL INSTALĂRII UNUI ADAPTOR

Cerințele din următoarele capitole indică modul în care trebuie înțelese cerințele din prezenta anexă în cazul utilizării unui adaptor. Numerele aferente cerințelor din anexa IC sunt menționate între paranteze.

ADA_005 Aparatura de înregistrare a oricărui vehicul prevăzut cu un adaptor trebuie să respecte toate dispozițiile prezentei anexe, cu excepția cazului în care se prevede altfel în prezentul apendice.

ADA_006 Atunci când este instalat un adaptor, aparatura de înregistrare include cabluri, adaptorul în sine (inclusiv un senzor de mișcare) și o VU (01).

ADA_007 Funcția de detectare a evenimentelor și/sau a anomaliilor aparaturii de înregistrare se modifică după cum urmează:

— evenimentul „întreruperea alimentării cu energie electrică" este declanșat de VU, atunci când aceasta nu se află în modul de etalonare, în cazul oricărei întreruperi de peste 200 de milisecunde a alimentării cu energie electrică a senzorului de mișcare integrat (79)

— evenimentul „eroare a datelor de mișcare" este declanșat de VU în cazul întreruperii fluxului normal de date dintre senzorul de mișcare integrat și VU și/sau în cazul unor erori de integritate sau de autentificare a datelor survenite în timpul schimbului de date dintre senzorul de mișcare integrat și VU (83)

— evenimentul „tentativă de încălcare a securității” este declanșat de VU, atunci când aceasta nu se află în modul de etalonare, în cazul oricărui eveniment care afectează securitatea senzorului de mișcare integrat (85)

— anomalia „aparatura de înregistrare” este declanșată de VU, atunci când aceasta nu se află în modul de etalonare, în cazul oricărei defecțiuni a senzorului de mișcare integrat (88)

ADA_008 Anomaliile adaptorului care pot fi detectate de aparatura de înregistrare sunt cele legate de senzorul de mișcare integrat (88).

ADA_009 Funcția de etalonare a VU permite asocierea automată a senzorului de mișcare integrat cu VU (202, 204).

4. CERINȚE FUNCȚIONALE ȘI DE CONSTRUCȚIE PENTRU ADAPTOR

4.1. **Interfațare și adaptarea impulsurilor de viteză de intrare**

ADA_011 Interfața de intrare a adaptorului trebuie să accepte impulsuri de frecvență care sunt reprezentative pentru viteza vehiculului și pentru distanța parcursă de acesta. Caracteristicile electrice ale impulsurilor de intrare sunt: *a se defini de către producător*. Trebuie să existe reglaje, accesibile numai producătorului adaptorului și numai atelierului autorizat care efectuează instalarea adaptorului, care să permită interfațarea corectă a intrării adaptorului cu vehiculul, dacă este cazul.

ADA_012 Interfața de intrare a adaptorului trebuie să fie capabilă, dacă este cazul, să înmulțească sau să împartă impulsurile de frecvență ale impulsurilor de viteză de intrare la un factor fix, pentru adaptarea semnalului la intervalul de factori k definit în prezenta anexă (4 000-25 000 de impulsuri/km). Acest factor fix poate fi programat numai de producătorul adaptorului și de atelierul autorizat care efectuează instalarea adaptorului.

4.2. **Orientarea impulsurilor de intrare către senzorul de mișcare integrat**

ADA_013 Impulsurile de intrare, posibil adaptate după cum se specifică mai sus, sunt direcționate către senzorul de mișcare integrat, astfel încât fiecare impuls de intrare să fie detectat de senzorul de mișcare.

4.3. **Senzorul de mișcare integrat**

ADA_014 Senzorul de mișcare integrat este stimulat de impulsurile induse, permițându-i astfel să genereze date de mișcare care redau cu precizie deplasarea vehiculului, ca și cum ar fi interfațat mecanic cu o parte mobilă a vehiculului.

ADA_015 Datele de identificare ale senzorului de mișcare integrat sunt folosite de VU pentru identificarea adaptorului (95).

ADA_016 Se consideră că datele de instalare stocate în senzorul de mișcare integrat reprezintă datele de instalare ale adaptorului (122).

4.4. **Cerințe de securitate**

ADA_017 Carcasa adaptorului se proiectează în așa fel încât să nu poată fi deschisă. Carcasa se sigilează, astfel încât tentativele de manipulare fizică frauduloasă să fie ușor de detectat (de exemplu, prin inspecție vizuală, a se vedea ADA_035). Sigiliile respectă aceleași cerințe ca cele folosite pentru sigiliile senzorilor de mișcare (398-406)

ADA_018 Nu trebuie să fie posibilă scoaterea senzorului de mișcare integrat din adaptor fără ruperea sigiliului sau a sigiliilor carcasei adaptorului sau fără ruperea sigiliului dintre senzor și carcasa adaptorului (a se vedea ADA_034).

ADA_019 Adaptorul trebuie să asigure faptul că datele de mișcare nu pot fi prelucrate și extrase decât din intrarea adaptorului.

4.5. **Caracteristici de performanță**

ADA_020 Adaptorul trebuie să fie perfect funcțional în intervalul de temperatură definit de producător.

ADA_021 Adaptorul este perfect funcțional în intervalul de umiditate 10 %-90 % (214).

ADA_022 Adaptorul este protejat împotriva supratensiunilor, a inversării polarității sursei de alimentare și a scurtcircuitelor (216).

ADA_023 Adaptorul trebuie fie:

— să reacționeze la un câmp magnetic care perturbă detectarea deplasării vehiculului; în acest caz, unitatea montată pe vehicul va înregistra și va stoca o anomalie a senzorului (88), fie

— să fie prevăzut cu un element detector care să fie protejat împotriva câmpurilor magnetice sau imun la acestea (217).

ADA_024 Adaptorul trebuie să respecte dispozițiile Regulamentului internațional CEE-ONU nr. 10, referitor la compatibilitatea electromagnetică, și trebuie să fie protejat împotriva descărcărilor electrostatice și a curenților tranzitorii (218).

4.6. **Materiale**

ADA_025 Adaptorul trebuie să corespundă indicelui de protecție *(a se defini de către producător, în funcție de poziția de instalare)* (220, 221).

ADA_026 Carcasa adaptorului este de culoare galbenă.

4.7. **Marcaje**

ADA_027 Pe adaptor trebuie fixată o plăcuță descriptivă care conține următoarele detalii:

— denumirea și adresa producătorului adaptorului,

— numărul de componentă al producătorului și anul de fabricație al adaptorului,

— marca de omologare a tipului de adaptor sau a aparaturii de înregistrare care conține adaptorul,

— data instalării adaptorului,

— numărul de identificare al vehiculului pe care acesta a fost instalat.

ADA_028 Plăcuța descriptivă trebuie să includă de asemenea următoarele detalii (dacă acestea nu pot fi citite direct din afară pe senzorul de mișcare integrat):

— denumirea producătorului senzorului de mișcare integrat,

— numărul de componentă al producătorului și anul de fabricație al senzorului de mișcare integrat,

— marca de omologare a senzorului de mișcare integrat.

5. INSTALAREA APARATURII DE ÎNREGISTRARE ÎN CAZUL UTILIZĂRII UNUI ADAPTOR

5.1. **Instalarea**

ADA_029 Adaptoarele care urmează a fi instalate pe vehicule trebuie instalate numai de producătorii vehiculelor sau de ateliere aprobate, autorizate să instaleze, să activeze și să etaloneze tahografe digitale și tahografe inteligente.

ADA_030 Un astfel de atelier aprobat care instalează adaptorul reglează interfața de intrare și selectează raportul de divizare al semnalului de intrare (dacă este cazul).

ADA_031 Un astfel de atelier aprobat care instalează adaptorul sigilează apoi carcasa adaptorului.

ADA_032 Adaptorul este instalat cât mai aproape de acea parte a vehiculului care furnizează impulsurile de intrare.

ADA_033 Cablurile de alimentare ale adaptorului sunt de culoare roșie (polul pozitiv), respectiv neagră (masa).

5.2. **Sigilarea**

ADA_034 Se aplică următoarele cerințe privind sigilarea:

— carcasa adaptorului se sigilează (a se vedea ADA_017),

— carcasa senzorului integrat se sigilează de carcasa adaptorului, cu excepția situației în care nu este posibilă scoaterea senzorului din carcasa adaptorului fără ruperea sigiliului (sigiliilor) carcasei adaptorului (a se vedea ADA_18),

— carcasa adaptorului se sigilează de vehicul,

— conexiunea dintre adaptor și echipamentul care furnizează impulsurile de intrare ale acestuia se sigilează la ambele capete (în măsura în care este posibil în mod rezonabil).

6. CONTROALE, INSPECȚII ȘI REPARAȚII

6.1. **Inspecții periodice**

ADA_035 Atunci când este folosit un adaptor, fiecare inspecție periodică [inspecție periodică înseamnă o inspecție în conformitate cu cerințele (409)-(413) din anexa 1C] asupra aparaturii de înregistrare trebuie să includă următoarele controale:

— verificarea faptului că adaptorul poartă marcajele de omologare de tip corespunzătoare,

— verificarea faptului că sigiliul de pe adaptor și cel de pe conexiunile sale sunt intacte,

— verificarea faptului că adaptorul este instalat astfel cum este indicat pe plăcuța de instalare,

— verificarea faptului că adaptorul este instalat astfel cum este specificat de producătorului adaptorului și/sau al vehiculului,

— verificarea faptului că este autorizată montarea unui adaptor pe vehiculul care face obiectul inspecției.

ADA_036 Aceste inspecții includ o etalonare și o înlocuire a tuturor sigiliilor, indiferent de starea lor.

7. OMOLOGAREA DE TIP A APARATURII DE ÎNREGISTRARE ÎN CAZUL UTILIZĂRII UNUI ADAPTOR

7.1. **Considerații generale**

ADA_037 Aparatura de înregistrare este prezentată completă în vederea omologării, împreună cu adaptorul (425).

ADA_038 Orice adaptor poate fi prezentat pentru propria omologare de tip sau pentru omologarea de tip în calitate de componentă a unei aparaturi de înregistrare.

ADA_039 O asemenea omologare de tip include teste de funcționare care implică folosirea adaptorului. Rezultatele pozitive obținute în cadrul acestor teste sunt menționate într-un certificat corespunzător (426).

7.2. **Certificat de funcționare**

ADA_040 Producătorului adaptorului i se eliberează un certificat de funcționare pentru un adaptor sau pentru o aparatură de înregistrare care include un adaptor numai în cazul în care au fost înregistrate rezultate pozitive în cadrul tuturor testelor de funcționare minime menționate mai jos.

Nr.	Test	Descriere	Cerințe conexe
1.	**Examinare administrativă**		
1.1	Documentație	Corectitudinea documentației adaptorului	
2.	**Inspecție vizuală**		
2.1.	Respectarea documentației de către adaptor		
2.2.	Identificare/marcaje a(le) adaptorului		ADA_027, ADA_028
2.3	Materiale ale adaptorului		(219)-(223) ADA_026
2.4.	Sigilarea		ADA_017, ADA_018, ADA_034
3.	**Teste de funcționare**		
3.1	Orientarea impulsurilor de viteză către senzorul de mișcare integrat		ADA_013
3.2	Interfațare și adaptarea impulsurilor de viteză de intrare		ADA_011, ADA_012
3.3	Precizia măsurării deplasării		(30) – (35), (217)
4.	**Teste de mediu**		
4.1	Rezultatele testelor efectuate de producător	Rezultatele testelor de mediu efectuate de producător	ADA_020, ADA_021, ADA_022, ADA_024
5.	**EMC**		
5.1	emisii radiate și susceptibilitate	Verificarea conformității cu Directiva 2006/28/CE	ADA_024
5.2	Rezultatele testelor efectuate de producător	Rezultatele testelor de mediu efectuate de producător	ADA_024