II

(Nelegislatívne akty)

NARIADENIA

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2016/799

z 18. marca 2016,

ktorým sa vykonáva nariadenie Európskeho parlamentu a Rady (EÚ) č. 165/2014, ktorým sa ustanovujú požiadavky na konštrukciu, skúšanie, montáž, prevádzku a opravu tachografov a ich komponentov

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 165/2014 zo 4. februára 2014 o tachografoch v cestnej doprave ([1]), a najmä na jeho článok 11 a článok 12 ods. 7,

keďže:

(1) Nariadením (EÚ) č. 165/2014 sa zaviedla druhá generácia digitálnych tachografov nazývaných inteligentné tachografy, ktoré zahŕňajú pripojenie k zariadeniu globálneho navigačného satelitného systému (GNSS), komunikačné zariadenie na diaľkovú včasnú detekciu a rozhranie s inteligentnými dopravnými systémami. Je potrebné určiť špecifikácie technických požiadaviek na konštrukciu inteligentných tachografov.

(2) Zariadenie na diaľkovú včasnú detekciu zavedené článkom 9 ods. 4 nariadenia (EÚ) č. 165/2014 by malo prenášať úradníkovi cestnej kontroly údaje z digitálneho tachografu a informácie týkajúce sa hmotnosti a hmotnosti na nápravu celej jazdnej súpravy (ťahač a príves alebo náves), v súlade so smernicou Európskeho parlamentu a Rady 96/53/ES ([2]). To by malo umožniť účinnú a rýchlu kontrolu vozidiel kontrolnými orgánmi s menším počtom elektronických zariadení v kabíne vozidla.

(3) V súlade so smernicou 96/53/ES by sa v prípade zariadenia na diaľkovú včasnú detekciu mali používať normy CEN DSRC ([3]) uvedené v tejto smernici, a to vo frekvenčnom pásme 5795 – 5805 MHz. Keďže toto frekvenčné pásmo sa využíva aj pri elektronickom vyberaní mýta a s cieľom vyhnúť sa rušeniu medzi mýtnymi a kontrolnými aplikáciami, nemali by úradníci cestnej kontroly používať zariadenia na diaľkovú včasnú detekciu na miestach výberu mýta.

(4) Na zachovanie úrovne bezpečnosti digitálneho tachografu je potrebné v prípade inteligentného tachografu zaviesť nové bezpečnostné mechanizmy, aby sa odstránili súčasné bezpečnostné medzery. Jednou z takýchto medzier je neurčený dátum skončenia platnosti digitálneho certifikátu. Na zabezpečenie súladu s najlepšími postupmi v otázkach bezpečnosti sa odporúča zabrániť používaniu digitálnych certifikátov bez určeného dátumu skončenia platnosti. Obdobie platnosti pre bežnú prevádzku jednotky vozidla by malo byť 15 rokov a malo by začať plynúť dňom vydania digitálnych certifikátov jednotky vozidla. Po uplynutí obdobia platnosti by sa jednotky vozidla mali vymeniť.

([1]) Ú. v. EÚ L 60, 28.2.2014, s. 1.

([2]) Smernica Rady 96/53/ES z 25. júla 1996, ktorou sa v Spoločenstve stanovujú najväčšie prípustné rozmery niektorých vozidiel vo vnútroštátnej a medzinárodnej cestnej doprave a maximálna povolená hmotnosť v medzinárodnej cestnej doprave (Ú. v. ES L 235, 17.9.1996, s. 59).

([3]) Normy Európskeho výboru pre normalizáciu (CEN) týkajúce sa vyhradenej komunikácie krátkeho dosahu (DSRC): EN 12253, EN 12795, EN 12834, EN 13372 a ISO 14906.

(5) Poskytovanie zabezpečených a spoľahlivých informácií o polohe je dôležitým prvkom účinnej prevádzky inteligentných tachografov. Preto je vhodné zabezpečiť ich kompatibilitu so službami s pridanou hodnotou, ktoré poskytuje program Galileo, ako je stanovené v nariadení Európskeho parlamentu a Rady (EÚ) č. 1285/2013 ([1]), s cieľom zvýšiť zabezpečenie inteligentných tachografov.

(6) V súlade s článkom 8 ods. 1, článkom 9 ods. 1 a článkom 10 ods. 1 a 2 nariadenia (EÚ) č. 165/2014 by sa bezpečnostné mechanizmy zavedené týmto nariadením mali uplatňovať 36 mesiacov po nadobudnutí účinnosti potrebných vykonávacích aktov, aby sa výrobcom umožnil vývoj novej generácie inteligentných tachografov a získanie osvedčení o typovom schválení od príslušných orgánov.

(7) V súlade s nariadením (EÚ) č. 165/2014 by vozidlá prvýkrát evidované v členskom štáte 36 mesiacov po nadobudnutí účinnosti tohto nariadenia Komisie mali byť vybavené inteligentným tachografom, ktorý spĺňa požiadavky stanovené v tomto nariadení Komisie. V každom prípade by každé vozidlo prevádzkované v inom členskom štáte, než je členský štát, v ktorom bolo vozidlo zaevidované, malo byť vybavené inteligentným tachografom spĺňajúcim príslušné požiadavky, a to 15 rokov po dni začiatku uplatňovania týchto požiadaviek.

(8) V nariadení Komisie (ES) č. 68/2009 ([2]) bolo počas prechodného obdobia, ktoré sa skončilo 31. decembra 2013, povolené používať adaptér umožňujúci montáž tachografov vo vozidlách typu M1 a N1. V dôsledku technických ťažkostí spojených s hľadaním alternatívy k používaniu adaptéra odborníci z oblasti automobilového priemyslu a výroby tachografov spolu s Komisiou dospeli k záveru, že nie je realizovateľné žiadne alternatívne riešenie nahrádzajúce adaptér, ktoré by pre výrobu neznamenalo vysoké náklady, neúmerné veľkosti trhu. Preto by používanie adaptéra vo vozidlách typu M1 a N1 malo byť trvalo povolené.

(9) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru uvedeným v článku 42 ods. 3 nariadenia (EÚ) č. 165/2014,

PRIJALA TOTO NARIADENIE:

Článok 1

Predmet úpravy a rozsah pôsobnosti

1. V tomto nariadení sú stanovené ustanovenia potrebné na jednotné uplatňovanie týchto aspektov týkajúcich sa tachografov:

a) zaznamenávanie polohy vozidla na určitých miestach počas denného pracovného času vodiča;

b) diaľková včasná detekcia možnej manipulácie alebo zneužitia inteligentných tachografov;

c) rozhranie s inteligentnými dopravnými systémami;

d) administratívne a technické požiadavky na postupy typového schvaľovania tachografov vrátane bezpečnostných mechanizmov.

2. Konštrukcia, skúšanie, montáž, kontrola, prevádzka a oprava inteligentných tachografov a ich komponentov musí spĺňať technické požiadavky stanovené v prílohe 1C k tomuto nariadeniu.

3. Iné tachografy ako inteligentné tachografy musia naďalej spĺňať, pokiaľ ide o konštrukciu, skúšanie, montáž, kontrolu, prevádzku a opravu, požiadavky stanovené v prílohe 1, prípadne v prílohe 1B k nariadeniu Rady (EHS) č. 3821/85 ([3]).

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1285/2013 z 11. decembra 2013 o zriadení a využívaní európskych systémov satelitnej navigácie, ktorým sa ruší nariadenie Rady (ES) č. 876/2002 a nariadenie Európskeho parlamentu a Rady (ES) č. 683/2008 (Ú. v. EÚ L 347, 20.12.2013, s. 1).

([2]) Nariadenie Komisie (ES) č. 68/2009 z 23. januára 2009, ktorým sa deviatykrát prispôsobuje technickému pokroku nariadenie Rady (EHS) č. 3821/85 o záznamovom zariadení v cestnej doprave (Ú. v. EÚ L 21, 24.1.2009, s. 3).

([3]) Nariadenie Rady (EHS) č. 3821/85 z 20. decembra 1985 o záznamovom zariadení v cestnej doprave (Ú. v. ES L 370, 31.12.1985, s. 8).

4. Podľa článku 10d smernice Rady 96/53/ES zariadenia na diaľkovú včasnú detekciu prenášajú aj údaje o hmotnosti, ktoré poskytuje interný palubný vážiaci systém, na účely včasnej detekcie podvodov.

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje vymedzenie pojmov stanovené v článku 2 nariadenia (EÚ) č. 165/2014.

Okrem toho sa uplatňuje toto vymedzenie pojmov:

1. „digitálny tachograf“ alebo „tachograf prvej generácie“ je iný digitálny tachograf ako inteligentný tachograf;

2. „externé zariadenie GNSS“ je zariadenie, ktoré obsahuje prijímač GNSS, ak jednotku vozidla netvorí jediná jednotka, ako aj ďalšie komponenty potrebné na ochranu prenosu údajov o polohe do zvyšnej časti jednotky vozidla;

3. „informačná zložka“ je úplná zložka v elektronickej alebo papierovej forme, ktorá obsahuje všetky informácie poskytnuté výrobcom alebo jeho obchodným zástupcom orgánu pre typové schvaľovanie na účely typového schválenia tachografu alebo jeho komponentu, vrátane osvedčení uvedených v článku 12 ods. 3 nariadenia (EÚ) č. 165/2014, výsledkov skúšok stanovených v prílohe 1C k tomuto nariadeniu, ako aj nákresov, fotografií a ďalších príslušných dokumentov;

4. „informačný balík“ je informačná zložka v elektronickej alebo papierovej forme, doplnená akýmikoľvek ďalšími dokumentmi, ktoré k informačnej zložke pridal orgán pre typové schvaľovanie počas výkonu svojich funkcií, vrátane osvedčenia o typovom schválení ES tachografu alebo jeho komponentu na konci postupu typového schvaľovania;

5. „obsah informačného balíka“ je dokument so zoznamom očíslovaných položiek obsahu informačného balíka, v ktorom sú uvedené všetky dôležité časti tohto balíka. Formát daného dokumentu musí rozlišovať jednotlivé za sebou idúce kroky postupu typového schvaľovania ES vrátane dátumov všetkých revízií a aktualizácií príslušného balíka;

6. „zariadenie na diaľkovú včasnú detekciu“ je vybavenie jednotky vozidla, ktoré sa používa na vykonávanie cielených cestných kontrol;

7. „inteligentný tachograf“ alebo „tachograf druhej generácie“ je digitálny tachograf, ktorý spĺňa požiadavky stanovené v článkoch 8, 9 a 10 nariadenia (EÚ) č. 165/2014, ako aj v prílohe 1C k tomuto nariadeniu;

8. „komponent tachografu“ alebo „komponent“ je každý z týchto prvkov: jednotka vozidla, snímač pohybu, tachografová karta, záznamový list, externé zariadenie GNSS a zariadenie na diaľkovú včasnú detekciu;

9. „orgán pre typové schvaľovanie“ je orgán členského štátu oprávnený vykonávať typové schvaľovanie tachografu alebo jeho komponentov, schvaľovací proces, vydávanie a v prípade potreby odnímanie osvedčení o typovom schválení, plniť úlohu kontaktného miesta pre orgány pre typové schvaľovanie ostatných členských štátov a zabezpečovať, aby výrobcovia plnili svoje povinnosti, pokiaľ ide o dodržiavanie požiadaviek stanovených v tomto nariadení.

Článok 3

Služby založené na lokalizácii

1. Výrobcovia musia zabezpečiť, aby inteligentné tachografy boli kompatibilné so službami určovania polohy, ktoré poskytujú systémy Galileo a Európska geostacionárna navigačná prekrývacia služba (EGNOS).

2. Výrobcovia sa môžu rozhodnúť, že popri systémoch uvedených v odseku 1 zabezpečia kompatibilitu aj s ďalšími satelitnými navigačnými systémami.

Článok 4

Postup typového schvaľovania tachografu a komponentov tachografu

1. Výrobca alebo jeho obchodný zástupca podajú žiadosť o typové schválenie tachografu, niektorého z jeho komponentov alebo skupiny komponentov orgánu pre typové schvaľovanie, ktorý si určí každý členský štát. Žiadosť musí obsahovať informačnú zložku s informáciami o každom z príslušných komponentov, v prípade potreby spolu s osvedčeniami o typovom schválení ostatných komponentov potrebných na zostavenie tachografu, ako aj so všetkými ostatnými príslušnými dokumentmi.

2. Členský štát udelí typové schválenie podľa potreby každému tachografu, komponentu alebo skupine komponentov, ktoré spĺňajú administratívne a technické požiadavky uvedené v článku 1 ods. 2 alebo 3, podľa potreby. V tom prípade orgán pre typové schvaľovanie vydá žiadateľovi osvedčenie o typovom schválení, ktoré musí byť v súlade so vzorom stanoveným v prílohe II k tomuto nariadeniu.

3. Orgán pre typové schvaľovanie môže požiadať výrobcu alebo jeho obchodného zástupcu o poskytnutie doplňujúcich informácií.

4. Výrobca alebo jeho obchodný zástupca poskytnú orgánom pre typové schvaľovanie, ako aj subjektom zodpovedným za vydávanie osvedčení uvedených v článku 12 ods. 3 nariadenia (EÚ) č. 165/2014 toľko tachografov alebo komponentov tachografu, koľko je potrebných na uspokojivé vykonanie postupu typového schvaľovania.

5. Ak výrobca alebo jeho obchodný zástupca žiadajú o typové schválenie určitých komponentov alebo skupín komponentov tachografu, poskytnú orgánom pre typové schvaľovanie ostatné komponenty, ktoré už majú osvedčenie o typovom schválení, ako aj všetky ďalšie diely potrebné na zostavenie celého tachografu, aby tieto orgány mohli vykonať potrebné skúšky.

Článok 5

Zmeny typového schválenia

1. Výrobca alebo jeho obchodný zástupca musia bez meškania informovať orgán pre typové schvaľovanie, ktorý udelil pôvodné typové schválenie, o každej zmene softvéru alebo hardvéru tachografu alebo o zmene povahy materiálov použitých na jeho výrobu, ktoré sú uvedené v informačnom balíku, a musia podať žiadosť o zmenu typového schválenia.

2. Orgán pre typové schvaľovania môže revidovať alebo rozšíriť existujúce typové schválenie, alebo udeliť nové typové schválenie podľa povahy a vlastností zmien.

Orgán pre typové schvaľovanie vykoná „revíziu“, ak zmeny softvéru alebo hardvéru tachografu alebo zmeny povahy materiálov použitých na jeho výrobu považuje za malé. V takých prípadoch orgán pre typové schvaľovanie vydá revidované dokumenty v rámci informačného balíka, v ktorých uvedie povahu vykonaných zmien a dátum ich schválenia. Na splnenie tejto požiadavky postačuje aktualizovaná verzia informačného balíka v konsolidovanej forme doplnená podrobným opisom vykonaných zmien.

Orgán pre typové schvaľovanie vykoná „rozšírenie“, ak zmeny softvéru alebo hardvéru tachografu alebo zmeny povahy materiálov použitých na jeho výrobu považuje za podstatné. V takých prípadoch môže orgán požadovať vykonanie nových skúšok a informovať o tom výrobcu alebo jeho obchodného zástupcu. Ak sú výsledky skúšok uspokojivé, orgán pre typové schvaľovanie vydá revidované osvedčenie o typovom schválení, v ktorom je uvedené číslo odkazujúce na udelené rozšírenie. V osvedčení o typovom schválení sa uvedie dôvod rozšírenia a dátum jeho vydania.

3. V obsahu informačného balíka sa uvádza dátum posledného rozšírenia alebo revízie typového schválenia, alebo dátum poslednej konsolidácie aktualizovanej verzie typového schválenia.

4. Nové typové schválenie je potrebné, ak by požadované zmeny tachografu alebo jeho komponentov s udeleným typovým schválením viedli k vydaniu nového osvedčenia zabezpečenia alebo interoperability.

Článok 6

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Uplatňuje sa od 2. marca 2016.

Prílohy sa však uplatňujú od 2. marca 2019, s výnimkou dodatku 16, ktorý sa uplatňuje od 2. marca 2016.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 18. marca 2016

Za Komisiu

predseda

Jean-Claude JUNCKER

PRÍLOHA I C

Požiadavky na konštrukciu, skúšanie, montáž a kontrolu

ÚVOD 12

1 VYMEDZENIE POJMOV 13

2 VŠEOBECNÉ CHARAKTERISTIKY A FUNKCIE ZÁZNAMOVÉHO ZARIADENIA 19

2.1 Všeobecné charakteristiky 19

2.2 Funkcie 20

2.3 Režimy prevádzky 21

2.4 Zabezpečenie 22

3 KONŠTRUKČNÉ A FUNKČNÉ POŽIADAVKY NA ZÁZNAMOVÉ ZARIADENIE 22

3.1 Monitorovanie vkladania a vyberania kariet 22

3.2 Meranie rýchlosti a vzdialenosti a zisťovanie polohy 23

3.2.1 Meranie prejdenej vzdialenosti 23

3.2.2 Meranie rýchlosti 23

3.2.3 Zisťovanie polohy 24

3.3 Meranie času 24

3.4 Monitorovanie činností vodiča 24

3.5 Monitorovanie stavu jazdy 25

3.6 Zápisy vodičov 25

3.6.1 Zápis o mieste, kde sa denný pracovný čas začína a/alebo končí 25

3.6.2 Manuálne zapisovanie činností vodiča a súhlas vodiča týkajúci sa rozhrania ITS 25

3.6.3 Zápis špecifických podmienok 27

3.7 Podnikové blokovanie 27

3.8 Monitorovanie kontrolných činností 28

3.9 Detekcia udalostí a/alebo porúch 28

3.9.1 Udalosť „vloženie neplatnej karty“ 28

3.9.2 Udalosť „konflikt karty“ 28

3.9.3 Udalosť „prekrývanie časov“ 28

3.9.4 Udalosť „jazda bez príslušnej karty“ 29

3.9.5 Udalosť „vloženie karty za jazdy“ 29

3.9.6 Udalosť „nesprávne uzavretá posledná relácia karty“ 29

3.9.7 Udalosť „prekročenie rýchlosti“ 29

3.9.8 Udalosť „prerušenie napájania“ 29

3.9.9 Udalosť „chyba komunikácie s diaľkovým komunikačným zariadením“ 29

3.9.10 Udalosť „chýbajúce informácie o polohe z prijímača GNSS“ 29

3.9.11 Udalosť „chyba komunikácie s externým zariadením GNSS“ 30

3.9.12 Udalosť „chyba údajov o pohybe“ 30

3.9.13 Udalosť „nesúlad údajov o pohybe vozidla“ 30

3.9.14. Udalosť „pokus o narušenie zabezpečenia“ 30

3.9.15 Udalosť „časový konflikt“ 30

3.9.16 Porucha „karty“ 30

3.9.17 Porucha „záznamového zariadenia“ 30

3.10 Zabudované a automatické skúšky 31

3.11 Čítanie z dátovej pamäte 31

3.12 Zaznamenávanie a uloženie v dátovej pamäti 31

3.12.1 Identifikačné údaje zariadenia 32

3.12.1.1 Identifikačné údaje jednotky vozidla 32

3.12.1.2 Identifikačné údaje snímača pohybu 32

3.12.1.3 Identifikačné údaje globálnych navigačných satelitných systémov 33

3.12.2 Kľúče a certifikáty 33

3.12.3 Údaje o vložení a vybratí karty vodiča alebo dielenskej karty 33

3.12.4 Údaje o činnosti vodiča 34

3.12.5 Miesta a polohy, kde sa denný pracovný čas začína a/alebo končí, a/alebo kde sa dosiahne 3-hodinový čas nepretržitej jazdy 34

3.12.6 Údaje počítadla kilometrov 35

3.12.7 Podrobné údaje o rýchlosti 35

3.12.8 Údaje o udalostiach 35

3.12.9 Údaje o poruchách 37

3.12.10 Kalibračné údaje 38

3.12.11 Údaje o úprave času 39

3.12.12 Údaje o kontrolnej činnosti 39

3.12.13 Údaje o podnikovom blokovaní 39

3.12.14 Údaje o činnosti sťahovania 39

3.12.15 Údaje o špecifických podmienkach 40

3.12.16 Údaje o tachografovej karte 40

3.13 Čítanie z tachografovej karty 40

3.14 Zaznamenávanie a ukladanie na tachografovú kartu 40

3.14.1 Zaznamenávanie a ukladanie na tachografové karty prvej generácie 40

3.14.2 Zaznamenávanie a ukladanie na tachografové karty druhej generácie 41

3.15 Zobrazovanie 41

3.15.1 Zobrazenie predvolených údajov 42

3.15.2	Zobrazenie výstrahy	43
3.15.3	Prístup k menu	43
3.15.4	Iné zobrazenia	43
3.16	Tlač	43
3.17	Výstrahy	44
3.18	Sťahovanie údajov na externé médiá	45
3.19	Diaľková komunikácia v prípade cielených cestných kontrol	45
3.20	Výstupné údaje pre doplnkové externé zariadenia	46
3.21	režim kalibrácie	47
3.22	Kontrola kalibrácie pri cestnej kontrole	47
3.23	Úprava času	48
3.24	Výkonnostné charakteristiky	48
3.25	Materiály	48
3.26	Označenia	49
4	KONŠTRUKČNÉ A FUNKČNÉ POŽIADAVKY NA TACHOGRAFOVÉ KARTY	49
4.1	Viditeľné údaje	49
4.2	Zabezpečenie	52
4.3	Normy	53
4.4	Elektrické špecifikácie a špecifikácie prostredia	53
4.5	Uchovávanie údajov	53
4.5.1	Elementárne súbory na identifikáciu a riadenie karty	54
4.5.2	Identifikácia karty s integrovaným obvodom (IC)	54
4.5.2.1	Identifikácia čipu	54
4.5.2.2	DIR (len v tachografových kartách druhej generácie)	54
4.5.2.3	Informácie ATR (podmienené, len v tachografových kartách druhej generácie)	54
4.5.2.4	Informácie o rozšírenej dĺžke (podmienené, len v tachografových kartách druhej generácie)	55
4.5.3	Karta vodiča	55
4.5.3.1	Aplikácia tachografu (prístupné pre jednotky vozidla prvej a druhej generácie)	55
4.5.3.1.1	Identifikácia aplikácie	55
4.5.3.1.2	Kľúč a certifikáty	55
4.5.3.1.3	Identifikácia karty	55
4.5.3.1.4	Identifikácia držiteľa karty	55
4.5.3.1.5	Sťahovanie údajov z karty	55
4.5.3.1.6	Informácie o vodičskom preukaze	55
4.5.3.1.7	Údaje o udalostiach	56

4.5.3.1.8 Údaje o poruchách ... 56
4.5.3.1.9 Údaje o činnosti vodiča ... 57
4.5.3.1.10 Údaje o použitých vozidlách ... 57
4.5.3.1.11 Miesta, kde sa denný pracovný čas začína a/alebo končí ... 58
4.5.3.1.12 Údaje o relácii karty ... 58
4.5.3.1.13 Údaje o kontrolnej činnosti ... 58
4.5.3.1.14 Údaje o špecifických podmienkach ... 58
4.5.3.2 Aplikácia tachografu druhej generácie (neprístupné jednotke vozidla prvej generácie) ... 59
4.5.3.2.1 Identifikácia aplikácie ... 59
4.5.3.2.2 Kľúče a certifikáty ... 59
4.5.3.2.3 Identifikácia karty ... 59
4.5.3.2.4 Identifikácia držiteľa karty ... 59
4.5.3.2.5 Sťahovanie údajov z karty ... 59
4.5.3.2.6 Informácie o vodičskom preukaze ... 59
4.5.3.2.7 Údaje o udalostiach ... 59
4.5.3.2.8 Údaje o poruchách ... 60
4.5.3.2.9 Údaje o činnosti vodiča ... 61
4.5.3.2.10 Údaje o použitých vozidlách ... 61
4.5.3.2.11 Miesta a polohy, kde sa denný pracovný čas začína a/alebo končí ... 62
4.5.3.2.12 Údaje o relácii karty ... 62
4.5.3.2.13 Údaje o kontrolnej činnosti ... 62
4.5.3.2.14 Údaje o špecifických podmienkach ... 63
4.5.3.2.15 Údaje o použitých jednotkách vozidla ... 63
4.5.3.2.16 Údaje o miestach počas troch hodín nepretržitej jazdy ... 63
4.5.4 Dielenská karta ... 63
4.5.4.1 Aplikácia tachografu (prístupné pre jednotky vozidla prvej a druhej generácie) ... 63
4.5.4.1.1 Identifikácia aplikácie ... 63
4.5.4.1.2 Kľúče a certifikáty ... 63
4.5.4.1.3 Identifikácia karty ... 64
4.5.4.1.4 Identifikácia držiteľa karty ... 64
4.5.4.1.5 Sťahovanie údajov z karty ... 64
4.5.4.1.6 Údaje o kalibrácii a úprave času ... 64

4.5.4.1.7 Údaje o udalostiach a poruchách ... 65
4.5.4.1.8 Údaje o činnosti vodiča ... 65
4.5.4.1.9 Údaje o použitých vozidlách ... 65
4.5.4.1.10 Údaje o začiatku a/alebo konci denného pracovného času ... 65
4.5.4.1.11 Údaje o relácii karty ... 65
4.5.4.1.12 Údaje o kontrolnej činnosti ... 65
4.5.4.1.13 Údaje o špecifických podmienkach ... 65
4.5.4.2 Aplikácia tachografu druhej generácie (neprístupné jednotke vozidla prvej generácie) ... 65
4.5.4.2.1 Identifikácia aplikácie ... 65
4.5.4.2.2 Kľúče a certifikáty ... 66
4.5.4.2.3 Identifikácia karty ... 66
4.5.4.2.4 Identifikácia držiteľa karty ... 66
4.5.4.2.5 Sťahovanie údajov z karty ... 66
4.5.4.2.6 Údaje o kalibrácii a úprave času ... 66
4.5.4.2.7 Údaje o udalostiach a poruchách ... 67
4.5.4.2.8 Údaje o činnosti vodiča ... 67
4.5.4.2.9 Údaje o použitých vozidlách ... 67
4.5.4.2.10 Údaje o začiatku a/alebo konci denného pracovného času ... 67
4.5.4.2.11 Údaje o relácii karty ... 67
4.5.4.2.12 Údaje o kontrolnej činnosti ... 67
4.5.4.2.13 Údaje o použitých jednotkách vozidla ... 67
4.5.4.2.14 Údaje o miestach počas troch hodín nepretržitej jazdy ... 68
4.5.4.2.15 Údaje o špecifických podmienkach ... 68
4.5.5 Kontrolná karta ... 68
4.5.5.1 Aplikácia tachografu (prístupné pre jednotky vozidla prvej a druhej generácie) ... 68
4.5.5.1.1 Identifikácia aplikácie ... 68
4.5.5.1.2 Kľúče a certifikáty ... 68
4.5.5.1.3 Identifikácia karty ... 68
4.5.5.1.4 Identifikácia držiteľa karty ... 68
4.5.5.1.5 Údaje o kontrolnej činnosti ... 69
4.5.5.2 Aplikácia tachografu druhej generácie (neprístupné jednotke vozidla prvej generácie) ... 69
4.5.5.2.1 Identifikácia aplikácie ... 69
4.5.5.2.2 Kľúče a certifikáty ... 69

4.5.5.2.3	Identifikácia karty	69
4.5.5.2.4	Identifikácia držiteľa karty	69
4.5.5.2.5	Údaje o kontrolnej činnosti	70
4.5.6	Podniková karta	70
4.5.6.1	Aplikácia tachografu (prístupné pre jednotky vozidla prvej a druhej generácie)	70
4.5.6.1.1	Identifikácia aplikácie	70
4.5.6.1.2	Kľúče a certifikáty	70
4.5.6.1.3	Identifikácia karty	70
4.5.6.1.4	Identifikácia držiteľa karty	70
4.5.6.1.5	Údaje o činnosti podniku	70
4.5.6.2	Aplikácia tachografu druhej generácie (neprístupné jednotke vozidla prvej generácie)	71
4.5.6.2.1	Identifikácia aplikácie	71
4.5.6.2.2	Kľúče a certifikáty	71
4.5.6.2.3	Identifikácia karty	71
4.5.6.2.4	Identifikácia držiteľa karty	71
4.5.6.2.5	Údaje o činnosti podniku	71
5	MONTÁŽ ZÁZNAMOVÉHO ZARIADENIA	72
5.1	Montáž	72
5.2	Montážny štítok	73
5.3	Plombovanie	74
6	KONTROLY, INŠPEKCIE A OPRAVY	74
6.1	Schválenie montážnych firiem, dielní a výrobcov vozidiel	74
6.2	Kontrola nových alebo opravených prístrojov	75
6.3	Inšpekcia inštalácie	75
6.4	Pravidelné inšpekcie	75
6.5	Meranie chýb	76
6.6	Opravy	76
7	VYDÁVANIE KARIET	76
8	TYPOVÉ SCHVÁLENIE ZÁZNAMOVÉHO ZARIADENIA A TACHOGRAFOVÝCH KARIET	77
8.1	Všeobecne	77
8.2	Osvedčenie zabezpečenia	78
8.3	Osvedčenie funkčnosti	78
8.4	Osvedčenie interoperability	78
8.5	Osvedčenie o typovom schválení	79
8.6	Výnimočný postup: prvé osvedčenia interoperability pre záznamové zariadenia a tachografové karty druhej generácie	80

ÚVOD

Prvá generácia systému digitálneho tachografu je v prevádzke od 1. mája 2006. V prípade vnútroštátnej dopravy sa môže používať až do konca svojej životnosti. V prípade medzinárodnej dopravy, 15 rokov po nadobudnutí účinnosti tohto nariadenia Komisie musia byť všetky vozidlá vybavené vyhovujúcimi inteligentnými tachografmi druhej generácie, zavedenými týmto nariadením.

Táto príloha obsahuje požiadavky na záznamové zariadenie a tachografové karty druhej generácie. Od dátumu zavedenia sa záznamové zariadenie druhej generácie musí montovať vo vozidlách registrovaných po prvýkrát, a musia byť vydané tachografové karty druhej generácie.

S cieľom podporiť plynulé zavedenie tachografového systému druhej generácie,

— musia byť tachografové karty druhej generácie technicky vyriešené tak, aby sa dali používať v jednotkách vozidla prvej generácie,

— nahradenie platných tachografových kariet prvej generácie nemožno požadovať od dátumu zavedenia.

To umožní vodičom ponechať si jedinečnú kartu vodiča a využívať ju s obidvoma systémami.

Záznamové zariadenie druhej generácie však musí byť kalibrované iba pomocou dielenských kariet druhej generácie.

Táto príloha obsahuje všetky požiadavky týkajúce sa interoperability medzi tachografovým systémom prvej a druhej generácie.

Dodatok 15 obsahuje ďalšie podrobnosti o súbežnom fungovaní oboch systémov.

Zoznam dodatkov

Dodatok 1: SLOVNÍK ÚDAJOV

Dodatok 2: ŠPECIFIKÁCIA TACHOGRAFOVÝCH KARIET

Dodatok 3: PIKTOGRAMY

Dodatok 4: VÝPISY

Dodatok 5: ZOBRAZENIE

Dodatok 6: PREDNÝ KONEKTOR NA KALIBRÁCIU A SŤAHOVANIE

Dodatok 7: PROTOKOLY SŤAHOVANIA ÚDAJOV

Dodatok 8: KALIBRAČNÝ PROTOKOL

Dodatok 9: TYPOVÉ SCHVÁLENIE A ZOZNAM MINIMÁLNE POŽADOVANÝCH SKÚŠOK

Dodatok 10: POŽIADAVKY NA ZABEZPEČENIE

Dodatok 11: SPOLOČNÉ BEZPEČNOSTNÉ MECHANIZMY

Dodatok 12: URČOVANIE POLOHY NA ZÁKLADE GLOBÁLNEHO NAVIGAČNÉHO SATELITNÉHO SYSTÉMU (GNSS)

Dodatok 13: ROZHRANIE ITS

Dodatok 14: FUNKCIA DIAĽKOVEJ KOMUNIKÁCIE

Dodatok 15: PRECHOD: RIADENIE KOEXISTENCIE JEDNOTLIVÝCH GENERÁCIÍ ZARIADENIA

Dodatok 16: ADAPTÉR PRE VOZIDLÁ KATEGÓRIÍ M1 A N1

1 VYMEDZENIE POJMOV

V tejto prílohe:

a) „aktivácia“ je:

fáza, v ktorej sa tachograf stáva použitím dielenskej karty plne funkčným a plní všetky funkcie vrátane bezpečnostných funkcií;

b) „autentifikácia“ je:

funkcia určená na zistenie a overenie uvádzanej totožnosti;

c) „autenticita“ znamená:

že informácia prichádza od osoby, ktorej totožnosť sa dá overiť;

d) „zabudovaná skúška (BIT)“ je:

skúška, ktorá sa vykonáva na požiadanie, iniciovaná operátorom alebo externým zariadením;

e) „kalendárny deň“ je:

deň od 00.00 hodín do 24.00 hodín. Všetky kalendárne dni sa vzťahujú na čas UTC (koordinovaný svetový čas);

f) „kalibrácia“ inteligentného tachografu je:

aktualizácia alebo potvrdenie parametrov vozidla, ktoré sa majú ukladať v dátovej pamäti. Parametre vozidla zahŕňajú identifikáciu vozidla (VIN, VRN a členský štát evidencie) a charakteristiky vozidla (w, k, l, rozmer pneumatík, nastavenie obmedzovača rýchlosti (v prípade potreby), aktuálny čas UTC, aktuálny stav počítadla kilometrov); počas kalibrácie záznamového zariadenia sa musia v dátovej pamäti uložiť aj typy a identifikátory všetkých umiestnených plomb týkajúcich sa typového schvaľovania;

každá aktualizácia alebo len potvrdenie času UTC sa považuje za úpravu času a nie za kalibráciu pod podmienkou, že nie je v rozpore s požiadavkou 409.

kalibrovanie záznamového zariadenia si vyžaduje použitie dielenskej karty;

g) „číslo karty“ je:

16 alfanumerických znakov, ktoré jednoznačne identifikujú tachografovú kartu v členskom štáte. Číslo karty obsahuje poradový index karty (v prípade potreby), index náhrady karty a index obnovy karty;

karta je preto jednoznačne identifikovaná kódom vydávajúceho členského štátu a číslom karty;

h) „poradový index karty“ je:

štrnásty alfanumerický znak čísla karty, ktorý sa používa na rozlíšenie rôznych kariet vydaných podniku, dielni alebo kontrolnému orgánu, ktorým sa môže vydať niekoľko tachografových kariet. Podnik, dielňa alebo kontrolný orgán je jednoznačne identifikovaný prvými 13 znakmi čísla karty;

i) „index obnovy karty“ je:

šestnásty alfanumerický znak čísla karty, ktorý sa zvýši pri každej obnove tachografovej karty;

j) „index náhrady karty“ je:

pätnásty alfanumerický znak čísla karty, ktorý sa zvýši pri každej náhrade tachografovej karty;

k) „charakteristický koeficient vozidla“ je:

numerická charakteristika udávajúca hodnotu výstupného signálu emitovaného časťou vozidla, ktorá ho prepája so záznamovým zariadením (výstupný hriadeľ prevodovky alebo náprava), zatiaľ čo vozidlo prejde vzdialenosť jedného kilometra za štandardných skúšobných podmienok vymedzených v rámci požiadavky 414. Charakteristický koeficient je vyjadrený v impulzoch na kilometer (w = … imp/km);

l) „podniková karta“ je:

tachografová karta vydaná orgánmi členského štátu dopravnému podniku, ktorý musí prevádzkovať vozidlá vybavené tachografom, ktorá identifikuje príslušný dopravný podnik a umožňuje zobraziť, stiahnuť a vytlačiť údaje uložené v tachografe, ktoré sú blokované príslušným dopravným podnikom;

m) „konštanta záznamového zariadenia“ je:

numerická veličina udávajúca hodnotu vstupného signálu potrebnú na zobrazenie a zaznamenanie prejdenej vzdialenosti 1 km; táto konštanta sa vyjadruje v impulzoch na kilometer (k = … imp/km);

n) „nepretržitý čas jazdy“ je vypočítaný v záznamovom zariadení ako ([1]):

nepretržitý čas jazdy vypočítaný ako súčet aktuálnych kumulovaných časov jazdy konkrétneho vodiča od konca jeho posledného časového úseku POHOTOVOSTI alebo PRESTÁVKY/ODPOČINKU alebo NEZNÁMEHO ([2]) časového úseku 45 alebo viac minút [tento časový úsek môže byť rozdelený podľa nariadenia Európskeho parlamentu a Rady (ES) č. 561/2006 ([3])]. Dané výpočty berú, podľa potreby, do úvahy doterajšie činnosti uložené na karte vodiča. Keď vodič nevložil svoju kartu, výpočty vychádzajú zo záznamov dátovej pamäte týkajúcich sa aktuálneho časového úseku, keď nebola vložená karta, a príslušného slotu;

o) „kontrolná karta“ je:

tachografová karta, ktorú vnútroštátnemu príslušnému kontrolnému orgánu vydali orgány členského štátu, ktorá identifikuje kontrolný orgán a prípadne aj kontrolného úradníka a ktorá umožňuje prístup k údajom uloženým v dátovej pamäti alebo na karte vodiča a prípadne na dielenských kartách na účel ich čítania, tlače a/alebo stiahnutia;

Okrem toho poskytuje prístup k funkcii kontroly kalibrácie pri cestnej kontrole a údajom o snímači komunikačného zariadenia na diaľkovú včasnú detekciu.

p) „kumulovaný čas prestávok“ sa vypočíta v záznamovom zariadení ako ([1]):

kumulovaná prestávka z času jazdy sa vypočíta ako aktuálny súčet časov POHOTOVOSTI alebo PRESTÁVKY/ODPOČINKU alebo NEZNÁMEHO ([2]) času v trvaní 15 alebo viac minút pre konkrétneho vodiča od konca jeho posledného časového úseku POHOTOVOSTI alebo PRESTÁVKY/ODPOČINKU alebo NEZNÁMEHO ([2]) časového úseku v trvaní 45 alebo viac minút (tento časový úsek môže byť rozdelený podľa nariadenia (ES) č. 561/2006).

Dané výpočty berú, podľa potreby, do úvahy doterajšie činnosti uložené na karte vodiča. Neznáme časové úseky s negatívnou dobou trvania (začiatok neznámeho časového úseku > koniec neznámeho časového úseku) z dôvodu prekrývania časov medzi dvoma rôznymi záznamovými zariadeniami, sa pri výpočte neberú do úvahy.

Keď vodič nevložil svoju kartu, výpočty vychádzajú zo záznamov dátovej pamäte týkajúcich sa aktuálneho časového úseku, kedy nebola vložená karta, a vzťahujúcich sa k príslušnému slotu.

([1]) Tento spôsob výpočtu nepretržitého času jazdy a kumulovaných časov prestávok slúži záznamovému zariadeniu na výpočet výstrahy pri nepretržitom čase jazdy. Nemá vplyv na právny výklad týchto časov. Ak sú tieto definície zastarané z dôvodu ich aktualizácie v iných príslušných právnych predpisoch, môžu sa namiesto nich použiť alternatívne spôsoby výpočtu nepretržitého času jazdy a kumulovaného času prestávok.

([2]) NEZNÁME časové úseky zodpovedajú časovým úsekom, počas ktorých nebola karta vodiča vložená v záznamovom zariadení a nevykonal sa žiadny manuálny záznam o činnosti vodiča.

([3]) Nariadenie Európskeho parlamentu a Rady (ES) č. 561/2006 z 15. marca 2006 o harmonizácii niektorých právnych predpisov v sociálnej oblasti, ktoré sa týkajú cestnej dopravy, ktorým sa menia a dopĺňajú nariadenia Rady (EHS) č. 3821/85 a (ES) č. 2135/98 a zrušuje nariadenie Rady (EHS) č. 3820/85 (Ú. v. EÚ L 102, 11.4.2006, s. 1).

q) „dátová pamäť“ je:

elektronické pamäťové dátové zariadenie zabudované do záznamového zariadenia;

r) „digitálny podpis“ znamená:

údaje pripojené k bloku údajov alebo kryptografická transformácia bloku údajov, ktorá umožňuje príjemcovi bloku údajov overiť si autenticitu a integritu bloku údajov;

s) „sťahovanie“ je:

kopírovanie spolu s digitálnym podpisom časti alebo celej sady dátových súborov zaznamenaných v dátovej pamäti jednotky vozidla alebo v pamäti tachografovej karty za predpokladu, že sa počas tohto procesu nezmenia ani nevymažú žiadne uložené údaje;

Výrobcovia inteligentných tachografových jednotiek vozidla a výrobcovia zariadenia navrhnutého a určeného na sťahovanie dátových súborov prijmú všetky primerané opatrenia s cieľom zabezpečiť, aby sťahovanie týchto údajov spôsobovalo dopravným podnikom alebo vodičom čo najmenšie časové straty.

Sťahovanie súboru s podrobnými údajmi o rýchlosti nemusí byť potrebné na určenie súladu s nariadením (ES) č. 561/2006, ale môže sa použiť na iné účely napr. pri vyšetrovaní nehody.

t) „karta vodiča“ je:

tachografová karta vydaná konkrétnemu vodičovi orgánmi členského štátu, ktorá identifikuje vodiča a umožňuje ukladať údaje o činnosti vodiča;

u) „skutočný obvod kolies“ je:

priemer vzdialeností prejdených každým z kolies poháňajúcich vozidlo (hnacie kolesá) v priebehu jednej úplnej rotácie. Meranie týchto vzdialeností sa vykoná za štandardných skúšobných podmienok vymedzených v požiadavke 414 a vyjadrí sa vo forme „l = … mm“. Výrobcovia vozidiel môžu nahradiť meranie týchto vzdialeností teoretickým výpočtom, ktorý berie do úvahy rozloženie hmotnosti na nápravy nenaloženého vozidla v normálnom prevádzkovom stave ([1]). Metódy takéhoto teoretického výpočtu podliehajú schváleniu príslušným orgánom členského štátu a môže sa vykonať len pred aktiváciou tachografu;

v) „udalosť“ je:

nezvyčajná operácia zistená inteligentným tachografom, ktorá môže byť dôsledkom pokusu o podvod;

w) „externé zariadenie GNSS“ je

zariadenie, ktoré obsahuje prijímač GNSS, keď jednotka vozidla nie je jednotný celok, ako aj ostatné komponenty potrebné na ochranu prenosu údajov o polohe do zvyšnej časti jednotky vozidla;

x) „porucha“ je:

nezvyčajná operácia zistená inteligentným tachografom, ktorá môže byť dôsledkom nesprávneho fungovania alebo zlyhania zariadenia;

y) „prijímač GNSS“ je:

elektronické zariadenie, ktoré prijíma a digitálne spracováva signály z jedného alebo viacerých globálnych navigačných satelitných systémov (GNSS v angličtine) s cieľom poskytnúť informácie o polohe, rýchlosti a čase.

z) „montáž“ je:

montáž tachografu do vozidla;

([1]) Nariadenie Komisie (EÚ) č. 1230/2012 z 12. decembra 2012, ktorým sa vykonáva nariadenie Európskeho parlamentu a Rady (ES) č. 661/2009, pokiaľ ide o požiadavky na typové schválenie v prípade hmotností a rozmerov motorových vozidiel a ich prípojných vozidiel, a mení a dopĺňa smernica Európskeho parlamentu a Rady 2007/46/ES (Ú. v. EÚ L 353, 21.12.2012, s. 31) v znení posledných zmien.

aa) „interoperabilita“ je:

schopnosť systémov a základných prevádzkových postupov vymieňať si údaje a informácie;

bb) „rozhranie“ je:

zariadenie medzi systémami, prostredníctvom ktorého sa tieto systémy môžu spájať a spolupracovať;

cc) „poloha“ znamená:

zemepisné súradnice vozidla v danom čase;

dd) „snímač pohybu“ je:

časť tachografu, ktorá poskytuje signál udávajúci rýchlosť vozidla a/alebo prejdenú vzdialenosť;

ee) „neplatná karta“ je:

karta, pri ktorej sa zistilo, že je chybná, alebo pri ktorej zlyhala počiatočná autentifikácia, alebo ešte nenastal začiatok jej platnosti, alebo jej platnosť sa skončila;

ff) „otvorená norma“ je:

norma stanovená v dokumente o špecifikácii noriem dostupnom bezplatne alebo za symbolický poplatok, ktorá je dostupná na účely kopírovania, distribúcie alebo na použitie, a to bezplatne alebo za symbolický poplatok;

gg) „záznamové zariadenie sa nevyžaduje“ znamená:

keď sa používanie záznamového zariadenia nevyžaduje podľa ustanovení nariadenia (ES) č. 561/2006;

hh) „prekročenie rýchlosti“ je

prekročenie povolenej rýchlosti vozidla, vymedzené ako každý časový úsek nad 60 sekúnd, počas ktorého nameraná rýchlosť vozidla presiahne limit pre nastavenie obmedzovača rýchlosti stanovený v smernici Rady 92/6/EHS [1] v znení posledných zmien;

ii) „pravidelná inšpekcia“ je:

súbor činností vykonávaných na overenie, či tachograf riadne funguje, či jeho nastavenie zodpovedá parametrom vozidla a či k nemu neboli pripojené manipulačné zariadenia;

jj) „tlačiareň“ je:

komponent záznamového zariadenia, ktorý zabezpečuje výpisy uložených údajov;

kk) „komunikácia na diaľkovú včasnú detekciu“ je:

komunikácia medzi komunikačným zariadením na diaľkovú včasnú detekciu a snímačom komunikačného zariadenia na diaľkovú včasnú detekciu počas cielených cestných kontrol s cieľom diaľkovo odhaľovať možnú manipuláciu alebo zneužitie záznamového zariadenia;

ll) „diaľkové komunikačné zariadenie“ je:

zariadenie jednotky vozidla, ktoré sa používa na vykonávanie cielených cestných kontrol;

[1] Smernica Rady 92/6/EEC z 10. februára 1992 o montáži a používaní zariadení obmedzujúcich rýchlosť pre určité kategórie motorových vozidiel v Spoločenstve (Ú. v. ES L 57, 2.3.1992, s. 27).

mm) „snímač komunikačného zariadenia na diaľkovú včasnú detekciu“ je:

systém používaný kontrolnými úradníkmi na cielené cestné kontroly;

nn) „obnova“ je:

vydanie novej tachografovej karty keď existujúcej karte skončí platnosť alebo nefunguje správne a bola vrátená vydávajúcemu orgánu. Z obnovy vždy vyplýva istota, že nemôžu súčasne existovať dve platné karty;

oo) „oprava“ je:

akákoľvek oprava snímača pohybu alebo jednotky vozidla alebo kábla, ktorá si vyžaduje odpojenie napájania alebo jeho odpojenie od iných komponentov tachografu, alebo otvorenie snímača pohybu alebo jednotky vozidla;

pp) „náhrada karty“ je:

vydanie tachografovej karty ako náhrady za existujúcu tachografovú kartu, ktorá bola nahlásená ako stratená, odcudzenú alebo nefungovala správne a nebola vrátená vydávajúcemu orgánu. Z náhrady vždy vyplýva riziko súčasnej existencie dvoch platných kariet;

qq) „osvedčovanie zabezpečenia“ je:

proces, ktorým orgán osvedčovania na základe spoločných kritérií osvedčuje, že overované záznamové zariadenie (alebo komponent) alebo tachografová karta spĺňajú požiadavky zabezpečenia vymedzené v súvisiacich profiloch ochrany;

rr) „automatická skúška“ je:

cyklická a automatická skúška vykonávaná záznamovým zariadením na zisťovanie porúch;

ss) „meranie času“ je:

nepretržitý digitálny záznam koordinovaného univerzálneho dátumu a času (universal date and time – UTC);

tt) „úprava času“ je:

automatická úprava aktuálneho času v pravidelných intervaloch a s toleranciou v rozmedzí maximálne jednej minúty alebo úprava vykonaná počas kalibrácie;

uu) „rozmer pneumatiky“ je:

označenie rozmerov pneumatík (vonkajších hnacích kolies) v súlade so smernicou Rady 92/23/EHS ([1]) v znení posledných zmien;

vv) „identifikácia vozidla“ znamená:

čísla identifikujúce vozidlo: evidenčné číslo vozidla (VRN) s identifikáciou členského štátu evidencie a identifikačné číslo vozidla (VIN) ([2]);

ww) na účely výpočtu v záznamovom zariadení „týždeň“ je:

časový úsek od 00.00 hodín UTC v pondelok do 24.00 UTC v nedeľu;

([1]) Smernica Rady 92/23/EHS z 31. marca 1992 o pneumatikách motorových vozidiel a ich prípojných vozidiel a ich montáži (Ú. v. ES L 129, 14.5.1992, s. 95).

([2]) Smernica Rady 76/114/EHS z 18. decembra 1975 o aproximácii právnych predpisov členských štátov o povinných štítkoch a nápisoch pre motorové vozidlá a ich prípojné vozidlá a ich umiestnení a spôsobe ich pripevnenia (Ú. v. ES L 24, 30.1.1976, s. 1).

xx) „dielenská karta“ je:

tachografová karta vydaná orgánmi členského štátu určenému personálu výrobcu tachografov, montážnej firme, výrobcovi vozidla alebo dielni schváleným uvedeným členským štátom, ktorá identifikuje držiteľa karty a umožňuje skúšanie, kalibráciu a aktiváciu tachografov a/alebo stiahnutie údajov z nich;

yy) „adaptér“ je:

zariadenie permanentne zabezpečujúce signál udávajúci rýchlosť vozidla a/alebo prejdenú vzdialenosť, iné než zariadenie na nezávislé zisťovanie pohybu, a ktoré:

— sa montuje a používa iba vo vozidlách typu M1 a N1 (vymedzených v prílohe II k smernici Európskeho parlamentu a Rady 2007/46/ES ([1]) v znení posledných zmien) uvedených do prevádzky od 1. mája 2006,

— sa montuje v prípade, ak nie je mechanicky možné namontovať iný typ existujúceho snímača pohybu, ktorý inak spĺňa požiadavky ustanovení tejto prílohy a jej dodatkov 1 až 15,

— sa montuje medzi jednotku vozidla a miesto, kde sa impulzy rýchlosti/vzdialenosti vytvárajú prostredníctvom integrovaných snímačov alebo iných rozhraní,

— z hľadiska jednotky vozidla sa adaptér správa rovnako, ako keby bol k jednotke vozidla pripojený snímač pohybu, ktorý spĺňa požiadavky ustanovení tejto prílohy a jej dodatkov 1 až 16;

používanie tohto adaptéra v uvedených vozidlách musí umožňovať montáž a správne používanie jednotky vozidla, ktorá spĺňa všetky požiadavky tejto prílohy,

v prípade týchto vozidiel tvoria súčasť inteligentného tachografu káble, adaptér a jednotka vozidla;

zz) „integrita údajov“ je:

presnosť a konzistentnosť uložených údajov, ktorú predstavuje absencia akejkoľvek zmeny údajov medzi dvoma aktualizáciami dátového záznamu. Integrita údajov znamená, že údaje sú presnou kópiou pôvodnej verzie, napr. že neboli poškodené v procese zápisu na tachografovú kartu a spätného čítania z nej alebo do špecializovaného vybavenia alebo počas prenosu akýmkoľvek komunikačným kanálom;

aaa) „ochrana údajov“ znamená:

súbor technických opatrení prijatých s cieľom zabezpečiť riadne vykonávanie zásad stanovených v smernici Európskeho parlamentu a Rady 95/46/ES ([2]), ako aj zásad stanovených v smernici Európskeho parlamentu a Rady 2002/58/ES ([3]);

bbb) „systém inteligentného tachografu“ je:

záznamové zariadenie, tachografové karty a súbor všetkých priamo alebo nepriamo prepojených zariadení počas ich výroby, montáže, použitia, skúšania a kontroly, ako napríklad karty, snímač diaľkového komunikačného zariadenia a akékoľvek iné zariadenia na sťahovanie údajov, analýzu údajov, kalibráciu, vytváranie, spravovanie alebo zavádzanie prvkov zabezpečenia atď.;

ccc) „dátum zavedenia“:

36 mesiacov po nadobudnutí účinnosti podrobných ustanovení uvedených v článku 11 nariadenia Európskeho parlamentu a Rady (EÚ) č. 165/2014 ([4]).

([1]) Smernica Európskeho parlamentu a Rady 2007/46/ES z 5. septembra 2007, ktorou sa zriaďuje rámec pre typové schválenie motorových vozidiel a ich prípojných vozidiel, systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá (Rámcová smernica) (Ú. v. EÚ L 263, 9.10.2007, s. 1).

([2]) Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 23.11.1995, s. 31).

([3]) Smernica Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 165/2014 zo 4. februára 2014 o tachografoch v cestnej doprave, ktorým sa ruší nariadenie Rady (EHS) č. 3821/85 o záznamovom zariadení v cestnej doprave a mení nariadenie Európskeho parlamentu a Rady (ES) č. 561/2006 o harmonizácii niektorých právnych predpisov v sociálnej oblasti, ktoré sa týkajú cestnej dopravy (Ú. v. EÚ L 60, 28.2.2014, s. 1).

Toto je dátum, po ktorom vozidlá pri prvej evidencii:

— *musia byť vybavené tachografom napojeným na službu určovania polohy založenú na satelitnom navigačnom systéme,*

— *musia byť schopné prenášať údaje pre cielené cestné kontroly príslušným kontrolným orgánom, keď je vozidlo v pohybe,*

— *a môžu byť vybavené štandardizovanými rozhraniami umožňujúcimi, aby údaje, ktoré tachograf zaznamenal alebo vytvoril, používalo v prevádzkovom režime externé zariadenie.*

ddd) „profil ochrany“ je:

dokument používaný v rámci osvedčovania podľa spoločných kritérií, ktorý špecifikuje požiadavky na zabezpečenie informácií nezávisle od implementácie;

eee) „presnosť GNSS“ je:

v kontexte zaznamenávania polohy z globálneho navigačného satelitného systému (GNSS) s tachografmi hodnota Horizontal Dilution of Precision (HDOP) vypočítaná ako minimum hodnôt HDOP získaných z dostupných systémov GNSS.

2 VŠEOBECNÉ CHARAKTERISTIKY A FUNKCIE ZÁZNAMOVÉHO ZARIADENIA

2.1 **Všeobecné charakteristiky**

Účelom záznamového zariadenia je zaznamenávať, ukladať, zobrazovať, tlačiť údaje o činnosti vodiča a generovať z nich výstupy.

Súčasťou každého vozidla vybaveného záznamovým zariadením, ktoré spĺňa ustanovenia tejto prílohy, musí byť ukazovateľ rýchlosti a počítadlo kilometrov. Tieto funkcie môžu byť súčasťou záznamového zariadenia.

01) Záznamové zariadenie obsahuje káble, snímač pohybu a jednotku vozidla.

02) Rozhranie medzi snímačmi pohybu a jednotkami vozidla musí spĺňať požiadavky uvedené v dodatku 11.

03) Jednotka vozidla musí byť pripojená ku globálnemu navigačnému satelitnému systému resp. systémom, ako je uvedené v dodatku 12.

04) Jednotka vozidla musí komunikovať so snímačom komunikačného zariadenia na diaľkovú včasnú detekciu, ako je uvedené v dodatku 14.

05) Jednotka vozidla môže obsahovať rozhranie ITS, ktoré je špecifikované v dodatku 13.

Záznamové zariadenie môže byť spojené s inými zariadeniami prostredníctvom doplnkových rozhraní a/alebo prostredníctvom nepovinného rozhrania ITS.

06) Žiadne funkcie alebo zariadenia zabudované alebo pripojené k záznamovému zariadeniu, bez ohľadu na to, či sú schválené, nesmú rušiť alebo byť schopné rušiť riadnu a bezpečnú prevádzku záznamového zariadenia a porušovať ustanovenia tohto nariadenia.

Používatelia záznamového zariadenia sa sami zariadeniu identifikujú tachografovými kartami.

07) Záznamové zariadenie poskytuje selektívne prístupové práva k údajom a funkciám podľa typu a/alebo totožnosti používateľa.

Záznamové zariadenie zaznamenáva a ukladá údaje do svojej dátovej pamäte, diaľkového komunikačného zariadenia a tachografovej karty.

To sa uskutočňuje v súlade so smernicou 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov ([1]), so smernicou 2002/58/ES z 12. júla 2002 týkajúcou sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií ([2]) a v súlade s článkom 7 nariadenia (EÚ) č. 165/2014.

2.2 **Funkcie**

08) Záznamové zariadenie zabezpečuje tieto funkcie:

— monitorovanie vkladania a vyberania kariet,

— meranie rýchlosti, vzdialenosti a polohy,

— meranie času,

— monitorovanie činností vodiča,

— monitorovanie stavu jazdy,

— manuálne zápisy vodiča:

  — zápisy o mieste, kde sa denný pracovný čas začína a/alebo končí,

  — manuálny zápis o činnostiach vodiča,

  — zápis o špecifických podmienkach,

— podnikové blokovanie,

— monitorovanie kontrolných činností,

— detekcia udalostí a/alebo porúch,

— zabudované a automatické skúšky,

— čítanie z dátovej pamäte,

— zaznamenávanie a ukladanie v dátovej pamäti,

— čítanie z tachografových kariet,

— zaznamenávanie a ukladanie na tachografové karty,

— zobrazovanie,

— tlač,

— výstraha,

— sťahovanie údajov na externé médiá,

— diaľková komunikácia pre cielené cestné kontroly,

— generovanie výstupných údajov pre doplnkové zariadenia,

— kalibrácia,

— kontrola kalibrácie pri cestnej kontrole,

— úprava času.

([1]) Ú. v. ES L 281, 23.11.1995, s. 31.
([2]) Ú. v. ES L 201, 31.7. 2002, s. 37.

2.3 **Režimy prevádzky**

09) Záznamové zariadenie pracuje v štyroch režimoch prevádzky:

— prevádzkový režim,

— režim kontroly,

— režim kalibrácie,

— podnikový režim.

10) Záznamové zariadenie sa po vložení príslušných platných tachografových kariet do zariadení s rozhraním karty prepne do týchto režimov prevádzky. Na určenie režimu prevádzky nemá vplyv generácia tachografovej karty, za predpokladu, že je vložená karta platná. Dielenská karta prvej generácie sa vždy považuje za neplatnú, ak je vložená do VU druhej generácie.

Režim prevádzky		Slot vodiča				
		Žiadna karta	Karta vodiča	Kontrolná karta	Dielenská karta	Podniková karta
Slot druhého vodiča	Žiadna karta	prevádzkový režim	prevádzkový režim	režim kontroly	režim kalibrácie	podnikový režim
	Karta vodiča	prevádzkový režim	prevádzkový režim	režim kontroly	režim kalibrácie	podnikový režim
	Kontrolná karta	režim kontroly	režim kontroly	Režim kontroly (*)	prevádzkový režim	prevádzkový režim
	Dielenská karta	režim kalibrácie	režim kalibrácie	prevádzkový režim	Režim kalibrácie (*)	prevádzkový režim
	Podniková karta	podnikový režim	podnikový režim	prevádzkový režim	prevádzkový režim	podnikový režim (*)

(*) V týchto situáciách záznamové zariadenie používa len tachografovú kartu vloženú do slotu vodiča.

11) Záznamové zariadenie ignoruje vložené neplatné karty, musí byť však možné zobraziť, vytlačiť alebo stiahnuť údaje uložené na karte, ktorá je už neplatná.

12) Všetky funkcie uvedené 2.2 musia fungovať v ktoromkoľvek režime prevádzky s týmito výnimkami:

— kalibračná funkcia je k dispozícii len v režime kalibrácie,

— funkcia kontroly kalibrácie pri cestnej kontrole je k dispozícii len v režime kontroly,

— funkcia podnikového blokovania je k dispozícii len v podnikovom režime,

— funkcia monitorovania kontrolných činností je k dispozícii len v režime kontroly,

— Funkcia sťahovania nie je k dispozícii v prevádzkovom režime (s výnimkou uvedenou v požiadavke 193), a s výnimkou sťahovania karty vodiča, keď vo VU nie je vložený iný typ karty.

13) Záznamové zariadenie môže poskytnúť ktorékoľvek údaje na zobrazenie, tlač alebo pre externé rozhrania s týmito výnimkami:

— v prevádzkovom režime sa akákoľvek osobná identifikácia (priezvisko a meno(á)), ktorá nezodpovedá vloženej tachografovej karte, zneviditeľní a akékoľvek číslo karty, ktoré nezodpovedá vloženej tachografovej karte, sa čiastočne zneviditeľní (nepárne znaky zľava doprava sa zneviditeľnia),

— v podnikovom režime údaje vzťahujúce sa k vodičovi (požiadavky 102, 105 a 108) sa môžu poskytnúť len za časové úseky, pri ktorých neexistuje blokovanie, alebo ktoré nie sú zablokované iným podnikom (identifikovaným prvými 13 číslicami čísla podnikovej karty),

— ak nie je do záznamového zariadenia vložená žiadna karta, údaje týkajúce sa vodiča sa môžu poskytnúť len za aktuálny kalendárny deň a osem predchádzajúcich kalendárnych dní,

— osobné údaje pochádzajúce z VU sa nesmú poskytnúť prostredníctvom rozhrania ITS jednotky vozidla, pokiaľ sa neoverí súhlas vodiča, ktorého sa údaje týkajú,

— bežná prevádzková platnosť VU je 15 rokov od dátumu vydania osvedčenia jednotky vozidla, ale jednotky vozidla sa môžu používať ďalšie 3 mesiace, výlučne na sťahovanie údajov.

2.4 **Zabezpečenie**

Zabezpečenie systému je zamerané na ochranu dátovej pamäte tak, aby bolo zabránené neoprávnenému prístupu k údajom a ich manipulácii, aby bol odhalený každý takýto pokus, na ochranu integrity a autenticity údajov vymieňaných medzi snímačom pohybu a jednotkou vozidla, na ochranu integrity a autenticity údajov vymieňaných medzi záznamovým zariadením a tachografovými kartami, na ochranu integrity a autenticity údajov vymieňaných medzi záznamovým zariadením a externým zariadením GNSS, na ochranu dôvernosti, integrity a autenticity údajov vymieňaných pri komunikácii na diaľkovú včasnú detekciu na účely kontroly, a na overenie integrity a autenticity sťahovaných údajov.

14) Na zaručenie zabezpečenia systému musia tieto komponenty spĺňať požiadavky zabezpečenia uvedené vo svojich profiloch ochrany, ako sa to vyžaduje v dodatku 10:

— jednotka vozidla,

— tachografová karta,

— snímač pohybu,

— externé zariadenie GNSS (tento profil je potrebný a uplatniteľný len pre variant externého GNSS).

3 KONŠTRUKČNÉ A FUNKČNÉ POŽIADAVKY NA ZÁZNAMOVÉ ZARIADENIE

3.1 **Monitorovanie vkladania a vyberania kariet**

15) Záznamové zariadenie monitoruje zariadenia s rozhraním karty, aby sa zistilo ich vkladanie a vyberanie.

16) Po vložení karty záznamové zariadenie zistí, či je vložená platná tachografová karta a v takom prípade identifikuje jej typ a generáciu.

Karta sa vyhlási za neplatnú, ak už bola do záznamového zariadenia vložená karta s rovnakým číslom, ale vyšším indexom obnovy.

Karta sa vyhlási za neplatnú, ak už bola do záznamového zariadenia vložená karta s rovnakými číslom a indexom obnovy, ale vyšším indexom náhrady.

17) Tachografové karty prvej generácie považuje záznamové zariadenie za neplatné potom, ako dielňa zrušila možnosť používania tachografových kariet prvej generácie, v súlade s dodatkom 15 (požiadavka MIG 003).

18) Dielenské karty prvej generácie, ktoré sa vkladajú do záznamového zariadenia druhej generácie, sa považujú za neplatné.

19) Záznamové zariadenie musí byť technicky navrhnuté tak, aby tachografové karty po správnom vložení do zariadení s rozhraním karty zaistilo v správnej polohe.

20) Zariadenie tachografové karty uvoľní len keď vozidlo stojí a potom, ako sa na nich uložili príslušné údaje. Kartu musí aktívne uvoľniť používateľ.

3.2 **Meranie rýchlosti a vzdialenosti a zisťovanie polohy**

21) Snímač pohybu (prípadne zabudovaný do adaptéra) je hlavným zdrojom na meranie rýchlosti a vzdialenosti.

22) Táto funkcia musí nepretržite merať a udávať stav počítadla kilometrov zodpovedajúci celkovej vzdialenosti prejdenej vozidlom pomocou impulzov zo snímača pohybu.

23) Táto funkcia musí nepretržite merať a udávať rýchlosť vozidla pomocou impulzov zo snímača pohybu.

24) Funkcia merania rýchlosti musí poskytovať aj informácie o tom, či sa vozidlo pohybuje alebo stojí. Vozidlo sa považuje za pohybujúce, akonáhle funkcia zistí zo snímača pohybu viac než 1 imp/s počas minimálne piatich sekúnd, inak sa vozidlo považuje za stojace.

25) Zariadenia ukazujúce rýchlosť (rýchlomer) a celkovú prejdenú vzdialenosť (počítadlo kilometrov) namontované v každom vozidle vybavenom záznamovým zariadením spĺňajúcim ustanovenia tohto nariadenia, musia spĺňať požiadavky týkajúce sa maximálnych tolerancií stanovené v tejto prílohe (pozri 3.2.1 a 3.2.2).

26) Na zistenie manipulácie s údajmi o pohybe sa informácie zo snímača pohybu musia potvrdiť informáciami o pohybe vozidla získanými z prijímača GNSS a prípadne z jedného alebo viacerých zdrojov nezávislých od snímača pohybu.

27) Táto funkcia musí zistiť polohu vozidla, aby sa umožnilo automatické zaznamenávanie:

— polohy, kde vodič a/alebo druhý vodič začína svoj denný pracovný čas;

— polohy, kde nepretržitý čas jazdy vodiča dosiahne násobok troch hodín;

— polohy, kde vodič a/alebo druhý vodič skončí svoj denný pracovný čas.

3.2.1 *Meranie prejdenej vzdialenosti*

28) Prejdená vzdialenosť sa môže merať buď:

— tak, že sa spočítajú pohyby dopredu a dozadu, alebo

— tak, že sa zahrnie len pohyb dopredu.

29) Záznamové zariadenie meria vzdialenosť od 0 do 9 999 999,9 km.

30) Nameraná vzdialenosť musí byť v rámci nasledovných tolerancií (vzdialenosti minimálne 1 000 m):

— ± 1 % pred montážou,

— ± 2 % pri montáži a pri pravidelnej inšpekcii,

— ± 4 % počas používania.

31) Nameraná vzdialenosť sa musí merať s presnosťou aspoň 0,1 km.

3.2.2 *Meranie rýchlosti*

32) Záznamové zariadenie meria rýchlosť od 0 do 220 km/h.

33) Aby sa zaistilo ukazovanie rýchlosti s maximálnou toleranciou ± 6 km/h a berúc do úvahy:

— toleranciu ± 2 km/h pre zmeny vstupov (odchýlky pneumatík, …),

— toleranciu ±1 km/h pri meraniach vykonávaných počas montáže alebo pravidelných inšpekcií,

záznamové zariadenie musí v prípade rýchlostí od 20 do 180 km/h a v prípade charakteristických koeficientov vozidla od 4 000 do 25 000 imp/km merať rýchlosť s toleranciou ± 1 km/h (pri konštantnej rýchlosti).

Poznámka: Z rozlíšenia ukladania údajov vyplýva ďalšia tolerancia ± 0,5 km/h pre rýchlosti uložené záznamovým zariadením.

34) Rýchlosť sa musí správne merať v rámci normálnych tolerancií do 2 sekúnd po skončení zmeny rýchlosti, keď sa rýchlosť zmenila do 2 m/s^2.

35) Rýchlosť sa musí merať s rozlíšením minimálne 1 km/h.

3.2.3 *Zisťovanie polohy*

36) Záznamové zariadenie zisťuje absolútnu polohu vozidla pomocou prijímača GNSS.

37) Absolútna poloha sa zisťuje pomocou geografických súradníc zemepisnej šírky a dĺžky v stupňoch a minútach s rozlíšením 1/10 minúty.

3.3 **Meranie času**

38) Funkcia merania času meria čas stále a digitálne udáva dátum a čas UTC.

39) Dátum a čas UTC sa používajú pre datovanie údajov v rámci záznamového zariadenia (zaznamenávanie, výmena údajov) a pre všetky výpisy uvedené v dodatku 4 „Výpisy“.

40) Aby bolo možné udať miestny čas, musí sa dať meniť zobrazený časový údaj v polhodinových krokoch. Neumožňuje sa žiadny iný posun než záporné a kladné násobky polhodiny;

41) Časová odchýlka musí byť v rozmedzí ± 2 sekundy za deň v podmienkach typového schvaľovania, pri absencii akejkoľvek úpravy času.

42) Čas sa musí merať s rozlíšením minimálne 1 sekundy.

43) Meranie času nesmie byť v podmienkach typového schválenia ovplyvnené prerušením externého napájania v trvaní do 12 mesiacov.

3.4 **Monitorovanie činností vodiča**

44) Táto funkcia nepretržite a osobitne monitoruje činnosti jedného vodiča a jedného druhého vodiča.

45) Činnosťou vodiča je JAZDA, PRÁCA, POHOTOVOSŤ alebo PRESTÁVKA/ODPOČINOK.

46) Vodič a/alebo druhý vodič musí mať možnosť manuálne zvoliť PRÁCU, POHOTOVOSŤ alebo PRESTÁVKA/ODPOČINOK.

47) Keď sa vozidlo pohybuje, pre vodiča sa automaticky zvolí JAZDA a pre druhého vodiča sa automaticky zvolí POHOTOVOSŤ.

48) Keď vozidlo zastane, pre vodiča sa automaticky zvolí PRÁCA.

49) Prvá zmena činnosti na ODPOČINOK alebo POHOTOVOSŤ do 120 sekúnd po automatickej zmene na PRÁCA v dôsledku zastavenia vozidla sa považuje za zmenu, ktorá nastala v čase zastavenia vozidla (preto je možné, že sa zruší zmena na PRÁCA).

50) Výstupy tejto funkcie o zmenách činnosti určené pre záznamové funkcie sa vykonajú s presnosťou jednej minúty.

51) Ak je v rámci určitej kalendárnej minúty registrovaná počas bezprostredne predchádzajúcej a bezprostredne nadchádzajúcej minúty činnosť JAZDA, celá táto minúta sa berie ako JAZDA.

52) Kalendárna minúta, ktorá sa nepovažuje za JAZDU podľa požiadavky 051, sa celá priraďuje k tej činnosti, ktorá v priebehu minúty trvala najdlhšie (alebo k poslednej z rovnako dlhých činností).

53) Táto funkcia taktiež permanentne monitoruje nepretržitý čas jazdy a kumulovaný čas prestávky vodiča.

3.5 **Monitorovanie stavu jazdy**

54) Táto funkcia permanentne a automaticky monitoruje stav jazdy.

55) Stav jazdy POSÁDKA sa zvolí vtedy, keď sú v zariadení vložené dve platné karty vodiča; stav jazdy JEDEN VODIČ sa zvolí v ostatných prípadoch.

3.6 **Zápisy vodičov**

3.6.1 *Zápis o mieste, kde sa denný pracovný čas začína a/alebo končí*

56) Táto funkcia umožňuje zapísať miesta, kde sa podľa vodiča a/alebo druhého vodiča, jeho denný pracovný čas začína a/alebo končí.

57) Miesta sú definované ako štáty a prípadne regióny, ktoré sa zapisujú alebo potvrdzujú manuálne.

58) Pri vyberaní karty vodiča záznamové zariadenie vyzve (druhého) vodiča, aby zaznamenal „miesto, kde sa denný pracovný čas končí“.

59) Vodič následne zapíše súčasné miesto vozidla, ktoré sa považuje za dočasný zápis.

60) Príkazmi v menu musí byť možné vložiť miesta, kde sa denný pracovný čas začína a/alebo končí. Ak sa v rámci jednej kalendárnej minúty zadáva viac ako jeden takýto údaj, zostane zaznamenané iba posledné miesto začatia práce a posledné miesto ukončenia práce v rámci tohto časového úseku.

3.6.2 *Manuálne zapisovanie činností vodiča a súhlas vodiča týkajúci sa rozhrania ITS*

61) Pri vložení karty vodiča (alebo dielenskej karty), a iba v tomto čase, umožní záznamové zariadenie manuálne zadávanie činností. Činnosti sa manuálne zapisujú s použitím miestneho času a dátumu v časovej zóne (posun času UTC) aktuálne nastavených pre jednotku vozidla.

Pri vložení karty vodiča alebo dielenskej karty sa držiteľovi karty zobrazí:

— dátum a čas jeho posledného vybratia karty;

— nepovinné: posun miestneho času aktuálne stanovený pre jednotku vozidla.

Pri prvom vložení danej karty vodiča alebo dielenskej karty, ktorá je pre jednotku vozidla v súčasnosti neznáma, sa držiteľ karty vyzve, aby vyjadril súhlas s odosielaním jeho osobných údajov súvisiacich s tachografom prostredníctvom nepovinného rozhrania ITS.

Súhlas vodiča (alebo dielne) možno kedykoľvek aktivovať alebo deaktivovať príkazmi v menu, za predpokladu, že karta vodiča (alebo dielenskej karty) je vložená.

Musí byť možné zadávať činnosti s týmito obmedzeniami:

— Druh činnosti je PRÁCA, POHOTOVOSŤ alebo PRESTÁVKA/ODPOČINOK;

— čas začatia a skončenia každej činnosti sa nachádza iba v rámci časového úseku medzi posledným vybratím karty a jej aktuálnym vložením,

— neumožňuje sa vzájomné časové prekrývanie jednotlivých činností.

V prípade potreby musí byť možné manuálne zapisovanie pri prvom vložení predtým nepoužitej karty vodiča (alebo dielenskej karty).

Postup manuálneho zapisovania činností musí zahŕňať toľko po sebe idúcich krokov, koľko je potrebných na stanovenie druhu, času začatia a času skončenia každej činnosti. V ktorejkoľvek časti časového úseku medzi posledným vytiahnutím karty a aktuálnym vložením karty musí mať držiteľ karty možnosť neuviesť žiadnu z činností.

Počas manuálneho zapisovania spojeného s vložením karty musí mať držiteľ možnosť zadať prípadne:

— miesto, kde sa skončil predchádzajúci denný pracovný čas, a príslušný čas (teda prepísanie zápisu vykonaného pri poslednom vytiahnutí karty),

— miesto, kde sa začína aktuálny denný pracovný čas, a príslušný čas.

Ak držiteľ karty nezapíše miesto, kde sa pracovný čas začína alebo končí, počas manuálneho zapisovania spojeného s vložením karty, považuje sa to za vyhlásenie, že jeho pracovný čas sa nezmenil od posledného vytiahnutia karty. Najbližší zápis miesta, kde predchádzajúci denný pracovný čas končí, potom prepíše dočasný zápis vykonaný pri poslednom vytiahnutí karty.

Ak sa zapisuje nejaké miesto, musí sa zaznamenať na príslušnej tachografovej karte.

Manuálne zapisovanie sa preruší, ak:

— sa karta vytiahne alebo

— sa vozidlo pohybuje a karta je v slote vodiča.

Povolené sú aj ďalšie prerušenia, napr. vypršanie časového limitu po určitom trvaní nečinnosti používateľa. V prípade prerušenia manuálneho zapisovania záznamové zariadenie musí overiť všetky vykonané úplné zápisy miesta a činnosti (tie, ktoré majú buď jednoznačné miesto a čas, alebo druh činnosti, čas začatia a skončenia).

Ak počas manuálneho zapisovania činností pre predtým vloženú kartu dôjde k vloženiu druhej karty vodiča alebo dielenskej karty, musí byť povolené ukončiť manuálne zapisovanie pre túto predtým vloženú kartu skôr, ako sa začne manuálne zapisovanie pre druhú kartu.

Držiteľ karty musí mať možnosť manuálne zapisovať podľa tohto minimálneho postupu:

— Manuálne zapisovanie činností v chronologickom poradí za obdobie medzi posledným vytiahnutím karty a aktuálnym vložením karty.

— Čas začatia prvej činnosti sa nastaví na čas vytiahnutia karty. Pri každom nasledujúcom zápise sa čas začiatku prednastaví tak, aby nasledoval bezprostredne po čase skončenia predchádzajúceho zápisu. Pre každú činnosť sa zvolí druh činnosti a čas skončenia.

Tento postup sa skončí vtedy, keď sa čas skončenia manuálne zapísanej činnosti zhoduje s časom vloženia karty. Záznamové zariadenie môže potom umožniť držiteľovi karty zmeniť každú manuálne zapísanú činnosť, a to do okamihu potvrdenia konkrétnym príkazom. Po tomto okamihu sa zakazuje akákoľvek takáto úprava.

3.6.3 *Zápis špecifických podmienok*

62) Záznamové zariadenie musí v reálnom čase vodičovi umožniť zápis týchto dvoch špecifických podmienok:

— „ZÁZNAMOVÉ ZARIADENIE SA NEVYŽADUJE“ (začiatok, koniec)

— „PREVOZ TRAJEKTOM/VLAKOM“ (začiatok, koniec).

Pri otvorenej podmienke „ZÁZNAMOVÉ ZARIADENIE SA NEVYŽADUJE“ nesmie nastať podmienka „PREVOZ TRAJEKTOM/VLAKOM“.

Ak je karta vodiča vložená alebo vytiahnutá, musí záznamové zariadenie automaticky uzavrieť otvorenú podmienku „ZÁZNAMOVÉ ZARIADENIE SA NEVYŽADUJE“.

Pri otvorenej podmienke „ZÁZNAMOVÉ ZARIADENIE SA NEVYŽADUJE“ nesmie dôjsť k týmto udalostiam a výstrahám:

— Jazda bez príslušnej karty,

— Varovania týkajúce sa nepretržitého času jazdy.

Začiatočný znak pre PREVOZ TRAJEKTOM/VLAKOM sa musí stanoviť pred zastavením motora na trajekte/vlaku.

Otvorená podmienka PREVOZ TRAJEKTOM/VLAKOM sa musí skončiť, ak nastane ktorákoľvek z týchto možností:

— vodič ukončí PREVOZ TRAJEKTOM/VLAKOM manuálne

— vodič vytiahne svoju kartu

Otvorená podmienka PREVOZ TRAJEKTOM/VLAKOM sa musí skončiť, ak už nie je viac platná na základe pravidiel uvedených v nariadení (ES) č. 561/2006.

3.7 **Podnikové blokovanie**

63) Táto funkcia umožňuje riadiť blokovanie zavedené podnikom, aby si podnik vyhradil prístup k údajom v podnikovom režime.

64) Podnikové blokovanie pozostáva z dátumu/času začiatku (zablokovanie – lock-in) a dátumu/času skončenia (odblokovanie – lock-out) v súvislosti s identifikáciou podniku na základe čísla podnikovej karty (pri blokovaní).

65) Blokovanie sa môže zapnúť alebo vypnúť len v reálnom čase.

66) Odblokovanie môže vykonať len podnik, ktorého blokovanie je zapnuté (identifikovaný prvými 13 číslicami čísla podnikovej karty), alebo

67) odblokovanie je automatické, ak iný podnik zapne blokovanie.

68) V prípade, keď podnik aktivuje (lock-in) blokovanie a keď predchádzajúce blokovanie platilo pre rovnaký podnik, potom sa predpokladá, že predchádzajúce blokovanie nebolo vypnuté a je stále zapnuté.

3.8 **Monitorovanie kontrolných činností**

69) Táto funkcia monitoruje ZOBRAZOVANIE, TLAČ, SŤAHOVANIE z VU a karty a činnosti kontroly KALIBRÁCIE PRI CESTNEJ kontrole vykonané v priebehu režimu kontroly.

70) Táto funkcia monitoruje aj činnosti KONTROLY PREKROČENIA RÝCHLOSTI v priebehu režimu kontroly. Kontrola prekročenia rýchlosti sa považuje za uskutočnenú, ak bol v režime kontroly vytlačený alebo zobrazený výpis „prekročení rýchlosti“, alebo keď boli z dátovej pamäte VU stiahnuté údaje „udalosti a poruchy“.

3.9 **Detekcia udalostí a/alebo porúch**

71) Táto funkcia zisťuje tieto udalosti a/alebo poruchy:

3.9.1 *Udalosť „vloženie neplatnej karty“*

72) Táto udalosť sa spustí po vložení akejkoľvek neplatnej karty, po vložení karty vodiča, ktorá bola už nahradená a/alebo keď sa skončí platnosť vloženej karty.

3.9.2 *Udalosť „konflikt karty“*

73) Táto udalosť sa spustí, keď vznikne ktorákoľvek z kombinácií platných kariet označená X v tejto tabuľke:

Konflikt karty		Slot vodiča				
		Žiadna karta	Karta vodiča	Kontrolná karta	Dielenská karta	Podniková karta
Slot druhého vodiča	Žiadna karta					
	Karta vodiča				X	
	Kontrolná karta			X	X	X
	Dielenská karta		X	X	X	X
	Podniková karta			X	X	X

3.9.3 *Udalosť „prekrývanie časov“*

74) Táto udalosť sa spustí, keď dátum/čas posledného vytiahnutia karty vodiča čítaný z karty, je neskorší než aktuálny dátum/čas záznamového zariadenia, do ktorého je karta vložená.

3.9.4 *Udalosť „jazda bez príslušnej karty“*

75) Táto udalosť sa spustí pri ktorejkoľvek z kombinácií platných tachografových kariet označených X v tejto tabuľke, keď sa činnosť vodiča zmení na JAZDA, alebo keď nastane počas činnosti vodiča JAZDA zmena režimu prevádzky:

Jazda bez príslušnej karty		Slot vodiča				
		Žiadna (alebo neplatná) karta	Karta vodiča	Kontrolná karta	Dielenská karta	Podniková karta
Slot druhého vodiča	Žiadna (alebo neplatná) karta	X		X		X
	Karta vodiča	X		X	X	X
	Kontrolná karta	X	X	X	X	X
	Dielenská karta	X	X	X		X
	Podniková karta	X	X	X	X	X

3.9.5 *Udalosť „vloženie karty za jazdy“*

76) Táto udalosť sa spustí, keď sa vloží tachografová karta do ktoréhokoľvek slotu, pričom činnosť vodiča je JAZDA.

3.9.6 *Udalosť „nesprávne uzavretá posledná relácia karty“*

77) Táto udalosť sa spustí, keď pri vložení karty záznamové zariadenie zistí, že napriek ustanoveniam uvedeným v odseku 3.1, nebola správne uzavretá predchádzajúca relácia karty (karta bola vytiahnutá predtým, než boli na karte uložené všetky relevantné údaje). Túto udalosť môže spustiť iba karta vodiča alebo dielenská karta.

3.9.7 *Udalosť „prekročenie rýchlosti“*

78) Táto udalosť sa spustí pri každom prekročení rýchlosti.

3.9.8 *Udalosť „prerušenie napájania“*

79) Táto udalosť sa spustí, pokiaľ záznamové zariadenie nie je v režime kalibrácie alebo kontroly, v prípade akéhokoľvek viac než 200 milisekundového prerušenia napájania snímača pohybu a/alebo jednotky vozidla. Prah prerušenia určí výrobca. Pokles napätia počas štartovania motora vozidla nesmie spustiť túto udalosť.

3.9.9 *Udalosť „chyba komunikácie s diaľkovým komunikačným zariadením“*

80) Táto udalosť sa spustí **mimo režimu kalibrácie**, keď diaľkové komunikačné zariadenie nepotvrdí úspešné prijatie údajov diaľkovej komunikácie zasielaných z jednotky vozidla po viac ako troch pokusoch.

3.9.10 *Udalosť „chýbajúce informácie o polohe z prijímača GNSS“*

81) Táto udalosť sa spustí **mimo režimu kalibrácie** v prípade chýbajúcej informácie o polohe pochádzajúcej z prijímača GNSS (interného alebo externého) po viac ako tri hodiny kumulovaného času jazdy.

3.9.11 *Udalosť „chyba komunikácie s externým zariadením GNSS“*

82) Táto udalosť sa spustí **mimo režimu kalibrácie** v prípade prerušenia komunikácie medzi externým zariadením GNSS a jednotkou vozidla, ktorá trvá dlhšie ako 20 neprerušených minút, keď je vozidlo v pohybe.

3.9.12 *Udalosť „chyba údajov o pohybe“*

83) Táto udalosť sa spustí **mimo režimu kalibrácie** v prípade prerušenia normálneho dátového toku medzi snímačom pohybu a jednotkou vozidla a/alebo v prípade chyby v integrite alebo autentifikácie údajov počas výmeny údajov medzi snímačom pohybu a jednotkou vozidla.

3.9.13 *Udalosť „nesúlad údajov o pohybe vozidla“*

84) Táto udalosť sa spustí **mimo režimu kalibrácie**, ak informácie o pohybe vypočítané zo snímača pohybu sú v rozpore s informáciami o pohybe vypočítanými z interného prijímača GNSS alebo z externého zariadenia GNSS a prípadne z iných nezávislých zdrojov, ako je uvedené v dodatku 12. Táto udalosť sa nesmie spustiť počas prevozu trajektom/vlakom, podmienky ZÁZNAMOVÉ ZARIADENIE SA NEVYŽADUJE alebo ak informácie o polohe z prijímača GNSS nie sú k dispozícii.

3.9.14. *Udalosť „pokus o narušenie zabezpečenia“*

85) Táto udalosť sa spustí mimo režimu kalibrácie pri akejkoľvek inej udalosti ovplyvňujúcej zabezpečenie snímača pohybu a/alebo jednotky vozidla a/alebo externého zariadenia GNSS, ako sa vyžaduje v dodatku 10.

3.9.15 *Udalosť „časový konflikt“*

86) Táto udalosť sa spustí **mimo režimu kalibrácie**, keď VU zistí rozdiel väčší ako 1 minútu medzi časom pochádzajúcim z funkcie merania času jednotky vozidla a časom pochádzajúcich z prijímača GNSS. Táto udalosť sa zaznamenáva spolu s časom z vstavaných hodín z jednotky vozidla a spolu s automatickou úpravou času. Keď sa spustila udalosť časového konfliktu, počas nasledujúcich 12 hodín VU nebude generovať ďalšie udalosti časového konfliktu. Táto udalosť sa nespustí, ak prijímač GNSS nezistil v priebehu posledných 30 dní žiadny platný GNSS signál. Avšak keď sa informácie o polohe z prijímača GNSS opäť sprístupnia, vykoná sa automatická úprava času.

3.9.16 *Porucha „karty“*

87) Táto porucha nastane, keď počas prevádzky dôjde k zlyhaniu tachografovej karty.

3.9.17 *Porucha „záznamového zariadenia“*

88) Táto porucha nastane, pokiaľ záznamové zariadenie nie je v režime kalibrácie, pri ktorejkoľvek z týchto porúch:

— Interná porucha VU

— Porucha tlače

— Porucha zobrazenia

— Porucha sťahovania

— Porucha snímača

— Porucha prijímača GNSS alebo externého zariadenia GNSS

— Porucha diaľkového komunikačného zariadenia

3.10 **Zabudované a automatické skúšky**

89) Záznamové zariadenie musí automaticky zistiť poruchy pomocou automatických a zabudovaných skúšok podľa tejto tabuľky:

Skúšobná podskupina	Automatická skúška	Zabudovaná skúška
Softvér		Integrita
Dátová pamäť	Prístup	Prístup, integrita údajov
Zariadenia s rozhraním karty	Prístup	Prístup
Klávesnica		Manuálna kontrola
Tlačiareň	(ponecháva sa výrobcovi)	Výpis
Displej		Vizuálna kontrola
Sťahovanie (vykonávané len počas sťahovania)	Správna činnosť	
Snímač	Správna činnosť	Správna činnosť
Diaľkové komunikačné zariadenie	Správna činnosť	Správna činnosť
Zariadenie GNSS	Správna činnosť	Správna činnosť

3.11 **Čítanie z dátovej pamäte**

90) Záznamové zariadenie musí byť schopné čítať všetky údaje v jeho dátovej pamäti.

3.12 **Zaznamenávanie a uloženie v dátovej pamäti**

Na účely tohto odseku,

— „365 dní“ je 365 kalendárnych dní priemernej činnosti vodiča v jednom vozidle. Priemerná činnosť za deň vo vozidle je minimálne šesť vodičov alebo druhých vodičov, šesť cyklov vloženia a vybratia karty a 256 zmien činnosti. „365 dní“ preto zahŕňa minimálne 2 190 (druhých) vodičov, 2 190 vložení a vybratí karty a 93 440 zmien činnosti,

— priemerný počet polôh za deň je vymedzený ako minimálne 6 polôh, kde sa denný pracovný čas začína, 6 polôh, kde nepretržitá jazda vodiča dosiahne násobok troch hodín, a 6 polôh, kde sa denný pracovný čas končí, takže „365 dní“ zahŕňa najmenej 6 570 polôh,

— časy sa zaznamenávajú s presnosťou jednej minúty, pokiaľ nie je špecifikované inak,

— stav počítadla kilometrov sa zaznamenáva s presnosťou jedného kilometra,

— rýchlosť sa zaznamenáva s presnosťou 1 km/h,

— polohy (zemepisná šírka a dĺžka) sa zaznamenávajú v stupňoch a minútach s rozlíšením 1/10 minúty, so príslušnou presnosťou GNSS a časom získania.

91) Údaje ukladané do dátovej pamäte nesmú byť ovplyvnené prerušením externého napájania v trvaní do dvanástich mesiacov v podmienkach typového schvaľovania. Navyše údaje uložené v externom diaľkovom komunikačnom zariadení, podľa vymedzenia v dodatku 14, nesmie ovplyvniť prerušenie napájania trvajúce menej ako 28 dní.

92) Záznamové zariadenie musí byť schopné implicitne alebo explicitne zaznamenávať a ukladať vo svojej pamäti toto:

3.12.1 *Identifikačné údaje zariadenia*

3.12.1.1 Identifikačné údaje jednotky vozidla

93) Záznamové zariadenie musí byť schopné uchovávať vo svojej dátovej pamäti tieto identifikačné údaje jednotky vozidla:

— názov výrobcu,

— adresu výrobcu,

— číslo časti,

— sériové číslo,

— generácia VU,

— schopnosť používať tachografové karty prvej generácie,

— číslo softvérovej verzie,

— dátum inštalácie softvérovej verzie,

— dátum výroby zariadenia,

— schvaľovacie číslo.

94) Identifikačné údaje jednotky vozidla sú zaznamenané a natrvalo uchovávané výrobcom jednotky vozidla, s výnimkou údajov vzťahujúcich sa k softvéru a schvaľovacieho čísla, ktoré sa môžu zmeniť v prípade modernizácie softvéru a schopnosti používať tachografové karty prvej generácie.

3.12.1.2 Identifikačné údaje snímača pohybu

95) Snímač pohybu musí byť schopný uložiť vo svojej pamäti tieto identifikačné údaje:

— názov výrobcu,

— sériové číslo,

— schvaľovacie číslo.

— identifikátor zabudovaného komponentu zabezpečenia (napr. číslo dielu vnútorného čipu/procesora),

— identifikátor operačného systému (napr. číslo softvérovej verzie).

96) Výrobca snímača pohybu zaznamená a natrvalo uloží v snímači pohybu identifikačné údaje snímača pohybu.

97) Jednotka vozidla musí byť schopná zaznamenať a uložiť vo svojej dátovej pamäti nasledujúce údaje vzťahujúce sa k 20 najnovším spárovaniam snímačov pohybu (ak sa niekoľko spárovaní uskutoční v priebehu jedného kalendárneho dňa, uloží sa iba prvé a posledné v daný deň):

Za každé z týchto spárovaní sa zaznamenajú tieto údaje:

— identifikačné údaje snímača pohybu:

— sériové číslo

— schvaľovacie číslo

— údaje o spárovaní snímača pohybu:

— dátum spárovania.

3.12.1.3 Identifikačné údaje globálnych navigačných satelitných systémov

98) Externé zariadenie GNSS musí byť schopné uložiť vo svojej pamäti tieto identifikačné údaje:

— názov výrobcu,

— sériové číslo,

— schvaľovacie číslo.

— identifikátor zabudovaného komponentu zabezpečenia (napr. číslo dielu vnútorného čipu/procesora),

— identifikátor operačného systému (napr. číslo softvérovej verzie).

99) Identifikačné údaje sú zaznamenané a natrvalo uložené v externom zariadení GNSS výrobcom externého zariadenia GNSS.

100) Jednotka vozidla musí byť schopná zaznamenať a uložiť vo svojej dátovej pamäti nasledujúce údaje vzťahujúce sa k 20 najnovším spojeniam s externými zariadeniami GNSS (ak sa niekoľko spojení uskutoční v priebehu jedného kalendárneho dňa, uloží sa iba prvé a posledné v daný deň).

Za každé z týchto spojení sa musia zaznamenať tieto údaje:

— identifikačné údaje externého zariadenia GNSS:

— sériové číslo,

— schvaľovacie číslo.

— údaje o spojení s externým zariadením GNSS:

— dátum spojenia

3.12.2 *Kľúče a certifikáty*

101) Záznamové zariadenie musí byť schopné ukladať niekoľko kryptografických kľúčov a certifikátov, ako je uvedené v dodatku 11 časti A a časti B.

3.12.3 *Údaje o vložení a vybratí karty vodiča alebo dielenskej karty*

102) Pri každom cykle vloženia karty vodiča alebo dielenskej karty do zariadenia a jej vytiahnutia zo zariadenia, záznamové zariadenie zaznamená a uloží vo svojej dátovej pamäti:

— priezvisko a meno(-á) držiteľa karty uložené na karte,

— číslo karty, vydávajúci členský štát a dátum skončenia platnosti, ako sú uložené na karte,

— generáciu karty,

— dátum a čas vloženia,

— stav počítadla kilometrov pri vložení karty,

— slot, do ktorého je karta vložená,

— dátum a čas vybratia,

— stav počítadla kilometrov pri vybratí karty,

— nasledovné informácie o predchádzajúcom vozidle, ktoré vodič použil, uložené na karte:

— evidenčné číslo vozidla a členský štát evidencie,

— generácia VU (ak je k dispozícii),

— dátum a čas vybratia karty,

— znak udávajúci, či pri vložení karty držiteľ karty manuálne zapísal alebo nezapísal činnosti.

103) Dátová pamäť musí byť schopná uchovať tieto údaje aspoň 365 dní.

104) Keď je kapacita pamäte vyčerpaná, najstaršie údaje sa prepíšu novými údajmi.

3.12.4 *Údaje o činnosti vodiča*

105) Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti každú zmenu činnosti vodiča a/alebo druhého vodiča, a/alebo každú zmenu stavu jazdy, a/alebo každé vloženie alebo vybratie karty vodiča alebo dielenskej karty:

— stav vedenia vozidla (POSÁDKA, JEDEN VODIČ),

— slot (VODIČ, DRUHÝ VODIČ),

— stav karty v príslušnom slote (VLOŽENÁ, NEVLOŽENÁ)

— činnosť (JAZDA, POHOTOVOSŤ, PRÁCA, PRESTÁVKA/ODPOČINOK).

— dátum a čas zmeny.

VLOŽENÁ znamená, že je v slote vložená platná karta vodiča alebo dielenská karta. NEVLOŽENÁ znamená opak, teda že v slote nie je vložená žiadna platná karta vodiča ani dielenská karta (napr. je tam vložená podniková karta alebo tam nie je vložená karta)

Údaje o činnosti zapísané manuálne vodičom sa v dátovej pamäti nezaznamenávajú.

106) Dátová pamäť musí byť schopná uchovať údaje o činnosti vodiča aspoň 365 dní.

107) Keď je kapacita pamäte vyčerpaná, najstaršie údaje sa prepíšu novými údajmi.

3.12.5 *Miesta a polohy, kde sa denný pracovný čas začína a/alebo končí, a/alebo kde sa dosiahne 3-hodinový čas nepretržitej jazdy*

108) Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti:

— miesta a polohy, kde vodič a/alebo druhý vodič začína svoj denný pracovný čas;

— polohy, kde nepretržitý čas jazdy vodiča dosiahne násobok troch hodín;

— miesta a polohy, kde vodič a/alebo druhý vodič končí svoj denný pracovný čas.

109) Ak poloha vozidla nie je v týchto časoch k dispozícii z prijímača GNSS, záznamové zariadenie musí použiť poslednú dostupnú polohu a súvisiaci dátum a čas.

110) Spolu s každým miestom alebo polohou musí záznamové zariadenie zaznamenať a uložiť vo svojej dátovej pamäti:

— číslo karty (druhého) vodiča a vydávajúci členský štát,

— generáciu karty,

— dátum a čas zápisu,

— typ zápisu (začiatok, koniec alebo 3-hodinový čas nepretržitej jazdy),

— súvisiacu presnosť GNSS, prípadne dátum a čas;

— stav počítadla kilometrov.

111) Dátová pamäť musí byť schopná uchovať miesta a polohy, kde sa denný pracovný čas začína a/alebo končí, a/alebo kde sa dosiahol 3 hodinový čas nepretržitej jazdy aspoň počas 365 dní.

112) Keď je kapacita pamäte vyčerpaná, najstaršie údaje sa prepíšu novými údajmi.

3.12.6 *Údaje počítadla kilometrov*

113) Záznamové zariadenie musí každý kalendárny deň o polnoci zaznamenať vo svojej dátovej pamäti stav počítadla kilometrov vozidla a zodpovedajúci dátum.

114) Dátová pamäť musí byť schopná uložiť polnočné stavy počítadla kilometrov aspoň počas 365 dní.

115) Keď je kapacita pamäte vyčerpaná, najstaršie údaje sa prepíšu novými údajmi.

3.12.7 *Podrobné údaje o rýchlosti*

116) Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti okamžitú rýchlosť vozidla a zodpovedajúci dátum a čas v každej sekunde aspoň posledných 24 hodín, v priebehu ktorých sa vozidlo pohybuje.

3.12.8 *Údaje o udalostiach*

Na účely tohto pododseku sa čas musí zaznamenať s presnosťou jednej sekundy.

117) Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti tieto údaje za každú zistenú udalosť podľa nasledovných pravidiel ukladania:

Udalosť	Pravidlá ukladania	Údaje zaznamenané podľa udalosti
Vloženie neplatnej karty	— 10 posledných udalostí.	— dátum a čas udalosti, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia karty, ktorá udalosť spôsobila, — počet podobných udalostí v daný deň.
Konflikt karty	— 10 posledných udalostí.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia dvoch kariet, ktoré spôsobujú konflikt.
Jazda bez príslušnej karty	— najdlhšie trvajúca udalosť za každý z 10 posledných dní výskytu, — 5 najdlhšie trvajúcich udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia každej karty vloženej na začiatku a/alebo konci udalosti, — počet podobných udalostí v daný deň.

Udalosť	Pravidlá ukladania	Údaje zaznamenané podľa udalosti
Vloženie karty za jazdy	— posledná udalosť za každý z 10 posledných dní výskytu,	— dátum a čas udalosti, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia, — počet podobných udalostí v daný deň.
Nesprávne uzavretá posledná relácia karty	— 10 posledných udalostí.	— dátum a čas vloženia karty, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia, — údaje poslednej relácie tak, ako sú čítané z karty: — dátum a čas vloženia karty, — evidenčné číslo vozidla, členský štát evidencie a generácia VU.
Prekročenie rýchlosti (1)	— najvážnejšia udalosť za každý z posledných 10 dní výskytu (t. j. tá, pri ktorej bola priemerná rýchlosť najvyššia), — 5 najvážnejších udalostí počas posledných 365 dní. — prvá udalosť, ktorá sa vyskytla po poslednej kalibrácii.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — maximálna rýchlosť nameraná počas udalosti, — aritmetický priemer rýchlostí nameraných počas udalosti, — typ karty, číslo, vydávajúci členský štát a generácia karty vodiča (v prípade potreby), — počet podobných udalostí v daný deň.
Prerušenie napájania (2)	— najdlhšie trvajúca udalosť za každý z 10 posledných dní výskytu, — 5 najdlhšie trvajúcich udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia každej karty vloženej na začiatku a/alebo konci udalosti, — počet podobných udalostí v daný deň.
Chyba komunikácie s diaľkovým komunikačným zariadením	— najdlhšie trvajúca udalosť za každý z 10 posledných dní výskytu, — 5 najdlhšie trvajúcich udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia každej karty vloženej na začiatku a/alebo konci udalosti, — počet podobných udalostí v daný deň.
Chýbajúce informácie o polohe z prijímača GNSS	— najdlhšie trvajúca udalosť za každý z 10 posledných dní výskytu, — 5 najdlhšie trvajúcich udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia každej karty vloženej na začiatku a/alebo konci udalosti, — počet podobných udalostí v daný deň.

Udalosť	Pravidlá ukladania	Údaje zaznamenané podľa udalosti
Chyba údajov o pohybe	— najdlhšie trvajúca udalosť za každý z 10 posledných dní výskytu, — 5 najdlhšie trvajúcich udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia každej karty vloženej na začiatku a/alebo konci udalosti, — počet podobných udalostí v daný deň.
Nesúlad údajov o pohybe vozidla	— najdlhšie trvajúca udalosť za každý z 10 posledných dní výskytu, — 5 najdlhšie trvajúcich udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia každej karty vloženej na začiatku a/alebo konci udalosti, — počet podobných udalostí v daný deň.
Pokus o narušenie zabezpečenia	— 10 posledných udalostí za každý typ udalosti.	— dátum a čas začiatku udalosti, — dátum a čas skončenia udalosti (ak je relevantný), — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia každej karty vloženej na začiatku a/alebo konci udalosti, — typ udalosti.
Časový konflikt	— najdlhšie trvajúca udalosť za každý z 10 posledných dní výskytu, — 5 najdlhšie trvajúcich udalostí počas posledných 365 dní.	— dátum a čas záznamového zariadenia — dátum a čas GNSS, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia každej karty vloženej na začiatku a/alebo konci udalosti, — počet podobných udalostí v daný deň.

(1) Záznamové zariadenie musí vo svojej dátovej pamäti zaznamenávať a ukladať aj:

— dátum a čas poslednej KONTROLY PREKROČENIA RÝCHLOSTI,

— dátum a čas prvého prekročenia rýchlosti nasledujúceho po tejto KONTROLE PREKROČENIA RÝCHLOSTI,

— počet udalostí prekročenia rýchlosti od poslednej KONTROLY PREKROČENIA RÝCHLOSTI.

(2) Tieto údaje sa môžu zaznamenať len pri opätovnom pripojení napájania, časy môžu byť známe s presnosťou na minútu.

3.12.9 *Údaje o poruchách*

Na účely tohto pododseku sa čas musí zaznamenať s presnosťou jednej sekundy.

118) Záznamové zariadenie sa musí pokúsiť zaznamenať a uložiť vo svojej dátovej pamäti tieto údaje za každú zistenú poruchu podľa nasledovných pravidiel ukladania:

Porucha	Pravidlá ukladania	Údaje, ktoré sa majú zaznamenať podľa poruchy
Porucha karty	— 10 posledných porúch karty vodiča.	— dátum a čas začiatku poruchy, — dátum a čas konca poruchy, — typ(-y) karty(-iet), číslo, vydávajúci členský štát a generácia.
Poruchy záznamového zariadenia	— 10 najnovších porúch za každý typ poruchy, — prvá porucha po poslednej kalibrácii.	— dátum a čas začiatku poruchy, — dátum a čas konca poruchy, — typ poruchy, — typ(-y) karty(-iet), číslo a vydávajúci členský štát a generácia každej karty vloženej na začiatku a/alebo konci poruchy.

3.12.10 *Kalibračné údaje*

119) Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti údaje vzťahujúce sa k:

— známym kalibračným parametrom v okamihu aktivácie,

— jeho skutočne prvej kalibrácii po jeho aktivácii,

— jeho prvej kalibrácii v súčasnom vozidle (identifikovanom jeho identifikačným číslom vozidla (VIN)),

— 20 posledným kalibráciám (ak sa niekoľko kalibrácií uskutočnilo v priebehu jedného kalendárneho dňa, uloží sa len prvá a posledná v tomto dni).

120) Za každú z týchto kalibrácií sa zaznamenajú tieto údaje:

— účel kalibrácie (aktivácia, prvá montáž, montáž, pravidelná inšpekcia),

— názov dielne a adresa,

— číslo dielenskej karty, jej vydávajúci členský štát a dátum skončenia platnosti karty,

— identifikácia vozidla,

— aktualizované alebo potvrdené parametre: w, k, l, rozmery pneumatík, nastavenia obmedzovača rýchlosti, počítadlo kilometrov (staré a nové hodnoty), dátum a čas (staré a nové hodnoty),

— druhy a identifikátory všetkých používaných plomb.

121) Okrem toho musí záznamové zariadenie zaznamenať a uložiť vo svojej dátovej pamäti svoju schopnosť používať tachografové karty prvej generácie (stále aktivované alebo nie).

122) Snímač pohybu musí zaznamenať a uložiť vo svojej dátovej pamäti tieto údaje o montáži snímača pohybu:

— prvé spárovanie s jednotkou vozidla (dátum, čas, schvaľovacie číslo VU, sériové číslo VU),

— posledné spárovanie s VU (dátum, čas, schvaľovacie číslo VU, sériové číslo VU).

123) Externé zariadenie GNSS musí zaznamenať a uložiť vo svojej pamäti tieto údaje o montáži externého zariadenia GNSS:

— prvé spojenie s jednotkou vozidla (dátum, čas, schvaľovacie číslo VU, sériové číslo VU),

— posledné spojenie s jednotkou vozidla (dátum, čas, schvaľovacie číslo VU, sériové číslo VU).

3.12.11 *Údaje o úprave času*

124) Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti údaje vzťahujúce sa k úpravám času vykonaným v režime kalibrácie mimo rámca pravidelnej kalibrácie (vymedzenie pojmov, písm. f)):

— najnovšia úprava času,

— 5 najväčších úprav času.

125) Za každú z týchto úprav času sa zaznamenajú tieto údaje:

— dátum a čas, stará hodnota,

— dátum a čas, nová hodnota,

— názov dielne a adresa,

— číslo dielenskej karty, jej vydávajúci členský štát, generácia karty a dátum skončenia platnosti karty.

3.12.12 *Údaje o kontrolnej činnosti*

126) Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti tieto údaje vzťahujúce sa k 20 najnovším kontrolným činnostiam:

— dátum a čas kontroly,

— číslo kontrolnej karty, jej vydávajúci členský štát a generácia karty,

— typ kontroly (zobrazovanie a/alebo tlač a/alebo sťahovanie z VU a/alebo sťahovanie z karty a/alebo kontrola kalibrácie pri cestnej kontrole).

127) Pri sťahovaní údajov sa musia zaznamenať aj dátumy najstarších a najnovších stiahnutých dní.

3.12.13 *Údaje o podnikovom blokovaní*

128) Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti tieto údaje vzťahujúce sa k 255 posledným podnikovým blokovaniam:

— dátum a čas zablokovania,

— dátum a čas odblokovania,

— číslo podnikovej karty, jej vydávajúci členský štát a generácia karty,

— názov a adresa podniku.

Údaje, ktoré boli predtým zablokované blokovaním odstráneným z pamäte v dôsledku uvedeného limitu, sa považujú za nezablokované.

3.12.14 *Údaje o činnosti sťahovania*

129) Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti tieto údaje vzťahujúce sa k poslednému stiahnutiu dátovej pamäte na externé médium počas podnikového režimu alebo režimu kalibrácie:

— dátum a čas stiahnutia,

— číslo podnikovej alebo dielenskej karty, jej vydávajúci členský štát a generácia karty,

— názov podniku alebo dielne.

3.12.15 *Údaje o špecifických podmienkach*

130) Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti tieto údaje vzťahujúce sa k špecifickým podmienkam:

— dátum a čas zápisu,

— druh špecifickej podmienky.

131) Dátová pamäť musí byť schopná uchovať údaje o špecifických podmienkach aspoň 365 dní (s predpokladom, že v priemere je denne otvorená a uzatvorená jedna podmienka). Keď je kapacita pamäte vyčerpaná, najstaršie údaje sa prepíšu novými údajmi.

3.12.16 *Údaje o tachografovej karte*

132) Záznamové zariadenie musí byť schopné uložiť tieto údaje týkajúce sa rôznych tachografových kariet, ktoré sa použili vo VU:

— číslo tachografovej karty a jej sériové číslo,

— výrobca tachografovej karty,

— typ tachografovej karty,

— verzia tachografovej karty.

133) Záznamové zariadenie musí byť schopné uložiť aspoň 88 takých záznamov.

3.13 **Čítanie z tachografovej karty**

134) Záznamové zariadenie musí byť schopné odčítať z tachografovej karty prvej a druhej generácie v prípade potreby údaje potrebné na:

— identifikáciu typu karty, držiteľa karty, predtým použitého vozidla, dátumu a času posledného vytiahnutia karty a činnosti zvolenej v tomto čase,

— kontrolu správneho uzatvorenia poslednej relácie karty,

— výpočet nepretržitého času jazdy vodiča, kumulovaného času prestávok a kumulovaných časov jazdy za predchádzajúci a súčasný týždeň,

— tlač požadovaných výpisov vzťahujúcich sa k údajom zaznamenaným na karte vodiča,

— stiahnutie karty vodiča na externé médium.

Táto požiadavka sa týka len tachografových kariet prvej generácie, ak dielňa ich používanie nezrušila.

135) V prípade chyby čítania sa musí záznamové zariadenie pokúsiť znovu, maximálne trikrát, o rovnaký príkaz na čítanie, a ak je znovu neúspešný, potom musí vyhlásiť kartu za chybnú a neplatnú.

3.14 **Zaznamenávanie a ukladanie na tachografovú kartu**

3.14.1 *Zaznamenávanie a ukladanie na tachografové karty prvej generácie*

136) Za predpokladu, že používanie tachografových kariet prvej generácie dielňa nezrušila, záznamové zariadenie musí zaznamenať a uložiť údaje presne rovnakým spôsobom, ako by to vykonalo záznamové zariadenie prvej generácie.

137) Záznamové zariadenie musí nastaviť „údaje o relácii karty“ na karte vodiča alebo na dielenskej karte hneď po vložení karty.

138) Záznamové zariadenie musí aktualizovať údaje uložené na platnej karte vodiča, dielenskej karte, podnikovej a/alebo kontrolnej karte o všetky nevyhnutné údaje relevantné pre časový úsek, počas ktorého je karta vložená, a ktoré sa týkajú držiteľa karty. Údaje uložené na týchto kartách sú špecifikované v kapitole 4.

139) Záznamové zariadenie aktualizuje údaje o činnosti vodiča a o miestach (špecifikované v bodoch 4.5.3.1.9 a 4.5.3.1.11) uložené na platnej karte vodiča a/alebo na dielenskej karte, o údaje o činnosti a miestach, ktoré manuálne zapísal držiteľ karty.

140) Žiadne udalosti, ktoré pre prvú generáciu záznamového zariadenia nie sú vymedzené, sa nesmú ukladať na kartu vodiča ani na dielenskú kartu.

141) Aktualizácia údajov tachografovej karty prebieha tak, že keď je to potrebné a berúc do úvahy skutočnú úložnú kapacitu karty, najstaršie údaje sa nahradia najnovšími údajmi.

142) V prípade chybného zápisu sa záznamové zariadenie pokúsi znovu, a maximálne trikrát, o rovnaký príkaz zápisu, a ak je znovu neúspešný, potom musí vyhlásiť kartu za chybnú a neplatnú.

143) Pred vytiahnutím karty vodiča a potom, ako boli uložené všetky relevantné údaje na karte, záznamové zariadenie resetuje údaje týkajúce sa relácie karty.

3.14.2 *Zaznamenávanie a ukladanie na tachografové karty druhej generácie*

144) Tachografové karty druhej generácie musia obsahovať 2 rozdielne aplikácie, z ktorých prvá musí byť rovnaká ako aplikácia TACHO pri tachografových kartách prvej generácie, a druhá aplikácia „TACHO_G2“ musí zodpovedať požiadavkám kapitoly 4 a dodatku 2.

145) Záznamové zariadenie musí nastaviť „údaje o relácii karty“ na karte vodiča alebo na dielenskej karte hneď po vložení karty.

146) Záznamové zariadenie aktualizuje údaje uložené v oboch aplikáciách platnej karty vodiča, dielenskej karty, podnikovej a/alebo kontrolnej karty o všetky nevyhnutné údaje relevantné pre časový úsek, počas ktorého je karta vložená, a ktoré sa týkajú držiteľa karty. Údaje uložené na týchto kartách sú špecifikované v kapitole 4.

147) Záznamové zariadenie aktualizuje údaje o činnosti vodiča a o miestach a polohách (špecifikované v bodoch 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 a 4.5.3.2.11) uložené na platnej karte vodiča a/alebo na dielenskej karte, o údaje o činnosti a miestach, ktoré manuálne zapísal držiteľ karty.

148) Aktualizácia údajov tachografovej karty prebieha tak, že keď je to potrebné a berúc do úvahy skutočnú úložnú kapacitu karty, najstaršie údaje sa nahradia najnovšími údajmi.

149) V prípade chybného zápisu sa záznamové zariadenie pokúsi znovu, a maximálne trikrát, o rovnaký príkaz zápisu, a ak je znovu neúspešný, potom musí vyhlásiť kartu za chybnú a neplatnú.

150) Pred vytiahnutím karty vodiča a potom, ako boli uložené všetky relevantné údaje na oboch aplikáciách karty, záznamové zariadenie resetuje údaje týkajúce sa relácie karty.

3.15 **Zobrazovanie**

151) Displej musí obsahovať aspoň 20 znakov.

152) Minimálna výška znaku musí byť 5 mm a šírka 3,5 mm.

153) Displej musí podporovať znaky uvedené v dodatku 1, kapitole 4 „Množiny znakov“. Displej môže používať zjednodušené zobrazenie (napr. znaky s diakritikou môžu byť zobrazované bez nej, alebo malé písmená môžu byť zobrazované ako veľké písmená).

154) Displej musí byť vybavený primeraným neoslňujúcim osvetlením.

155) Údaje musia byť viditeľné zvonka záznamového zariadenia.

156) Záznamové zariadenie musí byť schopné zobraziť:

— predvolené údaje,

— údaje o výstrahách,

— údaje o prístupe k menu,

— ostatné údaje požadované používateľom.

Záznamové zariadenie môže zobraziť doplňujúce informácie za predpokladu, že sa dajú zreteľne odlíšiť od informácií uvedených vyššie.

157) Displej záznamového zariadenia musí používať piktogramy alebo kombinácie piktogramov uvedené v dodatku 3. Doplňujúce piktogramy alebo kombinácie piktogramov môže displej zobrazovať za predpokladu, že sa dajú zreteľne odlíšiť od prv uvedených piktogramov.

158) Displej musí byť zapnutý (ON) vždy, keď sa vozidlo pohybuje.

159) Záznamové zariadenie môže obsahovať manuálnu alebo automatickú funkciu, ktorá vypne displej (OFF), keď sa vozidlo nepohybuje.

Zobrazovací formát je špecifikovaný v dodatku 5.

3.15.1 *Zobrazenie predvolených údajov*

160) Keď nemusia byť zobrazené žiadne iné informácie, záznamové zariadenie musí štandardne zobraziť toto:

— miestny čas (ako výsledok času UTC + posun nastavený vodičom),

— režim prevádzky,

— súčasná činnosť vodiča a súčasná činnosť druhého vodiča,

— informácie vzťahujúce sa k vodičovi:

— ak jeho súčasná činnosť je JAZDA, jeho aktuálny nepretržitý čas jazdy a jeho aktuálny kumulovaný čas prestávok,

— ak jeho súčasná činnosť nie je JAZDA, aktuálny čas trvania tejto inej činnosti (od času, kedy bola zvolená) a jeho aktuálny kumulovaný čas prestávok.

161) Zobrazenie údajov týkajúcich sa každého vodiča musí byť jasné, jednoduché a jednoznačné. V prípade, ak sa informácie týkajúce sa vodiča a druhého vodiča nemôžu zobraziť súčasne, záznamové zariadenie musí štandardne zobraziť informácie týkajúce sa vodiča a umožniť používateľovi zobraziť informácie týkajúce sa druhého vodiča.

162) Ak šírka displeja neumožňuje zobraziť štandardne režim prevádzky, záznamové zariadenie pri zmene režimu krátko zobrazí nový režim prevádzky.

163) Záznamové zariadenie pri vložení karty krátko zobrazí meno držiteľa karty.

164) Keď je otvorená podmienka „ZÁZNAMOVÉ ZARIADENIE SA NEVYŽADUJE“ alebo „PREVOZ TRAJEKTOM/VLAKOM“ , potom štandardné zobrazenie musí s využitím príslušného piktogramu ukázať, že je konkrétna podmienka otvorená (pripúšťa sa, že súčasne sa nemusí zobraziť aktuálna činnosť vodiča).

3.15.2 *Zobrazenie výstrahy*

165) Záznamové zariadenie musí zobraziť výstražné informácie najmä s použitím piktogramov uvedených v dodatku 3, doplnené v prípade potreby dodatočnými numericky kódovanými informáciami. Možno pridať aj textový opis výstrahy zobrazený v jazyku, ktorý si vodič vyberie.

3.15.3 *Prístup k menu*

166) Záznamové zariadenie musí poskytovať nevyhnutné príkazy vo vhodnej štruktúre menu.

3.15.4 *Iné zobrazenia*

167) Na požiadanie musí byť možné selektívne zobraziť:

— čas UTC a dátum, ako aj posun miestneho času,

— obsah každého zo šiestich výpisov v rovnakom formáte, v akom sú samotné výpisy,

— nepretržitý čas jazdy a kumulovaný čas prestávok vodiča,

— nepretržitý čas jazdy a kumulovaný čas prestávok druhého vodiča,

— kumulovaný čas jazdy vodiča za predchádzajúci a aktuálny týždeň,

— kumulovaný čas jazdy druhého vodiča za predchádzajúci a prebiehajúci týždeň,

voliteľné:

— aktuálny čas trvania činnosti druhého vodiča (od času, kedy bola zvolená).

— kumulovaný čas jazdy vodiča za prebiehajúci týždeň,

— kumulovaný čas jazdy druhého vodiča počas prebiehajúceho denného pracovného času,

— kumulovaný čas jazdy vodiča počas prebiehajúceho denného pracovného času,

168) Zobrazenie obsahu výpisu musí byť sekvenčné, riadok po riadku. Ak je šírka displeja menšia než 24 znakov, používateľ musí vhodne dostať úplné informácie (niekoľko riadkov, rolovanie …).

Riadky tlačených výpisov pre ručné záznamy sa nemusia zobraziť.

3.16 **Tlač**

169) Záznamové zariadenie musí byť schopné vytlačiť informácie zo svojej dátovej pamäte a/alebo z tachografovej karty v týchto siedmich výpisoch:

— denný výpis činností vodiča z karty,

— denný výpis činností vodiča z jednotky vozidla,

— výpis udalostí a porúch z karty,

— výpis udalostí a porúch z jednotky vozidla,

— výpis technických údajov,

— výpis prekročenia rýchlosti.

— História údajov tachografovej karty pre danú VU (pozri kapitolu 3.12.16)

Podrobné formáty a obsah týchto výpisov sú uvedené v dodatku 4.

Na konci výpisov môžu byť poskytnuté doplňujúce údaje.

Záznamové zariadenie môže poskytnúť aj doplňujúce výpisy za predpokladu, že sa dajú zreteľne odlíšiť od siedmich predchádzajúcich výpisov.

170) „Denný výpis činností vodiča z karty“ a „výpis udalostí a porúch z karty“ je k dispozícii len vtedy, keď je karta vodiča alebo dielenská karta vložená do záznamového zariadenia. Záznamové zariadenie aktualizuje údaje uložené na relevantnej karte pred začiatkom tlače.

171) Aby sa vyhotovil „denný výpis činností vodiča z karty“ alebo „výpis udalostí a porúch z karty“, záznamové zariadenie:

— buď automaticky zvolí kartu vodiča alebo dielenskú kartu, ak je vložená len jedna z týchto kariet,

— alebo umožní príkaz, ktorým sa zvolí zdroj karty, alebo sa zvolí karta v slote vodiča, ak sú do záznamového zariadenia vložené dve tieto karty.

172) Tlačiareň musí byť schopná tlačiť 24 znakov v každom riadku.

173) Minimálna výška znaku musí byť 2,1 mm a šírka 1,5 mm.

174) Tlačiareň musí podporovať znaky uvedené v dodatku 1, kapitole 4 „Množiny znakov“.

175) Tlačiarne musia byť konštruované tak, aby výpisy boli k dispozícii s úrovňou rozlíšenia, ktorá zabráni nejednoznačnosti pri ich čítaní.

176) Rozmery výpisov a údaje nesmú vykazovať žiadne zmeny v normálnych podmienkach vlhkosti (10 až 90 %) a teploty.

177) Typovo schválený papier výpisu používaný v záznamovom zariadení musí mať relevantnú značku typového schválenia a údaj o type(-och) záznamového zariadenia, v ktorom sa môže používať.

178) V normálnych podmienkach skladovania, pokiaľ ide o intenzitu svetla, vlhkosť a teplotu, musia zostať výpisy zreteľne čitateľné a identifikovateľné aspoň dva roky.

179) Výpisy musia spĺňať aspoň skúšobné špecifikácie vymedzené v dodatku 9.

180) Musí byť možné doplniť tieto dokumenty rukou písanými poznámkami, ako je podpis vodiča.

181) Ak počas tlače nastane udalosť „v zásobníku nie je papier“, po doplnení papiera naštartuje záznamové zariadenie tlač od začiatku výpisu, alebo pokračuje v tlači, pričom poskytne jednoznačný odkaz na predchádzajúcu vytlačenú časť.

3.17 **Výstrahy**

182) Záznamové zariadenie musí varovať vodiča, ak zistí akúkoľvek udalosť a/alebo poruchu.

183) Výstraha pri udalosti prerušenie napájania sa môže oneskoriť, kým nie je znovu obnovené napájanie.

184) Záznamové zariadenie musí varovať vodiča 15 minút pred prekročením maximálneho povoleného nepretržitého času jazdy a pri prekročení tohto času.

185) Výstrahy musia byť vizuálne. Môžu byť k dispozícii aj zvukové výstrahy za predpokladu, že sú doplnkom k vizuálnym výstrahám.

186) Vizuálne výstrahy musia byť používateľom jednoznačne rozpoznateľné, musia byť umiestnené v zornom poli vodiča a musia byť zreteľne čitateľné cez deň, ako aj v noci.

187) Vizuálne výstrahy môžu byť zabudované do záznamového zariadenia a/alebo namontované v určitej vzdialenosti od zariadenia.

188) V druhom prípade musí mať symbol „T".

189) Čas trvania výstrah musí byť aspoň 30 sekúnd, kým ich používateľ jedným alebo viacerými špecifickými tlačidlami záznamového zariadenia nepotvrdí. Toto prvé potvrdenie nesmie vymazať zobrazenie príčiny výstrahy uvedené v nasledujúcom odseku.

190) Príčina výstrahy sa musí zobraziť na záznamovom zariadení a zostať viditeľná až kým ju používateľ nepotvrdí osobitným tlačidlom alebo príkazom záznamového zariadenia.

191) Môžu byť k dispozícii doplnkové výstrahy, pokiaľ si ich vodič nemôže zameniť s už vymedzenými výstrahami.

3.18 Sťahovanie údajov na externé médiá

192) Záznamové zariadenie musí byť na požiadanie schopné stiahnuť údaje zo svojej dátovej pamäte alebo z karty vodiča na externé pamäťové médiá cez kalibračný/sťahovací konektor. Záznamové zariadenie aktualizuje údaje uložené na príslušnej karte pred začiatkom sťahovania.

193) Okrem toho a nepovinne môže záznamové zariadenie v ktoromkoľvek režime prevádzky sťahovať údaje akýmkoľvek iným spôsobom pre podnik autentifikovaný prostredníctvom tohto kanálu. V takom prípade platia pre toto sťahovanie prístupové práva k údajom v podnikovom režime.

194) Sťahovanie nesmie zmeniť alebo vymazať žiadne uložené údaje.

195) Elektrické rozhranie konektora kalibrácie/sťahovania je špecifikované v dodatku 6.

196) Protokoly sťahovania sú špecifikované v dodatku 7.

3.19 Diaľková komunikácia v prípade cielených cestných kontrol

197) Keď je zapaľovanie zapnuté, jednotka vozidla musí v diaľkovom komunikačnom zariadení ukladať každých 60 sekúnd posledné údaje potrebné na účel cielených cestných kontrol. Tieto údaje sú šifrované a podpísané, ako je uvedené v dodatku 11 a dodatku 14.

198) Údaje, ktoré sa majú skontrolovať diaľkovo, musia byť k dispozícii snímaču komunikačného zariadenia prostredníctvom bezdrôtovej komunikácie, ako je uvedené v dodatku 14.

199) Údaje, ktoré sú potrebné na účely cielených cestných kontrol, sa týkajú:

— posledného pokusu o narušenie zabezpečenia,

— najdlhšieho prerušenia napájania,

— poruchy snímača,

— chyby údajov o pohybe,

— nesúladu údajov o pohybe vozidla,

— jazdy bez platnej karty,

— vloženia karty za jazdy,

— údajov o úprave času,

— kalibračných údajov vrátane dátumov posledných dvoch uložených záznamov o kalibrácii,

— evidenčného čísla vozidla,

— rýchlosti zaznamenanej tachografom.

3.20 **Výstupné údaje pre doplnkové externé zariadenia**

200) Záznamové zariadenie môže byť tiež vybavené štandardizovanými rozhraniami umožňujúcimi, aby údaje, ktoré tachograf zaznamenal alebo vytvoril, používalo v prevádzkovom režime alebo režime kalibrácie externé zariadenie.

V dodatku 13 je špecifikované a štandardizované nepovinné rozhranie ITS. Zároveň možno používať aj iné podobné rozhrania, ak plne vyhovujú požiadavkám dodatku 13 z hľadiska minimálneho zoznamu údajov, zabezpečenia a súhlasu vodiča.

Na údaje ITS sa uplatňujú tieto požiadavky sprístupnené prostredníctvom daného rozhrania:

— tieto údaje predstavujú súbor vybraných existujúcich údajov zo slovníka údajov tachografu (dodatok 1),

— podsúbor týchto vybraných údajov sa označuje „osobné údaje“,

— podsúbor „osobné údaje“ je k dispozícii, len keď je aktivovaný overiteľný súhlas vodiča, ktorým akceptuje, že jeho osobné údaje môžu opustiť sieť vozidla,

— súhlas vodiča možno kedykoľvek aktivovať alebo deaktivovať príkazmi v menu, za predpokladu, že karta vodiča je vložená,

— tento súbor a podsúbor údajov sa vysiela cez bezdrôtový Bluetooth protokol v kabíne vozidla, s obnovovacou frekvenciou 1 minúty,

— párovanie externého zariadenia s rozhraním ITS bude chránené vyhradeným a náhodným PIN kódom s aspoň 4 číslicami, ktorý sa zaznamená a sprístupní prostredníctvom displeja každej jednotky vozidla,

— za žiadnych okolností nemôže prítomnosť rozhrania ITS narušiť alebo ovplyvniť správne fungovanie a zabezpečenie jednotky vozidla.

Okrem daného minimálneho súboru existujúcich údajov môžu byť výstupom aj ďalšie údaje, ak ich nemožno považovať za osobné.

Záznamové zariadenie musí informovať ostatné externé zariadenia o súhlase vodiča.

Keď je zapaľovanie vozidla zapnuté (ON), tieto údaje sa musia nepretržite vysielať.

201) Tachografy sa z dôvodu spätnej kompatibility môžu aj naďalej vybavovať rozhraním sériového spojenia podľa špecifikácie v prílohe 1B k nariadeniu (EHS) č. 3821/85 v znení posledných zmien. Stále sa však vyžaduje súhlas vodiča v prípade vysielania osobných údajov.

3.21 **režim kalibrácie**

202) Kalibračná funkcia musí umožniť:

— automatické spárovanie snímača pohybu s VU,

— v prípade potreby automatické spojenie externého zariadenia GNSS s VU,

— digitálne prispôsobenie konštanty záznamového zariadenia (k) charakteristickému koeficientu vozidla (w),

— úpravu aktuálneho času v rámci platnosti vloženej dielenskej karty,

— úpravu aktuálneho stavu počítadla kilometrov,

— aktualizáciu identifikačných údajov snímača pohybu, ktoré sú uložené v dátovej pamäti,

— v prípade potreby aktualizáciu identifikačných údajov externého zariadenia GNSS, ktoré sú uložené v dátovej pamäti,

— aktualizáciu druhov a identifikátorov všetkých používaných plomb,

— aktualizáciu alebo potvrdenie ostatných parametrov, ktoré pozná záznamové zariadenie: identifikácia vozidla, w, l, rozmer pneumatík a prípadne nastavenie obmedzovača rýchlosti.

203) Okrem toho musí kalibračná funkcia umožniť zrušenie používania tachografových kariet prvej generácie v záznamovom zariadení, pokiaľ sú splnené podmienky stanovené v dodatku 15.

204) Spárovanie snímača pohybu s VU pozostáva minimálne z:

— aktualizácie údajov o montáži snímača pohybu uchovávaných snímačom pohybu (ak je to potrebné),

— kopírovania nevyhnutných identifikačných údajov snímača pohybu zo snímača pohybu do dátovej pamäte VU.

205) Spojenie externého zariadenia GNSS s VU pozostáva minimálne z:

— aktualizácie údajov o montáži externého zariadenia GNSS, ktoré sú uchovávané v externom zariadení GNSS (v prípade potreby),

— kopírovania potrebných identifikačných údajov externého zariadenia GNSS vrátane sériového čísla externého zariadenia GNSS z externého zariadenia GNSS do dátovej pamäte VU,

Po spojení nasleduje overenie informácie o polohe z GNSS.

206) Kalibračná funkcia musí byť schopná zaviesť nevyhnutné údaje cez kalibračný/sťahovací konektor v súlade s kalibračným protokolom vymedzeným v dodatku 8. Kalibračná funkcia môže zavádzať nevyhnutné údaje aj inými prostriedkami.

3.22 **Kontrola kalibrácie pri cestnej kontrole**

207) Funkcia kontroly kalibrácie pri cestnej kontrole musí v čase žiadosti umožniť čítanie sériového čísla snímača pohybu (prípadne zabudovaného do adaptéra) a sériového čísla externého zariadenia GNSS (v prípade potreby), pripojených k jednotke vozidla.

208) Tento údaj sa musí dať zobraziť aspoň na displeji jednotky vozidla príkazmi v menu.

209) Funkcia kontroly kalibrácie pri cestnej kontrole musí umožniť kontrolu voľby I/O režimu kalibračného vstupného/výstupného signalizačného vedenia uvedeného v dodatku 6 cez rozhranie K-vedenia. To sa musí vykonať prostredníctvom ECUAdjustmentSession, ako sa uvádza v dodatku 8 oddiele 7 Riadenie skúšobných impulzov – Riadenie vstupu/výstupu funkčnej jednotky.

3.23 **Úprava času**

210) Funkcia úpravy času musí umožniť automatickú úpravu aktuálneho času. Pre úpravu času sa používajú v záznamovom zariadení dva zdroje času: 1) vstavané hodiny VU, 2) prijímač GNSS.

211) Nastavenie času vstavaných hodín VU musí byť automaticky opätovne upravené v intervaloch maximálne 12 hodín. Ak tento čas uplynul a signál GNSS nie je k dispozícii, nastavenie času sa musí vykonať akonáhle VU má prístup k platnému času poskytnutému prijímačom GNSS, podľa podmienok týkajúcich sa zapaľovania vozidla. Referenčný čas pre automatické nastavenie času vstavaných hodín VU musí byť odvodený z prijímača GNSS. Udalosť časového konfliktu sa spustí, ak sa aktuálny čas líši o viac ako jednu (1) minútu od časových informácií poskytnutých prijímačom GNSS.

212) Funkcia úpravy času musí v režime kalibrácie umožniť vyvolanú úpravu aktuálneho času.

3.24 **Výkonnostné charakteristiky**

213) Jednotka vozidla musí byť plne funkčná v rozsahu teplôt od – 20 °C do 70 °C, externé zariadenie GNSS v rozsahu teplôt od – 20 °C do 70 °C a snímač pohybu v rozsahu teplôt od – 40 °C do 135 ° C. Obsah dátovej pamäte sa musí uchovať pri teplote do – 40 °C.

214) Tachograf musí byť plne funkčný v rozsahu vlhkosti od 10 % do 90 %.

215) Plomby použité v inteligentnom tachografe musia zniesť rovnaké podmienky ako tie, ktoré sa uplatňujú na komponenty tachografu, ku ktorým sú pripevnené.

216) Záznamové zariadenie musí byť chránené proti prepätiu, zmene polarity napájania a skratom.

217) Snímače pohybu musia buď:

— reagovať na magnetické pole, ktoré ruší zisťovanie pohybu vozidla. Za takýchto okolností jednotka vozidla zaznamená a uloží poruchu snímača (požiadavka 88); alebo

— musia mať snímací prvok, ktorý je chránený pred magnetickými poľami alebo je voči nim odolný.

218) Záznamové zariadenie a externé zariadenie GNSS musí zodpovedať medzinárodnému predpisu EHK OSN R10 a musí byť chránené proti elektrostatickým výbojom a prechodovým javom.

3.25 **Materiály**

219) Všetky konštrukčné časti záznamového zariadenia musia byť vyrobené z materiálov s dostatočnou stabilitou a mechanickou pevnosťou a so stálymi elektrickými a magnetickými charakteristikami.

220) Na zaručenie normálnych podmienok prevádzky musia byť všetky vnútorné diely zariadenia chránené proti vlhkosti a prachu.

221) Jednotka vozidla a externé zariadenie GNSS musia spĺňať stupeň ochrany IP 40 a snímač pohybu musí spĺňať stupeň ochrany IP 64 podľa normy IEC 60529:1989 vrátane A1:1999 a A2:2013.

222) Záznamové zariadenie musí zodpovedať platným technickým požiadavkám ergonomického dizajnu.

223) Záznamové zariadenie musí byť chránené proti neúmyselnému poškodeniu.

3.26 **Označenia**

224) Ak záznamové zariadenie zobrazuje stav počítadla kilometrov a rýchlosť, na displeji sa musia zobraziť tieto údaje:

— vedľa čísla udávajúceho vzdialenosť, jednotka merania vzdialenosti označená skratkou „km“,

— vedľa čísla udávajúceho rýchlosť, skratka „km/h“.

Záznamové zariadenie sa môže prepnúť tak, aby zobrazovalo rýchlosť v míľach za hodinu; v tomto prípade sa ako jednotka merania rýchlosti zobrazí skratka „mph“. Záznamové zariadenie sa môže prepnúť tak, aby zobrazovalo vzdialenosť v míľach; v tomto prípade sa ako jednotka merania vzdialenosti zobrazí skratka „mi“.

225) Na každý samostatný komponent záznamového zariadenia musí byť pripevnený popisný štítok s týmito údajmi:

— názov a adresa výrobcu zariadenia,

— číslo dielu zariadenia a rok výroby zariadenia,

— sériové číslo zariadenia,

— schvaľovacia značka typu zariadenia.

226) Ak nie je dostatok miesta pre všetky vyššie uvedené údaje, popisný štítok musí udávať aspoň: názov alebo logo výrobcu a číslo dielu zariadenia.

4 KONŠTRUKČNÉ A FUNKČNÉ POŽIADAVKY NA TACHOGRAFOVÉ KARTY

4.1 **Viditeľné údaje**

Predná strana musí obsahovať:

227) slová „karta vodiča“ alebo „kontrolná karta“ alebo „dielenská karta“ alebo „podniková karta“, vytlačené veľkými písmenami v úradnom jazyku alebo jazykoch členského štátu, ktorý kartu vydal, podľa typu karty;

228) názov členského štátu, ktorý kartu vydal (nepovinné);

229) negatív rozlišovacieho znaku členského štátu, ktorý kartu vydal, v modrom obdĺžniku a obkolesený 12 žltými hviezdičkami. Rozlišovacie znaky sú tieto:

B	Belgicko	LV	Lotyšsko
BG	Bulharsko	L	Luxembursko
CZ	Česká republika	LT	Litva
CY	Cyprus	M	Malta
DK	Dánsko	NL	Holandsko

D EST	Nemecko Estónsko	A PL	Rakúsko Poľsko
GR	Grécko	P RO SK SLO	Portugalsko Rumunsko Slovensko Slovinsko
E	Španielsko	FIN	Fínsko
F HR H	Francúzsko Chorvátsko Maďarsko	S	Švédsko
IRL	Írsko	UK	Spojené kráľovstvo
I	Taliansko		

230) informácie špecifické pre vydanú kartu, očíslované takto:

	Karta vodiča	Kontrolná karta	Podniková alebo dielenská karta
1.	Priezvisko vodiča	Názov kontrolného orgánu	Názov podniku alebo dielne
2.	Meno(á) vodiča	Priezvisko kontrolóra (v prípade potreby)	priezvisko držiteľa karty (v prípade potreby)
3.	Dátum narodenia vodiča	Meno(á) kontrolóra (v prípade potreby)	meno(á) držiteľa karty (v prípade potreby)
4.a	Dátum začiatku platnosti karty		
4.b	Dátum skončenia platnosti karty		
4.c	Názov vydávajúceho orgánu (môže byť vytlačený na zadnej strane)		
4.d	iné číslo, než je číslo v bode 5, na administratívne účely (nepovinné)		
5. a	Číslo vodičského preukazu (k dátumu vydania karty vodiča)	—	—
5. b	Číslo karty		
6.	Fotografia vodiča	Fotografia kontrolóra (nepovinné)	Fotografia montéra (nepovinné)

	Karta vodiča	Kontrolná karta	Podniková alebo dielenská karta
7.	Podpis držiteľa (nepovinné)		
8.	bydlisko alebo poštová adresa držiteľa (nepovinné).	Poštová adresa kontrolného orgánu	Poštová adresa podniku alebo dielne

231) forma písania dátumu je „dd/mm/rrrr“ alebo „dd.mm.rrrr“ (deň, mesiac, rok).

zadná strana musí obsahovať:

232) vysvetlenie k očíslovaným údajom na prednej strane karty;

233) s výslovným písomným súhlasom držiteľa môžu byť doplnené aj informácie, ktoré sa netýkajú administratívnych záležitosti súvisiacich s kartou; takéto doplnenie nijako nemení používanie modelu ako tachografovej karty.

234) Tachografové karty musia byť vytlačené s týmito prevažujúcimi farbami pozadia:

— karta vodiča: biela,

— kontrolná karta: modrá,

— dielenská karta: červená,

— podniková karta: žltá.

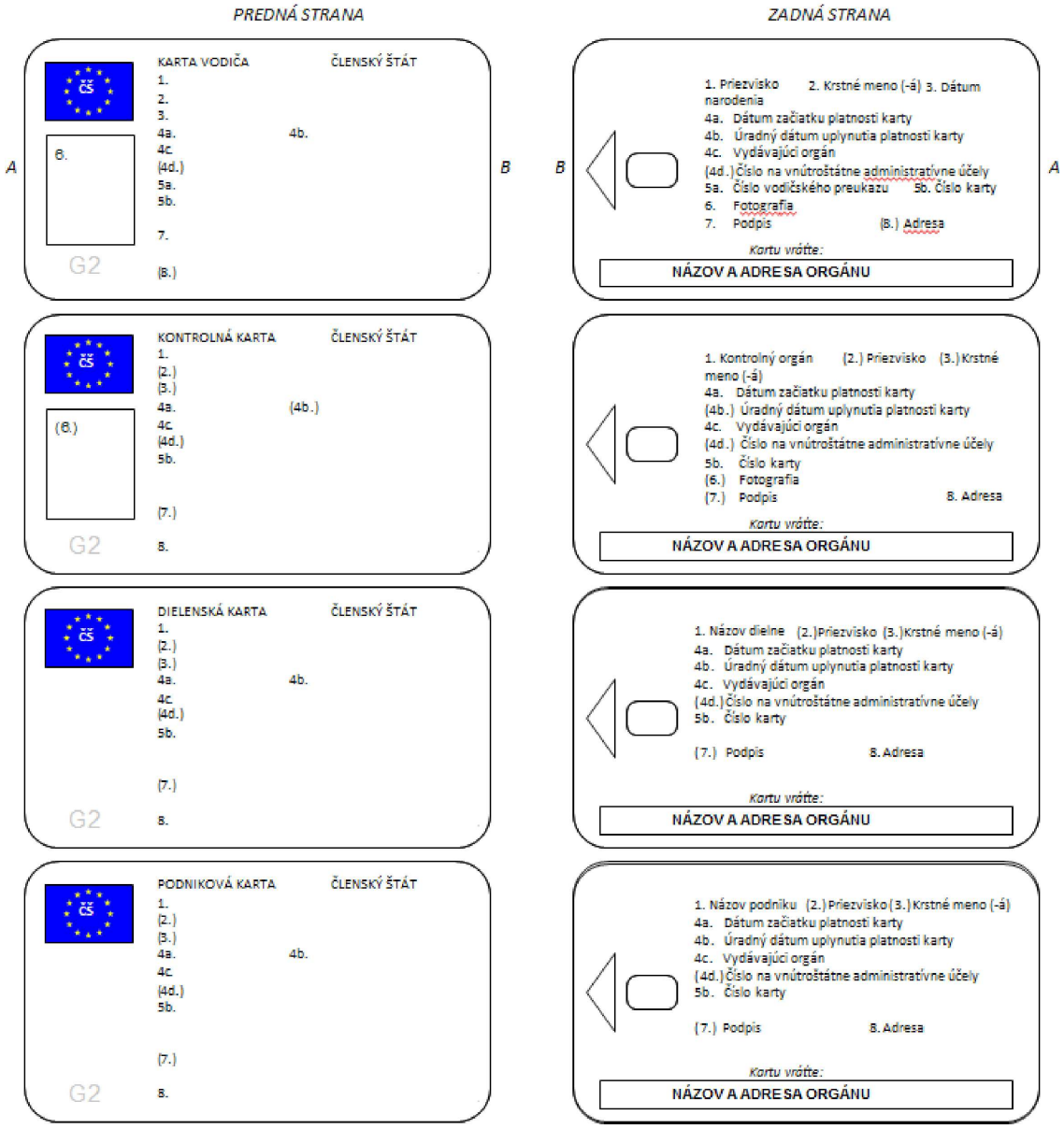
235) Telo tachografovej karty musí byť vybavené aspoň týmito ochrannými prvkami proti falšovaniu alebo neoprávneným zásahom:

— ochranná podtlač s gilošovaným vzorom a írisovou tlačou.

— v oblasti fotografie sa ochranná podtlač musí prekrývať s fotografiou.

— aspoň jeden dvojfarebný mikrotlačový prúžok.

VZOR TACHOGRAFOVÝCH KARIET SPOLOČENSTVA



236) Po konzultácii s Komisiou môžu členské štáty doplniť farby alebo značenia, ako sú symboly členského štátu a prvky zabezpečenia bez toho, aby tým boli dotknuté ostatné ustanovenia tejto prílohy.

237) Dočasné karty uvedené v článku 26 ods. 4 nariadenia (EÚ) č. 165/2014 musia byť v súlade s ustanoveniami tejto prílohy.

4.2 Zabezpečenie

Cieľom zabezpečenia systému je ochrana integrity a autenticity údajov vymieňaných medzi kartami a záznamovým zariadením, ochrana integrity a autenticity údajov sťahovaných z kariet, umožnenie určitých zapisovacích operácií na karte len pre záznamové zariadenie, dešifrovanie určitých údajov, vylúčenie akejkoľvek možnosti falšovania údajov uložených na kartách, zabránenie neoprávnenému zásahu a zistenie každého pokusu tohto druhu.

238) S cieľom dosiahnuť zabezpečenie systému musia tachografové karty spĺňať požiadavky zabezpečenia vymedzené v dodatkoch 10 a 11.

239) Tachografové karty musia byť čitateľné inými zariadeniami, ako sú napríklad osobné počítače.

4.3 **Normy**

240) Tachografové karty musia byť v súlade s týmito normami:

— ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti,

— ISO/IEC 7816 Identifikačné karty. Karty s integrovanými obvodmi:

— Časť 1: Fyzikálne vlastnosti,

— Časť 2: Rozmery a umiestnenie kontaktov (ISO/IEC 7816-2: 2007),

— Časť 3: Elektronické signály a prenosové protokoly (ISO/IEC 7816-3: 2006),

— Časť 4: Organizácia, zabezpečenie a príkazy pre výmenu (ISO/IEC 7816-4: 2013 + Cor. 1: 2014),

— Časť 6: Medziodborové dátové prvky pre výmenu (ISO/IEC 7816-6: 2004 + Cor. 1: 2006),

— Časť 8: Príkazy pre operácie zabezpečenia (ISO/IEC 7816-8: 2004).

— Tachografové karty musia byť skúšané v súlade s normou ISO/IEC 10373-3: 2010 Identifikačné karty. Skúšobné metódy. Časť 3: Karty s integrovanými obvodmi a s kontaktmi a súvisiace zariadenia s rozhraním.

4.4 **Elektrické špecifikácie a špecifikácie prostredia**

241) Tachografové karty si musia zachovať správnu funkčnosť za všetkých klimatických podmienok bežných na území Spoločenstva a minimálne v rozsahu teplôt od – 25 °C do + 70 °C s príležitostnou špičkou do + 85 °C, pričom „príležitostná“ znamená jednorazovo maximálne 4 hodiny a maximálne 100 krát v priebehu životnosti karty.

242) Tachografové karty musia správne fungovať v rozsahu vlhkosti od 10 % do 90 %.

243) Tachografové karty si musia zachovať správnu funkčnosť päť rokov, ak sa používajú v súlade so špecifikáciami prostredia a elektrickými špecifikáciami.

244) Počas prevádzky musia tachografové karty zodpovedať predpisu EHK R10, týkajúcemu sa elektromagnetickej kompatibility, a musia byť chránené proti elektrostatickým výbojom.

4.5 **Uchovávanie údajov**

Na účely tohto odseku,

— časy sa zaznamenávajú s presnosťou jednej minúty, pokiaľ nie je špecifikované inak,

— stav počítadla kilometrov sa zaznamenáva s presnosťou jedného kilometra,

— rýchlosť sa zaznamenáva s presnosťou 1 km/h,

— polohy (zemepisná šírka a dĺžka) sa zaznamenávajú v stupňoch a minútach s rozlíšením 1/10 minúty.

Funkcie tachografových kariet, príkazy a logické štruktúry, ktoré slúžia na splnenie požiadaviek na uloženie údajov, sú špecifikované v dodatku 2.

Ak nie je uvedené inak, ukladanie údajov na tachografových kartách musí byť organizované tak, že nové údaje nahradia uložené najstaršie údaje v prípade, že predpokladaná veľkosť pamäte pre osobitné záznamy je vyčerpaná.

245) Tento odsek špecifikuje minimálnu úložnú kapacitu pre dátové súbory rôznych aplikácií. Tachografové karty musia byť schopné poskytnúť záznamovému zariadeniu informácie o skutočnej úložnej kapacite týchto dátových súborov.

246) Akékoľvek doplnkové údaje, ktoré môžu byť uložené na tachografových kartách, týkajúce sa iných aplikácií, ktoré môžu byť na karte, musia byť uložené v súlade so smernicou 95/46/ES a smernicou 2002/58/ES a v súlade s článkom 7 nariadenia (EÚ) č. 165/2014.

247) Každý hlavný súbor (MF) každej tachografovej karty musí obsahovať najviac päť elementárnych súborov (EF) na riadenie karty, identifikáciu aplikácie a čipu, a dva vyhradené súbory (DF):

— DF Tachograph, ktorý obsahuje aplikáciu prístupnú jednotkám vozidla prvej generácie, ktorá je prítomná aj v tachografových kartách prvej generácie,

— DF Tachograph_G2, ktorý obsahuje aplikáciu prístupnú len jednotkám vozidla druhej generácie, ktorá je prítomná len v tachografových kartách druhej generácie.

Všetky podrobnosti štruktúry tachografovej karty sú špecifikované v dodatku 2.

4.5.1 *Elementárne súbory na identifikáciu a riadenie karty*

4.5.2 *Identifikácia karty s integrovaným obvodom (IC)*

248) Tachografové karty musia byť schopné uložiť tieto identifikačné údaje inteligentnej karty:

— zastavenie času,

— sériové číslo karty (vrátane výrobných údajov),

— číslo typového schválenia karty,

— identifikácia personalizátora karty (ID),

— ID zostavovateľa,

— identifikátor IC.

4.5.2.1 Identifikácia čipu

249) Tachografové karty musia byť schopné uložiť tieto identifikačné údaje týkajúce sa integrovaného obvodu (IC):

— sériové číslo IC,

— výrobné informácie IC.

4.5.2.2 DIR (len v tachografových kartách druhej generácie)

250) Tachografové karty musia byť schopné uložiť dátové objekty na identifikáciu aplikácie uvedené v dodatku 2.

4.5.2.3 Informácie ATR (podmienené, len v tachografových kartách druhej generácie)

251) Tachografové karty musia byť schopné uložiť tento dátový objekt s informáciou o rozšírenej dĺžke:

— ak tachografová karta podporuje rozšírenú dĺžku polí, dátový objekt s informáciou o rozšírenej dĺžke uvedený v dodatku 2.

4.5.2.4 Informácie o rozšírenej dĺžke (podmienené, len v tachografových kartách druhej generácie)

252) Tachografové karty musia byť schopné uložiť tieto dátové objekty s informáciami o rozšírenej dĺžke:

— ak tachografová karta podporuje rozšírenú dĺžku polí, dátový objekt s informáciami o rozšírenej dĺžke uvedený v dodatku 2.

4.5.3 *Karta vodiča*

4.5.3.1 Aplikácia tachografu (prístupné pre jednotky vozidla prvej a druhej generácie)

4.5.3.1.1 Identifikácia aplikácie

253) Karta vodiča musí byť schopná uložiť tieto identifikačné údaje o aplikácii:

— identifikácia aplikácie tachografu,

— identifikácia typu tachografovej karty.

4.5.3.1.2 Kľúč a certifikáty

254) Karta vodiča musí byť schopná uložiť niekoľko šifrovacích kľúčov a certifikátov, ako je uvedené v dodatku 11 časti A.

4.5.3.1.3 Identifikácia karty

255) Karta vodiča musí byť schopná uložiť tieto identifikačné údaje karty:

— číslo karty,

— vydávajúci členský štát, názov vydávajúceho orgánu, dátum vydania,

— dátum začiatku platnosti karty, dátum skončenia platnosti karty.

4.5.3.1.4 Identifikácia držiteľa karty

256) Karta vodiča musí byť schopná uložiť tieto identifikačné údaje držiteľa karty:

— priezvisko držiteľa,

— meno(á) držiteľa,

— dátum narodenia,

— preferovaný jazyk.

4.5.3.1.5 Sťahovanie údajov z karty

257) Karta vodiča musí byť schopná uložiť tieto údaje týkajúce sa sťahovania z karty:

— Dátum a čas posledného sťahovania z karty (na iné účely, než je kontrola).

258) Karta vodiča musí byť schopná uchovať jeden taký záznam.

4.5.3.1.6 Informácie o vodičskom preukaze

259) Karta vodiča musí byť schopná uložiť tieto údaje o vodičskom preukaze:

— vydávajúci členský štát, názov vydávajúceho orgánu,

— číslo vodičského preukazu (k dátumu vydania karty).

4.5.3.1.7 Údaje o udalostiach

Na účely tohto pododseku sa čas musí uložiť s presnosťou jednej sekundy.

260) Karta vodiča musí byť schopná uložiť údaje týkajúce sa týchto udalostí zistených záznamovým zariadením, zatiaľ čo bola karta vložená:

— prekrývanie časov (keď je táto karta príčinou udalosti),

— vloženie karty za jazdy (keď je táto karta predmetom udalosti),

— nesprávne uzavretá posledná relácia karty (keď je táto karta predmetom udalosti),

— prerušenie napájania,

— chyba údajov o pohybe,

— pokusy o narušenie zabezpečenia.

261) Karta vodiča musí byť pri daných udalostiach schopná uložiť tieto údaje:

— kód udalosti,

— dátum a čas začiatku udalosti (alebo vloženia karty, ak udalosť v danom čase trvala),

— dátum a čas skončenia udalosti (alebo vybratia karty, ak udalosť v danom čase trvala),

— evidenčné číslo vozidla a členský štát evidencie vozidla, v ktorom udalosť nastala.

Poznámka: pre udalosť „prekrývanie časov“:

— dátum a čas začiatku udalosti musí zodpovedať dátumu a času vytiahnutia karty z prechádzajúceho vozidla,

— dátum a čas skončenia udalosti musí zodpovedať dátumu a času vloženia karty do súčasného vozidla,

— údaje o vozidle musia zodpovedať súčasnému vozidlu, kde udalosť nastala.

Poznámka: pre udalosť „nesprávne uzavretá posledná relácia karty“:

— dátum a čas začiatku udalosti musí zodpovedať dátumu a času vloženia karty pri nesprávne uzavretej poslednej relácii karty,

— dátum a čas skončenia udalosti musí zodpovedať dátumu a času vloženia karty pri relácii, počas ktorej bola udalosť zistená (súčasná relácia),

— údaje o vozidle musia zodpovedať vozidlu, v ktorom bola relácia nesprávne uzavretá.

262) Karta vodiča musí byť schopná uložiť údaje o šiestich posledných udalostiach každého typu (t. j. 36 udalostí).

4.5.3.1.8 Údaje o poruchách

Na účely tohto pododseku sa čas musí zaznamenať s presnosťou jednej sekundy.

263) Karta vodiča musí byť schopná uložiť údaje týkajúce sa týchto porúch zistených záznamovým zariadením, zatiaľ čo bola karta vložená:

— porucha karty (keď je táto karta predmetom udalosti),

— porucha záznamového zariadenia.

264) Karta vodiča musí byť schopná pri daných poruchách uložiť tieto údaje:

— kód poruchy,

— dátum a čas začiatku poruchy (alebo vloženia karty, ak porucha v danom čase trvala),

— dátum a čas skončenia poruchy (alebo vybratia karty, ak porucha v danom čase trvala),

— evidenčné číslo vozidla a členský štát evidencie vozidla, v ktorom porucha nastala.

265) Karta vodiča musí byť schopná uložiť údaje o dvanástich posledných poruchách každého typu (t. j. 24 porúch).

4.5.3.1.9 Údaje o činnosti vodiča

266) Karta vodiča musí byť schopná uložiť za každý kalendárny deň používania karty alebo deň, za ktorý vodič manuálne zapísal činnosti, tieto údaje:

— dátum,

— počítadlo dennej prítomnosti (zvýšené o jeden za každý z týchto kalendárnych dní),

— celkovú vzdialenosť prejdenú vodičom počas tohto dňa,

— stav vodiča o 00.00 hod.,

— vždy, keď vodič zmenil činnosť a/alebo zmenil stav vedenia vozidla, a/alebo vložil alebo vybral svoju kartu:

— stav vedenia vozidla (POSÁDKA, JEDEN VODIČ),

— slot (VODIČ, DRUHÝ VODIČ),

— stav karty (VLOŽENÁ, NEVLOŽENÁ),

— činnosť (JAZDA, POHOTOVOSŤ, PRÁCA, PRESTÁVKA/ODPOČINOK).

— čas zmeny.

267) Pamäť karty vodiča musí byť schopná uchovať údaje o činnosti vodiča aspoň 28 dní (priemerná činnosť vodiča je definovaná ako 93 zmien činnosti za deň).

268) Údaje uvedené v požiadavkách 261, 264 a 266 musia byť uložené spôsobom, ktorý umožní vyvolať činnosti v poradí, v akom nastali, dokonca aj v prípade prekrývania časov.

4.5.3.1.10 Údaje o použitých vozidlách

269) Karta vodiča musí byť schopná uložiť za každý kalendárny deň používania karty a za každý časový úsek používania daného vozidla v uvedenom dni (časový úsek používania zahŕňa všetky po sebe idúce cykly vloženia/vytiahnutia karty vo vozidle, z hľadiska tejto karty), tieto údaje:

— dátum a čas prvého použitia vozidla (t. j. prvé vloženie karty v tomto časovom úseku použitia vozidla, alebo 00.00, ak časový úsek používania v uvedenom čase trvá),

— stav počítadla kilometrov v uvedenom čase,

— dátum a čas posledného použitia vozidla (t. j. posledné vytiahnutie karty v tomto časovom úseku použitia vozidla, alebo 23.59, ak časový úsek používania v uvedenom čase trvá),

— stav počítadla kilometrov v uvedenom čase,

— evidenčné číslo vozidla a členský štát evidencie vozidla.

270) Karta vodiča musí byť schopná uložiť aspoň 84 takých záznamov.

4.5.3.1.11 Miesta, kde sa denný pracovný čas začína a/alebo končí

271) Karta vodiča musí byť schopná uložiť tieto údaje týkajúce sa miest, kde sa denný pracovný čas začína a/alebo končí, zapísané vodičom:

— dátum a čas zápisu (alebo dátum/čas týkajúci sa zápisu, ak sa zápis vykoná počas postupu manuálneho zápisu),

— typ zápisu (začiatok alebo koniec, podmienky zápisu),

— zapísaný štát alebo región,

— stav počítadla kilometrov.

272) Pamäť karty vodiča musí byť schopná uchovať aspoň 42 párov takých záznamov.

4.5.3.1.12 Údaje o relácii karty

273) Karta vodiča musí byť schopná uložiť údaje týkajúce sa vozidla, v ktorom bola otvorená prebiehajúca relácia:

— dátum a čas otvorenia relácie (t. j. vloženie karty) s presnosťou jednej sekundy,

— evidenčné číslo vozidla a členský štát evidencie.

4.5.3.1.13 Údaje o kontrolnej činnosti

274) Karta vodiča musí byť schopná uložiť tieto údaje týkajúce sa kontrolných činností:

— dátum a čas kontroly,

— číslo kontrolnej karty a jej vydávajúci členský štát,

— druh kontroly (zobrazovanie a/alebo tlač a/alebo sťahovanie z jednotky vozidla a/alebo sťahovanie z karty (pozri poznámku)),

— stiahnutý časový úsek, v prípade sťahovania,

— evidenčné číslo vozidla a členský štát evidencie vozidla, v ktorom sa kontrola uskutočnila.

Poznámka: sťahovanie z karty sa zaznamená len vtedy, keď sa vykonáva cez záznamové zariadenie.

275) Karta vodiča musí byť schopná uchovať jeden taký záznam.

4.5.3.1.14 Údaje o špecifických podmienkach

276) Karta vodiča musí byť schopná uložiť tieto údaje týkajúce sa špecifických podmienok zapísaných, zatiaľ čo bola karta vložená (bez ohľadu na slot):

— dátum a čas zápisu,

— druh špecifickej podmienky.

277) Karta vodiča musí byť schopná uložiť aspoň 56 takých záznamov.

4.5.3.2 Aplikácia tachografu druhej generácie (neprístupné jednotke vozidla prvej generácie)

4.5.3.2.1 Identifikácia aplikácie

278) Karta vodiča musí byť schopná uložiť tieto identifikačné údaje o aplikácii:

— identifikácia aplikácie tachografu,

— identifikácia typu tachografovej karty.

4.5.3.2.2 Kľúče a certifikáty

279) Karta vodiča musí byť schopná uložiť niekoľko šifrovacích kľúčov a certifikátov, ako je uvedené v dodatku 11 časti B.

4.5.3.2.3 Identifikácia karty

280) Karta vodiča musí byť schopná uložiť tieto identifikačné údaje karty:

— číslo karty,

— vydávajúci členský štát, názov vydávajúceho orgánu, dátum vydania,

— dátum začiatku platnosti karty, dátum skončenia platnosti karty.

4.5.3.2.4 Identifikácia držiteľa karty

281) Karta vodiča musí byť schopná uložiť tieto identifikačné údaje držiteľa karty:

— priezvisko držiteľa,

— meno(á) držiteľa,

— dátum narodenia,

— preferovaný jazyk.

4.5.3.2.5 Sťahovanie údajov z karty

282) Karta vodiča musí byť schopná uložiť tieto údaje týkajúce sa sťahovania z karty:

— Dátum a čas posledného sťahovania z karty (na iné účely, než je kontrola).

283) Karta vodiča musí byť schopná uchovať jeden taký záznam.

4.5.3.2.6 Informácie o vodičskom preukaze

284) Karta vodiča musí byť schopná uložiť tieto údaje o vodičskom preukaze:

— vydávajúci členský štát, názov vydávajúceho orgánu,

— číslo vodičského preukazu (k dátumu vydania karty).

4.5.3.2.7 Údaje o udalostiach

Na účely tohto pododseku sa čas musí uložiť s presnosťou jednej sekundy.

285) Karta vodiča musí byť schopná uložiť údaje týkajúce sa týchto udalostí zistených záznamovým zariadením, zatiaľ čo bola karta vložená:

— prekrývanie časov (keď je táto karta príčinou udalosti),

— vloženie karty za jazdy (keď je táto karta predmetom udalosti),

— nesprávne uzavretá posledná relácia karty (keď je táto karta predmetom udalosti),

— prerušenie napájania,

— chyba komunikácie s diaľkovým komunikačným zariadením,

— udalosť „chýbajúce informácie o polohe z prijímača GNSS“,

— chyba komunikácie s externým zariadením GNSS

— chyba údajov o pohybe,

— nesúlad údajov o pohybe vozidla,

— pokusy o narušenie zabezpečenia,

— časový konflikt.

286) Karta vodiča musí byť pri daných udalostiach schopná uložiť tieto údaje:

— kód udalosti,

— dátum a čas začiatku udalosti (alebo vloženia karty, ak udalosť v danom čase trvala),

— dátum a čas skončenia udalosti (alebo vybratia karty, ak udalosť v danom čase trvala),

— evidenčné číslo vozidla a členský štát evidencie vozidla, v ktorom udalosť nastala.

Poznámka: pre udalosť „prekrývanie časov“:

— dátum a čas začiatku udalosti musí zodpovedať dátumu a času vytiahnutia karty z prechádzajúceho vozidla,

— dátum a čas skončenia udalosti musí zodpovedať dátumu a času vloženia karty do súčasného vozidla,

— údaje o vozidle musia zodpovedať súčasnému vozidlu, kde udalosť nastala.

Poznámka: pre udalosť „nesprávne uzavretá posledná relácia karty“:

— dátum a čas začiatku udalosti musí zodpovedať dátumu a času vloženia karty pri nesprávne uzavretej poslednej relácii karty,

— dátum a čas skončenia udalosti musí zodpovedať dátumu a času vloženia karty pri relácii, počas ktorej bola udalosť zistená (súčasná relácia),

— údaje o vozidle musia zodpovedať vozidlu, v ktorom bola relácia nesprávne uzavretá.

287) Karta vodiča musí byť schopná uložiť údaje o šiestich posledných udalostiach každého typu (t. j. 66 udalostí).

4.5.3.2.8 Údaje o poruchách

Na účely tohto pododseku sa čas musí zaznamenať s presnosťou jednej sekundy.

288) Karta vodiča musí byť schopná uložiť údaje týkajúce sa týchto porúch zistených záznamovým zariadením, zatiaľ čo bola karta vložená:

— porucha karty (keď je táto karta predmetom udalosti),

— porucha záznamového zariadenia.

289) Karta vodiča musí byť schopná pri daných poruchách uložiť tieto údaje:

— kód poruchy,

— dátum a čas začiatku poruchy (alebo vloženia karty, ak porucha v danom čase trvala),

— dátum a čas skončenia poruchy (alebo vybratia karty, ak porucha v danom čase trvala),

— evidenčné číslo vozidla a členský štát evidencie vozidla, v ktorom porucha nastala.

290) Karta vodiča musí byť schopná uložiť údaje o dvanástich posledných poruchách každého typu (t. j. 24 porúch).

4.5.3.2.9 Údaje o činnosti vodiča

291) Karta vodiča musí byť schopná uložiť za každý kalendárny deň používania karty alebo deň, za ktorý vodič manuálne zapísal činnosti, tieto údaje:

— dátum,

— počítadlo dennej prítomnosti (zvýšené o jeden za každý z týchto kalendárnych dní),

— celkovú vzdialenosť prejdenú vodičom počas tohto dňa,

— stav vodiča o 00.00 hod.,

— vždy, keď vodič zmenil činnosť a/alebo zmenil stav vedenia vozidla, a/alebo vložil alebo vybral svoju kartu:

— stav vedenia vozidla (POSÁDKA, JEDEN VODIČ)

— slot (VODIČ, DRUHÝ VODIČ),

— stav karty (VLOŽENÁ, NEVLOŽENÁ),

— činnosť (VEDENIE, POHOTOVOSŤ, PRÁCA, PRESTÁVKA/ODPOČINOK).

— čas zmeny.

292) Pamäť karty vodiča musí byť schopná uchovať údaje o činnosti vodiča aspoň 28 dní (priemerná činnosť vodiča je definovaná ako 93 zmien činnosti za deň).

293) Údaje uvedené v požiadavkách 286, 289 a 291 musia byť uložené spôsobom, ktorý umožní vyvolať činnosti v poradí, v akom nastali, dokonca aj v prípade prekrývania časov.

4.5.3.2.10 Údaje o použitých vozidlách

294) Karta vodiča musí byť schopná uložiť za každý kalendárny deň používania karty a za každý časový úsek používania daného vozidla v uvedenom dni (časový úsek používania zahŕňa všetky po sebe idúce cykly vloženia/vytiahnutia karty vo vozidle, z hľadiska tejto karty), tieto údaje:

— dátum a čas prvého použitia vozidla (t. j. prvé vloženie karty v tomto časovom úseku použitia vozidla, alebo 00.00, ak časový úsek používania v uvedenom čase trvá),

— stav počítadla kilometrov v čase prvého použitia,

— dátum a čas posledného použitia vozidla (t. j. posledné vytiahnutie karty v tomto časovom úseku použitia vozidla, alebo 23.59, ak časový úsek používania v uvedenom čase trvá),

— stav počítadla kilometrov v čase posledného použitia,

— evidenčné číslo vozidla a členský štát evidencie vozidla,

— VIN vozidla.

295) Karta vodiča musí byť schopná uložiť aspoň 84 takých záznamov.

4.5.3.2.11 Miesta a polohy, kde sa denný pracovný čas začína a/alebo končí

296) Karta vodiča musí byť schopná uložiť tieto údaje týkajúce sa miest, kde sa denný pracovný čas začína a/alebo končí, zapísané vodičom:

— dátum a čas zápisu (alebo dátum/čas týkajúci sa zápisu, ak sa zápis vykoná počas postupu manuálneho zápisu),

— typ zápisu (začiatok alebo koniec, podmienky zápisu),

— zapísaný štát alebo región,

— stav počítadla kilometrov,

— poloha vozidla,

— presnosť GNSS, dátum a čas, keď bola poloha určená.

297) Pamäť karty vodiča musí byť schopná uchovať aspoň 84 párov takých záznamov.

4.5.3.2.12 Údaje o relácii karty

298) Karta vodiča musí byť schopná uložiť údaje týkajúce sa vozidla, v ktorom bola otvorená prebiehajúca relácia:

— dátum a čas otvorenia relácie (t. j. vloženie karty) s presnosťou jednej sekundy,

— evidenčné číslo vozidla a členský štát evidencie.

4.5.3.2.13 Údaje o kontrolnej činnosti

299) Karta vodiča musí byť schopná uložiť tieto údaje týkajúce sa kontrolných činností:

— dátum a čas kontroly,

— číslo kontrolnej karty a jej vydávajúci členský štát,

— druh kontroly (zobrazovanie a/alebo tlač a/alebo sťahovanie z jednotky vozidla a/alebo sťahovanie z karty (pozri poznámku)),

— stiahnutý časový úsek, v prípade sťahovania,

— evidenčné číslo vozidla a členský štát evidencie vozidla, v ktorom sa kontrola uskutočnila.

Poznámka: Z požiadaviek na zabezpečenie vyplýva, že sťahovanie z karty sa zaznamená len vtedy, keď sa vykonáva cez záznamové zariadenie.

300) Karta vodiča musí byť schopná uchovať jeden taký záznam.

4.5.3.2.14 Údaje o špecifických podmienkach

301) Karta vodiča musí byť schopná uložiť tieto údaje týkajúce sa špecifických podmienok zapísaných, zatiaľ čo bola karta vložená (bez ohľadu na slot):

— dátum a čas zápisu,

— druh špecifickej podmienky.

302) Karta vodiča musí byť schopná uložiť aspoň 56 takých záznamov.

4.5.3.2.15 Údaje o použitých jednotkách vozidla

303) Karta vodiča zariadenie musí byť schopná uložiť tieto údaje týkajúce sa rôznych jednotiek vozidla, v ktorých bola karta použitá:

— dátum a čas začiatku časového úseku používania jednotky vozidla (t. j. prvé vloženie karty do jednotky vozidla za daný časový úsek),

— výrobca jednotky vozidla,

— typ jednotky vozidla,

— číslo verzie softvéru použitého v jednotke vozidla.

304) Karta vodiča musí byť schopná uložiť aspoň 84 takých záznamov.

4.5.3.2.16 Údaje o miestach počas troch hodín nepretržitej jazdy

305) Karta vodiča musí byť schopná uložiť tieto údaje o polohe vozidla, keď nepretržitý čas jazdy vodiča dosiahne násobok troch hodín:

— dátum a čas, keď nepretržitý čas jazdy držiteľa karty dosiahne násobok troch hodín,

— polohu vozidla,

— presnosť GNSS, dátum a čas, keď bola poloha určená.

306) Karta vodiča musí byť schopná uložiť aspoň 252 takých záznamov.

4.5.4 *Dielenská karta*

4.5.4.1 Aplikácia tachografu (prístupné pre jednotky vozidla prvej a druhej generácie)

4.5.4.1.1 Identifikácia aplikácie

307) Dielenská karta musí byť schopná uložiť tieto identifikačné údaje o aplikácii:

— identifikácia aplikácie tachografu,

— identifikácia typu tachografovej karty.

4.5.4.1.2 Kľúče a certifikáty

308) Dielenská karta musí byť schopná uložiť niekoľko šifrovacích kľúčov a certifikátov, ako je uvedené v dodatku 11 časti A.

309) Dielenská karta musí byť schopná uložiť osobné identifikačné číslo (PIN kód).

4.5.4.1.3 Identifikácia karty

310) Dielenská karta musí byť schopná uložiť tieto identifikačné údaje karty:

— číslo karty,

— vydávajúci členský štát, názov vydávajúceho orgánu, dátum vydania,

— dátum začiatku platnosti karty, dátum skončenia platnosti karty.

4.5.4.1.4 Identifikácia držiteľa karty

311) Dielenská karta musí byť schopná uložiť tieto identifikačné údaje držiteľa karty:

— názov dielne,

— adresu dielne,

— priezvisko držiteľa,

— meno(á) držiteľa,

— preferovaný jazyk.

4.5.4.1.5 Sťahovanie údajov z karty

312) Dielenská karta musí byť schopná uložiť záznamy o sťahovaní údajov z karty rovnako ako karta vodiča.

4.5.4.1.6 Údaje o kalibrácii a úprave času

313) Dielenská karta musí byť schopná uchovať záznamy o kalibrácii a/alebo úprave času, ktoré sa vykonávali, keď bola karta vložená v záznamovom zariadení.

314) Každý záznam o kalibrácii musí byť schopný uchovať tieto údaje:

— účel kalibrácie (aktivácia, prvá montáž, montáž, pravidelná inšpekcia),

— identifikácia vozidla,

— aktualizované alebo potvrdené parametre (w, k, l, rozmer pneumatík, nastavenia obmedzovača rýchlosti, počítadlo kilometrov (nové a staré hodnoty), dátum a čas (nové a staré hodnoty)),

— identifikácia záznamového zariadenia (číslo dielu VU, sériové číslo VU, sériové číslo snímača pohybu).

315) Dielenská karta musí byť schopná uložiť aspoň 88 takýchto záznamov.

316) Dielenská karta musí mať počítadlo udávajúce celkový počet kalibrácií vykonaných s kartou.

317) Dielenská karta musí mať počítadlo udávajúce počet kalibrácií vykonaných od jej posledného stiahnutia.

4.5.4.1.7 Údaje o udalostiach a poruchách

318) Dielenská karta musí byť schopná uložiť záznamy údajov o udalostiach a poruchách rovnako ako karta vodiča.

319) Dielenská karta musí byť schopná uložiť údaje o posledných troch udalostiach každého typu (t. j. 18 udalostí) a posledných šiestich poruchách každého typu (t. j. 12 porúch).

4.5.4.1.8 Údaje o činnosti vodiča

320) Dielenská karta musí byť schopná uložiť údaje o činnosti vodiča rovnako ako karta vodiča.

321) Dielenská karta musí byť schopná uchovať údaje o činnosti vodiča za aspoň jeden deň priemernej činnosti vodiča.

4.5.4.1.9 Údaje o použitých vozidlách

322) Dielenská karta musí byť schopná uložiť záznamy údajov o použitých vozidlách rovnako ako karta vodiča.

323) Dielenská karta musí byť schopná uložiť aspoň 4 takéto záznamy.

4.5.4.1.10 Údaje o začiatku a/alebo konci denného pracovného času

324) Dielenská karta musí byť schopná uložiť záznamy údajov o začiatku a/alebo konci denného pracovného času rovnako ako karta vodiča.

325) Dielenská karta musí byť schopná uchovať aspoň tri páry takých záznamov.

4.5.4.1.11 Údaje o relácii karty

326) Dielenská karta musí byť schopná uložiť záznam údajov o relácii karty rovnako ako karta vodiča.

4.5.4.1.12 Údaje o kontrolnej činnosti

327) Dielenská karta musí byť schopná uložiť záznam údajov o kontrolnej činnosti rovnako ako karta vodiča.

4.5.4.1.13 Údaje o špecifických podmienkach

328) Dielenská karta musí byť schopná uložiť údaje relevantné pre špecifické podmienky rovnako ako karta vodiča.

329) Dielenská karta musí byť schopná uložiť aspoň 2 takéto záznamy.

4.5.4.2 Aplikácia tachografu druhej generácie (neprístupné jednotke vozidla prvej generácie)

4.5.4.2.1 Identifikácia aplikácie

330) Dielenská karta musí byť schopná uložiť tieto identifikačné údaje o aplikácii:

— identifikácia aplikácie tachografu,

— identifikácia typu tachografovej karty.

4.5.4.2.2 Kľúče a certifikáty

331) Dielenská karta musí byť schopná uložiť niekoľko šifrovacích kľúčov a certifikátov, ako je uvedené v dodatku 11 časti B.

332) Dielenská karta musí byť schopná uložiť osobné identifikačné číslo (PIN kód).

4.5.4.2.3 Identifikácia karty

333) Dielenská karta musí byť schopná uložiť tieto identifikačné údaje karty:

— číslo karty,

— vydávajúci členský štát, názov vydávajúceho orgánu, dátum vydania,

— dátum začiatku platnosti karty, dátum skončenia platnosti karty.

4.5.4.2.4 Identifikácia držiteľa karty

334) Dielenská karta musí byť schopná uložiť tieto identifikačné údaje držiteľa karty:

— názov dielne,

— adresu dielne,

— priezvisko držiteľa,

— meno(á) držiteľa,

— preferovaný jazyk.

4.5.4.2.5 Sťahovanie údajov z karty

335) Dielenská karta musí byť schopná uložiť záznamy o sťahovaní údajov z karty rovnako ako karta vodiča.

4.5.4.2.6 Údaje o kalibrácii a úprave času

336) Dielenská karta musí byť schopná uchovať záznamy o kalibrácii a/alebo úprave času, ktoré sa vykonávali, keď bola karta vložená v záznamovom zariadení.

337) Každý záznam o kalibrácii musí byť schopný uchovať tieto údaje:

— účel kalibrácie (aktivácia, prvá montáž, montáž, pravidelná inšpekcia),

— identifikácia vozidla,

— aktualizované alebo potvrdené parametre (w, k, l, rozmer pneumatík, nastavenia obmedzovača rýchlosti, počítadlo kilometrov (nové a staré hodnoty), dátum a čas (nové a staré hodnoty),

— Identifikácia záznamového zariadenia (číslo dielu VU, sériové číslo VU, sériové číslo snímača pohybu, sériové číslo diaľkového komunikačného zariadenia a sériové číslo externého zariadenia GNSS v prípade potreby),

— druhy plomb a identifikátory všetkých používaných plomb,

— schopnosť VU použiť tachografové karty prvej generácie (aktivovaná alebo nie).

338) Dielenská karta musí byť schopná uložiť aspoň 88 takýchto záznamov.

339) Dielenská karta musí mať počítadlo udávajúce celkový počet kalibrácií vykonaných s kartou.

340) Dielenská karta musí mať počítadlo udávajúce počet kalibrácií vykonaných od jej posledného stiahnutia.

4.5.4.2.7 Údaje o udalostiach a poruchách

341) Dielenská karta musí byť schopná uložiť záznamy údajov o udalostiach a poruchách rovnako ako karta vodiča.

342) Dielenská karta musí byť schopná uložiť údaje o posledných troch udalostiach každého typu (t. j. 33 udalostí) a posledných šiestich poruchách každého typu (t. j. 12 porúch).

4.5.4.2.8 Údaje o činnosti vodiča

343) Dielenská karta musí byť schopná uložiť údaje o činnosti vodiča rovnako ako karta vodiča.

344) Dielenská karta musí byť schopná uchovať údaje o činnosti vodiča za aspoň jeden deň priemernej činnosti vodiča.

4.5.4.2.9 Údaje o použitých vozidlách

345) Dielenská karta musí byť schopná uložiť záznamy údajov o použitých vozidlách rovnako ako karta vodiča.

346) Dielenská karta musí byť schopná uložiť aspoň 4 takéto záznamy.

4.5.4.2.10 Údaje o začiatku a/alebo konci denného pracovného času

347) Dielenská karta musí byť schopná uložiť záznamy údajov o začiatku a/alebo konci denného pracovného času rovnako ako karta vodiča.

348) Dielenská karta musí byť schopná uchovať aspoň tri páry takých záznamov.

4.5.4.2.11 Údaje o relácii karty

349) Dielenská karta musí byť schopná uložiť záznam údajov o relácii karty rovnako ako karta vodiča.

4.5.4.2.12 Údaje o kontrolnej činnosti

350) Dielenská karta musí byť schopná uložiť záznam údajov o kontrolnej činnosti rovnako ako karta vodiča.

4.5.4.2.13 Údaje o použitých jednotkách vozidla

351) Dielenská karta musí byť schopná uložiť tieto údaje týkajúce sa rôznych jednotiek vozidla, v ktorých bola karta použitá:

— dátum a čas začiatku časového úseku používania jednotky vozidla (t. j. prvé vloženie karty do jednotky vozidla za daný časový úsek),

— výrobca jednotky vozidla,

— typ jednotky vozidla,

— číslo verzie softvéru použitého v jednotke vozidla.

352) Dielenská karta musí byť schopná uložiť aspoň 4 takéto záznamy.

4.5.4.2.14 Údaje o miestach počas troch hodín nepretržitej jazdy

353) Dielenská karta musí byť schopná uložiť tieto údaje týkajúce sa polohy vozidla, keď nepretržitý čas jazdy vodiča dosiahne násobok troch hodín:

— dátum a čas, keď nepretržitý čas jazdy držiteľa karty dosiahne násobok troch hodín,

— polohu vozidla,

— presnosť GNSS, dátum a čas, keď bola poloha určená.

354) Dielenská karta musí byť schopná uložiť aspoň 18 takýchto záznamov.

4.5.4.2.15 Údaje o špecifických podmienkach

355) Dielenská karta musí byť schopná uložiť údaje relevantné pre špecifické podmienky rovnako ako karta vodiča.

356) Dielenská karta musí byť schopná uložiť aspoň 2 takéto záznamy.

4.5.5 *Kontrolná karta*

4.5.5.1 Aplikácia tachografu (prístupné pre jednotky vozidla prvej a druhej generácie)

4.5.5.1.1 Identifikácia aplikácie

357) Kontrolná karta musí byť schopná uložiť tieto identifikačné údaje o aplikácii:

— identifikácia aplikácie tachografu,

— identifikácia typu tachografovej karty.

4.5.5.1.2 Kľúče a certifikáty

358) Kontrolná karta musí byť schopná uložiť niekoľko šifrovacích kľúčov a certifikátov, ako je uvedené v dodatku 11 časti A.

4.5.5.1.3 Identifikácia karty

359) Kontrolná karta musí byť schopná uložiť tieto identifikačné údaje karty:

— číslo karty,

— vydávajúci členský štát, názov vydávajúceho orgánu, dátum vydania,

— dátum začiatku platnosti karty, dátum skončenia platnosti karty (prípadný dátum skončenia platnosti).

4.5.5.1.4 Identifikácia držiteľa karty

360) Kontrolná karta musí byť schopná uložiť tieto identifikačné údaje držiteľa karty:

— názov kontrolného orgánu,

— adresu kontrolného orgánu,

— priezvisko držiteľa,

— meno(á) držiteľa,

— preferovaný jazyk.

4.5.5.1.5 Údaje o kontrolnej činnosti

361) Kontrolná karta musí byť schopná uložiť tieto údaje o kontrolnej činnosti:

— dátum a čas kontroly,

— typ kontroly (zobrazovanie a/alebo tlač a/alebo sťahovanie z VU a/alebo sťahovanie z karty a/alebo kontrola kalibrácie pri cestnej kontrole),

— (prípadne) stiahnutý časový úsek,

— evidenčné číslo vozidla a orgán členského štátu, ktorý kontrolované vozidlo zaevidoval,

— číslo karty a členský štát, ktorý vydal kontrolovanú kartu vodiča.

362) Kontrolná karta musí byť schopná uchovať aspoň 230 takých záznamov.

4.5.5.2 Aplikácia tachografu druhej generácie (neprístupné jednotke vozidla prvej generácie)

4.5.5.2.1 Identifikácia aplikácie

363) Kontrolná karta musí byť schopná uložiť tieto identifikačné údaje o aplikácii:

— identifikácia aplikácie tachografu,

— identifikácia typu tachografovej karty.

4.5.5.2.2 Kľúče a certifikáty

364) Kontrolná karta musí byť schopná uložiť niekoľko šifrovacích kľúčov a certifikátov, ako je uvedené v dodatku 11 časti B.

4.5.5.2.3 Identifikácia karty

365) Kontrolná karta musí byť schopná uložiť tieto identifikačné údaje karty:

— číslo karty,

— vydávajúci členský štát, názov vydávajúceho orgánu, dátum vydania,

— dátum začiatku platnosti karty, dátum skončenia platnosti karty (prípadný dátum skončenia platnosti).

4.5.5.2.4 Identifikácia držiteľa karty

366) Kontrolná karta musí byť schopná uložiť tieto identifikačné údaje držiteľa karty:

— názov kontrolného orgánu,

— adresu kontrolného orgánu,

— priezvisko držiteľa,

— meno(á) držiteľa,

— preferovaný jazyk.

4.5.5.2.5 Údaje o kontrolnej činnosti

367) Kontrolná karta musí byť schopná uložiť tieto údaje o kontrolnej činnosti:

— dátum a čas kontroly,

— typ kontroly (zobrazovanie a/alebo tlač a/alebo sťahovanie z VU a/alebo sťahovanie z karty a/alebo kontroly kalibrácie pri cestnej kontrole),

— (prípadne) stiahnutý časový úsek,

— evidenčné číslo vozidla a orgán členského štátu, ktorý kontrolované vozidlo zaevidoval,

— číslo karty a členský štát, ktorý vydal kontrolovanú kartu vodiča.

368) Kontrolná karta musí byť schopná uchovať aspoň 230 takých záznamov.

4.5.6 *Podniková karta*

4.5.6.1 Aplikácia tachografu (prístupné pre jednotky vozidla prvej a druhej generácie)

4.5.6.1.1 Identifikácia aplikácie

369) Podniková karta musí byť schopná uložiť tieto identifikačné údaje o aplikácii:

— identifikácia aplikácie tachografu,

— identifikácia typu tachografovej karty.

4.5.6.1.2 Kľúče a certifikáty

370) Podniková karta musí byť schopná uložiť niekoľko šifrovacích kľúčov a certifikátov, ako je uvedené v dodatku 11 časti A.

4.5.6.1.3 Identifikácia karty

371) Podniková karta musí byť schopná uložiť tieto identifikačné údaje karty:

— číslo karty,

— vydávajúci členský štát, názov vydávajúceho orgánu, dátum vydania,

— dátum začiatku platnosti karty, dátum skončenia platnosti karty (prípadný dátum skončenia platnosti).

4.5.6.1.4 Identifikácia držiteľa karty

372) Podniková karta musí byť schopná uložiť tieto identifikačné údaje držiteľa karty:

— názov podniku,

— adresu podniku.

4.5.6.1.5 Údaje o činnosti podniku

373) Podniková karta musí byť schopná uložiť tieto údaje o činnosti podniku:

— dátum a čas činnosti,

— druh činnosti (zablokovanie a/alebo odblokovanie VU a/alebo stiahnutie z VU a/alebo stiahnutie z karty),

— (prípadne) stiahnutý časový úsek,

— evidenčné číslo vozidla a orgán členského štátu, ktorý vozidlo zaevidoval,

— číslo karty a členský štát, ktorý vydal kartu (v prípade sťahovania).

374) Podniková karta musí byť schopná uchovať aspoň 230 takých záznamov.

4.5.6.2 Aplikácia tachografu druhej generácie (neprístupné jednotke vozidla prvej generácie)

4.5.6.2.1 Identifikácia aplikácie

375) Podniková karta musí byť schopná uložiť tieto identifikačné údaje o aplikácii:

— identifikácia aplikácie tachografu,

— identifikácia typu tachografovej karty.

4.5.6.2.2 Kľúče a certifikáty

376) Podniková karta musí byť schopná uložiť niekoľko šifrovacích kľúčov a certifikátov, ako je uvedené v dodatku 11 časti B.

4.5.6.2.3 Identifikácia karty

377) Podniková karta musí byť schopná uložiť tieto identifikačné údaje karty:

— číslo karty,

— vydávajúci členský štát, názov vydávajúceho orgánu, dátum vydania,

— dátum začiatku platnosti karty, dátum skončenia platnosti karty (prípadný dátum skončenia platnosti).

4.5.6.2.4 Identifikácia držiteľa karty

378) Podniková karta musí byť schopná uložiť tieto identifikačné údaje držiteľa karty:

— názov podniku,

— adresu podniku.

4.5.6.2.5 Údaje o činnosti podniku

379) Podniková karta musí byť schopná uložiť tieto údaje o činnosti podniku:

— dátum a čas činnosti,

— druh činnosti (zablokovanie a/alebo odblokovanie VU a/alebo stiahnutie z VU a/alebo stiahnutie z karty),

— (prípadne) stiahnutý časový úsek,

— evidenčné číslo vozidla a orgán členského štátu, ktorý vozidlo zaevidoval,

— číslo karty a členský štát, ktorý vydal kartu (v prípade sťahovania).

380) Podniková karta musí byť schopná uchovať aspoň 230 takých záznamov.

5 MONTÁŽ ZÁZNAMOVÉHO ZARIADENIA

5.1 **Montáž**

381) Nové záznamové zariadenie sa musí montérom alebo výrobcom vozidla dodať v neaktivovanom stave so všetkými kalibračnými parametrami, ktoré sú uvedené v kapitole 3.21, nastavenými na vhodné a platné predvolené hodnoty. Ak nie je žiadna konkrétna hodnota vhodná, textové parametre sa nastavia na reťazec „?“ a numerické parametre na „0“. Dodávka častí záznamového zariadenia, ktoré súvisia so zabezpečením, sa môže obmedziť, ak sa to vyžaduje počas certifikácie zabezpečenia.

382) Pred aktiváciou musí záznamové zariadenie umožniť prístup ku kalibračnej funkcii, aj keď nie je v režime kalibrácie.

383) Pred aktiváciou nesmie záznamové zariadenie zaznamenávať ani ukladať údaje uvedené v bodoch 3.12.3, 3.12.9 a 3.12.12 až 3.12.15 vrátane.

384) Počas montáže musí výrobca vozidla prednastaviť všetky známe parametre.

385) Výrobcovia vozidiel alebo montéri musia aktivovať namontované záznamové zariadenie najneskôr predtým, než sa vozidlo použije v rozsahu pôsobnosti nariadenia (ES) č. 561/2006.

386) Aktivácia záznamového zariadenia sa spustí automaticky pri prvom vložení platnej dielenskej karty do jedného zo zariadení s rozhraním karty.

387) Špecifické párovacie operácie medzi snímačom pohybu a jednotkou vozidla sa v prípade potreby uskutočnia automaticky pred aktiváciou alebo počas nej.

388) Podobne, špecifické spájacie operácie medzi externým zariadením GNSS a jednotkou vozidla sa v prípade potreby uskutočnia automaticky pred aktiváciou alebo počas nej.

389) Po aktivácii záznamové zariadenie musí zabezpečovať všetky funkcie a prístupové práva k údajom.

390) Po aktivácii záznamové zariadenie musí oznámiť diaľkovému komunikačnému zariadeniu zabezpečené údaje nevyhnutné na účel cielených cestných kontrol.

391) Záznamové a ukladacie funkcie záznamového zariadenia musia byť po jeho aktivácii úplne prevádzkyschopné.

392) Po montáži nasleduje kalibrácia. Prvá kalibrácia nemusí nutne zahŕňať zadanie evidenčného čísla vozidla (VRN), ak ho schválená dielňa vykonávajúca túto kalibráciu nepozná. Za týchto okolností a iba v tomto čase sa vlastníkovi vozidla umožní zadať VRN s použitím podnikovej karty pred použitím vozidla v rozsahu pôsobnosti nariadenia (ES) č. 561/2006 (napr. použitím príkazov v príslušnej štruktúre menu rozhrania človek-stroj v jednotke vozidla) [1]. Všetky aktualizácie alebo potvrdenie tohto zadania sú možné iba s použitím dielenskej karty.

393) Montáž externého zariadenia GNSS vyžaduje spojenie s jednotkou vozidla a následné overenie informácie o polohe z GNSS.

394) Záznamové zariadenie musí byť umiestnené vo vozidle tak, aby umožňovalo vodičovi z jeho sedadla prístup k potrebným funkciám.

[1] Ú. v. EÚ L 102, 11.4.2006, s.1.

5.2 **Montážny štítok**

395) Po kontrole záznamového zariadenia vykonanej pri montáži sa na záznamové zariadenie pripevní montážny štítok, ktorý je trvalo vyrytý alebo vytlačený, zreteľne viditeľný a ľahko prístupný. Ak to nie je možné, štítok sa pripevní na „B“ stĺpik vozidla tak, aby bol zreteľne viditeľný. V prípade vozidiel, ktoré nemajú „B“ stĺpik, sa montážny štítok pripevní na rám dverí na strane vodiča a musí byť v každej situácii zreteľne viditeľný.

Po každej prehliadke vykonanej schváleným montérom alebo dielňou sa namiesto predchádzajúceho štítku pripevní nový.

396) Na štítku musia byť aspoň tieto údaje:

— meno, adresa alebo obchodný názov schváleného montéra alebo dielne,

— charakteristický koeficient vozidla vo forme „w = … imp/km“,

— konštanta záznamového zariadenia vo forme „k = … imp/km“,

— skutočný obvod pneumatík kolies vo forme „l = … mm“,

— rozmer pneumatík,

— dátum, kedy bol meraný charakteristický koeficient vozidla a skutočný obvod pneumatík kolies,

— identifikačné číslo vozidla,

— prítomnosť (alebo neprítomnosť) externého zariadenia GNSS,

— sériové číslo externého zariadenia GNSS,

— sériové číslo diaľkového komunikačného zariadenia,

— sériové čísla všetkých používaných plomb,

— časť vozidla, v ktorej je prípadne namontovaný adaptér,

— časť vozidla, v ktorej je namontovaný snímač pohybu, ak nie je pripojený k prevodovke alebo ak sa nepoužíva adaptér,

— farba kábla medzi adaptérom a časťou vozidla, ktorá mu dodáva vstupné impulzy,

— sériové číslo zabudovaného snímača pohybu adaptéra.

397) Len v prípade tých vozidiel kategórie M1 a N1, na ktorých je namontovaný adaptér v súlade s nariadením Komisie (ES) č. 68/2009 ([1]) v znení posledných zmien, a vtedy, keď nie je možné uviesť všetky nevyhnutné informácie podľa požiadavky 396, sa môže použiť druhý, dodatočný štítok. V takýchto prípadoch musí tento dodatočný štítok obsahovať aspoň posledné štyri zarážky uvedené v požiadavke 396.

Ak sa tento druhý dodatočný štítok použije, musí sa pripevniť vedľa alebo blízko prvého hlavného štítka uvedeného v požiadavke 396, pričom musí mať tú istú úroveň ochrany. Okrem toho musí druhý štítok takisto obsahovať meno, adresu alebo obchodný názov schváleného montéra alebo dielne, ktorá vykonala montáž, ako aj dátum montáže.

([1]) Nariadenie Komisie (ES) č. 68/2009 z 23. januára 2009, ktorým sa deviatykrát prispôsobuje technickému pokroku nariadenie Rady (EHS) č. 3821/85 o záznamovom zariadení v cestnej doprave (Ú. v. EÚ L 21, 24.1.2009, s. 3).

5.3 **Plombovanie**

398) Musia sa zaplombovať tieto časti:

— každý spoj, ktorý by pri odpojení mohol spôsobiť nezistiteľnú zmenu alebo nezistiteľnú stratu údajov (to môže napr. platiť pre snímač pohybu namontovaný na prevodovke, adaptér pre vozidlá M1/N1, externé spojenie GNSS alebo jednotku vozidla);

— montážny štítok, pokiaľ nie je pripevnený tak, že ho nemožno odstrániť bez poškodenia značiek, ktoré sa na ňom nachádzajú.

399) Uvedené plomby sa môžu odstrániť:

— v prípade núdze,

— v prípade montáže, nastavenia alebo opravy obmedzovača rýchlosti alebo akéhokoľvek iného zariadenia, ktoré prispieva k zvýšeniu cestnej bezpečnosti, za predpokladu, že záznamové zaradenie naďalej funguje spoľahlivo a správne a že ho opäť zaplombuje schválený montér alebo dielňa (v súlade s kapitolou 6) ihneď po namontovaní zariadenia obmedzujúceho rýchlosť alebo akéhokoľvek iného zariadenia, ktoré prispieva k zvýšeniu cestnej bezpečnosti, alebo do siedmich dní v ostatných prípadoch.

400) Pri každom porušení týchto plomb sa musí vyhotoviť písomné vyhlásenie s uvedením dôvodov takého porušenia a musí sa poskytnúť príslušnému orgánu.

401) Plomby musia mať identifikačné číslo, ktoré im prideľuje výrobca. Toto číslo je jedinečné a odlišuje sa od každého iného čísla plomby prideleného iným výrobcom.

Toto jedinečné identifikačné číslo je definované ako: MM NNNNNN uvedené neodstrániteľnou značkou; MM ako jedinečná identifikácia výrobcu (databázu evidencie spravuje EK) a NNNNNN alfanumerické číslo plomby, ktoré je v doméne výrobcu jedinečné.

402) Plomby musia mať voľné miesto, kam schválení montéri, výrobcovia vozidiel alebo schválené dielne môžu doplniť osobitnú značku podľa článku 22 ods. 3 nariadenia (EÚ) č. 165/2014.

Táto značka nesmie zakrývať identifikačné číslo plomby.

403) Výrobcovia plomb musia byť registrovaní v špecializovanej databáze a zverejniť svoje identifikačné čísla plomb postupom, ktorý stanoví Európska komisia.

404) Schválené dielne a výrobcovia vozidiel musia v rámci nariadenia (EÚ) č. 165/2014, používať len plomby od tých výrobcov plomb, ktorí sú uvedení v spomenutej databáze.

405) Výrobcovia plomb a ich distribútori musia uchovávať úplné záznamy sledovateľnosti plomb predaných na použitie v rámci nariadenia (EÚ) č. 165/2014 a musia byť pripravení kedykoľvek ich podľa potreby poskytnúť príslušným vnútroštátnym orgánom.

406) Jedinečné identifikačné čísla plomb musia byť viditeľné na montážnom štítku.

6 KONTROLY, INŠPEKCIE A OPRAVY

Okolnosti, za ktorých môžu byť plomby odstránené, ako je uvedené v článku 22 ods. 5 nariadenia (EÚ) č. 165/2014, sú definované v kapitole 5.3 tejto prílohy.

6.1 **Schválenie montážnych firiem, dielní a výrobcov vozidiel**

Členské štáty schvaľujú, pravidelne kontrolujú a certifikujú subjekty, ktoré vykonávajú:

— montáže,

— kontroly,

— inšpekcie,

— opravy.

Dielenské karty sa vydávajú len montérom a/alebo dielňam schváleným na vykonávanie aktivácie a/alebo kalibrácie záznamového zariadenia podľa tejto prílohy, a pokiaľ nie je riadne odôvodnená výnimka:

— ktorí(-é) nemajú nárok na podnikovú kartu

— a ktorých iné odborné činnosti nepredstavujú možné ohrozenie celkového zabezpečenia systému, ako sa vyžaduje v dodatku 10.

6.2 **Kontrola nových alebo opravených prístrojov**

407) Každé jednotlivé zariadenie bez ohľadu na to, či je nové alebo opravené, sa musí skontrolovať z hľadiska jeho správnej činnosti a presnosti jeho čítaných hodnôt a záznamov, v rámci limitov stanovených v kapitole 3.2.1, 3.2.2, 3.2.3 a 3.3, pomocou plombovania v súlade s kapitolou 5.3 a kalibrácie.

6.3 **Inšpekcia inštalácie**

408) Po namontovaní na vozidlo musí celková inštalácia (vrátane záznamového zariadenia) spĺňať požiadavky na maximálne odchýlky stanovené v kapitole 3.2.1, 3.2.2, 3.2.3 a 3.3.

6.4 **Pravidelné inšpekcie**

409) Pravidelné inšpekcie zariadenia namontovaného vo vozidle sa musia vykonať po každej oprave daného zariadenia alebo po každej zmene charakteristického koeficientu vozidla alebo skutočného obvodu pneumatík, alebo potom, čo sa čas UTC zariadenia odchyľuje o viac než 20 minút od správneho času, alebo keď bolo zmenené VRN, a aspoň raz za dva roky (24 mesiacov) od poslednej kontroly.

410) Tieto inšpekcie musia zahŕňať kontroly:

— správneho fungovania záznamového zariadenia vrátane funkcie ukladania údajov na tachografových kartách a komunikácie so snímačom diaľkovej komunikácie,

— dodržania súladu s ustanoveniami kapitoly 3.2.1 a 3.2.2 o maximálnych odchýlkach po montáži,

— dodržania súladu s ustanoveniami kapitoly 3.2.3 a 3.3,

— umiestnenia značky typového schválenia na zariadení,

— pripevnenia montážneho štítku, ako je vymedzené v požiadavke 396, a popisného štítku, ako je vymedzené v požiadavke 225,

— veľkosti pneumatík a skutočného obvodu pneumatík,

— že k zariadeniu nie sú pripojené žiadne manipulačné zariadenia,

— že plomby sú na správnych miestach, v dobrom stave, s platnými identifikačnými číslami (odkazy na výrobcu plomb v databáze EK), ktoré zodpovedajú značkám montážneho štítka (pozri požiadavku 401).

411) Ak sa zistilo, že od vykonania poslednej inšpekcie došlo k niektorej z udalostí uvedených v kapitole 3.9 (Detekcia udalostí a/alebo porúch), ktorú výrobcovia tachografu a/alebo vnútroštátne orgány považujú za takú, ktorá môže potenciálne ohroziť zabezpečenie zariadenia, dielňa musí:

a. porovnať identifikačné údaje snímača pohybu zapojeného v prevodovke s údajmi spárovaného snímača pohybu registrovaného v jednotke vozidla;

b. overiť, či sa informácie zaznamenané na montážnom štítku zhodujú s informáciami obsiahnutými v zázname jednotky vozidla;

c. overiť, či sa sériové číslo snímača pohybu a schvaľovacie číslo, ak je vytlačené na kryte snímača pohybu, zhoduje s informáciami uloženými v dátovej pamäti záznamového zariadenia,

d. porovnať prípadné identifikačné údaje označené na popisnom štítku externého zariadenia GNSS s údajmi uloženými v dátovej pamäti jednotky vozidla.

412) Dielne musia vo svojich správach z inšpekcie uchovávať záznam o všetkých zisteniach týkajúcich sa poškodených plomb alebo manipulačných zariadení. Dielne musia tieto správy uchovávať najmenej dva roky a na požiadanie ich musia kedykoľvek sprístupniť príslušnému orgánu.

413) Súčasťou týchto inšpekcií musí byť aj kalibrácia a preventívne nahradenie plomb, ktorých montáž je v zodpovednosti dielní.

6.5 **Meranie chýb**

414) Meranie chýb pri montáži a počas používania sa uskutoční za týchto podmienok, ktoré treba považovať za súčasť štandardných skúšobných podmienok:

— nezaťažené vozidlo v normálnom prevádzkovom stave,

— tlak pneumatík v súlade s pokynmi výrobcu,

— opotrebenie pneumatík v rámci limitov povolených vnútroštátnymi právnymi predpismi,

— pohyb vozidla:

— vozidlo sa pohybuje vpred vlastným pohonom po priamke na rovnom povrchu rýchlosťou 50 ± 5 km/h. Meracia vzdialenosť musí byť minimálne 1 000 m.

— Za predpokladu, že sú porovnateľne presné, môžu sa na skúšku použiť alternatívne metódy, ako je napríklad vyhovujúce skúšobné zariadenie.

6.6 **Opravy**

415) Dielne musia byť schopné stiahnuť údaje zo záznamového zariadenia, aby ich mohli odovzdať príslušnému dopravnému podniku.

416) Schválené dielne musia vydať dopravným podnikom osvedčenie o nemožnosti stiahnutia údajov, keď nesprávne fungovanie záznamového zariadenia bráni stiahnutiu zaznamenaných údajov, dokonca aj po oprave v tejto dielni. Dielne musia minimálne dva roky uchovávať kópiu každého vydaného osvedčenia.

7 VYDÁVANIE KARIET

Postup vydávania kariet zavedený členským štátom musí byť v súlade s týmto:

417) Číslo karty prvého vydania tachografovej karty žiadateľovi musí mať prípadný poradový index, ako aj index náhrady a index obnovy nastavený na „0“.

418) Čísla kariet všetkých tachografových kariet, ktoré sa nevzťahujú na osobu, vydaných jednému kontrolnému orgánu, jednej dielni alebo jednému dopravnému podniku, musia mať prvých 13 číslic rovnakých a všetky musia mať rôzny poradový index.

419) Tachografová karta vydaná ako náhrada existujúcej tachografovej karty musí mať rovnaké číslo ako karta, ktorú nahrádza, no index náhrady sa zvýši o „1“ (v poradí 0, …, 9, A, …, Z).

420) Tachografová karta vydaná ako náhrada existujúcej tachografovej karty musí mať rovnaký dátum skončenia platnosti ako karta, ktorú nahrádza.

421) Tachografová karta vydaná ako obnova existujúcej tachografovej karty musí mať rovnaké číslo ako karta, ktorú obnovuje, pričom sa však index náhrady znova nastaví na „0“ a index obnovy sa zvýši o „1“ (v poradí 0, …, 9, A, …, Z).

422) Výmena existujúcej tachografovej karty na účely zmeny administratívnych údajov sa riadi pravidlami obnovy, ak sa realizuje v rámci toho istého členského štátu, alebo pravidlami prvého vydania, ak bola vykonaná iným členským štátom.

423) V kolónke „priezvisko držiteľa karty“ v prípade dielenskej alebo kontrolnej karty, ktorá sa nevzťahuje na osobu, sa uvedie názov dielne alebo kontrolného orgánu, prípadne meno montéra či kontrolného úradníka, ak sa tak členské štáty rozhodnú.

424) Členské štáty si musia elektronicky vymieňať údaje s cieľom zabezpečiť jedinečnosť kariet vodičov, ktoré vydávajú, v súlade s článkom 31 nariadenia (EÚ) č. 165/2014.

8 TYPOVÉ SCHVÁLENIE ZÁZNAMOVÉHO ZARIADENIA A TACHOGRAFOVÝCH KARIET

8.1 **Všeobecne**

Na účely tejto kapitoly pojem „záznamové zariadenie“ znamená „záznamové zariadenie alebo jeho komponenty“. Pre kábel resp. káble prepájajúce snímač pohybu s VU, externé zariadenie GNSS s VU alebo diaľkové komunikačné zariadenie s VU sa nevyžaduje žiadne typové schválenie. Papier používaný záznamovým zariadením sa považuje za komponent záznamového zariadenia.

Výrobca môže požiadať o typové schválenie svojho komponentu s akýmkoľvek typom snímača pohybu, externého zariadenia GNSS a naopak, pod podmienkou, že každý komponent spĺňa požiadavky tejto prílohy. Alternatívne môžu výrobcovia tiež požiadať o typové schválenie záznamového zariadenia.

425) Záznamové zariadenie musí byť na schválenie predložené celé so všetkými zabudovanými doplnkovými zariadeniami.

426) Typové schválenie záznamového zariadenia a tachografových kariet musí zahŕňať skúšky týkajúce sa zabezpečenia, skúšky funkčnosti a skúšky interoperability. Kladné výsledky každej z týchto skúšok sú uvedené na príslušnom osvedčení.

427) Schvaľovacie úrady členských štátov neudelia osvedčenie o typovom schválení, pokiaľ nedostanú:

— osvedčenie zabezpečenia,

— osvedčenie funkčnosti,

— a osvedčenie interoperability

pre záznamové zariadenie alebo tachografovú kartu, ktoré sú predmetom žiadosti o typové schválenie.

428) Každá zmena softvéru alebo hardvéru zariadenia alebo vlastností materiálov použitých na jeho výrobu sa pred jeho použitím oznámi orgánu, ktorý zariadeniu udelil typové schválenie. Tento orgán potvrdí výrobcovi rozšírenie typového schválenia alebo môže požadovať aktualizáciu alebo potvrdenie príslušných osvedčení zabezpečenia, funkčnosti a/alebo interoperability.

429) Postupy p modernizácie softvéru záznamového zariadenia in situ musí schváliť orgán, ktorý záznamovému zariadeniu udelil typové schválenie. Modernizácia softvéru nesmie meniť ani vymazať žiadne údaje o činnosti vodiča uložené v záznamovom zariadení. Softvér sa môže upgradovať len na zodpovednosť výrobcu zariadenia.

430) Typové schválenie modifikácií softvéru zamerané na modernizáciu predtým typovo schváleného záznamového zariadenia nemožno odmietnuť, ak sa takéto zmeny vzťahujú len na funkcie, ktoré nie sú uvedené v tejto prílohe. Modernizácia softvéru záznamového zariadenia môže vylúčiť zavedenie nových množín znakov, ak to nie je technicky realizovateľné.

8.2 **Osvedčenie zabezpečenia**

431) Osvedčenie zabezpečenia sa udelí v súlade s ustanoveniami dodatku 10 tejto prílohy. Osvedčujú sa tieto komponenty záznamového zariadenia: jednotka vozidla, snímač pohybu, externé zariadenie GNSS a tachografové karty.

432) Za výnimočných okolností, keď orgány osvedčovania zabezpečenia odmietnu osvedčiť nové zariadenie z dôvodu zastaranosti mechanizmov zabezpečenia, sa typové schválenie bude naďalej udeľovať iba za týchto osobitných a výnimočných okolností a iba vtedy, keď neexistuje iné alternatívne riešenie v súlade s nariadením.

433) Vtedy príslušný členský štát bezodkladne informuje Európsku komisiu, ktorá do dvanástich mesiacov od udelenia typového schválenia začne postup s cieľom zabezpečiť, aby sa zabezpečenie dostalo na svoju pôvodnú úroveň.

8.3 **Osvedčenie funkčnosti**

434) Každý uchádzač o typové schválenie poskytne schvaľovaciemu úradu členského štátu všetky materiály a dokumentáciu, ktoré považuje tento úrad za potrebné.

435) Výrobcovia poskytnú príslušné vzorky výrobkov, ktoré sa majú typovo schváliť, a súvisiacu dokumentáciu, ktorú požadujú skúšobne poverené vykonávaním funkčných skúšok, a to do jedného mesiaca od žiadosti. Všetky náklady spojené s touto požiadavkou znáša žiadajúci subjekt. Skúšobne sú povinné uchovávať všetky komerčne citlivé informácie v tajnosti.

436) Osvedčenie funkčnosti dostane výrobca len po úspešnom absolvovaní minimálne všetkých funkčných skúšok špecifikovaných v dodatku 9.

437) Schvaľovací úrad udeľuje osvedčenie funkčnosti. Toto osvedčenie musí okrem názvu subjektu, ktorému sa udeľuje, a identifikácie modelu obsahovať podrobný zoznam vykonaných skúšok a dosiahnutých výsledkov.

438) Na osvedčení funkčnosti každého komponentu záznamového zariadenia sa musia uvádzať aj čísla typových schválení ostatných typovo schválených kompatibilných komponentov záznamového zariadenia skúšaných pri jeho osvedčovaní.

439) Na osvedčení funkčnosti každého komponentu záznamového zariadenia sa musia uvádzať aj ISO alebo CEN normy, podľa ktorých bolo funkčné rozhranie osvedčené.

8.4 **Osvedčenie interoperability**

440) Skúšky interoperability vykonáva len jedna skúšobňa, ktorá podlieha Európskej komisii a je pod jej zodpovednosťou.

441) Skúšobňa registruje žiadosti výrobcov o skúšky interoperability v poradí, v ktorom boli doručené.

442) Žiadosti sa oficiálne zaregistrujú len vtedy, keď skúšobňa má k dispozícii:

— úplný súbor materiálov a dokumentov potrebných na také skúšky interoperability,

— zodpovedajúce osvedčenie zabezpečenia,

— zodpovedajúce osvedčenie funkčnosti.

Dátum registrácie žiadosti sa oznámi výrobcovi.

443) Pri záznamovom zariadení alebo tachografových kartách, ktorým nebolo udelené osvedčenie zabezpečenia a osvedčenie funkčnosti, skúšobňa nevykonáva skúšky interoperability, s výnimkou osobitných okolností uvedených v požiadavke 432.

444) Každý výrobca žiadajúci o vykonanie skúšok interoperability sa zaviaže ponechať skúšobni poverenej vykonávaním týchto skúšok úplný súbor materiálov a dokumentov, ktoré poskytol na účely vykonania skúšok.

445) Skúšky interoperability sa v súlade s ustanoveniami dodatku 9 tejto prílohy musia vykonať vždy so všetkými typmi záznamového zariadenia alebo tachografových kariet:

— ktoré majú ešte platné typové schválenia, alebo

— pre ktoré sa požaduje typové schválenie a ktoré majú platné osvedčenie interoperability.

446) Skúšky interoperability sa musia vzťahovať na všetky generácie záznamového zariadenia alebo tachografových kariet, ktoré sa stále používajú.

447) Osvedčenie interoperability udeľuje skúšobňa výrobcovi len po všetkých úspešne absolvovaných skúškach interoperability.

448) Ak neboli skúšky interoperability úspešné s jedným alebo niekoľkými záznamovými zariadeniami alebo tachografovou kartou resp. kartami, osvedčenie interoperability sa nesmie vydať, kým žiadajúci výrobca nevykoná potrebné zmeny a neabsolvuje úspešne skúšky interoperability. Skúšobňa musí s pomocou výrobcu, ktorého sa táto porucha interoperability týka, zistiť príčinu problému a musí sa pokúsiť pomôcť žiadajúcemu výrobcovi pri hľadaní technického riešenia. Ak výrobca zmenil svoj výrobok, musí sa na všetkých relevantných orgánoch uistiť, že osvedčenie zabezpečenia a osvedčenia funkčnosti sú stále platné.

449) osvedčenie interoperability je platné šesť mesiacov. Ak výrobca nedostal zodpovedajúce osvedčenie o typovom schválení, na konci tohto obdobia sa odoberie. osvedčenie interoperability predloží výrobca schvaľovaciemu úradu členského štátu, ktorý udelil osvedčenie funkčnosti.

450) Žiaden prvok, ktorý by mohol byť príčinou problému s interoperabilitou, sa nesmie použiť na získanie prospechu alebo na získanie dominantného postavenia.

8.5 Osvedčenie o typovom schválení

451) Schvaľovací úrad členského štátu môže udeliť osvedčenie o typovom schválení, pokiaľ mu budú predložené tri požadované osvedčenia.

452) Na osvedčení o typovom schválení každého komponentu záznamového zariadenia sa musia nachádzať aj čísla typových schválení ostatných typovo schválených interoperabilných záznamových zariadení.

453) Kópiu osvedčenia o typovom schválení musí vyhotoviť schvaľovací úrad pre skúšobňu poverenú vykonávaním skúšok interoperability v čase udelenia osvedčenia výrobcovi.

454) Skúšobňa vykonávajúca skúšky interoperability musí prevádzkovať verejnú webovú stránku, na ktorej bude aktualizovať zoznam modelov záznamových zariadení alebo tachografových kariet:

— za ktoré bola zaregistrovaná žiadosť na vykonanie skúšok interoperability,

— ktorým bolo udelené osvedčenie interoperability (aj keď len predbežné),

— ktorým bolo udelené osvedčenie o typovom schválení.

8.6 **Výnimočný postup: prvé osvedčenia interoperability pre záznamové zariadenia a tachografové karty druhej generácie**

455) Do štyroch mesiacov potom, čo bola prvá sada záznamového zariadenia druhej generácie a tachografových kariet druhej generácie (karty vodiča, dielenské, kontrolné a podnikové karty) certifikovaná ako interoperabilná, sa každé udelené osvedčenie interoperability (vrátane prvých) vzťahujúce sa k žiadostiam zaregistrovaným počas tohto obdobia považuje za predbežné.

456) Ak sú na konci tohto obdobia všetky príslušné výrobky vzájomne interoperabilné, všetky zodpovedajúce osvedčenia interoperability sa stávajú definitívnymi.

457) Ak sa počas tohto obdobia zistia problémy s interoperabilitou, skúšobňa poverená vykonávaním skúšok interoperability musí s pomocou všetkých príslušných výrobcov zistiť príčiny problému a vyzve ich, aby vykonali nevyhnutné úpravy.

458) Ak na konci tohto obdobia pretrvávajú problémy z hľadiska interoperability, skúšobňa poverená vykonávaním skúšok interoperability v spolupráci s príslušnými výrobcami a so schvaľovacími orgánmi, ktoré udelili zodpovedajúce osvedčenia funkčnosti, musí zistiť príčiny problémov s interoperabilitou a určiť zmeny, ktoré musí vykonať každý príslušný výrobca. Hľadanie technických riešení môže trvať maximálne dva mesiace, po uplynutí ktorých, ak sa nenašlo žiadne spoločné riešenie, Komisia po konzultácii so skúšobňou poverenou vykonávaním skúšok interoperability rozhodne o tom, ktoré zariadenie(a) a karty dostanú definitívne osvedčenie interoperability, s uvedením dôvodov pre také rozhodnutie.

459) Každá žiadosť o vykonanie skúšok interoperability registrovaná skúšobňou od konca štvormesačného obdobia po udelení prvého predbežného osvedčenia interoperability do dátumu rozhodnutia Komisie uvedeného v požiadavke 455, sa odloží, kým nebudú vyriešené pôvodné problémy interoperability. Také žiadosti sa potom spracujú v poradí, v akom boli zaregistrované.

Dodatok 1

SLOVNÍK ÚDAJOV

OBSAH

1. ÚVOD 88
1.1. Prístup k vymedzeniu dátových typov 88
1.2. Referenčné dokumenty 88
2. VYMEDZENIE DÁTOVÝCH TYPOV 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. Certificate 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. VYMEDZENIE ROZSAHU HODNÔT A ROZMEROV 171
4. MNOŽINY ZNAKOV 171
5. KÓDOVANIE 171
6. OBJEKTOVÉ IDENTIFIKÁTORY A IDENTIFIKÁTORY APLIKÁCIÍ 171
6.1. Objektové identifikátory 171
6.2. Identifikátory aplikácií 172

1. ÚVOD

Tento dodatok špecifikuje dátové formáty, dátové prvky a dátové štruktúry používané v záznamovom zariadení a tachografových kartách.

1.1. Prístup k vymedzeniu dátových typov

V dodatku sa na vymedzenie dátových typov používa notácia Abstract Syntax Notation One (ASN.1). Umožňuje to jednoduchú a štruktúrovanú definíciu údajov bez implikácie akejkoľvek osobitnej prevodnej syntaxe (pravidiel kódovania), ktorá by bola závislá od aplikácie a prostredia.

Konvencie pomenovania typov ASN.1 vychádzajú z normy ISO/IEC 8824-1. To znamená, že:

— zvolený názov podľa možnosti implikuje význam dátového typu,

— ak sa dátový typ skladá z iných dátových typov, jeho názov je stále jediným reťazcom abecedných znakov začínajúcich sa veľkým písmenom; veľké písmená sa však v záujme objasnenia príslušného významu používajú aj vo vnútri názvu,

— názvy dátových typov vo všeobecnosti súvisia s názvami dátových typov, z ktorých sa skladajú, so zariadeniami, na ktorých sú údaje uložené, a s príslušnou funkciou.

Ak je typ ASN.1 už vymedzený ako súčasť inej normy a je relevantný pre použitie v záznamovom zariadení, bude tento typ ASN.1 vymedzený v tomto dodatku.

Na umožnenie viacerých typov kódovacích pravidiel sú niektoré typy ASN.1 v tomto dodatku obmedzené identifikátormi rozsahu hodnôt. Identifikátory rozsahu hodnôt sú vymedzené v odseku 3 a dodatku 2.

1.2. Referenčné dokumenty

V dodatku sa používajú tieto referenčné dokumenty:

ISO 639	Kódy názvov jazykov. Prvé vydanie: 1988.
ISO 3166	Kódy na reprezentáciu názvov krajín a ich častí. Časť 1: Kódy krajín, 2013
ISO 3779	Cestné vozidlá. Identifikačné číslo vozidla (VIN). Obsah a stavba. 2009
ISO/IEC 7816-5	Identifikačné karty. Karty s integrovanými obvodmi. Časť 5: Registrácia poskytovateľov aplikácií. Druhé vydanie: 2004.
ISO/IEC 7816-6	Identifikačné karty. Karty s integrovanými obvodmi. Časť 6: Medziodborové dátové prvky pre výmenu, 2004 + technické korigendum 1: 2006
ISO/IEC 8824-1	Informačné technológie. Jazyk ASN.1 (Zápis abstraktnej syntaxe č.1). Vymedzenie základnej notácie. 2008 + technické korigendum 1: 2012 a technické korigendum 2: 2014.
ISO/IEC 8825-2	Informačné technológie. Pravidlá kódovania v ASN.1: vymedzenie pravidiel zhusteného kódovania (Packed Encoding Rules – PER). 2008.
ISO/IEC 8859-1	Informačné technológie. Množiny grafických znakov kódované jednou 8-bitovou slabikou (jedným oktetom). Časť 1: Latinská abeceda č. 1. Prvé vydanie: 1998.
ISO/IEC 8859-7	Informačné technológie – Množiny grafických znakov kódované jednou 8-bitovou slabikou (jedným oktetom). Časť 7: Latinská abeceda/Grécka abeceda. 2003.

ISO 16844-3	Cestné vozidlá. Tachografové systémy. Rozhranie snímača pohybu. 2004 + technické korigendum 1: 2006.
TR-03110-3	Technické usmernenie BSI / ANSSI TR-03110-3: Vyspelé bezpečnostné mechanizmy pre strojovo čitateľné cestovné doklady a token eIDAS. Časť 3: Spoločné špecifikácie, verzia 2.20, 3. február 2015

2. VYMEDZENIE DÁTOVÝCH TYPOV

Pri všetkých nasledovných dátových typoch sa ako predvolená hodnota pri „neznámom“ alebo „neuplatniteľnom“ obsahu dátový prvok vyplní bajtmi ‘FF’.

Ak nie je uvedené inak, všetky dátové typy sa používajú pre aplikácie generácie 1 a generácie 2.

2.1. **ActivityChangeInfo**

Tento dátový typ umožňuje dvojbajtovým slovom kódovanie stavu slotu v čase 00.00 hod. a/alebo stavu vodiča v čase 00.00 hod. a/alebo pre vodiča a druhého vodiča zmeny činnosti a/alebo zmeny stavu vedenia vozidla a/alebo zmeny stavu karty. Tento dátový typ súvisí s požiadavkami prílohy 1C č. 105, 266, 291, 320, 321, 343 a 344.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Pridelenie hodnôt – usporiadaný oktet: ‘scpaatttttttttt’B (16 bitov)

Pre záznamy v dátovej pamäti (alebo stav slotu):

‘s’B	Slot:
	‘0’B: VODIČ,
	‘1’B: DRUHÝ VODIČ,
‘c’B	Stav vedenia vozidla:
	‘0’B: JEDEN VODIČ,
	‘1’B: POSÁDKA,
‘p’B	Stav karty vodiča (alebo dielenskej karty) v príslušnom slote:
	‘0’B: VLOŽENÁ, karta je vložená,
	‘1’B: NEVLOŽENÁ, nie je vložená žiadna karta (alebo je karta vytiahnutá),
‘aa’B	Činnosť:
	‘00’B: PRESTÁVKA/ODPOČINOK,
	‘01’B: POHOTOVOSŤ,
	‘10’B: PRÁCA,
	‘11’B: VEDENIE VOZIDLA,
‘ttttttttttt’B	Čas zmeny: Počet minút od 00h00 daného dňa.

Pre záznamy na karte vodiča (alebo dielenskej karte) (a stav vodiča):

‘s’B	Slot (irelevantné, ak ‘p’=1, s výhradou v poznámke nižšie):
	‘0’B: VODIČ,
	‘1’B: DRUHÝ VODIČ,
‘c’B	Stav vedenia vozidla (prípad ‘p’=0) alebo
	stav ďalšej činnosti (prípad ‘p’=1):
	‘0’B: JEDEN VODIČ,
	‘0’B: NEZNÁMY
	‘1’B: POSÁDKA,
	‘1’B: ZNÁMY (=manuálne zadané)
‘p’B	Stav karty:
	‘0’B: VLOŽENÁ, karta je vložená v záznamovom zariadení,
	‘1’B: NEVLOŽENÁ, karta nie je vložená (alebo je vytiahnutá),
‘aa’B	Činnosť (irelevantné, ak ‘p’=1 a ‘c’=0, s výhradou v poznámke nižšie):
	‘00’B: PRESTÁVKA/ODPOČINOK,
	‘01’B: POHOTOVOSŤ,
	‘10’B: PRÁCA,
	‘11’B: VEDENIE VOZIDLA,
‘ttttttttttt’B	Čas zmeny: Počet minút od 00h00 daného dňa.

Poznámka pre prípad „vytiahnutie karty“:

Ak je karta vytiahnutá:

— ‘s’ je relevantné a udáva slot, z ktorého je karta vytiahnutá,

— ‘c’ musí byť nastavené na 0,

— ‘p’ musí byť nastavené na 1,

— ‘aa’ musí kódovať aktuálnu činnosť zvolenú v danom čase,

Následkom manuálneho zápisu sa bity ‘c’ a ‘aa’ slova (uložené na karte) môžu neskôr prepísať, aby zohľadnili zápis.

2.2. **Address**

Adresa.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage určuje množinu znakov vymedzenú v kapitole 4,

address je adresa kódovaná určenou množinou znakov.

2.3. **AESKey**

Generácia 2:

Kľúč AES s dĺžkou 128, 192 alebo 256 bitov.

```
AESKey ::= CHOICE {
   aes128Key                          AES128Key,
   aes192Key                          AES192Key,
   aes256Key                          AES256Key
}
```

Priradenie hodnôt: bližšie neurčené.

2.4. **AES128Key**

Generácia 2:

Kľúč AES128.

```
AES128Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes128Key                          OCTET STRING (SIZE(16))
}
```

length určuje dĺžku kľúča AES128 v oktetoch.

aes128Key je kľúč AES s dĺžkou 128 bitov.

Priradenie hodnôt:

Dĺžka má hodnotu 16.

2.5. **AES192Key**

Generácia 2:

Kľúč AES192.

```
AES192Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes192Key                          OCTET STRING (SIZE(24))
}
```

length určuje dĺžku kľúča AES192 v oktetoch.

aes192Key je kľúč AES s dĺžkou 192 bitov.

Priradenie hodnôt:

Dĺžka má hodnotu 24.

2.6. **AES256Key**

Generácia 2:

Kľúč AES256.

```
AES256Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes256Key                               OCTET STRING (SIZE(32))
}
```

length určuje dĺžku kľúča AES256 v oktetoch.

aes256Key je kľúč AES s dĺžkou 256 bitov.

Priradenie hodnôt:

Dĺžka má hodnotu 32.

2.7. **BCDString**

BCDString sa používa na zápis dvojkovo kódovaných dekadických čísel. Tento dátový typ sa používa na zápis jednej dekadickej číslice v polovici oktetu (4 bity). BCDString je založený na type 'CharacterStringType' podľa normy ISO/IEC 8824-1.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString používa notáciu „hstring". Najkrajnejšia ľavá hexadecimálna číslica je v prvom oktete 4-bitová skupina najvyššieho rádu. Na získanie násobku oktetov sa podľa potreby od polohy najkrajnejšej ľavej 4-bitovej skupiny v prvom oktete pripoja 4-bitové skupiny s nulami.

Povolené číslice sú: 0, 1, ..9.

2.8. **CalibrationPurpose**

Kód vysvetľujúci, prečo bola zaznamenaná sada kalibračných parametrov. Tento dátový typ súvisí s požiadavkami bodov 097 a 098 v prílohe 1B a požiadavkami bodu 119 v prílohe 1C.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Priradenie hodnôt:

Generácia 1:

'00'H	vyhradená hodnota,
'01'H	aktivácia: záznam kalibračných parametrov známych v čase aktivácie VU,
'02'H	prvá inštalácia: prvá kalibrácia VU po jej aktivácii,
'03'H	inštalácia: prvá kalibrácia VU v aktuálnom vozidle,
'04'H	pravidelná inšpekcia.

Generácia 2:

Oproti generácii 1 sa navyše použijú tieto hodnoty:

'05'H	evidenčné číslo vozidla zadané spoločnosťou
'06'H	úprava času bez kalibrácie,
'07'H až '7F'H	vyhradené na budúce použitie (RFU),
'80'H až 'FF'H	podľa výrobcu.

2.9. CardActivityDailyRecord

Informácie uložené na karte, ktoré sa vzťahujú k činnostiam vodiča v určitom kalendárnom dni. Tento dátový typ súvisí s požiadavkami 266, 291, 320 a 343 v prílohe 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 je celková dĺžka predchádzajúceho denného záznamu v bajtoch. Maximálna hodnota je daná dĺžkou reťazca oktetov (OCTET STRING) obsahujúceho tieto záznamy (pozri CardActivityLengthRange, dodatok 2 odsek4). Keď je tento záznam najstarším denným záznamom, hodnota activityPreviousRecordLength sa musí nastaviť na 0.

activityRecordLength je celková dĺžka tohto záznamu v bajtoch. Maximálna hodnota je daná dĺžkou reťazca oktetov (OCTET STRING) obsahujúceho tieto záznamy.

activityRecordDate je dátum záznamu.

activityDailyPresenceCounter je počítadlo dennej prítomnosti pre kartu v tomto dni.

activityDayDistance je celková vzdialenosť prejdená v tomto dni.

activityChangeInfo je sada údajov ActivityChangeInfo pre vodiča v tomto dni. Môže obsahovať maximálne 1440 hodnôt (jedna zmena činnosti za minútu). Táto sada vždy zahŕňa activityChangeInfo určujúce stav vodiča o 00.00 hod.

2.10. CardActivityLengthRange

Počet bajtov na karte vodiča alebo dielenskej karte, ktorý je k dispozícii na uloženie záznamov činnosti vodiča.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Priradenie hodnôt: pozri dodatok 2.

2.11. CardApprovalNumber

Číslo typového schválenia karty.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Priradenie hodnôt:

Schvaľovacie číslo sa uvedie tak, ako je uverejnené na príslušných webových stránkach Európskej komisie, t. j. napríklad vrátane prípadných pomlčiek. Schvaľovacie číslo schválenia sa zarovná vľavo.

2.12. **CardCertificate**

Generácia 1:

Certifikát verejného kľúča karty.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Informácia uložená na karte, ktorá sa vzťahuje k identifikácii integrovaného obvodu (integrated circuit – IC) karty (požiadavka 249 v prílohe 1C). Čip karty jedinečne identifikuje kombinácia icSerialNumber a icManufacturingReferences. Samotné icSerialNumber nie je jedinečnou identifikáciou čipu karty.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber je sériové číslo IC.

icManufacturingReferences je špecifický identifikátor výrobcu IC.

2.14. **CardConsecutiveIndex**

Poradový index karty (definícia (h)).

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Priradenie hodnôt: (pozri prílohu 1C kapitolu 7)

Poradie zvyšovania: '0, …, 9, A, …, Z, a, …, z'

2.15. **CardControlActivityDataRecord**

Informácie uložené na karte vodiča alebo dielenskej karte o poslednej kontrole, ktorej sa vodič podrobil (požiadavky 274, 299, 327 a 350 v prílohe 1C).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                       ControlType,
   controlTime                       TimeReal,
   controlCardNumber                 FullCardNumber,
   controlVehicleRegistration        VehicleRegistrationIdentification,
   controlDownloadPeriodBegin        TimeReal,
   controlDownloadPeriodEnd          TimeReal
}
```

controlType je typ kontroly.

controlTime je dátum a čas kontroly.

controlCardNumber je číslo FullCardNumber kontrolného úradníka, ktorý kontrolu vykonal.

controlVehicleRegistration je evidenčné číslo vozidla (vehicle registration number – VRN) a členský štát evidencie kontrolovaného vozidla.

controlDownloadPeriodBegin a **controlDownloadPeriodEnd** v prípade sťahovania je stiahnutý časový úsek.

2.16. **CardCurrentUse**

Informácie o aktuálnom použití karty (požiadavky 273, 298, 326 a 349 v prílohe 1C).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                    TimeReal,
   sessionOpenVehicle                 VehicleRegistrationIdentification
}
```

sessionOpenTime je čas, kedy je karta vložená pre aktuálne použitie. Tento prvok sa pri vytiahnutí karty nastaví na nulu.

sessionOpenVehicle je identifikácia aktuálne používaného vozidla nastavená pri vložení karty. Tento prvok sa pri vytiahnutí karty nastaví na nulu.

2.17. **CardDriverActivity**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú na činnosti vodiča (požiadavky 267, 268, 292, 293, 321 a 344 v prílohe 1C).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord     INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord        INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords               OCTET STRING
                                      (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord je špecifikácia začiatku miesta uloženia (počet bajtov od začiatku reťazca) najstaršieho úplného denného záznamu v reťazci activityDailyRecords. Maximálna hodnota je daná dĺžkou reťazca.

activityPointerNewestRecord je špecifikácia začiatku miesta uloženia (počet bajtov od začiatku reťazca) najnovšieho denného záznamu v reťazci activityDailyRecords. Maximálna hodnota je daná dĺžkou reťazca.

activityDailyRecords je miesto, ktoré je k dispozícii na uloženie údajov o činnosti vodiča (dátová štruktúra: CardActivityDailyRecord) za každý kalendárny deň, v ktorom sa karta použila.

Priradenie hodnôt: tento oktet sa cyklicky vypĺňa záznamami CardActivityDailyRecord. Pri prvom použití sa ukladanie začína v prvom bajte reťazca. Každý nový záznam sa pripája na koniec predchádzajúceho. Keď je reťazec plný, ukladanie pokračuje v prvom bajte reťazca nezávisle na prerušení vo vnútri dátového prvku. Skôr, než sa do reťazca umiestnia nové údaje o činnosti (zväčšenie aktuálneho záznamu activityDailyRecord alebo zadanie nového activityDailyRecord), ktoré nahrádzajú staršie údaje o činnosti, treba aktualizovať activityPointerOldestDayRecord, aby odrážal novú polohu najstaršieho úplného denného záznamu a activityPreviousRecordLength tohto (nového) najstaršieho úplného denného záznamu sa musí znovu nastaviť na 0.

2.18. **CardDrivingLicenceInformation**

Informácie uložené na karte vodiča, ktoré sa týkajú údajov o vodičskom preukaze držiteľa karty (požiadavky 259 a 284 v prílohe 1C).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority je orgán zodpovedný za vydanie vodičského preukazu.

drivingLicenceIssuingNation je štátna príslušnosť orgánu, ktorý vydal vodičský preukaz.

drivingLicenceNumber je číslo vodičského preukazu.

2.19. **CardEventData**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k udalostiam súvisiacim s držiteľom karty (požiadavky 260, 285, 318 a 341 v prílohe 1C).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData je sekvencia záznamov cardEventRecords (okrem záznamov z pokusov o narušenie zabezpečenia – tie sa zhromaždia v poslednej sade sekvencie) usporiadaná vzostupne podľa hodnoty EventFaultType.

cardEventRecords je sada záznamov o udalostiach daného typu udalosti (alebo kategórie pri pokusoch o narušenie zabezpečenia).

2.20. **CardEventRecord**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k udalosti súvisiacej s držiteľom karty (požiadavky 261, 286, 318 a 341 v prílohe 1C).

```
CardEventRecord ::= SEQUENCE {
   eventType                            EventFaultType,
   eventBeginTime                       TimeReal,
   eventEndTime                         TimeReal,
   eventVehicleRegistration             VehicleRegistrationIdentification
}
```

eventType je typ udalosti.

eventBeginTime je dátum a čas začiatku udalosti.

eventEndTime je dátum a čas skončenia udalosti.

eventVehicleRegistration je evidenčné číslo vozidla a členský štát evidencie vozidla, u ktorého udalosť nastala.

2.21. **CardFaultData**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k poruchám súvisiacim s držiteľom karty (požiadavky 263, 288, 318 a 341 v prílohe 1C).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                     SET SIZE(NoOfFaultsPerType) OF
                                        CardFaultRecord
}
```

CardFaultData je sekvencia sady záznamov o poruchách záznamového zariadenia, za ktorou nasleduje sada záznamov o poruchách karty.

cardFaultRecords je sada záznamov o poruchách danej kategórie poruchy (záznamové zariadenie alebo karta).

2.22. **CardFaultRecord**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k poruche súvisiacej s držiteľom karty (požiadavky 264, 289, 318 a 341 v prílohe 1C).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType je typ poruchy.

faultBeginTime je dátum a čas začiatku poruchy.

faultEndTime je dátum a čas skončenia poruchy.

faultVehicleRegistration je evidenčné číslo vozidla a členský štát evidencie vozidla, u ktorého porucha nastala.

2.23. **CardIccIdentification**

Informácia uložená na karte, ktorá sa vzťahuje k identifikácii karty s integrovaným obvodom (IC) (požiadavka 248 v prílohe 1C).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop je režim zastavenia času (clockstop) vymedzený v dodatku 2.

cardExtendedSerialNumber je jedinečné sériové číslo IC karty bližšie určené dátovým typom ExtendedSerial-Number data type.

cardApprovalNumber je číslo typového schválenia karty.

cardPersonaliserID je personalizačné ID karty kódované ako ManufacturerCode.

embedderIcAssemblerId udáva informácie o zhotoviteľovi karty/zostavovateľovi IC.

icIdentifier je identifikátor IC na karte a výrobcu daného IC v zmysle normy ISO/IEC 7816-6.

2.24. **CardIdentification**

Informácie uložené na karte, ktoré súvisia s identifikáciou danej karty (požiadavky 255, 280, 310, 333, 359, 365, 371 a 377 v prílohe 1C).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState              NationNumeric,
   cardNumber                          CardNumber,
   cardIssuingAuthorityName            Name,
   cardIssueDate                       TimeReal,
   cardValidityBegin                   TimeReal,
   cardExpiryDate                      TimeReal
}
```

cardIssuingMemberState je kód členského štátu, ktorý kartu vydal.

cardNumber je číslo karty.

cardIssuingAuthorityName je názov orgánu, ktorý kartu vydal.

cardIssueDate je dátum vydania karty súčasnému držiteľovi.

cardValidityBegin je počiatočný dátum platnosti karty.

cardExpiryDate je konečný dátum platnosti karty.

2.25. CardMACertificate

Generácia 2:

Certifikát verejného kľúča karty pre vzájomnú autentifikáciu s VU. Štruktúra tohto certifikátu je stanovená v dodatku 11.

```
CardMACertificate ::= Certificate
```

2.26. CardNumber

Číslo karty definované vo vymedzení pojmov pod písmenom g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification             IA5String(SIZE(14)),
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification              IA5String(SIZE(13)),
      cardConsecutiveIndex             CardConsecutiveIndex,
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   }
}
```

driverIdentification je jedinečná identifikácia vodiča v členskom štáte.

ownerIdentification je jedinečná identifikácia podniku, dielne alebo kontrolného orgánu v členskom štáte.

cardConsecutiveIndex je poradový index karty.

cardReplacementIndex je index náhrady karty.

cardRenewalIndex je index obnovy karty.

Prvá sekvencia voľby je vhodná na kódovanie čísla karty vodiča, druhá sekvencia voľby je vhodná na kódovanie čísla dielenskej, kontrolnej a podnikovej karty.

2.27. **CardPlaceDailyWorkPeriod**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa týkajú miest, kde sa začína alebo končí denný pracovný čas (požiadavky 272, 297, 325 a 348 v prílohe 1C).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord je index naposledy aktualizovaného záznamu o mieste.

Priradenie hodnôt: číslo zodpovedajúce počítadlu záznamu o mieste začínajúce sa od '0' pre prvý výskyt záznamov o mieste v štruktúre.

placeRecords je sada záznamov obsahujúcich informácie spojené so zadanými miestami.

2.28. **CardPrivateKey**

Generácia 1:

Súkromný kľúč karty.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Verejný kľúč karty.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Index obnovy karty (vymedzenie pojmov, písm. i)).

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Priradenie hodnôt: (pozri kapitolu VII v tejto prílohe).

'0' Prvé vydanie.

Poradie zvyšovania: '0, …, 9, A, …, Z'

2.31. **CardReplacementIndex**

Index náhrady karty (vymedzenie pojmov, písm. j)).

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Priradenie hodnôt: (pozri kapitolu VII v tejto prílohe).

'0' Pôvodná karta.

Poradie zvyšovania: '0, …, 9, A, …, Z'

2.32. **CardSignCertificate**

Generácia 2:

Certifikát verejného kľúča karty na podpis. Štruktúra tohto certifikátu je stanovená v dodatku 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Kód na rozlíšenie dvoch slotov jednotky vozidla.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Priradenie hodnôt: bližšie neurčené.

2.34. **CardSlotsStatus**

Kód udávajúci typ karty vloženej do dvoch slotov jednotky vozidla.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Priradenie hodnôt – usporiadaný oktet: 'ccccdddd'B

'cccc'B identifikácia typu karty vloženej do slotu druhého vodiča,

'dddd'B identifikácia typu karty vloženej do slotu vodiča,

s nasledovnými identifikačnými kódmi:

'0000'B nie je vložená žiadna karta,

'0001'B vložená karta vodiča,

'0010'B vložená dielenská karta,

'0011'B vložená kontrolná karta,

'0100'B vložená podniková karta.

2.35. **CardSlotsStatusRecordArray**

Generácia 2:

CardSlotsStatus plus metaúdaje použité v sťahovacom protokole.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType určuje typ záznamu (CardSlotsStatus). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu CardSlotsStatus v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov CardSlotsStatus.

2.36. **CardStructureVersion**

Kód udávajúci verziu štruktúry implementovanej v tachografovej karte.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Priradenie hodnôt: 'aabb'H:

'aa'H index zmien štruktúry.

'00'H pre aplikácie generácie 1

'01'H pre aplikácie generácie 2

'bb'H index pre zmeny týkajúce sa používania dátových prvkov definovaných pre štruktúru danú najvýznamnejším bajtom (high byte).

'00'H pre túto verziu aplikácií generácie 1

'00'H pre túto verziu aplikácií generácie 2

2.37. **CardVehicleRecord**

Informácie uložené na karte vodiča alebo dielenskej karte spojené s časovým úsekom používania vozidla počas kalendárneho dňa (požiadavky 269, 294, 322 a 345 v prílohe 1C).

Generácia 1:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin je stav počítadla kilometrov na začiatku časového úseku používania vozidla.

vehicleOdometerEnd je stav počítadla kilometrov na konci časového úseku používania vozidla.

vehicleFirstUse je dátum a čas začiatku časového úseku používania vozidla.

vehicleLastUse je dátum a čas skončenia časového úseku používania vozidla.

vehicleRegistration je evidenčné číslo vozidla (VRN) a členský štát evidencie vozidla.

vuDataBlockCounter je hodnota VuDataBlockCounter pri poslednej extrakcii časového úseku používania vozidla.

Generácia 2:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Oproti generácii 1 sa navyše použije tento dátový prvok:

VehicleIdentificationNumber je identifikačné číslo vozidla ako celku.

2.38. **CardVehiclesUsed**

Informácie uložené na karte vodiča alebo dielenskej karte súvisiace s vozidlami, ktoré držiteľ karty používa (požiadavky 270, 295, 323 a 346 v prílohe 1C).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord je index naposledy aktualizovaného záznamu o vozidle.

Priradenie hodnôt: číslo zodpovedajúce počítadlu záznamu o vozidle začínajúce sa od '0' pre prvý výskyt záznamov o vozidle v štruktúre.

cardVehicleRecords je sada záznamov obsahujúcich informácie o použitých vozidlách.

2.39. **CardVehicleUnitRecord**

Generácia 2:

Informácie uložené na karte vodiča alebo dielenskej karte súvisiace s použitou jednotkou vozidla (požiadavky 303 a 351 v prílohe 1C).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                           TimeReal,
   manufacturerCode                    ManufacturerCode,
   deviceID                            INTEGER(0..255),
   vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp je začiatok časového úseku používania jednotky vozidla (t. j. prvé vloženie karty do jednotky vozidla za dané obdobie).

manufacturerCode identifikuje výrobcu jednotky vozidla.

deviceID identifikuje typ jednotky vozidla výrobcu. Hodnota je špecifická podľa výrobcu.

vuSoftwareVersion je číslo verzie softvéru jednotky vozidla.

2.40. **CardVehicleUnitsUsed**

Generácia 2:

Informácie uložené na karte vodiča alebo dielenskej karte súvisiace s jednotkami vozidla, ktoré držiteľ karty používa (požiadavky 306 a 352 v prílohe 1C).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord je index naposledy aktualizovaného záznamu o jednotke vozidla.

Priradenie hodnôt: číslo zodpovedajúce počítadlu záznamu o jednotke vozidla začínajúce sa od '0' pre prvý výskyt záznamov o jednotke vozidla v štruktúre.

cardVehicleUnitRecords je sada záznamov obsahujúcich informácie o použitých jednotkách vozidla.

2.41. **Certificate**

Certifikát verejného kľúča vydaný certifikačnou autoritou.

Generácia 1:

```
Certificate ::= OCTET STRING (SIZE(194))
```

Priradenie hodnôt: digitálny podpis s čiastočnou obnovou CertificateContent podľa dodatku 11 Spoločné bezpečnostné mechanizmy: Podpis (128 bajtov) || zostatok verejného kľúča (58 bajtov) || ref. certifikačnej autority (8 bajtov).

Generácia 2:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Priradenie hodnôt: Pozri dodatok 11

2.42. **CertificateContent**

Generácia 1:

(Čistý) obsah certifikátu verejného kľúča podľa dodatku 11 Spoločné bezpečnostné mechanizmy.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier         INTEGER(0..255),
   certificationAuthorityReference      KeyIdentifier,
   certificateHolderAuthorisation       CertificateHolderAuthorisation,
   certificateEndOfValidity             TimeReal,
   certificateHolderReference           KeyIdentifier,
   publicKey                            PublicKey
}
```

certificateProfileIdentifier je verzia príslušného certifikátu.

Priradenie hodnôt: '01h' pre túto verziu.

certificationAuthorityReference identifikuje certifikačnú autoritu, ktorá daný certifikát vydala. Je zároveň referenciou na verejný kľúč tejto certifikačnej autority.

certificateHolderAuthorisation identifikuje práva držiteľa certifikátu.

certificateEndOfValidity je dátum, ktorým sa končí administratívna platnosť certifikátu.

certificateHolderReference identifikuje držiteľa certifikátu. Je zároveň referenciou na jeho verejný kľúč.

publicKey je verejný kľúč, ktorý sa týmto certifikátom potvrdzuje.

2.43. **CertificateHolderAuthorisation**

Identifikácia práv držiteľa certifikátu.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

Generácia 1:

tachographApplicationID je identifikátor aplikácie pre tachografovú aplikáciu.

Priradenie hodnôt: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Tento AID je chránený neregistrovaný identifikátor aplikácie v súlade s normou ISO/IEC 7816-5.

equipmentType je identifikácia typu zariadenia, pre ktoré je certifikát určený.

Priradenie hodnôt: v súlade s dátovým typom EquipmentType. **0** ak ide o certifikát členského štátu.

Generácia 2:

tachographApplicationID určuje 6 najvýznamnejších bajtov identifikátora (AID) aplikácie tachografovej karty generácie 2. AID aplikácie tachografovej karty je stanovený v kapitole 6.2.

Priradenie hodnôt: 'FF 53 4D 52 44 54'.

equipmentType je identifikácia typu zariadenia vymedzeného pre generáciu 2, pre ktoré je certifikát určený.

Priradenie hodnôt: v súlade s dátovým typom EquipmentType.

2.44. **CertificateRequestID**

Jedinečná identifikácia žiadosti o certifikát. Môže sa použiť aj ako identifikátor verejného kľúča jednotky vozidla, ak nie je v čase vygenerovania certifikátu známe sériové číslo jednotky vozidla, ktorej je kľúč určený.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber je sériové číslo žiadosti o certifikát jedinečné pre nasledujúceho výrobcu a mesiac.

requestMonthYear je identifikácia mesiaca a roku žiadosti o certifikát.

Priradenie hodnôt: BCD kódovanie mesiaca (dve číslice) a roku (dve posledné číslice).

crIdentifier: je identifikátor na rozlíšenie žiadosti o certifikát od rozšíreného sériového čísla.

Priradenie hodnôt: 'FFh'.

manufacturerCode: je numerický kód výrobcu, ktorý žiada o certifikát.

2.45. **CertificationAuthorityKID**

Identifikátor verejného kľúča certifikačnej autority (členský štát alebo Európsky certifikačný úrad).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric je numerický kód štátu certifikačnej autority.

nationAlpha je alfanumerický kód štátu certifikačnej autority.

keySerialNumber je sériové číslo na rozlíšenie rôznych kľúčov certifikačnej autority, ak sa kľúče zmenia.

additionalInfo je dvojbajtové pole pre doplnkové kódovanie (podľa certifikačnej autority).

caIdentifier je identifikátor na rozlíšenie identifikátora kľúča certifikačnej autority od iných identifikátorov kľúčov.

Priradenie hodnôt: '01h'

2.46. **CompanyActivityData**

Informácie uložené na podnikovej karte súvisiace s činnosťami, ktoré sa s kartou vykonávajú (požiadavka 373 a 379 v prílohe 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 je index naposledy aktualizovaného záznamu companyActivityRecord.

Priradenie hodnôt: číslo zodpovedajúce počítadlu záznamu o činnosti podniku začínajúce sa od '0' pre prvý výskyt záznamu o činnosti podniku v štruktúre.

companyActivityRecords je sada všetkých záznamov o činnosti podniku.

companyActivityRecord je sekvencia informácií súvisiacich s jednou činnosťou podniku.

companyActivityType je typ činnosti podniku.

companyActivityTime je dátum a čas činnosti podniku.

cardNumberInformation je číslo karty a vydávajúci členský štát prípadne sťahovanej karty.

vehicleRegistrationInformation je evidenčné číslo vozidla a členský štát evidencie vozidla, ktorého údaje sa sťahujú, blokujú alebo odblokúvajú.

downloadPeriodBegin a **downloadPeriodEnd** v prípade sťahovania je stiahnutý časový úsek z VU.

2.47. **CompanyActivityType**

Kód udávajúci činnosť vykonávanú podnikom s použitím podnikovej karty.

```
CompanyActivityType ::= INTEGER {
   card downloading                    (1),
   VU downloading                      (2),
   VU lock-in                          (3),
   VU lock-out                         (4)
}
```

2.48. **CompanyCardApplicationIdentification**

Informácie uložené na podnikovej karte súvisiace s identifikáciou aplikácie karty (požiadavky 369 a 375 v prílohe 1C).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId špecifikuje implementovaný typ karty.

cardStructureVersion špecifikuje verziu štruktúry, ktorá je implementovaná v karte.

noOfCompanyActivityRecords je počet záznamov o činnosti podniku, ktoré možno na karte uložiť.

2.49. **CompanyCardHolderIdentification**

Informácie uložené na podnikovej karte súvisiace s identifikáciou držiteľa karty (požiadavky 372 a 378 v prílohe 1C).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName je názov podniku, ktorý je držiteľom karty.

companyAddress je adresa podniku, ktorý je držiteľom karty.

cardHolderPreferredLanguage je preferovaný jazyk držiteľa karty.

2.50. **ControlCardApplicationIdentification**

Informácie uložené na kontrolnej karte súvisiace s identifikáciou aplikácie karty (požiadavky 357 a 363 v prílohe 1C).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId špecifikuje implementovaný typ karty.

cardStructureVersion špecifikuje verziu štruktúry, ktorá je implementovaná v karte.

noOfControlActivityRecords je počet záznamov o kontrolnej činnosti, ktoré možno na karte uložiť.

2.51. **ControlCardControlActivityData**

Informácie uložené na kontrolnej karte súvisiace s kontrolnými činnosťami, ktoré sa s kartou vykonávajú (požiadavka 361 a 367 v prílohe 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 je index naposledy aktualizovaného záznamu o kontrolnej činnosti.

Priradenie hodnôt: číslo zodpovedajúce počítadlu záznamu o kontrolnej činnosti začínajúce sa od '0' pre prvý výskyt záznamu o kontrolnej činnosti v štruktúre.

controlActivityRecords je sada všetkých záznamov o kontrolnej činnosti.

controlActivityRecord je sekvencia informácií súvisiacich s jednou kontrolou.

controlType je typ kontroly.

controlTime je dátum a čas kontroly.

controlledCardNumber je číslo karty a vydávajúci členský štát kontrolovanej karty.

controlledVehicleRegistration je evidenčné číslo vozidla (VRN) a členský štát evidencie kontrolovaného vozidla.

controlDownloadPeriodBegin a **controlDownloadPeriodEnd** je eventuálne sťahovaný časový úsek.

2.52. **ControlCardHolderIdentification**

Informácie uložené na kontrolnej karte súvisiace s identifikáciou držiteľa karty (požiadavky 360 a 366 v prílohe 1C).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                    Name,
   controlBodyAddress                 Address,
   cardHolderName                     HolderName,
   cardHolderPreferredLanguage        Language
}
```

controlBodyName je názov kontrolného orgánu držiteľa karty.

controlBodyAddress je adresa kontrolného orgánu držiteľa karty.

cardHolderName je priezvisko a meno(-á) držiteľa kontrolnej karty.

cardHolderPreferredLanguage je preferovaný jazyk držiteľa karty.

2.53. **ControlType**

Kód udávajúci činnosti vykonávané počas kontroly. Tento dátový typ súvisí s požiadavkami 126, 274, 299, 327 a 350 v prílohe 1C.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Generácia 1:

Priradenie hodnôt – usporiadaný oktet: 'cvpdxxxx'B (8 bitov)

'c'B sťahovanie karty:

'0'B: pri tejto kontrolnej činnosti karta nestiahnutá,

'1'B: pri tejto kontrolnej činnosti karta stiahnutá,

'v'B sťahovanie VU:

'0'B: pri tejto kontrolnej činnosti VU nestiahnutá,

'1'B: pri tejto kontrolnej činnosti VU stiahnutá,

'p'B tlač:

'0'B: pri tejto kontrolnej činnosti sa tlač nevykonáva,

'1'B: pri tejto kontrolnej činnosti sa tlač vykonáva,

'd'B zobrazenie:

'0'B: pri tejto kontrolnej činnosti sa nepoužíva zobrazenie,

'1'B: pri tejto kontrolnej činnosti sa používa zobrazenie

'xxxx'B Nepoužité.

Generácia 2:

Priradenie hodnôt – usporiadaný oktet: 'cvpdexxx'B (8 bitov)

'c'B sťahovanie karty:

'0'B: pri tejto kontrolnej činnosti karta nestiahnutá,

'1'B: pri tejto kontrolnej činnosti karta stiahnutá,

'v'B sťahovanie VU:

'0'B: pri tejto kontrolnej činnosti VU nestiahnutá,

'1'B: pri tejto kontrolnej činnosti VU stiahnutá,

'p'B tlač:

'0'B: pri tejto kontrolnej činnosti sa tlač nevykonáva,

'1'B: pri tejto kontrolnej činnosti sa tlač vykonáva,

'd'B zobrazenie:

'0'B: pri tejto kontrolnej činnosti sa nepoužíva zobrazenie,

'1'B: pri tejto kontrolnej činnosti sa používa zobrazenie

‘e’B	kontrola kalibrácie pri cestnej kontrole:
	‘0’B: pri tejto kontrolnej činnosti sa nekontrolujú kalibračné parametre
	‘1’B: pri tejto kontrolnej činnosti sa kontrolujú kalibračné parametre
‘xxx’B	Vyhradené na budúce použitie (RFU).

2.54. **CurrentDateTime**

Aktuálny dátum a čas záznamového zariadenia.

```
CurrentDateTime ::= TimeReal
```

Priradenie hodnôt: bližšie neurčené.

2.55. **CurrentDateTimeRecordArray**

Generácia 2:

Aktuálny dátum a čas plus metaúdaje použité v sťahovacom protokole.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType určuje typ záznamu (CurrentDateTime). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu CurrentDateTime v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o aktuálnom dátume a čase.

2.56. **DailyPresenceCounter**

Počítadlo uložené na karte vodiča alebo na dielenskej karte sa zvýši o 1 za každý kalendárny deň, v ktorom bola karta vložená vo VU. Tento dátový typ súvisí s požiadavkami 266, 299, 320 a 343 prílohy 1C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Priradenie hodnôt: postupné čísla s maximálnou hodnotou = 9 999, začínajúc opäť s 0. V čase prvého vydania karty je číslo nastavené na 0.

2.57. **Datef**

Dátum vyjadrený v ľahko vytlačiteľnom numerickom formáte.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Priradenie hodnôt:

yyyy	Rok
mm	Mesiac
dd	Deň
'00000000'H	označuje explicitne „žiadny dátum“.

2.58. **DateOfDayDownloaded**

Generácia 2:

Dátum a čas sťahovania.

```
DateOfDayDownloaded ::= TimeReal
```

Priradenie hodnôt: bližšie neurčené.

2.59. **DateOfDayDownloadedRecordArray**

Generácia 2:

Dátum a čas sťahovania plus metaúdaje použité v sťahovacom protokole.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType určuje typ záznamu (DateOfDayDownloaded). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu CurrentDateTime v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o dátume a čase sťahovania.

2.60. **Distance**

Prejdená vzdialenosť (výsledok výpočtu rozdielu medzi dvoma hodnotami počítadla stavu kilometrov v kilometroch).

```
Distance ::= INTEGER(0..2^16-1)
```

Priradenie hodnôt: dvojkové číslo bez znamienka. Hodnota v km v prevádzkovom rozsahu od 0 do 9 999 km.

2.61. **DriverCardApplicationIdentification**

Informácie uložené na karte vodiča súvisiace s identifikáciou aplikácie karty (požiadavky 253 a 278 v prílohe 1C).

Generácia 1:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId špecifikuje implementovaný typ karty.

cardStructureVersion špecifikuje verziu štruktúry, ktorá je implementovaná v karte.

noOfEventsPerType je počet udalostí pre každý typ udalosti, ktorý karta dokáže zaznamenať.

noOfFaultsPerType je počet porúch pre každý typ poruchy, ktorý karta dokáže zaznamenať.

activityStructureLength udáva počet bajtov, ktoré sú k dispozícii na uloženie záznamov o činnosti.

noOfCardVehicleRecords je počet záznamov o vozidle, ktoré môže karta obsahovať.

noOfCardPlaceRecords je počet miest, ktorý karta dokáže zaznamenať.

Generácia 2:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Oproti generácii 1 sa navyše použijú tieto dátové prvky:

noOfGNSSCDRecords je počet záznamov o nepretržitej jazde z GNSS, ktoré možno na karte uložiť.

noOfSpecificConditionRecords je počet záznamov o špecifických podmienkach, ktoré možno na karte uložiť.

2.62. DriverCardHolderIdentification

Informácie uložené na karte vodiča súvisiace s identifikáciou držiteľa karty (požiadavky 256 a 281 v prílohe 1C).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

cardHolderName je priezvisko a meno(-á) držiteľa karty vodiča.

cardHolderBirthDate je dátum narodenia držiteľa karty vodiča.

cardHolderPreferredLanguage je preferovaný jazyk držiteľa karty.

2.63. **DSRCSecurityData**

Generácia 2:

Informácie vo formáte nešifrovaného textu („plain text“) a MAC, ktoré sa majú preniesť cez DSRC z tachografu do diaľkového snímača (RI) – podrobnosti v dodatku 11 časti B kapitole 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 je súčasťou kódovania DER-TLV a nastaví sa na ‘81 10’ (pozri dodatok 11 časť B kapitolu 13).

currentDateTime je aktuálny dátum a čas jednotky vozidla.

counter je počítadlo správ RTM.

vuSerialNumber je sériové číslo jednotky vozidla.

dSRCMKVersionNumber je číslo verzie hlavného kľúča DSRC, z ktorého boli odvodené osobitné kľúče DSRC pre VU.

tagLengthMac je tag a dĺžka dátového objektu MAC v rámci kódovania DER-TLV. Tag sa nastaví na ‘8E’, dĺžka kóduje dĺžku MAC v oktetoch (pozri dodatok 11 časť B kapitolu 13).

mac je kód MAC vypočítaný pre správu RTM (pozri dodatok 11 časť B kapitolu 13).

2.64. **EGFCertificate**

Generácia 2:

Certifikát verejného kľúča externého zariadenia GNSS pre vzájomnú autentifikáciu s VU. Štruktúra tohto certifikátu je stanovená v dodatku 11.

```
EGFCertificate ::= Certificate
```

2.65. **EmbedderIcAssemblerId**

Poskytuje informácie o zhotoviteľovi integrovaného obvodu.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode je dvojpísmenný kód krajiny zostavovateľa modulu podľa normy ISO 3166.

moduleEmbedder identifikuje zostavovateľa modulu.

manufacturerInformation na interné účely výrobcu.

2.66. EntryTypeDailyWorkPeriod

Kód na rozlíšenie začiatku a konca zápisu denného pracovného času, miesta a podmienok zápisu.

Generácia 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)
}
```

Priradenie hodnôt: podľa normy ISO/IEC8824-1.

Generácia 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)
}
```

Priradenie hodnôt: podľa normy ISO/IEC8824-1.

2.67. EquipmentType

Kód na rozlíšenie typov zariadenia pre tachografovú aplikáciu.

```
EquipmentType ::= INTEGER(0..255)
```

Generácia 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)
```

Priradenie hodnôt: Podľa normy ISO/IEC8824-1.

Hodnota 0 je vyhradená na určenie členského štátu alebo Európy v certifikátoch v poli CHA.

Generácia 2:

Použijú sa rovnaké hodnoty ako v generácii 1, plus tieto dodatočné:

```
--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)
```

Poznámka: Hodnoty „Plaque“, „Adapter“ a „External GNSS connection“ v generácii 2, ako aj hodnoty „Vehicle Unit“ a „Motion Sensor“ v generácii 1 možno použiť v type SealRecord (ak sa uplatňuje).

2.68. **EuropeanPublicKey**

Generácia 1:

Európsky verejný kľúč.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Kód vysvetľujúci, prečo bola zaznamenaná udalosť alebo porucha.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Priradenie hodnôt:

‘00’H	jedna z 10 najnovších udalostí alebo porúch (alebo posledná)
‘01’H	najdlhšia udalosť za jeden z 10 posledných dní výskytu
‘02’H	jedna z 5 najdlhších udalostí za posledných 365 dní
‘03’H	posledná udalosť za jeden z 10 posledných dní výskytu
‘04’H	najzávažnejšia udalosť za jeden z 10 posledných dní výskytu
‘05’H	jedna z 5 najzávažnejších udalostí za posledných 365 dní
‘06’H	prvá udalosť alebo porucha, ku ktorej došlo po poslednej kalibrácii
'07'H	aktívna/prebiehajúca udalosť alebo porucha
‘08’H to ‘7F’H	vyhradené na budúce použitie (RFU)
‘80’H to ‘FF’H	špecifické podľa výrobcu

2.70. **EventFaultType**

Kód bližšie opisujúci udalosť alebo poruchu.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Priradenie hodnôt:

Generácia 1:

‘0x’H	Všeobecné udalosti,
‘00’H	Bez ďalších podrobností,
‘01’H	Vloženie neplatnej karty,
‘02’H	Konflikt karty,
‘03’H	Prekrývanie časov,
‘04’H	Jazda bez príslušnej karty,
‘05’H	Vloženie karty za jazdy,
‘06’H	Nesprávne uzavretá posledná relácia karty,
‘07’H	Prekročenie rýchlosti,
‘08’H	Prerušenie napájania,
‘09’H	Chyba údajov o pohybe,
‘0A’H	Nesúlad údajov o pohybe vozidla,
‘0B’ to ‘0F’H	vyhradené na budúce použitie (RFU),

	Pokusy o narušenie zabezpečenia v súvislosti s jednotkou vozidla,
‘1x’H	Bez ďalších podrobností,
‘10’H	Zlyhanie autentifikácie snímača pohybu,
‘11’H	Zlyhanie autentifikácie tachografovej karty,
‘12’H	Neoprávnená zmena snímača pohybu,
‘13’H	Chyba integrity vstupných údajov karty,
‘14’H	Chyba integrity uložených údajov o používateľovi,
‘15’H	Interná chyba prenosu údajov,
‘16’H	Neoprávnené otvorenie krytu,
‘17’H	Manipulácia s hardvérom,
‘18’H	RFU,
‘19’H to ‘1F’H	
‘2x’H	Pokusy o narušenie zabezpečenia v súvislosti so snímačom,
‘20’H	Bez ďalších podrobností,
‘21’H	Zlyhanie autentifikácie,
‘22’H	Chyba integrity uložených údajov,
‘23’H	Interná chyba prenosu údajov,
‘24’H	Neoprávnené otvorenie krytu,
‘25’H	Manipulácia s hardvérom,
‘26’H to ‘2F’H	RFU,
‘3x’H	Poruchy záznamového zariadenia,
‘30’H	Bez ďalších podrobností,
‘31’H	Interná porucha VU,
‘32’H	Porucha tlače,
‘33’H	Porucha zobrazenia,
‘34’H	Porucha sťahovania,
‘35’H	Porucha snímača,
‘36’H to ‘3F’H	RFU,
‘4x’H	Poruchy karty,
‘40’H	Bez ďalších podrobností,
‘41’H to ‘4F’H	RFU,
‘50’H to ‘7F’H	RFU,
‘80’H to ‘FF’H	Špecifické podľa výrobcu.

Generácia 2:

Použijú sa rovnaké hodnoty ako v generácii 1, plus tieto dodatočné:

‘0B’H	Časový konflikt (medzi GNSS a vstavanými hodinami VU),
‘0C’ to ‘0F’H	RFU,
‘5x’H	Poruchy spojené s GNSS,
‘50’H	Bez ďalších podrobností,
‘51’H	Interná porucha prijímača GNSS,
‘52’H	Externá porucha prijímača GNSS,
‘53’H	Externá porucha komunikácie GNSS,
‘54’H	Chýbajú údaje GNSS o polohe,
‘55’H	Zistená manipulácia GNSS,
‘56’H	Platnosť certifikátu externého zariadenia GNSS sa skončila,
‘57’H to ‘5F’H	RFU,
‘6x’H	Poruchy spojené s modulom diaľkovej komunikácie,
‘60’H	Bez ďalších podrobností,
‘61’H	Porucha modulu diaľkovej komunikácie,
‘62’H	Komunikačná porucha modulu diaľkovej komunikácie,
‘63’H to ‘6F’H	RFU,
‘7x’H	Poruchy rozhrania ITS,
‘70’H	Bez ďalších podrobností,
‘71’H to ‘7F’H	RFU.

2.71. **ExtendedSealIdentifier**

Generácia 2:

Rozšírený identifikátor plomby jednoznačne identifikuje plombu (požiadavka 401 v prílohe 1C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode: je kód výrobcu plomby.

sealIdentifier je identifikátor plomby jedinečný pre daného výrobcu.

2.72. **ExtendedSerialNumber**

Jedinečná identifikácia zariadenia. Môže sa použiť aj ako identifikátor verejného kľúča zariadenia.

Generácia 1:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber je sériové číslo zariadenia jedinečné pre výrobcu, typ zariadenia a mesiac a rok uvedený nižšie.

monthYear je identifikácia mesiaca a roku výroby (alebo pridelenia sériového čísla).

Priradenie hodnôt: BCD kódovanie mesiaca (dve číslice) a roku (dve posledné číslice).

type je identifikátor typu zariadenia.

Priradenie hodnôt: špecifické podľa výrobcu, s vyhradenou hodnotou 'FFh'.

manufacturerCode: je numerický kód identifikujúci výrobcu typovo schváleného zariadenia.

Generácia 2:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                EquipmentType,
   manufacturerCode                    ManufacturerCode
}
```

serialNumber pozri generáciu 1

monthYear pozri generáciu 1

type udáva typ zariadenia

manufacturerCode: pozri generáciu 1.

2.73. **FullCardNumber**

Kód na úplnú identifikáciu tachografovej karty.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType je typ tachografovej karty.

cardIssuingMemberState je kód členského štátu, ktorý kartu vydal.

cardNumber je číslo karty.

2.74. **FullCardNumberAndGeneration**

Generácia 2:

Kód na úplnú identifikáciu tachografovej karty a jej generácie.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identifikuje tachografovú kartu.

generation udáva generáciu použitej tachografovej karty.

2.75. **Generation**

Generácia 2:

Udáva generáciu použitého tachografu.

```
Generation ::= INTEGER(0..255)
```

Priradenie hodnôt:

'00'H	Vyhradené na budúce použitie (RFU)
'01'H	Generácia 1
'02'H	Generácia 2
'03'H .. 'FF'H	RFU

2.76. **GeoCoordinates**

Generácia 2:

Geo-súradnice sa kódujú ako celé čísla (integer) Ide o násobky kódovania ±DDMM.M pre zemepisnú šírku a ±DDDMM.M pre zemepisnú dĺžku. ±DD a ±DDD tu určuje stupne a MM.M minúty.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude (zemepisná šírka) je kódovaná ako násobok (faktor 10) zápisu ±DDMM.M.

longitude (zemepisná dĺžka) je kódovaná ako násobok (faktor 10) zápisu ±DDDMM.M.

2.77. **GNSSAccuracy**

Generácia 2:

Presnosť údajov GNSS o polohe (vymedzenie pojmov, písm. eee)). Táto presnosť je kódovaná ako celé číslo a je násobkom (faktor 10) hodnoty X.Y z vety GSA NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Generácia 2:

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k polohe vozidla podľa GNSS, ak vodičov nepretržitý čas jazdy dosiahne násobok troch hodín (požiadavky 306 a 354 v prílohe 1C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord            INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords         SET SIZE(NoOfGNSSCDRecords) OF
                                        GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord je index naposledy aktualizovaného záznamu GNSS o nepretržitej jazde.

Priradenie hodnôt: číslo zodpovedajúce počítadlu záznamu GNSS o nepretržitej jazde začínajúce sa od '0' pre prvý výskyt záznamu GNSS o nepretržitej jazde v štruktúre.

gnssContinuousDrivingRecords je sada záznamov obsahujúcich dátum a čas, keď nepretržitá jazda dosiahne násobok troch hodín, ako aj informácie o polohe vozidla.

2.79. **GNSSContinuousDrivingRecord**

Generácia 2:

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k polohe vozidla podľa GNSS, ak vodičov nepretržitý čas jazdy dosiahne násobok troch hodín (požiadavky 305 a 353 v prílohe 1C).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssPlaceRecord                      GNSSPlaceRecord
}
```

timeStamp je dátum a čas, keď nepretržitý čas jazdy držiteľa karty dosiahne násobok troch hodín.

gnssPlaceRecord obsahuje informácie o polohe vozidla.

2.80. **GNSSPlaceRecord**

Generácia 2:

Informácie súvisiace s polohou vozidla podľa GNSS (požiadavky 108, 109, 110, 296, 305, 347 a 353 v prílohe 1C).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssAccuracy                         GNSSAccuracy,
   geoCoordinates                       GeoCoordinates
}
```

timeStamp je dátum a čas určenia polohy vozidla podľa GNSS.

gnssAccuracy je presnosť údajov GNSS o polohe.

geoCoordinates je poloha zaznamenaná pomocou GNSS.

2.81. **HighResOdometer**

Stav kilometrov udávaný počítadlom vozidla: Akumulovaná vzdialenosť prejdená vozidlom počas prevádzky.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Priradenie hodnôt: dvojkové číslo bez znamienka. Hodnota v 1/200 km v prevádzkovom rozsahu od 0 do 21 055 406 km.

2.82. **HighResTripDistance**

Vzdialenosť prejdená v rámci celej cesty alebo jej časti.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Priradenie hodnôt: dvojkové číslo bez znamienka. Hodnota v 1/200 km v prevádzkovom rozsahu od 0 do 21 055 406 km.

2.83. **HolderName**

Priezvisko a meno(-á) držiteľa karty.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname je priezvisko držiteľa. Nezahŕňa tituly.

Priradenie hodnôt: Pokiaľ nejde o kartu vydanú určitej osobe, holderSurname obsahuje rovnaké informácie ako companyName, workshopName alebo controlBodyName.

holderFirstNames – krstné meno(-á) a iniciály držiteľa.

2.84. **InternalGNSSReceiver**

Generácia 2:

Informácia o tom, či je prijímač GNSS integrovaný v jednotke vozidla, alebo je externý. True znamená, že prijímač GNSS je integrovaný vo VU. False znamená, že ide o externý prijímač GNSS.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Konštanta záznamového zariadenia (vymedzenie pojmov, písm. m)).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Priradenie hodnôt: Impulzy na kilometer v prevádzkovom rozsahu 0 až 64 255 impulzov/km.

2.86. **KeyIdentifier**

Jedinečný identifikátor verejného kľúča použitý ako odkaz na kľúč a na jeho voľbu. Zároveň identifikuje držiteľa kľúča.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber                ExtendedSerialNumber,
   certificateRequestID                CertificateRequestID,
   certificationAuthorityKID           CertificationAuthorityKID
}
```

Prvá voľba je vhodná ako odkaz na verejný kľúč jednotky vozidla alebo tachografovej karty.

Druhá voľba je vhodná ako odkaz na verejný kľúč jednotky vozidla (ak sériové číslo jednotky vozidla nie je známe v čase generovania certifikátu).

Tretia voľba je vhodná ako odkaz na verejný kľúč členského štátu.

2.87. **KMWCKey**

Generácia 2:

Kľúč AES a príslušná verzia kľúča použité pri párovaní VU a snímača pohybu. Podrobnosti sú uvedené v dodatku 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                             AESKey,
   keyVersion                          INTEGER (SIZE(1))
}
```

kMWCKey je dĺžka kľúča AES zreťazená s kľúčom, ktorý sa používa na párovanie VU a snímača pohybu.

keyVersion určuje verziu kľúča AES.

2.88. **Language**

Kód identifikujúci jazyk.

```
Language ::= IA5String(SIZE(2))
```

Priradenie hodnôt: dve malé písmená, kódovanie podľa normy ISO 639.

2.89. **LastCardDownload**

Dátum a čas posledného sťahovania údajov z karty, uložené na karte vodiča (na iné účely než kontrolu), požiadavky 257 a 282 v prílohe 1C. Tento dátum môže aktualizovať VU alebo akákoľvek čítačka kariet.

```
LastCardDownload ::= TimeReal
```

Priradenie hodnôt: bližšie neurčené.

2.90. **LinkCertificate**

Generácia 2:

Certifikát prepojenia medzi kľúčovými pármi Európskeho úradu prvotnej certifikácie (ERCA).

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Skutočný obvod pneumatík kolies (vymedzenie pojmov, písm. u)).

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

Priradenie hodnôt: dvojkové číslo bez znamienka, hodnota v 1/8 mm v prevádzkovom rozsahu od 0 do 8 031 mm.

2.92. **MAC**

Generácia 2:

Kryptografický kontrolný súčet dĺžky 8, 12 alebo 16 bajtov podľa šifrovacích zostáv uvedených v dodatku 11.

```
MAC ::= CHOICE {
   mac8                                 OCTET STRING (SIZE(8)),
   mac12                                OCTET STRING (SIZE(12)),
   mac16                                OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Kód určujúci, či držiteľ karty pri vložení karty manuálne zadal činnosti vodiča alebo nie (požiadavka 081 v prílohe 1B a požiadavka 102 v prílohe 1C).

```
ManualInputFlag ::= INTEGER {
   noEntry                              (0)
   manualEntries                        (1)
}
```

Priradenie hodnôt: bližšie neurčené.

2.94. **ManufacturerCode**

Kód identifikujúci výrobcu typovo schváleného zariadenia.

```
ManufacturerCode ::= INTEGER(0..255)
```

Skúšobňa oprávnená na vykonávanie skúšok interoperability vedie a uverejňuje na svojej webovej stránke zoznam kódov výrobcov (požiadavka 454 v prílohe 1C).

Kódy výrobcov sa spoločnostiam vyvíjajúcim tachografické zariadenia prideľujú dočasne na základe žiadosti predloženej skúšobni oprávnenej vykonávať skúšky interoperability.

2.95. **ManufacturerSpecificEventFaultData**

Generácia 2:

Chybové kódy výrobcu uľahčujú analýzu chýb a údržbu jednotiek vozidla.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                     ManufacturerCode,
   manufacturerSpecificErrorCode        OCTET STRING(SIZE(3))
}
```

manufacturerCode identifikuje výrobcu jednotky vozidla.

manufacturerSpecificErrorCode je chybový kód špecifický pre daného výrobcu.

2.96. **MemberStateCertificate**

Certifikát verejného kľúča členského štátu vydaný európskou certifikačnou autoritou.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Generácia 2:

Certifikát členského štátu plus metaúdaje použité v sťahovacom protokole.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType určuje typ záznamu (MemberStateCertificate). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu MemberStateCertificate v bajtoch.

noOfRecords je počet záznamov v sade. Hodnota sa nastaví na 1, keďže certifikáty môžu mať rôznu dĺžku.

records je sada certifikátov členských štátov.

2.98. **MemberStatePublicKey**

Generácia 1:

Verejný kľúč členského štátu.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Názov.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage určuje množinu znakov vymedzenú v kapitole 4,

name je názov kódovaný špecifikovanou množinou znakov.

2.100. **NationAlpha**

Písmenné označenie krajiny musí byť v súlade s rozlišujúcimi značkami používanými na vozidlách v medzinárodnej doprave (Viedenský dohovor Organizácie Spojených národov o cestnej premávke, 1968).

```
NationAlpha ::= IA5String(SIZE(3))
```

Písmenné a číselné kódy krajín sa uvádzajú na zozname vedenom na webovej stránke skúšobne oprávnenej vykonávať skúšky interoperability podľa požiadavky 440 v prílohe 1C.

2.101. **NationNumeric**

Číselné označenie krajiny.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Priradenie hodnôt: pozri dátový typ 2.100 (NationAlpha).

Všetky zmeny alebo aktualizácie špecifikácie abecedných a číselných kódov krajín uvedených v predchádzajúcom odseku sa vykonajú až potom, čo určená skúšobňa získa stanoviská od výrobcov typovo schválených VU digitálnych a inteligentných tachografov.

2.102. **NoOfCalibrationRecords**

Počet kalibračných záznamov, ktoré možno uložiť na dielenskej karte.

Generácia 1:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Priradenie hodnôt: pozri dodatok 2.

Generácia 2:

$$\texttt{NoOfCalibrationRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Priradenie hodnôt: pozri dodatok 2.

2.103. **NoOfCalibrationsSinceDownload**

Počítadlo udávajúce počet kalibrácií vykonaných s dielenskou kartou od posledného stiahnutia (požiadavka 317 a 340 v prílohe 1C).

$$\texttt{NoOfCalibrationsSinceDownload ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Priradenie hodnôt: nie je bližšie špecifikované.

2.104. **NoOfCardPlaceRecords**

Počet záznamov o mieste, ktoré môžu byť uložené na karte vodiča alebo na dielenskej karte.

Generácia 1:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Priradenie hodnôt: pozri dodatok 2.

Generácia 2:

$$\texttt{NoOfCardPlaceRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Priradenie hodnôt: pozri dodatok 2.

2.105. **NoOfCardVehicleRecords**

Počet záznamov o použitých vozidlách, ktoré možno uložiť na karte vodiča alebo na dielenskej karte.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Priradenie hodnôt: pozri dodatok 2.

2.106. **NoOfCardVehicleUnitRecords**

Generácia 2:

Počet záznamov o použitých jednotkách vozidla, ktoré možno uložiť na karte vodiča alebo na dielenskej karte.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Priradenie hodnôt: pozri dodatok 2.

2.107. **NoOfCompanyActivityRecords**

Počet záznamov o činnosti podniku, ktoré možno uložiť na dielenskej karte.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Priradenie hodnôt: pozri dodatok 2.

2.108. **NoOfControlActivityRecords**

Počet záznamov o kontrolnej činnosti, ktoré možno uložiť na kontrolnej karte.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Priradenie hodnôt: pozri dodatok 2.

2.109. **NoOfEventsPerType**

Počet udalostí každého typu, ktoré možno uložiť na karte.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Priradenie hodnôt: pozri dodatok 2.

2.110. **NoOfFaultsPerType**

Počet porúch každého typu, ktoré možno uložiť na karte.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Priradenie hodnôt: pozri dodatok 2.

2.111. **NoOfGNSSCDRecords**

Generácia 2:

Počet záznamov o nepretržitej jazde z GNSS, ktoré možno na karte uložiť.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Priradenie hodnôt: pozri dodatok 2.

2.112. **NoOfSpecificConditionRecords**

Generácia 2:

Počet záznamov o špecifických podmienkach, ktoré možno na karte uložiť.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Priradenie hodnôt: pozri dodatok 2.

2.113. **OdometerShort**

Skrátený zápis stavu počítadla kilometrov vozidla.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Priradenie hodnôt: dvojkové číslo bez znamienka. Hodnota v km v prevádzkovom rozsahu od 0 do 9 999 999 km.

2.114. **OdometerValueMidnight**

Hodnota počítadla kilometrov o polnoci daného dňa (požiadavka 090 v prílohe 1B a požiadavka 113 v prílohe 1C).

```
OdometerValueMidnight ::= OdometerShort
```

Priradenie hodnôt: bližšie neurčené.

2.115. **OdometerValueMidnightRecordArray**

Generácia 2:

OdometerValueMidnight plus metaúdaje použité v sťahovacom protokole.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType určuje typ záznamu (OdometerValueMidnight). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu OdometerValueMidnight v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov OdometerValueMidnight.

2.116. **OverspeedNumber**

Počet prekročení rýchlosti od poslednej kontroly prekročenia rýchlosti.

```
OverspeedNumber ::= INTEGER(0..255)
```

Priradenie hodnôt: 0 znamená, že od poslednej kontroly prekročenia rýchlosti nebola prekročená rýchlosť, 1 znamená, že od poslednej kontroly bola rýchlosť prekročená raz … 255 znamená, že od poslednej kontroly bola rýchlosť prekročená 255 krát alebo viac.

2.117. **PlaceRecord**

Informácie o mieste, kde sa začína alebo končí denný pracovný čas (požiadavky 108, 271, 296, 324 a 347 v prílohe 1C).

Generácia 1:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort
}
```

entryTime je dátum a čas vzťahujúci sa k zápisu.

entryTypeDailyWorkPeriod je typ zápisu.

dailyWorkPeriodCountry je zapísaná krajina.

dailyWorkPeriodRegion je zapísaný región.

vehicleOdometerValue je stav počítadla kilometrov v čase zápisu miesta.

Generácia 2:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort,
   entryGNSSPlaceRecord               GNSSPlaceRecord
}
```

Oproti generácii 1 sa navyše použije tento komponent:

entryGNSSPlaceRecord je zaznamenaná poloha a čas.

2.118. **PreviousVehicleInfo**

Informácie vzťahujúce sa k predchádzajúcemu vozidlu použitému vodičom pri vložení jeho karty do jednotky vozidla (požiadavka 081 v prílohe 1B a požiadavka 102 v prílohe 1C).

Generácia 1:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification je evidenčné číslo vozidla a členský štát evidencie vozidla.

cardWithdrawalTime je dátum a čas vytiahnutia karty.

Generácia 2:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Oproti generácii 1 sa navyše použije tento dátový prvok:

vuGeneration identifikuje generáciu jednotky vozidla.

2.119. **PublicKey**

Generácia 1:

Verejný kľúč RSA.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                    RSAKeyModulus,
   rsaKeyPublicExponent             RSAKeyPublicExponent
}
```

rsaKeyModulus je modul kľúčového páru.

rsaKeyPublicExponent je verejný exponent kľúčového páru.

2.120. **RecordType**

Generácia 2:

Odkaz na typ záznamu. Tento dátový typ sa používa v RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

Priradenie hodnôt:

'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	Špecifické podľa výrobcu.

2.121. **RegionAlpha**

Písmenné označenie regiónu v špecifikovanej krajine.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Generácia 1:

Priradenie hodnôt:

```
‘   ’        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
```

Generácia 2:

Kódy RegionAlpha sa uvádzajú na zozname vedenom na webovej stránke skúšobne oprávnenej vykonávať skúšky interoperability.

2.122. **RegionNumeric**

Číselné označenie regiónu v špecifikovanej krajine.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Generácia 1:

Priradenie hodnôt:

```
‘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
```

Generácia 2:

Kódy RegionNumeric sa uvádzajú na zozname vedenom na webovej stránke skúšobne oprávnenej vykonávať skúšky interoperability.

2.123. **RemoteCommunicationModuleSerialNumber**

Generácia 2:

Sériové číslo modulu diaľkovej komunikácie.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Generácia 1:

Modul kľúčového páru RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Priradenie hodnôt: Neurčené.

2.125. **RSAKeyPrivateExponent**

Generácia 1:

Súkromný exponent kľúčového páru RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Priradenie hodnôt: Neurčené.

2.126. **RSAKeyPublicExponent**

Generácia 1:

Verejný exponent kľúčového páru RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Priradenie hodnôt: Neurčené.

2.127. **RtmData**

Generácia 2:

Tento dátový typ je vymedzený v dodatku 14.

2.128. **SealDataCard**

Generácia 2:

Tento dátový typ ukladá informácie o plombách na rôznych dieloch vozidla a je určený na uloženie na karte. Tento dátový typ sa vzťahuje k požiadavke 337 v prílohe 1C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords je počet záznamov v sealRecords.

sealRecords je sada záznamov o plombách.

2.129. **SealDataVu**

Generácia 2:

Tento dátový typ ukladá informácie o plombách na rôznych dieloch vozidla a je určený na uloženie v jednotke vozidla.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords je sada záznamov o plombách. Ak je k dispozícii menej než 5 plomb, hodnota EquipmentType vo všetkých nepoužitých záznamoch sealRecords sa nastaví na 16 – nepoužité.

2.130. **SealRecord**

Generácia 2:

Tento dátový typ ukladá informácie o plombe pripojenej k dielu. Tento dátový typ sa vzťahuje k požiadavke 337 v prílohe 1C.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType určuje typ zariadenia, ku ktorému je plomba pripojená.

extendedSealIdentifier je identifikátor plomby pripojenej k danému zariadeniu.

2.131. **SensorApprovalNumber**

Číslo typového schválenia snímača.

Generácia 1:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Priradenie hodnôt: Neurčené.

Generácia 2:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Priradenie hodnôt:

Schvaľovacie číslo sa uvedie tak, ako je uverejnené na príslušných webových stránkach Európskej komisie, t. j. napríklad vrátane prípadných pomlčiek. Schvaľovacie číslo schválenia sa zarovná vľavo.

2.132. **SensorExternalGNSSApprovalNumber**

Generácia 2:

Číslo typového schválenia vonkajšieho zariadenia GNSS.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Priradenie hodnôt:

Schvaľovacie číslo sa uvedie tak, ako je uverejnené na príslušných webových stránkach Európskej komisie, t. j. napríklad vrátane prípadných pomlčiek. Schvaľovacie číslo schválenia sa zarovná vľavo.

2.133. **SensorExternalGNSSCoupledRecord**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú identifikácie externého zariadenia GNSS spojeného s jednotkou vozidla (požiadavka 100 v prílohe 1C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber je sériové číslo externého zariadenia GNSS spojeného s jednotkou vozidla.

sensorApprovalNumber je schvaľovacie číslo tohto externého zariadenia GNSS.

sensorCouplingDate je dátum spojenia tohto externého zariadenia GNSS s jednotkou vozidla.

2.134. **SensorExternalGNSSIdentification**

Generácia 2:

Informácie týkajúce sa identifikácie externého zariadenia GNSS (požiadavka 98 v prílohe 1C).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber je rozšírené sériové číslo externého zariadenia GNSS.

sensorApprovalNumber je schvaľovacie číslo externého zariadenia GNSS.

sensorSCIdentifier je identifikátor bezpečnostného komponentu externého zariadenia GNSS.

sensorOSIdentifier je identifikátor operačného systému externého zariadenia GNSS.

2.135. **SensorExternalGNSSInstallation**

Generácia 2:

Informácie uložené na externom zariadení GNSS, ktoré sa týkajú inštalácie externého snímača GNSS (požiadavka 123 v prílohe 1C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst je dátum prvého spojenia externého zariadenia GNSS s jednotkou vozidla.

firstVuApprovalNumber je schvaľovacie číslo prvej jednotky vozidla spojenej s externým zariadením GNSS.

firstVuSerialNumber je sériové číslo prvej jednotky vozidla spárovanej s externým zariadením GNSS.

sensorCouplingDateCurrent je dátum aktuálneho spojenia externého zariadenia GNSS s jednotkou vozidla.

currentVuApprovalNumber je schvaľovacie číslo jednotky vozidla aktuálne spojenej s externým zariadením GNSS.

currentVUSerialNumber je sériové číslo jednotky vozidla aktuálne spojenej s externým zariadením GNSS.

2.136. **SensorExternalGNSSOSIdentifier**

Generácia 2:

Identifikátor operačného systému externého zariadenia GNSS.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Priradenie hodnôt: špecifické podľa výrobcu.

2.137. **SensorExternalGNSSSCIdentifier**

Generácia 2:

Tento typ sa používa napr. na identifikáciu kryptografického modulu externého zariadenia GNSS.

Identifikátor bezpečnostného komponentu externého zariadenia GNSS.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Priradenie hodnôt: špecifické podľa výrobcu komponentu.

2.138. **SensorGNSSCouplingDate**

Generácia 2:

Dátum spojenia externého zariadenia GNSS s jednotkou vozidla.

```
SensorGNSSCouplingDate ::= TimeReal
```

Priradenie hodnôt: Neurčené.

2.139. **SensorGNSSSerialNumber**

Generácia 2:

Tento typ sa používa na uloženie sériového čísla prijímača GNSS, či už je vo vnútri VU alebo mimo.

Sériové číslo prijímača GNSS.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Informácie uložené v snímači pohybu, ktoré sa vzťahujú k identifikácii snímača pohybu (požiadavka 077 v prílohe 1B a požiadavka 95 v prílohe 1C).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                SensorSerialNumber,
   sensorApprovalNumber              SensorApprovalNumber,
   sensorSCIdentifier                SensorSCIdentifier,
   sensorOSIdentifier                SensorOSIdentifier
}
```

sensorSerialNumber je rozšírené sériové číslo snímača pohybu (zahŕňa číslo dielu aj kód výrobcu).

sensorApprovalNumber je schvaľovacie číslo snímača pohybu.

sensorSCIdentifier je identifikátor bezpečnostného komponentu snímača pohybu.

sensorOSIdentifier je identifikátor operačného systému snímača pohybu.

2.141. **SensorInstallation**

Informácie uložené v snímači pohybu, ktoré sa vzťahujú k montáži snímača pohybu (požiadavka 099 v prílohe 1B a požiadavka 122 v prílohe 1C).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst            SensorPairingDate,
   firstVuApprovalNumber             VuApprovalNumber,
   firstVuSerialNumber               VuSerialNumber,
   sensorPairingDateCurrent          SensorPairingDate,
   currentVuApprovalNumber           VuApprovalNumber,
   currentVUSerialNumber             VuSerialNumber
}
```

sensorPairingDateFirst je dátum prvého párovania snímača pohybu s jednotkou vozidla.

firstVuApprovalNumber je schvaľovacie číslo prvej jednotky vozidla spárovanej so snímačom pohybu.

firstVuSerialNumber je sériové číslo prvej jednotky vozidla spárovanej so snímačom pohybu.

sensorPairingDateCurrent je dátum aktuálneho párovania snímača pohybu s jednotkou vozidla.

currentVuApprovalNumber je schvaľovacie číslo jednotky vozidla aktuálne spárovanej so snímačom pohybu.

currentVUSerialNumber je sériové číslo jednotky vozidla aktuálne spárovanej so snímačom pohybu.

2.142. **SensorInstallationSecData**

Informácie uložené na dielenskej karte, ktoré sa vzťahujú k bezpečnostným údajom potrebným na párovanie snímačov pohybu s jednotkami vozidla (požiadavky 308 a 331 v prílohe 1C).

Generácia 1:

```
SensorInstallationSecData ::= TdesSessionKey
```

Priradenie hodnôt: v súlade s normou ISO 16844-3.

Generácia 2:

Ako je opísané v dodatku 11, dielenská karta musí byť schopná uložiť až tri kľúče pre párovanie VU a snímača pohybu. Tieto kľúče majú rôzne verzie.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                           KMWCKey,
   kMWCKey2                           KMWCKey OPTIONAL,
   kMWCKey3                           KMWCKey OPTIONAL
}
```

2.143. **SensorOSIdentifier**

Identifikátor operačného systému snímača pohybu.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Priradenie hodnôt: špecifické podľa výrobcu.

2.144. **SensorPaired**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú identifikácie snímača pohybu spárovaného s jednotkou vozidla (požiadavka 079 v prílohe 1B).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                 SensorSerialNumber,
   sensorApprovalNumber               SensorApprovalNumber,
   sensorPairingDateFirst             SensorPairingDate
}
```

sensorSerialNumber je sériové číslo snímača pohybu aktuálne spárovaného s jednotkou vozidla.

sensorApprovalNumber je schvaľovacie číslo snímača pohybu aktuálne spárovaného s jednotkou vozidla.

sensorPairingDateFirst je dátum prvého párovania snímača pohybu s jednotkou vozidla, s ktorou je v súčasnosti spárovaný.

2.145. **SensorPairedRecord**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú identifikácie snímača pohybu spárovaného s jednotkou vozidla (požiadavka 97 v prílohe 1C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber je sériové číslo snímača pohybu spárovaného s jednotkou vozidla.

sensorApprovalNumber je schvaľovacie číslo tohto snímača pohybu.

sensorPairingDate je dátum párovania tohto snímača pohybu s jednotkou vozidla.

2.146. **SensorPairingDate**

Dátum párovania snímača pohybu s jednotkou vozidla.

```
SensorPairingDate ::= TimeReal
```

Priradenie hodnôt: Neurčené.

2.147. **SensorSCIdentifier**

Identifikátor bezpečnostného komponentu snímača pohybu.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Priradenie hodnôt: špecifické podľa výrobcu komponentu.

2.148. **SensorSerialNumber**

Sériové číslo snímača pohybu.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Digitálny podpis.

Generácia 1:

```
Signature ::= OCTET STRING (SIZE(128))
```

Priradenie hodnôt: v súlade s dodatkom 11 Spoločné bezpečnostné mechanizmy.

Generácia 2:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Priradenie hodnôt: v súlade s dodatkom 11 Spoločné bezpečnostné mechanizmy.

2.150. **SignatureRecordArray**

Generácia 2:

Sada podpisov plus metaúdaje použité v sťahovacom protokole.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType určuje typ záznamu (Signature). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu Signature v bajtoch.

noOfRecords je počet záznamov v sade. Hodnota sa nastaví na 1, keďže podpisy môžu mať rôznu dĺžku.

records je sada podpisov.

2.151. **SimilarEventsNumber**

Počet podobných udalostí v jednom určitom dni (požiadavka 094 v prílohe 1B a požiadavka 117 v prílohe 1C).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Priradenie hodnôt: 0 sa nepoužije, 1 znamená, že v uvedenom dni nastala a bola uložená len jedna udalosť daného typu, 2 znamená, že v uvedenom dni nastali dve udalosti daného typu (len jedna bola uložená), … 255 znamená, že v uvedenom dni nastalo 255 alebo viac udalostí daného typu.

2.152. **SpecificConditionRecord**

Informácie uložené na karte vodiča, dielenskej karte alebo v jednotke vozidla, ktoré sa vzťahujú k špecifickej podmienke (požiadavky 130, 276, 301, 328 a 355 v prílohe 1C).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                           TimeReal,
   specificConditionType               SpecificConditionType
}
```

entryTime je dátum a čas zápisu.

specificConditionType je kód identifikujúci špecifickú podmienku.

2.153. **SpecificConditions**

Informácie uložené na karte vodiča, dielenskej karte alebo v jednotke vozidla, ktoré sa vzťahujú k špecifickej podmienke (požiadavky 131, 277, 302, 329 a 356 v prílohe 1C).

Generácia 2:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                       SpecificConditionRecord
}
```

conditionPointerNewestRecord je index naposledy aktualizovaného záznamu o špecifickej podmienke.

Priradenie hodnôt: číslo zodpovedajúce počítadlu záznamu o špecifickej podmienke začínajúce sa od '0' pre prvý výskyt záznamu o špecifickej podmienke v štruktúre.

specificConditionRecords je sada záznamov obsahujúcich informácie o zaznamenaných špecifických podmienkach.

2.154. **SpecificConditionType**

Kód identifikujúci špecifickú podmienku (požiadavky 050b, 105a, 212a a 230a v prílohe 1B a požiadavka 62 v prílohe 1C).

```
SpecificConditionType ::= INTEGER(0..255)
```

Generácia 1:

Priradenie hodnôt:

'00'H	Vyhradené na budúce použitie (RFU)
'01'H	Záznamové zariadenie sa nevyžaduje – začiatok
'02'H	Záznamové zariadenie sa nevyžaduje – koniec
'03'H	Prevoz trajektom / vlakom
'04'H .. 'FF'H	RFU

Generácia 2:

Priradenie hodnôt:

'00'H	Vyhradené na budúce použitie (RFU)
'01'H	Záznamové zariadenie sa nevyžaduje – začiatok
'02'H	Záznamové zariadenie sa nevyžaduje – koniec
'03'H	Prevoz trajektom / vlakom – začiatok
'04'H	Prevoz trajektom / vlakom – koniec
'05'H .. 'FF'H	RFU

2.155. **Speed**

Rýchlosť vozidla (km/h).

```
Speed ::= INTEGER(0..255)
```

Priradenie hodnôt: kilometre za hodinu v prevádzkovom rozsahu od 0 do 220 km/h.

2.156. **SpeedAuthorised**

Maximálna povolená rýchlosť vozidla (vymedzenie pojmov, písm. hh)).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Priemerná rýchlosť vo vopred stanovenom časovom úseku (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Maximálna rýchlosť nameraná vo vopred stanovenom časovom úseku.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Generácia 2:

Tento dátový typ je vymedzený v dodatku 14.

2.160. **TachographPayloadEncrypted**

Generácia 2:

Obsah tachografu šifrovaný v DER-TLV, t. j. odosielané údaje šifrované v správe RTM. Šifrovanie je opísané v dodatku 11 časti B kapitole 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 je súčasťou kódovania DER-TLV a nastaví sa na '87' (pozri dodatok 11 časť B kapitolu 13).

length je súčasťou kódovania DER-TLV a kóduje dĺžku nasledujúceho paddingContentIndicatorByte a údajov encryptedData.

paddingContentIndicatorByte sa nastaví na '00'.

encryptedData sú šifrované údaje tachographPayload podľa dodatku 11 časti B kapitoly 13. Dĺžka týchto údajov v oktetoch musí vždy byť násobkom 16.

2.161. **TDesSessionKey**

Generácia 1:

Trojnásobný relačný kľúč DES.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Priradenie hodnôt: bližšie neurčené.

2.162. **TimeReal**

Kód pre kombinované pole s dátumom a časom, kde je dátum a čas vyjadrený ako sekundy po 1. januári 1970 00h.00m.00s. GMT.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Priradenie hodnôt – usporiadaný oktet: počet sekúnd od polnoci 1. januára 1970 GMT.

Maximálny možný dátum/čas je rok 2106.

2.163. **TyreSize**

Určenie rozmerov pneumatík.

```
TyreSize ::= IA5String(SIZE(15))
```

Priradenie hodnôt: v súlade so smernicou 92/23 (EHS) 31/03/92 Ú. v. ES L129 s.95.

2.164. **VehicleIdentificationNumber**

Identifikačné číslo vozidla (VIN) vzťahujúce sa k vozidlu ako celku, spravidla sériové číslo podvozku alebo rámu.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Priradenie hodnôt: podľa normy ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Generácia 2:

Identifikačné číslo vozidla (VIN) plus metaúdaje použité v sťahovacom protokole.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType určuje typ záznamu (VehicleIdentificationNumber). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VehicleIdentificationNumber v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada čísel VIN.

2.166. **VehicleRegistrationIdentification**

Identifikácia vozidla jedinečná pre Európu (evidenčné číslo vozidla – VRN a členský štát).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation je štát, kde je vozidlo zaevidované.

vehicleRegistrationNumber je evidenčné číslo vozidla (VRN).

2.167. **VehicleRegistrationNumber**

Evidenčné číslo vozidla (VRN). Evidenčné číslo prideľuje oprávnený orgán registrácie.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   vehicleRegNumber                    OCTET STRING (SIZE(13))
}
```

codePage určuje množinu znakov vymedzenú v kapitole 4,

vehicleRegNumber je VRN kódované špecifikovanou množinou znakov.

Priradenie hodnôt: špecifické podľa krajiny.

2.168. **VehicleRegistrationNumberRecordArray**

Generácia 2:

Evidenčné číslo vozidla plus metaúdaje použité v sťahovacom protokole.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleRegistrationNumber
}
```

recordType určuje typ záznamu (VehicleRegistrationNumber). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VehicleRegistrationNumber v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada čísel VRN.

2.169. **VuAbility**

Generácia 2:

Informácie uložené vo VU o tom, či VU podporuje tachografové karty generácie 1 alebo nie (požiadavka 121 v prílohe 1C).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Pridelenie hodnôt – usporiadaný oktet: 'xxxxxxxa'B (8 bitov)

Pre podporu generácie 1:

'a'B	Možnosť podpory tachografových kariet generácie 1:
	'0' B generácia 1 je podporovaná,
	'1'B generácia 1 nie je podporovaná,
'xxxxxxx'B	RFU

2.170. **VuActivityDailyData**

Generácia 1:

Informácie uložené vo VU o zmenách činnosti a/alebo zmenách stavu vedenia vozidla a/alebo zmenách stavu karty v danom kalendárnom dni (požiadavka 084 v prílohe 1B a požiadavky 105, 106 a 107 v prílohe 1C) a o stave slotov o 00.00 h daného dňa.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                INTEGER SIZE(0..1440),
   activityChangeInfos                SET SIZE(noOfActivityChanges) OF
                                      ActivityChangeInfo
}
```

noOfActivityChanges je počet slov ActivityChangeInfo v sade activityChangeInfos.

activityChangeInfos je sada slov ActivityChangeInfo uložených vo VU za daný deň. Vždy obsahuje dve slová ActivityChangeInfo udávajúce stav dvoch slotov o 00.00 h daného dňa.

2.171. **VuActivityDailyRecordArray**

Generácia 2:

Informácie uložené vo VU o zmenách činnosti a/alebo zmenách stavu vedenia vozidla a/alebo zmenách stavu karty v danom kalendárnom dni (požiadavky 105, 106 a 107 v prílohe 1C) a o stave slotov o 00.00 h daného dňa.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType určuje typ záznamu (ActivityChangeInfo). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu ActivityChangeInfo v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada slov ActivityChangeInfo uložených vo VU za daný deň. Vždy obsahuje dve slová ActivityChangeInfo udávajúce stav dvoch slotov o 00.00 h daného dňa.

2.172. **VuApprovalNumber**

Číslo typového schválenia jednotky vozidla.

Generácia 1:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Priradenie hodnôt: Neurčené.

Generácia 2:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

Priradenie hodnôt:

Schvaľovacie číslo sa uvedie tak, ako je uverejnené na príslušných webových stránkach Európskej komisie, t. j. napríklad vrátane prípadných pomlčiek. Schvaľovacie číslo schválenia sa zarovná vľavo.

2.173. **VuCalibrationData**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú kalibrácií záznamového zariadenia (požiadavka 098 v prílohe 1B).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords             INTEGER(0..255),
   vuCalibrationRecords                 SET SIZE(noOfVuCalibrationRecords) OF
                                        VuCalibrationRecord
}
```

noOfVuCalibrationRecords je počet záznamov obsiahnutých v sade vuCalibrationRecords.

vuCalibrationRecords je sada záznamov o kalibrácii.

2.174. **VuCalibrationRecord**

Informácie uložené v jednotke vozidla, ktoré sa týkajú kalibrácie záznamového zariadenia (požiadavka 098 v prílohe 1B a požiadavky 119 a 120 v prílohe 1C).

Generácia 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 je účel kalibrácie.

workshopName, workshopAddress je názov a adresa dielne.

workshopCardNumber identifikuje dielenskú kartu použitú počas kalibrácie.

workshopCardExpiryDate je konečný dátum platnosti karty.

vehicleIdentificationNumber je VIN.

vehicleRegistrationIdentification obsahuje VRN a členský štát evidencie.

wVehicleCharacteristicConstant je charakteristický koeficient vozidla.

kConstantOfRecordingEquipment je konštanta záznamového zariadenia.

lTyreCircumference je skutočný obvod pneumatík kolies.

tyreSize je určenie rozmerov pneumatík na vozidle.

authorisedSpeed je povolená rýchlosť vozidla.

oldOdometerValue, newOdometerValue je pôvodná a nová hodnota počítadla kilometrov.

oldTimeValue, newTimeValue je pôvodná a nová hodnota dátumu a času.

nextCalibrationDate je dátum najbližšej kalibrácie typu špecifikovaného v CalibrationPurpose, ktorú má vykonať oprávnený kontrolný orgán.

Generácia 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
}
```

Oproti generácii 1 sa navyše použije tento dátový prvok:

sealDataVu poskytuje informácie o plombách na rôznych dieloch vozidla.

2.175. **VuCalibrationRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú kalibrácií záznamového zariadenia (požiadavky 119 a 120 v prílohe 1C).

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCalibrationRecord
}
```

recordType určuje typ záznamu (VuCalibrationRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuCalibrationRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada kalibračných záznamov.

2.176. **VuCardIWData**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú cyklov vloženia kariet vodiča alebo dielenských kariet do jednotky vozidla a ich vytiahnutia z nej (požiadavka 081 v prílohe 1B a požiadavka 103 v prílohe 1C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords je počet záznamov v sade vuCardIWRecords.

vuCardIWRecords je sada záznamov súvisiacich s cyklami vloženia a vytiahnutia karty.

2.177. **VuCardIWRecord**

Informácie uložené v jednotke vozidla, ktoré sa týkajú cyklu vloženia karty vodiča alebo dielenskej karty do jednotky vozidla a jej vytiahnutia (požiadavka 081 v prílohe 1B a požiadavka 102 v prílohe 1C).

Generácia 1:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

cardHolderName je priezvisko a meno(-á) držiteľa karty vodiča alebo dielenskej karty, ako sú uložené na karte.

fullCardNumber je typ karty, vystavujúci členský štát a číslo karty, ako sú uložené na karte.

cardExpiryDate je konečný dátum platnosti karty, ako je uložený na karte.

cardInsertionTime je dátum a čas vloženia.

vehicleOdometerValueAtInsertion je stav počítadla kilometrov vozidla pri vložení karty.

cardSlotNumber je slot, do ktorého sa karta vkladá.

cardWithdrawalTime je dátum a čas vytiahnutia.

vehicleOdometerValueAtWithdrawal je stav počítadla kilometrov vozidla pri vytiahnutí karty.

previousVehicleInfo obsahuje informácie o predchádzajúcom vozidle, ktoré vodič použil, ako sú uložené na karte.

manualInputFlag je znak udávajúci, že držiteľ karty manuálne zapísal činnosti vodiča pri vložení karty.

Generácia 2:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

Miesto dátového prvku fullCardNumber používa dátová štruktúra generácie 2 tento dátový prvok:

fullCardNumberAndGeneration je typ karty, vystavujúci členský štát, číslo karty a generácia, ako sú uložené na karte.

2.178. **VuCardIWRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú cyklov vloženia kariet vodiča alebo dielenských kariet do jednotky vozidla a ich vytiahnutia z nej (požiadavka 103 v prílohe 1C).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType určuje typ záznamu (VuCardIWRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuCardIWRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov súvisiacich s cyklami vloženia a vytiahnutia karty.

2.179. **VuCardRecord**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú použitej tachografovej karty (požiadavka 132 v prílohe 1C).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber načítané zo súboru EF_ICC v rámci MF karty.

cardPersonaliserID načítané zo súboru EF_ICC v rámci MF karty.

typeOfTachographCardId načítané zo súboru EF_Application_Identification v rámci DF_Tachograph_G2.

cardStructureVersion načítané zo súboru EF_Application_Identification v rámci DF_Tachograph_G2.

cardNumber načítané zo súboru EF_Identification v rámci DF_Tachograph_G2.

2.180. **VuCardRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú tachografových kariet použitých s touto VU. Tieto informácie sú určené na analýzu problémov medzi JV a kartou (požiadavka 132 v prílohe 1C).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType určuje typ záznamu (VuCardRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuCardRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov súvisiacich s tachografovými kartami použitými s VU.

2.181. **VuCertificate**

Certifikát verejného kľúča jednotky vozidla.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Generácia 2:

Certifikát VU plus metaúdaje použité v sťahovacom protokole.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType určuje typ záznamu (VuCertificate). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuCertificate v bajtoch.

noOfRecords je počet záznamov v sade. Hodnota sa nastaví na 1, keďže certifikáty môžu mať rôznu dĺžku.

records je sada certifikátov VU.

2.183. **VuCompanyLocksData**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú podnikových blokovaní (požiadavka 104 v prílohe 1B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                          INTEGER(0..255),
   vuCompanyLocksRecords              SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks je počet blokovaní uvedených v sade vuCompanyLocksRecords.

vuCompanyLocksRecords je sada záznamov o podnikových blokovaniach.

2.184. **VuCompanyLocksRecord**

Informácie uložené v jednotke vozidla, ktoré sa týkajú jedného podnikového blokovania (požiadavka 104 v prílohe 1B a požiadavka 128 v prílohe 1C).

Generácia 1:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumber                  FullCardNumber
}
```

lockInTime, lockOutTime je dátum a čas zablokovania a odblokovania.

companyName, companyAddress je názov a adresa spoločnosti súvisiace s blokovaním.

companyCardNumber identifikuje kartu použitú pri zablokovaní.

Generácia 2:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumberAndGeneration     FullCardNumberAndGeneration
}
```

Miesto dátového prvku companyCardNumber používa dátová štruktúra generácie 2 tento dátový prvok:

companyCardNumberAndGeneration identifikuje kartu použitú pri zablokovaní vrátane jej generácie.

2.185. **VuCompanyLocksRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú podnikových blokovaní (požiadavka 128 v prílohe 1C).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType určuje typ záznamu (VuCompanyLocksRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuCompanyLocksRecord v bajtoch.

noOfRecords je počet záznamov v sade. Hodnota 0..255.

records je sada záznamov o podnikových blokovaniach.

2.186. **VuControlActivityData**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú kontrol vykonávaných s použitím tejto VU (požiadavka 102 v prílohe 1B).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls je počet kontrol uvedených v sade vuControlActivityRecords.

vuControlActivityRecords je sada záznamov o kontrolnej činnosti.

2.187. **VuControlActivityRecord**

Informácie uložené v jednotke vozidla, ktoré sa týkajú kontroly vykonanej s použitím tejto VU (požiadavka 102 v prílohe 1B a požiadavka 126 v prílohe 1C).

Generácia 1:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType je typ kontroly.

controlTime je dátum a čas kontroly.

controlCardNumber identifikuje kontrolnú kartu použitú pri kontrole.

downloadPeriodBeginTime je čas začiatku prípadne sťahovaného časového úseku.

downloadPeriodEndTime je čas konca prípadne sťahovaného časového úseku.

Generácia 2:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Miesto dátového prvku controlCardNumber používa dátová štruktúra generácie 2 tento dátový prvok:

controlCardNumberAndGeneration identifikuje kontrolnú kartu použitú pri kontrole vrátane jej generácie.

2.188. **VuControlActivityRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú kontrol vykonávaných s použitím tejto VU (požiadavka 126 v prílohe 1C).

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuControlActivityRecord
}
```

recordType určuje typ záznamu (VuControlActivityRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuControlActivityRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o kontrolnej činnosti VU.

2.189. **VuDataBlockCounter**

Počítadlo uložené na karte, ktoré sekvenčne identifikuje cykly vloženia karty do jednotiek vozidla a jej vytiahnutia z nich.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Priradenie hodnôt: postupné čísla s maximálnou hodnotou 9 999, začínajúc opäť s 0.

2.190. **VuDetailedSpeedBlock**

Podrobné informácie uložené v jednotke vozidla o rýchlosti vozidla za minútu, počas ktorej bolo vozidlo v pohybe (požiadavka 093 v prílohe 1B a požiadavka 116 v prílohe 1C).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate je dátum a čas prvej hodnoty rýchlosti v rámci bloku.

speedsPerSecond je chronologické poradie rýchlostí nameraných každú sekundu v rámci minúty, začínajúc pri speedBlockBeginDate (vrátane).

2.191. **VuDetailedSpeedBlockRecordArray**

Generácia 2:

Podrobné informácie o rýchlosti vozidla uložené v jednotke vozidla.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDetailedSpeedBlock
}
```

recordType určuje typ záznamu (VuDetailedSpeedBlock). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuDetailedSpeedBlock v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada blokov podrobných informácií o rýchlosti.

2.192. **VuDetailedSpeedData**

Generácia 1:

Podrobné informácie o rýchlosti vozidla uložené v jednotke vozidla.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                     INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks               SET SIZE(noOfSpeedBlocks) OF
                                       VuDetailedSpeedBlock
}
```

noOfSpeedBlocks je počet blokov rýchlostí v sade vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks je sada blokov podrobných informácií o rýchlosti.

2.193. **VuDownloadablePeriod**

Najstarší a najnovší dátum, za ktorý jednotka vozidla uchováva údaje o činnostiach vodiča (požiadavky 081, 084 alebo 087 v prílohe 1B a požiadavky 102, 105, 108 v prílohe 1C).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                 TimeReal
   maxDownloadableTime                 TimeReal
}
```

minDownloadableTime je najstarší dátum a čas vloženia karty alebo zmeny činnosti alebo zápisu miesta uložený vo VU.

maxDownloadableTime je najnovší dátum a čas vytiahnutia karty alebo zmeny činnosti alebo zápisu miesta uložený vo VU.

2.194. **VuDownloadablePeriodRecordArray**

Generácia 2:

VUDownloadablePeriod plus metaúdaje použité v sťahovacom protokole.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDownloadablePeriod
}
```

recordType určuje typ záznamu (VuDownloadablePeriod). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuDownloadablePeriod v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov VuDownloadablePeriod.

2.195. **VuDownloadActivityData**

Informácie uložené v jednotke vozidla, ktoré sa týkajú jej posledného stiahnutia (požiadavka 105 v prílohe 1B a požiadavka 129 v prílohe 1C).

Generácia 1:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumber                      FullCardNumber,
   companyOrWorkshopName               Name
}
```

downloadingTime je dátum a čas sťahovania.

fullCardNumber identifikuje kartu použitú na autorizáciu stiahnutia.

companyOrWorkshopName je názov spoločnosti alebo dielne.

Generácia 2:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   companyOrWorkshopName               Name
}
```

Miesto dátového prvku fullCardNumber používa dátová štruktúra generácie 2 tento dátový prvok:

fullCardNumberAndGeneration identifikuje kartu použitú na autorizáciu stiahnutia a jej generáciu.

2.196. **VuDownloadActivityDataRecordArray**

Generácia 2:

Informácie o poslednom sťahovaní VU (požiadavka 129 v prílohe 1C).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType určuje typ záznamu (VuDownloadActivityData). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuDownloadActivityData v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov s údajmi o sťahovaní.

2.197. **VuEventData**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú udalostí (požiadavka 094 v prílohe 1B, okrem udalosti prekročenia rýchlosti).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents je počet udalostí uvedených v sade vuEventRecords.

vuEventRecords je sada záznamov o udalostiach.

2.198. **VuEventRecord**

Informácie uložené v jednotke vozidla, ktoré sa týkajú udalosti (požiadavka 094 v prílohe 1B a požiadavka 117 v prílohe 1C, okrem udalosti prekročenia rýchlosti).

Generácia 1:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType je typ udalosti.

eventRecordPurpose je účel, na ktorý bola táto udalosť zaznamenaná.

eventBeginTime je dátum a čas začiatku udalosti.

eventEndTime je dátum a čas skončenia udalosti.

cardNumberDriverSlotBegin identifikuje kartu vloženú v slote vodiča na začiatku udalosti.

cardNumberCodriverSlotBegin identifikuje kartu vloženú v slote druhého vodiča na začiatku udalosti.

cardNumberDriverSlotEnd identifikuje kartu vloženú v slote vodiča na konci udalosti.

cardNumberCodriverSlotEnd identifikuje kartu vloženú v slote druhého vodiča na konci udalosti.

similarEventsNumber je počet podobných udalostí v danom dni.

Túto sekvenciu možno použiť pre všetky udalosti okrem prekročenia rýchlosti.

Generácia 2:

```
VuEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber,
   manufacturerSpecificEventFaultData ManufacturerSpecificEventFaultData
}
```

Oproti generácii 1 sa navyše použijú tieto dátové prvky:

manufacturerSpecificEventFaultData obsahuje dodatočné informácie o udalosti špecifické pre výrobcu.

V dátovej štruktúre generácie 2 sa miesto dátových prvkov cardNumberDriverSlotBegin, cardNumberCodriver-SlotBegin, cardNumberDriverSlotEnd a cardNumberCodriverSlotEnd používajú tieto dátové prvky:

cardNumberAndGenDriverSlotBegin identifikuje kartu vloženú v slote vodiča na začiatku udalosti vrátane jej generácie.

cardNumberAndGenCodriverSlotBegin identifikuje kartu vloženú v slote druhého vodiča na začiatku udalosti vrátane jej generácie.

cardNumberAndGenDriverSlotEnd identifikuje kartu vloženú v slote vodiča na konci udalosti vrátane jej generácie.

cardNumberAndGenCodriverSlotEnd identifikuje kartu vloženú v slote druhého vodiča na konci udalosti vrátane jej generácie.

V prípade časového konfliktu sa prvky eventBeginTime a eventEndTime interpretujú takto:

eventBeginTime je dátum a čas záznamového zariadenia.

eventEndTime je dátum a čas GNSS.

2.199. **VuEventRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú udalostí (požiadavka 117 v prílohe 1C, okrem udalosti prekročenia rýchlosti).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType určuje typ záznamu (VuEventRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuEventRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o udalostiach.

2.200. **VuFaultData**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú porúch (požiadavka 096 v prílohe 1B).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults je počet porúch uvedených v sade vuFaultRecords.

vuFaultRecords je sada záznamov o poruchách.

2.201. **VuFaultRecord**

Informácie uložené v jednotke vozidla, ktoré sa týkajú poruchy (požiadavka 096 v prílohe 1B a požiadavka 118 v prílohe 1C).

Generácia 1:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType je typ poruchy záznamového zariadenia.

faultRecordPurpose je účel, na ktorý bola táto porucha zaznamenaná.

faultBeginTime je dátum a čas začiatku poruchy.

faultEndTime je dátum a čas skončenia poruchy.

cardNumberDriverSlotBegin identifikuje kartu vloženú v slote vodiča na začiatku poruchy.

cardNumberCodriverSlotBegin identifikuje kartu vloženú v slote druhého vodiča na začiatku poruchy.

cardNumberDriverSlotEnd identifikuje kartu vloženú v slote vodiča na konci poruchy.

cardNumberCodriverSlotEnd identifikuje kartu vloženú v slote druhého vodiča na konci poruchy.

Generácia 2:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Oproti generácii 1 sa navyše použije tento dátový prvok:

manufacturerSpecificEventFaultData obsahuje dodatočné informácie o poruche špecifické podľa výrobcu.

V dátovej štruktúre generácie 2 sa miesto dátových prvkov cardNumberDriverSlotBegin, cardNumberCodriver-SlotBegin, cardNumberDriverSlotEnd a cardNumberCodriverSlotEnd používajú tieto dátové prvky:

cardNumberAndGenDriverSlotBegin identifikuje kartu vloženú v slote vodiča na začiatku poruchy vrátane jej generácie.

cardNumberAndGenCodriverSlotBegin identifikuje kartu vloženú v slote druhého vodiča na začiatku poruchy vrátane jej generácie.

cardNumberAndGenDriverSlotEnd identifikuje kartu vloženú v slote vodiča na konci poruchy vrátane jej generácie.

cardNumberAndGenCodriverSlotEnd identifikuje kartu vloženú v slote druhého vodiča na konci poruchy vrátane jej generácie.

2.202. **VuFaultRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú porúch (požiadavka 118 v prílohe 1C).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType určuje typ záznamu (VuFaultRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuFaultRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o poruchách.

2.203. **VuGNSSCDRecord**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa vzťahujú k polohe vozidla podľa GNSS, ak vodičov nepretržitý čas jazdy dosiahne násobok troch hodín (požiadavky 108 a 110 v prílohe 1C).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp je dátum a čas, keď nepretržitý čas jazdy držiteľa karty dosiahne násobok troch hodín.

cardNumberAndGenDriverSlot identifikuje kartu vloženú v slote vodiča vrátane jej generácie.

cardNumberAndGenCodriverSlot identifikuje kartu vloženú v slote druhého vodiča vrátane jej generácie.

gnssPlaceRecord obsahuje informácie o polohe vozidla.

2.204. **VuGNSSCDRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa vzťahujú k polohe vozidla podľa GNSS, ak vodičov nepretržitý čas jazdy dosiahne násobok troch hodín (požiadavky 108 a 110 v prílohe 1C).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType určuje typ záznamu (VuGNSSCDRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuGNSSCDRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o nepretržitej jazde z GNSS.

2.205. **VuIdentification**

Informácie uložené v jednotke vozidla, ktoré sa týkajú identifikácie jednotky vozidla (požiadavka 075 v prílohe 1B a požiadavky 93 a 121 v prílohe 1C).

Generácia 1:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                     VuManufacturerName,
   vuManufacturerAddress                  VuManufacturerAddress,
   vuPartNumber                           VuPartNumber,
   vuSerialNumber                         VuSerialNumber,
   vuSoftwareIdentification               VuSoftwareIdentification,
   vuManufacturingDate                    VuManufacturingDate,
   vuApprovalNumber                       VuApprovalNumber
}
```

vuManufacturerName je názov výrobcu jednotky vozidla.

vuManufacturerAddress je adresa výrobcu jednotky vozidla.

vuPartNumber je číslo dielu jednotky vozidla.

vuSerialNumber je sériové číslo jednotky vozidla.

vuSoftwareIdentification identifikuje softvér v jednotke vozidla.

vuManufacturingDate je dátum výroby jednotky vozidla.

vuApprovalNumber je číslo typového schválenia jednotky vozidla.

Generácia 2:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber,
   vuGeneration                        Generation,
   vuAbility                           VuAbility
}
```

Oproti generácii 1 sa navyše použijú tieto dátové prvky:

vuGeneration identifikuje generáciu jednotky vozidla.

vuAbility poskytuje informácie o tom, či VU podporuje tachografové karty generácie 1 alebo nie.

2.206. **VuIdentificationRecordArray**

Generácia 2:

VuIdentification plus metaúdaje použité v sťahovacom protokole.

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType určuje typ záznamu (VuIdentification). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuIdentification v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov VuIdentification.

2.207. **VuITSConsentRecord**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú súhlasu vodiča s použitím inteligentných dopravných systémov (ITS).

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identifikuje kartu vrátane jej generácie. Musí ísť o kartu vodiča alebo dielenskú kartu.

consent je znak určujúci, či vodič súhlasil s použitím inteligentných dopravných systémov v danom vozidle / jednotke vozidla.

Priradenie hodnôt:

TRUE znamená, že vodič súhlasil s použitím inteligentných dopravných systémov.

FALSE znamená, že vodič odmietol použitie inteligentných dopravných systémov.

2.208. **VuITSConsentRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú súhlasu vodiča s použitím inteligentných dopravných systémov (požiadavka 200 v prílohe 1C).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType určuje typ záznamu (VuITSConsentRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuITSConsentRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o súhlase s ITS.

2.209. **VuManufacturerAddress**

Adresa výrobcu jednotky vozidla.

```
VuManufacturerAddress ::= Address
```

Priradenie hodnôt: Neurčené.

2.210. **VuManufacturerName**

Názov výrobcu jednotky vozidla.

```
VuManufacturerName ::= Name
```

Priradenie hodnôt: Neurčené.

2.211. **VuManufacturingDate**

Dátum výroby jednotky vozidla.

```
VuManufacturingDate ::= TimeReal
```

Priradenie hodnôt: Neurčené.

2.212. **VuOverSpeedingControlData**

Informácie uložené v jednotke vozidla, ktoré sa týkajú udalostí prekročenia rýchlosti od poslednej kontroly prekročenia rýchlosti (požiadavka 095 v prílohe 1B a požiadavka 117 v prílohe 1C).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime            TimeReal,
   firstOverspeedSince                 TimeReal,
   numberOfOverspeedSince              OverspeedNumber
}
```

lastOverspeedControlTime je dátum a čas poslednej kontroly prekročenia rýchlosti.

firstOverspeedSince je dátum a čas prvého prekročenia rýchlosti po tejto kontrole prekročenia rýchlosti.

numberOfOverspeedSince je počet udalostí prekročenia rýchlosti od poslednej kontroly prekročenia rýchlosti.

2.213. **VuOverSpeedingControlDataRecordArray**

Generácia 2:

VuOverSpeedingControlData plus metaúdaje použité v sťahovacom protokole.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuOverSpeedingControlData
}
```

recordType určuje typ záznamu (VuOverSpeedingControlData). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuOverSpeedingControlData v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov s údajmi o kontrole prekročenia rýchlosti.

2.214. **VuOverSpeedingEventData**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú udalostí prekročenia rýchlosti (požiadavka 094 v prílohe 1B).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents            INTEGER(0..255),
   vuOverSpeedingEventRecords          SET SIZE(noOfVuOverSpeedingEvents) OF
                                       VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents je počet udalostí uvedený v sade vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords je sada záznamov o udalostiach prekročenia rýchlosti.

2.215. **VuOverSpeedingEventRecord**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú udalostí prekročenia rýchlosti (požiadavka 094 v prílohe 1B a požiadavka 117 v prílohe 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberDriverSlotBegin          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType je typ udalosti.

eventRecordPurpose je účel, na ktorý bola táto udalosť zaznamenaná.

eventBeginTime je dátum a čas začiatku udalosti.

eventEndTime je dátum a čas skončenia udalosti.

maxSpeedValue je maximálna rýchlosť nameraná počas udalosti.

averageSpeedValue je aritmeticky priemerná rýchlosť nameraná počas udalosti.

cardNumberDriverSlotBegin identifikuje kartu vloženú v slote vodiča na začiatku udalosti.

similarEventsNumber je počet podobných udalostí v danom dni.

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú udalostí prekročenia rýchlosti (požiadavka 094 v prílohe 1B a požiadavka 117 v prílohe 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

Miesto dátového prvku cardNumberDriverSlotBegin používa dátová štruktúra generácie 2 tento dátový prvok:

cardNumberAndGenDriverSlotBegin identifikuje kartu vloženú v slote vodiča na začiatku udalosti vrátane jej generácie.

2.216. **VuOverSpeedingEventRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú udalostí prekročenia rýchlosti (požiadavka 117 v prílohe 1C).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuOverSpeedingEventRecord
}
```

recordType určuje typ záznamu (VuOverSpeedingEventRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuOverSpeedingEventRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o udalostiach prekročenia rýchlosti.

2.217. **VuPartNumber**

Číslo dielu – jednotka vozidla.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Priradenie hodnôt: špecifické podľa výrobcu VU.

2.218. **VuPlaceDailyWorkPeriodData**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú miest, kde sa vodičom začína alebo končí denný pracovný čas (požiadavka 087 v prílohe 1B a požiadavky 108 a 110 v prílohe 1C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords je počet záznamov uvedených v sade vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords je sada záznamov vzťahujúcich sa k miestu.

2.219. **VuPlaceDailyWorkPeriodRecord**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú miesta, kde sa vodičovi začína alebo končí denný pracovný čas (požiadavka 087 v prílohe 1B a požiadavky 108 a 110 v prílohe 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber je typ karty vodiča, vystavujúci členský štát a číslo karty.

placeRecord obsahuje informácie súvisiace so zadaným miestom.

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú miesta, kde sa vodičovi začína alebo končí denný pracovný čas (požiadavka 087 v prílohe 1B a požiadavky 108 a 110 v prílohe 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Miesto dátového prvku fullCardNumber používa dátová štruktúra generácie 2 tento dátový prvok:

fullCardNumberAndGeneration je typ karty, vystavujúci členský štát, číslo karty a generácia, ako sú uložené na karte.

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú miest, kde sa vodičom začína alebo končí denný pracovný čas (požiadavky 108 a 110 v prílohe 1C).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType určuje typ záznamu (VuPlaceDailyWorkPeriodRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuPlaceDailyWorkPeriodRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov súvisiacich s miestom.

2.221. **VuPrivateKey**

Generácia 1:

Súkromný kľúč jednotky vozidla.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Generácia 1:

Verejný kľúč jednotky vozidla.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Sériové číslo jednotky vozidla (požiadavka 075 v prílohe 1B a požiadavka 93 v prílohe 1C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Dátum inštalácie softvérovej verzie jednotky vozidla.

```
VuSoftInstallationDate ::= TimeReal
```

Priradenie hodnôt: Neurčené.

2.225. **VuSoftwareIdentification**

Informácie uložené v jednotke vozidla, ktoré sa týkajú nainštalovaného softvéru.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion je číslo verzie softvéru jednotky vozidla.

vuSoftInstallationDate je dátum inštalácie softvérovej verzie.

2.226. **VuSoftwareVersion**

Číslo verzie softvéru jednotky vozidla.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Priradenie hodnôt: Neurčené.

2.227. **VuSpecificConditionData**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú špecifických podmienok.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords je počet záznamov uvedených v sade specificConditionRecords.

specificConditionRecords je sada záznamov súvisiacich so špecifickými podmienkami.

2.228. **VuSpecificConditionRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú špecifických podmienok (požiadavka 130 v prílohe 1C).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType určuje typ záznamu (SpecificConditionRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu SpecificConditionRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov súvisiacich so špecifickými podmienkami.

2.229. **VuTimeAdjustmentData**

Generácia 1:

Informácie uložené v jednotke vozidla, ktoré sa týkajú úpravy času mimo rámca pravidelnej kalibrácie (požiadavka 101 v prílohe 1B).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                INTEGER(0..6),
   vuTimeAdjustmentRecords             SET SIZE(noOfVuTimeAdjRecords) OF
                                       VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords je počet záznamov v sade vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords je sada záznamov o úprave času.

2.230. **VuTimeAdjustmentGNSSRecord**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú úpravy času na základe časových údajov z GNSS (požiadavky 124 a 125 v prílohe 1C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal
}
```

oldTimeValue, newTimeValue je pôvodná a nová hodnota dátumu a času.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú úpravy času na základe časových údajov z GNSS (požiadavky 124 a 125 v prílohe 1C).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuTimeAdjustmentGNSSRecord
}
```

recordType určuje typ záznamu (VuTimeAdjustmentGNSSRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuTimeAdjustmentGNSSRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov úpravy času na základe GNSS.

2.232. **VuTimeAdjustmentRecord**

Informácie uložené v jednotke vozidla, ktoré sa týkajú úpravy času mimo rámca pravidelnej kalibrácie (požiadavka 101 v prílohe 1B a požiadavky 124 a 125 v prílohe 1C).

Generácia 1:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue je pôvodná a nová hodnota dátumu a času.

workshopName, workshopAddress je názov a adresa dielne.

workshopCardNumber identifikuje dielenskú kartu použitú na úpravu času.

Generácia 2:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Miesto dátového prvku workshopCardNumber používa dátová štruktúra generácie 2 tento dátový prvok:

workshopCardNumberAndGeneration identifikuje dielenskú kartu použitú na úpravu času vrátane jej generácie.

2.233. **VuTimeAdjustmentRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú úprav času mimo rámca pravidelnej kalibrácie (požiadavky 124 a 125 v prílohe 1C).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType určuje typ záznamu (VuTimeAdjustmentRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuTimeAdjustmentRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov úpravy času.

2.234. **WorkshopCardApplicationIdentification**

Informácie uložené na dielenskej karte súvisiace s identifikáciou aplikácie karty (požiadavky 307 a 330 v prílohe 1C).

Generácia 1:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfCalibrationRecords              NoOfCalibrationRecords
}
```

typeOfTachographCardId špecifikuje implementovaný typ karty.

cardStructureVersion špecifikuje verziu štruktúry, ktorá je implementovaná v karte.

noOfEventsPerType je počet udalostí pre každý typ udalosti, ktorý karta dokáže zaznamenať.

noOfFaultsPerType je počet porúch pre každý typ poruchy, ktorý karta dokáže zaznamenať.

activityStructureLength udáva počet bajtov, ktoré sú k dispozícii na uloženie záznamov o činnosti.

noOfCardVehicleRecords je počet záznamov o vozidle, ktoré môže karta obsahovať.

noOfCardPlaceRecords je počet miest, ktorý karta dokáže zaznamenať.

noOfCalibrationRecords je počet záznamov o kalibrácii, ktoré možno na karte uložiť.

Generácia 2:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfCalibrationRecords              NoOfCalibrationRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Oproti generácii 1 sa navyše použijú tieto dátové prvky:

noOfGNSSCDRecords je počet záznamov o nepretržitej jazde z GNSS, ktoré možno na karte uložiť.

noOfSpecificConditionRecords je počet záznamov o špecifických podmienkach, ktoré možno na karte uložiť.

2.235. **WorkshopCardCalibrationData**

Informácie uložené na dielenskej karte súvisiace s dielenskými činnosťami, ktoré sa s kartou vykonávajú (požiadavky 314, 316, 337 a 339 v prílohe 1C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber je celkový počet kalibrácií vykonaných s kartou.

calibrationPointerNewestRecord je index naposledy aktualizovaného záznamu o kalibrácii.

Priradenie hodnôt: číslo zodpovedajúce počítadlu záznamu o kalibrácii začínajúce sa od '0' pre prvý výskyt záznamov o kalibrácii v štruktúre.

calibrationRecords je sada záznamov obsahujúcich informácie o kalibráciách a/alebo úpravách času.

2.236. **WorkshopCardCalibrationRecord**

Informácie uložené na dielenskej karte súvisiace s kalibráciou vykonanou pomocou karty (požiadavka 314 a 337 v prílohe 1C).

Generácia 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 je účel kalibrácie.

vehicleIdentificationNumber je VIN.

vehicleRegistration obsahuje VRN a členský štát evidencie.

wVehicleCharacteristicConstant je charakteristický koeficient vozidla.

kConstantOfRecordingEquipment je konštanta záznamového zariadenia.

lTyreCircumference je skutočný obvod pneumatík kolies.

tyreSize je určenie rozmerov pneumatík na vozidle.

authorisedSpeed je maximálna povolená rýchlosť vozidla.

oldOdometerValue, newOdometerValue je pôvodná a nová hodnota počítadla kilometrov.

oldTimeValue, newTimeValue je pôvodná a nová hodnota dátumu a času.

nextCalibrationDate je dátum najbližšej kalibrácie typu špecifikovaného v CalibrationPurpose, ktorú má vykonať oprávnený kontrolný orgán.

vuPartNumber, **vuSerialNumber** a **sensorSerialNumber** sú dátové prvky na identifikáciu záznamového zariadenia.

Generácia 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
}
```

Oproti generácii 1 sa navyše použijú tieto dátové prvky:

sensorGNSSSerialNumber identifikuje externé zariadenie GNSS.

rcmSerialNumber identifikuje modul diaľkovej komunikácie.

sealDataCard poskytuje informácie o plombách na rôznych dieloch vozidla.

2.237. **WorkshopCardHolderIdentification**

Informácie uložené na dielenskej karte súvisiace s identifikáciou držiteľa karty (požiadavky 311 a 334 v prílohe 1C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName je názov dielne držiteľa karty.

workshopAddress je adresa dielne držiteľa karty.

cardHolderName je priezvisko a meno(-á) držiteľa (napr. meno mechanika).

cardHolderPreferredLanguage je preferovaný jazyk držiteľa karty.

2.238. **WorkshopCardPIN**

Osobné identifikačné číslo dielenskej karty (požiadavk 309 a 332 v prílohe 1C).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Priradenie hodnôt: PIN kód známy držiteľovi karty doplnený sprava bajtmi 'FF' až do 8 bajtov.

2.239. **W-VehicleCharacteristicConstant**

Charakteristický koeficient vozidla (vymedzenie pojmov, písm. k)).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Priradenie hodnôt: Impulzy na kilometer v prevádzkovom rozsahu 0 až 64 255 impulzov/km.

2.240. **VuPowerSupplyInterruptionRecord**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú udalostí prerušenia napájania (požiadavka 117 v prílohe 1C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventRecordPurpose                  EventFaultRecordPurpose,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin   FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd     FullCardNumberAndGeneration,
   similarEventsNumber                 SimilarEventsNumber
}
```

eventType je typ udalosti.

eventRecordPurpose je účel, na ktorý bola táto udalosť zaznamenaná.

eventBeginTime je dátum a čas začiatku udalosti.

eventEndTime je dátum a čas skončenia udalosti.

cardNumberAndGenDriverSlotBegin identifikuje kartu vloženú v slote vodiča na začiatku udalosti vrátane jej generácie.

cardNumberAndGenDriverSlotEnd identifikuje kartu vloženú v slote vodiča na konci udalosti vrátane jej generácie.

cardNumberAndGenCodriverSlotBegin identifikuje kartu vloženú v slote druhého vodiča na začiatku udalosti vrátane jej generácie.

cardNumberAndGenCodriverSlotEnd identifikuje kartu vloženú v slote druhého vodiča na konci udalosti vrátane jej generácie.

similarEventsNumber je počet podobných udalostí v danom dni.

2.241. **VuPowerSupplyInterruptionRecordArray**

Generácia 2:

Informácie uložené v jednotke vozidla, ktoré sa týkajú udalostí prerušenia napájania (požiadavka 117 v prílohe 1C).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType určuje typ záznamu (VuPowerSupplyInterruptionRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu VuPowerSupplyInterruptionRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o udalostiach prerušenia napájania.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Generácia 2:

Sada SensorExternalGNSSCoupledRecord plus metaúdaje použité v sťahovacom protokole.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType určuje typ záznamu (SensorExternalGNSSCoupledRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu SensorExternalGNSSCoupledRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o spojení snímača s externým GNSS.

2.243. **VuSensorPairedRecordArray**

Generácia 2:

Sada SensorPairedRecord plus metaúdaje použité v sťahovacom protokole.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType určuje typ záznamu (SensorPairedRecord). **Priradenie hodnôt**: Pozri RecordType

recordSize je veľkosť záznamu SensorPairedRecord v bajtoch.

noOfRecords je počet záznamov v sade.

records je sada záznamov o spárovaní snímača.

3. VYMEDZENIE ROZSAHU HODNÔT A ROZMEROV

Vymedzenie premenných hodnôt použitých v definíciách v odseku 2.

```
TimeRealRange ::= 2^32-1
```

4. MNOŽINY ZNAKOV

V reťazcoch IA5Strings sú použité znaky ASCII podľa normy ISO/IEC 8824-1. Pre čitateľnosť a uľahčenie prístupu je priradenie hodnôt uvedené nižšie. V prípade nezhody s týmito informačnými údajmi má vždy prednosť norma ISO/IEC 8824-1.

```
  ! " # $ % & ' ( ) * + , - . / 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 { | } ~
```

V ďalších reťazcoch znakov (Address, Name, VehicleRegistrationNumber) sa navyše používajú znaky z rozsahu kódov dekadických znakov 161 – 255 týchto 8-bitových štandardných množín znakov určených číslom kódovej stránky: Štandardná množina znakov	Kódová stránka (dekadické)
ISO/IEC 8859-1 Latinka-1 západoeurópske jazyky	1
ISO/IEC 8859-2 Latinka-2 stredoeurópske jazyky	2
ISO/IEC 8859-3 Latinka-3 juhoeurópske jazyky	3
ISO/IEC 8859-5 Latinka/cyrilika	5
ISO/IEC 8859-7 Latinka/grécka abeceda	7
ISO/IEC 8859-9 Latinka-5 turečtina	9
ISO/IEC 8859-13 Latinka-7 pobaltské jazyky	13
ISO/IEC 8859-15 Latinka-9	15
ISO/IEC 8859-16 Latinka-10 jazyky juhovýchodnej Európy	16
KOI8-R Latinka/cyrilika	80
KOI8-U Latinka/cyrilika	85

5. KÓDOVANIE

Pri kódovaní podľa kódovacích pravidiel ASN.1 sa všetky vymedzené dátové typy kódujú podľa normy ISO/IEC 8825-2, usporiadaný variant.

6. OBJEKTOVÉ IDENTIFIKÁTORY A IDENTIFIKÁTORY APLIKÁCIÍ

6.1. **Objektové identifikátory**

Objektové identifikátory (OID) uvedené v tejto kapitole sú relevantné iba pre generáciu 2. OID sú vymedzené v TR-03110-3 a tu sú zopakované len pre úplnosť. Vetva stromovej štruktúry bsi-de obsahuje tieto OID:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Identifikátory protokolu autentifikácie 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}
```

Príklad: Povedzme, že sa VU má autentifikovať pomocou SHA-384; potom sa použije objektový identifikátor (v notácii ASN.1) `bsi-de protocols(2) smartcard(2) 2 2 4`. Hodnota tohto objektového identifikátora v bodkovej notácii je `0.4.0.127.0.7.2.2.2.2.4`.

	Bodková notácia	Bajtová notácia
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’

Identifikátory protokolu autentifikácie čipu

```
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}
```

Príklad: Povedzme, že čip sa autentifikuje algoritmom ECDH, takže kľúč relácie AES bude mať dĺžku 128 bitov. Tento kľúč relácie sa neskôr použije v režime prevádzky CBC, aby sa zaistila dôvernosť údajov, a s algoritmom CMAC, aby sa zaistila ich autenticita. Preto sa použije objektový identifikátor (v notácii ASN.1) `bsi-de protocols(2) smartcard(2) 3 2 2`. Hodnota tohto objektového identifikátora v bodkovej notácii je `0.4.0.127.0.7.2.2.3.2.2`.

	Bodková notácia	Bajtová notácia
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. Identifikátory aplikácií

Generácia 2:

Identifikátor aplikácie (AID) pre externé zariadenie GNSS (Generácia 2) je daný ako ‘FF 44 54 45 47 4D’. Ide o chránený AID podľa normy ISO/IEC 7816-4.

Poznámka: Posledných 5 bajtov kóduje DTEGM pre externé zariadenie GNSS inteligentných tachografov.

Identifikátor aplikácie tachografovej karty generácie 2 je daný ako ‘FF 53 4D 52 44 54’. Ide o chránený AID podľa normy ISO/IEC 7816-4.

Dodatok 2

ŠPECIFIKÁCIA TACHOGRAFOVÝCH KARIET

OBSAH

1. ÚVOD ... 175
1.1. Skratky ... 175
1.2. Referenčné dokumenty ... 176
2. ELEKTRICKÉ A FYZIKÁLNE CHARAKTERISTIKY ... 176
2.1. Napájanie a spotreba prúdu ... 177
2.2. Programovacie napätie V_{pp} ... 177
2.3. Generovanie a frekvencia hodinových impulzov ... 177
2.4. I/O kontakt ... 177
2.5. Stavy karty ... 177
3. HARDVÉR A KOMUNIKÁCIA ... 177
3.1. Úvod ... 177
3.2. Prenosový protokol ... 178
3.2.1 Protokoly ... 178
3.2.2 ATR ... 179
3.2.3 PTS ... 179
3.3. Pravidlá prístupu ... 180
3.4. Prehľad príkazov a kódov chýb ... 183
3.5. Opisy príkazov ... 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. ŠTRUKTÚRA TACHOGRAFOVÝCH KARIET ... 216
4.1. Hlavný súbor (MF) ... 216

4.2. Aplikácie karty vodiča 217
4.2.1 Aplikácia karty vodiča generácie 1 217
4.2.2 Aplikácia karty vodiča generácie 2 221
4.3. Aplikácie dielenskej karty 224
4.3.1 Aplikácia dielenskej karty generácie 1 224
4.3.2 Aplikácia dielenskej karty generácie 2 228
4.4. Aplikácie kontrolnej karty 233
4.4.1 Aplikácia kontrolnej karty generácie 1 233
4.4.2 Aplikácia kontrolnej karty generácie 2 235
4.5. Aplikácie podnikovej karty 237
4.5.1 Aplikácia podnikovej karty generácie 1 237
4.5.2 Aplikácia podnikovej karty generácie 2 238

1. ÚVOD

1.1. **Skratky**

V dodatku sa používajú tieto skratky:

AC	Access Conditions (podmienky prístupu)
AES	Advanced Encryption Standard (štandard pokročilého šifrovania)
AID	Application Identifier (identifikátor aplikácie)
ALW	Always (vždy)
APDU	Application Protocol Data Unit (dátová jednotka aplikačného protokolu – štruktúra príkazu)
ATR	Answer To Reset (odozva na reset)
AUT	autentifikované
C6, C7	kontakty č. 6 a 7 karty opísané v ISO/IEC 7816-2
cc	clock cycles (cykly hodinových impulzov)
CHV	Card holder Verification Information (informácia na overenie držiteľa karty)
CLA	Class byte of an APDU command (bajt triedy v príkaze APDU)
DSRC	Dedicated Short Range Communication (vyhradená komunikácia krátkeho dosahu)
DF	Dedicated File (vyhradený súbor). DF môže obsahovať iné súbory (EF alebo DF)
ECC	Elliptic Curve Cryptography (kryptografia na báze eliptických kriviek)
EF	Elementary File (elementárny súbor)
etu	elementary time unit (elementárna časová jednotka)
G1	generácia 1
G2	generácia 2
IC	Integrated Circuit (integrovaný obvod)
ICC	Integrated Circuit Card (karta s integrovaným obvodom)
ID	identifikátor
IFD	Interface Device (zariadenie s rozhraním)
IFS	Information Field Size (veľkosť informačného poľa)
IFSC	Information Field Size for the card (veľkosť informačného poľa karty)

IFSD	Information Field Size Device (veľkosť informačného poľa zariadenia – pre koncové zariadenie)
INS	Instruction byte of an APDU command (príkazový bajt pre príkaz APDU)
Lc	dĺžka vstupných dát pre príkaz APDU
Le	dĺžka predpokladaných údajov (výstupné údaje pre príkaz)
MF	Master File (hlavný súbor –root DF)
NAD	Node Address used in T=1 protocol (uzlová adresa používaná v protokole T=1)
NEV	Never (nikdy)
P1-P2	parametrické bajty
PIN	Personal Identification Number (osobné identifikačné číslo)
PRO SM	Protected with secure messaging (chránené zabezpečeným spracovaním správ)
PTS	Protocol Transmission Selection (voľba prenosu protokolu)
RFU	Reserved for Future Use (vyhradené na budúce použitie)
RST	reset (karty)
SFID	Short EF Identifier (skrátený identifikátor EF)
SM	Secure Messaging (zabezpečené spracovanie správ)
SW1-SW2	stavové bajty
TS	počiatočný znak ATR
VPP	programovacie napätie
VU	Vehicle Unit (jednotka vozidla)
XXh	hexadecimálna hodnota XX
'XXh'	hexadecimálna hodnota XX
||	symbol zreťazenia 03||04=0304

1.2. **Referenčné dokumenty**

V dodatku sa používajú tieto referenčné dokumenty:

ISO/IEC 7816-2 Identifikačné karty. Karty s integrovanými obvodmi. Časť 2: rozmery a umiestnenie kontaktov. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Identifikačné karty. Karty s integrovanými obvodmi. Časť 3: elektronické signály a prenosové protokoly. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Identifikačné karty. Karty s integrovanými obvodmi. Časť 4: organizácia, zabezpečenie a príkazy pre výmenu). ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Identifikačné karty. Karty s integrovanými obvodmi. Časť 6: medziodborové dátové prvky pre výmenu. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Identifikačné karty. Karty s integrovanými obvodmi. Časť 8: príkazy pre operácie zabezpečenia. ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Informačné technológie. Techniky zabezpečenia. Kontrolný kód správy (MAC). Časť 2: mechanizmy s vyhradenou funkciou hash. ISO/IEC 9797-2:2011.

2. ELEKTRICKÉ A FYZIKÁLNE CHARAKTERISTIKY

TCS_01 Pokiaľ nie je uvedené inak, všetky elektronické signály musia byť v súlade s normou ISO/IEC 7816-3.

TCS_02 Umiestnenie a rozmery kontaktov karty musia spĺňať požiadavky normy ISO/IEC 7816-2.

2.1. **Napájanie a spotreba prúdu**

TCS_03 Karta musí pracovať v súlade so špecifikáciami v rámci limitov spotreby špecifikovaných v ISO/IEC 7816-3.

TCS_04 Karta musí pracovať s Vcc = 3V (± 0,3V) alebo Vcc = 5V (± 0,5V).

Voľba napätia sa vykoná podľa ISO/IEC 7816-3.

2.2. **Programovacie napätie V_{pp}**

TCS_05 Karta nevyžaduje programovacie napätie pri kontakte C6. Predpokladá sa, že kontakt C6 nie je pripojený k prepojovaciemu zariadeniu (IFD). Kontakt C6 môže byť pripojený k V_{cc} v karte, ale nesmie byť uzemnený. Toto napätie nesmie byť v žiadnom prípade interpretované.

2.3. **Generovanie a frekvencia hodinových impulzov**

TCS_06 Karta pracuje vo frekvenčnom rozsahu 1 až 5 MHz a môže podporovať aj vyššie frekvencie. V rámci jednej relácie karty môže frekvencia hodinových impulzov kolísať v rozsahu ± 2 %. Frekvencia hodinových impulzov je generovaná jednotkou vozidla a nie samotnou kartou. Pracovný cyklus sa môže meniť od 40 do 60 %.

TCS_07 Za podmienok obsiahnutých v kartovom súbore EF ICC sa môžu vonkajšie hodiny zastaviť. Prvý bajt hlavnej časti súboru EF ICC kóduje podmienky pre režim zastavenia času (Clockstop):

Úroveň nízka	Úroveň vysoká		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop povolený, žiadna preferovaná úroveň
0	1	1	Clockstop povolený, preferuje sa vysoká úroveň
1	0	1	Clockstop povolený, preferuje sa nízka úroveň
0	0	0	Clockstop nepovolený
0	1	0	Clockstop povolený len na vysokej úrovni
1	0	0	Clockstop povolený len na nízkej úrovni

Bity 4 až 8 sa nepoužijú.

2.4. **I/O kontakt**

TCS_08 I/O kontakt C7 sa použije na príjem dát z IFD a vysielanie dát na IFD. Počas prevádzky je vo vysielacom režime buď iba karta alebo iba IFD. Ak by vo vysielacom režime boli obe jednotky, karta sa nesmie poškodiť. Pokiaľ karta nevysiela, aktivuje sa na nej prijímací režim.

2.5. **Stavy karty**

TCS_09 Karta pod napájacím napätím pracuje v dvoch stavoch:

stav prevádzky počas vykonávania príkazov alebo počas spojenia s digitálnou jednotkou,

stav pokoja vo všetkých ostatných prípadoch – v tomto stave musí karta uchovať všetky údaje.

3. HARDVÉR A KOMUNIKÁCIA

3.1. **Úvod**

Tento odsek opisuje minimálnu funkčnosť tachografových kariet a jednotiek vozidla požadovanú na zabezpečenie správnej činnosti a interoperability.

Tachografové karty sú v maximálnej možnej zhode s platnými normami ISO/IEC (hlavne s ISO/IEC 7816). Príkazy a protokoly sú však opísané úplne s cieľom stanoviť obmedzené použitie alebo prípadné rozdiely. Pokiaľ nie je uvedené inak, špecifikované príkazy plne zodpovedajú daným normám.

3.2. **Prenosový protokol**

TCS_10 Prenosový protokol musí spĺňať normu ISO/IEC 7816-3 pre T = 0 a T = 1. VU musí rozoznať najmä predĺženia čakacieho času vysielané kartou.

3.2.1 *Protokoly*

TCS_11 Karta podporuje protokol **T=0**, ako aj protokol **T=1**. Okrem toho môže karta podporovať aj ďalšie kontaktovo orientované protokoly.

TCS_12 Predvolený je protokol **T=0**; zmena na protokol **T=1** teda vyžaduje príkaz **PTS**.

TCS_13 Zariadenia musia v oboch protokoloch podporovať metódu „**direct convention**“ (priama konvencia), ktorá je teda pre kartu povinná.

TCS_14 Bajt pre **veľkosť informačného poľa karty** sa v ATR prezentuje v znaku TA3. Táto hodnota je minimálne ‘F0h’ (= 240 bajtov).

Pre protokoly platia tieto obmedzenia:

TCS_15 **T=0**

— Zariadenie s rozhraním musí podporovať odpoveď pri I/O po stúpajúcej hrane signálu na RST od 400 cc.

— Zariadenie s rozhraním musí byť schopné čítať znaky s rozostupom 12 etu.

— Zariadenie s rozhraním musí prečítať chybný znak a jeho opakovanie, ak rozostup činí 13 etu. Ak sa zistí chybný znak, objaví sa na I/O chybový signál medzi 1 etu a 2 etu. Zariadenie musí podporovať oneskorenie 1 etu.

— Zariadenie s rozhraním musí akceptovať 33-bajtové ATR (TS+32).

— Ak sa v ATR nachádza TC1, musí byť pre znaky vysielané zariadením s rozhraním k dispozícii dodatočný ochranný čas (Extra Guard Time), zatiaľ čo znaky vysielané kartou môžu zostať oddelené rozostupom 12 etu. Platí to aj pre znak ACK vysielaný kartou po znaku P3 vyslanom zariadením s rozhraním.

— Zariadenie s rozhraním musí zohľadňovať znak NUL vyslaný kartou.

— Zariadenie s rozhraním musí akceptovať doplnkový režim pre ACK.

— Príkaz get-response sa nemôže použiť v režime reťazenia na získanie údajov, ktorých dĺžka by mohla presiahnuť 255 bajtov.

TCS_16 **T=1**

— Bajt NAD: nepoužíva sa (NAD sa nastaví na ‘00’).

— S-block ABORT: nepoužíva sa.

— S-block VPP state error: nepoužíva sa.

— Celková dĺžka reťazenia pre dátové pole nepresiahne 255 bajtov (zaisťuje IFD).

— IFD uvedie veľkosť informačného poľa zariadenia (IFSD) okamžite po ATR: IFD odošle po ATR požiadavku na S-Block IFS a karta zašle späť S-Block IFS. Odporúčaná hodnota pre IFSD je 254 bajtov.

— Karta nebude vyžadovať dodatočné nastavenie IFS.

3.2.2 *ATR*

TCS_17 Zariadenie kontroluje bajty ATR podľa ISO/IEC 7816-3. Historické znaky ATR sa neoverujú.

Príklad základného biprotokolu ATR podľa ISO/IEC 7816-3

Character	Value	Remarks
TS	'3Bh'	Indicates direct convention.
T0	'85h'	TD1 present; 5 historical bytes are presents.
TD1	'80h'	TD2 present; T=0 to be used
TD2	'11h'	TA3 present; T=1 to be used
TA3	'XXh' (at least 'F0h')	Information Field Size Card (IFSC)
TH1 to TH5	'XXh'	Historical characters
TCK	'XXh'	Check Character (exclusive OR)

TCS_18 Po odozve na reset (ATR) sa implicitne zvolí hlavný súbor (MF) a stáva sa aktuálnym adresárom.

3.2.3 *PTS*

TCS_19 Predvolený protokol je T=0. Nastavenie protokolu T=1 si vyžaduje, aby karta zariadeniu odoslala príkaz PTS (známy aj ako PPS).

TCS_20 Keďže sú pre kartu povinné oba protokoly T=0 aj T=1, základný PTS na prepínanie protokolov je pre kartu tiež povinný.

PTS možno v súlade s normou ISO/IEC 7816-3 použiť na prepnutie na vyššie prenosové rýchlosti, než je prípadne prednastavená rýchlosť, ktorú v ATR navrhuje karta (bajt TA(1)).

Vyššie prenosové rýchlosti sú pre kartu voliteľné.

TCS_21 Ak nie je podporovaná iná než prednastavená prenosová rýchlosť (alebo ak nie je podporovaná zvolená prenosová rýchlosť), karta odpovedá na PTS správne podľa ISO/IEC 7816-3 tak, že vynechá bajt PPS1.

Príklady základného PTS pre voľbu protokolu sú tieto:

Character	Value	Remarks
PPSS	'FFh'	The Initiate Character.
PPS0	'00h' or '01h'	PPS1 to PPS3 are not present; '00h' to select T0, '01h' to select T1.
PK	'XXh'	Check Character: 'XXh' = 'FFh' if PPS0 = '00h', 'XXh' = 'FEh' if PPS0 = '01h'.

3.3. **Pravidlá prístupu**

TCS_22 Pravidlo prístupu určuje pre režim prístupu (t. j. príkaz) príslušné podmienky zabezpečenia. Ak sú tieto podmienky zabezpečenia splnené, daný príkaz sa spracuje.

TCS_23 Pre tachografovú kartu platia tieto podmienky zabezpečenia:

Skratka	Význam
ALW	Úkon je vždy možný a možno ho vykonať bez akýchkoľvek obmedzení. Príkaz a odpoveď APDU sa posielajú ako nešifrovaný text, teda bez zabezpečeného spracovania.
NEV	Úkon nie je možný nikdy.
PLAIN-C	Príkaz APDU sa posiela ako nešifrovaný text, teda bez zabezpečeného spracovania.
PWD	Úkon možno vykonať, iba ak bol úspešne overený PIN dielenskej karty, t. j. ak je nastavený interný bezpečnostný stav karty „PIN_Verified“. Príkaz musí byť odoslaný bez zabezpečeného spracovania.
EXT-AUT-G1	Úkon možno vykonať, iba ak úspešne prebehol príkaz External Authenticate pre autentifikáciu generácie 1 (pozri aj dodatok 11 časť A).
SM-MAC-G1	APDU (príkaz aj odpoveď) sa musí uplatniť so zabezpečeným spracovaním generácie 1 v režime iba na základe autentifikácie (pozri dodatok 11 časť A).
SM-C-MAC-G1	Príkaz APDU sa musí uplatniť so zabezpečeným spracovaním generácie 1 v režime iba na základe autentifikácie (pozri dodatok 11 časť A).
SM-R-ENC-G1	Odpoveď APDU sa musí uplatniť so zabezpečeným spracovaním generácie 1 v režime šifrovania (pozri dodatok 11 časť A).
SM-R-ENC-MAC-G1	Odpoveď APDU sa musí uplatniť so zabezpečeným spracovaním generácie 1 v režime šifrovania a následnej autentifikácie (pozri dodatok 11 časť A).
SM-MAC-G2	APDU (príkaz aj odpoveď) sa musí uplatniť so zabezpečeným spracovaním generácie 2 v režime iba na základe autentifikácie (pozri dodatok 11 časť B).
SM-C-MAC-G2	Príkaz APDU sa musí uplatniť so zabezpečeným spracovaním generácie 2 v režime iba na základe autentifikácie (pozri dodatok 11 časť B).
SM-R-ENC-MAC-G2	Odpoveď APDU sa musí uplatniť so zabezpečeným spracovaním generácie 2 v režime šifrovania a následnej autentifikácie (pozri dodatok 11 časť B).

TCS_24 Uvedené podmienky zabezpečenia môžu byť prepojené týmito operátormi:

AND: Musia byť splnené všetky podmienky zabezpečenia.

OR: Musí byť splnená aspoň jedna podmienka zabezpečenia.

Prístupové pravidlá pre systém súborov, t. j. príkazy SELECT, READ BINARY a UPDATE BINARY sú vymedzené v kapitole 4. Prístupové pravidlá pre zvyšné príkazy sú uvedené v nasledujúcich tabuľkách.

TCS_25 V aplikácii DF Tachograph_G1 sa používajú tieto prístupové pravidlá:

Príkaz	Karta vodiča	Dielenská karta	Kontrolná karta	Podniková karta
External Authenticate				
— na autentifikáciu generácie 1	ALW	ALW	ALW	ALW
— na autentifikáciu generácie 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	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	neuplatňuje sa	neuplatňuje sa
PSO: Hash	neuplatňuje sa	neuplatňuje sa	ALW	neuplatňuje sa
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	neuplatňuje sa	neuplatňuje sa
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	neuplatňuje sa	neuplatňuje sa	ALW	neuplatňuje sa
Verify	neuplatňuje sa	ALW	neuplatňuje sa	neuplatňuje sa

TCS_26 V aplikácii DF Tachograph_G2 sa používajú tieto prístupové pravidlá:

Príkaz	Karta vodiča	Dielenská karta	Kontrolná karta	Podniková karta
External Authenticate				
— na autentifikáciu generácie 1	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa
— na autentifikáciu generácie 2	ALW	PWD	ALW	ALW
Internal Authenticate	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa

Príkaz	Karta vodiča	Dielenská karta	Kontrolná karta	Podniková karta
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	neuplatňuje sa	ALW	ALW	neuplatňuje sa
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	neuplatňuje sa	neuplatňuje sa
PSO: Hash	neuplatňuje sa	neuplatňuje sa	ALW	neuplatňuje sa
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	neuplatňuje sa	neuplatňuje sa
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	neuplatňuje sa	neuplatňuje sa	ALW	neuplatňuje sa
Verify	neuplatňuje sa	ALW	neuplatňuje sa	neuplatňuje sa

TCS_27 V MF sa používajú tieto prístupové pravidlá:

Príkaz	Karta vodiča	Dielenská karta	Kontrolná karta	Podniková karta
External Authenticate				
— na autentifikáciu generácie 1	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa
— na autentifikáciu generácie 2	ALW	PWD	ALW	ALW
Internal Authenticate	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa
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	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa

Príkaz	Karta vodiča	Dielenská karta	Kontrolná karta	Podniková karta
PSO: Compute Digital Signature	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa
PSO: Hash	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa
PSO: Hash of File	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa	neuplatňuje sa
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	neuplatňuje sa	ALW	neuplatňuje sa	neuplatňuje sa

TCS_28 Tachografová karta môže, ale nemusí akceptovať príkaz s vyšším stupňom zabezpečenia, než je stanovený v podmienkach zabezpečenia. To znamená, že ak je podmienka zabezpečenia ALW (alebo PLAIN-C), karta môže akceptovať príkaz so zabezpečeným spracovaním (režim šifrovania a/alebo autentifikácie). Ak si podmienka zabezpečenia vyžaduje zabezpečené spracovanie s režimom autentifikácie, tachografová karta môže akceptovať príkaz so zabezpečeným spracovaním rovnakej generácie v režime autentifikácie a šifrovania.

Poznámka: Viac informácií o podpore príkazov pre rôzne typy tachografových kariet a rôzne DF možno nájsť v opisoch príkazov.

3.4. **Prehľad príkazov a kódov chýb**

Organizácia príkazov a súborov sa odvodí z normy ISO/IEC 7816-4, ktorej požiadavky musia byť splnené.

Tento odsek popisuje nasledovné páry príkazov a odpovedí APDU: Varianty príkazov podporované aplikáciou generácie 1 a 2 sú uvedené v opise príslušného príkazu.

Príkaz	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	

Príkaz	INS
INTERNAL AUTHENTICATE	'88h'
EXTERNAL AUTHENTICATE	'82h'
MANAGE SECURITY ENVIRONMENT	'22h'
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	'86h'

TCS_29 Stavové slová SW1 SW2 sa vrátia v každej odpovedi a označujú stav spracovania príkazu.

SW1	SW2	Význam
90	00	Normálne spracovanie.
61	XX	Normálne spracovanie. XX = počet bajtov odpovede k dispozícii.
62	81	Spracovanie s výstrahou. Časť vrátených údajov môže byť poškodená.
63	00	Neúspešné overenie (výstraha).
63	CX	Chybné CHV (PIN). „X" uvádza počet zostávajúcich pokusov.
64	00	Chyba pri vykonaní – stav energeticky nezávislej pamäte nezmenený. Chyba integrity.
65	00	Chyba pri vykonaní – stav energeticky nezávislej pamäte zmenený.
65	81	Chyba pri vykonaní – stav energeticky nezávislej pamäte zmenený – zlyhanie pamäte.
66	88	Chyba zabezpečenia: nesprávny kryptografický kontrolný súčet (pri zabezpečenom spracovaní) alebo chybný certifikát (pri overovaní certifikátu) alebo chybný kryptogram (pri externej autentifikácii) alebo chybný podpis (pri overovaní podpisu).
67	00	Nesprávna dĺžka (nesprávne Lc alebo Le).
68	82	Zabezpečené spracovanie nepodporované.
68	83	Očakáva sa posledný príkaz reťazca.
69	00	Zakázaný príkaz (v T=0 nie je k dispozícii žiadna odpoveď).
69	82	Nesplnený bezpečnostný stav.
69	83	Blokovaná autentifikačná metóda.
69	85	Nesplnené podmienky používania.
69	86	Príkaz nepovolený (žiaden aktuálny EF).

SW1	SW2	Význam
69	87	Chýbajú predpokladané dátové objekty zabezpečeného spracovania.
69	88	Nesprávne dátové objekty zabezpečeného spracovania.
6A	80	Nesprávne parametre v dátovom poli.
6A	82	Súbor nenájdený.
6A	86	Chybné parametre P1-P2.
6A	88	Referenčné údaje nenájdené.
6B	00	Chybné parametre (offset mimo EF).
6C	XX	Nesprávne dĺžka, SW2 udáva presnú dĺžku. Nevráti sa žiadne dátové pole.
6D	00	Príkazový kód nepodporovaný alebo neplatný.
6E	00	Nepodporovaná trieda.
6F	00	Iné kontrolné chyby.

TCS_30 Ak je v jednom príkaze APDU splnených viacero chybných podmienok, karta môže vrátiť ktorékoľvek z príslušných stavových slov.

3.5. **Opisy príkazov**

V tejto kapitole sú opísané povinné príkazy pre tachografové karty.

Ďalšie relevantné podrobnosti o príslušných kryptografických operáciách sú uvedené v dodatku 11 Spoločné mechanizmy zabezpečenia pre tachografy generácie 1 a 2.

Všetky príkazy sú opísané nezávisle od použitého protokolu (T=0 alebo T=1). Vždy sú udané APDU bajty CLA, INS, P1, P2, Lc a Le. Ak opísaný príkaz nevyžaduje Lc alebo Le, príslušná dĺžka, hodnota a opis sú prázdne.

TCS_31 Ak sa vyžadujú oba dĺžkové bajty (Lc a Le), opísaný príkaz treba rozdeliť na dve časti, ak IFD používa protokol T=0: IFD odošle príkaz podľa opisu s P3=Lc + údaje a potom odošle príkaz GET RESPONSE (pozri § 3.5.6) s P3=Le.

TCS_32 Ak sa vyžadujú oba dĺžkové bajty a Le=0 (zabezpečené spracovanie):

— Pri protokole T=1 karta odpovedá na Le=0 odoslaním všetkých disponibilných výstupných údajov.

— Pri protokole T=0 IFD vyšle prvý príkaz s P3=Lc + údaje, karta odpovie (na túto implicitnú Le=0) stavovými bajtami '**61La**', pričom La je počet dostupných bajtov odpovede. IFD potom na prečítanie dát vygeneruje príkaz GET RESPONSE s P3=La.

TCS_33 Tachografová karta môže voliteľne podporovať polia s rozšírenou dĺžkou podľa ISO/IEC 7816-4. Ak tachografová karta podporuje rozšírenú dĺžku polí, musí

— uvádzať podporu rozšírenej dĺžky polí v ATR

— uvádzať podporované veľkosti vyrovnávacej pamäte v informáciách o rozšírenej dĺžke v EF ATR/INFO pozri TCS_146.

— uvádzať, či podporuje rozšírenú dĺžku polí pre T=1 a/alebo T=0 v EF Extended Length, pozri TCS_147.

— podporovať rozšírenú dĺžku polí pre aplikáciu tachograf generácie 1 a 2.

Poznámky:

Všetky príkazy sú špecifikované pre krátke polia. Použitie APDU rozšírenej dĺžky vyplýva z ISO/IEC 7816-4.

Vo všeobecnosti sú príkazy špecifikované pre nešifrovaný režim, teda bez zabezpečeného spracovania, keďže vrstvu zabezpečeného spracovania určuje dodatok 11. Z prístupových pravidiel každého príkazu je zrejmé, či daný príkaz podporuje zabezpečené spracovanie alebo nie, a či príkaz podporí zabezpečené spracovanie generácie 1 a/alebo generácie 2. Niektoré varianty príkazov sú opísané so zabezpečeným spracovaním na ilustráciu jeho používania.

TCS_34 VU vykoná úplný protokol vzájomnej autentifikácie generácie 2 medzi VU a kartou pre reláciu vrátane overenia certifikátu (ak sa vyžaduje) buď v DF Tachograph, DF Tachograph_G2 alebo v MF.

3.5.1 *SELECT*

Tento príkaz zodpovedá norme ISO/IEC 7816-4, no v porovnaní s príkazom vymedzeným v norme má obmedzené použitie.

Príkaz SELECT sa používa:

— na voľbu DF aplikácie (musí sa použiť voľba podľa názvu)

— na voľbu elementárneho súboru zodpovedajúceho ID predloženého súboru

3.5.1.1 Voľba podľa názvu (AID)

Tento príkaz umožňuje voľbu DF aplikácie na karte.

TCS_35 Príkaz možno vykonať odkiaľkoľvek v štruktúre súboru (po ATR alebo kedykoľvek).

TCS_36 Voľba aplikácie resetuje aktuálne prostredie zabezpečenia. Po vykonaní voľby aplikácie už nie je zvolený žiadny aktuálny verejný kľúč. Stratí sa aj prístupová podmienka EXT-AUT-G1. Ak bol príkaz vykonaný bez zabezpečeného spracovania, kľúče z predošlej relácie zabezpečeného spracovania už nie sú k dispozícii.

TCS_37 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Voľba podľa názvu (AID)
P2	1	'0Ch'	Neočakáva sa odpoveď
Lc	1	'NNh'	Počet bajtov poslaných na kartu (dĺžka AID): '06h' pre aplikáciu tachografu
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' pre aplikáciu tachografu generácie 1 AID:'FF 53 4D 52 44 54' pre aplikáciu tachografu generácie 2

Na príkaz SELECT nie je potrebná žiadna odpoveď (v T=1 chýba Le alebo v T=0 sa nevyžaduje odpoveď).

TCS_38 **Odpovedacia správa (nevyžaduje sa žiadna odpoveď)**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— ak sa nenašla aplikácia zodpovedajúca AID, vrátený stav spracovania je '**6A82**'.

— Pri T=1, ak je prítomný bajt Le, vrátený stav je '**6700**'.

— Pri T=0, ak sa po príkaze SELECT vyžaduje odpoveď, vrátený stav je '**6900**'.

— Ak sa zvolená aplikácia považuje za poškodenú (zistila sa chyba integrity v atribútoch súboru), vrátený stav spracovania je '**6400**' alebo '**6581**'.

3.5.1.2 Voľba elementárneho súboru s použitím jeho identifikátora

TCS_39 **Príkazová správa**

TCS_40 Tachografová karta musí pre tento variant príkazu podporovať zabezpečené spracovanie generácie 2 podľa dodatku 11 časti B.

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Voľba EF v rámci aktuálneho DF
P2	1	'0Ch'	Neočakáva sa odpoveď
Lc	1	'02h'	Počet bajtov poslaných na kartu
#6-#7	2	'XXXXh'	Identifikátor súboru

Na príkaz SELECT nie je potrebná žiadna odpoveď (v T=1 chýba Le alebo v T=0 sa nevyžaduje odpoveď).

TCS_41 **Odpovedacia správa (nevyžaduje sa žiadna odpoveď)**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak sa nenašiel súbor zodpovedajúci identifikátoru súboru, vrátený stav spracovania je '**6A82**'.

— Pri T=1, ak je prítomný bajt Le, vrátený stav je '**6700**'.

— Pri T=0, ak sa po príkaze SELECT vyžaduje odpoveď, vrátený stav je '**6900**'.

— Ak sa zvolený súbor považuje za poškodený (zistila sa chyba integrity v atribútoch súboru), vrátený stav spracovania je '**6400**' alebo '**6581**'.

3.5.2 *READ BINARY*

Tento príkaz zodpovedá norme ISO/IEC 7816-4, no v porovnaní s príkazom vymedzeným v norme má obmedzené použitie.

Príkaz READ BINARY sa používa na čítanie údajov z transparentného súboru.

Karta ako odpoveď vráti prečítané údaje, ktoré môžu byť uzavreté v štruktúre zabezpečeného spracovania.

3.5.2.1 Príkaz s offsetom v P1-P2

Tento príkaz umožňuje IFD čítanie údajov z aktuálne zvoleného EF bez zabezpečeného spracovania.

Poznámka: Tento príkaz bez zabezpečeného spracovania možno použiť len na čítanie súboru, ktorý podporuje podmienku zabezpečenia ALW v režime prístupu na čítanie.

TCS_42 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Offset od začiatku súboru v bajtoch: bajt najvyššieho rádu
P2	1	'XXh'	Offset od začiatku súboru v bajtoch: bajt najnižšieho rádu
Le	1	'XXh'	Očakávaná dĺžka údajov. Počet bajtov, ktoré sa majú čítať.

Poznámka: bit 8 P1 musí byť nastavený na 0.

TCS_43 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
#1-#X	X	'XX..XXh'	Prečítané údaje
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak nie je zvolený žiadny EF, vrátený stav spracovania je '**6986**'.

— Ak nie sú splnené podmienky zabezpečenia zvoleného súboru, príkaz sa preruší s '**6982**'.

— Ak offset nie je kompatibilný s veľkosťou EF (offset > veľkosť EF), vrátený stav spracovania je '**6B00**'.

— Ak nie je veľkosť čítaných údajov kompatibilná s veľkosťou EF (offset + Le > veľkosť EF), vrátený stav spracovania je '**6700**' alebo '**6Cxx**', pričom „xx" je presná dĺžka.

— Ak sa zistila chyba integrity v atribútoch súboru, karta považuje súbor za poškodený a neopraviteľný, vrátený stav spracovania je '**6400**' alebo '**6581**'.

— Ak sa zistila chyba integrity v uložených údajoch, karta vráti požadované údaje a vrátený stav spracovania je '**6281**'.

3.5.2.1.1 Príkaz so zabezpečeným spracovaním (príklady)

Tento príkaz umožňuje IFD čítanie dát z aktuálne zvoleného EF so zabezpečeným spracovaním s cieľom overiť integritu prijatých údajov a chrániť ich dôvernosť, ak sa uplatňuje podmienka zabezpečenia SM-R-ENC-MAC-G1 (generácia 1) alebo SM-R-ENC-MAC-G2 (generácia 2).

TCS_44 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	‘0Ch’	Požaduje sa zabezpečené spracovanie správ
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	P1 (offset od začiatku súboru v bajtoch): bajt najvyššieho rádu
P2	1	‘XXh’	P2 (offset od začiatku súboru v bajtoch): bajt najnižšieho rádu
Lc	1	‘XXh’	Dĺžka vstupných údajov pre zabezpečené spracovanie
#6	1	‘97h’	T_{LE}: Tag pre špecifikáciu očakávanej dĺžky.
#7	1	‘01h’	L_{LE}: Dĺžka očakávanej dĺžky
#8	1	‘NNh’	Špecifikácia očakávanej dĺžky (pôvodná Le): počet bajtov, ktoré sa majú čítať
#9	1	‘8Eh’	T_{CC}: Tag pre kryptografický kontrolný súčet
#10	1	‘XXh’	L_{CC}: Dĺžka nasledujúceho kryptografického kontrolného súčtu ‘04h’ pre zabezpečené spracovanie v generácii 1 (pozri dodatok 11 časť A) ‘08h’, ‘0Ch’ alebo ‘10h’ v závislosti od dĺžky kľúča AES pre zabezpečené spracovanie v generácii 2 (pozri dodatok 11 časť B)
#11-#(10+L)	L	‘XX..XXh’	Kryptografický kontrolný súčet
Le	1	‘00h’	Špecifikované v ISO/IEC 7816-4

TCS_45 **Odpovedacia správa, ak sa nevyžaduje SM-R-ENC-MAC-G1 (generácia 1) / SM-R-ENC-MAC-G2 (generácia 2) a ak je správny vstupný formát zabezpečeného spracovania:**

Bajt	Dĺžka	Hodnota	Opis
#1	1	‘99h’	Tag pre stav spracovania (SW1-SW2) – voliteľné pre zabezpečené spracovanie v generácii 1
#2	1	‘02h’	Dĺžka stavu spracovania
#3 – #4	2	‘XX XXh’	Stav spracovania nechránenej odpovede APDU
#5	1	‘81h’	T_{PV}: Tag pre údaje s nešifrovanou hodnotou
#6	L	‘NNh’ alebo ‘81 NNh’	L_{PV}: dĺžka vrátených údajov (= pôvodná Le). L je 2 bajty, ak L_{PV}>127 bajtov.

Bajt	Dĺžka	Hodnota	Opis
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Hodnota nešifrovaných údajov
#(6+L+NN)	1	'8Eh'	T_{CC}: Tag pre kryptografický kontrolný súčet
#(7+L+NN)	1	'XXh'	L_{CC}: Dĺžka nasledujúceho kryptografického kontrolného súčtu '04h' pre zabezpečené spracovanie v generácii 1 (pozri dodatok 11 časť A) '08h', '0Ch' alebo '10h' v závislosti od dĺžky kľúča AES pre zabezpečené spracovanie v generácii 2 (pozri dodatok 11 časť B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kryptografický kontrolný súčet
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

TCS_46 **Odpovedacia správa, ak sa vyžaduje SM-R-ENC-MAC-G1 (generácia 1) / SM-R-ENC-MAC-G2 (generácia 2) a ak je správny vstupný formát zabezpečeného spracovania:**

Bajt	Dĺžka	Hodnota	Opis
#1	1	'87h'	$T_{PI\ CG}$: Tag pre šifrované údaje (kryptogram)
#2	L	'MMh' alebo '81 MMh'	$L_{PI\ CG}$: dĺžka vrátených šifrovaných údajov (odlišná od pôvodnej Le príkazu v dôsledku výplne – „padding“). L je 2 bajty, ak $L_{PI\ CG}$ > 127 bajtov.
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Šifrované údaje: Indikátor výplne a kryptogram
#(2+L+MM)	1	'99h'	Tag pre stav spracovania (SW1-SW2) – voliteľné pre zabezpečené spracovanie v generácii 1
#(3+L+MM)	1	'02h'	Dĺžka stavu spracovania
#(4+L+MM) – #(5+L+MM)	2	'XX XXh'	Stav spracovania nechránenej odpovede APDU
#(6+L+MM)	1	'8Eh'	T_{CC}: Tag pre kryptografický kontrolný súčet
#(7+L+MM)	1	'XXh'	L_{CC}: Dĺžka nasledujúceho kryptografického kontrolného súčtu '04h' pre zabezpečené spracovanie v generácii 1 (pozri dodatok 11 časť A) '08h', '0Ch' alebo '10h' v závislosti od dĺžky kľúča AES pre zabezpečené spracovanie v generácii 2 (pozri dodatok 11 časť B)
#(8+L+MM)-#(7+N+L+MM)	N	'XX..XXh'	Kryptografický kontrolný súčet
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

Príkaz READ BINARY môže vrátiť bežné stavy spracovania uvedené v TCS_43 pod tagom '99h' opísaným v TCS_59 pomocou štruktúry odpovede v rámci zabezpečeného spracovania.

Okrem toho sa môžu vyskytnúť niektoré chyby špecifické pre zabezpečené spracovanie. V takom prípade sa stav spracovania jednoducho vráti bez akéhokoľvek zapojenia štruktúry zabezpečeného spracovania:

TCS_47 **Odpovedacia správa pri nesprávnom vstupnom formáte zabezpečeného spracovania**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak nie je dostupný aktuálny kľúč relácie, vrátený stav spracovania je '**6A88**'. Stane sa to, ak ešte nebol vygenerovaný kľúč relácie alebo ak uplynula jeho platnosť (v takom prípade musí IFD opäť spustiť vzájomnú autentifikáciu a nastaviť nový kľúč relácie).

— Ak vo formáte zabezpečeného spracovania chýbajú niektoré očakávané dátové objekty (opísané vyššie), vráti sa stav spracovania '**6987**': táto chyba nastane, ak chýba očakávaný tag alebo ak nie je správne zostavené telo príkazu.

— Ak sú niektoré dátové objekty nesprávne, vráti sa stav spracovania '**6988**': táto chyba nastane, ak sú prítomné všetky požadované tagy, ale niektoré dĺžky sú iné, než sa očakáva.

— Ak zlyhá overenie kryptografického kontrolného súčtu vráti sa stav spracovania '**6688**'.

3.5.2.2 Príkaz s krátkym identifikátorom EF (elementárneho súboru).

Tento príkazový variant umožňuje IFD zvoliť EF jeho krátkym identifikátorom a prečítať z neho údaje.

TCS_48 Tachografová karta musí tento príkazový variant podporovať pre všetky elementárne súbory so stanoveným krátkym identifikátorom EF. Krátke identifikátory sú špecifikované v kapitole 4.

TCS_49 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Bit 8 je nastavený na 1 Bity 7 a 6 sú nastavené na 00 Bity 5 – 1 určujú krátky identifikátor príslušného EF
P2	1	'XXh'	Určuje offset od 0 do 255 bajtov v EF uvedenom v P1.
Le	1	'XXh'	Očakávaná dĺžka údajov. Počet bajtov, ktoré sa majú čítať.

Poznámka: Krátke identifikátory EF použité pre tachografovú aplikáciu generácie 2 sú špecifikované v kapitole 4.

Ak P1 určuje krátky identifikátor EF a príkaz je úspešný, identifikovaný EF sa stáva aktuálne zvoleným EF (aktuálny EF).

TCS_50 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
#1-#L	L	'XX..XXh'	Prečítané údaje
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak sa nenašiel súbor zodpovedajúci krátkemu identifikátoru EF, vrátený stav spracovania je '**6A82**'.

— Ak nie sú splnené podmienky zabezpečenia zvoleného súboru, príkaz sa preruší s '**6982**'.

— Ak offset nie je kompatibilný s veľkosťou EF (offset > veľkosť EF), vrátený stav spracovania je '**6B00**'.

— Ak nie je veľkosť čítaných údajov kompatibilná s veľkosťou EF (offset + Le > veľkosť EF), vrátený stav spracovania je '**6700**' alebo '**6Cxx**', pričom „xx" je presná dĺžka.

— Ak sa zistila chyba integrity v atribútoch súboru, karta považuje súbor za poškodený a neopraviteľný, vrátený stav spracovania je '**6400**' alebo '**6581**'.

— Ak sa zistila chyba integrity v uložených údajoch, karta vráti požadované údaje a vrátený stav spracovania je '**6281**'.

3.5.2.3 Príkaz s nepárnym príkazovým bajtom (odd instruction byte)

Tento príkazový variant umožňuje IFD čítanie údajov z EF o veľkosti 32 768 alebo viac bajtov.

TCS_51 Tachografová karta, ktorá podporuje EF o veľkosti 32 768 alebo viac bajtov musí tento príkazový variant pre dané EF podporovať. Tachografová karta môže, ale nemusí podporovať tento príkazový variant pre ostatné EF, s výnimkou EF Sensor_Installation_Data, pozri TCS_156 a TCS_160.

TCS_52 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'B1h'	Read Binary
P1	1	'00h'	Aktuálny EF
P2	1	'00h'	
Lc	1	'NNh'	Lc dĺžka offsetového dátového objektu.
#6-#(5+NN)	NN	'XX..XXh'	Offsetový dátový objekt: Tag '54h' Dĺžka '01h' alebo '02h' Hodnota offset
Le	1	'XXh'	Počet bajtov, ktoré sa majú čítať.

IFD musí kódovať dĺžku offsetového dátového objektu minimálnym možným počtom oktetov, teda IFD kóduje offset od 0 do 255 dĺžkovým bajtom '01h' a offset od '256' do '65 535' bajtov dĺžkovým bajtom '02h'.

TCS_53 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
#1-#L	L	'XX..XXh'	Čítané údaje uzavreté v diskrečnom dátovom objekte s tagom '53h'.
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak nie je zvolený žiadny EF, vrátený stav spracovania je '**6986**'.

— Ak nie sú splnené podmienky zabezpečenia zvoleného súboru, príkaz sa preruší s '**6982**'.

— Ak offset nie je kompatibilný s veľkosťou EF (offset > veľkosť EF), vrátený stav spracovania je '**6B00**'.

— Ak nie je veľkosť čítaných údajov kompatibilná s veľkosťou EF (offset + Le > veľkosť EF), vrátený stav spracovania je '**6700**' alebo '**6Cxx**', pričom „xx" je presná dĺžka.

— Ak sa zistila chyba integrity v atribútoch súboru, karta považuje súbor za poškodený a neopraviteľný, vrátený stav spracovania je '**6400**' alebo '**6581**'.

— Ak sa zistila chyba integrity v uložených údajoch, karta vráti požadované údaje a vrátený stav spracovania je '**6281**'.

3.5.2.3.1 Príkaz so zabezpečeným spracovaním (príklad)

Nasledujúci príklad ukazuje použitie zabezpečeného spracovania, ak sa uplatňuje podmienka zabezpečenia SM-MAC-G2.

TCS_54 Príkazová správa

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'0Ch'	Požaduje sa zabezpečené spracovanie správ
INS	1	'B1h'	Read Binary
P1	1	'00h'	Aktuálny EF
P2	1	'00h'	
Lc	1	'XXh'	Dĺžka zabezpečeného dátového poľa
#6	1	'B3h'	Tag pre údaje s nešifrovanou hodnotou kódované v BER-TLV
#7	1	'NNh'	L_{PV}: dĺžka prenášaných údajov
#(8)-#(7+NN)	NN	'XX..XXh'	Nešifrované údaje kódované v BER-TLV, t. j. offsetový dátový objekt s tagom '54'
#(8+NN)	1	'97h'	T_{LE}: Tag pre špecifikáciu očakávanej dĺžky.
#(9+NN)	1	'01h'	L_{LE}: Dĺžka očakávanej dĺžky
#(10+NN)	1	'XXh'	Špecifikácia očakávanej dĺžky (pôvodná Le): počet bajtov, ktoré sa majú čítať
#(11+NN)	1	'8Eh'	T_{CC}: Tag pre kryptografický kontrolný súčet
#(12+NN)	1	'XXh'	L_{CC}: Dĺžka nasledujúceho kryptografického kontrolného súčtu '08h', '0Ch' alebo '10h' v závislosti od dĺžky kľúča AES pre zabezpečené spracovanie v generácii 2 (pozri dodatok 11 časť B)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Kryptografický kontrolný súčet
Le	1	'00h'	Špecifikované v ISO/IEC 7816-4

TCS_55 Odpovedacia správa, ak je príkaz úspešný

Bajt	Dĺžka	Hodnota	Opis
#1	1	'B3h'	Nešifrované údaje kódované v BER-TLV
#2	L	'NNh' alebo '81 NNh'	L_{PV}: dĺžka vrátených údajov (= pôvodná Le). L je 2 bajty, ak L_{PV}>127 bajtov.
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Hodnota nešifrovaných údajov kódovaná v BER-TLV, t. j. čítané údaje uzavreté v diskrečnom dátovom objekte s tagom '53h'.
#(2+L+NN)	1	'99h'	Stav spracovania nechránenej odpovede APDU
#(3+L+NN)	1	'02h'	Dĺžka stavu spracovania
#(4+L+NN) – #(5+L+NN)	2	'XX XXh'	Stav spracovania nechránenej odpovede APDU
#(6+L+NN)	1	'8Eh'	T_{CC}: Tag pre kryptografický kontrolný súčet
#(7+L+NN)	1	'XXh'	L_{CC}: Dĺžka nasledujúceho kryptografického kontrolného súčtu '08h', '0Ch' alebo '10h' v závislosti od dĺžky kľúča AES pre zabezpečené spracovanie v generácii 2 (pozri dodatok 11 časť B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kryptografický kontrolný súčet
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

3.5.3 *UPDATE BINARY*

Tento príkaz zodpovedá norme ISO/IEC 7816-4, no v porovnaní s príkazom vymedzeným v norme má obmedzené použitie.

Príkazová správa UPDATE BINARY iniciuje aktualizáciu (výmaz + zápis) bitov, ktoré už sú prítomné v binárnom EF, bitmi danými v príkaze APDU.

3.5.3.1 Príkaz s offsetom v P1-P2

Tento príkaz umožňuje IFD písať údaje do aktuálne zvoleného EF bez toho, aby karta overila integritu prijímaných dát.

Poznámka: Tento príkaz bez zabezpečeného spracovania možno použiť len na aktualizáciu súboru, ktorý podporuje podmienku zabezpečenia ALW v režime prístupu na aktualizáciu.

TCS_56 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'D6h'	Update Binary

Bajt	Dĺžka	Hodnota	Opis
P1	1	'XXh'	Offset od začiatku súboru v bajtoch: bajt najvyššieho rádu
P2	1	'XXh'	Offset od začiatku súboru v bajtoch: bajt najnižšieho rádu
Lc	1	'NNh'	Lc dĺžka údajov, ktoré sa majú aktualizovať. Počet bajtov, ktoré sa majú zapísať.
#6-#(5+NN)	NN	'XX..XXh'	Údaje na zápis

Poznámka: bit 8 P1 musí byť nastavený na 0.

TCS_57 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak nie je zvolený žiadny EF, vrátený stav spracovania je '**6986**'.

— Ak nie sú splnené podmienky zabezpečenia zvoleného súboru, príkaz sa preruší s '**6982**'.

— Ak offset nie je kompatibilný s veľkosťou EF (offset > veľkosť EF), vrátený stav spracovania je '**6B00**'.

— Ak nie je veľkosť údajov na zápis kompatibilná s veľkosťou EF (offset + Lc > veľkosť EF), vrátený stav spracovania je '**6700**'.

— Ak sa zistila chyba integrity v atribútoch súboru, karta považuje súbor za poškodený a neopraviteľný, vrátený stav spracovania je '**6400**' alebo '**6500**'.

— Ak je neúspešný zápis, vrátený stav spracovania je '**6581**'.

3.5.3.1.1 Príkaz so zabezpečeným spracovaním (príklady)

Tento príkaz umožňuje IFD písať údaje do aktuálne zvoleného EF, pričom karta overuje integritu prijímaných dát. Keďže sa nevyžaduje dôvernosť, údaje nie sú šifrované.

TCS_58 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'0Ch'	Požaduje sa zabezpečené spracovanie správ
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Offset od začiatku súboru v bajtoch: bajt najvyššieho rádu
P2	1	'XXh'	Offset od začiatku súboru v bajtoch: bajt najnižšieho rádu
Lc	1	'XXh'	Dĺžka zabezpečeného dátového poľa

Bajt	Dĺžka	Hodnota	Opis
#6	1	'81h'	T_{PV}: Tag pre údaje s nešifrovanou hodnotou
#7	L	'NNh' alebo '81 NNh'	L_{PV}: dĺžka prenášaných údajov. L je 2 bajty, ak L_{PV} > 127 bajtov.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Hodnota nešifrovaných údajov (údaje na zápis)
#(7+L+NN)	1	'8Eh'	T_{CC}: Tag pre kryptografický kontrolný súčet
#(8+L+NN)	1	'XXh'	L_{CC}: Dĺžka nasledujúceho kryptografického kontrolného súčtu '04h' pre zabezpečené spracovanie v generácii 1 (pozri dodatok 11 časť A) '08h', '0Ch' alebo '10h' v závislosti od dĺžky kľúča AES pre zabezpečené spracovanie v generácii 2 (pozri dodatok 11 časť B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Kryptografický kontrolný súčet
Le	1	'00h'	Špecifikované v ISO/IEC 7816-4

TCS_59 **Odpovedacia správa ak je vstupný formát zabezpečeného spracovania správny**

Bajt	Dĺžka	Hodnota	Opis
#1	1	'99h'	T_{SW}: Tag pre stavové slová (ktoré má chrániť CC)
#2	1	'02h'	L_{SW}: dĺžka vrátených stavových slov
#3-#4	2	'XXXXh'	Stav spracovania nechránenej odpovede APDU
#5	1	'8Eh'	T_{CC}: Tag pre kryptografický kontrolný súčet
#6	1	'XXh'	L_{CC}: Dĺžka nasledujúceho kryptografického kontrolného súčtu '04h' pre zabezpečené spracovanie v generácii 1 (pozri dodatok 11 časť A) '08h', '0Ch' alebo '10h' v závislosti od dĺžky kľúča AES pre zabezpečené spracovanie v generácii 2 (pozri dodatok 11 časť B)
#7-#(6+L)	L	'XX..XXh'	Kryptografický kontrolný súčet
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

„Bežné" stavy spracovania opísané pre príkaz UPDATE BINARY bez zabezpečeného spracovania (pozri §3.5.3.1) môžu byť vrátené s použitím vyššie opísanej štruktúry odpovedacej správy.

Okrem toho sa môžu vyskytnúť niektoré chyby špecifické pre zabezpečené spracovanie. V takom prípade sa stav spracovania jednoducho vráti bez akéhokoľvek zapojenia štruktúry zabezpečeného spracovania:

TCS_60 **Odpovedacia správa pri chybe v zabezpečenom spracovaní**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak nie je dostupný aktuálny kľúč relácie, vrátený stav spracovania je '**6A88**'.

— Ak vo formáte zabezpečeného spracovania chýbajú niektoré očakávané dátové objekty (opísané vyššie), vráti sa stav spracovania '**6987**': táto chyba nastane, ak chýba očakávaný tag alebo ak nie je správne zostavené telo príkazu.

— Ak sú niektoré dátové objekty nesprávne, vráti sa stav spracovania '**6988**': táto chyba nastane, ak sú prítomné všetky požadované tagy, ale niektoré dĺžky sú iné, než sa očakáva.

— Ak zlyhá overenie kryptografického kontrolného súčtu vráti sa stav spracovania '**6688**'.

3.5.3.2 Príkaz s krátkym identifikátorom EF

Tento príkazový variant umožňuje IFD zvoliť EF jeho krátkym identifikátorom a zapísať z neho údaje.

TCS_61 Tachografová karta musí tento príkazový variant podporovať pre všetky elementárne súbory so stanoveným krátkym identifikátorom EF. Krátke identifikátory sú špecifikované v kapitole 4.

TCS_62 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Bit 8 je nastavený na 1 Bity 7 a 6 sú nastavené na 00 Bity 5 – 1 určujú krátky identifikátor príslušného EF
P2	1	'XXh'	Určuje offset od 0 do 255 bajtov v EF uvedenom v P1
Lc	1	'NNh'	Lc dĺžka údajov, ktoré sa majú aktualizovať. Počet bajtov, ktoré sa majú zapísať.
#6-#(5+NN)	NN	'XX..XXh'	Údaje na zápis

TCS_63 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

Poznámka: Krátke identifikátory EF použité pre tachografovú aplikáciu generácie 2 sú špecifikované v kapitole 4.

Ak P1 určuje krátky identifikátor EF a príkaz je úspešný, identifikovaný EF sa stáva aktuálne zvoleným EF (aktuálny EF).

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak sa nenašiel súbor zodpovedajúci krátkemu identifikátoru EF, vrátený stav spracovania je '**6A82**'.

— Ak nie sú splnené podmienky zabezpečenia zvoleného súboru, príkaz sa preruší s '**6982**'.

— Ak offset nie je kompatibilný s veľkosťou EF (offset > veľkosť EF), vrátený stav spracovania je '**6B00**'.

— Ak nie je veľkosť údajov na zápis kompatibilná s veľkosťou EF (offset + Lc > veľkosť EF), vrátený stav spracovania je '**6700**'.

— Ak sa zistila chyba integrity v atribútoch súboru, karta považuje súbor za poškodený a neopraviteľný, vrátený stav spracovania je '**6400**' alebo '**6581**'.

— Ak je neúspešný zápis, vrátený stav spracovania je '**6581**'.

3.5.3.3 Príkaz s nepárnym príkazovým bajtom (odd instruction byte)

Tento príkazový variant umožňuje IFD zápis údajov do EF o veľkosti 32 768 alebo viac bajtov.

TCS_64 Tachografová karta, ktorá podporuje EF o veľkosti 32 768 alebo viac bajtov musí tento príkazový variant pre dané EF podporovať. Tachografová karta môže, ale nemusí podporovať tento príkaz variant pre ostatné EF.

TCS_65 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'D7h'	Update Binary
P1	1	'00h'	Aktuálny EF
P2	1	'00h'	
Lc	1	'NNh'	Lc Dĺžka údajov v príkazovom dátovom poli
#6-#(5+NN)	NN	'XX..XXh'	Offsetový dátový objekt s tagom '54h' || diskrečný dátový objekt s tagom '53h', v ktorom sú uzavreté údaje na zápis

IFD musí kódovať dĺžku offsetového dátového objektu a diskrečného dátového objektu minimálnym možným počtom oktetov, teda IFD kóduje offset / dĺžku od 0 do 255 dĺžkovým bajtom '01h' a offset / dĺžku od '256' do '65 535' bajtov dĺžkovým bajtom '02h'.

TCS_66 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak nie je zvolený žiadny EF, vrátený stav spracovania je '**6986**'.

— Ak nie sú splnené podmienky zabezpečenia zvoleného súboru, príkaz sa preruší s '**6982**'.

— Ak offset nie je kompatibilný s veľkosťou EF (offset > veľkosť EF), vrátený stav spracovania je '**6B00**'.

— Ak nie je veľkosť údajov na zápis kompatibilná s veľkosťou EF (offset + Lc > veľkosť EF), vrátený stav spracovania je '**6700**'.

— Ak sa zistila chyba integrity v atribútoch súboru, karta považuje súbor za poškodený a neopraviteľný, vrátený stav spracovania je '**6400**' alebo '**6500**'.

— Ak je neúspešný zápis, vrátený stav spracovania je '**6581**'.

3.5.3.3.1 Príkaz so zabezpečeným spracovaním (príklad)

Nasledujúci príklad ukazuje použitie zabezpečeného spracovania, ak sa uplatňuje podmienka zabezpečenia SM-MAC-G2.

TCS_67 Príkazová správa

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'0Ch'	Požaduje sa zabezpečené spracovanie správ
INS	1	'D7h'	Update Binary
P1	1	'00h'	Aktuálny EF
P2	1	'00h'	
Lc	1	'XXh'	Dĺžka zabezpečeného dátového poľa
#6	1	'B3h'	Tag pre údaje s nešifrovanou hodnotou kódované v BER-TLV
#7	L	'NNh' alebo '81 NNh'	L_{PV}: dĺžka prenášaných údajov. L je 2 bajty, ak L_{PV} > 127 bajtov.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Nešifrované údaje kódované v BER-TLV, t. j. offsetový dátový objekt s tagom '54h' || diskrečný dátový objekt s tagom '53h', v ktorom sú uzavreté údaje na zápis.
#(7+L+NN)	1	'8Eh'	T_{CC}: Tag pre kryptografický kontrolný súčet
#(8+L+NN)	1	'XXh'	L_{CC}: Dĺžka nasledujúceho kryptografického kontrolného súčtu '08h', '0Ch' alebo '10h' v závislosti od dĺžky kľúča AES pre zabezpečené spracovanie v generácii 2 (pozri dodatok 11 časť B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Kryptografický kontrolný súčet
Le	1	'00h'	Špecifikované v ISO/IEC 7816-4

TCS_68 Odpovedacia správa, ak je príkaz úspešný

Bajt	Dĺžka	Hodnota	Opis
#1	1	'99h'	T_{SW}: Tag pre stavové slová (ktoré má chrániť CC)
#2	1	'02h'	L_{SW}: dĺžka vrátených stavových slov
#3-#4	2	'XXXXh'	Stav spracovania nechránenej odpovede APDU
#5	1	'8Eh'	T_{CC}: Tag pre kryptografický kontrolný súčet

Bajt	Dĺžka	Hodnota	Opis
#6	1	'XXh'	L_{CC}: Dĺžka nasledujúceho kryptografického kontrolného súčtu '08h', '0Ch' alebo '10h' v závislosti od dĺžky kľúča AES pre zabezpečené spracovanie v generácii 2 (pozri dodatok 11 časť B)
#7-#(6+L)	L	'XX..XXh'	Kryptografický kontrolný súčet
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

3.5.4 *GET CHALLENGE*

Tento príkaz zodpovedá norme ISO/IEC 7816-4, no v porovnaní s príkazom vymedzeným v norme má obmedzené použitie.

Príkaz GET CHALLENGE žiada od karty, aby vydala výzvu na účely použitia pri bezpečnostnom postupe, v ktorom sa karte zasiela kryptogram alebo určité šifrované údaje.

TCS_69 Výzva vydaná kartou je platná len pre nasledujúci príkaz, ktorý použije výzvu odoslanú na kartu.

TCS_70 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (očakávaná dĺžka výzvy).

TCS_71 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
#1-#8	8	'XX..XXh'	Výzva
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak sa Le líši od '08h', stav spracovania je '**6700**'

— ak sú parametre P1-P2 nesprávne, stav spracovania je '**6A86**'.

3.5.5 *VERIFY*

Tento príkaz zodpovedá norme ISO/IEC 7816-4, no v porovnaní s príkazom vymedzeným v norme má obmedzené použitie.

Príkaz musí podporovať iba dielenská karta.

Ostatné typy tachografových kariet tento príkaz môžu, ale nemusia implementovať, no pri týchto kartách nie je žiadna referencia CHV personalizovaná. Preto takéto karty nedokážu daný príkaz úspešne vykonať. Pri iných než dielenských tachografových kartách je správanie (teda vrátený kód chyby) mimo rozsahu tejto špecifikácie, ak sa príkaz odošle.

Príkaz Verify iniciuje na karte porovnanie údajov CHV (PIN) odoslaných z príkazu s referenčným CHV uloženým na karte.

TCS_72 PIN zadaný používateľom musí IFD kódovať v ASCI a sprava doplniť bajtmi 'FFh' do dĺžky 8 bajtov, pozri tiež dátový typ WorkshopCardPIN v dodatku 1.

TCS_73 Tachografové aplikácie generácie 1 a 2 používajú rovnaké referenčné CHV.

TCS_74 Tachografová karta overí, či je príkaz kódovaný správne. Ak príkaz nie je kódovaný správne, karta neporovnáva hodnoty CHV, ani nezníži počet zostávajúcich pokusov o zadanie CHV a neresetuje bezpečnostný stav „PIN_Verified", ale príkaz preruší. Príkaz je kódovaný správne, ak majú bajty CLA, INS, P1, P2, Lc určené hodnoty, Le absentuje a dátové pole príkazu má správnu dĺžku.

TCS_75 Ak je príkaz úspešný, počítadlo zostávajúcich pokusov o zadanie CHV sa vráti na počiatočnú hodnotu. Počiatočná hodnota počítadla zostávajúcich pokusov o zadanie CHV je 5. Ak je príkaz úspešný, karta odošle interný bezpečnostný stav „PIN_Verified". Karta tento bezpečnostný stav resetuje, ak je karta resetovaná alebo ak kód CHV prenášaný príkazom nezodpovedá uloženému referenčnému CHV.

Poznámka: Ak sa použije rovnaké referenčné CHV a globálny bezpečnostný stav, zamestnanec dielne nemusí opätovne zadávať PIN pri výbere iného DF tachografovej aplikácie.

TCS_76 Neúspešné porovnanie sa zaznamená na karte, t. j. počítadlo zostávajúcich pokusov o zadanie CHV sa zníži o 1, aby sa obmedzil počet ďalších pokusov o použitie referenčného CHV.

TCS_77 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (overované CHV je implicitne známe)
Lc	1	'08h'	Dĺžka prenášaného kódu CHV
#6-#13	8	'XX..XXh'	CHV

TCS_78 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak sa nenašlo referenčné CHV, vrátený stav spracovania je '**6A88**'.

— Ak je CHV blokované, (počítadlo zostávajúcich pokusov je na nule), vrátený stav spracovania je '**6983**'. Keď sa dosiahne tento stav, nesmie sa CHV už nikdy opäť úspešne prezentovať.

— Ak je porovnanie neúspešné, počítadlo zostávajúcich pokusov sa zníži a vráti sa stav '**63CX**' (X > 0 a X sa rovná stavu počítadla zostávajúcich pokusov).

— Ak sa referenčné CHV považuje za poškodené, vrátený stav spracovania je '**6400**' alebo '**6581**'.

— Ak sa Lc líši od '08h', stav spracovania je '**6700**'.

3.5.6 *GET RESPONSE*

Tento príkaz zodpovedá norme ISO/IEC 7816-4.

Tento príkaz (potrebný a dostupný len pre protokol T=0) sa používa na prenos pripravených údajov z karty do zariadenia s rozhraním (prípad, keď príkaz zahŕňal Lc aj Le).

Príkaz GET RESPONSE musí byť vydaný hneď po príkaze, ktorý pripravuje údaje, inak sa údaje stratia. Po vykonaní príkazu GET RESPONSE (okrem prípadu, keď nastane chyba '**61xx**' alebo '**6Cxx**', pozri nižšie), už predtým pripravené údaje nie sú dostupné.

TCS_79 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Očakávaný počet bajtov

TCS_80 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
#1-#X	X	'XX..XXh'	Údaje
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak karta nepripravila žiadne údaje, vrátený stav spracovania je '**6900**' alebo '**6F00**'.

— Ak Le presiahne počet dostupných bajtov alebo ak je Le nulová, vrátený stav spracovania je '**6Cxx**', pričom „xx" uvádza presný počet dostupných bajtov. V takom prípade sú pripravené údaje stále dostupné pre nasledujúci príkaz GET RESPONSE.

— Ak Le nie je nulová a je menšia než počet dostupných bajtov, karta zašle požadované údaje normálne a vrátený stav spracovania je '**61xx**', pričom „xx" uvádza počet dodatočných bajtov, ktoré sú ešte stále dostupné pre nasledujúci príkaz GET RESPONSE.

— Ak príkaz nie je podporovaný (protokol T=1), karta vráti '**6D00**'.

3.5.7 *PSO: VERIFY CERTIFICATE*

Tento príkaz zodpovedá norme ISO/IEC 7816-8, no v porovnaní s príkazom vymedzeným v norme má obmedzené použitie.

Príkaz VERIFY CERTIFICATE karta použije na získanie verejného kľúča zvonku a na kontrolu jeho platnosti.

3.5.7.1 Pár príkaz – odpoveď v generácii 1

TCS_81 Tento príkazový variant podporuje len aplikácia tachografu generácie 1.

TCS_82 Keď je príkaz VERIFY CERTIFICATE úspešný, verejný kľúč sa uloží na budúce použitie v prostredí zabezpečenia. Tento kľúč sa explicitne nastaví na použitie v príkazoch vzťahujúcich sa k zabezpečeniu (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE alebo VERIFY CERTIFICATE) prostredníctvom príkazu MSE (pozri §3.5.11) s použitím jeho identifikátora kľúča.

TCS_83 V každom prípade príkaz VERIFY CERTIFICATE používa verejný kľúč, ktorý bol predtým zvolený príkazom MSE na otvorenie certifikátu. Musí ísť o verejný kľúč jedného z členských štátov alebo Európy.

TCS_84 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'2Ah'	Perform Security Operation (vykonanie operácie zabezpečenia)
P1	1	'00h'	P1
P2	1	'AEh'	P2: údaje nekódované v BER-TLV (zreťazenie dátových prvkov)
Lc	1	'C2h'	Lc: Dĺžka certifikátu, 194 bajtov
#6-#199	194	'XX..XXh'	Certifikát: zreťazenie dátových prvkov (podľa dodatku 11)

TCS_85 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak zlyhá overenie certifikátu, vrátený stav spracovania je '**6688**'. Proces overenia a rozbalenia certifikátu je pre G1 a G2 opísaný v dodatku 11.

— Ak nie je v prostredí zabezpečenia prítomný žiadny verejný kľúč, vráti sa '**6A88**'.

— Ak sa zvolený verejný kľúč (použitý na rozbalenie certifikátu) považuje za poškodený, vrátený stav spracovania je '**6400**' alebo '**6581**'.

— Len pre generáciu 1: Ak má zvolený verejný kľúč (použitý na rozbalenie certifikátu) CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) iné než '00' (teda nejde o kľúč členského štátu ani Európy), vráti sa stav spracovania '**6985**'.

3.5.7.2 Pár príkaz – odpoveď v generácii 2

V závislosti od veľkosti krivky môžu byť certifikáty ECC také dlhé, že ich nemožno preniesť v jednom APDU. Vtedy treba použiť reťazenie príkazov podľa ISO/IEC 7816-4 a prenos certifikátu prebehne v dvoch nadväzujúcich APDU PSO: Verify Certificate.

Štruktúra certifikátu a parametre domény sú vymedzené v dodatku 11.

TCS_86 Príkaz možno vykonať v MF, DF Tachograph a DF Tachograph_G2, pozri tiež TCS_33.

TCS_87 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'X0h'	Bajt CLA udávajúci reťazenie príkazu: '00h' jediný alebo posledný príkaz v reťazci '10h' iný než posledný príkaz v reťazci
INS	1	'2Ah'	Perform Security Operation (vykonanie operácie zabezpečenia)
P1	1	'00h'	
P2	1	'BEh'	Verify self-descriptive certificate (overenie samoopisného certifikátu)
Lc	1	'XXh'	Dĺžka dátového poľa príkazu, pozri TCS_88 a TCS_89.
#6-#5+L	L	'XX..XXh'	Údaje kódované DER-TLV: Dátový objekt ECC Certificate Body (hlavná časť certifikátu) ako prvý dátový objekt zreťazený s dátovým objektom ECC Certificate Signature (podpis) ako druhým dátovým objektom, alebo časť tohto reťazca. Tag '7F21' a príslušná dĺžka sa neprenášajú. Poradie týchto dátových objektov je nemenné.

TCS_88 Pri krátkych APDU platia tieto pravidlá: IFD použije minimálny počet APDU potrebný na prenos obsahu príkazu, pričom v prvom APDU prenesie maximálny počet bajtov, v závislosti od hodnoty bajtu „veľkosť informačného poľa karty", pozri TCS_14. Ak sa IFD správa inak, správanie karty je mimo rozsahu.

TCS_89 Pri rozšírených APDU platia tieto pravidlá: Ak sa certifikát nezmestí do jediného APDU, karta musí podporovať reťazenie príkazov. IFD použije minimálny počet APDU potrebný na prenos obsahu príkazu, pričom v prvom APDU prenesie maximálny počet bajtov. Ak sa IFD správa inak, správanie karty je mimo rozsahu.

Poznámka: Podľa dodatku 11 karta uchová certifikát alebo relevantný obsah certifikátu a aktualizuje svoj currentAuthenticatedTime.

Štruktúra odpovedacej správy a stavové slová sú vymedzené v TCS_85.

TCS_90 Okrem kódov chýb uvedených v TCS_85môže karta vrátiť tieto kódy chýb:

— Ak má zvolený verejný kľúč (použitý na rozbalenie certifikátu) CHA.LSB (CertificateHolderAuthorisation.equipmentType) nevhodné na overenie certifikátu podľa dodatku 11, vráti sa stav spracovania '**6985**'.

— Ak je čas currentAuthenticatedTime na karte neskorší, než dátum uplynutia platnosti certifikátu, vráti sa stav spracovania '**6985**'.

— Ak sa očakáva posledný príkaz reťazca, karta vráti '**6883**'.

— Ak sú v dátovom poli príkazu odoslané nesprávne parametre, karta vráti '**6A80**' (platí aj keď dátové objekty nie sú zaslané v stanovenom poradí).

3.5.8 *INTERNAL AUTHENTICATE*

Tento príkaz zodpovedá norme ISO/IEC 7816-4.

TCS_91 Všetky tachografové karty musia tento príkaz podporovať v DF Tachograph generácie 1. Príkaz môže, ale nemusí byť dostupný v MF a/alebo v DF Tachograph_G2. V takom prípade sa príkaz preruší vhodným kódom chyby, keďže súkromný kľúč karty (Card.SK) pre autentifikačný protokol generácie 1 je dostupný len v DF_Tachograph generácie 1.

Príkazom INTERNAL AUTHENTICATE môže IFD autentifikovať kartu. Proces autentifikácie je opísaný v dodatku 11. Zahŕňa tieto prvky:

TCS_92 Príkaz INTERNAL AUTHENTICATE používa súkromný kľúč karty (zvolený implicitne) na podpis autentifikačných údajov vrátane K1 (prvý prvok kľúčovej dohody relácie) a RND1 a používa aktuálne zvolený verejný kľúč (pomocou posledného príkazu MSE) na zašifrovanie podpisu a vytvorenie autentifikačného znaku (bližšie informácie v dodatku 11).

TCS_93 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Dĺžka údajov poslaných na kartu
#6 – #13	8	'XX..XXh'	Výzva použitá na autentifikáciu karty
#14 -#21	8	'XX..XXh'	VU.CHR (pozri dodatok 11)
Le	1	'80h'	Dĺžka údajov očakávaných od karty

TCS_94 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
#1-#128	128	'XX..XXh'	Overovací znak karty (pozri dodatok 11)
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak nie je v prostredí zabezpečenia prítomný žiadny verejný kľúč, vrátený stav spracovania je '**6A88**'.

— Ak nie je v prostredí zabezpečenia prítomný žiadny súkromný kľúč, vrátený stav spracovania je '**6A88**'.

— Ak sa VU.CHR nezhoduje s aktuálnym identifikátorom verejného kľúča, vrátený stav spracovania je '**6A88**'.

— Ak sa zvolený súkromný kľúč považuje za poškodený, vrátený stav spracovania je '**6400**' alebo '**6581**'.

TCS_95 Ak je príkaz INTERNAL AUTHENTICATE úspešný, aktuálny kľúč relácie (ak existuje) sa vymaže a nie je naďalej dostupný. Aby bol k dispozícii nový kľúč relácie, musí sa úspešne vykonať príkaz EXTERNAL AUTHENTICATE pre mechanizmus autentifikácie generácie 1.

3.5.9 *EXTERNAL AUTHENTICATE*

Tento príkaz zodpovedá norme ISO/IEC 7816-4.

Príkazom EXTERNAL AUTHENTICATE môže karta autentifikovať IFD. Proces autentifikácie je opísaný v dodatku 11 pre tachograf G1 a G2 (autentifikácia VU).

TCS_96 Príkazový variant pre mechanizmus vzájomnej autentifikácie v generácii 1 podporuje len aplikácia tachografu generácie 1.

TCS_97 Príkazový variant pre mechanizmus vzájomnej autentifikácie medzi VU a kartou v druhej generácii možno vykonať v MF, DF Tachograph a DF Tachograph_G2, pozri tiež TCS_34.

TCS_98 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Kľúče a algoritmy implicitne známe
P2	1	'00h'	
Lc	1	'XXh'	Lc (dĺžka údajov poslaných na kartu)
#6-#(5+L)	L	'XX..XXh'	Autentifikácia v generácii 1: Kryptogram (pozri dodatok 11 časť A) Autentifikácia v generácii 2: Podpis vygenerovaný IFD (pozri dodatok 11 časť B)

TCS_99 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak CHA aktuálne nastaveného verejného kľúča nie je zreťazením tachografovej aplikácie AID a typu zariadenia VU, vrátený stav spracovania je '**6F00**'.

— Ak bezprostredne pred príkazom nie je príkaz GET CHALLENGE, vrátený stav spracovania je '**6985**'.

Aplikácia tachografu generácie 1 môže vrátiť tieto dodatočné kódy chýb:

— Ak nie je v prostredí zabezpečenia prítomný žiadny verejný kľúč, vráti sa '**6A88**'.

— Ak nie je v prostredí zabezpečenia prítomný žiadny súkromný kľúč, vrátený stav spracovania je '**6A88**'.

— Ak je overenie kryptogramu chybné, vrátený stav spracovania je '**6688**'.

— Ak sa zvolený súkromný kľúč považuje za poškodený, vrátený stav spracovania je '**6400**' alebo '**6581**'.

Príkazový variant pre autentifikáciu v generácii 2 môže navyše vrátiť tento kód chyby:

— Ak zlyhalo overenie podpisu, karta vráti '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Tento príkaz sa používa v generácii 2 v rámci protokolu autentifikácie čipu podľa dodatku 11 časti B a zodpovedá norme ISO/IEC 7816-4.

TCS_100 Príkaz možno vykonať v MF, DF Tachograph a DF Tachograph_G2, pozri tiež TCS_34.

TCS_101 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Kľúče a protokol implicitne známe
P2	1	'00h'	
Lc	1	'NNh'	Lc: dĺžka nasledujúceho dátového poľa
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	Hodnota efemérneho (dočasného) verejného kľúča kódovaná v DER-TLV (pozri dodatok 11) VU posiela dátové objekty v tomto poradí.

TCS_102 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	Údaje dynamickej autentifikácie kódované v DER-TLV: jednorazová hodnota „nonce“ a autentifikačný znak (pozri dodatok 11)
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Karta vráti '**6A80**', čím upozorní na nesprávne parametre v dátovom poli.

— Karta vráti '**6982**', ak nebol príkaz External Authenticate vykonaný úspešne

Objekt odpovede Údaje dynamickej autentifikácie '7Ch'

— Musí byť prítomný, ak je operácia úspešná, t. j. stavové slová sú '**9000**',

— musí absentovať, ak došlo k chybe pri vykonaní alebo kontrole, t. j. stavové slová sú v rozmedzí '**6400**' – '**6FFF**' a

— môže absentovať v prípade výstrahy, t. j. stavové slová sú v rozsahu '**6200**' – '**63FF**'.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Tento príkaz sa používa na nastavenie verejného kľúča na účely autentifikácie.

3.5.11.1 Pár príkaz – odpoveď v generácii 1

Tento príkaz zodpovedá norme ISO/IEC 7816-4. Použitie tohto príkazu je v porovnaní s príslušnou normou obmedzené.

TCS_103 Príkaz podporuje len aplikácia tachografu generácie 1.

TCS_104 Referenčný kľúč, na ktorý sa odkazuje v dátovom poli MSE, zostáva aktuálnym verejným kľúčom až do nasledovného správneho príkazu MSE, kým nie je zvolený DF alebo kým sa neresetuje karta.

TCS_105 Ak referenčný kľúč nie je (už) na karte k dispozícii, prostredie zabezpečenia zostáva nezmenené.

TCS_106 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: referenčný kľúč platný pre všetky kryptografické operácie
P2	1	'B6h'	P2 (referenčné údaje o digitálnom podpise)
Lc	1	'0Ah'	Lc: dĺžka nasledujúceho dátového poľa
#6	1	'83h'	Tag referencie na verejný kľúč v asymetrických prípadoch
#7	1	'08h'	Dĺžka referencie na kľúč (identifikátora kľúča)
#8-#15	8	'XX..XXh'	Identifikátor kľúča v zmysle dodatku 11

TCS_107 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak nie na karte prítomný referenčný kľúč, vrátený stav spracovania je '**6A88**'.

— Ak vo formáte zabezpečeného spracovania chýbajú určité očakávané dátové objekty, vrátený stav spracovania je '**6987**'. Môže sa to stať, ak chýba tag '83h'.

— Ak sú niektoré dátové objekty nesprávne, vrátený stav spracovania je '**6988**'. Môže sa to stať, ak dĺžka identifikátora kľúča nie je '08h'.

— Ak sa zvolený kľúč považuje za poškodený, vrátený stav spracovania je '**6400**' alebo '**6581**'.

3.5.11.2 Páry príkaz – odpoveď v generácii 2

Na autentifikáciu generácie 2 tachografová karta podporuje tieto MSE: Stanovené verzie príkazov, ktoré sú v súlade s normou ISO/IEC 7816-4. Tieto verzie príkazov nie sú podporované pre autentifikáciu v generácii 1.

3.5.11.2.1 MSE:SET AT pre autentifikáciu čipu

Nasledujúci príkaz MSE:SET AT sa používa na voľbu parametrov autentifikácie čipu, ktorú vykonáva následný príkaz General Authenticate.

TCS_108 Príkaz možno vykonať v MF, DF Tachograph a DF Tachograph_G2, pozri tiež TCS_34.

TCS_109 **Príkazová správa MSE:SET AT pre autentifikáciu čipu**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'22h'	

Bajt	Dĺžka	Hodnota	Opis
P1	1	'41h'	Stanovené pre internú autentifikáciu
P2	1	'A4h'	Autentifikácia
Lc	1	'NNh'	Lc: dĺžka nasledujúceho dátového poľa
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Referencia kryptografického mechanizmu kódovaného v DER-TLV: Objektový identifikátor autentifikácie čipu (iba hodnota, tag '06h' sa vynecháva). Hodnoty objektových identifikátorov sú uvedené v dodatku 1; použije sa bajtová notácia. Usmernenie k voľbe jedného z týchto objektových identifikátorov je uvedené v dodatku 11.

3.5.11.2.2 MSE:SET AT pre autentifikáciu VU

Nasledujúci príkaz MSE:SET AT sa používa na voľbu parametrov a kľúčov autentifikácie VU, ktorú vykonáva následný príkaz External Authenticate.

TCS_110 Príkaz možno vykonať v MF, DF Tachograph a DF Tachograph_G2, pozri tiež TCS_34.

TCS_111 **Príkazová správa MSE:SET AT pre autentifikáciu VU**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Stanovené pre externú autentifikáciu
P2	1	'A4h'	Autentifikácia
Lc	1	'NNh'	Lc: dĺžka nasledujúceho dátového poľa
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Referencia kryptografického mechanizmu kódovaného v DER-TLV: Objektový identifikátor autentifikácie VU (iba hodnota, tag '06h' sa vynecháva). Hodnoty objektových identifikátorov sú uvedené v dodatku 1; použije sa bajtová notácia. Usmernenie k voľbe jedného z týchto objektových identifikátorov je uvedené v dodatku 11.
		'83h' + '08h' + 'XX..XXh'	Referencia verejného kľúča VU kódovaná v DER-TLV podľa referencie držiteľa certifikátu uvedeného v jeho certifikáte.
		'91h' + L_{91} + 'XX..XXh'	Komprimované vyjadrenie efemérneho verejného kľúča VU kódovaného v DER-TLV, ktorý sa použije pri autentifikácii čipu (pozri dodatok 11)

3.5.11.2.3 MSE:SET DST

Nasledujúci príkaz MSE:SET DST sa použije na nastavenie verejného kľúča buď

— na overenie podpisu, ktorý sa uvádza v následnom príkaze PSO: Verify Digital Signature, alebo

— na overenie podpisu na certifikáte, ktorý sa uvádza v následnom príkaze PSO: Verify Ceretificate

TCS_112 Príkaz možno vykonať v MF, DF Tachograph a DF Tachograph_G2, pozri tiež TCS_33.

TCS_113 **Príkazová správa MSE:SET DST**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Stanovené pre overovanie
P2	1	'B6h'	Digitálny podpis
Lc	1	'NNh'	Lc: dĺžka nasledujúceho dátového poľa
#6-#(5+L)	L	'83h' + '08h' + 'XX…XXh'	Referencia verejného kľúča kódovaná v DER-TLV – t. j. referencia držiteľa certifikátu na certifikáte verejného kľúča (pozri dodatok 11)

Pre všetky príkazové verzie určuje štruktúru odpovedacej správy a stavové slová:

TCS_114 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'. Protokol bol zvolený a inicializovaný.

— '**6A80**' znamená nesprávne parametre v dátovom poli príkazu.

— '**6A88**' znamená, že údaje, na ktoré sa odkazuje (napríklad referenčný kľúč) nie sú k dispozícii.

3.5.12 *PSO: HASH*

Tento príkaz sa používa na prenos výsledkov hash výpočtu niektorých údajov na kartu. Tento príkaz sa používa na overenie digitálnych podpisov. Hash hodnota sa dočasne uloží pre následný príkaz PSO: Verify Digital Signature.

Tento príkaz zodpovedá norme ISO/IEC 7816-8. Použitie tohto príkazu je v porovnaní s príslušnou normou obmedzené.

Podpora tohto príkazu v DF Tachograph a DF Tachograph_G2 sa vyžaduje iba na kontrolnej karte.

Ostatné typy tachografových kariet tento príkaz môžu, ale nemusia implementovať. Príkaz môže, ale nemusí byť dostupný v MF.

Aplikácia kontrolnej karty generácie 1 podporuje iba SHA-1.

TCS_115 Dočasne uložená hash hodnota sa vymaže, ak sa príkazom PSO: HASH vypočíta nová hash hodnota, ak je zvolený DF a ak sa tachografová karta resetuje.

TCS_116 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation (vykonanie operácie zabezpečenia)
P1	1	'90h'	Vrátený hash kód
P2	1	'A0h'	Tag: dátové pole obsahuje DO relevantné pre hašovanie
Lc	1	'XXh'	Dĺžka Lc následného dátového poľa
#6	1	'90h'	Tag hash kódu
#7	1	'XXh'	Dĺžka L hash kódu: '14h' v aplikácii generácie 1 (pozri dodatok 11 časť A) '20h', '30h' alebo '40h' v aplikácii generácie 2 (pozri dodatok 11 časť B)
#8-#(7+L)	L	'XX..XXh'	Hash kód

TCS_117 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak niektoré očakávané dátové objekty (špecifikované vyššie) chýbajú, vrátený stav spracovania je '**6987**'. Môže sa to stať, ak chýba jeden z tagov '90h'.

— Ak sú niektoré dátové objekty nesprávne, vrátený stav spracovania je '**6988**'. K tejto chybe dochádza, keď je požadovaný tag prítomný, ale s dĺžkou inou než '14h' pre SHA-1, '20h' pre SHA-256, '30h' pre SHA-384, '40h' pre SHA-512 (aplikácia generácie 2).

3.5.13 *PERFORM HASH of FILE*

Tento príkaz nezodpovedá norme ISO/IEC 7816-8. CLA bajt tohto príkazu teda udáva, že ide o chránené použitie PERFORM SECURITY OPERATION/HASH.

Podpora tohto príkazu v DF Tachograph a DF Tachograph_G2 sa vyžaduje iba na karte vodiča a dielenskej karte.

Ostatné typy tachografových kariet tento príkaz môžu, ale nemusia implementovať. Ak tento príkaz implementuje podniková alebo kontrolná karta, príkaz sa vykoná podľa tejto kapitoly.

Príkaz môže, ale nemusí byť dostupný v MF. Ak áno, príkaz sa vykoná podľa tejto kapitoly, t. j. nesmie umožniť výpočet hash hodnoty, ale sa preruší vhodným kódom chyby.

TCS_118 Príkaz PERFORM HASH of FILE sa používa na hašovanie dátovej oblasti aktuálne zvoleného transparentného EF.

TCS_119 Tachografová karta musí tento príkaz podporovať iba pre EF uvedené v kapitole 4 v rámci DF_Tachograph a DF_Tachograph_G2 s nasledujúcou výnimkou. Tachografová karta nesmie príkaz podporovať pre EF Sensor_Installation_Data v rámci DF Tachograph_G2.

TCS_120 Výsledok operácie hash sa dočasne uloží na karte. Následne sa môže použiť na získanie digitálneho podpisu súboru s použitím príkazu PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Dočasne uložená hodnota hash of file sa vymaže, ak sa príkazom PSO: Hash of File vypočíta nová hodnota hash of file, ak je zvolený DF a ak sa tachografová karta resetuje.

TCS_122 Aplikácia tachografu generácie 1 musí podporovať SHA-1.

TCS_123 Aplikácia tachografu generácie 2 musí podporovať SHA-1 a SHA-2 (256, 384 a 512 bitov).

TCS_124 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'80h'	CLA
INS	1	'2Ah'	Perform Security Operation (vykonanie operácie zabezpečenia)
P1	1	'90h'	Tag: Hash
P2	1	'XXh'	P2: Označuje algoritmus, ktorý sa má použiť na hašovanie údajov aktuálne zvoleného transparentného súboru: '00h' pre SHA-1 '01h' pre SHA-256 '02h' pre SHA-384 '03h' pre SHA-512

TCS_125 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak aktuálny EF nepovoľuje tento príkaz (EF Sensor_Installation_Data v DF Tachograph_G2), vrátený stav spracovania je '**6985**'.

— Ak sa zvolený EF považuje za poškodený (chyby atribútov súboru alebo integrity uložených údajov), vrátený stav spracovania je '**6400**' alebo '**6581**'.

— Ak zvolený súbor nie je transparentným súborom alebo ak neexistuje aktuálny EF, vrátený stav spracovania je '**6986**'.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Príkaz sa používa na výpočet digitálneho podpisu predtým vypočítaného hash kódu (pozri PERFORM HASH of FILE, §3.5.13).

Podpora tohto príkazu v DF Tachograph a DF Tachograph_G2 sa vyžaduje iba na karte vodiča a dielenskej karte.

Ostatné typy tachografových kariet tento príkaz môžu, ale nemusia implementovať, no nebudú mať podpisový kľúč. Tieto karty preto nemôžu príkaz úspešne vykonať, ale sa preruší vhodným kódom chyby.

Príkaz môže, ale nemusí byť dostupný v MF. Ak áno, príkaz sa preruší vhodným kódom chyby.

Tento príkaz zodpovedá norme ISO/IEC 7816-8. Použitie tohto príkazu je v porovnaní s príslušnou normou obmedzené.

TCS_126 Príkaz nevypočíta digitálny podpis hash kódu predtým vypočítaného príkazom PSO: HASH.

TCS_127 Na výpočet digitálneho podpisu sa použije súkromný kód karty a karta ho implicitne pozná.

TCS_128 Aplikácia tachografu generácie 1 vykoná digitálny podpis s použitím vyplňovacej metódy zodpovedajúcej PKCS1 (podrobnosti v dodatku 11).

TCS_129 Aplikácia tachografu generácie 2 vypočíta digitálny podpis na báze eliptickej krivky (podrobnosti v dodatku 11).

TCS_130 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation (vykonanie operácie zabezpečenia)
P1	1	'9Eh'	Digitálny podpis, ktorý sa má vrátiť
P2	1	'9Ah'	Tag: dátové pole obsahuje údaje na podpísanie Keďže nie je zahrnuté žiadne dátové pole, údaje už majú byť prítomné na karte (hash of file)
Le	1	'NNh'	Dĺžka očakávaného podpisu

TCS_131 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
#1-#L	L	'XX..XXh'	Podpis predtým vypočítaného hash
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak sa implicitne zvolený súkromný kľúč považuje za poškodený, vrátený stav spracovania je '**6400**' alebo '**6581**'.

— Ak hash vypočítaný v predošlom príkaze Perform Hash of File nie je k dispozícii, vrátený stav spracovania je '**6985**'.

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Tento príkaz sa používa na overenie digitálneho podpisu ako vstupu, ktorého hash karta implicitne pozná. Karta implicitne pozná algoritmus podpisu.

Tento príkaz zodpovedá norme ISO/IEC 7816-8. Použitie tohto príkazu je v porovnaní s príslušnou normou obmedzené.

Podpora tohto príkazu v DF Tachograph a DF Tachograph_G2 sa vyžaduje iba na kontrolnej karte.

Ostatné typy tachografových kariet tento príkaz môžu, ale nemusia implementovať. Príkaz môže, ale nemusí byť dostupný v MF.

TCS_132 Príkaz VERIFY DIGITAL SIGNATURE vždy používa verejný kľúč zvolený predchádzajúcim príkazom Manage Security Environment MSE: Set DST a predchádzajúci hash kód zadaný príkazom PSO: HASH.

TCS_133 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation (vykonanie operácie zabezpečenia)
P1	1	'00h'	
P2	1	'A8h'	Tag: dátové pole obsahuje DO relevantné pre overenie
Lc	1	'83h'	Dĺžka Lc následného dátového poľa
6	1	'9Eh'	Tag pre digitálny podpis
#7-#8	2	'81 XXh'	Dĺžka digitálneho podpisu: 128 bajtov kódovaných v súlade s dodatkom 11 časťou A pre aplikáciu tachografu generácie 1 v závislosti od zvolenej krivky pre aplikáciu tachografu generácie 2 (pozri dodatok 11 časť B)
#9-#(8+L)	L	'XX..XXh'	Obsah digitálneho podpisu

TCS_134 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— Ak zlyhá overenie podpisu, vrátený stav spracovania je '**6688**'. Proces overovania je opísaný v dodatku 11.

— Ak nie je zvolený žiadny verejný kľúč, vrátený stav spracovania je '**6A88**'.

— Ak niektoré očakávané dátové objekty (špecifikované vyššie) chýbajú, vrátený stav spracovania je '**6987**'. Môže sa to stať, ak chýba jeden z požadovaných tagov.

— Ak nie je k dispozícii žiadny hash kód na spracovanie príkazu (ako výsledok predchádzajúceho príkazu PSO: Hash), vrátený stav spracovania je '**6985**'.

— Ak sú niektoré dátové objekty nesprávne, vrátený stav spracovania je '**6988**'. Môže sa to stať, ak má niektorý z požadovaných dátových objektov nesprávnu dĺžku.

— Ak sa zvolený verejný kľúč považuje za poškodený, vrátený stav spracovania je '**6400**' alebo '**6581**'.

3.5.16 *PROCESS DSRC MESSAGE*

Tento príkaz sa používa na overenie integrity a autentickosti správy DSRC a na dešifrovanie údajov, ktoré VU zasiela kontrolnému orgánu alebo dielni spojením DSRC. Karta odvodzuje šifrovací kľúč a kľúč MAC použitý na zabezpečenie správy DSRC v súlade s dodatkom 11 časťou B kapitolou 13.

Podpora tohto príkazu v DF Tachograph_G2 sa vyžaduje iba na kontrolnej karte a dielenskej karte.

Ostatné typy tachografových kariet tento príkaz môžu, ale nemusia implementovať, no nebudú mať univerzálny kľúč DSRC (master key). Tieto karty preto nemôžu príkaz úspešne vykonať, ale sa preruší vhodným kódom chyby.

Príkaz môže, ale nemusí byť dostupný v MF a/alebo v DF Tachograph. Ak áno, príkaz sa preruší vhodným kódom chyby.

TCS_135 Univerzálny kľúč DSRC je dostupný iba v DF Tachograph_G2, t. j. kontrolná a dielenská karta podporia úspešné vykonanie príkazu iba v DF Tachograph_G2.

TCS_136 Príkaz iba dešifruje údaje DSRC a overí kryptografický kontrolný súčet, ale neinterpretuje vstupné údaje.

TCS_137 Poradie dátových objektov v dátovom poli príkazu je pevne stanovené touto špecifikáciou.

TCS_138 **Príkazová správa**

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'80h'	Chránené CLA
INS	1	'2Ah'	Perform Security Operation (vykonanie operácie zabezpečenia)
P1	1	'80h'	Údaje odpovede: nešifrovaná hodnota
P2	1	'B0h'	Údaje príkazu: nešifrovaná hodnota kódovaná v BER-TLV vrátane dátových objektov SM
Lc	1	'NNh'	Dĺžka Lc následného dátového poľa
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	Bajt s indikátorom obsahu výplne kódovaný v DER-TLV nasledovaný šifrovanými obsahovými údajmi tachografu. Pre bajt s indikátorom obsahu výplne sa použije hodnota '00h' („bez bližšieho určenia" podľa tabuľky 52 v ISO/IEC 7816-4:2013). Šifrovací mechanizmus je opísaný v dodatku 11 časti B kapitole 13. Pre dĺžku L_{87} sú povolenými hodnotami násobky blokovej dĺžky AES plus 1 pre bajt s indikátorom obsahu výplne, t. j. od 17 po 193 bajtov vrátane. *Poznámka:* dátový objekt SM s tagom '87h' je uvedený v tabuľke 49 normy ISO/IEC 7816-4:2013.
		'81h' + '10h'	Kontrolný referenčný vzor pre dôvernosť kódovaný v DER-TLV, v ktorom je zahrnuté zreťazenie týchto dátových prvkov (pozri dodatok 1 DSRCSecurityData a dodatok 11 časť B kapitolu 13): — 4-bajtová časová pečiatka — 3-bajtové počítadlo — 8-bajtové sériové číslo VU — 1-bajtová verzia univerzálneho kľúča DSRC *Poznámka:* dátový objekt SM s tagom '81h' je uvedený v tabuľke 49 normy ISO/IEC 7816-4:2013.
		'8Eh' + L_{8E} + 'XX..XXh'	Autentifikačný kód správy DSRC (MAC) kódovaný v DER-TLV Algoritmus a výpočet MAC je opísaný v dodatku 11 časti B kapitole 13. *Poznámka:* dátový objekt SM s tagom '8Eh' je uvedený v tabuľke 49 normy ISO/IEC 7816-4:2013.

TCS_139 **Odpovedacia správa**

Bajt	Dĺžka	Hodnota	Opis
#1-#L	L	'XX..XXh'	Absentuje (v prípade chyby) alebo dešifrované údaje (s odstránenou výplňou)
SW	2	'XXXXh'	Stavové slová (SW1, SW2)

— Ak je príkaz úspešný, karta vráti '**9000**'.

— '**6A80**' označuje nesprávne parametre v dátovom poli príkazu (použije sa aj v prípade, ak dátové objekty nie sú zaslané v určenom poradí).

— '**6A88**' znamená, že nie sú k dispozícii údaje, na ktoré sa odkazuje, t. j. že nie je k dispozícii referenčný univerzálny kľúč DSRC.

— '**6900**' znamená, že zlyhalo overovanie kryptografického kontrolného súčtu alebo dešifrovanie údajov.

4. ŠTRUKTÚRA TACHOGRAFOVÝCH KARIET

Tento odsek špecifikuje štruktúry súborov tachografových kariet na uloženie dostupných údajov.

Nešpecifikuje vnútorné štruktúry závislé od výrobcu karty ako napr. záhlavia súborov, ani ukladanie a spracovávanie dátových prvkov potrebných len na interné použitie ako napr. `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` alebo `WorkshopCardPin`.

TCS_140 Tachografová karta generácie 2 musí zahŕňať MF (hlavný súbor) a tachografovú aplikáciu generácie 1 a generácie 2 rovnakého typu (napr. aplikácie karty vodiča).

TCS_141 Tachografová karta musí podporovať aspoň minimálny počet záznamov určený pre príslušné aplikácie a nesmie podporovať viac než maximálny počet záznamov určený pre príslušné aplikácie.

Maximálne a minimálne počty záznamov pre rôzne aplikácie sú určené v tejto kapitole.

Podmienky zabezpečenia použité v pravidlách prístupu na účely tejto kapitoly sú uvedené v kapitole 3.3. Prístupový režim čítania („read“) vo všeobecnosti označuje príkaz READ BINARY s párnym a (ak sa podporuje) nepárnym bajtom INS, s výnimkou EF Sensor_Installation_Data na dielenskej karte, pozri TCS_156 a TCS_160. Prístupový režim aktualizácie („update“) označuje príkaz Update Binary s párnym a (ak sa podporuje) nepárnym bajtom INS a prístupový režim voľby („select“) príkaz SELECT.

4.1. Hlavný súbor (MF)

TCS_142 Po personalizácii musí mať hlavný súbor MF nasledovnú stálu štruktúru súborov a pravidlá prístupu k nim:

Poznámka: Krátky identifikátor EF SFID je daný ako číslo v desiatkovej sústave – napr. hodnota 30 zodpovedá hodnote 11110 v binárnom vyjadrení.

			Pravidlá prístupu	
Súbor	**ID súboru**	**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 (conditional)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (conditional)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

V tejto tabuľke sa používa nasledovná skratka podmienky zabezpečenia:

SC1 ALW alebo SM-MAC-G2

TCS_143 Štruktúry všetkých EF musia byť transparentné.

TCS_144 Hlavný súbor MF má túto dátovú štruktúru:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
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*	
See TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
See TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
See TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Elementárny súbor EF DIR obsahuje tieto aplikačné dátové objekty: ‘61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54’

TCS_146 Elementárny súbor EF ATR/INFO musí byť prítomný, ak tachografová karta v ATR uvádza, že podporuje polia s rozšírenou dĺžkou. V tomto prípade EF ATR/INFO obsahuje dátový objekt s informáciou o rozšírenej dĺžke (DO‘7F66’) v zmysle ISO/IEC 7816-4:2013 bodu 12.7.1.

TCS_147 Elementárny súbor EF Extended_Length musí byť prítomný, ak tachografová karta v ATR uvádza, že podporuje polia s rozšírenou dĺžkou. V tomto prípade musí EF obsahovať nasledovný dátový objekt: ‘02 01 xx’, kde hodnota ‘xx’ určuje, či sa polia s rozšírenou dĺžkou podporujú pre protokol T = 1 a/alebo T = 0.

Hodnota ‘01’ označuje podporu polí s rozšírenou dĺžkou pre protokol T = 1.

Hodnota ‘10’ označuje podporu polí s rozšírenou dĺžkou pre protokol T = 0.

Hodnota ‘11’ označuje podporu polí s rozšírenou dĺžkou pre protokol T = 1 aj T = 0.

4.2. Aplikácie karty vodiča

4.2.1 *Aplikácia karty vodiča generácie 1*

TCS_148 Po personalizácii musí mať aplikácia karty vodiča generácie 1 nasledovnú stálu štruktúru súborov a pravidlá prístupu k nim:

		Pravidlá prístupu		
Súbor	**ID súboru**	**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

V tejto tabuľke sa používajú nasledovné skratky podmienok zabezpečenia:

SC1 ALW alebo SM-MAC-G2

SC2 ALW alebo SM-MAC-G1 alebo SM-MAC-G2

SC3 SM-MAC-G1 alebo SM-MAC-G2

TCS_149 Štruktúry všetkých EF musia byť transparentné.

TCS_150 Aplikácia karty vodiča generácie 1 má túto dátovú štruktúru:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
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 Nasledovné hodnoty použité na určenie veľkostí v predošlej tabuľke sú minimálne a maximálne hodnoty počtu záznamov, ktoré musí dátová štruktúra karty vodiča uplatňovať v aplikácii generácie 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 bajtov (28 dní * 93 zmien činnosti)	13 776 bajtov (28 dní * 240 zmien činnosti)

4.2.2 *Aplikácia karty vodiča generácie 2*

TCS_152 Po personalizácii musí mať aplikácia karty vodiča generácie 2 nasledovnú stálu štruktúru súborov a pravidlá prístupu k nim:

Poznámka: Krátky identifikátor EF SFID je daný ako číslo v desiatkovej sústave – napr. hodnota 30 zodpovedá hodnote 11110 v binárnom vyjadrení.

			Pravidlá prístupu	
Súbor	**ID súboru**	**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

V tejto tabuľke sa používa nasledovná skratka podmienky zabezpečenia:

SC1 ALW alebo SM-MAC-G2

TCS_153 Štruktúry všetkých EF musia byť transparentné.

TCS_154 Aplikácia karty vodiča generácie 2 má túto dátovú štruktúru:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
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 Nasledovné hodnoty použité na určenie veľkostí v predošlej tabuľke sú minimálne a maximálne hodnoty počtu záznamov, ktoré musí dátová štruktúra karty vodiča uplatňovať v aplikácii generácie 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 bajtov (28 dní * 93 zmien činnosti)	13 776 bajtov (28 dní * 240 zmien činnosti)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. Aplikácie dielenskej karty

4.3.1 *Aplikácia dielenskej karty generácie 1*

TCS_156 Po personalizácii musí mať aplikácia dielenskej karty generácie 1 nasledovnú stálu štruktúru súborov a pravidlá prístupu k nim:

		Pravidlá prístupu		
Súbor	**ID súboru**	**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

V tejto tabuľke sa používajú nasledovné skratky podmienok zabezpečenia:

SC1 ALW alebo SM-MAC-G2

SC2 ALW alebo SM-MAC-G1 alebo SM-MAC-G2

SC3 SM-MAC-G1 alebo SM-MAC-G2

SC4 Pre príkaz READ BINARY s párnym bajtom INS:

(PLAIN-C a SM-R-ENC-G1) alebo (SM-C-MAC-G1 a SM-R-ENC-MAC-G1) alebo

(SM-C-MAC-G2 a SM-R-ENC-MAC-G2)

Pre príkaz READ BINARY s nepárnym bajtom INS (ak sa podporuje): NEV

TCS_157 Štruktúry všetkých EF musia byť transparentné.

TCS_158 Aplikácia dielenskej karty generácie 1 má túto dátovú štruktúru:

Súbor/dátový prvok	Počet záznamov	Veľkosť (bajty) Min	Max	Predvolené hodnoty
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 Nasledovné hodnoty použité na určenie veľkostí v predošlej tabuľke sú minimálne a maximálne hodnoty počtu záznamov, ktoré musí dátová štruktúra dielenskej karty uplatňovať v aplikácii generácie 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 bajtov (1 deň * 93 zmien činnosti)	492 bajtov (1 deň * 240 zmien činnosti)

4.3.2 *Aplikácia dielenskej karty generácie 2*

TCS_160 Po personalizácii musí mať aplikácia dielenskej karty generácie 2 nasledovnú stálu štruktúru súborov a pravidlá prístupu k nim:

Poznámka: Krátky identifikátor EF SFID je daný ako číslo v desiatkovej sústave – napr. hodnota 30 zodpovedá hodnote 11110 v binárnom vyjadrení.

			Pravidlá prístupu		
Súbor	**ID súboru**	**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

V tejto tabuľke sa používajú nasledovné skratky podmienok zabezpečenia:

SC1 ALW alebo SM-MAC-G2

SC5 Pre príkaz Read Binary s párnym bajtom INS: SM-C-MAC-G2 a SM-R-ENC-MAC-G2

Pre príkaz Read Binary s nepárnym bajtom INS (ak sa podporuje): NEV

TCS_161 Štruktúry všetkých EF musia byť transparentné.

TCS_162 Aplikácia dielenskej karty generácie 2 má túto dátovú štruktúru:

Súbor/dátový prvok	Počet záznamov	Veľkosť (bajty) Min	Max	Predvolené hodnoty
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 Nasledovné hodnoty použité na určenie veľkostí v predošlej tabuľke sú minimálne a maximálne hodnoty počtu záznamov, ktoré musí dátová štruktúra dielenskej karty uplatňovať v aplikácii generácie 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 bajtov (1 deň * 93 zmien činnosti)	492 bajtov (1 deň * 240 zmien činnosti)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Aplikácie kontrolnej karty

4.4.1 *Aplikácia kontrolnej karty generácie 1*

TCS_164 Po personalizácii musí mať aplikácia kontrolnej karty generácie 1 nasledovnú stálu štruktúru súborov a pravidlá prístupu k nim:

		Pravidlá prístupu		
Súbor	**ID súboru**	**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

V tejto tabuľke sa používajú nasledovné skratky podmienok zabezpečenia:

SC1 ALW alebo SM-MAC-G2

SC2 ALW alebo SM-MAC-G1 alebo SM-MAC-G2

SC3 SM-MAC-G1 alebo SM-MAC-G2

SC6 EXT-AUT-G1 alebo SM-MAC-G1 alebo SM-MAC-G2

TCS_165 Štruktúry všetkých EF musia byť transparentné.

TCS_166 Aplikácia kontrolnej karty generácie 1 má túto dátovú štruktúru:

Súbor/dátový prvok	Počet záznamov	Veľkosť (bajty) 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 Nasledovné hodnoty použité na určenie veľkostí v predošlej tabuľke sú minimálne a maximálne hodnoty počtu záznamov, ktoré musí dátová štruktúra kontrolnej karty uplatňovať v aplikácii generácie 1:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Aplikácia kontrolnej karty generácie 2*

TCS_168 Po personalizácii musí mať aplikácia kontrolnej karty generácie 2 nasledovnú stálu štruktúru súborov a pravidlá prístupu k nim:

Poznámka: Krátky identifikátor EF SFID je daný ako číslo v desiatkovej sústave – napr. hodnota 30 zodpovedá hodnote 11110 v binárnom vyjadrení.

			Pravidlá prístupu	
Súbor	**ID súboru**	**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

V tejto tabuľke sa používa nasledovná skratka podmienky zabezpečenia:

SC1 ALW alebo SM-MAC-G2

TCS_169 Štruktúry všetkých EF musia byť transparentné.

TCS_170 Aplikácia kontrolnej karty generácie 2 má túto dátovú štruktúru:

Súbor/dátový prvok	Počet záznamov	Veľkosť (bajty) 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 Nasledovné hodnoty použité na určenie veľkostí v predošlej tabuľke sú minimálne a maximálne hodnoty počtu záznamov, ktoré musí dátová štruktúra kontrolnej karty uplatňovať v aplikácii generácie 2:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.5. Aplikácie podnikovej karty

4.5.1 *Aplikácia podnikovej karty generácie 1*

TCS_172 Po personalizácii musí mať aplikácia podnikovej karty generácie 1 nasledovnú stálu štruktúru súborov a pravidlá prístupu k nim:

		Pravidlá prístupu		
Súbor	**ID súboru**	**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

V tejto tabuľke sa používajú nasledovné skratky podmienok zabezpečenia:

SC1 ALW alebo SM-MAC-G2

SC2 ALW alebo SM-MAC-G1 alebo SM-MAC-G2

SC3 SM-MAC-G1 alebo SM-MAC-G2

SC6 EXT-AUT-G1 alebo SM-MAC-G1 alebo SM-MAC-G2

TCS_173 Štruktúry všetkých EF musia byť transparentné.

TCS_174 Aplikácia podnikovej karty generácie 1 má túto dátovú štruktúru:

Súbor/dátový prvok	**Počet záznamov**	**Veľkosť (bajty) Min**	**Max**	**Predvolené hodnoty**
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 Nasledovné hodnoty použité na určenie veľkostí v predošlej tabuľke sú minimálne a maximálne hodnoty počtu záznamov, ktoré musí dátová štruktúra podnikovej karty uplatňovať v aplikácii generácie 1:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Aplikácia podnikovej karty generácie 2*

TCS_176 Po personalizácii musí mať aplikácia podnikovej karty generácie 2 nasledovnú stálu štruktúru súborov a pravidlá prístupu k nim:

Poznámka: Krátky identifikátor EF SFID je daný ako číslo v desiatkovej sústave – napr. hodnota 30 zodpovedá hodnote 11110 v binárnom vyjadrení.

			Pravidlá prístupu	
Súbor	**ID súboru**	**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

V tejto tabuľke sa používa nasledovná skratka podmienky zabezpečenia:

SC1 ALW alebo SM-MAC-G2

TCS_177 Štruktúry všetkých EF musia byť transparentné.

TCS_178 Aplikácia podnikovej karty generácie 2 má túto dátovú štruktúru:

Súbor/dátový prvok	Počet záznamov	Veľkosť (bajty) Min	Max	Predvolené hodnoty
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 Nasledovné hodnoty použité na určenie veľkostí v predošlej tabuľke sú minimálne a maximálne hodnoty počtu záznamov, ktoré musí dátová štruktúra podnikovej karty uplatňovať v aplikácii generácie 2:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

Dodatok 3

PIKTOGRAMY

PIC_001 Tachograf môže voliteľne používať tieto piktogramy a ich kombinácie (alebo piktogramy a kombinácie dostatočne podobné, aby nemohlo dôjsť k zámene):

1. ZÁKLADNÉ PIKTOGRAMY

	Osoby	**Činnosti**	**Režimy prevádzky**
	Podnik		Podnikový režim
	Kontrolór	Kontrola	Kontrolný režim
	Vodič	Jazda	Prevádzkový režim
	Dielňa/skúšobňa	Inšpekcia/kalibrácia	Kalibračný režim
	Výrobca		

	Činnosti	**Trvanie**
	Pohotovosť	Aktuálny čas pohotovosti
	Jazda	Nepretržitý čas jazdy
	Odpočinok	Aktuálny čas odpočinku
	Iná práca	Aktuálny pracovný čas
	Prestávka	Kumulovaný čas prestávok
?	Neznáme	

	Vybavenie	**Funkcie**
1	Slot vodiča	
2	Slot druhého vodiča	
	Karta	
	Hodiny	
	Displej	Zobrazovanie
	Externá pamäť	Sťahovanie
	Napájanie	
	Tlačiareň/výpis	Tlač
	Snímač	
	Rozmer pneumatík	
	Vozidlo/jednotka vozidla	
	zariadenie GNSS	
	Zariadenie diaľkovej detekcie	
	rozhranie IDS	

	Špecifické podmienky
OUT	Zariadenie sa nevyžaduje
	Prevoz trajektom/vlakom

Rôzne

!	Udalosti	✕	Poruchy
⏵	Začiatok denného pracovného času	⏵|	Koniec denného pracovného času
●	Miesto		
M	Manuálny záznam o činnostiach vodiča		
🔒	Zabezpečenie		
>	Rýchlosť		
◷	Čas		
Σ	Celkom/súhrn		

Kvalifikátory

24h	Za deň
|	Za týždeň
||	Za dva týždne
+	Od alebo do

2. KOMBINÁCIE PIKTOGRAMOV

Rôzne

🗑●	Miesto kontroly		
●⏵	Miesto začiatku denného pracovného času	⏵|●	Miesto konca denného pracovného času
◷+	Čas začiatku	+◷	Čas skončenia
🚗+	Z vozidla		
OUT+	Zariadenie sa nevyžaduje – začiatok	+OUT	Zariadenie sa nevyžaduje – koniec

Karty

⊙🖳	Karta vodiča
🏠🖳	Podniková karta
🗑🖳	Kontrolná karta
T🖳	Dielenská karta
🖳– – –	Žiadna karta

Jazda

⊙⊙	V posádke
⊙ |	Čas jazdy za jeden týždeň
⊙ ||	Čas jazdy za dva týždne

Výpisy

24h 🖳▼	Denný výpis činností vodiča z karty
24h 🚗▼	Denný výpis činností vodiča z VU
! ✕🖳▼	Výpis udalostí a porúch z karty
! ✕🚗▼	Výpis udalostí a porúch z VU
T◷▼	Výpis technických údajov
>>▼	Výpis prekročenia rýchlosti

Udalosti

Vloženie neplatnej karty

Konflikt karty

Prekrývanie časov

Jazda bez príslušnej karty

Vloženie karty za jazdy

Nesprávne uzavretá posledná relácia karty

Prekročenie rýchlosti

Prerušenie napájania

Chyba údajov o pohybe

Nesúlad údajov o pohybe vozidla

Narušenie zabezpečenia

Úprava času (v dielni)

Kontrola prekročenia rýchlosti

Poruchy

Porucha karty (slot vodiča)

Porucha karty (slot druhého vodiča)

Porucha zobrazenia

Porucha sťahovania

Porucha tlače

Porucha snímača

Interná porucha VU

porucha GNSS

Porucha diaľkovej detekcie

Postup manuálnych zápisov

Stále ten istý denný pracovný čas?

Koniec predošlého pracovného času?

Potvrdiť alebo zadať miesto konca pracovného času

Zadať čas začiatku

Zadať miesto začiatku pracovného času.

Poznámka: Ďalšie kombinácie piktogramov, ktorými sa skladajú bloky tlače alebo identifikátory záznamov, sú vymedzené v dodatku 4.

Dodatok 4

VÝPISY

OBSAH

1. VŠEOBECNE 243
2. ŠPECIFIKÁCIE DÁTOVÝCH BLOKOV 243
3. ŠPECIFIKÁCIE VÝPISOV 250
3.1. Denný výpis činností vodiča z karty 250
3.2. Denný výpis činností vodiča z VU 251
3.3. Výpis udalostí a porúch z karty 252
3.4. Výpis udalostí a porúch z VU 252
3.5. Výpis technických údajov 253
3.6. Výpis prekročenia rýchlosti 253
3.7. História vložených kariet 254

1. VŠEOBECNE

Každý výpis pozostáva z reťazcov rôznych dátových blokov, ktoré môžu byť identifikované identifikátorom bloku.

Dátový blok obsahuje jeden alebo viac záznamov, ktoré môžu byť identifikované identifikátorom záznamu.

PRT_001 Keď stojí identifikátor bloku bezprostredne pred identifikátorom záznamu, identifikátor záznamu sa nevytlačí.

PRT_002 Ak sú dátové údaje neznáme alebo sa nesmú vytlačiť z dôvodu prístupových práv, vypíšu sa miesto nich medzery.

PRT_003 Ak je obsah celého riadku neznámy alebo jeho tlač nie je potrebná, celý riadok sa vynechá.

PRT_004 Numerické dátové polia sa vytlačia zarovnané sprava s medzerou pre tisíce a milióny a bez úvodných núl.

PRT_005 Reťazcové dátové polia sa vytlačia zarovnané zľava a podľa potreby sa vyplnia medzerami do dĺžky dátového prvku alebo sa skrátia na dĺžku dátového prvku (mená a adresy).

PRT_006 V prípade zalomenia riadku pri dlhom texte by sa na novom riadku mal ako prvý vytlačiť špeciálny znak (bodka v strede výšky riadku „•“).

2. ŠPECIFIKÁCIE DÁTOVÝCH BLOKOV

V tejto kapitole sa použila táto formátová notácia:

— znaky vytlačené **tučným písmom** znamenajú nešifrovaný text na tlač (tlačia sa normálne znaky),

— normálne znaky znamenajú premenné (piktogramy alebo údaje), ktoré sa majú pri tlači nahradiť ich hodnotami,

— označenia premenných boli doplnené podčiarkovníkmi, aby sa zviditeľnila dĺžka dátového prvku, ktorá je pre premennú k dispozícii,

— dátumy sú vo formáte „dd/mm/rrrr“ (deň, mesiac, rok). Môže sa použiť aj formát „dd.mm.rrrr“,

— pojem „identifikácia karty“ znamená zoskupenie týchto prvkov: typ karty určený kombináciou piktogramov, kód vystavujúceho členského štátu, lomka a číslo karty s indexom náhrady a indexom obnovy, ktoré sú oddelené medzerou:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kombinácia piktogramu karty		Kód vydávajúceho členského štátu				Prvých 14 znakov čísla karty (prípadne vrátane poradového indexu)														Index náhrady		Index obnovy

PRT_007 Výpisy používajú tieto dátové bloky a/alebo záznamy údajov s týmito významami a formátmi:

Číslo bloku alebo záznamu Význam	Data Format
1 ***Dátum a čas tlače dokumentu***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Typ výpisu*** Identifikátor bloku Kombinácia piktogramu výpisu (pozri dodatok 3) nastavenie obmedzovača rýchlosti (len výpis prekročenia rýchlosti)	----------▼---------- Picto xxx **km/h**
3 ***Identifikácia držiteľa karty*** Identifikátor bloku P = piktogram osoby Priezvisko držiteľa karty Prípadne meno(-á) držiteľa karty Identifikácia karty Prípadný dátum skončenia platnosti karty a číslo generácie karty (GEN 1 alebo GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

V prípade neosobnej karty bez priezviska držiteľa sa tu vytlačí názov podniku, dielne alebo kontrolného orgánu.

(*) Číslo generácie karty možno vytlačiť len pri inteligentnom tachografe.

4 ***Identifikácia vozidla*** Identifikátor bloku VIN Členský štát evidencie a VRN	----------🚘---------- 🚘 VIN_____ Nat/VRN_____
5 ***Identifikácia VU*** Identifikátor bloku Meno výrobcu VU Číslo dielu VU Číslo generácie VU (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Číslo generácie karty možno vytlačiť len pri inteligentnom tachografe.

6 ***Posledná kalibrácia tachografu*** Identifikátor bloku Názov dielne Identifikácia dielenskej karty Dátum kalibrácie	----------⍑---------- ⍑ Last_Name_____ Card_Identification_____ ⍑ dd/mm/yyyy

7 ***Posledná kontrola (kontrolórom)***

Identifikátor bloku
Identifikácia kontrolnej karty
Dátum, čas a druh kontroly

```
----------▯----------
Card_Identification_____
▯ dd/mm/yyyy hh:mm ppppp
```

Druh kontroly: Do päť piktogramov. Druh kontroly môže byť (aj kombinácia):
▮: Sťahovanie z karty, ↧: sťahovanie z VU, ⍑: tlač, ☐: zobrazenie, ⍑: kontrola kalibrácie pri cestnej kontrole

8 ***Činnosti vodiča uložené na karte v poradí, v akom sa vykonávajú***

Identifikátor bloku
Dátum dopytu (vypisovaný kalendárny deň) + počítadlo dennej prítomnosti pre kartu

```
----------⊙----------
    dd/mm/yyyy  xxx
```

8a *Podmienka „Záznamové zariadenie sa nevyžaduje" na začiatku tohto dňa* (ponechá sa prázdne, ak nie je otvorená podmienka)

```
----------OUT----------
```

8.1 *Časový úsek, počas ktorého nebola karta vložená*
8.1a Identifikátor záznamu (začiatok časového úseku)
8.1b *Neznámy časový úsek*. Čas začiatku, trvanie
8.1c *Činnosť zadaná manuálne*.
Piktogram činnosti, čas začiatku, trvanie

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Vloženie karty do slotu S*
Identifikátor záznamu; S = piktogram slotu
Členský štát evidencie vozidla a VRN
Stav kilometrov pri vložení karty

```
  ---------S---------
Nat/VRN_____________
  x xxx xxx km
```

8.3 *Činnosť (zatiaľ čo je karta vložená)*
Piktogram činnosti, čas začiatku, trvanie, stav vedenia vozidla (piktogram posádky, ak je stav POSÁDKA, prázdne miesto, ak je stav JEDEN VODIČ).

```
A       hh:mm hhhmm ⊙⊙
```

8.3a *Špecifická podmienka*. Čas zadania, piktogram špecifickej podmienky (alebo kombinácia piktogramov).

```
        hh:mm ---pppp---
```

8.4 *Vytiahnutie karty*
Stav kilometrov a prejdená vzdialenosť od posledného vloženia, pri ktorom je známy stav kilometrov

```
  x xxx xxx km; x xxx km
```

9 ***Činnosti vodiča uložené vo VU podľa slotu v chronologickom poradí***

Identifikátor bloku
Dátum dopytu (vypisovaný kalendárny deň)
Stav kilometrov vozidla pri 00:00 a 24:00

```
----------⊙----------
       dd/mm/rrrr
x xxx xxx - x xxx xxx km
```

10 ***Činnosti v slote S***

Identifikátor bloku

```
----------S----------
```

10a *Podmienka „Záznamové zariadenie sa nevyžaduje" na začiatku tohto dňa* (ponechá sa prázdne, ak nie je otvorená podmienka)

```
----------OUT----------
```

10.1 *Časový úsek, počas ktorého nie je vložená v slote S žiadna karta*
Identifikátor záznamu.
Nie je vložená žiadna karta
Stav kilometrov na začiatku časového úseku

```
  --------------------
⊙▮---
  x xxx xxx km
```

10.2 *Vloženie karty*
Identifikátor záznamu vloženia karty
Priezvisko vodiča

```
  --------------------
⊙ Last_Name_____________
```

	Meno vodiča	First_Name_____
	Identifikácia karty vodiča	Card_Identification_____
	Prípadný dátum skončenia platnosti karty a číslo generácie karty (GEN 1 alebo GEN 2) (*)	dd/mm/yyyy - GEN 2
	Členský štát evidencie vozidla a VRN predchádzajúceho použitého vozidla	+Nat/VRN_____
	Dátum a čas vytiahnutia karty z predchádzajúceho vozidla	dd/mm/yyyy hh:mm
	Prázdny riadok	
	Stav kilometrov pri vložení karty, manuálne zadanie znaku činností vodiča (M ak áno, prázdne ak nie).	x xxx xxx **km** M
	Ak v deň, za ktorý sa pripravuje výpis, nebola karta vodiča vložená, v bloku 10.2 sa použijú údaje o stave kilometrov odčítané pri poslednom dostupnom vložení karty pred daným dňom.	
10.3	*Činnosť*	
	Piktogram činnosti, čas začiatku, trvanie, stav vedenia vozidla (piktogram posádky, ak je stav POSÁDKA, prázdne miesto, ak je stav JEDEN VODIČ).	A hh:mm hh**h**mm
10.3a	*Špecifická podmienka*. Čas zadania, piktogram špecifickej podmienky (alebo kombinácia piktogramov).	hh:mm ---pppp---
10.4	*Vytiahnutie karty alebo koniec časového úseku „Žiadna karta“*	
	Stav kilometrov pri vytiahnutí karty alebo na konci časového úseku „Žiadna karta“ a prejdená vzdialenosť od vloženia, alebo od začiatku časového úseku „Žiadna karta“.	x xxx xxx **km**; x xxx **km**

(*) Číslo generácie karty možno vytlačiť len pri inteligentnom tachografe.

11	***Denný súhrn***	
	Identifikátor bloku	----------Σ----------
11.1	***Súhrn časových úsekov VU bez karty v slote vodiča***	
	Identifikátor bloku	1
11.2	***Súhrn časových úsekov VU bez karty v slote druhého vodiča***	
	Identifikátor bloku	2
11.3	***Denný súhrn VU za každého vodiča***	
	Identifikátor záznamu	----------
	Priezvisko vodiča	Last_Name_____
	Meno(-á) vodiča	First_Name_____
	Identifikácia karty vodiča	Card_Identification_____
11.4	*Zadanie miesta, kde sa začína a/alebo končí denný pracovný čas*	
	pi=piktogram počiatočného / koncového miesta, čas, krajina, región,	pihh:mm Cou Reg
	Počítadlo stavu kilometrov	x xxx xxx **km**
11.5	*Zadanie miesta, kde sa začína a/alebo končí denný pracovný čas*	
	a po 3 hodinách nepretržitej jazdy	hh:mm
	Počítadlo stavu kilometrov	x xxx xxx **km**

11.6	*Činnosti celkom (z karty)*	
	Celkový čas vedenia vozidla, prejdená vzdialenosť	hh**h**mm x xxx **km**
	Celkový čas práce a pohotovosti	hh**h**mm hh**h**mm
	Celkový čas odpočinku a neznámej činnosti	hh**h**mm hh**h**mm
	Celkové trvanie činností posádky	hh**h**mm
11.7	*Činnosti celkom (časové úseky bez karty v slote vodiča)*	
	Celkový čas vedenia vozidla, prejdená vzdialenosť	hh**h**mm x xxx **km**
	Celkový čas práce a pohotovosti	hh**h**mm hh**h**mm
	Celkový čas odpočinku	hh**h**mm

11.8	*Činnosti celkom (časové úseky bez karty v slote druhého vodiča)*	
	Celkový čas práce a pohotovosti	⚒ hh**h**mm ⧈ hh**h**mm
	Celkový čas odpočinku	⊢ hh**h**mm
11.9	*Činnosti celkom (za každého vodiča, oba sloty)*	
	Celkový čas vedenia vozidla, prejdená vzdialenosť	⊙ hh**h**mm x xxx **km**
	Celkový čas práce a pohotovosti	⚒ hh**h**mm ⧈ hh**h**mm
	Celkový čas odpočinku	⊢ hh**h**mm
	Celkové trvanie činností posádky	⊙⊙ hh**h**mm

Keď sa vyžaduje výpis za aktuálny deň, denné súhrnné informácie sa vypočítajú z údajov dostupných v čase výpisu.

12	***Udalosti a/alebo poruchy uložené na karte***	
12.1	Identifikátor bloku posledných 5 „udalostí a porúch“ z karty	----------!×▪----------
12.2	Identifikátor bloku všetky zaznamenané „udalosti“ na karte	----------!▪----------
12.3	Identifikátor bloku všetky zaznamenané „poruchy“ na karte	----------×▪----------
12.4	*Záznam udalosti a/alebo poruchy*	
	Identifikátor záznamu	----------
	Piktogram udalosti/poruchy, účel záznamu, dátum a čas začiatku,	Pic (p) dd/mm/yyyy hh:mm
	Prípadný ďalší kód udalosti/poruchy, trvanie	!xx hh**h**mm
	Členský štát evidencie a VRN vozidla, v ktorom došlo k udalosti alebo poruche	🖷 Nat/VRN_____

13	***Udalosti a/alebo poruchy uložené alebo prebiehajúce vo VU***	
13.1	Identifikátor bloku posledných 5 „udalostí a porúch“ z VU	----------!×🖷----------
13.2	Identifikátor bloku všetky zaznamenané alebo prebiehajúce „udalosti“ vo VU	----------!🖷----------
13.3	Identifikátor bloku všetky zaznamenané alebo prebiehajúce „poruchy“ vo VU	----------×🖷----------
13.4	*Záznam udalosti a/alebo poruchy*	
	Identifikátor záznamu	----------
	Piktogram udalosti/poruchy, účel záznamu, dátum a čas začiatku,	Pic (p) dd/mm/yyyy hh:mm
	Prípadný ďalší kód udalosti/poruchy, počet podobných udalostí v ten deň, trvanie	!xx (xxx) hh**h**mm
	Identifikácia kariet vložených na začiatku alebo na konci udalosti alebo poruchy (max. 4 riadky bez opakovania tých istých čísel karty)	Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____
	Prípad, keď nebola vložená žiadna karta	▪---
	Údaje špecifické podľa výrobcu	< Literal><ErrorCode>

Účel záznamu (p) je číselný kód vysvetľujúci, prečo bola udalosť alebo porucha zaznamenaná, kódovaný v súlade s dátovým prvkom `EventFaultRecordPurpose`.

`Literal` je literál špecifický podľa výrobcu tachografu s max. 12 znakmi.

`ErrorCode` je kód chyby špecifický podľa výrobcu tachografu s max. 12 znakmi.

14 ***Identifikácia VU***

Identifikátor bloku	----------B----------
Názov výrobcu VU	B Name_____
Adresa výrobcu VU	Address_____
Číslo dielu VU	PartNumber_____
Schvaľovacie číslo VU	Apprv_____
Sériové číslo VU	S/N_____
Rok výroby VU	yyyy
Verzia a dátum inštalácie softvéru VU	V xxxx dd/mm/yyyy

15 ***Identifikačné údaje snímača***

Identifikátor bloku	----------Л----------

15.1 *Záznam o párovaní*

Sériové číslo snímača	Л S/N_____
Schvaľovacie číslo snímača	Apprv_____
Dátum párovania snímača	dd/mm/yyyy hh:mm

16 ***Identifikácia GNSS***

Identifikátor bloku	----------▚----------

16.1. *Záznam o spojení*

Sériové číslo externého zariadenia GNSS	▚ S/N_____
Schvaľovacie číslo externého zariadenia GNSS	Apprv_____
Dátum spojenia externého zariadenia GNSS	dd/mm/yyyy hh:mm

17 ***Kalibračné údaje***

Identifikátor bloku	----------T----------

17.1 *Záznam o kalibrácii*

Identifikátor záznamu	----------
Dielňa, ktorá kalibráciu vykonala	T Workshop_name_____
Adresa dielne	Workshop_address_____
Identifikácia dielenskej karty	Card_Identification_____
Dátum skončenia platnosti dielenskej karty	dd/mm/yyyy
Prázdny riadok	
Dátum kalibrácie + účel kalibrácie	T dd/mm/yyyy (p)
VIN	A VIN_____
Členský štát evidencie a VRN	Nat/VRN_____
Charakteristický koeficient vozidla	w xx xxx Imp/km
Konštanta záznamového zariadenia	k xx xxx Imp/km
Effective circumference of wheel tyres	l xx xxx mm
Rozmer pneumatík na vozidle	● TyreSize_____
Nastavenie obmedzovača rýchlosti	> xxx km/h
Pôvodný a nový stav kilometrov	x xxx xxx – x xxx xxx km

Účel kalibrácie (p) je číselný kód vysvetľujúci, prečo sa tieto kalibračné parametre zaznamenali, kódovaný v súlade s dátovým prvkom `CalibrationPurpose`.

18 ***Úprava času***

	Identifikátor bloku	`----------◷----------`
18.1	*Záznam o úprave času*	
	Identifikátor záznamu	`--------------------`
	Pôvodný dátum a čas	`!◷ dd/mm/yyyy hh:mm`
	Nový dátum a čas	`◷ dd/mm/yyyy hh:mm`
	Dielňa, ktorá úpravu času vykonala	`T Workshop_name_____`
	Adresa dielne	`Workshop_address_____`
	Identifikácia dielenskej karty	`Card_Identification_____`
	Dátum skončenia platnosti dielenskej karty	`dd/mm/yyyy`

19 ***Najnovšia udalosť a porucha zaznamenaná vo VU***

	Identifikátor bloku	`----------!×🚙----------`
	Dátum a čas najnovšej udalosti	`! dd/mm/yyyy hh:mm`
	Dátum a čas najnovšej poruchy	`× dd/mm/yyyy hh:mm`

20 ***Informácie o kontrole prekročenia rýchlosti***

	Identifikátor bloku	`----------»»----------`
	Dátum a čas poslednej KONTROLY PREKROČENIA RÝCHLOSTI	`»▫dd/mm/yyyy hh:mm`
	Dátum/čas prvého prekročenia rýchlosti a počet následných prekročení	`»»dd/mm/yyyy hh:mm (nnn)`

21 ***Záznam o prekročení rýchlosti***

21.1	Identifikátor bloku „Prvé prekročenie rýchlosti po poslednej kalibrácii“	`--------»»T---------`
21.2	Identifikátor bloku „5 najzávažnejších za posledných 365 dní“	`-------»»(365)------`
21.3	Identifikátor bloku „Najvážnejšie za každý z posledných 10 dní výskytu“	`-------»»(10)-------`
21.4	Identifikátor záznamu	`--------------------`
	Dátum, čas a trvanie	`»»dd/mm/yyyy hh:mm hhhmm`
	Maximálna a priemerná rýchlosť, počet podobných udalostí v tento deň	`xxx km/h xxx km/h(xxx)`
	Priezvisko vodiča	`◙ Last_Name_____`
	Meno(-á) vodiča	`First_Name_____`
	Identifikácia karty vodiča	`Card_Identification_____`
21.5	Ak v bloku neexistuje záznam o prekročení rýchlosti	`»»---`

22 ***Rukou písané informácie***

	Identifikátor bloku	`------------------------`
22.1	Miesto kontroly	`▫● .....`
22.2	Podpis kontrolóra	`▫ .....`
22.3	Čas začiatku	`◷+ .....`
22.4	Čas skončenia	`+◷ .....`
22.5	Podpis vodiča	`◙ .....`

„Rukou písané informácie“; nad každú položku treba vložiť dosť prázdnych riadkov, aby sa dala vyplniť/podpísať rukou.

23 ***Karty naposledy vložené do VU***

Identifikátor bloku

23.1 Vložená karta

Identifikátor záznamu

Typ karty, generácia, verzia, výrobca (*)

Identifikácia karty

Sériové číslo karty

Dátum a čas posledného vloženia karty

```
-------- ⊟▣◷ --------

----
⊤ <gen> <version> <MC>
Card Identification
Card Serial Number
dd/mm/yyyy hh:mm
```

(*) (všetko v jednom riadku)

pričom

typ karty: Piktogram, jeden znak + medzera

gen: GEN1 alebo GEN2, 4 znaky + medzera

verzia: max. 10 znakov

VÝR: kód výrobcu, 3 znaky

3. ŠPECIFIKÁCIE VÝPISOV

V tejto kapitole sa použila táto notácia:

N	Tlačený blok alebo záznam s číslom N
N	Tlačený blok alebo záznam s číslom N, opakovaný toľko ráz, koľko treba
X/Y	Tlačené bloky alebo záznamy X a/alebo Y podľa potreby, opakované toľko ráz, koľko treba.

3.1. **Denný výpis činností vodiča z karty**

PRT_008 Denný výpis činností vodiča z karty musí mať tento formát:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia kontrolóra (ak je vo VU vložená kontrolná karta)
3	Identifikácia vodiča (z karty, pre ktorú sa výpis pripravuje + GEN)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
5	Identifikácia VU (VU, z ktorej sa výpis berie + GEN)
6	Posledná kalibrácia tejto VU
7	Posledná predošlá kontrola kontrolovaného vodiča
8	Oddeľovač činností vodiča
8a	Podmienka „Záznamové zariadenie sa nevyžaduje“ na začiatku tohto dňa
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Činnosti vodiča zoradené chronologicky
11	Oddeľovač denného súhrnu

11.4	Miesta zadané v chronologickom poradí
11.5	Údaje GNSS
11.6	Činnosti celkom
12.1	Oddeľovač udalostí alebo porúch z karty
12.4	Záznamy udalostí/porúch (posledných 5 udalostí alebo porúch uložených na karte)
13.1	Oddeľovač udalostí alebo porúch z VU
13.4	Záznamy udalostí/porúch (posledných 5 udalostí alebo porúch uložených alebo prebiehajúcich vo VU)
22.1	Miesto kontroly
22.2	Podpis kontrolóra
22.5	Podpis vodiča

3.2. **Denný výpis činností vodiča z VU**

PRT_009 Denný výpis činností vodiča z VU musí mať tento formát:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia držiteľa karty (pre všetky karty vložené do VU + GEN)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
5	Identifikácia VU (VU, z ktorej sa výpis berie + GEN)
6	Posledná kalibrácia tejto VU
7	Posledná kontrola tohto tachografu
9	Oddeľovač činností vodiča
10	Oddeľovač slotu vodiča (slot 1)
10a	Podmienka „Záznamové zariadenie sa nevyžaduje“ na začiatku tohto dňa
10.1 / 10.2 / 10.3 /10.3a / 10.4	Činnosti v chronologickom poradí (slot vodiča)
10	Oddeľovač slotu druhého vodiča (slot 2)
10a	Podmienka „Záznamové zariadenie sa nevyžaduje“ na začiatku tohto dňa
10.1 / 10.2 / 10.3 /10.3a / 10.4	Činnosti v chronologickom poradí (slot druhého vodiča)
11	Oddeľovač denného súhrnu
11.1	Súhrn časových úsekov bez karty v slote vodiča
11.4	Miesta zadané v chronologickom poradí
11.5	Údaje GNSS
11.6	Činnosti celkom
11.2	Súhrn časových úsekov bez karty v slote druhého vodiča
11.4	Miesta zadané v chronologickom poradí
11.5	Údaje GNSS

11.7	Činnosti celkom
11.3	Súhrn činností vodiča z oboch slotov
11.4	Miesta zadané týmto vodičom v chronologickom poradí
11.5	Údaje GNSS
11.8	Činnosti celkom za tohto vodiča
13.1	Oddeľovač udalostí a porúch
12.4	Záznamy udalostí/porúch (posledných 5 udalostí alebo porúch uložených alebo prebiehajúcich vo VU)
13.1	Miesto kontroly
22.2	Podpis kontrolóra
22.3	Čas začiatku (miesto, v ktorom môže vodič bez karty uviesť, ktoré časové úseky sa na neho vzťahujú)
22.4	Čas skončenia
22.5	Podpis vodiča

3.3. **Výpis udalostí a porúch z karty**

PRT_010 Výpis udalostí a porúch z karty musí mať tento formát:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia kontrolóra (ak je vo VU vložená kontrolná karta + GEN)
3	Identifikácia vodiča (z karty, pre ktorú sa výpis pripravuje)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
12.2	Oddeľovač udalostí
12.4	Záznamy udalostí (všetky udalosti uložené na karte)
12.3	Oddeľovač porúch
12.4	Záznamy porúch (všetky poruchy uložené na karte)
22.1	Miesto kontroly
22.2	Podpis kontrolóra
22.5	Podpis vodiča

3.4. **Výpis udalostí a porúch z VU**

PRT_011 Výpis udalostí a porúch z VU musí mať tento formát:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia držiteľa karty (pre všetky karty vložené do VU + GEN)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)

13.2	Oddeľovač udalostí
13.4	Záznamy udalostí (všetky udalosti uložené alebo prebiehajúce vo VU)
13.3	Oddeľovač porúch
13.4	Záznamy porúch (všetky poruchy uložené alebo prebiehajúce vo VU)
22.1	Miesto kontroly
22.2	Podpis kontrolóra
22.5	Podpis vodiča

3.5. **Výpis technických údajov**

PRT_012 Výpis technických údajov musí mať tento formát:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia držiteľa karty (pre všetky karty vložené do VU + GEN)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
14	Identifikácia VU
15	Identifikačné údaje snímača
15.1	Údaje o párovaní snímača (všetky dostupné údaje zoradené chronologicky)
16	Identifikácia GNSS
16.1	Údaje o spojení externého zariadenia GNSS (všetky dostupné údaje zoradené chronologicky)
17	Oddeľovač kalibračných údajov
17.1	Kalibračné záznamy (všetky dostupné záznamy v chronologickom poradí)
18	Oddeľovač úpravy času
18.1	Záznamy o úprave času (všetky záznamy dostupné zo záznamov o úprave času a kalibrácii)
19	Najnovšia udalosť a porucha zaznamenaná vo VU

3.6. **Výpis prekročenia rýchlosti**

PRT_013 Výpis prekročenia rýchlosti musí mať tento formát:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia držiteľa karty (pre všetky karty vložené do VU + GEN)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
20	Informácie o kontrole prekročenia rýchlosti
21.1	Identifikátor údajov o prekročení rýchlosti
21.4 / 21.5	Prvé prekročenie rýchlosti po poslednej kalibrácii

21.2	Identifikátor údajov o prekročení rýchlosti
21.4 / 21.5	5 najzávažnejších udalostí prekročenia rýchlosti za posledných 365 dní
21.3	Identifikátor údajov o prekročení rýchlosti
21.4 / 21.5	Najzávažnejšia udalosť prekročenia rýchlosti za každý z 10 posledných dní výskytu
22.1	Miesto kontroly
22.2	Podpis kontrolóra
22.5	Podpis vodiča

3.7. **História vložených kariet**

PRT_014 Výpis histórie vložených kariet musí mať tento formát:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia držiteľa karty (pre všetky karty vložené vo VU)
23	Karta naposledy vložená do VU
23.1	Vložené karty (do 88 záznamov)
12.3	Oddeľovač porúch

Dodatok 5

ZOBRAZENIE

V tomto dodatku sa použila táto formátová notácia:

— znaky vytlačené **tučným písmom** znamenajú nekódovaný text na zobrazenie (zobrazia sa normálne znaky),

— normálne znaky znamenajú premenné (piktogramy alebo dáta), ktoré sa majú pri zobrazení nahradiť ich hodnotami:

— dd mm rrrr: deň, mesiac, rok,

— hh: hodiny,

— mm: minúty

— D: piktogram trvania,

— EF: kombinácia piktogramov udalostí alebo porúch,

— O: piktogram režimu prevádzky.

DIS_001 Tachograf musí údaje zobrazovať v týchto formátoch:

Údaje	Formát
Predvolené zobrazenie	
Miestny čas	hh:mm
Režim prevádzky	O
Informácie o vodičovi	1 Dhh**h**mm ▮▮hh**h**mm
informácie o druhom vodičovi	2 Dhh**h**mm
Otvorená podmienka „zariadenie sa nevyžaduje“	OUT
Výstražné zobrazenie	
Prekročenie nepretržitého času jazdy	1 ⊙ hh**h**mm ▮▮hh**h**mm
Udalosť alebo porucha	EF
Iné zobrazenia	
Dátum UTC čas	UTC ◔ dd/mm/rrrr alebo UTC ◔ dd.mm.rrrr hh:mm
Nepretržitý čas jazdy a kumulovaný čas prestávok vodiča	1 ⊙ hh**h**mm ▮▮hh**h**mm
Nepretržitý čas jazdy a kumulovaný čas prestávok druhého vodiča	2 ⊙ hh**h**mm ▮▮hh**h**mm
Kumulovaný čas jazdy vodiča za predošlý a aktuálny týždeň	1 ⊙ ▮ hhh**h**mm
Kumulovaný čas jazdy druhého vodiča za predošlý a aktuálny týždeň	2 ⊙ ▮ hhh**h**mm

Dodatok 6

PREDNÝ KONEKTOR NA KALIBRÁCIU A SŤAHOVANIE

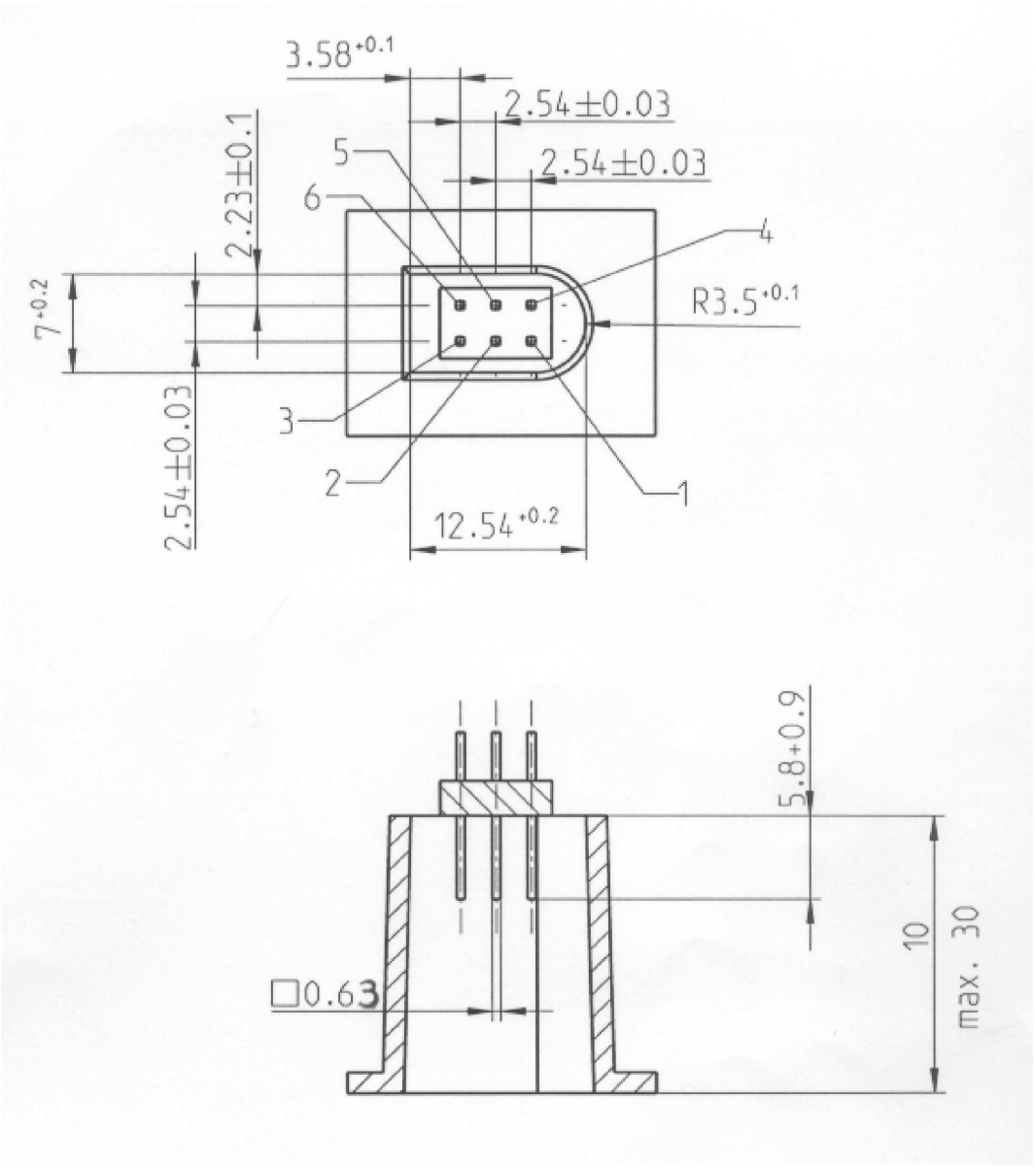
OBSAH

1. HARDVÉR 256
1.1. Konektor 256
1.2. Rozloženie kontaktov 257
1.3. Bloková schéma 258
2. ROZHRANIE SŤAHOVANIA 258
3. ROZHRANIE KALIBRÁCIE 259

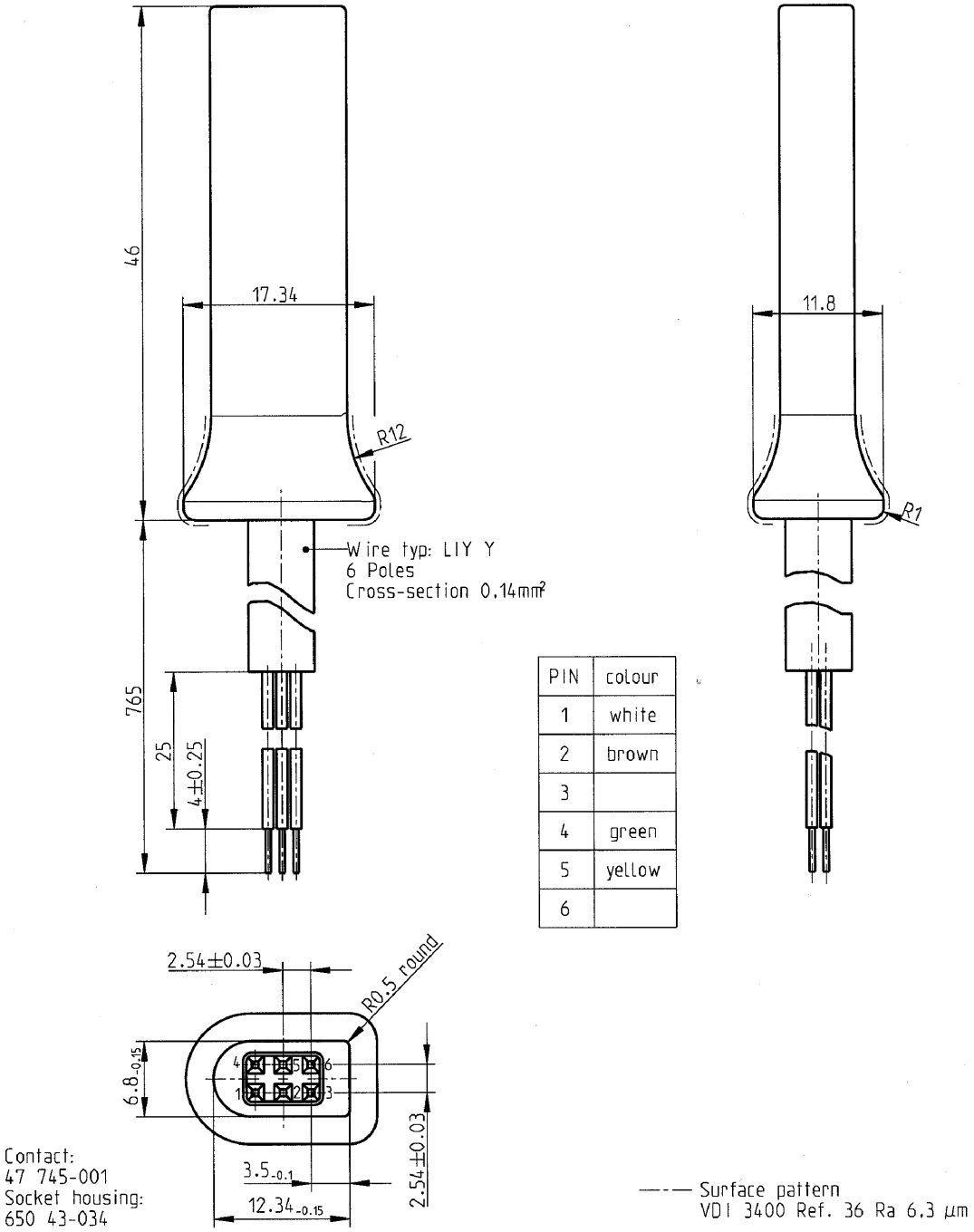
1. HARDVÉR

1.1. **Konektor**

INT_001 Konektor sťahovania/kalibrácie musí byť šesťkolíkový, prístupný z predného panelu bez potreby odpojenia akejkoľvek časti tachografu a musí zodpovedať týmto náčrtom (všetky rozmery v milimetroch):



Na nasledovnom náčrte je zobrazená bežná šesťkolíková zástrčka:



1.2. **Rozloženie kontaktov**

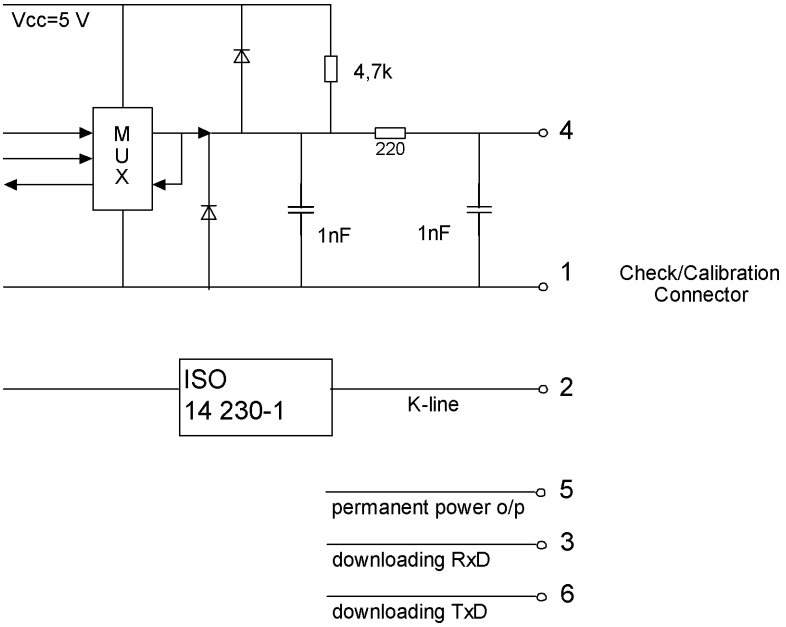
INT_002 Kontakty musia byť rozložené v súlade s touto tabuľkou:

Kolík	Opis	Poznámka
1	Záporný pól batérie	Pripojený k zápornému pólu batérie vozidla
2	Dátová komunikácia	K-vedenie (ISO 14230-1)

Kolík	Opis	Poznámka
3	RxD – sťahovanie	Dátový vstup do tachografu
4	Vstupný/výstupný signál	Kalibrácia
5	Stály výstupný prúd	Rozsah napätia je špecifikovaný ako napätie vozidla mínus 3V vzhľadom na možnosť poklesu napätia v ochrannom prúdovom obvode Výstup 40 mA
6	TxD – sťahovanie	Dátový výstup z tachografu

1.3. **Bloková schéma**

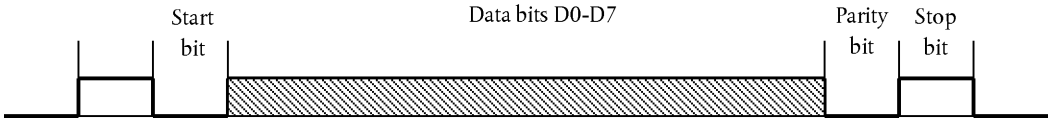
INT_003 Bloková schéma musí zodpovedať tejto:



2. ROZHRANIE SŤAHOVANIA

INT_004 Rozhranie sťahovania musí zodpovedať špecifikáciám RS232.

INT_005 Rozhranie sťahovania používa jeden úvodný bit (start bit), 8 dátových bitov s bitom najnižšieho rádu na prvom mieste, jeden bit párnej parity a jeden záverečný bit (stop bit).



Organizácia dátového bajtu

Start bit:	jeden bit s logickou úrovňou 0
Dátové bity:	prvý sa prenáša bit najnižšieho rádu;
Bit parity (kontrolný súčet):	párna parita
Stop bit:	jeden bit s logickou úrovňou 1

Keď sa prenášajú numerické dáta zložené z viac než jedného bajtu, bajt najvyššieho rádu sa prenáša prvý a bajt najnižšieho rádu posledný.

INT_006 Prenosová rýchlosť musí byť nastaviteľná od 9 600 bps do 115 200 bps. Prenos sa uskutoční pri najvyššej možnej prenosovej rýchlosti, pričom počiatočná prenosová rýchlosť po začiatku komunikácie sa nastaví na 9 600 bps.

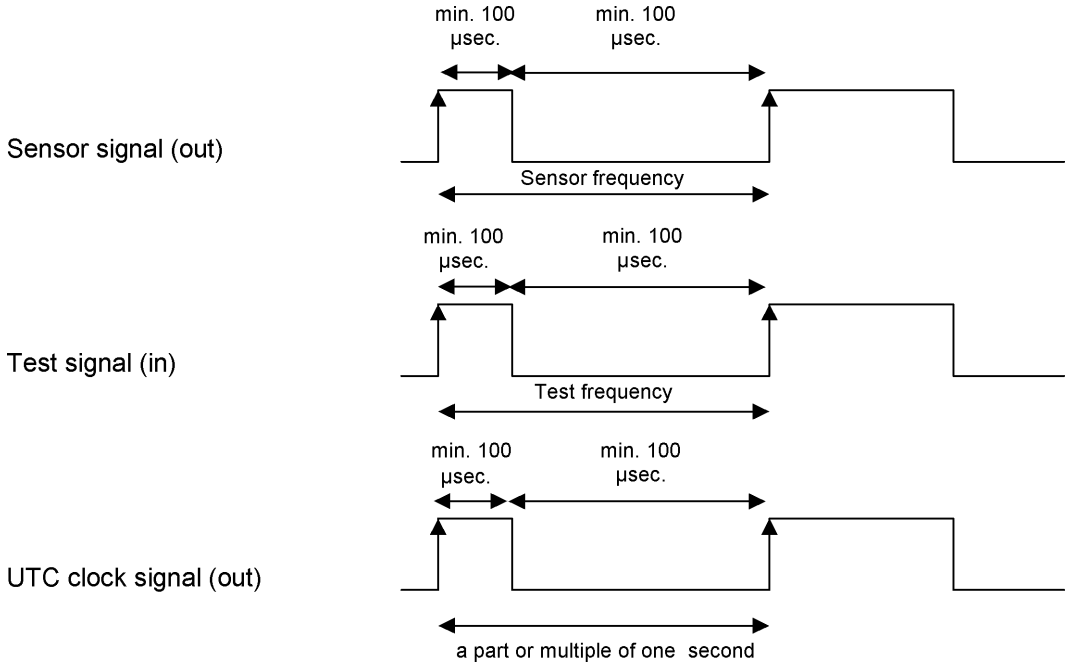
3. ROZHRANIE KALIBRÁCIE

INT_007 Dátová komunikácia musí zodpovedať norme ISO 14230-1 Cestné vozidlá. Diagnostické systémy. Protokol Kľúčového slova 2000. Časť 1: Fyzikálna vrstva. Prvé vydanie: 1999.

INT_008 Vstupný/výstupný signál musí zodpovedať týmto elektrickým špecifikáciám:

Paramter	Minimum	Bežne	Maximum	Poznámka
U_{low} (vstup)			1,0 V	I = 750 µA
U_{high} (vstup)	4 V			I = 200 µA
Frekvencia			4 kHz	
U_{low} (výstup)			1,0 V	I = 1 mA
U_{high} (výstup)	4 V			I = 1 mA

INT_009 Vstupný/výstupný signál musí zodpovedať týmto časovým diagramom:



Dodatok 7

PROTOKOLY SŤAHOVANIA ÚDAJOV

OBSAH

1. ÚVOD 261
1.1. Rozsah pôsobnosti 261
1.2. Akronymy a notácie 261
2. SŤAHOVANIE ÚDAJOV Z JEDNOTKY VOZIDLA 262
2.1. Postup sťahovania 262
2.2. Protokol sťahovania údajov 262
2.2.1 Štruktúra správy 262
2.2.2 Typy správ 264
2.2.2.1 Start Communication Request (SID 81) 266
2.2.2.2 Positive Response Start Communication (SID C1) 266
2.2.2.3 Start Diagnostic Session Request (SID 10) 266
2.2.2.4 Positive Response Start Diagnostic (SID 50) 266
2.2.2.5 Link Control Service (SID 87) 266
2.2.2.6 Link Control Positive Response (SID C7) 266
2.2.2.7 Request Upload (SID 35) 266
2.2.2.8 Positive Response Request Upload (SID 75) 266
2.2.2.9 Transfer Data Request (SID 36) 266
2.2.2.10 Positive Response Transfer Data (SID 76) 267
2.2.2.11 Request Transfer Exit (SID 37) 267
2.2.2.12 Positive Response Request Transfer Exit (SID 77) 267
2.2.2.13 Stop Communication Request (SID 82) 267
2.2.2.14 Positive Response Stop Communication (SID C2) 267
2.2.2.15 Acknowledge Sub Message (SID 83) 267
2.2.2.16 Negative Response (SID 7F) 268
2.2.3 Tok správ 268
2.2.4 Časovanie 269
2.2.5 Spracovanie chýb 270
2.2.5.1 Start Communication phase 270
2.2.5.2 Communication phase 270
2.2.6 Obsah správy s odpoveďou 272
2.2.6.1 Positive Response Transfer Data Overview 273
2.2.6.2 Positive Response Transfer Data Activities 274
2.2.6.3 Positive Response Transfer Data Events and Faults 275
2.2.6.4 Positive Response Transfer Data Detailed Speed 276
2.2.6.5 Positive Response Transfer Data Technical Data 276
2.3. Pamäť ESM 277

3. PROTOKOL SŤAHOVANIA ÚDAJOV Z TACHOGRAFOVÝCH KARIET 277
3.1. Rozsah pôsobnosti 277
3.2. Vymedzenie pojmov 277
3.3. Sťahovanie údajov z karty 277
3.3.1 Inicializácia sekvencie 278
3.3.2 Sekvencia pre nepodpísané dátové súbory 278
3.3.3 Sekvencia pre podpísané dátové súbory 279
3.3.4 Sekvencia pre resetovanie kalibračného počítadla 279
3.4. Formát dátovej pamäte 280
3.4.1 Úvod 280
3.4.2 Formát súboru 280
4. SŤAHOVANIE ÚDAJOV Z TACHOGRAFOVEJ KARTY CEZ JEDNOTKU VOZIDLA 281

1. ÚVOD

V tomto dodatku sa špecifikujú postupy pre rôzne druhy sťahovania údajov na externé pamäťové médium (ESM) spolu s protokolmi, ktoré musia byť zavedené preto, aby bol zaručený správny prenos údajov a úplná kompatibilita formátu sťahovaných údajov, tak aby kontrolór mohol overiť tieto údaje a mohol pred ich analýzou skontrolovať ich autenticitu a integritu.

1.1 Rozsah pôsobnosti

údaje sa môžu na ESM sťahovať z:

— jednotky vozidla (VU) pomocou inteligentného vyhradeného zariadenia (IDE) pripojeného k VU,

— tachografovej karty pomocou IDE vybaveného zariadením s rozhraním karty (IFD),

— tachografovej karty cez jednotku vozidla pomocou IDE pripojeného k VU.

Na to, aby bolo možné overiť autenticitu a integritu sťahovaných údajov uložených na ESM, sa údaje sťahujú s pripojeným podpisom v súlade s dodatkom 11 Spoločné bezpečnostné mechanizmy. Sťahujú sa aj údaje o identifikácii zdrojového zariadenia (VU alebo karty) a jeho osvedčení zabezpečenia (členský štát a zariadenie). Verifikátor údajov musí vlastniť nezávislý a spoľahlivý európsky verejný kľúč.

DDP_001 Údaje stiahnuté počas jednej relácie sťahovania musia byť uložené v ESM v jednom súbore.

1.2 Akronymy a notácie

V tomto dodatku sa používajú tieto akronymy a notácie:

AID Application Identifier (identifikátor aplikácie)

ATR Answer To Reset (odozva na reset)

CS Checksum byte (bajt kontrolného súčtu)

DF Dedicated File (vyhradený súbor)

DS_ Diagnostic Session (diagnostická relácia)

EF Elementary File (elementárny súbor)

ESM External Storage Medium (externé pamäťové médium)

FID File Identifier (File ID, identifikátor súboru)

FMT Format Byte (formátový bajt – prvý bajt záhlavia správy)

ICC Integrated Circuit Card (karta s integrovaným obvodom)

IDE Intelligent Dedicated Equipment (inteligentné vyhradené zariadenie): zariadenie používané na sťahovanie údajov na ESM (napr. osobný počítač)

IFD Interface Device (zariadenie s rozhraním)

KWP Keyword Protocol 2000 (protokol kľúčového slova 2000)

LEN Length Byte (dĺžkový bajt – posledný bajt záhlavia správy)

PPS Protocol Parameter Selection (voľba parametra protokolu)

PSO Perform Security Operation (vykonanie operácie zabezpečenia)

SID Service Identifier (identifikátor služby)

SRC Source byte (zdrojový bajt)

TGT Target Byte (cieľový bajt)

TLV Tag Length Value (hodnota dĺžky tagu)

TREP Transfer Response Parameter (parameter prenosu odpovede)

TRTP Transfer Request Parameter (parameter prenosu požiadavky)

VU Vehicle Unit (jednotka vozidla – VU)

2. SŤAHOVANIE ÚDAJOV Z JEDNOTKY VOZIDLA

2.1 **Postup sťahovania**

Pri sťahovaní údajov z VU musí operátor vykonať tieto operácie:

— vložiť svoju tachografovú kartu do slotu VU (*),

— pripojiť IDE ku konektoru sťahovania VU,

— vytvoriť spojenie medzi IDE a VU,

— zvoliť na IDE údaje, ktoré sa majú sťahovať, a odoslať požiadavku VU,

— uzavrieť reláciu sťahovania údajov.

2.2 **Protokol sťahovania údajov**

Protokol je štruktúrovaný na základe „master/slave“, s IDE ako nadradeným zariadením („master“) a s VU ako podriadeným zariadením („slave“).

Štruktúra, typy a tok správ sú v zásade založené na protokole kľúčového slova 2000 (KWP) (ISO 14230-2 Cestné vozidlá.Diagnostické systémy.Protokol kľúčového slova 2000.Časť 2: Vrstva údajového spojenia).

Aplikačná vrstva spočíva v zásade na súčasnom návrhu normy ISO 14229-1 (Cestné vozidlá.Diagnostické systémy.Časť 1: Diagnostické služby, verzia 6 z 22. februára 2001).

2.2.1 *Štruktúra správy*

DDP_002 Všetky správy vymieňané medzi IDE a VU sú formátované so štruktúrou pozostávajúcou z troch častí:

— záhlavie pozostávajúce z formátového bajtu (FMT), cieľového bajtu (TGT) a zo zdrojového bajtu (SRC) a prípadne z dĺžkového bajtu (LEN),

— dátové pole pozostávajúce z bajtu identifikátora služby (SID) a variabilného počtu dátových bajtov, ktoré môžu zahŕňať voliteľný bajt diagnostickej relácie (DS_) alebo voliteľný bajt parametra prenosu (TRTP alebo TREP),

— kontrolný súčet pozostávajúci z bajtu kontrolného súčtu (CS).

Záhlavie				Dátové pole					Kontrolný súčet
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bajty				Maximálne 255 bajtov					1 bajt

(*) Vložená karta spustí príslušné prístupové práva k funkcii sťahovania a k údajom. Musí však byť možné sťahovať údaje z karty vodiča vloženej do jedného zo slotov VU, keď v druhom slote nie je vložená žiadna karta iného typu.

Bajty TGT a SRC predstavujú fyzickú adresu príjemcu a pôvodcu správy. Hodnoty sú F0 Hex pre IDE a EE Hex pre VU.

Bajt LEN je dĺžka časti dátového poľa.

Bajt kontrolného súčtu je 8-bitový súčet modulov 256 všetkých bajtov správy, okrem samotného CS.

Bajty FMT, SID, DS_, TRTP a TREP sú vymedzené na inom mieste tohto dokumentu.

DDP_003 V prípade, keď sú údaje, ktoré sa majú prenášať v správe, dlhšie než disponibilné miesto v časti dátového poľa, správa sa odošle vo viacerých čiastkových správach. Každá čiastková správa musí mať záhlavie, rovnaké bajty SID a TREP a dvojbajtové počítadlo čiastkovej správy udávajúce číslo čiastkovej správy v rámci celej správy. S cieľom umožniť kontrolu chýb a zrušenie zariadenie IDE potvrdzuje každú čiastkovú správu. IDE môže prijať čiastkovú správu, požiadať o jej nový prenos, ako aj požadovať od VU, aby znovu začala alebo zrušila prenos.

DDP_004 Ak posledná čiastková správa obsahuje presne 255 bajtov v dátovom poli, musí byť pripojená záverečná čiastková správa s prázdnym dátovým poľom (okrem bajtov SID a TREP a počítadla čiastkovej správy), aby bol zrejmý koniec správy.

Príklad:

Záhlavie	SID	TREP	Správa	CS
4 bajty	Dlhšia než 255 bajtov			

Bude sa prenášať ako:

Záhlavie	SID	TREP	00	01	Čiastková správa 1	CS
4 bajty	255 bajtov					

Záhlavie	SID	TREP	00	02	Čiastková správa 2	CS
4 bajty	255 bajtov					

…

Záhlavie	SID	TREP	xx	yy	Čiastková správa n	CS
4 bajtov	Menej než 255 bajtov					

alebo ako:

Záhlavie	SID	TREP	00	01	Čiastková správa 1	CS
4 bajtov	255 bajtov					

Záhlavie	SID	TREP	00	02	Čiastková správa 2	CS
4 bajtov	255 bajtov					

…

Záhlavie	SID	TREP	xx	yy	Čiastková správa n	CS
4 bajtov	255 bajtov					

Záhlavie	SID	TREP	xx	yy + 1	CS
4 bajtov	4 bajty				

2.2 *Typy správ*

Komunikačný protokol pre údaje sťahované medzi VU a IDE si vyžaduje výmenu ôsmich rôznych typov správ.

V nasledujúcej tabuľke sú uvedené správy zhrnuté.

Štruktúra správy	Max. 4 bajty Záhlavie				Max. 255 bajtov Údaje			1 bajt Kontrolný súčet
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (stage 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
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0 A	35		00,00, 00,00, 00,FF,FF, FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5

Štruktúra správy	Max. 4 bajty Záhlavie				Max. 255 bajtov Údaje			1 bajt Kontrolný súčet
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9 A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06	Slot	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Poznámky:

— Sid Req = Sid zodpovedajúcej požiadavky.

— TREP = TRTP zodpovedajúcej požiadavky.

— Tmavé okienka znamenajú, že sa nič neprenáša.

— Výraz „odoslanie údajov“ („upload“, z pohľadu IDE) sa používa vzhľadom na kompatibilitu s normou ISO 14229. Znamená to isté ako „sťahovanie údajov“ („download“, z pohľadu VU).

— Možné dvojbajtové počítadlá čiastkovej správy nie sú v tejto tabuľke uvedené.

— Slot je číslo slotu, buď „1“ (karta v slote vodiča), alebo „2“ (karta v slote druhého vodiča).

— V prípade, že slot nie je špecifikovaný, VU zvolí slot 1, ak je karta vložená v tomto slote, a slot 2 zvolí iba v prípade, že ho výslovne zvolí používateľ.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 Túto správu vydáva IDE na vytvorenie komunikačného spojenia s VU. Počiatočné komunikácie sa vždy vykonávajú prenosovou rýchlosťou 9 600 baudov (pokiaľ sa prenosová rýchlosť prípadne nezmení s použitím vhodnej služby Link control service).

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Túto správu vydáva VU ako kladnú odpoveď na požiadavku Start communication request. Obsahuje dva kľúčové bajty „EA“ „8F“, ktoré udávajú, že jednotka podporuje protokol so záhlavím vrátane cieľových, zdrojových a dĺžkových informácií.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 Správu Start diagnostic session request vydáva IDE, aby sa začala nová diagnostická relácia s VU. Subfunkcia „default session“ (81 Hex) udáva, že sa zaviedla štandardná diagnostická relácia.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 Správu Positive response start diagnostic posiela VU ako kladnú odpoveď na požiadavku Diagnostic session request.

2.2.2.5 Link Control Service (SID 87)

DDP_052 Službu Link control service používa IDE na začatie zmeny prenosovej rýchlosti. Vykonáva sa v dvoch krokoch. V prvom kroku zariadenie IDE navrhne zmenu prenosovej rýchlosti a uvedie novú rýchlosť. Po prijatí kladnej odpovede z VU odošle IDE potvrdenie zmeny prenosovej rýchlosti na VU (druhý krok). IDE potom zmení prenosovú rýchlosť. Po prijatí potvrdenia prejde VU na novú prenosovú rýchlosť.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 Správu Link control positive response pošle VU ako kladnú odpoveď na požiadavku Link control service request (prvý krok). Všimnite si, že na potvrdzujúcu správu sa nedáva žiadna odpoveď (druhý krok).

2.2.2.7 Request Upload (SID 35)

DDP_009 Správu Request upload vydáva zariadenie IDE ako oznámenie pre VU, že sa požaduje operácia sťahovania. V zhode s normou ISO 14229 táto požiadavka obsahuje údaje o adrese, veľkosti a formáte požadovaných údajov. Keďže tieto údaje nie sú pre IDE známe pred sťahovaním, adresa pamäte je nastavená na 0, formát sa nešifrovaný a nekomprimovaný a veľkosť pamäte je nastavená na maximum.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 Správu Positive response request upload posiela VU, aby oznámila IDE, že VU je pripravená na sťahovanie údajov. V zhode s normou ISO 14229 táto správa s kladnou odpoveďou obsahuje aj údaje, ktorými sa IDE oznamuje, že ďalšie správy Positive response transfer data budú obsahovať maximálne 00FF hex bajtov.

2.2.2.9 Transfer Data Request (SID 36)

DDP_011 Správu Transfer data request posiela IDE, aby pre VU špecifikovalo typ údajov, ktoré sa majú sťahovať. Jednobajtový Transfer Request Parameter (TRTP) udáva typ prenosu.

Existuje šesť typov prenosu údajov:

— prehľad (TRTP 01),

— činnosti určitého dňa (TRTP 02),

— udalosti a poruchy (TRTP 03),

— presné údaje o rýchlosti (TRTP 04),

— technické údaje (TRTP 05),

— sťahovanie karty (TRTP 06).

DDP_054 IDE musí požiadať o prehľad prenosu údajov (TRTP 01) počas relácie sťahovania, keďže len to zabezpečí, že sa certifikáty VU zaznamenajú v rámci sťahovaného súboru (a bude možné overiť digitálny podpis).

V druhom prípade (TRTP 02) správa Transfer Data Request obsahuje údaje kalendárneho dňa (formát `TimeReal`), ktorý sa má sťahovať.

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 Správu Positive response transfer data posiela VU ako odpoveď na požiadavku Transfer data request. Správa obsahuje požadované údaje s Transfer Response Parameter (TREP), ktorý zodpovedá parametru TRTP požiadavky.

DDP055 V prvom prípade (TREP 01) posiela VU údaje, ktoré pomáhajú operátorovi zariadenia IDE pri výbere údajov, ktoré chce ďalej sťahovať. Informácie obsiahnuté v správe sú tieto:

— osvedčenia zabezpečenia,

— identifikácia vozidla,

— aktuálny dátum a čas VU,

— minimálny a maximálny sťahovateľný dátum (údaje VU),

— údaje o prítomnosti kariet vo VU,

— predchádzajúce sťahovanie pre podnik,

— podnikové blokovanie,

— predchádzajúce kontroly.

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 Správu Request Transfer Exit posiela IDE, aby bola VU informovaná, že relácia sťahovania sa skončila.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 Správu Positive Response Request transfer exit posiela VU ako potvrdenie požiadavky Request Transfer Exit.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 Správu Stop Communication Request posiela IDE, aby sa prerušilo komunikačné spojenie s VU.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 Správu Positive Response Stop Communication posiela VU ako potvrdenie požiadavky Stop Communication Request.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 Správu Acknowledge Sub Message posiela IDE, aby sa potvrdilo prijatie jednotlivých častí správy, ktorá sa prenáša vo viacerých čiastkových správach. Dátové pole obsahuje identifikátor služby SID prijatý z VU a dvojbajtový kód takto:

— MsgC + 1 potvrdzuje správne prijatie čiastkovej správy s číslom MsgC.

Požiadavku z IDE na VU, aby poslala ďalšiu čiastkovú správu.

— MsgC poukazuje na problém s prijatím čiastkovej správy s číslom MsgC.

Požiadavku z IDE na VU, aby znovu poslala čiastkovú správu.

— FFFF požaduje ukončenie správy.

Toto môže IDE použiť na ukončenie prenosu správy VU z akéhokoľvek dôvodu.

Posledná čiastková správa správy (LEN bajt < 255) sa môže potvrdiť použitím ktoréhokoľvek z týchto kódov alebo sa nemusí potvrdiť vôbec.

Odpovede VU pozostávajúce z viacerých čiastkových správ:

— Positive Response Transfer Data (SID 76)

2.2.2.16 Negative Response (SID 7F)

DDP_018 Správu Negative Response posiela VU ako odpoveď na správy týkajúce sa uvedenej požiadavky, keď VU nemôže túto požiadavku splniť. Dátové polia správy obsahujú SID odpovede (7F), SID požiadavky a kód špecifikujúci dôvod zápornej odpovede. K dispozícii sú tieto kódy:

— 10 general reject

Činnosť sa nemôže vykonať, lebo nebol uvedený príslušný dôvod.

— 11 service not supported

SID požiadavky nie je zrozumiteľný.

— 12 sub function not supported

Bajty DS_ alebo TRTP požiadavky nie sú zrozumiteľné alebo neexistuje žiadna ďalšia čiastková správa, ktorá by sa mala prenášať.

— 13 incorrect message length

Dĺžka prijatej správy nie je správna.

— 22 conditions not correct or request sequence error

Požadovaná služba nie je aktívna alebo sekvencia správ s požiadavkami nie je správna.

— 31 Request out of range

Záznam o parametri požiadavky (dátové pole) nie je platný.

— 50 upload not accepted

Požiadavka sa nemôže splniť (VU v nevhodnom režime prevádzky alebo vnútorná porucha VU).

— 78 response pending

Požadovaná činnosť sa nemôže dokončiť načas a VU nie je pripravená na prijatie ďalšej požiadavky.

— FA data not available

Dátový objekt požiadavky na prenos údajov nie je v VU k dispozícii (napr. nie je vložená žiadna karta…).

2.2.3 *Tok správ*

Typický tok správ počas bežného postupu sťahovania údajov je takýto:

IDE		VU
Start Communication Request	⇨ ⇦	Positive Response
Start Diagnostic Service Request	⇨ ⇦	Positive Response
Request Upload	⇨ ⇦	Positive Response

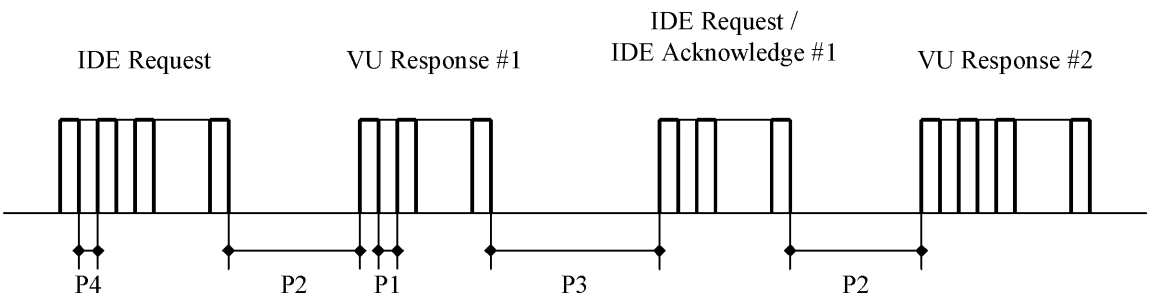
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field<255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Časovanie*

DDP_019 Počas bežnej prevádzky sú príslušné parametre časovania znázornené na tomto obrázku:

Obrázok 1

Tok správ, časovanie



Kľúč:

P1 = čas medzi bajtmi pri odpovedi VU,

P2 = čas medzi koncom požiadavky IDE a začiatkom odpovede VU, alebo medzi koncom potvrdenia IDE a začiatkom ďalšej odpovede VU,

P3 = čas medzi koncom odpovede VU a začiatkom novej požiadavky IDE, alebo medzi koncom odpovede VU a začiatkom potvrdenia IDE, alebo medzi koncom požiadavky IDE a začiatkom novej požiadavky IDE, ak VU neodpovedá,

P4 = čas medzi bajtmi pri požiadavke IDE,

P5 = rozšírená hodnota P3 pre sťahovanie karty.

Povolené hodnoty pre parametre časovania sú uvedené v tejto tabuľke (rozšírený súbor parametrov časovania KWP, použitý v prípade fyzického adresovania pre rýchlejšiu komunikáciu).

Parameter časovania	Hodnota dolného limitu (ms)	Hodnota horného limitu (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minút

(*) Ak VU reaguje prostredníctvom Negative Response, ktorá obsahuje kód, ktorý znamená „požiadavka správne prijatá, odpoveď nasleduje“, táto hodnota sa zvýši na rovnaký horný limit ako P3.

2.2.5 *Spracovanie chýb*

Ak počas výmeny správ nastane chyba, tok správ sa modifikuje v závislosti od zariadenia, na ktorom sa chyba zistila, a od správy, ktorá chybu vyvolala.

Na obrázku 2 a obrázku 3 sú znázornené postupy spracovania chýb pre VU a IDE.

2.2.5.1 Start Communication phase

DDP_020 Ak IDE zistí chybu počas fázy Start communication phase, buď časovaním, alebo prúdom bitov, čaká P3min, kým znovu vydá požiadavku.

DDP_021 Ak VU zistí chybu v sekvencii prichádzajúcej z IDE, nepošle žiadnu odpoveď a čaká na ďalšiu správu Start Communication Request v rámci časového úseku P3max.

2.2.5.2 Communication phase

Je možné vymedziť dve rôzne oblasti spracovania chýb:

1. **VU zistí prenosovú chybu IDE**

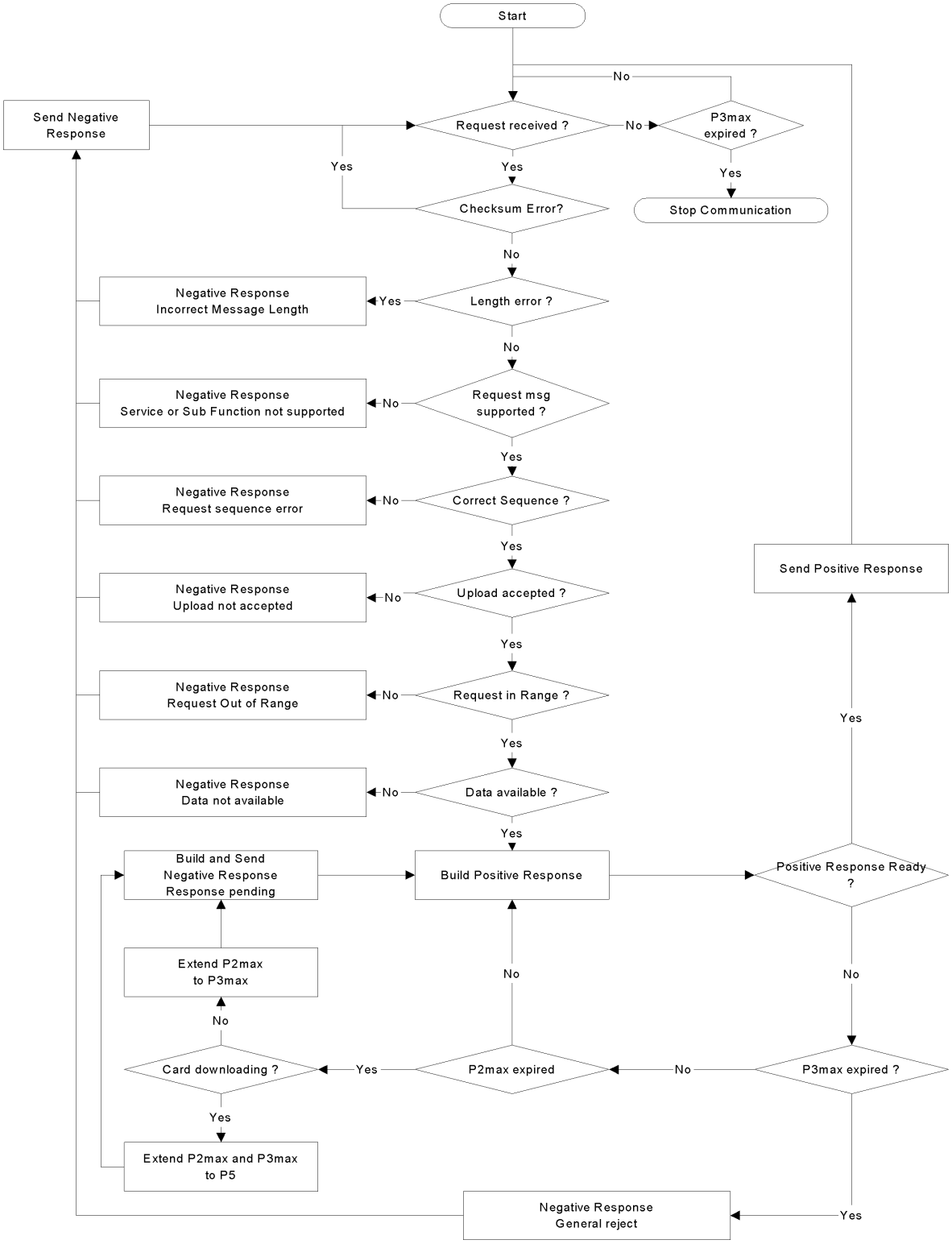
DDP_022 VU zisťuje pri každej prijatej správe chyby časovania, chyby bajtového formátu (napr. poškodenia start a stop bitu) a chyby dátového paketu (chybné číslo prijatých bajtov, chybný bajt kontrolného súčtu).

DDP_023 Ak VU zistí jednu z uvedených chýb, nepošle žiadnu odpoveď a ignoruje prijatú správu.

DDP_024 VU môže zistiť iné chyby vo formáte alebo obsahu prijatej správy (napr. nepodporovaná správa) dokonca aj vtedy, keď správa spĺňa požiadavky na dĺžku a kontrolný súčet. V takom prípade VU odpovedá IDE správou Negative Response, pričom špecifikuje druh chyby

Obrázok 2

Spracovanie chýb na strane VU



2. **Zariadenie IDE zistí chybu prenosu z VU**

DDP_025 Zariadenie IDE zisťuje pri každej prijatej správe chyby časovania, chyby bajtového formátu (napr. poškodenia start a stop bitu) a chyby dátového paketu (chybné číslo prijatých bajtov, chybný bajt kontrolného súčtu).

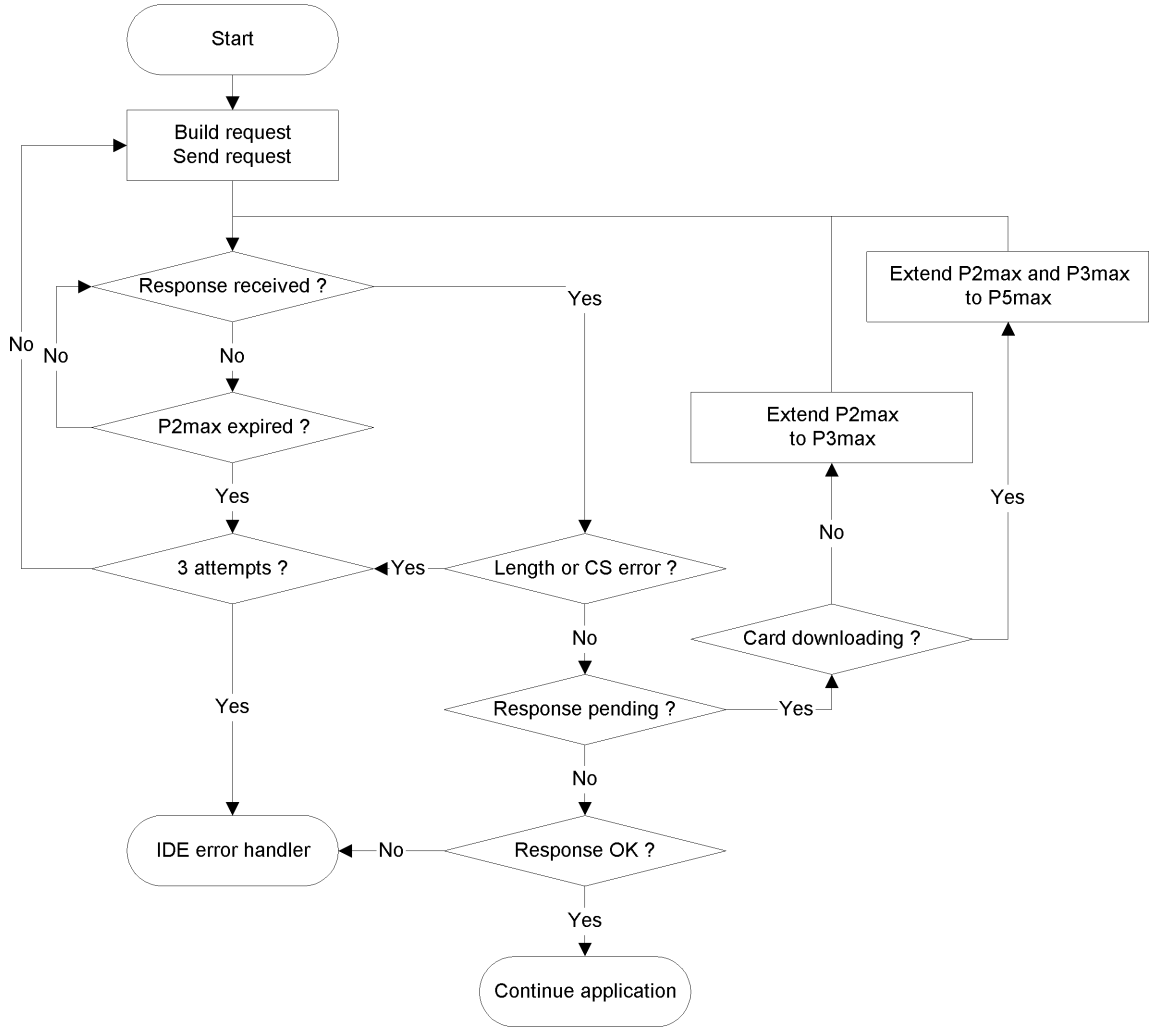
DDP_026 IDE zisťuje sekvenčné chyby, napr. nesprávne zvyšovanie počítadla čiastkovej správy v postupne prijímaných správach.

DDP_027 Ak IDE zistí chybu alebo ak nie je žiadna odpoveď z VU v rámci časového úseku P2max, správa s požiadavkou sa pošle znovu pre celkovo maximálne tri prenosy. Na účely tohto zisťovania chýb sa potvrdenie čiastkovej správy bude považovať za požiadavku na VU.

DDP_028 IDE čaká minimálne P3min pred začiatkom každého prenosu, pričom interval čakania sa meria od posledného vypočítaného výskytu stop bitu po zistení chyby.

Obrázok 3

Spracovanie chýb na strane IDE



2.2.6 *Obsah správy s odpoveďou*

V tomto odseku je špecifikovaný obsah dátových polí rôznych správ s kladnou odpoveďou.

Dátové prvky sú vymedzené v slovníku údajov v dodatku 1.

Poznámka: Pri sťahovaní údajov v prípade tachografov druhej generácie každý dátový prvok najvyššej úrovne predstavuje záznamové pole, aj keď obsahuje iba jeden záznam. Záznamové pole sa začína záhlavím. Toto záhlavie obsahuje typ záznamu, veľkosť záznamu a počet záznamov. Názvy záznamových polí „… RecordArray“ (so záhlavím) sú uvedené v nasledujúcich tabuľkách.

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 Dátové pole správy „Positive Response Transfer Data Overview“ poskytuje tieto údaje v uvedenom poradí, pričom sa použije SID 76 Hex, TREP 01 Hex a primerané rozdelenie a sčítanie čiastkových správ:

Dátová štruktúra prvej generácie

Dátový prvok	Poznámka
MemberStateCertificate VUCertificate	Certifikáty zabezpečenia VU
VehicleIdentificationNumber VehicleRegistrationIdentification	Identifikácia vozidla
CurrentDateTime	Aktuálny dátum a čas VU
VuDownloadablePeriod	Sťahovateľné obdobie
CardSlotsStatus	Typ kariet vložených vo VU
VuDownloadActivityData	Predchádzajúce sťahovanie z VU
VuCompanyLocksData	Všetky uložené podnikové blokovania. Ak je táto časť prázdna, odošle sa iba noOfLocks = 0.
VuControlActivityData	Všetky kontrolné záznamy uložené vo VU. Ak je táto časť prázdna, odošle sa iba noOfControls = 0.
Signature	Podpis RSA všetkých údajov (okrem certifikátov) od prvku VehicleIdentificationNumber po posledný bajt posledného prvku VuControlActivityData.

Dátová štruktúra druhej generácie

Dátový prvok	Poznámka
MemberStateCertificateRecordArray	Certifkát členského štátu
VUCertificateRecordArray	Certifikát VU
VehicleIdentificationNumberRecordArray	Identifikácia vozidla
VehicleRegistrationNumberRecordArray	Registračné číslo vozidla
CurrentDateTimeRecordArray	Aktuálny dátum a čas VU
VuDownloadablePeriodRecordArray	Sťahovateľné obdobie
CardSlotsStatusRecordArray	Typ kariet vložených vo VU
VuDownloadActivityDataRecordArray	Predchádzajúce sťahovanie z VU
VuCompanyLocksRecordArray	Všetky uložené podnikové blokovania. Ak je táto časť prázdna, odošle sa záhlavie poľa s noOfRecords = 0.
VuControlActivityRecordArray	Všetky kontrolné záznamy uložené vo VU. Ak je táto časť prázdna, odošle sa záhlavie poľa s noOfRecords = 0.
SignatureRecordArray	Podpis ECC všetkých predchádzajúcich údajov okrem certifikátov.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 Dátové pole správy „Positive Response Transfer Data Overview“ poskytuje tieto údaje v uvedenom poradí, pričom sa použije SID 76 Hex, TREP 02 Hex a primerané rozdelenie a sčítanie čiastkových správ:

Dátová štruktúra prvej generácie

Dátový prvok	Poznámka
TimeReal	Dátum sťahovaného dňa
OdometerValueMidnight	Počítadlo kilometrov na konci sťahovaného dňa
VuCardIWData	údaje cyklov vkladania a vyberania kariet. — Ak táto časť neobsahuje dostupné údaje, odošle sa iba noOfVuCardIWRecords = 0. — Ak dátový prvok VuCardIWRecord zahŕňa čas 00:00 (vloženie karty v predchádzajúci deň) alebo čas 24:00 (vybratie karty v nasledujúci deň), uvedený bude vcelku v rámci obidvoch príslušných dní.
VuActivityDailyData	Stav slotu v čase 00:00 a zmeny v činnosti zaznamenané počas sťahovaného dňa
VuPlaceDailyWorkPeriodData	údaje súvisiace s miestami zaznamenané počas sťahovaného dňa. Ak je táto časť prázdna, odošle sa iba noOfPlaceRecords = 0.
VuSpecificConditionData	údaje špecifických podmienok zaznamenané počas sťahovaného dňa. Ak je táto časť prázdna, odošle sa iba noOfSpecificConditionRecords = 0.
Signature	Podpis RSA všetkých údajov od prvku TimeReal po posledný bajt posledného záznamu špecifických podmienok.

Dátová štruktúra druhej generácie

Dátový prvok	Poznámka
DateOfDayDownloadedRecordArray	Dátum sťahovaného dňa
OdometerValueMidnightRecordArray	Počítadlo kilometrov na konci sťahovaného dňa
VuCardIWRecordArray	údaje cyklov vkladania a vyberania kariet. — Ak táto časť neobsahuje dostupné údaje, odošle sa záhlavie poľa s noOfRecords = 0. — Ak dátový prvok VuCardIWRecord zahŕňa čas 00:00 (vloženie karty v predchádzajúci deň) alebo čas 24:00 (vybratie karty v nasledujúci deň), uvedený bude celý v rámci obidvoch príslušných dní.
VuActivityDailyRecordArray	Stav slotu v čase 00:00 a zmeny v činnosti zaznamenané počas sťahovaného dňa
VuPlaceDailyWorkPeriodRecordArray	údaje súvisiace s miestami zaznamenané počas sťahovaného dňa. Ak je táto časť prázdna, odošle sa záhlavie poľa s noOfRecords = 0.
VuGNSSCDRecordArray	Polohy vozidla podľa GNSS, ak nepretržitý čas jazdy vodiča dosiahne násobok troch hodín; Ak je táto časť prázdna, odošle sa záhlavie poľa s noOfRecords = 0.
VuSpecificConditionRecordArray	údaje špecifických podmienok zaznamenané počas sťahovaného dňa. Ak je táto časť prázdna, odošle sa záhlavie poľa s noOfRecords = 0.
SignatureRecordArray	Podpis ECC všetkých predchádzajúcich údajov.

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 Dátové pole správy „Positive Response Transfer Data Events and Faults“ poskytuje tieto údaje v uvedenom poradí, pričom sa použije SID 76 Hex, TREP 03 Hex a primerané rozdelenie a sčítanie čiastkových správ:

Dátová štruktúra prvej generácie

Dátový prvok	Poznámka
VuFaultData	Všetky poruchy uložené alebo prebiehajúce vo VU. Ak je táto časť prázdna, odošle sa iba noOfVuFaults = 0.
VuEventData	Všetky udalosti (okrem prekročenia rýchlosti) uložené alebo prebiehajúce vo VU. Ak je táto časť prázdna, odošle sa iba noOfVuEvents = 0.
VuOverSpeedingControlData	údaje súvisiace s poslednou kontrolou prekročenia rýchlosti (predvolená hodnota, ak nie sú k dispozícii žiadne údaje)
VuOverSpeedingEventData	Všetky prípady prekročenia rýchlosti uložené vo VU. Ak je táto časť prázdna, odošle sa iba noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Všetky prípady nastavenia času uložené vo VU (mimo rámca celkovej kalibrácie). Ak je táto časť prázdna, odošle sa iba noOfVuTimeAdjRecords = 0.
Signature	Podpis RSA všetkých údajov od prvku noOfVuFaults po posledný bajt posledného záznamu nastavenia času.

Dátová štruktúra druhej generácie

Dátový prvok	Poznámka
VuFaultRecordArray	Všetky poruchy uložené alebo prebiehajúce vo VU. Ak je táto časť prázdna, odošle sa záhlavie poľa s noOfRecords = 0.
VuEventRecordArray	Všetky udalosti (okrem prekročenia rýchlosti) uložené alebo prebiehajúce vo VU. Ak je táto časť prázdna, odošle sa záhlavie poľa s noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	údaje súvisiace s poslednou kontrolou prekročenia rýchlosti (predvolená hodnota, ak nie sú k dispozícii žiadne údaje)
VuOverSpeedingEventRecordArray	Všetky prípady prekročenia rýchlosti uložené vo VU. Ak je táto časť prázdna, odošle sa záhlavie poľa s noOfRecords = 0.
VuTimeAdjustmentRecordArray	Všetky prípady nastavenia času uložené vo VU (mimo rámca celkovej kalibrácie). Ak je táto časť prázdna, odošle sa záhlavie poľa s noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Podpis ECC všetkých predchádzajúcich údajov.

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 Dátové pole správy „Positive Response Transfer Data Detailed Speed“ poskytuje tieto dáta v uvedenom poradí, pričom sa použije SID 76 Hex, TREP 04 Hex a primerané rozdelenie a sčítanie čiastkových správ:

Dátová štruktúra prvej generácie

Dátový prvok	Poznámka
VuDetailedSpeedData	Všetky podrobné údaje o rýchlosti uložené vo VU (jeden blok rýchlostí za minútu, počas ktorej sa vozidlo pohybovalo) 60 hodnôt rýchlosti za minútu (jedna za sekundu)
Signature	Podpis RSA všetkých údajov od prvku noOfSpeedBlocks po posledný bajt posledného bloku rýchlostí.

Dátová štruktúra druhej generácie

Dátový prvok	Poznámka
VuDetailedSpeedBlockRecordArray	Všetky podrobné údaje o rýchlosti uložené vo VU (jeden blok rýchlostí za minútu, počas ktorej sa vozidlo pohybovalo) 60 hodnôt rýchlosti za minútu (jedna za sekundu)
SignatureRecordArray	Podpis ECC všetkých predchádzajúcich údajov.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 Dátové pole správy „Positive Response Transfer Data Technical Data“ poskytuje tieto údaje v uvedenom poradí, pričom sa použije SID 76 Hex, TREP 05 Hex a primerané rozdelenie a sčítanie čiastkových správ:

Dátová štruktúra prvej generácie

Dátový prvok	Poznámka
VuIdentification	
SensorPaired	
VuCalibrationData	Všetky kalibračné záznamy uložené vo VU.
Signature	Podpis RSA všetkých údajov od prvku vuManufacturerName po posledný bajt posledného prvku VuCalibrationRecord.

Dátová štruktúra druhej generácie

Dátový prvok	Poznámka
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Všetky párovania snímačov pohybu uložené vo VU.
VuSensorExternalGNSSCoupledRecordArray	Všetky spojenia s externými zariadeniami GNSS uložené vo VU
VuCalibrationRecordArray	Všetky kalibračné záznamy uložené vo VU.
VuCardRecordArray	Všetky údaje o vložení karty uložené vo VU.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Podpis ECC všetkých predchádzajúcich údajov.

2.3 **Pamäť ESM**

DDP_034 Ak relácia sťahovania zahŕňa prenos údajov z VU, IDE uloží v rámci jedného fyzického súboru všetky údaje prijaté z VU počas relácie sťahovania v správach Positive Response Transfer Data. Uložené údaje nezahŕňajú záhlavia správ, počítadlá čiastkových správ, prázdne čiastkové správy a kontrolné súčty, ale zahŕňajú SID a TREP (len prvej čiastkovej správy v prípade viacerých čiastkových správ).

3. PROTOKOL SŤAHOVANIA ÚDAJOV Z TACHOGRAFOVÝCH KARIET

3.1 **Rozsah pôsobnosti**

V tomto odseku sa opisuje priame sťahovanie kartových údajov z tachografovej karty na IDE. IDE nie je časťou zabezpečeného prostredia, preto sa nevykonáva žiadna autentifikácia medzi kartou a IDE.

3.2 **Vymedzenie pojmov**

Relácia sťahovania údajov: vždy, keď sa vykoná sťahovanie údajov z karty s integrovaným obvodom (ICC). Relácia obsahuje úplný postup od resetovania ICC prostredníctvom IFD až po deaktiváciu ICC (vytiahnutie karty alebo ďalší reset).

Súbor s podpísanými údajmi: súbor z karty ICC. Súbor sa prenáša na zariadenie IFD v zrozumiteľnom texte. Na ICC sa súbor označí hash kódom, podpíše a podpis sa prenáša na IFD.

3.3 **Sťahovanie údajov z karty**

DDP_035 Sťahovanie údajov z tachografovej karty zahŕňa tieto kroky:

— Sťahovanie spoločných informácií karty v elementárnych súboroch (EF) ICC a IC. Tieto informácie nie sú povinné a nie sú zabezpečené digitálnym podpisom.

— Sťahovanie EF Card_Certificate (alebo CardSignCertificate) a CA_Certificate. Tieto informácie nie sú zabezpečené digitálnym podpisom.

Sťahovanie týchto súborov je povinné pre každú reláciu sťahovania.

— Sťahovanie iných aplikačných dátových EF (v rámci Tachograph DF a Tachograph_G2 DF v prípade potreby) okrem EF Card_Download. Tieto informácie sú zabezpečené digitálnym podpisom.

— Pre každú reláciu sťahovania je povinné stiahnuť prinajmenšom EF Application_Identification a ID.

— Pri sťahovaní údajov z karty vodiča je tiež povinné stiahnuť tieto EF:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- GNSS_Places (ak je relevantné),
- Control_Activity_Data,
- Specific_Conditions.

— Pri sťahovaní údajov z karty vodiča sa aktualizuje dátum LastCardDownload v EF Card_Download.

— Pri sťahovaní údajov z dielenskej karty sa resetuje kalibračné počítadlo v EF Card_Download.

— Pri sťahovaní údajov z dielenskej karty sa nesťahuje EF Sensor_Installation_Data.

3.3.1 *Inicializácia sekvencie*

DDP_036 IDE iniciuje túto sekvenciu:

Karta	Smer	IDE/IFD	Význam/Poznámky
	⇦	Reset hardvéru	
ATR	⇨		

Pomocou voľby parametra protokolu (PPS) sa môže zvoliť vyššia prenosová rýchlosť, pokiaľ to ICC podporuje.

3.3.2 *Sekvencia pre nepodpísané dátové súbory*

DDP_037 Sekvencia pre sťahovanie EF ICC, IC, Card_Certificate (alebo CardSignCertificate) a CA_Certificate je takáto:

Karta	Smer	IDE/IFD	Význam/Poznámky
	⇦	**Select File**	Voľba podľa identifikátorov súboru
OK	⇨		
	⇦	**Read Binary**	Ak súbor obsahuje viac údajov, než je kapacita vyrovnávacej pamäte čítacieho zariadenia alebo karty, príkaz sa musí opakovať, až kým sa nenačíta celý súbor.
File Data **OK**	⇨	Uloženie údajov na externé pamäťové médium (ESM)	Podľa **3.4** (formát dátovej pamäte) Data storage format

Poznámka 1: Pred voľbou EF Card_Certificate (alebo CardSignCertificate) sa musí zvoliť aplikácia tachografu [výber prostredníctvom identifikátora aplikácie (AID)].

Poznámka 2: Výber a čítanie súboru sa môže vykonať aj v rámci jedného kroku použitím príkazu Read Binary s krátkym identifikátorom EF.

3.3.3 *Sekvencia pre podpísané dátové súbory*

DDP_038 Táto sekvencia sa používa pre každý z uvedených súborov, ktoré sa musia sťahovať s podpisom:

Karta	Smer	IDE/IFD	Význam/Poznámky
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	Vypočíta sa hash hodnota celého dátového obsahu zvoleného súboru s použitím predpísaného algoritmu hash v súlade s dodatkom 11. Tento príkaz nie je príkazom ISO.
Vypočíta sa Hash of File a dočasne sa uloží hash hodnota.			
OK	⇨		
	⇦	**Read Binary**	Ak súbor obsahuje viac údajov, než je kapacita vyrovnávacej pamäte čítacieho zariadenia alebo karty, príkaz sa musí opakovať, až kým sa nenačíta celý súbor.
File Data **OK**	⇨	Uloženie údajov na externé pamäťové médium (ESM)	Podľa **3.4** (formát dátovej pamäte) Data storage format
	⇦	**PSO: Compute Digital Signature**	
Vykonanie operácie zabezpečenia „Compute Digital Signature“ pomocou dočasne uloženej hash hodnoty			
Signature **OK**	⇨	Pripojiť údaje k predchádzajúcim údajom uloženým v pamäti ESM	Podľa **3.4** (formát dátovej pamäte) Data storage format

Poznámka: Výber a čítanie súboru sa môže vykonať aj v rámci jedného kroku použitím príkazu Read Binary s krátkym identifikátorom EF. V tomto prípade sa EF môže zvoliť a čítať pred uplatnením príkazu Perform Hash of File.

3.3.4 *Sekvencia pre resetovanie kalibračného počítadla*

DDP_039 Sekvencia pre resetovanie počítadla `NoOfCalibrationsSinceDownload` v EF `Card_Download` na dielenskej karte je takáto:

Karta	Smer	IDE/IFD	Význam/Poznámky
	⇦	**Select File** EF Card_Download	Voľba podľa identifikátorov súboru
OK	⇨		

Karta	Smer	IDE/IFD	Význam/Poznámky
	⇦	**Update Binary** NoOfCalibrationsSince-Download = '00 00'	
Resetovanie počtu sťahovaní z karty			
OK	⇨		

Poznámka: Voľba a aktualizácia súboru sa môže vykonať aj v rámci jedného kroku použitím príkazu Update Binary s krátkym identifikátorom EF.

3.4 Formát dátovej pamäte

3.4.1 *Úvod*

DDP_040 Sťahované údaje sa musia uložiť podľa týchto podmienok:

— údaje sa musia ukladať transparentne. To znamená, že počas uloženia musí byť zachované poradie bajtov, ako aj poradie bitov v rámci bajtu, ktoré sa prenášajú z karty.

— Všetky súbory sťahované z karty počas relácie sťahovania sú uložené v jednom súbore v pamäti ESM.

3.4.2 *Formát súboru*

DDP_041 Formát súboru je zreťazením viacerých objektov hodnoty dĺžky tagu (TLV).

DDP_042 Tag pre EF je identifikátor súboru (FID) spolu s dodatkom „00“.

DDP_043 Tag podpisu EF je FID súboru spolu s dodatkom „01“.

DDP_044 Dĺžka je dvojbajtová hodnota. Hodnota stanovuje počet bajtov v hodnotovom poli. Hodnota „FF FF“ v dĺžkovom poli je vyhradená na budúce použitie.

DDP_045 Ak sa súbor nesťahuje, nič z toho, čo sa vzťahuje k súboru, sa nemusí ukladať (žiadny tag a žiadna nulová dĺžka).

DDP_046 Podpis sa ukladá ako ďalší objekt TLV bezprostredne za objektom TLV, ktorý obsahuje údaje súboru.

Definícia	Význam	Dĺžka
FID (2 bajty) || „00“	Tag pre EF (FID)	3 bajtov
FID (2 bajty) || „01“	Tag pre podpis EF(FID)	3 bajtov
xx xx	Dĺžka hodnotového poľa	2 bajtov

Príklad údajov v sťahovanom súbore v ESM:

Tag	Dĺžka	Hodnota
00 02 00	00 11	údaje EF ICC
C1 00 00	00 C2	údaje EF Card_Certificate
		…
05 05 00	0A 2E	údaje EF Vehicles_Used
05 05 01	00 80	Podpis EF Vehicles_Used

4. SŤAHOVANIE ÚDAJOV Z TACHOGRAFOVEJ KARTY CEZ JEDNOTKU VOZIDLA

DDP_047 VU musí umožniť stiahnutie obsahu karty vodiča vloženej do pripojeného IDE.

DDP_048 IDE pošle správu „Transfer Data Request Card Download“ na VU, aby sa začal tento režim (pozri 2.2.2.9).

DDP_049 VU potom stiahne celú kartu súbor po súbore, v súlade s protokolom sťahovania karty vymedzeným v odseku 3, a odošle všetky údaje prijaté z karty na IDE v rámci vhodného TLV formátu súboru (pozri 3.4.2) a uzavrie ich v správe „Positive Response Transfer Data“.

DDP_050 IDE vyvolá dáta karty zo správy „Positive Response Transfer Data“ (s vynechaním všetkých záhlaví, SID, TREP, počítadiel čiastkových správ a kontrolných súčtov) a uloží ich v jednom fyzickom súbore opísanom v odseku 2.3.

DDP_051 VU potom prípadne aktualizuje súbor `Control_Activity_Data` alebo `Card_Download` karty vodiča.

Dodatok 8

KALIBRAČNÝ PROTOKOL

OBSAH

1. ÚVOD 283
2. POJMY, VYMEDZENIE POJMOV A REFERENČNÉ DOKUMENTY 283
3. PREHĽAD SLUŽIEB 284
3.1. Dostupné služby 284
3.2. Kódy odpovedí 285
4. KOMUNIKAČNÉ SLUŽBY 285
4.1. Služba StartCommunication 285
4.2. Služba StopCommunication 287
4.2.1 Opis správy 287
4.2.2 Formát správy 288
4.2.3 Vymedzenie parametrov 289
4.3. Služba TesterPresent 289
4.3.1 Opis správy 289
4.3.2 Formát správy 289
5. RIADIACE SLUŽBY 291
5.1. Služba StartDiagnosticSession 291
5.1.1 Opis správy 291
5.1.2 Formát správy 292
5.1.3 Vymedzenie parametrov 293
5.2. Služba SecurityAccess 294
5.2.1 Opis správy 294
5.2.2 Formát správy – SecurityAccess – requestSeed 295
5.2.3 Formát správy – SecurityAccess – sendKey 296
6. SLUŽBY PRENOSU ÚDAJOV 297
6.1. Služba ReadDataByIdentifier 298
6.1.1 Opis správy 298
6.1.2 Formát správy 298
6.1.3 Vymedzenie parametrov 299
6.2. Služba WriteDataByIdentifier 300
6.2.1 Opis správy 300
6.2.2 Formát správy 300
6.2.3 Vymedzenie parametrov 302

7. KONTROLA SKÚŠOBNÝCH IMPULZOV – KONTROLA VSTUPU/VÝSTUPU FUNKČNEJ JEDNOTKY 302

7.1. Služba InputOutputControlByIdentifier 302

7.1.1 Opis správy 302

7.1.2 Formát správy 303

7.1.3 Vymedzenie parametrov 304

8. FORMÁTY DATARECORDS 305

8.1. Rozsahy hodnôt prenášaných parametrov 305

8.2. Formáty dataRecords 306

1. ÚVOD

Tento dodatok opisuje výmenu údajov medzi jednotkou vozidla a skúšobným zariadením cez K-vedenie, ktoré tvorí časť kalibračného rozhrania opísaného v dodatku 6. Opisuje aj riadenie vstupného/výstupného signalizačného vedenia na kalibračnom konektore.

Nadviazanie komunikácie cez K-vedenie je opísané v oddiele 4 „Komunikačné služby“ (Communication Services).

V tomto dodatku sa používa koncepcia diagnostických „relácií“ na stanovenie rozsahu riadenia K-vedenia v rôznych podmienkach. Štandardná relácia je „StandardDiagnosticSession“, keď môžu byť všetky údaje prečítané z jednotky vozidla, no žiadne údaje nemôžu byť do nej zapísané.

Voľba diagnostickej relácie je opísaná v oddiele 5 „Riadiace služby“ (Management Services).

Tento dodatok sa musí považovať za relevantný pre obidve generácie VU a dielenských kariet v súlade s požiadavkami interoperability uvedenými v tomto nariadení.

CPR_001 „ECUProgrammingSession“ umožňuje zápis údajov do jednotky vozidla. V prípade zápisu kalibračných údajov musí byť jednotka vozidla navyše v režime prevádzky KALIBRÁCIA.

Prenos údajov cez K-vedenie je opísaný v oddiele 6 „Služby prenosu údajov“ (Data Transmission Services). Formáty prenášaných údajov sú podrobne opísané v oddiele 8 „dataRecords formats“.

CPR_002 „ECUAdjustmentSession“ umožňuje voľbu vstupného/výstupného režimu kalibrácie vstupného/výstupného signalizačného vedenia cez rozhranie K-vedenia. Riadenie kalibrácie vstupného/výstupného signalizačného vedenia je opísané v oddiele 7 „Kontrola skúšobných impulzov – kontrola vstupu/výstupu funkčnej jednotky“ Control of Test Pulses – Input/Output Control functional unit.

CPR_003 V tomto dokumente sa ako adresa skúšobného zariadenia používa „tt“. Bez ohľadu na to, že sa môžu používať prioritné adresy pre skúšobné zariadenia, VU musí správne odpovedať na každú adresu skúšobného zariadenia. Fyzická adresa VU je 0xEE.

2. POJMY, VYMEDZENIE POJMOV A REFERENČNÉ DOKUMENTY

Protokoly, správy a chybové kódy sú v zásade založené na návrhu normy ISO 14229-1 (Cestné vozidlá. Diagnostické systémy. Časť 1: Diagnostické služby, verzia 6 z 22. februára 2001).

Kódovanie bajtov a hexadecimálne hodnoty sa používajú pre identifikátory služby, požiadavky a odpovede vzťahujúce sa na službu a pre štandardné parametre.

Pojem „skúšobné zariadenie“ sa vzťahuje na zariadenie používané na zápis programovacích/kalibračných údajov do VU.

Pojem „klient“ a „server“ sa vzťahuje na skúšobné zariadenie, resp. na VU.

Pojem ECU znamená „elektronická riadiaca jednotka“ a vzťahuje sa na VU.

Referenčné dokumenty:

ISO 14230-2: Cestné vozidlá.Diagnostické systémy. Protokol kľúčového slova 2000. Časť 2: Vrstva údajového spojenia.

Prvé vydanie: 1999.

Vozidlá – Diagnostika.

3. PREHĽAD SLUŽIEB

3.1. **Dostupné služby**

Táto tabuľka poskytuje prehľad o službách, ktoré sú k dispozícii v tachografe a sú definované v tomto dokumente.

CPR_004 V tabuľke sú uvedené služby, ktoré sú k dispozícii pri aktivovanej diagnostickej relácii.

— V **prvom stĺpci** sú uvedené služby, ktoré sú k dispozícii.

— V **druhom stĺpci** je uvedené číslo oddielu v tomto dodatku, v ktorom sú služby vymedzené podrobnejšie.

— V **treťom stĺpci** sa priraďujú hodnoty identifikátora služby pre správy s požiadavkou.

— V **štvrtom stĺpci** sa špecifikujú služby**„StandardDiagnosticSession“ (SD)**, ktoré sa musia implementovať do každej VU.

— V **piatom stĺpci** sa špecifikujú služby **„ECUAdjustmentSession“ (ECUAS)**, ktoré sa musia implementovať, aby bola možná kontrola vstupného/výstupného signalizačného vedenia v kalibračnom konektore predného panelu VU.

— V **šiestom stĺpci** sa špecifikujú služby **„ECUProgrammingSession“ (ECUPS)**, ktoré sa musia implementovať, aby bolo možné programovanie parametrov do VU.

Tabuľka 1

Prehľad o hodnotách identifikátora služby

			Diagnostické relácie		
Názov diagnostickej služby	Oddiel č.	Hodnota SId (identifikátor služby) požiadavky	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		■	

■ Tento symbol znamená, že v tejto diagnostickej relácii je služba povinná.

Žiadny symbol znamená, že v tejto diagnostickej relácii nie je služba povolená.

3.2. **Kódy odpovedí**

Kódy odpovedí sú vymedzené pre každú službu.

4. KOMUNIKAČNÉ SLUŽBY

Niektoré služby sú nevyhnutné na nadviazanie a udržanie komunikácie. Nezobrazujú sa na aplikačnej úrovni. Dostupné služby sú uvedené v tejto tabuľke:

Tabuľka 2

Komunikačné služby

Názov služby	Opis
StartCommunication	Klient žiada začatie komunikačnej relácie so serverom(-mi).
StopCommunication	Klient žiada skončenie prebiehajúcej komunikačnej relácie.
TesterPresent	Klient oznamuje serveru, že spojenie je ešte stále aktívne.

CPR_005 Služba StartCommunication sa používa na začatie komunikácie. Na vykonanie každej služby sa musí začať komunikácia a komunikačné parametre musia zodpovedať požadovanému režimu.

4.1. **Služba StartCommunication**

CPR_006 Po prijatí indikačného prvku StartCommunication VU musí skontrolovať, či môže byť za súčasných podmienok inicializované požadované komunikačné spojenie. Platné podmienky pre začatie komunikačného spojenia sú opísané v dokumente ISO 14230-2.

CPR_007 Potom VU musí vykonať všetky činnosti potrebné na inicializovanie komunikačného spojenia a pošle odpovedací prvok StartCommunication so zvolenými parametrami kladnej odpovede.

CPR_008 Ak VU, ktorá je už inicializovaná (a vstúpila do diagnostickej relácie) prijme novú požiadavku StartCommunication (napr. na základe opravy chyby v skúšobnom zariadení), požiadavka sa prijme a VU sa musí znovu inicializovať.

CPR_009 Ak komunikačné spojenie nemôže byť inicializované z akýchkoľvek dôvodov, VU musí pokračovať v činnosti, ktorá bezprostredne predchádzala pokusu o začatie komunikačného spojenia.

CPR_010 Správa s požiadavkou StartCommunication musí byť fyzicky adresovaná.

CPR_011 Inicializácia VU pre služby sa vykoná pomocou metódy „rýchla inicializácia“:

— každej aktivite predchádza pokojový stav zbernice,

— skúšobné zariadenie potom odošle inicializačnú sekvenciu,

— všetky informácie, ktoré sú potrebné na nadviazanie komunikácie, sú obsiahnuté v odpovedi VU.

CPR_012 Po dokončení inicializácie:

— všetky komunikačné parametre sa nastavia na hodnoty definované v tabuľke 4 podľa kľúčových bajtov,

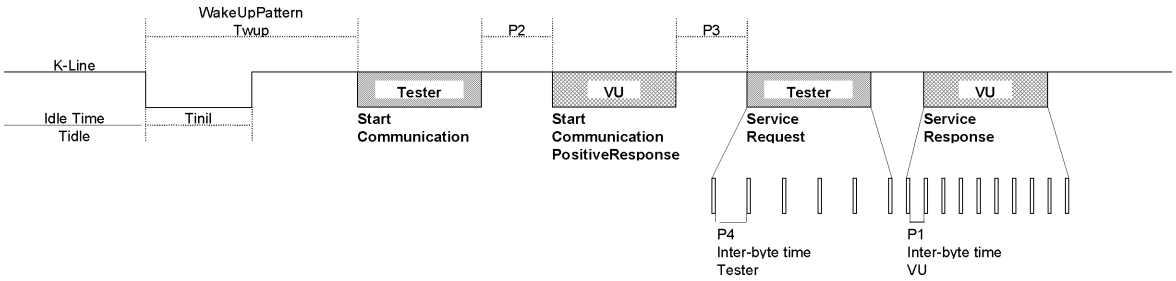
— VU čaká na prvú požiadavku skúšobného zariadenia,

— VU je v štandardnom diagnostickom režime, t. j. StandardDiagnosticSession,

— kalibračné vstupné/výstupné signalizačné vedenie je v štandardnom stave, t. j. v deaktivovanom stave.

CPR_014 Rýchlosť prenosu údajov na K-vedení je 10 400 baudov.

CPR_016 Rýchlu inicializáciu začne skúšobné zariadenie prenášajúce sekvenciu Wake up pattern (Wup) na K-vedení. Začína po pokojovom stave K-vedenia s krátkym časom Tinil. Skúšobné zariadenie prenáša prvý bit služby StartCommunication po čase Twup, ktorý začína po prvej klesajúcej hrane signálu.



CPR_017 Hodnoty časovania pre rýchlu inicializáciu a komunikácie vo všeobecnosti sú uvedené v tabuľkách ďalej. Pre pokojový stav existujú rôzne možnosti:

— prvý prenos po zapnutí, Tidle = 300 ms,

— po dokončení služby StopCommunication, Tidle = P3 min,

— po skončení komunikácie prekročením času P3 max, Tidle = 0.

Tabuľka 3

Hodnoty časovania pre rýchlu inicializáciu

Parameter		Min. hodnota	Max. hodnota
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabuľka 4

Hodnoty časovania komunikácie

Časovanie Parameter	Opis parametra	Dolné limitné hodnoty [ms]	Horné limitné hodnoty [ms]
		min.	max.
P1	Čas medzi bajtmi pre odpoveď VU	0	20
P2	Čas medzi požiadavkou skúšobného zariadenia a odpoveďou VU alebo dvomi odpoveďami VU	25	250
P3	Čas medzi skončením odpovedí VU a začiatkom novej požiadavky skúšobného zariadenia	55	5 000
P4	Čas medzi bajtmi pre požiadavku skúšobného zariadenia	5	20

CPR_018 Formát správy pre rýchlu inicializáciu je podrobne uvedený v ďalej uvedených tabuľkách. (POZNÁMKA: Hex znamená v hexadecimálnom vyjadrení)

Tabuľka 5

Správa StartCommunication Request

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	81	FMT
#2	Bajt cieľovej adresy	EE	TGT
#3	Bajt zdrojovej adresy	tt	SRC
#4	**StartCommunication Request Service Id**	**81**	**SCR**
#5	Kontrolný súčet	00-FF	CS

Tabuľka 6

Správa StartCommunication Positive Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	03	LEN
#5	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
#6	Kľúčový bajt 1	EA	KB1
#7	Kľúčový bajt 2	8F	KB2
#8	Kontrolný súčet	00-FF	CS

CPR_019 Nie je žiadna záporná odpoveď na správu StartCommunication Request; ak nie je žiadna správa s kladnou odpoveďou, ktorá sa má prenášať, potom VU nie je inicializovaná, nič sa neprenáša a VU zostáva vo svojej normálnej prevádzke.

4.2. **Služba StopCommunication**

4.2.1 *Opis správy*

Účelom tejto služby komunikačnej úrovne je ukončiť komunikačnú reláciu.

CPR_020 Po prijatí indikačného prvku StopCommunication musí VU skontrolovať, či súčasné podmienky dovoľujú ukončiť komunikáciu. Ak tomu tak je, VU musí vykonať všetky činnosti potrebné na ukončenie komunikácie.

CPR_021 Ak je možné ukončiť komunikáciu, VU musí pre ukončením komunikácie vydať odpovedací prvok StopCommunication so zvolenými parametrami kladnej odpovede.

CPR_022 Ak komunikácia nemôže byť ukončená z akéhokoľvek dôvodu, VU musí vydať odpovedací prvok StopCommunication so zvolenými parametrami zápornej odpovede.

CPR_023 Ak VU zistí prekročenie času P3max, komunikácia sa ukončí bez toho, aby bol vydaný akýkoľvek odpovedací prvok.

4.2.2 *Formát správy*

CPR_024 Formáty správ pre prvky StopCommunication sú uvedené v týchto tabuľkách:

Tabuľka 7

Správa StopCommunication Request

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	EE	TGT
#3	Bajt zdrojovej adresy	tt	SRC
#4	Bajt doplnkovej dĺžky	01	LEN
#5	**StopCommunication Request Service Id**	**82**	**SPR**
#6	Kontrolný súčet	00-FF	CS

Tabuľka 8

Správa StopCommunication Positive Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Kontrolný súčet	00-FF	CS

Tabuľka 9

Správa StopCommunication Negative Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	StopCommunication Request Service Identification	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Kontrolný súčet	00-FF	CS

4.2.3 *Vymedzenie parametrov*

Táto služba si nevyžaduje žiadne vymedzenie parametrov.

4.3. **Služba TesterPresent**

4.3.1 *Opis správy*

Službu TesterPresent používa skúšobné zariadenie na oznámenie svojej prítomnosti serveru, aby zabránilo serveru v automatickom návrate do normálnej prevádzky a prípadnému zastaveniu komunikácie. Táto služba pravidelne posiela požiadavku, aby sa zostala aktívna diagnostická relácia alebo komunikácia tým, že resetuje časovač P3 vždy, keď sa prijme požiadavka na túto službu.

4.3.2 *Formát správy*

CPR_079 Formáty správ pre prvky TesterPresent sú podrobne uvedené v týchto tabuľkách:

Tabuľka 10

Správa TesterPresent Request

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	EE	TGT
#3	Bajt zdrojovej adresy	tt	SRC
#4	Bajt doplnkovej dĺžky	02	LEN
#5	**TesterPresent Request Service Id**	**3E**	**TP**

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#6	Sub Function = responseRequired = [áno	01	RESPREQ_Y
	nie]	02	RESPREQ_NO
#7	Kontrolný súčet	00-FF	CS

CPR_080 Ak je parameter responseRequired nastavený na „áno“, potom server musí odpovedať touto správou s kladnou odpoveďou. Ak je nastavený na „nie“, server neposiela žiadnu odpoveď.

Tabuľka 11

Správa TesterPresent Positive Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Kontrolný súčet	00-FF	CS

CPR_081 Služba musí podporovať tieto kódy záporných odpovedí:

Tabuľka 12

Správa TesterPresent Negative Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	TesterPresent Request Service Identification	3E	TP

Bajt #	Názov parametra		Hexadecimálna hodnota	Mnemotechnická skratka
#7	responseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Kontrolný súčet		00-FF	CS

5. RIADIACE SLUŽBY

Dostupné služby sú uvedené v tejto tabuľke:

Tabuľka 13

Riadiace služby

Názov služby	Opis
StartDiagnosticSession	Klient žiada o začatie diagnostickej relácie s VU.
SecurityAccess	Klient žiada o prístup k funkciám vyhradeným pre oprávnených používateľov.

5.1. **Služba StartDiagnosticSession**

5.1.1 *Opis správy*

CPR_025 Služba StartDiagnosticSession sa používa na to, aby sa mohli v serveri aktivovať rôzne diagnostické relácie. Diagnostická relácia umožňuje aktivovať špecifický súbor služieb podľa tabuľky 17. Relácia môže aktivovať špecifické služby výrobcu vozidla, ktoré nie sú súčasťou tohto dokumentu. Implementačné pravidlá musia byť v súlade s týmito požiadavkami:

— vo VU je aktívna vždy len jedna diagnostická relácia,

— VU musí začať StandardDiagnosticSession pri každom zapnutí. Ak sa nezačne žiadna iná diagnostická relácia, potom StandardDiagnosticSession pokračuje tak dlho, ako dlho je zapnutá VU,

— ak si diagnostickú reláciu, ktorá už prebieha, vyžiadalo skúšobné zariadenie, potom VU musí poslať správu s kladnou odpoveďou,

— kedykoľvek skúšobné zariadenie požiada o novú diagnostickú reláciu, VU musí najprv poslať správu s kladnou odpoveďou na StartDiagnosticSession predtým, než sa aktivuje vo VU nová relácia. Ak VU nemôže začať požadovanú novú diagnostickú reláciu, potom musí odpovedať správou so zápornou odpoveďou na StartDiagnosticSession a pokračuje prebiehajúca relácia.

CPR_026 Diagnostická relácia sa môže začať len vtedy, keď bola medzi klientom a VU nadviazaná komunikácia.

CPR_027 Po úspešnej StartDiagnosticSession musia byť parametre časovania definované v tabuľke 4 aktívne, pričom je parameter diagnosticSession v správe s požiadavkou nastavený na „StandardDiagnosticSession“, ak bola predtým aktivovaná iná diagnostická relácia.

5.1.2 *Formát správy*

CPR_028 Formáty správ pre prvky StartDiagnosticSession sú podrobne uvedené v týchto tabuľkách:

Tabuľka 14

Správa StartDiagnosticSession Request

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	EE	TGT
#3	Bajt zdrojovej adresy	tt	SRC
#4	Bajt doplnkovej dĺžky	02	LEN
#5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
#6	diagnosticSession = [jedna hodnota z tabuľky 17]	xx	DS_…
#7	Kontrolný súčet	00-FF	CS

Tabuľka 15

Správa StartDiagnosticSession Positive Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	diagnosticSession = [rovnaká hodnota ako v bajte # 6 tabuľky 14]	xx	DS_…
#7	Kontrolný súčet	00-FF	CS

Tabuľka 16

Správa StartDiagnosticSession Negative Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT

Bajt #	Názov parametra		Hexadecimálna hodnota	Mnemotechnická skratka
#3	Bajt zdrojovej adresy		EE	SRC
#4	Bajt doplnkovej dĺžky		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	Kontrolný súčet		00-FF	CS

(a) – Hodnota vložená do bajtu # 6 správy s požiadavkou sa nepodporuje, t. j. nie je v tabuľke 17.
(b) – Dĺžka správy nie je správna.
(c) – Kritériá pre požiadavku StartDiagnosticSession nie sú splnené.

5.1.3 *Vymedzenie parametrov*

CPR_029 Parameter ***diagnosticSession (DS_)*** používa služba StartDiagnosticSession na voľbu špecifického správania servera(-ov). V tomto dokumente sú špecifikované tieto diagnostické relácie:

Tabuľka 17

Vymedzenie hodnôt diagnosticSession

Hex	Opis	Mnemotechnická skratka
81	**StandardDiagnosticSession** Táto diagnostická relácia umožňuje všetky služby špecifikované v **tabuľke 1 v stĺpci 4 „SD“**. Tieto služby umožňujú čítanie údajov zo servera (VU). Táto diagnostická relácia je aktívna po úspešne dokončenej inicializácii medzi klientom (skúšobným zariadením) a serverom (VU). Táto diagnostická relácia môže byť prepísaná inými diagnostickými reláciami špecifikovanými v tomto oddiele.	**SD**
85	**ECUProgrammingSession** Táto diagnostická relácia umožňuje všetky služby špecifikované v **tabuľke 1 v stĺpci 6 „ECUPS“**. Tieto služby podporujú programovanie pamäti servera (VU). Táto diagnostická relácia môže byť prepísaná inými diagnostickými reláciami špecifikovanými v tomto oddiele.	**ECUPS**
87	**ECUAdjustmentSession** Táto diagnostická relácia umožňuje všetky služby špecifikované v **tabuľke 1 v stĺpci 5 „ECUAS“.** Tieto služby podporujú riadenie vstupov/výstupov servera (VU). Táto diagnostická relácia môže byť prepísaná inými diagnostickými reláciami špecifikovanými v tomto oddiele.	**ECUAS**

5.2. **Služba SecurityAccess**

Zapisovanie kalibračných údajov nie je možné, pokiaľ VU nie je v režime KALIBRÁCIE. Okrem vloženia platnej dielenskej karty do VU je potrebné zapísať správny PIN do VU predtým, než je udelený prístup k režimu KALIBRÁCIE.

Ak je VU v režime KALIBRÁCIE alebo KONTROLY, prístup ku kalibračnému vstupnému/výstupnému vedeniu je tiež možný.

Služba SecurityAccess poskytuje možnosť zápisu PIN a oznámenia skúšobnému zariadeniu, či VU je alebo nie je v režime KALIBRÁCIE.

Pripúšťa sa zápis PIN alternatívnymi metódami.

5.2.1 *Opis správy*

Služba SecurityAccess obsahuje správu SecurityAccess „requestSeed-“, za ktorou prípadne nasleduje správa SecurityAccess „sendKey“. Služba SecurityAccess sa musí vykonať po službe StartDiagnosticSession.

CPR_033 Skúšobné zariadenie musí použiť správu SecurityAccess „requestSeed“ na kontrolu, či je jednotka vozidla pripravená akceptovať PIN.

CPR_034 Ak je jednotka vozidla už v režime KALIBRÁCIE, musí odpovedať na požiadavku odoslaním „seed“ 0x0000 pomocou služby SecurityAccess Positive Response.

CPR_035 Ak je jednotka vozidla pripravená akceptovať PIN na overenie dielenskou kartou, musí na požiadavku odpovedať odoslaním „seed“ väčším než 0x0000 pomocou služby SecurityAccess Positive Response.

CPR_036 Ak nie je jednotka vozidla pripravená akceptovať PIN zo skúšobného zariadenia, buď z dôvodu neplatnosti vloženej dielenskej karty, alebo preto, že nebola vložená žiadna dielenská karta, alebo preto, že jednotka vozidla očakáva vloženie PIN inou metódou, musí na požiadavku odpovedať zápornou odpoveďou s kódom odpovede nastaveným na conditionsNotCorrectOrRequestSequenceError.

CPR_037 Skúšobné zariadenie potom prípadne použije správu SecurityAccess „sendKey“ na odoslanie PIN jednotke vozidla. Aby bol dostatok času na uskutočnenie procesu autentifikácie karty, VU musí použiť záporný kód odpovede requestCorrectlyReceived-ResponsePending na predĺženie času na odpoveď. Avšak maximálny čas na odpoveď nesmie prekročiť 5 minút. Ihneď po dokončení požadovanej služby musí VU odoslať správu s kladnou alebo zápornou odpoveďou s iným kódom odpovede, než je tento. Záporný kód odpovede requestCorrectlyReceived-ResponsePending môže VU opakovať, až kým nie je požadovaná služba dokončená a nie je poslaná konečná správa s odpoveďou.

CPR_038 Jednotka vozidla môže odpovedať na túto správu pomocou služby SecurityAccess Positive Response len vtedy, keď je v režime KALIBRÁCIE.

CPR_039 V nasledujúcich prípadoch musí jednotka vozidla odpovedať na túto požiadavku zápornou odpoveďou s takto nastaveným kódom odpovede:

— subFunctionNot supported: neplatný formát pre parameter subfunkcie (accessType),

— conditionsNotCorrectOrRequestSequenceError: jednotka vozidla nie je pripravená akceptovať zápis PIN,

— invalidKey: PIN je neplatné a počet pokusov o kontrolu PIN sa neprekročil,

— exceededNumberOfAttempts: PIN je neplatné a počet pokusov o kontrolu PIN sa prekročil,

— generalReject: správne PIN, no vzájomná autentifikácia s dielenskou kartou zlyhala.

5.2.2 *Formát správy – SecurityAccess – requestSeed*

CPR_040 Formáty správ pre prvky SecurityAccess „requestSeed“ sú podrobne uvedené v týchto tabuľkách:

Tabuľka 18

Správa SecurityAccess Request- requestSeed

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	EE	TGT
#3	Bajt zdrojovej adresy	tt	SRC
#4	Bajt doplnkovej dĺžky	02	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Kontrolný súčet	00-FF	CS

Tabuľka 19

Správa SecurityAccess – requestSeed Positive Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	04	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	Seed High	00-FF	SEEDH
#8	Seed Low	00-FF	SEEDL
#9	Kontrolný súčet	00-FF	CS

Tabuľka 20

Správa SecurityAccess Negative Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#4	Bajt doplnkovej dĺžky	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	Kontrolný súčet	00-FF	CS

5.2.3 *Formát správy – SecurityAccess – sendKey*

CPR_041 Formáty správ pre prvky SecurityAccess „sendKey“ sú uvedené v týchto tabuľkách:

Tabuľka 21

Správa SecurityAccess Request – sendKey

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	EE	TGT
#3	Bajt zdrojovej adresy	tt	SRC
#4	Bajt doplnkovej dĺžky	m+2	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7 až #m +6	Kľúč #1 (High) … Kľúč #m (low, m musí mať hodnoty minimálne 4 a maximálne 8)	xx … xx	KEY
#m+7	Kontrolný súčet	00-FF	CS

Tabuľka 22

Správa SecurityAccess – sendKey Positive Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#4	Bajt doplnkovej dĺžky	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Kontrolný súčet	00-FF	CS

Tabuľka 23

Správa SecurityAccess Negative Response

Bajt #	Názov parametra		Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie		80	FMT
#2	Bajt cieľovej adresy		tt	TGT
#3	Bajt zdrojovej adresy		EE	SRC
#4	Bajt doplnkovej dĺžky		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	Kontrolný súčet		00-FF	CS

6. SLUŽBY PRENOSU ÚDAJOV

Dostupné služby sú uvedené v tejto tabuľke:

Tabuľka 24

Služby prenosu údajov

Názov služby	Opis
ReadDataByIdentifier	Klient žiada prenos aktuálnej hodnoty záznamu pomocou prístupu prostredníctvom recordDataIdentifier.
WriteDataByIdentifier	Klient žiada zapísať záznam sprístupnený pomocou recordDataIdentifier.

6.1. **Služba ReadDataByIdentifier**

6.1.1 *Opis správy*

CPR_050 Službu ReadDataByIdentifier používa klient na vyžiadanie hodnôt dátového záznamu zo servera. Údaje sa identifikujú pomocou recordDataIdentifier. Výrobca VU je zodpovedný za to, aby boli pri vykonávaní tejto služby splnené podmienky servera.

6.1.2 *Formát správy*

CPR_051 Formáty správ pre prvky ReadDataByIdentifier sú uvedené v týchto tabuľkách:

Tabuľka 25

Správa ReadDataByIdentifier Request

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	EE	TGT
#3	Bajt zdrojovej adresy	tt	SRC
#4	Bajt doplnkovej dĺžky	03	LEN
#5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
#6 až #7	recordDataIdentifier = [hodnota z tabuľky 28]	xxxx	RDI_…
#8	Kontrolný súčet	00-FF	CS

Tabuľka 26

Správa ReadDataByIdentifier Positive Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	m+3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 a #7	recordDataIdentifier = [the same value as bytes #6 and #7 tabuľky 25]	xxxx	RDI_…
#8 až #m +7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrolný súčet	00-FF	CS

Tabuľka 27

Správa ReadDataByIdentifier Negative Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	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	Kontrolný súčet	00-FF	CS

6.1.3 *Vymedzenie parametrov*

CPR_052 Parameter ***recordDataIdentifier (RDI_)*** v správe s požiadavkou ReadDataByIdentifier identifikuje dátový záznam.

CPR_053 Hodnoty recordDataIdentifier definované v tomto dokumente sú uvedené v tabuľke ďalej.

Tabuľka recordDataIdentifier sa skladá zo štyroch stĺpcov a viacerých riadkov.

— **Prvý stĺpec (Hex)** obsahuje „hexadecimálne hodnoty“ priradené k recordDataIdentifier špecifikovanému v treťom stĺpci.

— **V druhom stĺpci (Dátový prvok)** sa špecifikuje dátový prvok dodatku 1, na ktorom je založený recordDataIdentifier (niekedy je potrebné prekódovanie).

— **Tretí stĺpec (Opis)** obsahuje zodpovedajúci názov recordDataIdentifier.

— **Štvrtý stĺpec (Mnemotechnická skratka)** špecifikuje mnemotechnickú skratku tohto recordDataIdentifier.

Tabuľka 28

Vymedzenie hodnôt recordDataIdentifier

Hex	Dátový prvok	Názov recordDataIdentifier (pozri formát v oddiele 8.2)	Mnemotechnická skratka
F90B	`CurrentDateTime`	TimeDate	RDI_TD
F912	`HighResOdometer`	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	`K-ConstantOfRecordingEquipment`	Kfactor	RDI_KF

Hex	Dátový prvok	Názov recordDataIdentifier (pozri formát v oddiele 8.2)	Mnemotechnická skratka
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 Parameter ***dataRecord (DREC_)*** používa správa s kladnou odpoveďou na ReadDataByIdentifier na to, aby poskytla klientovi (skúšobnému zariadeniu) hodnotu dátového záznamu identifikovaného pomocou recordDataIdentifier. Dátové formáty sú špecifikované v oddiele 8. Môžu sa implementovať ďalšie dataRecords, ktoré si môže zvoliť používateľ, vrátane špecifických vstupných, interných a výstupných údajov VU, ktoré však v tomto dokumente nie sú definované.

6.2. **Služba WriteDataByIdentifier**

6.2.1 *Opis správy*

CPR_056 Službu WriteDataByIdentifier používa klient na zapísanie hodnôt dátového záznamu na server. Údaje sa identifikujú pomocou recordDataIdentifier. Výrobca VU je zodpovedný za to, aby boli pri vykonávaní tejto služby splnené podmienky servera. Na aktualizáciu parametrov uvedených v tabuľke 28 musí byť VU v režime KALIBRÁCIE.

6.2.2 *Formát správy*

CPR_057 Formáty správ pre prvky WriteDataByIdentifier sú uvedené v týchto tabuľkách:

Tabuľka 29

Správa WriteDataByIdentifier Request

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	EE	TGT
#3	Bajt zdrojovej adresy	tt	SRC
#4	Bajt doplnkovej dĺžky	m+3	LEN
#5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
#6 až #7	recordDataIdentifier = [hodnota z tabuľky 28]	xxxx	RDI_…

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#8 až m +7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrolný súčet	00-FF	CS

Tabuľka 30

Správa WriteDataByIdentifier Positive Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 až #7	recordDataIdentifier = [the same value as bytes #6 and #7 tabuľky 29]	xxxx	RDI_…
#8	Kontrolný súčet	00-FF	CS

Tabuľka 31

Správa WriteDataByIdentifier Negative Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	WriteDataByIdentifier Request Service Id	2E	WDBI

Bajt #	Názov parametra		Hexadecimálna hodnota	Mnemotechnická skratka
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrolný súčet		00-FF	CS

6.2.3 *Vymedzenie parametrov*

Parameter ***recordDataIdentifier (RDI_)*** je vymedzený v tabuľke 28.

Parameter ***dataRecord (DREC_)*** používa správa s požiadavkou WriteDataByIdentifier na to, aby poskytla serveru (VU) hodnoty dátového záznamu identifikované pomocou recordDataIdentifier. Dátové formáty sú špecifikované v oddiele 8.

7. KONTROLA SKÚŠOBNÝCH IMPULZOV – KONTROLA VSTUPU/VÝSTUPU FUNKČNEJ JEDNOTKY

Dostupné služby sú uvedené v tejto tabuľke:

Tabuľka 32

Kontrola vstupu/výstupu funkčnej jednotky

Názov služby	Opis
InputOutputControlByIdentifier	Klient požaduje kontrolu vstupu/výstupu špecifického pre server.

7.1. **Služba InputOutputControlByIdentifier**

7.1.1 *Opis správy*

Cez predný konektor je možné použitím vhodného skúšobného zariadenia kontrolovať alebo monitorovať skúšobné impulzy.

CPR_058 Toto kalibračné vstupné/výstupné signalizačné vedenie môže byť konfigurované príkazom K-vedenia použitím služby InputOutputControlByIdentifier na voľbu požadovanej vstupnej alebo výstupnej funkcie pre vedenie. Stavy vedenia sú tieto:

— deaktivované,

— speedSignalInput, kde sa kalibračné vstupné/výstupné signalizačné vedenie používa na vstup rýchlostného signálu (skúšobný signál), ktorým sa nahrádza rýchlostný signál snímača pohybu; táto funkcia nie je k dispozícii v KONTROLNOM režime,

— realTimeSpeedSignalOutputSensor, kde sa kalibračné vstupné/výstupné signalizačné vedenie používa na výstup rýchlostného signálu snímača pohybu,

— RTCOutput, kde sa kalibračné vstupné/výstupné signalizačné vedenie používa na výstup časového signálu UTC; táto funkcia nie je k dispozícii v KONTROLNOM režime.

CPR_059 Aby sa konfiguroval stav vedenia, musí sa jednotka vozidla nachádzať v relácii nastavenia a musí byť v režime KALIBRÁCIE alebo v KONTROLNOM režime. Ak je VU v režime KALIBRÁCIE, môžu sa zvoliť štyri stavy vedenia (deaktivované, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Ak je VU v KONTROLNOM režime, môžu sa zvoliť len dva stavy vedenia (deaktivované, realTimeSpeedOutputSensor). Pri skončení relácie nastavenia alebo režimu KALIBRÁCIE alebo KONTROLNÉHO režimu musí jednotka vozidla zabezpečiť, aby sa kalibračné vstupné/výstupné signalizačné vedenie vrátilo do „deaktivovaného“ (predvoleného) stavu.

CPR_060 Ak sa na vstupnom signalizačnom vedení rýchlosti v reálnom čase VU prijmú rýchlostné impulzy, zatiaľ čo je kalibračné vstupné/výstupné signalizačné vedenie nastavené na vstup, potom kalibračné vstupné/výstupné signalizačné vedenie musí byť nastavené na výstup, alebo sa musí vrátiť do deaktivovaného stavu.

CPR_061 Sekvencia má takýto priebeh:

— nadviazanie komunikácie prostredníctvom služby StartCommunication,

— zavedenie relácie nastavenia prostredníctvom služby StartDiagnosticSession a vstup do prevádzkového režimu KALIBRÁCIE alebo KONTROLY (poradie týchto dvoch režimov nie je dôležité).

— zmena stavu výstupu prostredníctvom služby InputOutputControlByIdentifier.

7.1.2 *Formát správy*

CPR_062 Formáty správ pre prvky InputOutputControlByIdentifier sú uvedené v týchto tabuľkách:

Tabuľka 33

Správa InputOutputControlByIdentifier Request

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	EE	TGT
#3	Bajt zdrojovej adresy	tt	SRC
#4	Bajt doplnkovej dĺžky	xx	LEN
#5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
#6 a #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 alebo #8 až #9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter – jedna hodnota z tabuľky 36	xx	IOCP_…
	controlState – jedna hodnota z tabuľky 37 (pozri poznámku ďalej)]	xx	CS_…
#9 alebo #10	Kontrolný súčet	00-FF	CS

Poznámka: Parameter controlState je k dispozícii len v niektorých prípadoch (pozri 7.1.3).

Tabuľka 34

Správa InputOutputControlByIdentifier Positive Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	xx	LEN
#5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 a #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 alebo #8 až #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (rovnaká hodnota ako v bajte #8 v tabuľke 33)	xx	IOCP_…
	controlState (rovnaká hodnota ako v bajte #9 v tabuľke 33)] (v prípade potreby)	xx	CS_…
#9 alebo #10	Kontrolný súčet	00-FF	CS

Tabuľka 35

Správa InputOutputControlByIdentifier Negative Response

Bajt #	Názov parametra	Hexadecimálna hodnota	Mnemotechnická skratka
#1	Formátový bajt – fyzické adresovanie	80	FMT
#2	Bajt cieľovej adresy	tt	TGT
#3	Bajt zdrojovej adresy	EE	SRC
#4	Bajt doplnkovej dĺžky	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	Kontrolný súčet	00-FF	CS

7.1.3 *Vymedzenie parametrov*

CPR_064 Parameter ***inputOutputControlParameter (IOCP_)*** je vymedzený v tejto tabuľke:

Tabuľka 36

Vymedzenie hodnôt inputOutputControlParameter

Hex	Opis	Mnemotechnická skratka
00	**ReturnControlToECU** Táto hodnota oznamuje serveru (VU), že skúšobné zariadenie už nemá kontrolu nad kalibračným vstupným/výstupným signalizačným vedením.	RCTECU
01	**ResetToDefault** Táto hodnota oznamuje serveru (VU), že sa od neho požaduje, aby resetoval kalibračné vstupné/výstupné signalizačné vedenie do jeho predvoleného stavu.	RTD
03	**ShortTermAdjustment** Táto hodnota oznamuje serveru (VU), že sa od neho požaduje, aby nastavil kalibračné vstupné/výstupné signalizačné vedenie na hodnotu obsiahnutú v parametri controlState.	STA

CPR_065 Parameter ***controlState*** je k dispozícii len vtedy, keď je inputOutputControlParameter nastavený na ShortTermAdjustment, a je vymedzený v tejto tabuľke:

Tabuľka 37

Vymedzenie hodnôt controlState

Režim	Hexadecimálna hodnota	Opis
Deaktivovať	00	vstupné/výstupné vedenie je deaktivované (predvolený stav)
Aktivovať	01	Aktivovať kalibračné vstupné/výstupné vedenie ako speedSignalInput
Aktivovať	02	Aktivovať kalibračné vstupné/výstupné vedenie ako realTimeSpeedSignalOutputSensor
Aktivovať	03	Aktivovať kalibračné vstupné/výstupné vedenie ako RTCOutput

8. FORMÁTY DATARECORDS

Tento oddiel obsahuje:

— všeobecné pravidlá, ktoré sa musia uplatňovať na rozsahy hodnôt parametrov prenášané jednotkou vozidla na skúšobné zariadenie,

— formáty, ktoré sa musia používať pre údaje prenášané cez služby prenosu údajov opísané v oddiele 6.

CPR_067 Všetky identifikované parametre musia byť podporované VU.

CPR_068 Údaje prenášané VU na skúšobné zariadenie ako odpoveď na správu s požiadavkou musia zodpovedať meranému typu (t. j. aktuálnej hodnote požadovaného parametra, ktorý VU meria alebo sleduje).

8.1. **Rozsahy hodnôt prenášaných parametrov**

CPR_069 Tabuľka 38 vymedzuje rozsahy hodnôt používané na stanovenie platnosti prenášaného parametra.

CPR_070 Hodnoty v rozsahu „indikátor chýb“ poskytujú jednotke vozidla spôsob, ako ihneď oznámiť, že platné údaje parametrov nie sú v súčasnosti k dispozícii v dôsledku určitého typu chyby v tachografe.

CPR_071 Hodnoty v rozsahu „nie je k dispozícii“ poskytujú jednotke vozidla spôsob, ako poslať správu obsahujúcu parameter, ktorý nie je dostupný, alebo nie je v danom module podporovaný. Hodnoty v rozsahu „nepožaduje sa“ poskytujú zariadeniu spôsob, ako poslať príkazovú správu a identifikovať také parametre, na ktoré sa od prijímajúceho zariadenia neočakáva žiadna odpoveď.

CPR_072 Ak zlyhanie komponentu zabráni prenosu platných údajov pre parameter, mal by sa namiesto požadovaných údajov parametra použiť indikátor chýb opísaný v tabuľke 38. Ak však namerané alebo vypočítané údaje majú hodnotu, ktorá je síce platná, ale presahuje vymedzený rozsah parametra, indikátor chýb by sa nemal použiť. Údaje by sa mali preniesť pomocou primeranej minimálnej alebo maximálnej hodnoty parametra.

Tabuľka 38

Rozsahy hodnôt pre dataRecords

Názov rozsahu hodnôt	1 bajt (Hexadecimálna hodnota)	2 bajty (Hexadecimálna hodnota)	4 bajty (Hexadecimálna hodnota)	ASCII
Platný signál	00 až FA	0000 až FAFF	00000000 až FAFFFFFF	1 až 254
Indikátor špecifický pre parameter	FB	FB00 až FBFF	FB000000 až FBFFFFFF	žiadne
Vyhradený rozsah pre budúce bity indikátora	FC až FD	FC00 až FDFF	FC000000 až FDFFFFFF	žiadne
Indikátor chýb	FE	FE00 až FEFF	FE000000 až FEFFFFFF	0
Nie je k dispozícii alebo sa nepožaduje	FF	FF00 až FFFF	FF000000 až FFFFFFFF	FF

CPR_073 Pre parametre kódované v ASCII, je znak ASCII „*“ vyhradený pre oddeľovač.

8.2. Formáty dataRecords

V tabuľke 39 až tabuľke 42 sú podrobne uvedené formáty, ktoré sa musia používať v službách ReadDataByIdentifier a WriteDataByIdentifier.

CPR_074 V tabuľke 39 je uvedená dĺžka, rozlíšenie a prevádzkový rozsah pre každý parameter identifikovaný pomocou jeho recordDataIdentifier:

Tabuľka 39

Formát dataRecords

Názov parametra	Dĺžka údajov (v bajtoch)	Rozlíšenie	Prevádzkový rozsah
TimeDate	8	Podrobné údaje sú v tabuľke 40	
HighResolutionTotalVehicleDistance	4	Prírastok 5 m/bit, offset 0 m	0 až + 21 055 406 km
Kfactor	2	Prírastok 0,001 impulz/m/bit, offset 0	0 až 64,255 impulz/m
LfactorTyreCircumference	2	Prírastok 0,125 10^{-3} m/bit, offset 0	0 až 8,031 m
WvehicleCharacteristicFactor	2	Prírastok 0,001 impulz/m/bit, offset 0	0 až 64,255 impulz/m
TyreSize	15	ASCII	ASCII

Názov parametra	Dĺžka údajov (v bajtoch)	Rozlíšenie	Prevádzkový rozsah
NextCalibrationDate	3	Podrobné údaje sú v tabuľke 41	
SpeedAuthorised	2	Prírastok 1/256 km/h/bit, offset 0	0 až 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Podrobné údaje sú v tabuľke 42	
VIN	17	ASCII	ASCII

CPR_075 Tabuľka 40 obsahuje formáty rôznych bajtov parametra TimeDate:

Tabuľka 40

Podrobný formát TimeDate (hodnota recordDataIdentifier # F90B)

Bajt	Vymedzenie parametrov	Rozlíšenie	Prevádzkový rozsah
1	Sekundy	Prírastok 0,25 s/bit, offset 0 s	0 až 59,75 s
2	Minúty	Prírastok 1 min/bit, offset 0 min	0 až 59 min
3	Hodiny	Prírastok 1 h/bit, offset 0 h	0 až 23 h
4	Mesiac	Prírastok 1 mesiac/bit, offset 0 mesiacov	1 až 12 mesiacov
5	Deň	Prírastok 0,25 dňa/bit, offset 0 dní (pozri POZNÁMKU v tabuľke 41)	0,25 až 31,75 dňa
6	Rok	Prírastok 1 rok/bit, offset rok + 1985 (pozri POZNÁMKU v tabuľke 41)	rok 1985 až 2235
7	Miestny minútový offset	Prírastok 1 min/bit, offset – 125 min	– 59 až + 59 min
8	Miestny hodinový offset	Prírastok 1 h/bit, offset – 125 h	– 23 až +2 3 h

CPR_076 Tabuľka 41 obsahuje formáty rôznych bajtov parametra NextCalibrationDate:

Tabuľka 41

Podrobný formát NextCalibrationDate (hodnota recordDataIdentifier # F922)

Bajt	Vymedzenie parametrov	Rozlíšenie	Prevádzkový rozsah
1	Mesiac	Prírastok 1 mesiac/bit, offset 0 mesiacov	1 až 12 mesiacov
2	Deň	Prírastok 0,25 dňa/bit, offset 0 dní (pozri POZNÁMKU ďalej)	0,25 až 31,75 dňa
3	Rok	Prírastok 1 rok/bit, offset rok +1985 (pozri POZNÁMKU ďalej)	rok 1985 až 2235

POZNÁMKA týkajúca sa použitia parametra „deň“:

1. Hodnota dátumu 0 je neplatná. Hodnoty 1, 2, 3 a 4 sa používajú na označenie prvého dňa mesiaca, hodnoty 5, 6, 7 a 8 označujú druhý deň mesiaca atď.

2. Tento parameter nemá vplyv ani nemení uvedený hodinový parameter.

POZNÁMKA týkajúca sa použitia bajtu parametra „rok“:

Hodnota 0 pre rok označuje rok 1985, hodnota 1 označuje rok 1986 atď.

CPR_078 Tabuľka 42 obsahuje formáty rôznych bajtov parametra VehicleRegistrationNumber:

Tabuľka 42

Podrobný formát VehicleRegistrationNumber (hodnota recordDataIdentifier # F97E)

Bajt	Vymedzenie parametrov	Rozlíšenie	Prevádzkový rozsah
1	Kódová stránka (vymedzená v dodatku 1)	ASCII	01 až 0A
2 – 14	Evidenčné číslo vozidla (vymedzené v dodatku 1)	ASCII	ASCII

Dodatok 9

TYPOVÉ SCHVÁLENIE ZOZNAM MINIMÁLNYCH VYŽADOVANÝCH SKÚŠOK

OBSAH

1. ÚVOD 309

2. FUNKČNÉ SKÚŠKY JEDNOTKY VOZIDLA 311

3. FUNKČNÉ SKÚŠKY SNÍMAČA POHYBU 315

4. FUNKČNÉ SKÚŠKY TACHOGRAFOVÝCH KARIET 318

5. SKÚŠKY EXTERNÉHO ZARIADENIA GNSS 328

6. SKÚŠKY DIAĽKOVÉHO KOMUNIKAČNÉHO ZARIADENIA 331

7. FUNKČNÉ SKÚŠKY PAPIERA 333

8. SKÚŠKY INTEROPERABILITY 335

1. ÚVOD

1.1. **Typové schválenie**

Typové schválenie ES pre záznamové zariadenie (alebo jeho komponent) či tachografovú kartu je založené na:

— **osvedčovaní zabezpečenia** podľa špecifikácií spoločných kritérií na základe bezpečnostného cieľa v úplnej zhode s dodatkom 10 tejto prílohy (ktorý sa doplní/upraví),

— **osvedčovaní funkčnosti** vykonanom orgánom členského štátu, ktorým sa potvrdzuje, že skúšaný diel spĺňa požiadavky tejto prílohy z hľadiska vykonávaných funkcií, presnosti merania a charakteristík prostredia,

— **osvedčovaní interoperability** vykonanom príslušným orgánom, ktorým sa potvrdzuje, že záznamové zariadenie (alebo tachografová karta) je plne interoperabilné(-á) s príslušnými modelmi tachografových kariet (alebo záznamových zariadení) (pozri kapitolu 8 tejto prílohy).

Tento dodatok špecifikuje minimálne skúšky, ktoré musí vykonať orgán členského štátu v rámci funkčných skúšok, a minimálne skúšky, ktoré musí vykonať príslušný orgán v rámci skúšok interoperability. Postupy vykonávania skúšok (prípadne ich druh) sa bližšie nešpecifikujú.

Aspekty osvedčovania zabezpečenia nie sú predmetom tohto dodatku. Ak sa niektoré skúšky potrebné na typové schválenie vykonajú v rámci posudzovania zabezpečenia a certifikačného procesu, potom sa tieto skúšky nemusia vykonávať znovu. V takom prípade sa môžu kontrolovať len výsledky týchto skúšok zabezpečenia. Pre informáciu, požiadavky, ktorých skúšanie sa očakáva (alebo ktoré sa úzko viažu k skúškam, ktoré sa majú vykonať) v rámci osvedčovania zabezpečenia, sú v tomto dodatku označené hviezdičkou („*“).

Číslované požiadavky odkazujú na text prílohy, zatiaľ čo ostatné požiadavky odkazujú na ostatné dodatky (napr. PIC_001 znamená požiadavku PIC_001 v piktogramoch dodatku 3).

Dodatok sa v rámci typového schvaľovania komponentov záznamového zariadenia venuje oddelene snímaču pohybu, jednotke vozidla a externému zariadeniu GNSS. Každý komponent dostane vlastné osvedčenie o typovom schválení, v ktorom sa uvedú ostatné kompatibilné komponenty. Funkčná skúška snímača pohybu (alebo externého zariadenia GNSS) sa vykonáva spoločne s jednotkou vozidla a naopak.

Nevyžaduje sa interoperabilita všetkých modelov snímačov pohybu (resp. externých zariadení GNSS) so všetkými modelmi jednotiek vozidla. V takom prípade možno typové schválenie snímača pohybu (resp. externého zariadenia GNSS) udeliť iba v kombinácii s typovým schválením príslušnej jednotky vozidla a naopak.

1.2. **Referenčné dokumenty**

V dodatku sa používajú tieto referenčné dokumenty:

IEC 60068-2-1: Skúšanie vplyvu prostredia. Časť 2-1: Skúšky. Skúška A: Chlad.

IEC 60068-2-2: Skúšanie vplyvu prostredia. Časť 2: Skúšky. Skúška B: Suché teplo (sínusoidne).

IEC 60068-2-6: Skúšanie vplyvu prostredia. Časť 2: Skúšky. Skúška Fc: Vibrácie.

IEC 60068-2-14: Skúšanie vplyvu prostredia. Časť 2-14: Skúšky. Skúška N: Zmena teploty.

IEC 60068-2-27: Skúšanie vplyvu prostredia. Časť 2: Skúšky. Skúška Ea a návod: Otrasy.

IEC 60068-2-30: Skúšanie vplyvu prostredia. Časť 2-30: Skúšky. Skúška Db: Vlhké teplo, cyklické (cyklus 12 + 12 h).

IEC 60068-2-64: Skúšanie vplyvu prostredia. Časť 2-64: Skúšky. Skúška Fh: Širokopásmové náhodné vibrácie, usmernenia.

IEC 60068-2-78 Skúšanie vplyvu prostredia. Časť 2-78: Skúšky. Skúška Cab: Vlhké teplo, konštantné.

ISO 16750-3 – Mechanické zaťaženie (2012-12).

ISO 16750-4 – Klimatické zaťaženie (2010-04).

ISO 20653: Cestné vozidlá. Stupeň ochrany (kód IP). Ochrana elektrických zariadení proti cudzím predmetom, vode a prístupu.

ISO 10605:2008 + technické korigendum:2010 + AMD1:2014 Cestné vozidlá. Metódy skúšania elektrických rušenie z elektrostatických výbojov.

ISO 7637-1:2002 + AMD1: 2008 Cestné vozidlá. Elektrické rušenie z vedenia a väzieb. Časť 1: Definície a všeobecné hľadiská.

ISO 7637-2 Cestné vozidlá. Elektrické rušenie z vedenia a väzieb. Časť 2: Prechodové elektrické vedenie len pozdĺž napájacieho vedenia.

ISO 7637-3 Cestné vozidlá. Elektrické rušenie z vedenia a väzieb. Časť 3: Prechodové elektrické vedenie kapacitnou a induktívnou väzbou iným než napájacím vedením.

ISO/IEC 7816-1 Identifikačné karty. Karty s integrovanými obvodmi a s kontaktmi. Časť 1: Fyzikálne vlastnosti.

ISO/IEC 7816-2 Informačné technológie. Identifikačné karty. Karty s integrovanými obvodmi a s kontaktmi. Časť 2: Rozmery a umiestnenie kontaktov.

ISO/IEC 7816-3 Informačné technológie. Identifikačné karty. Karty s integrovanými obvodmi a s kontaktmi. Časť 3: Elektronické signály a protokoly procesu.

ISO/IEC 10373-1:2006 + AMD1:2012 Identifikačné karty. Skúšobné metódy. Časť 1: Všeobecné charakteristiky.

ISO/IEC 10373-3:2010 + technické korigendum:2013 Identifikačné karty. Skúšobné metódy. Časť 3: Karty s integrovanými obvodmi a s kontaktmi a súvisiace zariadenia s rozhraním.

ISO 16844-3:2004, kor. 1:2006 Cestné vozidlá. Tachografové systémy. Časť 3: Rozhranie snímača pohybu (s jednotkami vozidla).

ISO 16844-4 Cestné vozidlá. Tachografové systémy. Časť 4: Rozhranie CAN.

ISO 16844-6 Cestné vozidlá. Tachografové systémy. Časť 6: Diagnostika.

ISO 16844-7 Cestné vozidlá. Tachografové systémy. Časť 7: Parametre.

ISO 534 Papier a lepenka. Stanovenie hrúbky, hustoty a merného objemu.

Predpis EHK OSN R10 (UN ECE R10) Jednotné ustanovenia o schvaľovaní vozidiel z hľadiska elektromagnetickej kompatibility (Európska hospodárska komisia OSN).

2. FUNKČNÉ SKÚŠKY JEDNOTKY VOZIDLA

Č.	Skúška	Opis	Súvisiace požiadavky
1	**Administratívne preskúmanie**		
1.1	Dokumentácia	Správnosť dokumentácie	
1.2	Výsledky skúšok výrobcu	Výsledky skúšky výrobcu vykonanej počas montáže. Predloženie písomných dokladov.	88, 89,91
2	**Vizuálna kontrola**		
2.1	Súlad s dokumentáciou		
2.2	Identifikácia/označenie		224 až 226
2.3	Materiály		219 až 223
2.4	Plomby		398, 401 až 405
2.5	Externé rozhrania		
3	**Funkčné skúšky**		
3.1	Poskytované funkcie		03, 04, 05, 07, 382,
3.2	Prevádzkové režimy		09 až 11*, 132, 133
3.3	Funkcie a práva na prístup k údajom		12* 13*,, 382, 383, 386 až 389
3.4	Monitorovanie vkladania a vyťahovania kariet		15, 16, 17, 18, 19*, 20*, 132
3.5	Meranie rýchlosti a vzdialenosti		21 až 31
3.6	Meranie času (test vykonaný pri 20 °C)		38 až 43
3.7	Monitorovanie činností vodiča		44 až 53, 132
3.8	Monitorovanie stavu vedenia vozidla		54, 55, 132

Č.	Skúška	Opis	Súvisiace požiadavky
3.9	Manuálne záznamy		56 až 62
3.10	Podnikové blokovanie		63 až 68
3.11	Monitorovanie kontrolných činností		69, 70
3.12	Detekcia udalostí a/alebo porúch		71 až 88 132
3.13	Identifikačné údaje zariadenia		93*, 94*, 97, 100
3.14	Údaje o vložení a vytiahnutí karty vodiča		102* až 104*
3.15	Údaje o činnosti vodiča		105* až 107*
3.16	Údaje o miestach a polohe		108* až 112*
3.17	Údaje o stave počítadla kilometrov		113* až 115*
3.18	Podrobné údaje o rýchlosti		116*
3.19	Údaje o udalostiach		117*
3.20	Údaje o poruchách		118*
3.21	Kalibračné údaje		119* až 121*
3.22	Údaje úpravy času		124*, 125*
3.23	Údaje o kontrolnej činnosti		126*, 127*
3.24	Údaje o podnikovom blokovaní		128*
3.25	Údaje o sťahovaní		129*
3.26	Údaje o špecifických podmienkach		130*, 131*
3.27	Zaznamenávanie a ukladanie na tachografových kartách		134, 135,, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Zobrazovanie		90, 132, 149 až 166, PIC_001, DIS_001
3.29	Tlač		90, 132, 167 až 179, PIC_001, PRT_001 až PRT_014
3.30	Výstraha		132, 180 až 189, PIC_001

Č.	Skúška	Opis	Súvisiace požiadavky
3.31	Sťahovanie údajov na externé médiá		90, 132, 190 až 194
3.32	Diaľková komunikácia na cielené cestné kontroly		195 až 197
3.33	Výstupné údaje pre doplnkové externé zariadenia		198, 199
3.34	Kalibrácia		202 až 206*, 383, 384, 386 až 391
3.35	Kontrola kalibrácie pri cestnej kontrole		207 až 209
3.36	Úprava času		210 až 212*
3.37	Nerušenie doplnkovými funkciami		06, 425
3.38	Rozhranie snímača pohybu		02, 122
3.39	Externé zariadenie GNSS		03, 123
3.40	Overenie, že VU zistí, zaznamená a uloží udalosť(-ti) a/alebo poruchu(-y) určenú(-é) výrobcom VU, keď spárovaný snímač pohybu reaguje na magnetické polia rušiace funkciu snímania pohybu vozidla.		217
3.41	Šifrovacia zostava a štandardizované parametre domény		CSM_48, CSM_50
4	**Skúšanie vplyvu prostredia**		
4.1	Teplota	Overenie funkčnosti: skúškou podľa ISO 16750-4, kapitoly 5.1.1.2: Skúška prevádzky pri nízkej teplote (72 h pri – 20 °C) Táto skúška sa týka IEC 60068-2-1: Skúšanie vplyvu prostredia. Časť 2-1: Skúšky. Skúška A: Chlad skúškou podľa ISO 16750-4: kapitola 5.1.2.2: Skúška prevádzky pri vysokej teplote (72 h pri 70 °C) Táto skúška sa týka IEC 60068-2-2: Skúšanie vplyvu prostredia. Časť 2: Skúšky. Skúška B: Suché teplo skúškou podľa ISO 16750-4: Kapitola 5.3.2: Rýchla zmena teploty so stanoveným trvaním prechodu (– 20 °C/70 °C, 20 cyklov, čas zotrvania na každej teplote: 2 h) Pri nižšej a vyššej teplote, ako aj počas teplotných cyklov možno vykonať redukovaný súbor skúšok (spomedzi skúšok vymedzených v bode 3 tejto tabuľky)	213

Č.	Skúška	Opis	Súvisiace požiadavky
4.2	Vlhkosť	Overí sa, či jednotka vozidla odolá cyklickej vlhkosti (teplotná skúška) podľa IEC 60068-2-30, skúške Db, šesť 24-hodinových cyklov, vždy pri meniacej sa teplote od + 25 °C po + 55 °C a relatívnej vlhkosti 97 % pri + 25 °C a 93 % pri + 55 °C	214
4.3	Mechanické zaťaženie	1. Sínusové vibrácie. Overí sa, či jednotka vozidla odolá sínusovým vibráciám s týmito charakteristikami: konštantný posuv medzi 5 a 11 Hz: max. 10 mm konštantné zrýchlenie medzi 11 a 300 Hz: 5g Táto požiadavka sa overí podľa IEC 60068-2-6, skúška Fc, s minimálnym trvaním 3 × 12 hodín (12 hodín na každú nápravu) ISO 16750-3 skúšku sínusových vibrácií nevyžaduje pri zariadeniach umiestnených v oddelenej kabíne vozidla. 2. Náhodné vibrácie: skúška podľa ISO 16750-3: kapitola 4.1.2.8: Skúška VIII: Úžitkové vozidlá s oddelenou kabínou Skúška náhodných vibrácií, 10…2 000 Hz, kvadratický priemer (RMS) v zvislej rovine 21,3 m/s^2, v pozdĺžnej rovine 11,8 m/s^2, v priečnej rovine 13,1 m/s^2, 3 osi, 32 h na každú os, vrátane teplotného cyklu – 20…70 °C. Táto skúška sa týka IEC 60068-2-64: Skúšanie vplyvu prostredia. Časť 2-64: Skúšky. Skúška Fh: Širokopásmové náhodné vibrácie, usmernenia 3. Otrasy: mechanický otras s polsínusom 3g podľa ISO 16750. Uvedená skúška sa vykoná na rôznych vzorkách skúšaného zariadenia.	219
4.4	Ochrana proti vode a cudzím telesám	Skúška podľa ISO 20653: Cestné vozidlá. Stupeň ochrany (kód IP). Ochrana elektrických zariadení proti cudzím predmetom, vode a prístupu (bez zmeny parametrov); minimálna hodnota IP 40	220, 221
4.5	Ochrana proti prepätiu	Overí sa, či jednotka vozidla odolá napájaciemu napätiu: Pre verzie 24V: 34 V pri + 40 °C 1 hodinu Pre verzie 12V: 17 V pri + 40 °C 1 hodinu (ISO 16750-2)	216
4.6	Ochrana proti zmene polarity	Overí sa, či jednotka vozidla odolá zmene polarity napájacieho napätia. (ISO 16750-2)	216

Č.	Skúška	Opis	Súvisiace požiadavky
4.7	Ochrana proti skratu	Overí sa, či sú vstupné/výstupné signály chránené proti skratu napájania a uzemnenia (ISO 16750-2)	216
5	**Skúšky EMC**		
5.1	Vyžarované emisie a citlivosť	Súlad s predpisom EHK OSN R10 (ECE R10)	218
5.2	Elektrostatický výboj	Súlad s ISO 10605:2008 + technické korigendum:2010 + AMD1:2014: +/– 4kV na kontaktoch a +/– 8kV pri vzdušnom výboji	218
5.3	Citlivosť na prechodové javy šírené vedením na napájaní	Pre verzie 24V: súlad s ISO 7637-2 + predpisom EHK 10 (ECE 10 Rev. 3): impulz 1a: Vs = – 450V Ri = 50 ohmov impulz 2a: Vs = + 37V Ri = 2 ohmy impulz 2b: Vs = + 20V Ri = 0,05 ohmu impulz 3a: Vs = – 150V Ri = 50 ohmov impulz 3b: Vs = + 150V Ri = 50 ohmov impulz 4: Vs = – 16V Va = – 12V t6 = 100ms impulz 5: Vs = + 120V Ri = 2,2 ohmov td = 250ms Pre verzie 12V: súlad s ISO 7637-1 + predpisom EHK 10 (ECE 10 Rev. 3): impulz 1: Vs = – 75V Ri = 10 ohmov impulz 2a: Vs = + 37V Ri = 2 ohmy impulz 2b: Vs = + 10V Ri = 0,05 ohmu impulz 3a: Vs = – 112V Ri = 50 ohmov impulz 3b: Vs = + 75V Ri=50 ohmov impulz 4: Vs = – 6V Va = – 5V t6 = 15ms impulz 5: Vs = + 65V Ri = 3 ohmy td = 100ms Impulz 5 sa skúša len v jednotkách vozidiel určených na montáž vo vozidlách bez externej spoločnej ochrany proti poklesu zaťaženia. Pre návrh súvisiaci s poklesom zaťaženia pozri ISO 16750-2, 4. vydanie, kapitola 4.6.4.	218

3. FUNKČNÉ SKÚŠKY SNÍMAČA POHYBU

Č.	Skúška	Opis	Súvisiace požiadavky
1.	**Administratívne preskúmanie**		
1.1	Dokumentácia	Správnosť dokumentácie	

Č.	Skúška	Opis	Súvisiace požiadavky
2.	**Vizuálna kontrola**		
2.1.	Súlad s dokumentáciou		
2.2.	Identifikácia/označenie		225, 226,
2.3	Materiály		219 až 223
2.4.	Plomby		398, 401 až 405
3.	**Funkčné skúšky**		
3.1	Identifikačné údaje snímača		95 až 97*
3.2	Párovanie snímača pohybu s jednotkou vozidla		122*, 204
3.3	Snímanie pohybu Presnosť merania pohybu		30 až 35
3.4	Rozhranie s jednotkou vozidla		02
3.5	Overí sa, že snímač pohybu je odolný voči stálemu magnetickému poľu. Alternatívou je overiť, či snímač pohybu reaguje na stále magnetické polia rušiace funkciu snímania pohybu vozidla tak, aby pripojená VU dokázala zistiť, zaznamenať a uložiť poruchy snímača.		217
4.	**Skúšanie vplyvu prostredia**		
4.1	Prevádzková teplota	Overí sa funkčnosť (v zmysle skúšky č. 3.3) v teplotnom rozsahu [– 40 °C; + 135 °C], a to: skúškou Ad podľa IEC 60068-2-1 v trvaní 96 hodín pri najnižšej teplote To_{min}, skúškou Bd podľa IEC 60068-2-2 v trvaní 96 hodín pri najvyššej teplote To_{max} skúškou podľa ISO 16750-4: kapitola 5.1.1.2: Skúška prevádzky pri nízkej teplote (24 h pri – 40 °C) Táto skúška sa týka IEC 60068-2-1: Skúšanie vplyvu prostredia. Časť 2-1: Skúšky. Skúška A: Skúška Bd (chlad) podľa IEC 68-2-2 v trvaní 96 hodín pri najnižšej teplote – 40 °C. skúškou podľa ISO 16750-4: kapitola 5.1.2.2: Skúška prevádzky pri vysokej teplote (96 h pri 135 °C) Táto skúška sa týka IEC 60068-2-2: Skúšanie vplyvu prostredia. Časť 2: Skúšky. Skúška B: Suché teplo	213

Č.	Skúška	Opis	Súvisiace požiadavky
4.2	Teplotné cykly	skúškou podľa ISO 16750-4: Kapitola 5.3.2: Rýchla zmena teploty so stanoveným trvaním prechodu (– 40 °C/135 °C, 20 cyklov, čas zotrvania na každej teplote: 30 min.) IEC 60068-2-14: Skúšanie vplyvu prostredia. Časť 2-14: Skúšky. Skúška N: Zmena teploty	213
4.3	Cykly vlhkosti	Overí sa funkčnosť (v zmysle skúšky č. 3.3), a to skúškou Db podľa IEC 60068-2-30 – šesť 24-hodinových cyklov, každý pri teplotách od + 25 °C po + 55 °C a relatívnej vlhkosti 97 % pri + 25 °C a rovnej 93 % pri + 55 °C	214
4.4	Vibrácie	ISO 16750-3: kapitola 4.1.2.6: Skúška VI: Úžitkové vozidlo, motor, prevodovka Skúška zmiešaných vibrácií vrátane a) skúšky sínusových vibrácií, 20…520 Hz, 11,4 … 120 m/s², <= 0,5 okt/min b) skúšky náhodných vibrácií, 10…2 000 Hz, RMS 177 m/s² 94 hodín na každej náprave vrátane teplotného cyklu – 20…70 °C Táto skúška sa týka IEC 60068-2-80: Skúšanie vplyvu prostredia. Časť 2-80: Skúšky. Skúška Fi: Vibrácie – kombinovaný mód	219
4.5	Mechanické otrasy	ISO 16750-3: kapitola 4.2.3: Skúška VI: Skúška zariadení v prevodovke alebo na nej polsínusový otras, zrýchlenie vecou dohody v rozsahu 3 000…15 000 m/s², trvanie impulzu vecou dohody, avšak < 1 ms, počet otrasov: vecou dohody Táto skúška sa týka IEC 60068-2-27: Skúšanie vplyvu prostredia. Časť 2: Skúšky. Skúška Ea a návod: Otrasy	219
4.6	Ochrana proti vode a cudzím telesám	Skúška podľa ISO 20653: Cestné vozidlá. Stupeň ochrany (kód IP). Ochrana elektrických zariadení proti cudzím predmetom, vode a prístupu (cieľová hodnota IP 64)	220, 221
4.7	Ochrana proti zmene polarity	Overí sa, či snímač pohybu odolá zmene polarity napájacieho napätia.	216
4.8	Ochrana proti skratu	Overí sa, či sú vstupné/výstupné signály chránené proti skratu napájania a uzemnenia	216

Č.	Skúška	Opis	Súvisiace požiadavky
5.	**EMC**		
5.1	Vyžarované emisie a citlivosť	Overí sa súlad s predpisom EHK OSN (ECE R10)	218
5.2	Elektrostatický výboj	Súlad s ISO 10605:2008 + technické korigendum:2010 + AMD1:2014: +/– 4kV na kontaktoch a +/– 8kV pri vzdušnom výboji	218
5.3	Citlivosť na prechodové javy šírené vedením na dátových vodičoch	Pre verzie 24V: súlad s ISO 7637-2 + predpisom EHK 10 (ECE 10 Rev. 3): impulz 1a: Vs = – 450V Ri = 50 ohmov impulz 2a: Vs = + 37V Ri = 2 ohmy impulz 2b: Vs = + 20V Ri = 0,05 ohmu impulz 3a: Vs = – 150V Ri = 50 ohmov impulz 3b: Vs = + 150V Ri = 50 ohmov impulz 4: Vs = – 16V Va = – 12V t6 = 100ms impulz 5: Vs = + 120V Ri = 2,2 ohmov td = 250ms Pre verzie 12V: súlad s ISO 7637-1 + predpisom EHK 10 (ECE 10 Rev. 3): impulz 1: Vs = – 75V Ri = 10 ohmov impulz 2a: Vs = + 37V Ri = 2 ohmy impulz 2b: Vs = + 10V Ri = 0,05 ohmu impulz 3a: Vs = – 112V Ri = 50 ohmov impulz 3b: Vs = + 75V Ri = 50 ohmov impulz 4: Vs = – 6V Va = – 5V t6=15ms impulz 5: Vs = + 65V Ri = 3 ohmy td = 100ms Impulz 5 sa skúša len v jednotkách vozidiel určených na montáž vo vozidlách bez externej spoločnej ochrany proti poklesu zaťaženia. Pre návrh súvisiaci s poklesom zaťaženia pozri ISO 16750-2, 4. vydanie, kapitola 4.6.4.	218

4. FUNKČNÉ SKÚŠKY TACHOGRAFOVÝCH KARIET

Skúšky podľa tohto oddielu 4,

č. 5 „Skúšky protokolov“,

č. 6 „Štruktúra karty“ a

č. 7 „Funkčné skúšky“

môže vykonať hodnotiteľ alebo osvedčovateľ v rámci procesu osvedčovania zabezpečenia čipového modulu na základe spoločných kritérií (CC).

Skúšky č. 2.3 a 4.2 sú rovnaké. Ide o mechanické skúšky kombinácie tela karty a čipového modulu. Ak sa jeden z týchto komponentov (telo karty, čipový modul) zmení, sú tieto skúšky potrebné.

Č.	Skúška	Opis	Súvisiace požiadavky
1.	**Administratívne preskúmanie**		
1.1	Dokumentácia	Správnosť dokumentácie	
2	**Telo karty**		
2.1	Potlač	Overí sa, že všetky ochranné prvky a viditeľné údaje sú na karte vytlačené správne a zodpovedajú predpisom [Určenie] Príloha 1C, kapitola 4.1 „Viditeľné údaje“, bod 227) Na prednej strane sa uvedie: nápis „karta vodiča“, „kontrolná karta“, „dielenská karta“ alebo „podniková karta“, vytlačené veľkými písmenami v úradnom jazyku alebo jazykoch členského štátu, ktorý kartu vydal, podľa typu karty. [Názov členského štátu] Príloha 1C, kapitola 4.1 „Viditeľné údaje“, bod 228) Na prednej strane sa uvedie: názov členského štátu, ktorý kartu vydal (nepovinné). [Znak] Príloha 1C, kapitola 4.1 „Viditeľné údaje“, bod 229) Na prednej strane sa uvedie: negatív rozlišovacieho znaku členského štátu, ktorý kartu vydal, v modrom obdĺžniku a obkolesený 12 žltými hviezdičkami. [Vysvetlivky] Príloha 1C, kapitola 4.1 „Viditeľné údaje“, bod 232) Na zadnej strane sa uvedie: vysvetlenie k očíslovaným údajom na prednej strane karty. [Farba] Príloha 1C, kapitola 4.1 „Viditeľné údaje“, bod 234) Tachografové karty musia byť vytlačené s týmito prevažujúcimi farbami pozadia: — karta vodiča: biela, — dielenská karta: červená, — kontrolná karta: modrá, — podniková karta: žltá.	227 až 229, 232, 234 až 236

Č.	Skúška	Opis	Súvisiace požiadavky
		[Zabezpečenie] Príloha 1C, kapitola 4.1 „Viditeľné údaje“, bod 235) Telo tachografovej karty musí byť vybavené aspoň týmito ochrannými prvkami proti falšovaniu alebo neoprávneným zásahom: — ochranná podtlač s gilošovaným vzorom a írisovou tlačou. — aspoň jeden dvojfarebný mikrotlačový prúžok.	
		[Označenia] Príloha 1C, kapitola 4.1 „Viditeľné údaje“, bod 236) Členské štáty môžu doplniť farby alebo označenia ako štátne symboly či prvky zabezpečenia.	
		[Schvaľovacia značka] Tachografové karty musia obsahovať schvaľovaciu značku. Schvaľovaciu značku tvorí: — obdĺžnik, v ktorom je umiestnené písmeno „e“, za ktorým nasleduje rozlišovacie číslo alebo písmeno štátu, ktorý vydal schválenie, — schvaľovacie číslo zodpovedajúce číslu schvaľovacieho osvedčenia udeleného pre tachografovú kartu, ktoré je umiestnené na akomkoľvek mieste v tesnej blízkosti uvedeného obdĺžnika.	
2.2	Mechanické skúšky	[Veľkosť karty] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [5] Rozmery karty, [5.1] Veľkosť karty, [5.1.1] Rozmery karty a tolerancie, typ karty ID-1 Nepoužitá karta	240, 243 ISO/IEC 7810
		[Hrany karty] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [5] Rozmery karty, [5.1] Veľkosť karty, [5.1.2] Hrany karty	

Č.	Skúška	Opis	Súvisiace požiadavky
		[Konštrukcia karty] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [6] Konštrukcia karty	
		[Materiály na karty] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [7] Materiály na karty	
		[Ohybová tuhosť] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.1] Ohybová tuhosť	
		[Toxicita] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.3] Toxicita	
		[Odolnosť voči chemikáliám] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.4] Odolnosť voči chemikáliám	
		[Stabilita karty] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.5] Stabilita rozmerov karty a deformácie v závislosti od teploty a vlhkosti vzduchu	

Č.	Skúška	Opis	Súvisiace požiadavky
		[Svetlo] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.6] Odolnosť proti svetlu	
		[Trvanlivosť] Príloha 1C, kapitola 4.4 „Elektrické špecifikácie a špecifikácie prostredia“, bod 241) Tachografové karty si musia zachovať správnu funkčnosť päť rokov, ak sa používajú v súlade so špecifikáciami prostredia a elektrickými špecifikáciami.	
		[Pevnosť prekrývajúcej vrstvy] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.8] Pevnosť prekrývacej vrstvy	
		[Adhézia alebo vytváranie blokov] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.9] Adhézia alebo vytváranie blokov	
		[Priehyb] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.11] Celkový priehyb karty	
		[Odolnosť voči teplu] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.12] Odolnosť voči teplu	

Č.	Skúška	Opis	Súvisiace požiadavky
		[Deformácia povrchu] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.13] Deformácia povrchu	
		[Kontaminácia] Tachografové karty musia zodpovedať norme ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti, [8] Vlastnosti kariet, [8.14] Kontaminácia a interakcia komponentov karty	
2.3	Mechanické skúšky s implantovaným čipovým modulom	[Ohýbanie] Tachografové karty musia zodpovedať norme ISO/IEC 7810:2003/Amd. 1:2009, Identifikačné karty. Fyzikálne vlastnosti. Zmena 1: Kritériá pre karty s integrovanými obvodmi [9.2] Dynamické ohybové zaťaženie Celkový počet ohýbacích cyklov: 4 000.	ISO/IEC 7810
		[Torzia] Tachografové karty musia zodpovedať norme ISO/IEC 7810:2003/Amd. 1:2009, Identifikačné karty. Fyzikálne vlastnosti. Zmena 1: Kritériá pre karty s integrovanými obvodmi [9.3] Dynamické torzné zaťaženie Celkový počet torzných cyklov: 4 000.	
3	**Modul**		
3.1	Modul	Modul je zapuzdrenie čipu a doštička s kontaktmi.	ISO/IEC 7816
		[Profil povrchu] Tachografové karty musia zodpovedať norme ISO/IEC 7816-1:2011 Identifikačné karty. Karty s integrovanými obvodmi. Časť 1: Karty s kontaktmi. Fyzikálne vlastnosti [4.2] Profil povrchu kontaktov	

Č.	Skúška	Opis	Súvisiace požiadavky
		[Mechanická pevnosť] Tachografové karty musia zodpovedať norme ISO/IEC 7816-1:2011 Identifikačné karty. Karty s integrovanými obvodmi. Časť 1: Karty s kontaktmi. Fyzikálne vlastnosti [4.3] Mechanická pevnosť (karty a kontaktov)	
		[Elektrický odpor] Tachografové karty musia zodpovedať norme ISO/IEC 7816-1:2011 Identifikačné karty. Karty s integrovanými obvodmi. Časť 1: Karty s kontaktmi. Fyzikálne vlastnosti [4.4] Elektrický odpor (kontaktov)	
		[Rozmery] Tachografové karty musia zodpovedať norme ISO/IEC 7816-2:2007 Identifikačné karty. Karty s integrovanými obvodmi. Časť 2: Karty s kontaktmi. Rozmery a umiestnenie kontaktov [3] Rozmery kontaktov	
		[Umiestnenie] Tachografové karty musia zodpovedať norme ISO/IEC 7816-2:2007 Identifikačné karty. Karty s integrovanými obvodmi. Časť 2: Karty s kontaktmi. Rozmery a umiestnenie kontaktov [4] Počet a umiestnenie kontaktov V prípade modulov so šiestimi kontaktmi sa táto skúšobná požiadavka nevzťahuje na kontakty ‘C4’ a ‘C8’.	
4	**Čip**		
4.1	Čip	[Prevádzková teplota] Čip tachografovej karty musí fungovať v rozsahu okolitých teplôt od – 25 °C po + 85 °C.	241 až 244 ECE R10 ISO/IEC 7810 ISO/IEC 10373

Č.	Skúška	Opis	Súvisiace požiadavky
		[Teplota a vlhkosť] Príloha 1C, kapitola 4.4 „Elektrické špecifikácie a špecifikácie prostredia“, bod 241) Tachografové karty si musia zachovať správnu funkčnosť za všetkých klimatických podmienok bežných na území Spoločenstva a minimálne v rozsahu teplôt od – 25 °C do + 70 °C s príležitostnou špičkou do + 85 °C, pričom „príležitostná“ znamená jednorazovo maximálne 4 hodiny a maximálne 100 krát v priebehu životnosti karty. Tachografové karty sa postupne vystavia týmto teplotám a vlhkostiam na príslušný časový interval. Po každom kroku sa vyskúša elektrická funkčnosť tachografovej karty. 1. Teplota – 20 °C počas 2 h. 2. Teplota +/– 0 °C počas 2 h. 3. Teplota + 20 °C, 50 % relatívna vlhkosť počas 2 h. 4. Teplota + 50 °C, 50 % relatívna vlhkosť počas 2 h. 5. Teplota + 70 °C, 50 % relatívna vlhkosť počas 2 h. Teplota sa zvyšuje prerušovane až na + 85 °C, 50 % relatívna vlhkosť počas 60 min. 6. Teplota +70 °C, 85 % relatívna vlhkosť počas 2 h. Teplota sa zvyšuje prerušovane až na + 85 °C, 85 % relatívna vlhkosť počas 30 min.	
		[Vlhkosť] Príloha 1C, kapitola 4.4 „Elektrické špecifikácie a špecifikácie prostredia“, bod 242) Tachografové karty musia správne fungovať v rozsahu vlhkosti od 10 % do 90 %.	
		[Elektromagnetická kompatibilita – EMC] Príloha 1C, kapitola 4.4 „Elektrické špecifikácie a špecifikácie prostredia“, bod 244) Počas prevádzky musia tachografové karty spĺňať požiadavky predpisu EHS (ECE R10) spojené s elektromagnetickou kompatibilitou.	

Č.	Skúška	Opis	Súvisiace požiadavky
		[Statická elektrina] Príloha 1C, kapitola 4.4 „Elektrické špecifikácie a špecifikácie prostredia“, bod 244) Počas prevádzky musia byť tachografové karty chránené proti elektrostatickým výbojom. Tachografové karty musia zodpovedať norme ISO/IEC 7810:2003/Amd. 1:2009, Identifikačné karty. Fyzikálne vlastnosti. Zmena 1: Kritériá pre karty s integrovanými obvodmi [9.4] Statická elektrina [9.4.1] Karty s integrovanými obvodmi a s kontaktmi Skúšobné napätie: 4 000 V.	
		[Röntgenové žiarenie] Tachografové karty musia zodpovedať norme ISO/IEC 7810:2003/Amd. 1:2009, Identifikačné karty. Fyzikálne vlastnosti. Zmena 1: Kritériá pre karty s integrovanými obvodmi [9.1] Röntgenové žiarenie	
		[Ultrafialové svetlo] ISO/IEC 10373-1:2006, Identifikačné karty. Skúšobné metódy. Časť 1: Všeobecné charakteristiky [5.11] Ultrafialové svetlo	
		[Trojvalcová skúška] Tachografové karty musia zodpovedať norme ISO/IEC 10373-1:2006/Amd. 1:2012, Identifikačné karty. Skúšobné metódy. Časť 1: Všeobecné charakteristiky. Zmena 1 [5.22] ICC – Mechanická pevnosť: Trojvalcová skúška (3-wheel test) kariet s integrovanými obvodmi a kontaktmi	
		[Odolnosť zlepenia] Tachografové karty musia zodpovedať norme MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Skúška odolnosti zlepenia pri ohýbaní [13.2.1.32] TM-422: Mechanická spoľahlivosť: Skúška zlepenia	

Č.	Skúška	Opis	Súvisiace požiadavky
4.2	Mechanické skúšky čipových modulov implantovaných v karte-> rovnaké ako pri 2.3	[Ohýbanie] Tachografové karty musia zodpovedať norme ISO/IEC 7810:2003/Amd. 1:2009, Identifikačné karty. Fyzikálne vlastnosti. Zmena 1: Kritériá pre karty s integrovanými obvodmi [9.2] Dynamické ohybové zaťaženie Celkový počet ohýbacích cyklov: 4 000. [Torzia] Tachografové karty musia zodpovedať norme ISO/IEC 7810:2003/Amd. 1:2009, Identifikačné karty. Fyzikálne vlastnosti. Zmena 1: Kritériá pre karty s integrovanými obvodmi [9.3] Dynamické torzné zaťaženie Celkový počet torzných cyklov: 4 000.	ISO/IEC 7810
5	**Skúšky protokolov**		
5.1	ATR	Kontrola, či ATR zodpovedá požiadavkám	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Kontrola, či protokol T=0 zodpovedá požiadavkám	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Kontrola, či príkaz PTS zodpovedá požiadavkám, prepnutím z T=0 na T=1.	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Kontrola, či protokol T=1 zodpovedá požiadavkám	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Štruktúra karty**		
6.1		Overí sa, či štruktúra súborov karty zodpovedá požiadavkám; na tento účel sa kontroluje prítomnosť povinných súborov na karte a ich prístupové podmienky	TCS_22 až TCS_28 TCS_140 až TCS_179
7	**Funkčné skúšky**		
7.1	Normálne spracovanie	Skúša sa aspoň raz každé povolené použitie každého príkazu. (príklad: skúška príkazu UPDATE BINARY s CLA = '00', CLA = '0C' a s rôznymi parametrami P1,P2 a Lc) Overí sa, či operácie skutočne prebehli na karte (napr. čítaním súboru, v ktorom sa vykonal príkaz)	TCS_29 až TCS_139

Č.	Skúška	Opis	Súvisiace požiadavky
7.2	Chybové správy	Každá chybová správa (podľa dodatku 2) sa skúša aspoň raz pre každý príkaz. Skúša sa aspoň raz každá generická chyba (okrem chýb integrity '**6400**', ktoré sa skúšajú v rámci osvedčovania zabezpečenia)	
7.3	Šifrovacia zostava a štandardizované parametre domény		CSM_48, CSM_50
8	**Personalizácia**		
8.1	optická personalizácia	Príloha 1C, kapitola 4.1 „Viditeľné údaje“, bod 230) Na prednej strane sa uvedú: informácie špecifické pre vydanú kartu. Príloha 1C, kapitola 4.1 „Viditeľné údaje“, bod 231) Na prednej strane sa uvedú: dátumy vo formáte „dd/mm/rrrr“ alebo „dd.mm.rrrr“ (deň, mesiac, rok). Príloha 1C, kapitola 4.1 „Viditeľné údaje“, bod 235) Telo tachografovej karty musí byť vybavené aspoň týmito ochrannými prvkami proti falšovaniu alebo neoprávneným zásahom: — v oblasti fotografie sa ochranná podtlač musí prekrývať s fotografiou.	230, 231, 235

5. SKÚŠKY EXTERNÉHO ZARIADENIA GNSS

Č.	Skúška	Opis	Súvisiace požiadavky
1.	**Administratívne preskúmanie**		
1.1	Dokumentácia	Správnosť dokumentácie	
2.	**Vizuálna kontrola externého zariadenia GNSS**		
2.1.	Súlad s dokumentáciou		
2.2.	Identifikácia/označenie		224 až 226
2.3	Materiály		219 až 223
3.	**Funkčné skúšky**		
3.1	Identifikačné údaje snímača		98,99
3.2	Spojenie externého modulu GNSS s jednotkou vozidla		123, 205

Č.	Skúška	Opis	Súvisiace požiadavky
3.3	Poloha GNSS		36, 37
3.4	Rozhranie jednotky vozidla, keď je prijímač GNSS mimo jednotky vozidla		03
3.5	Šifrovacia zostava a štandardizované parametre domény		CSM_48, CSM_50
4.	**Skúšanie vplyvu prostredia**		
4.1	Teplota	Overenie funkčnosti: skúškou podľa ISO 16750-4, kapitoly 5.1.1.2: Skúška prevádzky pri nízkej teplote (72 h pri – 20 °C) Táto skúška sa týka IEC 60068-2-1: Skúšanie vplyvu prostredia. Časť 2-1: Skúšky. Skúška A: Chlad skúškou podľa ISO 16750-4: kapitola 5.1.2.2: Skúška prevádzky pri vysokej teplote (72 h pri 70 °C) Táto skúška sa týka IEC 60068-2-2: Skúšanie vplyvu prostredia. Časť 2: Skúšky. Skúška B: Suché teplo skúškou podľa ISO 16750-4: Kapitola 5.3.2: Rýchla zmena teploty so stanoveným trvaním prechodu (– 20 °C/70 °C, 20 cyklov, čas zotrvania na každej teplote: 1 h) Pri nižšej a vyššej teplote, ako aj počas teplotných cyklov možno vykonať redukovaný súbor skúšok (spomedzi skúšok vymedzených v bode 3 tejto tabuľky)	213
4.2	Vlhkosť	Overí sa, či jednotka vozidla odolá cyklickej vlhkosti (teplotná skúška) podľa IEC 60068-2-30, skúške Db, šesť 24-hodinových cyklov, vždy pri meniacej sa teplote od + 25 ° C po + 55 °C a relatívnej vlhkosti 97 % pri + 25 °C a 93 % pri + 55 °C	214
4.3	Mechanické zaťaženie	1. Sínusové vibrácie. Overí sa, či jednotka vozidla odolá sínusovým vibráciám s týmito charakteristikami: konštantný posuv medzi 5 a 11 Hz: max. 10 mm konštantné zrýchlenie medzi 11 a 300 Hz: 5g Táto požiadavka sa overí podľa IEC 60068-2-6, skúška Fc, s minimálnym trvaním 3 × 12 hodín (12 hodín na každú nápravu) ISO 16750-3 skúšku sínusových vibrácií nevyžaduje pri zariadeniach umiestnených v oddelenej kabíne vozidla.	219

Č.	Skúška	Opis	Súvisiace požiadavky
		2. Náhodné vibrácie: skúška podľa ISO 16750-3: kapitola 4.1.2.8: Skúška VIII: Úžitkové vozidlá s oddelenou kabínou Skúška náhodných vibrácií, 10…2 000 Hz, kvadratický priemer (RMS) v zvislej rovine 21,3 m/s^2, v pozdĺžnej rovine 11,8 m/s^2, v priečnej rovine 13,1 m/s^2, 3 osi, 32 h na každú os, vrátane teplotného cyklu – 20…70 °C. Táto skúška sa týka IEC 60068-2-64: Skúšanie vplyvu prostredia. Časť 2-64: Skúšky. Skúška Fh: Širokopásmové náhodné vibrácie, usmernenia 3. Otrasy: mechanický otras s polsínusom 3g podľa ISO 16750. Uvedená skúška sa vykoná na rôznych vzorkách skúšaného zariadenia.	
4.4	Ochrana proti vode a cudzím telesám	Skúška podľa ISO 20653: Cestné vozidlá – stupeň ochrany (kód IP) – Ochrana elektrických zariadení proti cudzím predmetom, vode a prístupu (bez zmeny parametrov)	220, 221
4.5	Ochrana proti prepätiu	Overí sa, či jednotka vozidla odolá napájaciemu napätiu: Pre verzie 24V: 34 V pri + 40 °C 1 hodinu Pre verzie 12V: 17 V pri + 40 °C 1 hodinu (ISO 16750-2, kapitola 4.3)	216
4.6	Ochrana proti zmene polarity	Overí sa, či jednotka vozidla odolá zmene polarity napájacieho napätia. (ISO 16750-2, kapitola 4.7)	216
4.7	Ochrana proti skratu	Overí sa, či sú vstupné/výstupné signály chránené proti skratu napájania a uzemnenia (ISO 16750-2, kapitola 4.10)	216
5	**Skúšky EMC**		
5.1	Vyžarované emisie a citlivosť	Súlad s predpisom EHK OSN R10 (ECE R10)	218

Č.	Skúška	Opis	Súvisiace požiadavky
5.2	Elektrostatický výboj	Súlad s ISO 10605:2008 + technické korigendum:2010 + AMD1:2014: +/– 4kV na kontaktoch a +/– 8kV pri vzdušnom výboji	218
5.3	Citlivosť na prechodové javy šírené vedením na napájaní	Pre verzie 24V: súlad s ISO 7637-2 + predpisom EHK 10 (ECE 10 Rev. 3): impulz 1a: Vs = – 450V Ri = 50 ohmov impulz 2a: Vs = + 37V Ri = 2 ohmy impulz 2b: Vs = + 20V Ri = 0,05 ohmu impulz 3a: Vs = – 150V Ri = 50 ohmov impulz 3b: Vs = + 150V Ri = 50 ohmov impulz 4: Vs = 16V Va = – 12V t6 = 100ms impulz 5: Vs = + 120V Ri = 2,2 ohmov td = 250ms Pre verzie 12V: súlad s ISO 7637-1 + predpisom EHK 10 (ECE 10 Rev. 3): impulz 1: Vs = – 75V Ri=10 ohmov impulz 2a: Vs = + 37V Ri = 2 ohmy impulz 2b: Vs = + 10V Ri = 0,05 ohmu impulz 3a: Vs = – 112V Ri = 50 ohmov impulz 3b: Vs = + 75V Ri = 50 ohmov impulz 4: Vs = – 6V Va = 5V t6 = 15ms impulz 5: Vs = + 65V Ri = 3 ohmy td = 100ms Impulz 5 sa skúša len v jednotkách vozidiel určených na montáž vo vozidlách bez externej spoločnej ochrany proti poklesu zaťaženia. Pre návrh súvisiaci s poklesom zaťaženia pozri ISO 16750-2, 4. vydanie, kapitola 4.6.4.	218

6. SKÚŠKY DIAĽKOVÉHO KOMUNIKAČNÉHO ZARIADENIA

Č.	Skúška	Opis	Súvisiace požiadavky
1.	**Administratívne preskúmanie**		
1.1	Dokumentácia	Správnosť dokumentácie	
2.	**Vizuálna kontrola**		
2.1.	Súlad s dokumentáciou		
2.2.	Identifikácia/označenie		225, 226
2.3	Materiály		219 až 223

Č.	Skúška	Opis	Súvisiace požiadavky
4.	**Skúšanie vplyvu prostredia**		
4.1	Teplota	Overenie funkčnosti: skúškou podľa ISO 16750-4, kapitoly 5.1.1.2: Skúška prevádzky pri nízkej teplote (72 h pri – 20 °C) Táto skúška sa týka IEC 60068-2-1: Skúšanie vplyvu prostredia. Časť 2-1: Skúšky. Skúška A: Chlad skúškou podľa ISO 16750-4: kapitola 5.1.2.2: Skúška prevádzky pri vysokej teplote (72 h pri 70 °C) Táto skúška sa týka IEC 60068-2-2: Skúšanie vplyvu prostredia. Časť 2: Skúšky. Skúška B: Suché teplo skúškou podľa ISO 16750-4: Kapitola 5.3.2: Rýchla zmena teploty so stanoveným trvaním prechodu (– 20 °C/70 °C, 20 cyklov, čas zotrvania na každej teplote: 1 h (?)) Pri nižšej a vyššej teplote, ako aj počas teplotných cyklov možno vykonať redukovaný súbor skúšok (spomedzi skúšok vymedzených v bode 3 tejto tabuľky)	213
4.4	Ochrana proti vode a cudzím telesám	Skúška podľa ISO 20653: Cestné vozidlá. Stupeň ochrany (kód IP). Ochrana elektrických zariadení proti cudzím predmetom, vode a prístupu (cieľová hodnota IP40)	220, 221
5	**Skúšky EMC**		
5.1	Vyžarované emisie a citlivosť	Súlad s predpisom EHK OSN R10 (ECE R10)	218
5.2	Elektrostatický výboj	Súlad s ISO 10605:2008 + technické korigendum:2010 + AMD1:2014: +/– 4kV na kontaktoch a +/– 8kV pri vzdušnom výboji	218
5.3	Citlivosť na prechodové javy šírené vedením na napájaní	Pre verzie 24V: súlad s ISO 7637-2 + predpisom EHK 10 (ECE 10 Rev. 3): impulz 1a: Vs = – 450V Ri = 50 ohmov impulz 2a: Vs = + 37V Ri = 2 ohmy impulz 2b: Vs = + 20V Ri = 0,05 ohmu impulz 3a: Vs = – 150V Ri = 50 ohmov impulz 3b: Vs = + 150V Ri = 50 ohmov impulz 4: Vs = – 16V Va = – 12V t6 = 100ms impulz 5: Vs = + 120V Ri = 2,2 ohmov td = 250ms	218

Č.	Skúška	Opis	Súvisiace požiadavky
		Pre verzie 12V: súlad s ISO 7637-1 + predpisom EHK 10 (ECE 10 Rev. 3): impulz 1: Vs = – 75V Ri = 10 ohmov impulz 2a: Vs = + 37V Ri = 2 ohmy impulz 2b: Vs = + 10V Ri = 0,05 ohmu impulz 3a: Vs = – 112V Ri = 50 ohmov impulz 3b: Vs = + 75V Ri = 50 ohmov impulz 4: Vs = – 6V Va = – 5V t6 = 15ms impulz 5: Vs = + 65V Ri = 3 ohmy td=100ms Impulz 5 sa skúša len v jednotkách vozidiel určených na montáž vo vozidlách bez externej spoločnej ochrany proti poklesu zaťaženia. Pre návrh súvisiaci s poklesom zaťaženia pozri ISO 16750-2, 4. vydanie, kapitola 4.6.4.	

7. FUNKČNÉ SKÚŠKY PAPIERA

Č.	Skúška	Opis	Súvisiace požiadavky
1.	**Administratívne preskúmanie**		
1.1	Dokumentácia	Správnosť dokumentácie	
2	**Všeobecné skúšky**		
2.1	Počet znakov v každom riadku	Vizuálna kontrola výpisov.	172
2.2	Minimálna veľkosť znakov	Vizuálna kontrola výpisov a kontrola znakov.	173
2.3	Podporované množiny znakov	Tlačiareň musí podporovať znaky uvedené v dodatku 1 kapitole 4 „Množiny znakov“.	174
2.4	Rozlíšenie výpisov	Kontrola typového schválenia tachografu a vizuálna kontrola výpisov	174
2.5	Čitateľnosť a identifikácia výpisov	Kontrola výpisov Dokazujú skúšobné správy a protokoly výrobcu. Na tlačovom papieri sa uvedú homologizačné čísla všetkých tachografov, v ktorých ho možno použiť.	175, 177, 178
2.6	Doplnenie zápisov písaných rukou	Vizuálna kontrola: Je k dispozícii kolónka na vodičov podpis. Sú k dispozícii kolónky na ďalšie zápisy rukou.	180

Č.	Skúška	Opis	Súvisiace požiadavky
2.7	Ďalšie podrobnosti na oboch stranách papiera.	Predná i zadná strana papiera môže obsahovať aj ďalšie podrobnosti a informácie. Tie však nesmú zhoršovať čitateľnosť výpisov. Vizuálna kontrola.	177, 178
3	**Skúšky skladovania**		
3.1	Suché teplo.	Príprava: 16 hodín pri teplote + 23 °C ± 2 °C/relatívna vlhkosť 55 % ± 3 % Skúšobné prostredie: 72 hodín pri + 70 °C ± 2 °C Podmienky po skúške: 16 hodín pri teplote + 23 °C ± 2 °C/ relatívna vlhkosť 55 % ± 3 %	176, 178 IEC 60068-2-2-Bb
2.2	Vlhké teplo	Príprava: 16 hodín pri teplote + 23 °C ± 2 °C/relatívna vlhkosť 55 % ±3 % Skúšobné prostredie: 144 hodín pri teplote + 55 °C ± 2 °C a r. v. 93 % ± 3 % Podmienky po skúške: 16 hodín pri teplote + 23 °C ± 2 °C/ relatívna vlhkosť 55 % ± 3 %	176, 178 IEC 60068-2-78-Cab
4	**Skúšky papiera pri používaní**		
4.1	Odolnosť podkladu voči vlhkosti (nepotlačený papier)	Príprava: 16 hodín pri teplote + 23 °C ± 2 °C/relatívna vlhkosť 55 % ± 3 % Skúšobné prostredie: 144 hodín pri teplote + 55 °C ± 2 °C a r. v. 93 % ± 3 % Podmienky po skúške: 16 hodín pri teplote + 23 °C ± 2 °C/ relatívna vlhkosť 55 % ± 3 %	176, 178 IEC 60068-2-78-Cab
4.2	Potlačiteľnosť	Príprava: 24 hodín pri + 40 °C ± 2 °C/relatívna vlhkosť 93 % ± 3 % Skúšobné prostredie: výpis vytlačený pri + 23 °C ± 2 °C Podmienky po skúške: 16 hodín pri teplote + 23 °C ± 2 °C/ relatívna vlhkosť 55 % ± 3 %	176, 178
4.3	Odolnosť voči teplu	Príprava: 16 hodín pri teplote + 23 °C ± 2 °C/relatívna vlhkosť 55 % ± 3 % Skúšobné prostredie: 2 hodiny pri + 70 °C ± 2 °C, suché teplo Podmienky po skúške: 16 hodín pri teplote + 23 °C ± 2 °C/ relatívna vlhkosť 55 % ± 3 %	176, 178 IEC 60068-2-2-Bb
4.4	Odolnosť voči nízkej teplote	Príprava: 16 hodín pri teplote + 23 °C ± 2 °C/relatívna vlhkosť 55 % ± 3 % Skúšobné prostredie: 24 hodín pri – 20 °C ± 3 °C, suché teplo Podmienky po skúške: 16 hodín pri teplote + 23 °C ± 2 °C/ relatívna vlhkosť 55 % ± 3 %	176, 178 ISO 60068-2-1-Ab

Č.	Skúška	Opis	Súvisiace požiadavky
4.5	Svetelná odolnosť	Príprava: 16 hodín pri teplote + 23 °C ± 2 °C/relatívna vlhkosť 55 % ± 3 % Skúšobné prostredie: 100 hodín pod osvetlením 5 000 Lux pri + 23°C ± 2°C/relatívna vlhkosť 55 % ± 3 % Podmienky po skúške: 16 hodín pri teplote + 23 °C ± 2 °C/ relatívna vlhkosť 55 % ± 3 %	176, 178

Kritériá čitateľnosti pre skúšky 3.x a 4.x:

Výtlačok je čitateľný, ak optická hustota spĺňa tieto limity:

Tlačené znaky: min. 1,0

Podklad (nepotlačený papier): max. 0,2

Optická hustota výsledných výpisov sa meria podľa normy DIN EN ISO 534.

Výpisy nesmú vykazovať žiadne zmeny rozmerov a musia zostať jasne čitateľné.

8. SKÚŠKY INTEROPERABILITY

Č.	Skúška	Opis
		9.1. Skúšky interoperability jednotiek vozidla a tachografových kariet
1	Vzájomná autentifikácia	Overí sa normálny priebeh vzájomnej autentifikácie jednotky vozidla a tachografovej karty.
2	Skúšky zápisu/čítania	Vykonanie typického scenára činnosti na jednotke vozidla. Scenár sa prispôsobí typu skúšanej karty a musí zahŕňať zápis do maximálneho možného počtu EF na karte. Sťahovaním jednotky vozidla sa overí, či sa všetky príslušné údaje zaznamenali správne. Sťahovaním karty sa overí, či sa všetky príslušné údaje zaznamenali správne. Denným výpisom sa overí, či sa dajú všetky príslušné záznamy riadne čítať.
		9.2. Skúšky interoperability jednotiek vozidla a snímačov pohybu
1	Párovanie	Overí sa normálny priebeh párovania jednotky vozidla so snímačom pohybu.
2	Skúšky činnosti	Vykonanie typického scenára činnosti na snímači pohybu. Tento scenár musí zahŕňať bežnú činnosť a vyvolanie čo najväčšieho počtu udalostí alebo porúch. Sťahovaním jednotky vozidla sa overí, či sa všetky príslušné údaje zaznamenali správne. Sťahovaním karty sa overí, či sa všetky príslušné údaje zaznamenali správne. Denným výpisom sa overí, či sa dajú všetky príslušné záznamy riadne čítať.

Č.	Skúška	Opis
9.3. Skúšky interoperability jednotiek vozidla a externých zariadení GNSS (podľa potreby)		
1	Vzájomná autentifikácia	Overí sa normálny priebeh vzájomnej autentifikácie (spojenia) jednotky vozidla a externého zariadenia GNSS.
2	Skúšky činnosti	Vykonanie typického scenára činnosti na externom zariadení GNSS. Tento scenár musí zahŕňať bežnú činnosť a vyvolanie čo najväčšieho počtu udalostí alebo porúch. Sťahovaním jednotky vozidla sa overí, či sa všetky príslušné údaje zaznamenali správne. Sťahovaním karty sa overí, či sa všetky príslušné údaje zaznamenali správne. Denným výpisom sa overí, či sa dajú všetky príslušné záznamy riadne čítať.

Dodatok 10

POŽIADAVKY NA ZABEZPEČENIE

Tento dodatok stanovuje požiadavky IT zabezpečenia systémov inteligentných tachografov (tachografy druhej generácie).

SEC_001 Osvedčeniu zabezpečenia podľa schémy spoločných kritérií podliehajú tieto komponenty inteligentného tachografu:

— jednotka vozidla,

— tachografová karta,

— snímač pohybu,

— externé zariadenie GNSS.

SEC_002 Minimálne požiadavky IT zabezpečenia, ktoré musí spĺňať každý komponent podliehajúci osvedčeniu zabezpečenia, sa vymedzia v profile ochrany komponentu podľa schémy spoločných kritérií.

SEC_003 Európska komisia zaistí, aby sa sponzorovali a vypracovali štyri profily ochrany v súlade s touto prílohou, ktoré schvália vládne orgány osvedčujúce IT zabezpečenie v rámci pracovnej skupiny pre spoločnú interpretáciu (Joint Interpretation Working Group – JIWG) podporujúcej vzájomné uznávanie osvedčení pod záštitou európskej dohody SOGIS-MRA (dohoda o vzájomnom uznávaní osvedčení hodnotenia zabezpečenia informačných technológií), a aby sa tieto profily zaregistrovali:

— profil ochrany pre jednotku vozidla,

— profil ochrany pre tachografovú kartu,

— profil ochrany pre snímač pohybu,

— profil ochrany pre externé zariadenie GNSS.

Profil ochrany pre jednotku vozidla musí počítať s variantmi použitia VU s externým zariadením GNSS aj bez neho. V prvom z uvedených prípadov sa požiadavky na zabezpečenie externého zariadenia GNSS poskytnú v osobitnom profile ochrany.

SEC_004 Výrobcovia komponentov podľa potreby zdokonalia a doplnia príslušný profil ochrany (pričom však nesmú meniť alebo odstraňovať existujúce hrozby, ciele, postupy a funkčné špecifikácie presadzovania zabezpečenia), s cieľom dospieť k cieľu zabezpečenia, na základe ktorého sa bude zabezpečenie daného komponentu osvedčovať.

SEC_005 V procese hodnotenia sa musí stanoviť jednoznačný súlad daného špecifického cieľa zabezpečenia s príslušným profilom ochrany.

SEC_006 Každý profil ochrany musí mať úroveň istoty EAL4 posilnenú o prvky ATE_DPT.2 a AVA_VAN.5.

Dodatok 11

SPOLOČNÉ BEZPEČNOSTNÉ MECHANIZMY

OBSAH

PREAMBULA 340

ČASŤ A TACHOGRAFOVÝ SYSTÉM PRVEJ GENERÁCIE 341

1. ÚVOD 341

1.1. Referenčné dokumenty 341

1.2. Notácie a skratky 341

2. KRYPTOGRAFICKÉ SYSTÉMY A ALGORITMY 343

2.1. Kryptografické systémy 343

2.2. Kryptografické algoritmy 343

2.2.1 Algoritmus RSA 343

2.2.2 Hašovací algoritmus 343

2.2.3 Algoritmus šifrovania údajov 343

3. KĽÚČE A CERTIFIKÁTY 343

3.1. Generovanie a distribúcia kľúčov 343

3.1.1 Generovanie a distribúcia kľúčov RSA 343

3.1.2 Skúšobné kľúče RSA 345

3.1.3 Kľúče snímača pohybu 345

3.1.4 Generovanie a distribúcia T-DES kľúčov relácie 345

3.2. Kľúče 345

3.3. Certifikáty 345

3.3.1 Obsah certifikátov 346

3.3.2 Vydané certifikáty 348

3.3.3 Overenie a rozbalenie certifikátu 349

4. MECHANIZMUS VZÁJOMNEJ AUTENTIFIKÁCIE 349

5. MECHANIZMY DÔVERNOSTI, INTEGRITY A AUTENTIFIKÁCIE PRENOSU ÚDAJOV MEDZI VU A KARTAMI 352

5.1. Zabezpečené spracovanie správ 352

5.2. Spracovanie chýb zabezpečeného spracovania (SM) 354

5.3. Algoritmus na výpočet kryptografických kontrolných súčtov 354

5.4. Algoritmus výpočtu kryptogramov pre dôvernosť dátových objektov 355

6. MECHANIZMY DIGITÁLNEHO PODPISU PRI SŤAHOVANÍ ÚDAJOV 355

6.1. Generovanie podpisu 355

6.2. Overenie podpisu 356

ČASŤ B	TACHOGRAFOVÝ SYSTÉM DRUHEJ GENERÁCIE	357
7.	ÚVOD	357
7.1.	Referenčné dokumenty	357
7.2.	Notácie a skratky	357
7.3.	Vymedzenie pojmov	359
8.	KRYPTOGRAFICKÉ SYSTÉMY A ALGORITMY	359
8.1.	Kryptografické systémy	359
8.2.	Kryptografické algoritmy	360
8.2.1	Symetrické algoritmy	360
8.2.2	Asymetrické algoritmy a štandardizované parametre domény	360
8.2.3	Hašovacie algoritmy	361
8.2.4	Šifrovacie zostavy	361
9.	KĽÚČE A CERTIFIKÁTY	361
9.1.	Asymetrické kľúčové páry a certifikáty verejného kľúča	361
9.1.1	Všeobecné	361
9.1.2	Európska úroveň	362
9.1.3	Úroveň členského štátu	362
9.1.4	Úroveň zariadenia: Jednotky vozidla	363
9.1.5	Úroveň zariadenia: Tachografové karty	365
9.1.6	Úroveň zariadenia: Externé zariadenia GNSS	366
9.1.7	Prehľad: Náhrada certifikátu	367
9.2.	Symetrické kľúče	368
9.2.1	Kľúče na zabezpečenie komunikácie VU – snímač pohybu	368
9.2.2	Kľúče na zabezpečenie komunikácie DSRC	372
9.3.	Certifikáty	375
9.3.1	Všeobecné	375
9.3.2	Obsah certifikátu	375
9.3.3	Žiadosti o certifikáty	377
10.	VZÁJOMNÁ AUTENTIFIKÁCIA VU-KARTA A ZABEZPEČENÉ SPRACOVANIE	378
10.1.	Všeobecné	378
10.2.	Vzájomné overovanie certifikačných reťazcov	379
10.2.1	Overovanie certifikačných reťazcov karty zo strany VU	379
10.2.2	Overovanie certifikačných reťazcov VU kartou	381
10.3.	Autentifikácia VU	384
10.4.	Autentifikácia čipu a kľúčová dohoda relácie	385

10.5. Zabezpečené spracovanie správ 387
10.5.1 Všeobecné 387
10.5.2 Štruktúra zabezpečeného spracovania správ 388
10.5.3 Zrušenie relácie zabezpečeného spracovania 391
11. SPÁJANIE VU S EXTERNÝM ZARIADENÍM GNSS, VZÁJOMNÁ AUTENTIFIKÁCIA A ZABEZPEČENÉ SPRACOVANIE 392
11.1. Všeobecné 392
11.2. Spájanie VU a externého zariadenia GNSS 393
11.3. Vzájomné overovanie certifikačných reťazcov 393
11.3.1 Všeobecné 393
11.3.2 Počas spájania VU – EGF 393
11.3.3 Počas bežnej prevádzky 394
11.4. Autentifikácia VU, autentifikácia čipu a kľúčová dohoda relácie 395
11.5. Zabezpečené spracovanie správ 395
12. PÁROVANIE VU – SNÍMAČ POHYBU A KOMUNIKÁCIA 396
12.1. Všeobecné 396
12.2. Párovanie VU – snímač pohybu pomocou rôznych generácií kľúča 396
12.3. Párovanie VU – snímač pohybu a komunikácia pomocou AES 397
12.4. Párovanie VU – snímač pohybu v prípade rôznych generácií zariadenia 399
13. ZABEZPEČENIE DIAĽKOVEJ KOMUNIKÁCIE CEZ DSRC 399
13.1. Všeobecné 399
13.2. Šifrovanie obsahu tachografu a generácia MAC 400
13.3. Overovanie a dešifrovanie obsahu tachografu 401
14. PODPIS SŤAHOVANIA ÚDAJOV A OVEROVANIE PODPISOV 401
14.1. Všeobecné 401
14.2. Generovanie podpisu 402
14.3. Overenie podpisu 402

PREAMBULA

V tomto dodatku sa špecifikujú mechanizmy zabezpečenia, ktoré zaisťujú:

— vzájomnú autentifikáciu medzi rôznymi komponentmi tachografového systému.

— dôvernosť, integritu, autenticitu a/alebo nespochybniteľnosť údajov prenášaných medzi rôznymi komponentmi systému tachografov alebo stiahnutých na externé pamäťové médium.

Tento dodatok pozostáva z dvoch častí. V časti A sa vymedzujú mechanizmy zabezpečenia tachografového systému prvej generácie (digitálny tachograf). V časti B sa vymedzujú mechanizmy zabezpečenia tachografového systému druhej generácie (inteligentný tachograf).

Mechanizmy uvedené v časti A tohto dodatku sa uplatňujú, ak aspoň jeden z komponentov tachografového systému zapojený do procesu vzájomnej autentifikácie a/alebo prenosu údajov je komponent prvej generácie.

Mechanizmy uvedené v časti B tohto dodatku sa uplatňujú, ak obidva komponenty tachografového systému zapojené do procesu vzájomnej autentifikácie a/alebo prenosu údajov sú komponenty druhej generácie.

Dodatok 15 obsahuje viac informácií o použití komponentov prvej generácie v kombinácii s komponentmi druhej generácie.

ČASŤ A

TACHOGRAFOVÝ SYSTÉM PRVEJ GENERÁCIE

1. ÚVOD

1.1. **Referenčné dokumenty**

V tomto dodatku sa používajú tieto referenčné dokumenty:

SHA-1	Národný inštitút pre normy a technológie USA (NIST). *Publikácia FIPS 180-1: Norma Secure Hash*. Apríl 1995.
PKCS1	RSA Laboratories. PKCS # 1: *Norma šifrovania RSA*. Verzia 2.0. Október 1998.
TDES	Národný inštitút pre normy a technológie USA (NIST). *Publikácia FIPS 46-3: Norma šifrovania údajov*. Návrh 1999.
TDES-OP	ANSI X9.52, Prevádzkové režimy algoritmu trojitého šifrovania údajov. 1998.
ISO/IEC 7816-4	Informačné technológie. Identifikačné karty. Karty s integrovanými obvodmi a s kontaktmi. Časť 4: Medziodborové príkazy pre výmenu. Prvé vydanie: 1995 + zmena 1: 1997.
ISO/IEC 7816-6	Informačné technológie. Identifikačné karty. Karty s integrovanými obvodmi a s kontaktmi. Časť 6: Medziodborové dátové prvky. Prvé vydanie: 1996 + cor. 1: 1998.
ISO/IEC 7816-8	Informačné technológie. Identifikačné karty. Karty s integrovanými obvodmi a s kontaktmi. Časť 8: Medziodborové príkazy vzťahujúce sa k zabezpečeniu. Prvé vydanie: 1999.
ISO/IEC 9796-2	Informačné technológie. Bezpečnostné techniky. Digitálne podpisové mechanizmy umožňujúce obnovu správy. Časť 2: Mechanizmy používajúce hašovaciu funkciu. Prvé vydanie: 1997.
ISO/IEC 9798-3	Informačné technológie. Bezpečnostné techniky. Mechanizmus overovania entít. Časť 3: Overovanie entít pomocou algoritmu verejného kľúča. Druhé vydanie 1998.
ISO 16844-3	Cestné vozidlá. Tachografové systémy. Časť 3: Rozhranie snímača pohybu.

1.2. **Notácie a skratky**

V tomto dodatku sa použili tieto notácie a skratky:

(K_a, K_b, K_c)	Zväzok kľúčov, ktorý používa algoritmus trojitého šifrovania údajov,
CA	Certifikačná autorita (Certification Authority)
CAR	Referencia certifikačnej autority (Certification Authority Reference)
CC	Kryptografický kontrolný súčet (Cryptographic Checksum)
CG	Kryptogram (Cryptogram)
CH	Záhlavie príkazu (Command Header)
CHA	Autorizácia držiteľa certifikátu (Certificate Holder Authorisation)
CHR	Referencia držiteľa certifikátu (Certificate Holder Reference)
D()	Dešifrovanie s DES (Decryption with DES)

DE	Dátový prvok (Data Element)
DO	Dátový objekt (Data Object)
d	Súkromný kľúč RSA, súkromný exponent (RSA private key, private exponent)
e	Verejný kľúč RSA, verejný exponent (RSA public key, public exponent)
E()	Šifrovanie s DES (Encryption with DES)
EQT	Zariadenie (Equipment)
Hash()	Hašovacia hodnota, výstup *Hash* (hash value)
Hash	Hašovacia funkcia (hash function)
KID	Identifikátor kľúča (Key Identifier)
Km	Kľúč TDES Hlavný kľúč podľa ISO 16844-3.
Km_{VU}	Kľúč TDES zavedený v jednotkách vozidla.
Km_{WC}	Kľúč TDES zavedený v dielenských kartách.
m	Reprezentant správy, číslo medzi 0 a *n*-1 (message representative)
n	Kľúče RSA, modul (RSA keys, modulus)
PB	Výplňové bajty (Padding Bytes)
PI	Bajt indikátora výplne (použitie v kryptograme pre dôvernosť dátových objektov) (Padding Indicator byte)
PV	Nezašifrovaná hodnota (Plain Value)
s	Reprezentant podpisu, číslo medzi 0 a *n*-1 (signature representative)
SSC	Počítadlo sekvencie odosielania (Send Sequence Counter)
SM	Zabezpečené spracovanie správ (Secure Messaging)
TCBC	Prevádzkový režim reťazenia šifrovacieho bloku TDEA (TDEA Cipher Block Chaining Mode of Operation)
TDEA	Algoritmus trojitého šifrovania údajov (Triple Data Encryption Algorithm)
TLV	Hodnota dĺžky tagu (Tag Length Value)
VU	Jednotka vozidla (Vehicle Unit)
X.C	Certifikát používateľa X vydaný certifikačnou autoritou
X.CA	Certifikačná autorita používateľa X
X.CA.PK $_{o}$ X.C	Priebeh rozbaľovania certifikátu na získanie verejného kľúča. Ide o infixový operátor, ktorého ľavý operand je verejným kľúčom certifikačnej autority, a pravý operand je certifikátom vydaným touto certifikačnou autoritou. Výsledkom je verejný kľúč používateľa X, ktorého certifikát predstavuje pravý operand
X.PK	Verejný kľúč RSA používateľa X
X.PK[I]	RSA šifrovanie niektorých informácií I, s použitím verejného kľúča používateľa X
X.SK	Súkromný kľúč RSA používateľa X
X.SK[I]	RSA šifrovanie niektorých informácií I, s použitím súkromného kľúča používateľa X
‘xx’	Hexadecimálna hodnota
||	Operátor zreťazenia.

2. KRYPTOGRAFICKÉ SYSTÉMY A ALGORITMY

2.1. **Kryptografické systémy**

CSM_001 Jednotky vozidla a tachografové karty musia používať klasický kryptografický systém verejného kľúča RSA tak, aby boli k dispozícii tieto mechanizmy zabezpečenia:

— autentifikácia medzi jednotkami vozidla a kartami,

— prenos trojnásobných DES kľúčov relácie medzi jednotkami vozidla a tachografovými kartami,

— digitálny podpis údajov stiahnutých z jednotiek vozidla alebo tachografových kariet na externé médiá.

CSM_002 Jednotky vozidla a tachografové karty musia používať symetrický trojnásobný DES kryptografický systém tak, aby bol k dispozícii mechanizmus pre zabezpečenie integrity údajov počas výmeny používateľských údajov medzi jednotkami vozidla a tachografovými kartami, a aby bola podľa potreby zabezpečená dôvernosť výmeny údajov medzi jednotkami vozidla a tachografovými kartami.

2.2. **Kryptografické algoritmy**

2.2.1 *Algoritmus RSA*

CSM_003 Algoritmus RSA je úplne definovaný týmito vzťahmi:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

Podrobnejší opis funkcie RSA sa nachádza v referenčnom dokumente [PKCS1]. Verejný exponent, e, pre výpočet RSA je číslo medzi 3 a n-1 spĺňajúce gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Hašovací algoritmus*

CSM_004 Mechanizmy digitálneho podpisu musia používať hašovací algoritmus SHA-1, ako je vymedzený v referenčnom dokumente [SHA-1].

2.2.3 *Algoritmus šifrovania údajov*

CSM_005 Algoritmy založené na DES sa používajú v prevádzkovom režime reťazenia šifrovacieho bloku (Cipher Block Chaining).

3. KĽÚČE A CERTIFIKÁTY

3.1. **Generovanie a distribúcia kľúčov**

3.1.1 *Generovanie a distribúcia kľúčov RSA*

CSM_006 Kľúče RSA sa musia generovať na troch funkčne hierarchických úrovniach:

— európskej úrovni,

— úrovni členského štátu,

— úrovni zariadenia.

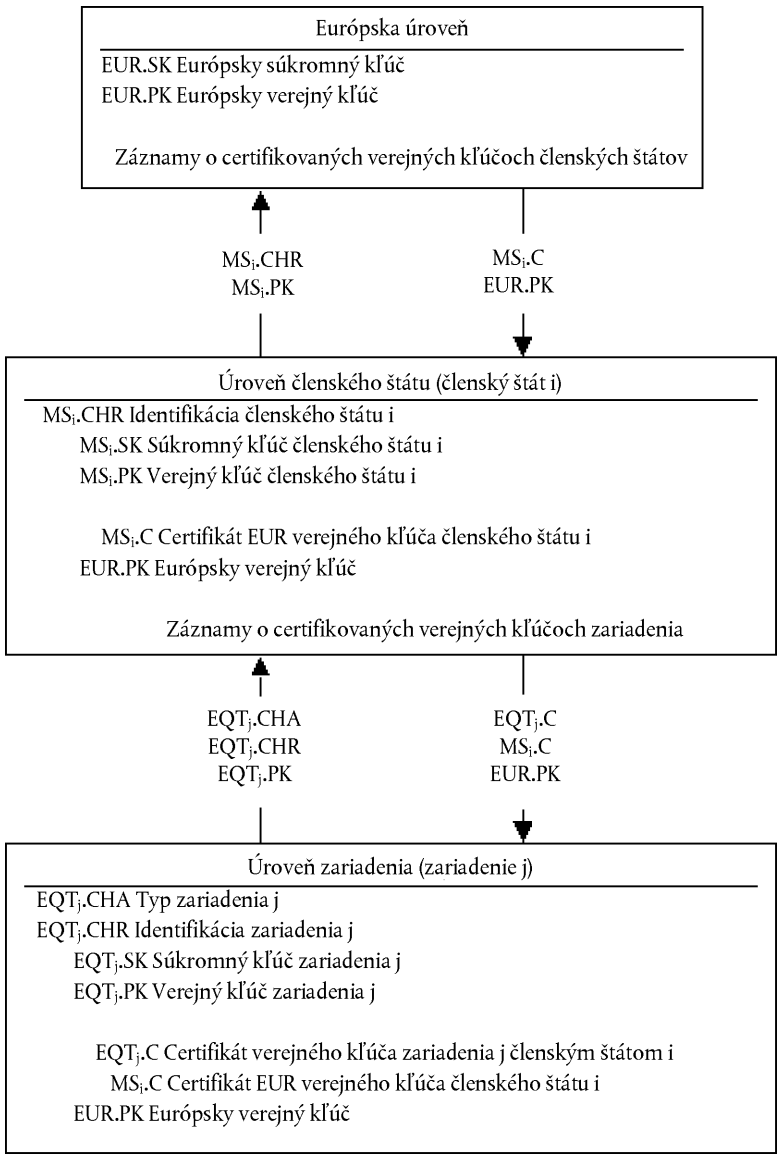
CSM_007 Na európskej úrovni sa generuje jeden európsky kľúčový pár (EUR.SK a EUR.PK). Európsky súkromný kľúč sa použije na certifikovanie verejných kľúčov členských štátov. Musia sa uchovávať záznamy všetkých certifikovaných kľúčov. Tieto úlohy plní európska certifikačná autorita, ktorá podlieha Európskej komisii a je pod jej zodpovednosťou.

CSM_008 Na úrovni členského štátu sa generuje jeden kľúčový pár členského štátu (MS.SK a MS.PK). Verejné kľúče členských štátov musia byť certifikované európskou certifikačnou autoritou. Súkromný kľúč členského štátu sa musí používať na certifikovanie verejných kľúčov, ktoré sa majú zaviesť do zariadenia (jednotka vozidla alebo tachografová karta). Musia sa uchovávať záznamy všetkých certifikovaných verejných kľúčov spolu s identifikáciou zariadenia, pre ktoré sú určené. Tieto úlohy plní certifikačná autorita členského štátu. Členský štát môže pravidelne meniť svoj kľúčový pár.

CSM_009 Na úrovni zariadenia sa generuje jeden kľúčový pár (EQT.SK a EQT.PK) a zavedie sa do každého zariadenia. Verejné kľúče zariadenia musia byť certifikované certifikačnou autoritou členského štátu. Tieto úlohy môžu plniť výrobcovia zariadenia, personalizátori zariadenia alebo orgány členského štátu. Tento kľúčový pár sa používa na autentifikáciu, digitálny podpis a šifrovacie služby.

CSM_010 Dôvernosť súkromných kľúčov sa musí zachovať počas generovania, (prípadného) prenosu a uloženia.

Na tomto obrázku je zhrnutý dátový tok tohto procesu:



3.1.2 *Skúšobné kľúče RSA*

CSM_011 Na skúšanie zariadenia (vrátane skúšok interoperability) musí európska certifikačná autorita vygenerovať osobitný jednotný európsky skúšobný kľúčový pár a aspoň dva skúšobné kľúčové páry členského štátu, ktorých verejné kľúče musia byť certifikované európskym súkromným skúšobným kľúčom. Výrobcovia musia zaviesť do zariadenia podliehajúceho schvaľovacím skúškam skúšobné kľúče certifikované jedným z týchto skúšobných kľúčov členského štátu.

3.1.3 *Kľúče snímača pohybu*

Dôvernosť troch trojnásobných DES kľúčov opísaných ďalej sa musí náležite uchovávať počas generovania, (prípadného) prenosu a uloženia.

Na zaručenie zhody komponentov tachografu s ISO 16844 musia európska certifikačná autorita a certifikačné autority členského štátu okrem toho zabezpečiť toto:

CSM_036 Európska certifikačná autorita vygeneruje KmVU a KmWC, dva nezávislé a jedinečné trojnásobné DES kľúče a vygeneruje Km ako: $Km = Km_{VU}$ XOR Km_{WC} . Európska certifikačná autorita musí, pomocou vhodne zabezpečeného postupu, na požiadanie odoslať tieto kľúče certifikačným autoritám členských štátov.

CSM_037 Certifikačné autority členských štátov:

— musia použiť Km na zašifrovanie údajov snímača pohybu, ktoré vyžadujú výrobcovia snímača pohybu (údaje, ktoré sa majú zašifrovať s Km, sú definované v ISO 16844-3),

— pošlú Km_{VU} pomocou vhodne zabezpečeného postupu výrobcom jednotiek vozidla na účely jeho zavedenia do jednotiek vozidla,

— zabezpečia, aby Km_{WC} bol zavedený vo všetkých dielenských kartách (`SensorInstallationSecData` v elementárnom súbore `Sensor_Installation_Data`) počas personalizácie karty.

3.1.4 *Generovanie a distribúcia T-DES kľúčov relácie*

CSM_012 Jednotky vozidla a tachografové karty musia, v rámci vzájomného procesu autentifikácie, generovať a vymieňať si údaje nevyhnutné na zhotovenie spoločného trojnásobného DES kľúča relácie. Táto výmena údajov musí byť chránená z hľadiska dôvernosti šifrovacím mechanizmom RSA.

CSM_013 Tento kľúč sa použije na všetky následné kryptografické operácie s použitím zabezpečeného spracovania. Jeho platnosť sa skončí na konci relácie (vytiahnutie karty alebo resetovanie karty) a/alebo po 240. použití (jedno použitie kľúča = jeden príkaz používajúci zabezpečené spracovanie odoslaný na kartu a príslušná odpoveď).

3.2. **Kľúče**

CSM_014 Kľúče RSA musia mať (na ktorejkoľvek úrovni) túto dĺžku: modul *n* 1 024 bitov, verejný exponent *e* maximálne 64 bitov, súkromný exponent *d* 1 024 bitov.

CSM_015 Trojnásobné DES kľúče musia mať formu (K_a, K_b, K_a) kde K_a a K_b sú nezávislé kľúče s dĺžkou 64 bitov. Nenastavia sa žiadne bity na zisťovanie chýb parity.

3.3. **Certifikáty**

CSM_016 Certifikáty verejného kľúča RSA nesmú byť „samoopisné“ a musia byť „kartou overiteľné“ (referenčný dokument: ISO/IEC 7816-8)

3.3.1 *Obsah certifikátov*

CSM_017 Certifikáty verejného kľúča RSA pozostávajú z týchto údajov v tomto poradí:

Údaje	Formát	Bajty	Poznámky
CPI	INTEGER (celé číslo)	1	Identifikátor profilu certifikátu ('01' pre túto verziu)
CAR	OCTET STRING (oktetový reťazec)	8	Referencia certifikačnej autority
CHA	OCTET STRING	7	Autorizácia držiteľa certifikátu
EOV	TimeReal	4	Koniec platnosti certifikátu. Nepovinné, ak sa nepoužije, vyplní sa s „FF“.
CHR	OCTET STRING	8	Referencia držiteľa certifikátu
n	OCTET STRING	128	Verejný kľúč (modul)
e	OCTET STRING	8	Verejný kľúč (verejný exponent)
		164	

Poznámky:

1. „Identifikátor profilu certifikátu“ (CPI) ohraničuje presnú štruktúru autentifikačného certifikátu. Môže sa použiť ako vnútorný identifikátor zariadenia príslušného zoznamu záhlaví, ktorý popisuje zreťazenie dátových prvkov v rámci certifikátu.

   Zoznam záhlaví pre tento obsah certifikátu je takýto:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Tag rozšíreného zoznamu záhlaví	Dĺžka zoznamu záhlaví	CPI Tag	Dĺžka CPI	CAR Tag	Dĺžka CAR	CHA Tag	Dĺžka CHA	EOV Tag	Dĺžka EOV	CHR Tag	Dĺžka CHR	Tag verejného kľúča (zostavený)	Dĺžka následných dátových objektov	Tag modulu	Dĺžka modulu	Tag verejného exponentu	Dĺžka verejného exponentu

2. „Referencia certifikačnej autority“ (CAR) má za účel identifikovať CA vydávajúcu certifikát tak, aby sa dátový prvok mohol použiť v rovnakom čase ako identifikátor kľúča autority na referenciu verejného kľúča certifikačnej autority (pre kódovanie pozri identifikátor kľúča ďalej).

3. „Autorizácia držiteľa certifikátu“ (CHA) sa používa na identifikovanie práv držiteľa certifikátu. Pozostáva z ID tachografovej aplikácie a typu zariadenia, ktorému je certifikát určený (podľa dátového prvku `EquipmentType`, ‘00’ pre členský štát).

4. „Referencia držiteľa certifikátu“ (CHR) má za účel identifikovať jednoznačne držiteľa certifikátu tak, aby sa dátový prvok mohol použiť v rovnakom čase ako identifikátor kľúča subjektu na referenciu verejného kľúča držiteľa certifikátu.

5. Identifikátory kľúča jedinečne identifikujú držiteľa certifikátu alebo certifikačné autority. Sú kódované takto:

5.1 Zariadenie (VU alebo karta):

Údaje	Sériové číslo zariadenia	Dátum	Typ	Výrobca
Dĺžka	4 bajty	2 bajty	1 bajt	1 bajt
Hodnota	Celé číslo	mm rr BCD kódovanie	Špecifické pre výrobcu	Kód výrobcu

V prípade VU výrobca pri žiadosti o certifikáty môže, ale nemusí poznať identifikáciu zariadenia, v ktorom majú byť kľúče zavedené.

V prvom prípade výrobca pošle identifikáciu zariadenia s verejným kľúčom na certifikáciu certifikačnej autority svojho členského štátu. Certifikát potom bude obsahovať identifikáciu zariadenia a výrobca musí zabezpečiť, aby boli kľúče a certifikát zavedené do príslušného zariadenia. Podoba identifikátora kľúča je uvedená vyššie.

V druhom prípade výrobca musí jedinečne identifikovať každú žiadosť o certifikát a poslať túto identifikáciu s verejným kľúčom na certifikáciu autorite svojho členského štátu. Tento certifikát bude obsahovať identifikáciu žiadosti. Výrobca musí autorite svojho členského štátu po inštalovaní kľúča v zariadení oznámiť priradenie kľúča k zariadeniu (t. j. identifikáciu žiadosti o certifikát, identifikáciu zariadenia). Identifikátor kľúča má túto podobu:

Údaje	Sériové číslo žiadosti o certifikát	Dátum	Typ	Výrobca
Dĺžka	4 bajty	2 bajty	1 bajt	1 bajt
Hodnota	Celé číslo	mm rr BCD kódovanie	‘FF’	Kód výrobcu

5.2. Certifikačná autorita:

Údaje	Identifikácia orgánu	Sériové číslo kľúča	Doplňujúce informácie	Identifikátor
Dĺžka	4 bajty	1 bajt	2 bajty	1 bajt

Hodnota	Numerický kód členského štátu – 1 bajt Alfanumerický kód členského štátu – 3 bajty	Celé číslo	Doplnkový kód (podľa CA) 'FF FF', ak sa nepoužíva	'01'

Sériové číslo kľúča sa používa na rozlíšenie rôznych kľúčov členského štátu v prípade zmeny kľúča.

6. Verifikátor certifikátu implicitne vie, že pri certifikovanom verejnom kľúči ide o kľúč RSA relevantný pre autentifikáciu, overenie digitálneho podpisu a šifrovanie v rámci služieb dôvernosti (certifikát neobsahuje žiadny objektový identifikátor pre jeho špecifikáciu).

3.3.2 *Vydané certifikáty*

CSM_018 Vydaný certifikát je digitálnym podpisom s čiastočne obnoviteľným obsahom certifikátu v súlade s normou ISO/IEC 9796-2 (s výnimkou jej prílohy A4), s priloženou „referenciou certifikačnej autority".

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, Hash(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

s obsahom certifikátu = Cc = C_r || C_n

106 bajtov 58 bajtov

Poznámky:

1. Tento certifikát má dĺžku 194 bajtov.

2. CAR skrytá podpisom je tiež priložená k podpisu tak, aby na overenie certifikátu mohol byť zvolený verejný kľúč certifikačnej autority.

3. Verifikátor certifikátu implicitne pozná algoritmus použitý certifikačnou autoritou na podpis certifikátu.

4. Zoznam záhlaví pre tento vydaný certifikát je takýto:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Tag certifikátu CV (zostavený)	Dĺžka následných dátových objektov	Tag podpisu	Dĺžka podpisu	Tag zostatku	Dĺžka zostatku	CAR Tag	Dĺžka CAR

3.3.3 *Overenie a rozbalenie certifikátu*

Overenie a rozbalenie certifikátu pozostáva z overenia podpisu v súlade s ISO/IEC 9796-2, vyvolania obsahu certifikátu a obsiahnutého verejného kľúča: X.PK = X.CA.PK $_o$ X.C, a overenie platnosti certifikátu.

CSM_019 Zahŕňa tieto kroky:

Overenie podpisu a vyvolanie obsahu:

— z X.C vyvolanie Sign, C_n' a CAR': X.C = Sign || C_n' || CAR'

128 bajtov 58 bajtov 8 bajtov

— z CAR' sa vyberie vhodný verejný kľúč certifikačnej autority (ak sa nevykonalo predtým inými prostriedkami)

— otvorenie Sign s verejným kľúčom CA: Sr'= X.CA.PK [Sign],

— kontrola Sr' sa začína s '6A' a končí s 'BC'

— výpočet C_r' a H' z: Sr' = '6 A' || C_r' || H' || 'BC'

106 bajtov 20 bajtov

— Opätovné zhotovenie obsahu certifikátu C' = C_r' || C_n',

— kontrola *Hash*(C') = H'

Ak sú kontroly v poriadku, certifikát je pravý a jeho obsah je C'.

Overenie platnosti. Z C':

— v prípade potreby kontrola dátumu skončenia platnosti,

Vyvolanie a uloženie verejného kľúča, identifikátora kľúča, autorizácie držiteľa certifikátu a skončenia platnosti certifikátu z C':

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECHANIZMUS VZÁJOMNEJ AUTENTIFIKÁCIE

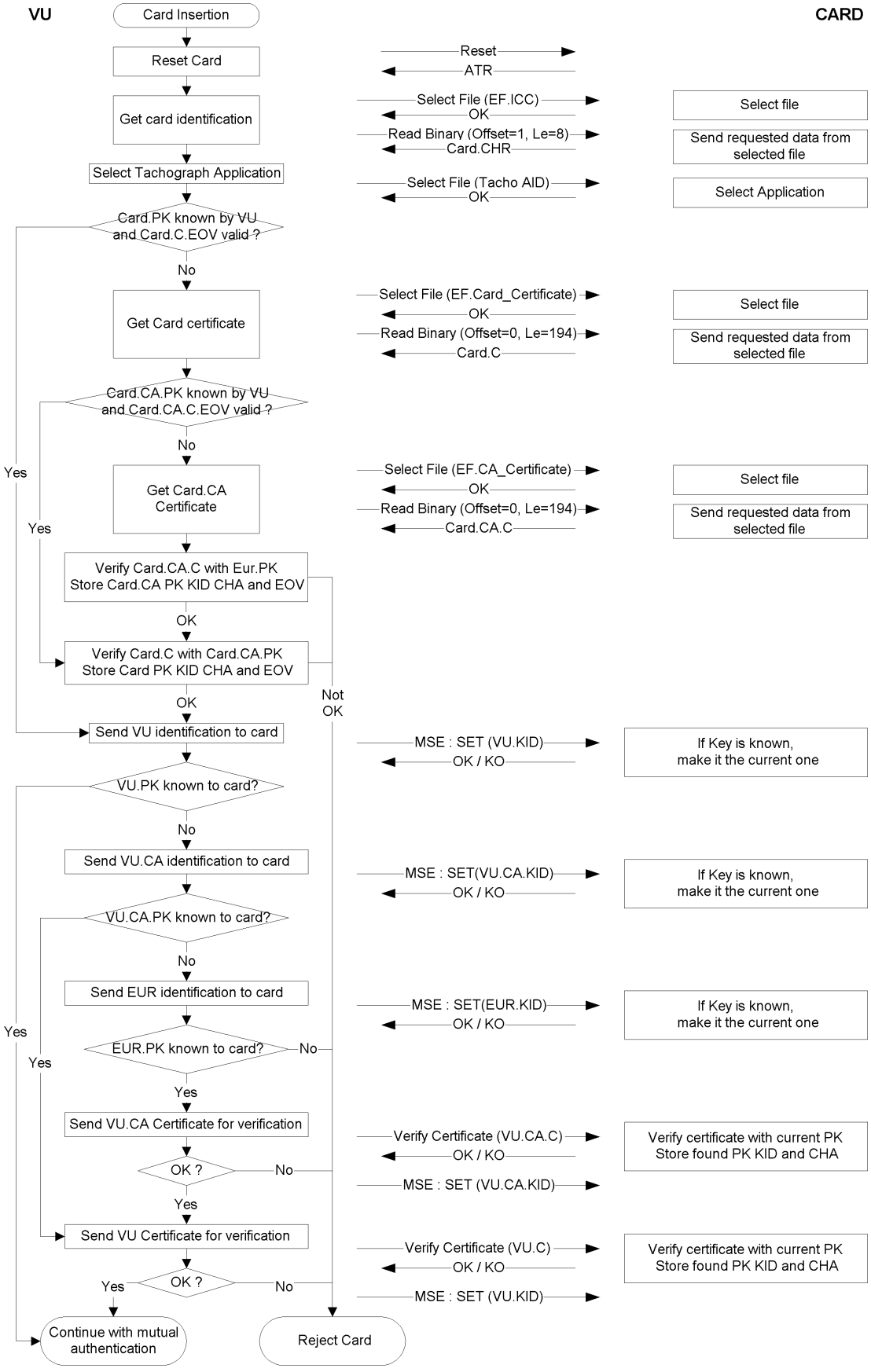
Vzájomná autentifikácia medzi kartami a VU je založená na týchto princípoch:

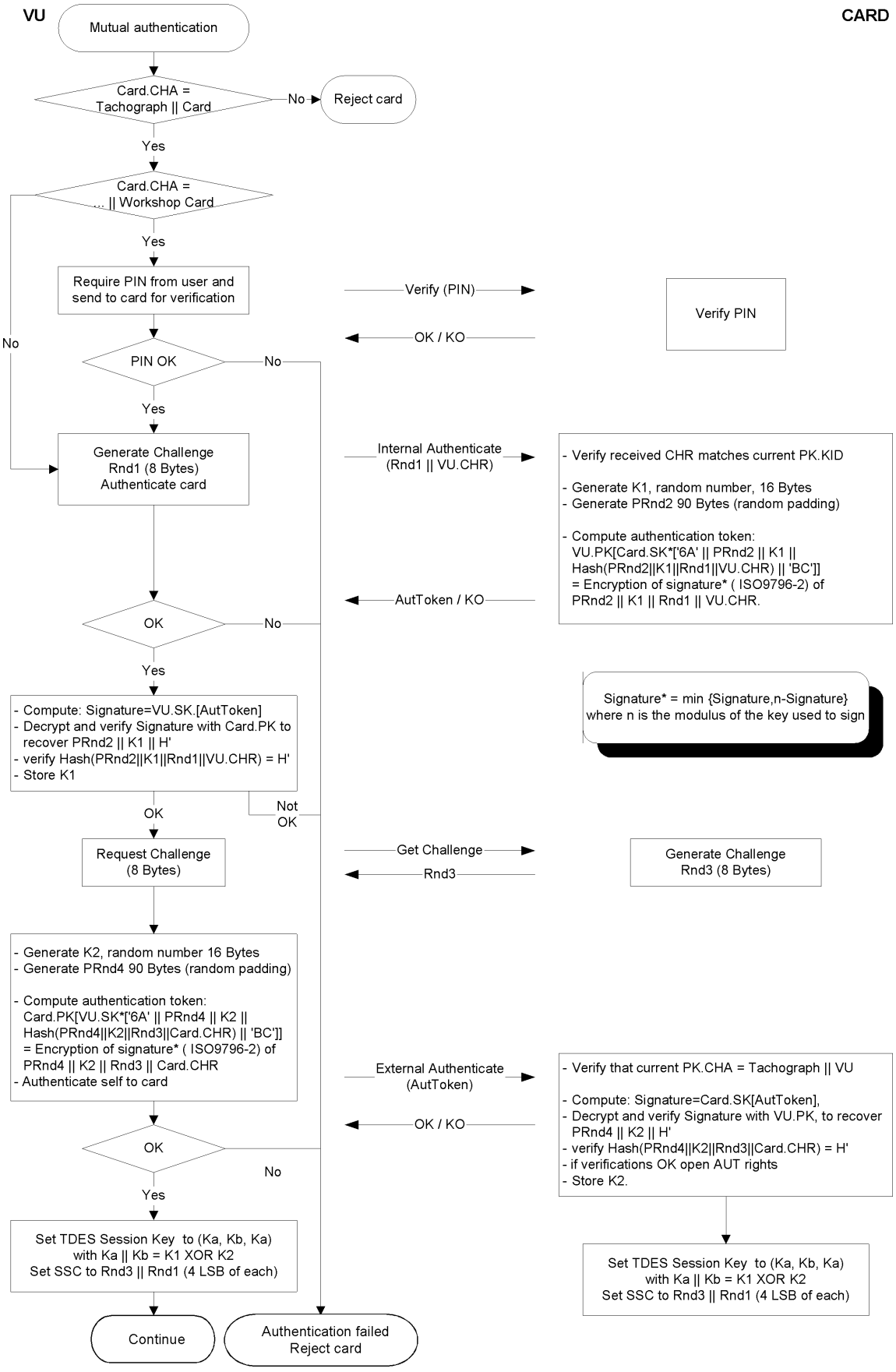
Každá strana preukáže druhej strane, že vlastní platný pár kľúčov, ktorého verejný kľúč bol certifikovaný certifikačnou autoritou členského štátu, ktorá samotná bola certifikovaná európskou certifikačnou autoritou.

Preukazuje sa podpisom súkromným kľúčom na náhodnom čísle od druhej strany, ktorá musí toto náhodné číslo dostať späť pri overovaní daného podpisu.

Mechanizmus spustí VU pri vložení karty. Začne sa výmenou certifikátov a rozbaľovaním verejných kľúčov a končí sa nastavením kľúča relácie.

CSM_020 Použije sa tento protokol (šípky označujú príkazy a vymieňané údaje (pozri dodatok 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. MECHANIZMY DÔVERNOSTI, INTEGRITY A AUTENTIFIKÁCIE PRENOSU ÚDAJOV MEDZI VU A KARTAMI

5.1. **Zabezpečené spracovanie správ**

CSM_021 Integrita prenosu údajov medzi VU a kartami je chránená zabezpečeným spracovaním v súlade s referenčnými dokumentmi [ISO/IEC 7816-4] a [ISO/IEC 7816-8].

CSM_022 Keď musia byť údaje počas prenosu chránené, v rámci príkazu alebo odpovede sa k odoslaným dátovým objektom pripojí dátový objekt „kryptografický kontrolný súčet“. Kryptografický kontrolný súčet overuje prijímateľ.

CSM_023 Kryptografický kontrolný súčet údajov odoslaných v rámci príkazu integruje záhlavie príkazu a všetky odoslané dátové objekty (=>CLA = '0C' a všetky dátové objekty musia byť uzavreté tagmi, pričom b1 = 1).

CSM_024 Keď odpoveď neobsahuje žiadne dátové pole, musia byť bajty týkajúce sa informácií o stave odpovede chránené kryptografickým kontrolným súčtom.

CSM_025 Kryptografický kontrolný súčet musí mať dĺžku štyri bajty.

Štruktúra príkazov a odpovedí pri použití zabezpečeného spracovania je preto takáto:

Použité dátové objekty sú podmnožinou dátových objektov zabezpečeného spracovania opísaných v ISO/IEC 7816-4:

Tag	Mnemotechnická skratka	Význam
'81'	T_{PV}	Nezašifrovaná hodnota nekódovaná v BER-TLV (chránená prostredníctvom CC)
'97'	$\mathbf{T_{LE}}$	Hodnota Le v nezabezpečenom príkaze (chránená prostredníctvom CC)
'99'	T_{SW}	Status-Info (chránená prostredníctvom CC)
'8E'	T_{CC}	Kryptografický kontrolný súčet
'87'	$T_{PI\ CG}$	Bajt indikátora výplne || Kryptogram (nezašifrovaná hodnota nekódovaná v BER-TLV)

Vychádzajúc z nezabezpečeného páru príkaz – odpoveď:

Záhlavie príkazu				Telo príkazu		
CLA	INS	P1	P2	[L_c pole]	[Dátové pole]	[L_e pole]
štyri bajty				Bajty L, označené ako B_1 až B_L		

Telo odpovede	Koncový znak odpovede	
[Dátové pole]	SW1	SW2
Dátové bajty L_r	dva bajty	

Zodpovedajúci zabezpečený pár príkaz – odpoveď je:

Zabezpečený príkaz:

Záhlavie príkazu (CH)				Telo príkazu										
CLA	INS	P1	P2	[Nové L_c pole]	[Nové dátové pole]									[Nové L_e pole]
'OC'				Dĺžka nového dátového poľa	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
					'81'	L_c	Dátové pole	'97'	'01'	L_e	'8E'	'04'	CC	

Údaje, ktoré sa majú integrovať v kontrolnom súčte = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Výplňové bajty (80 .. 00) podľa ISO/IEC 7816-4 a ISO 9797, metóda 2.

Dátové objekty PV a LE sú prítomné len keď existujú nejaké zodpovedajúce údaje v nezabezpečenom príkaze.

Zabezpečená odpoveď:

1. Keď dátové pole odpovede nie je prázdne a nemusí byť chránené vzhľadom na dôvernosť:

Telo odpovede						Koncový znak odpovede
[Nové dátové pole]						nové SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Dátové pole	'8E'	'04'	CC	

Údaje, ktoré sa majú integrovať v kontrolnom súčte = T_{PV} || L_{PV} || PV || PB

2. Keď dátové pole odpovede nie je prázdne a musí byť chránené vzhľadom na dôvernosť:

Telo odpovede						Koncový znak odpovede
[Nové dátové pole]						nové SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Údaje v CG: údaje nekódované v BER-TLV a výplňové bajty.

Údaje, ktoré sa majú integrovať v kontrolnom súčte = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Keď je dátové pole odpovede prázdne:

Telo odpovede						Koncový znak odpovede
[Nové dátové pole]						nové SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Nové SW1 SW2	'8E'	'04'	CC	

Údaje, ktoré sa majú integrovať v kontrolnom súčte = T_{SW} || L_{SW} || SW || PB

5.2. **Spracovanie chýb zabezpečeného spracovania (SM)**

CSM_026 Keď tachografová karta rozpozná chybu SM pri interpretácii príkazu, stavové bajty sa musia vrátiť bez SM. V súlade s ISO/IEC 7816-4 sú definované tieto stavové bajty na označenie chýb SM:

'66 88': overenie kryptografického kontrolného súčtu zlyhalo,

'69 87': chýbajú očakávané dátové objekty SM,

'69 88': nesprávne dátové objekty SM.

CSM_027 Keď tachografová karta vráti stavové bajty bez dátových objektov SM alebo s chybnými dátovými objektmi SM, VU musí reláciu ukončiť.

5.3. **Algoritmus na výpočet kryptografických kontrolných súčtov**

CSM_028 Kryptografické kontrolné súčty sú zostavené pomocou bežných MAC v súlade s ANSI X9.19 s DES:

— východisková etapa: počiatočný kontrolný blok y0 je E(Ka, SSC).

— nasledujúca etapa: Kontrolné bloky y1, .., yn sa vypočítajú s použitím Ka.

— konečná etapa: kryptografický kontrolný súčet sa vypočíta z posledného kontrolného bloku yn takto: E(Ka, D(Kb, yn)).

E() znamená šifrovanie s DES a D() znamená dešifrovanie s DES.

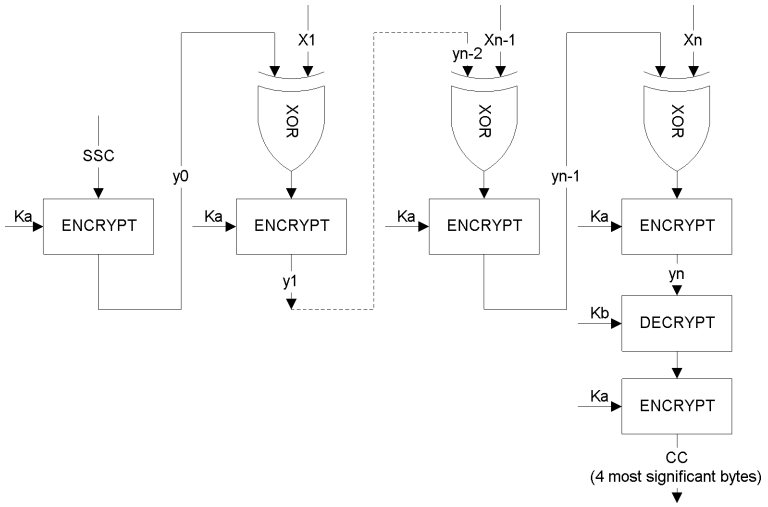
Prenášajú sa štyri bajty najvyššieho rádu kryptografického kontrolného súčtu.

CSM_029 Počítadlo sekvencie odosielania (SSC) sa iniciuje počas postupu kľúčovej dohody takto:

Počiatočné SSC: Rnd3 (4 bajty najnižšieho rádu) || Rnd1 (4 bajty najnižšieho rádu).

CSM_030 Počítadlo sekvencie odosielania sa musí zvýšiť o 1 vždy pred výpočtom MAC (t. j. SSC pre prvý príkaz je počiatočné SSC + 1, SSC pre prvú odpoveď je počiatočné SSC + 2).

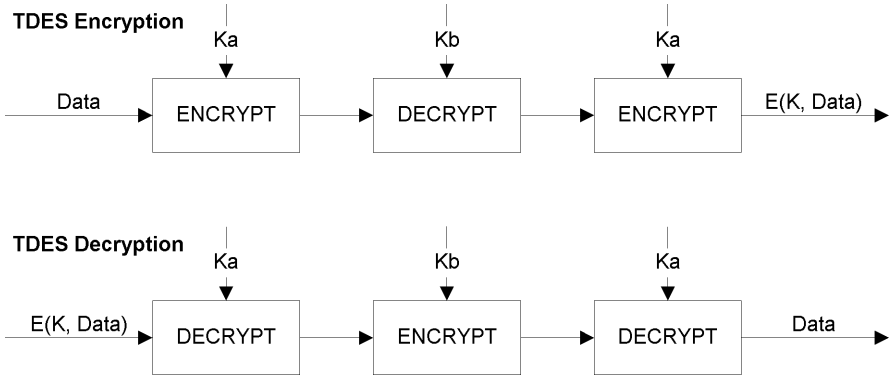
Tento obrázok ukazuje výpočet MAC:



5.4. Algoritmus výpočtu kryptogramov pre dôvernosť dátových objektov

CSM_031 Kryptogramy sa vypočítajú s použitím TDEA v prevádzkovom režime TCBC v súlade s referenčnými dokumentmi (TDES) a (TDES-OP) a nulovým vektorom ako počiatočný blok hodnôt (Initial Value Block).

Tento obrázok ukazuje aplikáciu kľúčov v TDES:



6. MECHANIZMY DIGITÁLNEHO PODPISU PRI SŤAHOVANÍ ÚDAJOV

CSM_032 Inteligentné vyhradené zariadenie (IDE) uchováva údaje prijímané zo zariadenia (VU alebo karty) počas jednej relácie sťahovania v jednom fyzickom dátovom súbore. Tento súbor musí obsahovať certifikáty MS_i.C a EQT.C. Súbor obsahuje digitálne podpisy dátových blokov, ako je špecifikované v dodatku 7 Protokoly sťahovania údajov.

CSM_033 Digitálne podpisy stiahnutých údajov musia použiť digitálny podpisový systém s dodatkom tak, aby sa stiahnuté údaje podľa potreby dali čítať bez dešifrovania.

6.1. Generovanie podpisu

CSM_034 Generovanie dátového podpisu zariadením sa musí vykonať podľa podpisového systému s dodatkom, ktorý je definovaný v referenčnom dokumente [PKCS1], s hašovacou funkciou SHA-1:

Podpis = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = výplňový reťazec oktetov s hodnotou 'FF' tak, aby bola dĺžka 128.

DER(SHA-1(*M*)) je kódovanie ID algoritmu pre hašovaciu funkciu a hašovaciu hodnotu na hodnotu ASN.1 typu DigestInfo (odlíšené kódovacie pravidlá – DER):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Hašovacia hodnota.

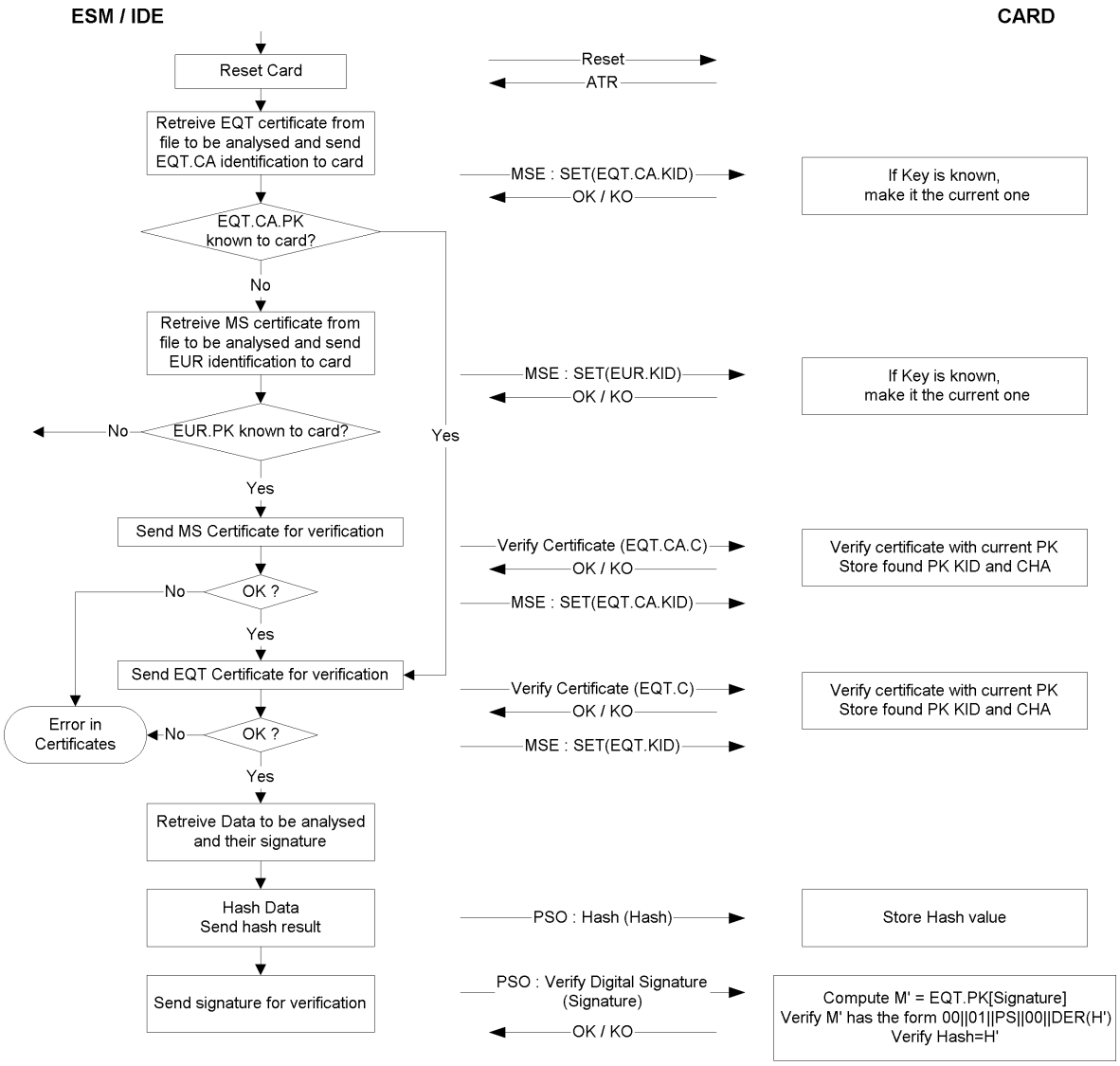
6.2. **Overenie podpisu**

CSM_035 Overenie podpisu stiahnutých údajov sa musí vykonať podľa podpisového systému s dodatkom, ktorý je definovaný v referenčnom dokumente [PKCS1], s hašovacou funkciou SHA-1.

Európsky verejný kľúč EUR.PK musí verifikátor poznať nezávisle (a dôverovať mu).

V tejto tabuľke je znázornený protokol, ktorým sa IDE s kontrolnou kartou môže riadiť pri overovaní integrity stiahnutých údajov ukladaných na ESM (externé pamäťové médium). Kontrolná karta sa používa na dešifrovanie digitálnych podpisov. Táto funkcia nesmie byť v tomto prípade implementovaná v IDE.

Zariadenie, ktoré stiahlo a podpísalo údaje, ktoré sa majú analyzovať, je označené ako EQT.



ČASŤ B

TACHOGRAFOVÝ SYSTÉM DRUHEJ GENERÁCIE

7. ÚVOD

7.1. **Referenčné dokumenty**

V tejto časti tohto dodatku sa používajú tieto referenčné dokumenty:

AES	Národný inštitút pre normy a technológie USA (NIST), FIPS PUB 197: Štandard pokročilého šifrovania (AES), 26. novembra 2001.
DSS	Národný inštitút pre normy a technológie USA (NIST), FIPS PUB 186-4: Štandard digitálneho podpisu (DSS), júl 2013
ISO 7816-4	ISO/IEC 7816-4 Identifikačné karty. Karty s integrovanými obvodmi. Časť 4: Štruktúra, bezpečnosť a príkazy pre výmenu. Tretie vydanie 2013-04-15
ISO 7816-8	ISO/IEC 7816-8 Identifikačné karty. Karty s integrovanými obvodmi. Časť 8: príkazy pre operácie zabezpečenia. Druhé vydanie 2004-06-01
ISO 8825-1	ISO/IEC 8825-1 Informačné technológie. Pravidlá kódovania v ASN.1: špecifikácia základných kódovacích pravidiel (BER), kánonických kódovacích pravidiel (CER) a odlíšených kódovacích pravidiel (DER). Štvrté vydanie, 2008-12-15
ISO 9797-1	ISO/IEC 9797-1 Informačné technológie. Bezpečnostné techniky. Autentifikačný kód správy (MAC). Časť 1: Mechanizmy používajúce blokovú šifru. Druhé vydanie, 2011-03-01
ISO 10116	ISO/IEC 10116 Informačné technológie. Bezpečnostné techniky. Prevádzkové režimy *n*-bitovej blokovej šifry. Tretie vydanie, 2006-02-01
ISO 16844-3	ISO 16844-3 Cestné vozidlá. Tachografové systémy. Časť 3: Rozhranie snímača pohybu. Prvé vydanie 2004 vrátane technického korigenda 1 2006
RFC 5480	Kryptografia na báze eliptických kriviek informácie subjektu verejného kľúča, marec 2009
RFC 5639	Kryptografia na báze eliptických kriviek (ECC) – Štandardné Brainpool krivky a generácia krivky, 2010
RFC 5869	Funkcia odvodenia kľúča s extrakciou a rozšírením na báze HMAC (HKDF), máj 2010
SHS	Národný inštitút pre normy a technológie USA (NIST), FIPS PUB 180-4: Secure Hash Standard, marec 2012
SP 800-38B	Národný inštitút pre normy a technológie USA (NIST), špeciálna publikácia 800-38B: Odporúčanie pre prevádzkové režimy blokovej šifry: Režim CMAC na autentifikáciu, 2005
TR-03111	BSI Technické usmernenie TR-03111, Kryptografia na báze eliptických kriviek, verzia 2.00, 2012-06-28

7.2. **Notácie a skratky**

V tomto dodatku sa použili tieto notácie a skratky:

AES	Štandard pokročilého šifrovania (Advanced Encryption Standard)
CA	Certifikačná autorita (Certificate Authority)
CAR	Referencia certifikačnej autority (Certificate Authority Reference)
CBC	Reťazenie šifrovacieho bloku (režim prevádzky) (Cipher Block Chaining (mode of operation))

CH	Záhlavie príkazu (Command Header)
CHA	Autorizácia držiteľa certifikátu (Certificate Holder Authorisation)
CHR	Referencia držiteľa certifikátu (Certificate Holder Reference)
CV	Konštantný vektor (Constant Vector)
DER	Odlíšené kódovacie pravidlá (Distinguished Encoding Rules)
DO	Dátový objekt (Data Object)
DSRC	Vyhradená komunikácia krátkeho dosahu (Dedicated Short Range Communication)
ECC	Kryptografia na báze eliptických kriviek (Elliptic Curve Cryptography)
ECDSA	Algoritmus digitálneho podpisu na báze eliptických kriviek (Elliptic Curve Digital Signature Algorithm)
ECDH	Eliptická krivka Diffie-Hellman (algoritmus kľúčovej dohody) (Elliptic Curve Diffie-Hellman)
EGF	Externé zariadenie GNSS (External GNSS Facility)
EQT	Zariadenie (Equipment)
IDE	Inteligentné vyhradené zariadenie (Intelligent Dedicated Equipment)
K_M	Hlavný kľúč snímača pohybu umožňujúci párovanie jednotky vozidla so snímačom pohybu
$K_{M\text{-}VU}$	Kľúč vložený do jednotiek vozidla, umožňujúci VU odvodiť hlavný kľúč snímača pohybu, ak je dielenská karta vložená do VU
$K_{M\text{-}WC}$	Kľúč vložený do dielenských kariet, umožňujúci VU odvodiť hlavný kľúč snímača pohybu, ak je dielenská karta vložená do VU
MAC	Autentifikačný kód správy (Message Authentication Code)
MoS	Snímač pohybu (Motion Sensor)
MSB	Bit najvyššieho rádu (Most Significant Bit)
PKI	Infraštruktúra verejného kľúča (Public Key Infrastructure)
RCF	Diaľkové komunikačné zariadenie (Remote Communication Facility)
SSC	Počítadlo sekvencie odosielania (Send Sequence Counter)
SM	Zabezpečené spracovanie správ (Secure Messaging)
TDES	Štandard trojitého šifrovania údajov (Triple Data Encryption Standard)
TLV	Hodnota dĺžky tagu (Tag Length Value)
VU	Jednotka vozidla (Vehicle Unit)
X.C	Certifikát verejného kľúča používateľa X
X.CA	Certifikačná autorita, ktorá vydala certifikát používateľa X
X.CAR	Referencia certifikačnej autority uvedená v certifikáte používateľa X
X.CHR	Referencia držiteľa certifikátu uvedená v certifikáte používateľa X
X.PK	Verejný kľúč používateľa X
X.SK	Súkromný kľúč používateľa X
$X.PK_{eph}$	Efemérny verejný kľúč používateľa X (ephemeral public key of user X)
$X.SK_{eph}$	Efemérny súkromný kľúč používateľa X (ephemeral private key of user X)
'xx'	hexadecimálna hodnota (a hexadecimal value)
||	Operátor zreťazenia (concatenation operator)

7.3. **Vymedzenie pojmov**

Vymedzenie pojmov použité v tomto dodatku je uvedené v oddiele I prílohy 1C.

8. KRYPTOGRAFICKÉ SYSTÉMY A ALGORITMY

8.1. **Kryptografické systémy**

CSM_38 Jednotky vozidla a tachografové karty musia používať kryptografický systém verejného kľúča na báze eliptických kriviek tak, aby poskytovali tieto služby zabezpečenia:

— vzájomnú autentifikáciu medzi jednotkou vozidla a kartou,

— dohodu kľúčov relácie AES medzi jednotkou vozidla a kartou,

— zaistenie autenticity, integrity a nespochybniteľnosti údajov stiahnutých z jednotiek vozidla alebo tachografových kariet na externé médiá.

CSM_39 Jednotky vozidla a externé zariadenia GNSS musia používať kryptografický systém verejného kľúča na báze eliptických kriviek, aby poskytovali tieto služby zabezpečenia:

— spojenie jednotky vozidla s externým zariadením GNSS,

— vzájomnú autentifikáciu medzi jednotkou vozidla a externým zariadením GNSS,

— dohodu kľúčov relácie AES medzi jednotkou vozidla a externým zariadením GNSS.

CSM_40 Jednotky vozidla a tachografové karty používajú symetrický kryptografický systém založený na AES, aby poskytovali tieto služby zabezpečenia:

— zaistenie autenticity a integrity údajov vymieňaných medzi jednotkou vozidla a tachografovou kartou,

— v prípade potreby zaistenie dôvernosti údajov vymieňaných medzi jednotkou vozidla a tachografovou kartou.

CSM_41 Jednotky vozidla a externé zariadenia GNSS musia používať symetrický kryptografický systém založený na AES, aby poskytovali tieto služby zabezpečenia:

— zaistenie autenticity a integrity údajov vymieňaných medzi jednotkou vozidla a externým zariadením GNSS.

CSM_42 Jednotky vozidla a snímače pohybu musia používať symetrický kryptografický systém založený na AES, aby poskytovali tieto služby zabezpečenia:

— párovanie jednotky vozidla a snímača pohybu,

— vzájomnú autentifikáciu medzi jednotkou vozidla a snímačom pohybu,

— zaistenie dôvernosti údajov vymieňaných medzi jednotkou vozidla a snímačom pohybu.

CSM_43 Jednotky vozidla a kontrolné karty používajú symetrický kryptografický systém založený na AES, aby na rozhraní diaľkovej komunikácie poskytovali tieto služby zabezpečenia:

— zaistenie dôvernosti, autenticity a integrity údajov odosielaných jednotkou vozidla na kontrolnú kartu.

Poznámky:

— V skutočnosti sa údaje prenášajú z jednotky vozidla do diaľkového snímača, ktorý ovláda kontrolný úradník prostredníctvom diaľkového komunikačného zariadenia, ktoré môže byť integrované vo VU alebo externé, pozri dodatok 14. Avšak diaľkový snímač posiela získané údaje na kontrolnú kartu na dešifrovanie a overenie autenticity. Z hľadiska zabezpečenia sú diaľkové komunikačné zariadenie a diaľkový snímač úplne transparentné.

— Dielenská karta poskytuje rovnaké služby zabezpečenia pre rozhranie DSRC ako kontrolná karta. To umožňuje dielni overiť správne fungovanie diaľkového komunikačného rozhrania VU vrátane zabezpečenia. Viac informácií sa uvádza v oddiele 9.2.2.

8.2. **Kryptografické algoritmy**

8.2.1 *Symetrické algoritmy*

CSM_44 Jednotky vozidla, tachografové karty, snímače pohybu a externé zariadenia GNSS musia podporovať algoritmus AES vymedzený v [AES] s dĺžkou kľúča 128, 192 a 256 bitov.

8.2.2 *Asymetrické algoritmy a štandardizované parametre domény*

CSM_45 Jednotky vozidla, tachografové karty a externé zariadenia GNSS musia podporovať kryptografiu na báze eliptických kriviek s veľkosťou kľúča 256, 384 a 512/521 bitov.

CSM_46 Jednotky vozidla, tachografové karty a externé zariadenia GNSS musia podporovať podpisový algoritmus ECDSA, ako je špecifikované v [DSS].

CSM_47 Jednotky vozidla, tachografové karty a externé zariadenia GNSS musia podporovať algoritmus kľúčovej dohody ECKA-EG, ako je špecifikované v [TR 03111].

CSM_48 V prípade kryptografie na báze eliptických kriviek musia jednotky vozidla, tachografové karty a externé zariadenia GNSS podporovať všetky štandardizované parametre domény uvedené v tabuľke 1 ďalej.

Tabuľka 1

Štandardizované parametre domény

Názov	Veľkosť (v bitoch)	Referencia	Objektový identifikátor
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`

Poznámka: objektové identifikátory uvedené v poslednom stĺpci tabuľky 1 sú špecifikované v [RFC 5639] v prípade Brainpool kriviek a v [RFC 5480] v prípade NIST kriviek.

Príklad 1: objektový identifikátor BrainpoolP256r1 krivky je `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

alebo v bodkovej notácii: `1.3.36.3.3.2.8.1.1.7`.

Príklad 2: objektový identifikátor NIST P-384 krivky je

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

alebo v bodkovej notácii: `1.3.132.0.34`.

8.2.3 *Hašovacie algoritmy*

CSM_49 Jednotky vozidla a tachografové karty musia podporovať algoritmy SHA-256, SHA-384 a SHA-512 uvedené v [SHS].

8.2.4 *Šifrovacie zostavy*

CSM_50 V prípade symetrického algoritmu sa asymetrický algoritmus a/alebo hašovací algoritmus spoločne používajú na vytvorenie bezpečnostného protokolu, pričom ich príslušné dĺžky kľúča a veľkosti hash-u musia mať (približne) rovnakú silu. Tabuľka 2 zobrazuje povolené šifrovacie zostavy:

Tabuľka 2

Povolené šifrovacie zostavy

ID šifrovacej zostavy	Veľkosť kľúča ECC (v bitoch)	Dĺžka kľúča AES (v bitoch)	Hašovací algoritmus	Dĺžka MAC (v bajtoch)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Poznámka: Veľkosti kľúčov ECC 512 bitov a 521 bitov sa na všetky účely v tomto dodatku považujú za rovnako silné.

9. KĽÚČE A CERTIFIKÁTY

9.1. **Asymetrické kľúčové páry a certifikáty verejného kľúča**

9.1.1 *Všeobecné*

Poznámka: kľúče opísané v tomto oddiele sa používajú na vzájomnú autentifikáciu a zabezpečené spracovanie medzi jednotkami vozidla a tachografovými kartami a medzi jednotkami vozidla a vonkajšími zariadeniami GNSS. Tieto postupy sú podrobne opísané v kapitolách 10 a 11 tohto dodatku.

CSM_51 V rámci európskeho systému inteligentných tachografov, sa kľúčové páry ECC a zodpovedajúce certifikáty musia generovať a spravovať na troch funkčných hierarchických úrovniach:

— európskej úrovni,

— úrovni členského štátu,

— úrovni zariadenia.

CSM_52 V rámci celého európskeho systému inteligentných tachografov sa verejné a súkromné kľúče a certifikáty musia generovať, spravovať a prenášať pomocou štandardizovaných a zabezpečených metód.

9.1.2 *Európska úroveň*

CSM_53 Na európskej úrovni sa musí generovať jeden jedinečný kľúčový pár ECC označený ako EUR. Musí pozostávať zo súkromného kľúča (EUR.SK) a verejného kľúča (EUR.PK). Tento kľúčový pár tvorí pár koreňových kľúčov celej PKI európskeho inteligentného tachografu. Túto úlohu musí plniť Európsky úrad prvotnej certifikácie (European Root Certificate Authority – ERCA), ktorý podlieha Európskej komisii a je pod jej zodpovednosťou.

CSM_54 ERCA musí použiť európsky súkromný kľúč na podpísanie (samopodpísaného) koreňového certifikátu európskeho verejného kľúča, a musí oznámiť tento európsky koreňový certifikát všetkým členským štátom.

CSM_55 Na požiadanie ERCA musí použiť európsky súkromný kľúč na podpísanie certifikátov verejných kľúčov členských štátov. ERCA musí uchovávať záznamy všetkých podpísaných certifikátov verejného kľúča členských štátov.

CSM_56 Ako sa uvádza na obrázku 1 v oddiele 9.1.7, ERCA musí vygenerovať nový európsky pár koreňových kľúčov každých 17 rokov. Vždy, keď ERCA vygeneruje nový európsky pár koreňových kľúčov, musí vytvoriť nový samopodpísaný koreňový certifikát pre nový európsky verejný kľúč. Obdobie platnosti európskeho koreňového certifikátu je 34 rokov a 3 mesiace.

Poznámka: Zavedenie nového páru koreňových kľúčov tiež znamená, že ERCA vygeneruje nový hlavný kľúč snímača pohybu a nový hlavný kľúč DRSC, pozri body 9.2.1.2 a 9.2.2.2.

CSM_57 Pred vytvorením nového európskeho páru koreňových kľúčov musí ERCA zanalyzovať kryptografickú silu, ktorá je potrebná pre nový kľúčový pár, keďže by mal byť bezpečný po nasledujúcich 34 rokov. Ak sa zistí, že je to potrebné, ERCA musí použiť šifrovaciu zostavu, ktorá je silnejšia, ako súčasná, ako je uvedené v CSM_50.

CSM_58 Vždy, keď sa generuje nový európsky pár koreňových kľúčov, ERCA musí pre nový európsky verejný kľúč vytvoriť prepájací certifikát a podpísať ho predchádzajúcim európskym súkromným kľúčom. Platnosť prepájacieho certifikátu je 17 rokov. Je to znázornené aj na obrázku 1 v oddiele 9.1.7.

Poznámka: Keďže prepájací certifikát obsahuje verejný kľúč ERCA generácie *X* a podpisuje sa súkromným kľúčom ERCA generácie *X-1*, prepájací certifikát poskytuje zaradeniu vydanému v rámci generácie *X-1* metódu, ako dôverovať zariadeniu vydanému v rámci generácie *X*.

CSM_59 ERCA nepoužije súkromný kľúč starého páru koreňových kľúčov na žiadne účely potom, ako nadobudne platnosť certifikát nového páru koreňových kľúčov.

CSM_60 ERCA musí mať neustále k dispozícii tieto kryptografické kľúče a certifikáty:

— aktuálny kľúčový pár EUR a zodpovedajúci certifikát

— všetky predchádzajúce certifikáty EUR, ktoré sa majú použiť na overovanie certifikátov MSCA, ktoré sú stále platné

— certifikáty prepojenia pre všetky generácie certifikátov EUR okrem prvej generácie.

9.1.3 *Úroveň členského štátu*

CSM_61 Na úrovni členských štátov musia všetky členské štáty, od ktorých sa požaduje podpísanie certifikátov tachografovej karty, vygenerovať jeden alebo viac jedinečných kľúčových párov ECC označených ako MSCA_Card. Všetky členské štáty, od ktorých sa požaduje podpísanie certifikátov pre jednotky vozidla alebo externé zariadenia GNSS, musia navyše vygenerovať jeden alebo viac jedinečných kľúčových párov ECC označených ako MSCA_VU-EGF.

CSM_62 Úlohu vygenerovať kľúčové páry členského štátu musí splniť certifikačná autorita členského štátu (MSCA). Vždy, keď MSCA vygeneruje kľúčový pár členského štátu, musí autorite ERCA poslať verejný kľúč s cieľom získať zodpovedajúci certifikát členského štátu podpísaný ERCA.

CSM_63 MSCA musí zvoliť silu kľúčového páru členského štátu, ktorá je rovnaká, ako sila európskeho páru koreňových kľúčov použitého na podpísanie zodpovedajúceho certifikátu členského štátu.

CSM_64 Ak kľúčový pár MSCA_VU-EGF existuje, musí pozostávať zo súkromného kľúča MSCA_VU-EGF.SK a verejného kľúča MSCA_VU-EGF.PK. MSCA musí používať súkromný kľúč MSCA_VU-EGF.SK výlučne na podpisovanie certifikátov verejného kľúča jednotiek vozidla a externých zariadení GNSS.

CSM_65 Kľúčový pár MSCA_Card musí pozostávať zo súkromného kľúča MSCA_Card.SK a verejného kľúča MSCA_Card.PK. MSCA musí používať súkromný kľúč MSCA_Card.SK výlučne na podpisovanie certifikátov verejného kľúča tachografových kariet.

CSM_66 MSCA musí uchovávať záznamy o všetkých podpísaných certifikátoch VU, certifikátoch externých zariadení GNSS a certifikátoch kariet, spolu s identifikáciou zariadenia, pre ktoré je certifikát určený.

CSM_67 Obdobie platnosti certifikátu MSCA_VU-EGF je 17 rokov a 3 mesiace. Obdobie platnosti certifikátu MSCA_Card je 7 rokov a 1 mesiac.

CSM_68 Ako sa uvádza na obrázku 1 v oddiele 9.1.7, musí byť obdobie použitia kľúča v prípade súkromného kľúča kľúčového páru MSCA_VU-EGF a súkromného kľúča kľúčového páru MSCA_Card dva roky.

CSM_69 Od okamihu, keď sa skončilo obdobie použitia súkromného kľúča kľúčového páru MSCA_VU-EGF, ho MSCA nesmie použiť na žiadne účely. Od okamihu, keď sa skončilo obdobie použitia súkromného kľúča kľúčového páru MSCA_Card, nesmie MSCA ani ten použiť na žiadne účely.

CSM_70 MSCA musí mať neustále k dispozícii tieto kryptografické kľúče a certifikáty:

— aktuálny kľúčový pár MSCA_Card a zodpovedajúci certifikát

— všetky predchádzajúce certifikáty MSCA_Card, ktoré sa majú použiť na overovanie certifikátov tachografových kariet, ktoré sú stále platné

— aktuálny certifikát EUR potrebný na overovanie aktuálneho certifikátu MSCA

— všetky predchádzajúce certifikáty EUR potrebné na overovanie všetkých certifikátov MSCA, ktoré sú stále platné

CSM_71 Ak sa vyžaduje, aby MSCA podpísal certifikáty pre jednotky vozidla alebo externé zariadenia GNSS, musí mať navyše k dispozícii aj tieto kľúče a certifikáty:

— aktuálny kľúčový pár MSCA_VU-EGF a zodpovedajúci certifikát

— všetky predchádzajúce verejné kľúče MSCA_VU-EGF, ktoré sa majú používať na overovanie certifikátov VU alebo externých zariadení GNSS, ktoré sú stále platné

9.1.4 *Úroveň zariadenia: Jednotky vozidla*

CSM_72 Dva jedinečné kľúčové páry ECC sa musia generovať pre každú jednotku vozidla, označené ako VU_MA a VU_Sign. To patrí medzi úlohy výrobcov VU. Vždy, keď sa vygeneruje kľúčový pár VU, strana, ktorá kľúč generuje, musí poslať verejný kľúč autorite MSCA krajiny, v ktorej má sídlo, s cieľom získať zodpovedajúci certifikát VU podpísaný MSCA. Súkromný kľúč musí používať len jednotka vozidla.

CSM_73 Certifikáty VU_MA a VU_Sign danej jednotky vozidla musia mať ten istý dátum účinnosti certifikátu.

CSM_74 Výrobca VU musí zvoliť silu kľúčového páru VU, ktorá je rovnaká, ako sila kľúčového páru MSCA použitého na podpísanie certifikátu príslušnej VU.

CSM_75 Jednotka vozidla musí použiť svoj kľúčový pár VU_MA, pozostávajúci zo súkromného kľúča VU_MA.SK a verejného kľúča VU_MA.PK, výlučne na VU autentifikáciu tachografových kariet a externých zariadení GNSS, ako sa uvádza v oddieloch 10.3 a 11.4 tohto dodatku.

CSM_76 Jednotka vozidla musí byť schopná generovať efemérne kľúčové páry ECC a musí použiť efemérny kľúčový pár výlučne na vykonanie kľúčovej dohody relácie s tachografovou kartou alebo externým zariadením GNSS, ako sa uvádza v oddieloch 10.4 a 11.4 tohto dodatku.

CSM_77 Jednotka vozidla musí použiť súkromný kľúč VU_Sign.SK jeho kľúčového páru VU_Sign výlučne na podpisovanie stiahnutých dátových súborov, ako je uvedené v kapitole 14 tohto dodatku. Zodpovedajúci verejný kľúč VU_Sign.PK sa musí použiť výlučne na overovanie podpisov vytvorených jednotkou vozidla.

CSM_78 Ako je znázornené na obrázku 1 v oddiele 9.1.7, obdobie platnosti certifikátu VU_MA je 15 rokov a 3 mesiace. Obdobie platnosti certifikátu VU_Sign je 15 rokov a 3 mesiace.

Poznámky:

— Obdobie predĺženej platnosti certifikátu VU_Sign umožňuje jednotke vozidla vytvoriť platné podpisy pre stiahnuté údaje počas prvých troch mesiacov po jej uplynutí, ako sa vyžaduje v nariadení (EÚ) č. 581/2010.

— Obdobie predĺženej platnosti certifikátu VU_MA je potrebné, aby sa umožnila autentifikácia VU pre kontrolnú alebo podnikovú kartu počas prvých troch mesiacov po jej uplynutí, tak, aby bolo možné vykonať sťahovanie údajov.

CSM_79 Jednotka vozidla nesmie použiť súkromný kľúč kľúčového páru VU po uplynutí platnosti zodpovedajúceho certifikátu na žiadne účely.

CSM_80 Kľúčové páry VU (okrem efemérnych kľúčových párov) a zodpovedajúce certifikáty danej jednotky vozidla sa nesmú nahradiť alebo obnoviť v praxi po tom, ako bola jednotka vozidla uvedená do prevádzky.

Poznámky:

— Efemérne kľúčové páry nie sú do tejto požiadavky zahrnuté, keďže nový efemérny kľúčový pár je generovaný VU vždy, keď sa vykonáva autentifikácia čipu a kľúčová dohoda relácie, pozri oddiel 10.4. Upozorňujeme, že efemérne kľúčové páry nemajú zodpovedajúce certifikáty.

— Táto požiadavka nezakazuje možnosť nahradenia statických kľúčových párov VU počas modernizácie alebo opravy v zabezpečenom prostredí kontrolovanom výrobcom VU.

CSM_81 Pri uvádzaní do prevádzky musia jednotky vozidla obsahovať tieto kryptografické kľúče a certifikáty:

— súkromný kľúč VU_MA a zodpovedajúci certifikát

— súkromný kľúč VU_Sign a zodpovedajúci certifikát

— certifikát MSCA_VU-EGF obsahujúci verejný kľúč MSCA_VU-EGF.PK, ktorý sa má použiť na overovanie certifikátu VU_MA a certifikátu VU_Sign

— certifikát EUR obsahujúci verejný kľúč EUR.PK, ktorý sa má použiť na overovanie certifikátu MSCA_VU-EGF

— certifikát EUR, ktorého platnosť priamo predchádza platnosti certifikátu EUR, ktorý sa má použiť na overovanie certifikátu MSCA_VU-EGF, ak takýto certifikát existuje

— prepájací certifikát prepájajúci tieto dva certifikáty EUR, ak existuje.

CSM_82 Okrem kryptografických kľúčov a certifikátov uvedených v CSM_81 musia jednotky vozidla obsahovať aj kľúče a certifikáty uvedené v časti A tohto dodatku, umožňujúce jednotke vozidla komunikovať s tachografovými kartami prvej generácie.

9.1.5 *Úroveň zariadenia: Tachografové karty*

CSM_83 Pre každú tachografovú kartu musí byť vygenerovaný jeden jedinečný kľúčový pár ECC, určený ako Card_MA. Pre každú kartu vodiča a dielenskú kartu sa musí navyše vygenerovať druhý jedinečný kľúčový pár ECC, určený ako Card_Sign. Tieto úlohy môžu plniť výrobcovia kariet alebo personalizátori kariet. Vždy, keď sa vygeneruje kľúčový pár karty, strana, ktorá kľúč generuje, musí poslať verejný kľúč autority MSCA krajiny, v ktorej má sídlo, s cieľom získať zodpovedajúci certifikát karty podpísaný MSCA. Súkromný kľúč musí používať len tachografová karta.

CSM_84 Certifikáty Card_MA a Card_Sign danej karty vodiča alebo dielenskej karty musia mať ten istý dátum účinnosti certifikátu.

CSM_85 Výrobca karty alebo personalizátor karty musí zvoliť silu kľúčového páru karty, ktorá je rovnaká, ako sila kľúčového páru MSCA použitého na podpísanie príslušného certifikátu karty.

CSM_86 Tachografová karta musí použiť svoj kľúčový pár Card_MA, pozostávajúci zo súkromného kľúča Card_MA.SK a verejného kľúča Card_MA.PK, výlučne na vykonanie vzájomnej autentifikácie a kľúčovej dohody relácie s jednotkami vozidla, ako sa uvádza v oddieloch 10.3 a 10.4 tohto dodatku.

CSM_87 Karta vodiča alebo dielenská karta musí použiť súkromný kľúč Card_Sign.SK jej kľúčového páru Card_Sign výlučne na podpisovanie stiahnutých dátových súborov, ako je uvedené v kapitole 14 tohto dodatku. Zodpovedajúci verejný kľúč Card_Sign.PK sa musí použiť výlučne na overovanie podpisov vytvorených kartou.

CSM_88 Obdobie platnosti certifikátu Card_MA je takéto:

— V prípade kariet vodiča: 5 rokov

— V prípade podnikových kariet: 2 roky

— V prípade kontrolných kariet: 2 roky

— V prípade dielenských kariet: 1 rok

CSM_89 Obdobie platnosti certifikátu Card_Sign je takéto:

— V prípade kariet vodiča: 5 rokov a 1 mesiac

— V prípade dielenských kariet: 1 rok a 1 mesiac

Poznámka: Obdobie predĺženej platnosti certifikátu Card_Sign umožňuje karte vodiča vytvoriť platné podpisy pre stiahnuté údaje počas prvého mesiaca po jej uplynutí. Je to potrebné z hľadiska nariadenia (EÚ) č. 581/2010, v ktorom sa vyžaduje, že sťahovanie údajov z karty vodiča musí byť možné do 28 dní po zaznamenaní posledných údajov.

CSM_90 Kľúčové páry a zodpovedajúce certifikáty danej tachografovej karty sa nesmú nahradiť alebo obnoviť potom, ako bola karta vydaná.

CSM_91 Po vydaní musia tachografové karty obsahovať tieto kryptografické kľúče a certifikáty:

— súkromný kľúč Card_MA a zodpovedajúci certifikát

— karty vodičov alebo dielenské karty obsahujú navyše: Súkromný kľúč Card_Sign a zodpovedajúci certifikát

— certifikát MSCA_Card obsahujúci verejný kľúč MSCA_Card.PK, ktorý sa má použiť na overovanie certifikátu Card_MA a certifikátu Card_Sign

— certifikát EUR obsahujúci verejný kľúč EUR.PK, ktorý sa má použiť na overovanie certifikátu MSCA_Card

— certifikát EUR, ktorého platnosť priamo predchádza platnosti certifikátu EUR, ktorý sa má použiť na overovanie certifikátu MSCA_Card, ak takýto certifikát existuje

— prepájací certifikát prepájajúci tieto dva certifikáty EUR, ak existuje.

CSM_92 Okrem kryptografických kľúčov a certifikátov uvedených v CSM_91 musia tachografové karty obsahovať aj kľúče a certifikáty uvedené v časti A tohto dodatku, umožňujúce týmto kartám komunikovať s VU prvej generácie.

9.1.6 *Úroveň zariadenia: Externé zariadenia GNSS*

CSM_93 Musí sa vygenerovať jeden jedinečný kľúčový pár ECC pre každé externé zariadenie GNSS, označený ako EGF_MA. To patrí medzi úlohy výrobcov externých zariadení GNSS. Vždy, keď sa vygeneruje kľúčový pár EGF_MA, verejný kľúč sa musí poslať autorite MSCA krajiny, v ktorej má sídlo, s cieľom získať zodpovedajúci certifikát EGF_MA podpísaný MSCA. Súkromný kľúč musí používať len externé zariadenie GNSS.

CSM_94 Výrobca EGF musí zvoliť silu kľúčového páru EGF_MA, ktorá je rovnaká, ako sila kľúčového páru MSCA použitého na podpísanie zodpovedajúceho certifikátu EGF_MA.

CSM_95 Externé zariadenie GNSS musí použiť svoj kľúčový pár EGF_MA, pozostávajúci zo súkromného kľúča EGF_MA.SK a verejného kľúča EGF_MA.PK, výlučne na vykonanie vzájomnej autentifikácie a kľúčovej dohody relácie s jednotkami vozidla, ako sa uvádza v oddieloch 11.4 a 11.4 tohto dodatku.

CSM_96 Obdobie platnosti certifikátu EGF_MA je 15 rokov.

CSM_97 Externé zariadenie GNSS nesmie použiť súkromný kľúč svojho kľúčového páru EGF_MA na spojenie s jednotkou vozidla po uplynutí platnosti zodpovedajúceho certifikátu.

Poznámka: ako je vysvetlené v oddiele 11.3.3, EGF prípadne môže použiť svoj súkromný kľúč na vzájomnú autentifikáciu s VU, s ktorou je už spojené, dokonca aj po uplynutí platnosti príslušného certifikátu.

CSM_98 Kľúčový pár EGF_MA a príslušný certifikát daného externého zariadenia GNSS sa nesmú nahradiť alebo obnoviť v praxi, po tom, ako bolo EGF uvedené do prevádzky.

Poznámka: Táto požiadavka nezakazuje možnosť nahradenia kľúčových párov EGF počas modernizácie alebo opravy v zabezpečenom prostredí kontrolovanom výrobcom EGF.

CSM_99 Pri uvádzaní do prevádzky musí externé zariadenie GNSS obsahovať tieto kryptografické kľúče a certifikáty:

— súkromný kľúč EGF_MA a zodpovedajúci certifikát

— certifikát MSCA_VU-EGF obsahujúci verejný kľúč MSCA_VU-EGF.PK, ktorý sa má použiť na overovanie certifikátu EGF_MA

— certifikát EUR obsahujúci verejný kľúč EUR.PK, ktorý sa má použiť na overovanie certifikátu MSCA_VU-EGF

— certifikát EUR, ktorého platnosť priamo predchádza platnosti certifikátu EUR, ktorý sa má použiť na overovanie certifikátu MSCA_VU-EGF, ak takýto certifikát existuje

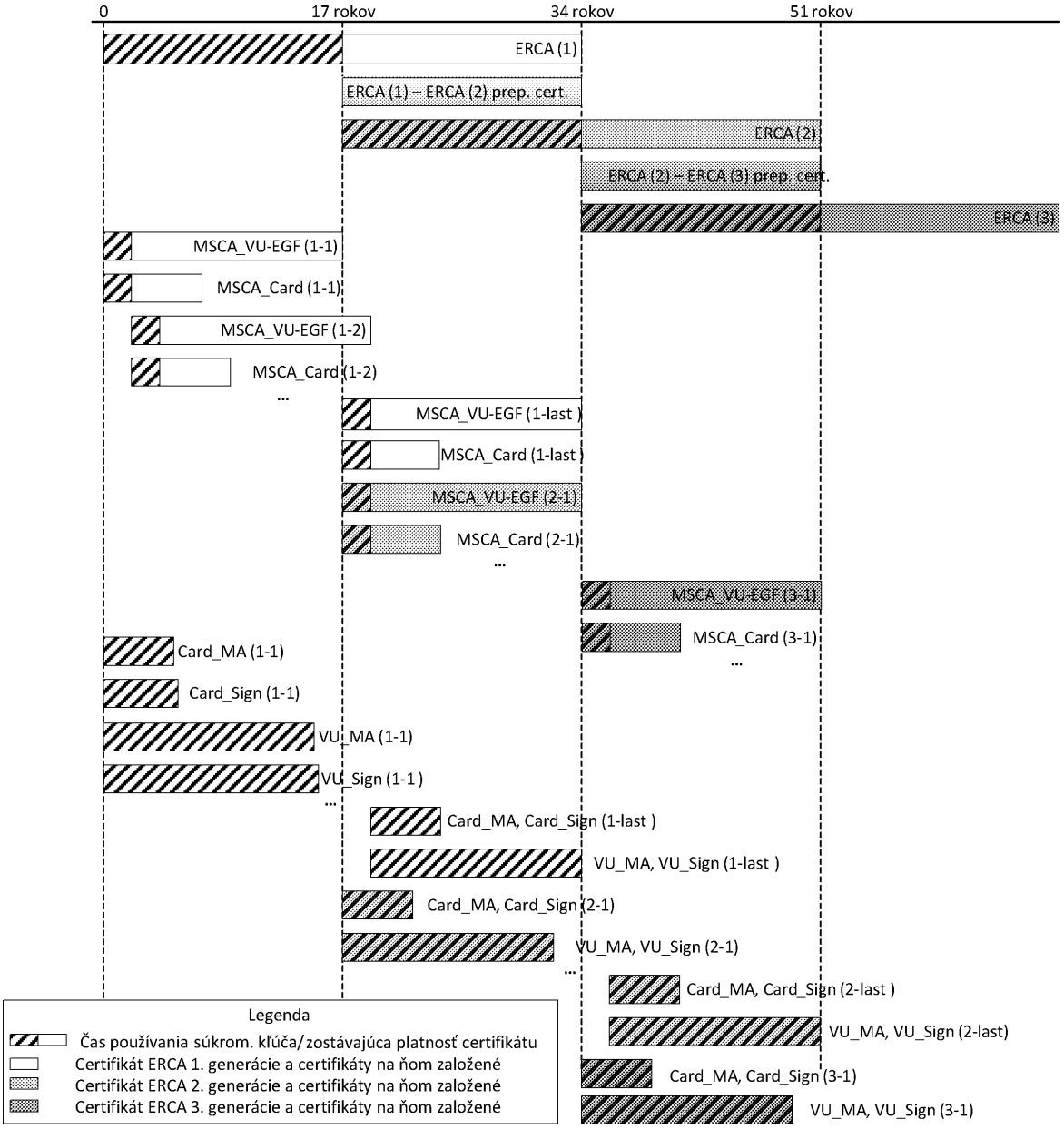
— prepájací certifikát prepájajúci tieto dva certifikáty EUR, ak existuje.

9.1.7 *Prehľad: Náhrada certifikátu*

Obrázok 1 ukazuje, ako sa rôzne generácie koreňových certifikátov ERCA, certifikátov prepojenia ERCA, certifikátov MSCA a certifikátov zariadenia (VU alebo karta) vydávajú a používajú v čase:

Obrázok 1

Vydávanie a používanie rôznych generácií koreňových certifikátov ERCA, certifikátov prepojenia ERCA, certifikátov MSCA a certifikátov zariadenia



Poznámky k obrázku 1:

1. Rôzne generácie koreňového certifikátu sú označované číslom v zátvorkách. Napr. ERCA (1) je prvá generácia koreňového certifikátu ERCA; ERCA (2) je druhá generácia atď.

2. Iné certifikáty sú označené dvomi číslami v zátvorkách, prvé číslo označuje generáciu koreňového certifikátu, v rámci ktorej sú vydané, druhé číslo označuje generáciu samotného certifikátu. Napr. MSCA_Card (1-1) je prvým certifikátom MSCA_Card vydaným na základe ERCA (1); MSCA_Card (2-1) je prvým certifikátom MSCA_Card vydaným na základe ERCA (2); MSCA_Card (2-last) je posledným certifikátom MSCA_Card vydaným na základe ERCA (2); Card_MA (2-1) je prvým certifikátom karty na vzájomnú autentifikáciu, ktorý je vydaný na základe ERCA (2) atď.

3. Certifikáty MSCA_Card (2-1) a MSCA_Card (1-last) sú vydané v takmer, ale nie presne v ten istý deň. MSCA_Card (2-1) je prvým certifikátom MSCA_Card vydaným na základe ERCA (2) a bude vydaný trochu neskôr ako MSCA_Card (1-last), posledný certifikát MSCA_Card na základe ERCA (1).

4. Ako je znázornené na obrázku, prvý certifikát VU a certifikát karty vydané na základe ERCA (2) sa objavia takmer dva roky predtým, ako sa objaví posledný certifikát VU a certifikát karty vydané na základe ERCA (1). Dôvodom je skutočnosť, že certifikáty VU a karty sú vydané na základe certifikátu MSCA, a nie priamo na základe certifikátu ERCA. Certifikát MSCA (2–1) bude vydaný hneď potom, ako ERCA (2) nadobudne platnosť, ale certifikát MSCA (1-last) bude vydaný len o trochu skôr – na samom konci platnosti certifikátu ERCA (1). Preto tieto dva certifikáty MSCA budú mať takmer rovnaké obdobie platnosti, napriek skutočnosti, že patria k odlišným generáciám.

5. Obdobie platnosti uvedené v prípade kariet je obdobie platné pre karty vodiča (5 rokov).

6. Aby sa ušetril priestor, rozdiel v období platnosti medzi certifikátmi Card_MA a Card_Sign a medzi certifikátmi VU_MA a VU_Sign sa uvádza len pre prvú generáciu.

9.2. **Symetrické kľúče**

9.2.1 *Kľúče na zabezpečenie komunikácie VU – snímač pohybu*

9.2.1.1 *Všeobecné*

Poznámka: predpokladá sa, že čitatelia tohto oddielu poznajú obsah normy [ISO 16844-3], kde sa opisujú rozhrania medzi jednotkou vozidla a snímačom pohybu. Proces párovania medzi VU a snímačom pohybu je podrobne opísaný v kapitole 12 tohto dodatku.

CSM_100 Ako sa uvádza v tabuľke 3, na párovanie jednotiek vozidla so snímačmi pohybu z dôvodu vzájomnej autentifikácie medzi jednotkami vozidla a snímačmi pohybu a na šifrovanie komunikácie medzi jednotkami vozidla a snímačmi pohybu je potrebných niekoľko symetrických kľúčov. Všetky tieto kľúče musia byť kľúčmi AES, s dĺžkou kľúča rovnajúcou sa dĺžke hlavného kľúča snímača pohybu, ktorý musí byť prepojený s dĺžkou (predpokladaného) európskeho páru koreňových kľúčov, ako je uvedené v CSM_50.

Tabuľka 3

Kľúče na zabezpečenie komunikácie jednotka vozidla – snímač pohybu

Kľúč	Symbol	Generuje	Metóda generovania	Ukladá
Hlavný kľúč snímača pohybu – časť VU	$K_{M\text{-}VU}$	ERCA	Náhodné	ERCA, MSCA zapojené do vydávania certifikátov VU, výrobcovia VU, jednotky vozidla

Kľúč	Symbol	Generuje	Metóda generovania	Ukladá
Hlavný kľúč snímača pohybu – časť dielňa	K_{M-WC}	ERCA	Náhodné	ERCA, MSCA, výrobcovia kariet, dielenské karty
Hlavný kľúč snímača pohybu	K_M	Samostatne sa negeneruje	Vypočítané ako $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, MSCA zapojené do vydávania kľúčov snímačov pohybu (nepovinne) (*)
Identifikačný kľúč	K_{ID}	Samostatne sa negeneruje	Vypočítané ako $K_{ID} = K_M$ XOR CV, kde CV je špecifikované v CSM_106	ERCA, MSCA zapojené do vydávania kľúčov snímačov pohybu (nepovinne) (*)
Párovací kľúč	K_P	Výrobca snímača pohybu	Náhodné	Jeden snímač pohybu
Kľúč relácie	K_S	VU (počas párovania VU so snímačom pohybu)	Náhodné	Jedna VU a jeden snímač pohybu

(*) Uloženie K_M a K_{ID} je nepovinné, keďže tieto kľúče možno odvodiť z K_{M-VU}, K_{M-WC} a CV.

CSM_101 Európsky úrad prvotnej certifikácie musí vygenerovať K_{M-VU} a K_{M-WC}, dva náhodné a jedinečné kľúče AES, z ktorých môže byť vypočítaný hlavný kľúč snímača pohybu ako K_{M-VU} XOR K_{M-WC}. ERCA musí certifikačným autoritám členských štátov na požiadanie oznámiť K_M, K_{M-VU} a K_{M-WC}.

CSM_102 ERCA musí prideliť každému hlavnému kľúču snímača pohybu K_M jedinečné číslo verzie, ktorá sa vzťahuje aj na podkladové kľúče K_{M-VU} a K_{M-WC} a na súvisiaci identifikačný kľúč K_{ID}. ERCA musí pri zasielaní K_{M-VU} a K_{M-WC} informovať MSCA o čísle verzie.

Poznámka: Číslo verzie sa používa na rozlíšenie rôznych generácií týchto kľúčov, ako je podrobne vysvetlené v oddiele 9.2.1.2.

CSM_103 Certifikačná autorita členského štátu musí výrobcom jednotiek vozidla na požiadanie poslať K_{M-VU} spolu s číslom jeho verzie. Výrobcovia VU musia vložiť K_{M-VU} a číslo jeho verzie do všetkých vyrobených VU.

CSM_104 Certifikačná autorita členského štátu musia zabezpečiť, aby K_{M-WC} spolu s číslom jeho verzie bolo vložené do každej dielenskej karty vydanej v rámci jeho zodpovednosti.

Poznámky:

— Pozri opis dátového typu `SensorInstallationSecData` v dodatku 2.

— Ako je vysvetlené v oddiele 9.2.1.2, v skutočnosti môže byť potrebné do jedinej dielenskej karty vložiť viaceré generácie K_{M-WC}.

CSM_105 Okrem kľúča AES špecifikovaného v CSM_104 musí MSCA zaistiť, aby sa kľúč TDES Km_{WC} špecifikovaný v požiadavke CSM_ 037 v časti A tohto dodatku vložil do každej dielenskej karty vydanej v rámci jeho zodpovednosti.

Poznámky:

— To umožňuje, aby sa dielenská karta druhej generácie mohla použiť na pripojenie VU prvej generácie.

— Dielenská karta druhej generácie bude obsahovať dve rôzne aplikácie, jedna v súlade s časťou B tohto dodatku a jedna v súlade s časťou A. Druhá aplikácia bude obsahovať kľúč TDES Km_{WC}.

CSM_106 MSCA zapojený do vydávania snímačov pohybu musí odvodiť identifikačný kľúč z hlavného kľúča snímača pohybu XOR šifrovaním s konštantným vektorom CV. Hodnota CV je takáto:

— V prípade 128-bitových hlavných kľúčov snímačov pohybu: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83'

— V prípade 192-bitových hlavných kľúčov snímačov pohybu: 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'

— V prípade 256-bitových hlavných kľúčov snímačov pohybu: 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'

Poznámka: Konštantné vektory boli vygenerované takto:

Pi_10 = prvých 10 bajtov desatinnej časti matematickej konštanty π = '24 3F 6A 88 85 A3 08 D3 13 19'

CV_128-bitov = prvých 16 bajtov SHA-256(Pi_10)

CV_192-bitov = prvých 24 bajtov SHA-384(Pi_10)

CV_256-bitov = prvých 32 bajtov SHA-512(Pi_10)

CSM_107 Výrobcovia snímačov pohybu musia pre každý snímač pohybu vygenerovať náhodný a jedinečný párovací kľúč K_P a poslať každý párovací kľúč certifikačnej autorite členského štátu. MSCA musí každý párovací kľúč zašifrovať samostatne s použitím hlavného kľúča snímača pohybu K_M a vrátiť zašifrovaný kľúč výrobcovi snímačov pohybu. V prípade každého zašifrovaného kľúča musí MSCA oznámiť výrobcovi snímačov pohybu číslo verzie príslušného K_M.

Poznámka: Ako je vysvetlené v oddiele 9.2.1.2, v skutočnosti je možné, že výrobca snímačov pohybu bude musieť pre jeden snímač pohybu generovať viacero jedinečných párovacích kľúčov.

CSM_108 Výrobcovia snímačov pohybu musia pre každý snímač pohybu vygenerovať jedinečné sériové číslo a poslať všetky sériové čísla certifikačnej autorite členského štátu. MSCA musí každé sériové číslo zašifrovať samostatne s identifikačným kľúčom K_{ID} a vrátiť zašifrované sériové číslo výrobcovi snímačov pohybu. V prípade každého zašifrovaného sériového čísla musí MSCA oznámiť výrobcovi snímačov pohybu číslo verzie príslušného K_{ID}.

CSM_109 Pre požiadavky CSM_107 a CSM_108 musí MSCA použiť algoritmus AES v prevádzkovom režime reťazenia šifrovacieho bloku, ako je vymedzené v norme [ISO 10116], s parametrom prekladania (interleave parameter) *m* = 1 a inicializačným vektorom SV = '00' {16}, t. j. šestnásť bajtov s binárnou hodnotu 0. V prípade potreby musí MSCA použiť metódu výplne 2 vymedzenú v norme [ISO 9797-1].

CSM_110 Výrobca snímačov pohybu musí uchovávať šifrovaný párovací kľúč a šifrované sériové číslo v určenom snímači pohybu, spolu so zodpovedajúcimi nezašifrovanými hodnotami textu a číslom verzie K_M a K_{ID} použitej na šifrovanie.

Poznámka: Ako je vysvetlené v oddiele 9.2.1.2, v skutočnosti je možné, že výrobca snímačov pohybu bude musieť do jedného snímača pohybu vložiť viaceré zašifrované párovacie kľúče a viaceré zašifrované sériové čísla.

CSM_111 Okrem kryptografického materiálu založeného na AES špecifikovaného v CSM_110 môže tiež výrobca snímačov pohybu v každom snímači pohybu uložiť kryptografický materiál založený na TDES špecifikovaný v požiadavke CSM_ 037 v časti A tohto dodatku.

Poznámka: to umožní snímaču pohybu druhej generácie, aby sa spojil s VU prvej generácie.

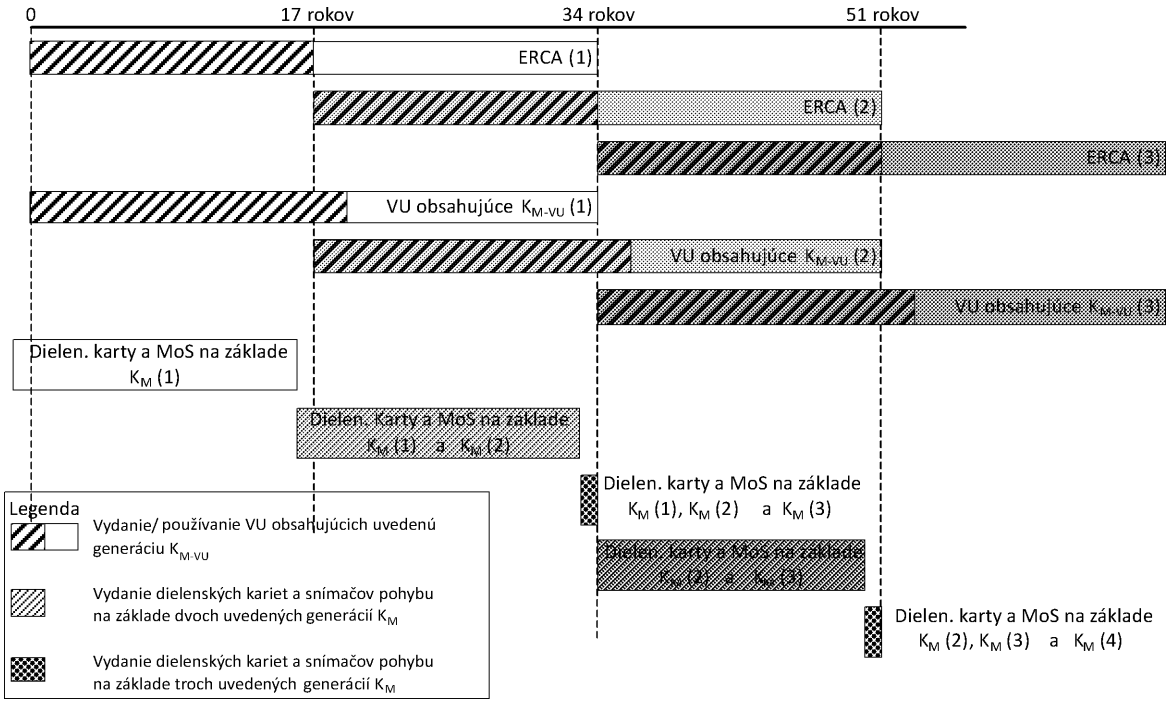
CSM_112 Dĺžka kľúča relácie K_S vygenerovaného VU počas párovania so snímačom pohybu musí byť prepojená s dĺžkou jeho K_{M-VU}, ako je opísané v CSM_50.

9.2.1.2 *Nahradenie hlavného kľúča snímača pohybu v zariadení druhej generácie*

CSM_113 Každý hlavný kľúč snímača pohybu a všetky súvisiace kľúče (pozri tabuľku 3) je spojený s konkrétnou generáciou páru koreňových kľúčov ERCA. Tieto kľúče sa preto musia nahradiť každých 17 rokov. Obdobie platnosti každej generácie hlavného kľúča snímača pohybu sa musí začať jeden rok predtým, ako príslušný pár koreňových kľúčov ERCA nadobudne platnosť a skončiť vtedy, keď sa skončí platnosť príslušného páru koreňových kľúčov ERCA. Je to znázornené na obrázku 2.

Obrázok 2

Vydávanie a používanie rôznych generácií hlavného kľúča snímača pohybu v jednotkách vozidla, snímačoch pohybu a dielenských kartách



CSM_114 Aspoň jeden rok pred vygenerovaním nového európskeho páru koreňových kľúčov, ako je opísané v CSM_56, musí ERCA vygenerovať nový hlavný kľúč snímača pohybu K_M vygenerovaním nového K_{M-VU} a K_{M-WC}. Dĺžka hlavného kľúča snímača pohybu musí byť, podľa CSM_50, prepojená s predpokladanou silou zabezpečenia nového európskeho páru koreňových kľúčov. Keď o to MSCA požiadajú, musí im ERCA oznámiť nové K_M, K_{M-VU} a K_{M-WC} spolu s číslami ich verzií.

CSM_115 MSCA musí zabezpečiť, aby boli všetky platné generácie K_{M-WC} uložené na každej dielenskej karte vydanej v rámci jeho právomoci, spolu s číslami ich verzií, ako sa uvádza na obrázku 2.

Poznámka: to znamená, že v poslednom roku obdobia platnosti certifikátu ERCA sa dielenské karty vydajú s tromi rôznymi generáciami K_{M-WC}, ako je znázornené na obrázku 2.

CSM_116 V súvislosti s procesom už opísaným v CSM_107 a CSM_108: MSCA musí zašifrovať každý párovací kľúč K_P, ktorý dostane od výrobcu snímačov pohybu, samostatne s každou platnou generáciou hlavného kľúča snímača pohybu K_M. MSCA musí zašifrovať aj každé sériové číslo, ktoré dostane o výrobcu snímačov pohybu, samostatne s každou platnou generáciou hlavného kľúča snímača pohybu K_{ID}. Výrobca snímačov pohybu musí uchovávať všetky šifry párovacieho kľúča a všetky šifry sériového čísla v určenom snímači pohybu, spolu so zodpovedajúcimi nezašifrovanými hodnotami textu a číslom(-ami) verzie K_M a K_{ID} použitej na šifrovanie.

Poznámka: to znamená, že v poslednom roku obdobia platnosti certifikátu ERCA sa snímače pohybu vydajú so zašifrovanými údajmi založenými na troch rôznych generáciách K_{M-WC}, ako je znázornené na obrázku obrázku 2.

CSM_117 V súvislosti s procesom už opísaným v CSM_107: Keďže dĺžka párovacieho kľúča K_P musí byť prepojená s dĺžkou K_M (pozri CSM_100), môže sa stať, že výrobca snímačov pohybu bude musieť vygenerovať až tri rôzne párovacie kľúče (rôznych dĺžok) pre jeden snímač pohybu, ak majú následné generácie K_M rôznu dĺžku. V takom prípade musí výrobca poslať MSCA každý párovací kľúč. MSCA musí zabezpečiť, aby bol každý párovací kľúč zašifrovaný správnou generáciou hlavného kľúča snímača pohybu, teda tou, ktorá má rovnakú dĺžku.

Poznámka: Ak sa výrobca snímačov pohybu rozhodne vygenerovať párovací kľúč založený na TDES pre snímač pohybu druhej generácie (pozri CSM_111), výrobca musí pre MSCA uviesť, že na šifrovanie tohto párovacieho kľúča sa musí použiť hlavný kľúč snímača pohybu založený na TDES. Je to preto, že dĺžka kľúča TDES môže byť rovnaká ako dĺžka kľúča AES, takže to MSCA nemôže posúdiť len z dĺžky kľúča.

CSM_118 Výrobcovia jednotiek vozidla musia do každej jednotky vozidla vložiť len jednu generáciu K_{M-VU} spolu číslom jej verzie. Táto generácia K_{M-VU} musí byť prepojená s certifikátom ERCA, na ktorom sú certifikáty VU založené.

Poznámky:

— Jednotka vozidla založená certifikáte ERCA generácie *X* musí obsahovať len K_{M-VU} generácie *X*, aj keď bolo vydané po začiatku obdobia platnosti certifikátu ERCA generácie *X+1*. Je to znázornené na obrázku 2.

— VU generácie *X* nemôže byť párovaná so snímačom pohybu generácie *X-1*.

— Keďže obdobie platnosti dielenských kariet je jeden rok, výsledkom CSM_113 – CSM_118 je, že všetky dielenské karty budú obsahovať nové K_{M-WC} v čase vydania prvej VU, ktorá obsahuje nové K_{M-VU}. Preto takáto VU bude vždy schopná vypočítať nové K_M. Okrem toho dovtedy bude väčšina nových snímačov pohybu tiež obsahovať šifrované údaje založené na novom K_M.

9.2.2 *Kľúče na zabezpečenie komunikácie DSRC*

9.2.2.1 *Všeobecné*

CSM_119 Autenticita a dôvernosť údajov oznámených z jednotky vozidla kontrolnému orgánu cez kanál diaľkovej komunikácie DRSC musí byť zabezpečená súborom kľúčov AES určených pre VU, odvodených od jediného hlavného kľúča DSRC, KM_{DRSC}.

CSM_120 Hlavný kľúč DSRC KM_{DRSC} musí byť kľúč AES, ktorý je bezpečne vygenerovaný, uložený a distribuovaný ERCA. Dĺžka kľúča môže byť 128, 192 alebo 256 bitov a musí byť prepojená s dĺžkou európskeho páru koreňových kľúčov, ako je opísané v CSM_50.

CSM_121 ERCA musí certifikačným autoritám členských štátov na ich žiadosť zabezpečene oznámiť hlavný kľúč DRSC, s cieľom umožniť im odvodiť DSRC kľúče určené pre VU a zabezpečiť, aby bol hlavný kľúč DRSC vložený do všetkých kontrolných a dielenských kariet vydaných v rámci ich zodpovednosti.

CSM_122 ERCA musí každému hlavnému kľúču DRSC prideliť jedinečné číslo verzie. ERCA musí pri zasielaní hlavného kľúča DRSC informovať MSCA o čísle verzie.

Poznámka: Číslo verzie sa používa na rozlíšenie rôznych generácií hlavného kľúča DRSC, ako je podrobne vysvetlené v oddiele 9.2.2.2.

CSM_123 Pre každú jednotku vozidla musí výrobca jednotiek vozidla vytvoriť jedinečné sériové číslo VU a poslať toto číslo certifikačnej autorite svojho členského štátu s cieľom získať súbor dvoch kľúčov DSRC určených pre VU. Sériové číslo VU musí mať dátový typ `VuSerialNumber`, a na kódovanie sa musia uplatniť odlíšené kódovacie pravidlá (DER) podľa normy [ISO 8825-1].

CSM_124 Po prijatí žiadosti o kľúče DRSC určené pre VU musí MSCA pre jednotku vozidla odvodiť dva kľúče AES, nazvané K_VU_{DSRC}_ENC a K_VU_{DSRC}_MAC. Tieto kľúče určené pre VU musia mať rovnakú dĺžku ako hlavný kľúč DRSC. MSCA musí použiť funkciu odvodenia kľúča vymedzenú v [RFC 5869]. Hašovacia funkcia, ktorá je potrebná na konkretizáciu funkcie HMAC-Hash, musí byť prepojená s dĺžkou hlavného kľúča DSRC, ako je uvedené v CSM_50. Funkcia odvodenia kľúča v [RFC 5869] sa musí použiť takto:

Krok 1 (Extrakcia):

— *PRK* = HMAC-Hash (*salt, IKM*) kde *salt* je prázdny reťazec ‘ ’ a *IKM* je KM_{DSRC}.

Krok 2 (Expanzia):

— *OKM* = *T(1)*, kde

T(1) = HMAC-Hash (*PRK, T(0)* || *info* || ‘01’) s

— *T(0)* = prázdny reťazec (‘ ’)

— *info* = sériové číslo VU, ako je špecifikované v CSM_123

— K_VU_{DSRC}_ENC = prvé *L* oktety *OKM* a

K_VU_{DSRC}_ENC = posledné *L* oktety *OKM*

kde *L* je požadovaná dĺžka K_VU_{DSRC}_ENC a K_VU_{DSRC}_MAC v oktetoch.

CSM_125 MSCA musí zabezpečene zaslať K_VU_{DSRC}_ENC a K_VU_{DSRC}_MAC výrobcovi VU, aby mohli byť vložené do určenej jednotky vozidla.

CSM_126 Po vydaní musí jednotka vozidla mať uložené K_VU_{DSRC}_ENC a K_VU_{DSRC}_MAC v zabezpečenej pamäti, aby bola schopná zaistiť integritu, autenticitu a dôvernosť údajov poslaných diaľkovým komunikačným kanálom. Jednotka vozidla musí uchovávať aj číslo verzie hlavného kľúča DSRC použitého na odvodenie týchto kľúčov určených pre VU.

CSM_127 Po vydaní musia kontrolné a dielenské karty mať uložené KM_{DSRC} v zabezpečenej pamäti, aby boli schopné overiť integritu a autenticitu údajov poslaných VU diaľkovým komunikačným kanálom a dešifrovať tieto údaje. Kontrolné a dielenské karty musia uložiť aj číslo verzie hlavného kľúča DRSC.

Poznámka: Ako je vysvetlené v oddiele 9.2.2.2, v skutočnosti môže byť potrebné, aby sa do jedinej dielenskej alebo kontrolnej karty vložili viaceré generácie KM_{DRSC}.

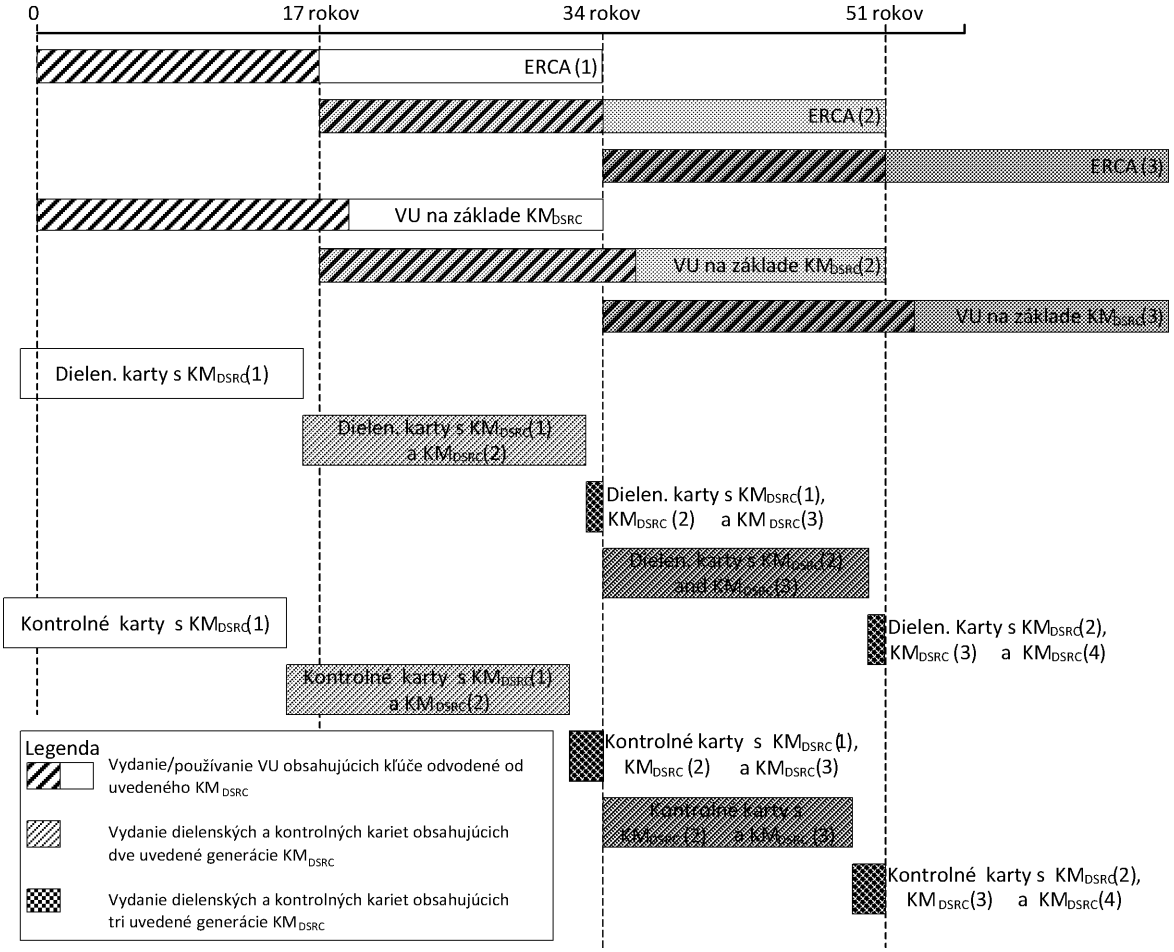
CSM_128 MSCA musí uchovávať záznamy o všetkých kľúčoch DSRC určených pre VU, ktoré vygeneroval, číslo ich verzií a identifikáciu VU, pre ktorú je každý súbor kľúčov určený.

9.2.2.2 *Nahradenie hlavného kľúča DSRC*

CSM_129 Každý hlavný kľúč DRSC je spojený s konkrétnou generáciou páru koreňových kľúčov ERCA. ERCA musí preto nahradiť hlavný kľúč DRSC každých 17 rokov. Obdobie platnosti každej generácie hlavného kľúča DRSC sa musí začať dva roky predtým, ako príslušný pár koreňových kľúčov ERCA nadobudne platnosť, a skončiť vtedy, keď sa skončí platnosť príslušného páru koreňových kľúčov ERCA. Je to znázornené na obrázku 3.

Obrázok 3

Vydávanie a používanie rôznych generácií hlavného kľúča DRSC v jednotkách vozidla, dielenských kartách a kontrolných kartách



CSM_130 Aspoň dva roky pred vygenerovaním nového európskeho páru koreňových kľúčov, ako je opísané v CSM_56, musí ERCA vygenerovať nový hlavný kľúč DRSC. Dĺžka kľúča DRSC musí byť, podľa CSM_50, prepojená s predpokladanou silou zabezpečenia nového európskeho páru koreňových kľúčov. Keď o to MSCA požiadajú, musí im ERCA oznámiť nový hlavný kľúč DRSC spolu s číslom jeho verzie.

CSM_131 MSCA musí zabezpečiť, aby boli všetky platné generácie KM_{DRSC} uložené na každej kontrolnej karte vydanej v rámci jej právomoci, spolu s číslami ich verzií, ako sa uvádza v obrázku 3.

Poznámka: to znamená, že v posledných dvoch rokoch obdobia platnosti certifikátu ERCA sa kontrolné karty vydajú s tromi rôznymi generáciami KM_{DRSC}, ako je znázornené na obrázku obrázku 3.

CSM_132 MSCA musí zabezpečiť, aby všetky generácie KM_{DRSC}, ktoré boli platné minimálne rok a stále sú platné, boli uložené na každej dielenskej karte vydanej v rámci jeho právomoci, spolu s číslami ich verzií, ako sa uvádza na obrázku 3.

Poznámka: to znamená, že v poslednom roku obdobia platnosti certifikátu ERCA sa dielenské karty vydajú s tromi rôznymi generáciami KM_{DRSC}, ako je znázornené na obrázku 3.

CSM_133 Výrobcovia jednotiek vozidla musia do každej jednotky vozidla vložiť len jednu sadu kľúčov DRSC určených pre VU, spolu s číslom verzie. Tento súbor kľúčov sa musí odvodiť z generácie KM_{DRSC} prepojenej s certifikátom ERCA, na ktorom sú certifikáty VU založené.

Poznámky:

— To znamená, že jednotka vozidla založená na certifikáte ERCA generácie *X* musí obsahovať len K_VU_{DSRC}_ENC a K_VU_{DSRC}_MAC generácie *X*, aj keď bola VU vydaná po začiatku obdobia platnosti certifikátu ERCA generácie *X+1*. Je to znázornené na obrázku 3.

— Keďže dielenské karty majú obdobie platnosti jeden rok a kontrolné karty dva roky, výsledkom CSM_131 – CSM_133 je, že všetky dielenské a kontrolné karty budú obsahovať nový hlavný kľúč DSRC v čase, keď budú vydané prvé VU obsahujúce kľúče určené pre VU založené na danom hlavnom kľúči.

9.3. **Certifikáty**

9.3.1 *Všeobecné*

CSM_134 Všetky certifikáty v európskom systéme inteligentných tachografov musia byť samoopisné, kartou overiteľné (CV) certifikáty podľa [ISO 7816-4] a [ISO 7816-8].

CSM_135 Na kódovanie dátových štruktúr ASN.1 i dátových objektov (pre konkrétne aplikácie) v rámci certifikátov sa musia použiť odlíšené kódovacie pravidlá (DER) podľa [ISO 8825-1].

Poznámka: Výsledkom tohto kódovania je takáto štruktúra tag-dĺžka-hodnota (TLV):

Tag: Tag je kódovaný v jednom alebo dvoch oktetoch a určuje obsah.

Dĺžka: dĺžka je kódovaná ako celé číslo bez znamienka v jednom, dvoch alebo troch oktetoch, čoho výsledkom je maximálna dĺžka 65 535 oktetov. Musí sa použiť minimálny počet oktetov.

Hodnota: Hodnota je kódovaná v nula alebo viac oktetoch

9.3.2 *Obsah certifikátu*

CSM_136 Všetky certifikáty musia mať štruktúru uvedenú v profile certifikátu v tabuľke 4.

Tabuľka 4

Verzia 1 profilu certifikátu

Pole	ID poľa	Tag	Dĺžka (v bajtoch)	Dátový typ ASN.1 (pozri dodatok 1)
Certifikát ECC	C	'7F 21'	var	
Hlavná časť certifikátu ECC	B	'7F 4E'	var	

Pole	ID poľa	Tag	Dĺžka (v bajtoch)	Dátový typ ASN.1 (pozri dodatok 1)
Identifikátor profilu certifikátu	CPI	‘5F 29’	‘01’	INTEGER(0..255)
Referencia certifikačnej autority (Certificate Authority Reference)	CAR	‘42’	‘08’	KeyIdentifier
Autorizácia držiteľa certifikátu	CHA	‘5F 4C’	‘07’	CertificateHolder Authorisation
Verejný kľúč	PK	‘7F 49’	var	
Parametre domény	DP	‘06’	var	OBJECT IDENTIFIER
Verejný bod	PP	‘86’	var	OCTET STRING
Referencia držiteľa certifikátu	CHR	‘5F 20’	‘08’	KeyIdentifier
Dátum nadobudnutia účinnosti certifikátu	CEfD	‘5F 25’	‘04’	TimeReal
Dátum uplynutia platnosti certifikátu	CExD	‘5F 24’	‘04’	TimeReal
Podpis certifikátu ECC	S	‘5F 37’	var	OCTET STRING

Poznámka: ID poľa sa použije v ďalších častiach tohto dodatku na označenie jednotlivých polí certifikátu, napr. X.CAR je referencia certifikačnej autority uvedená v certifikáte používateľa X.

9.3.2.1 Identifikátor profilu certifikátu

CSM_137 Certifikáty musia uvádzať identifikátor profilu certifikátu, aby sa identifikoval použitý profil certifikátu. Verzia 1 špecifikovaná v tabuľke 4 musí byť identifikovaná hodnotou ‘00’.

9.3.2.2 Referencia certifikačnej autority

CSM_138 Referencia certifikačnej autority sa použije na identifikáciu verejného kľúča, ktorý sa má použiť na overenie podpisu certifikátu. Referencia certifikačnej autority preto musí byť rovnaká, ako referencia držiteľa certifikátu v certifikáte zodpovedajúcej certifikačnej autority.

CSM_139 Koreňový certifikát ERCA musí byť samopodpísaný, t. j. referencia certifikačnej autority a referencia držiteľa v certifikáte musia byť rovnaké.

CSM_140 V prípade prepájacieho certifikátu ERCA musí byť referencia držiteľa certifikátu rovná CHR nového koreňového certifikátu ERCA. Referencia certifikačnej autority pre prepájací certifikát sa musí rovnať CHR predchádzajúceho koreňového certifikátu ERCA.

9.3.2.3 Autorizácia držiteľa certifikátu

CSM_141 Autorizácia držiteľa certifikátu sa použije na identifikovanie typu certifikátu. Pozostáva zo šiestich bajtov najvyššieho rádu ID tachografovej aplikácie zreťazených s typom zariadenia, pre ktorý je certifikát určený.

9.3.2.4 Verejný kľúč

Verejný kľúč obsahuje dva dátové prvky: štandardizované parametre domény, ktoré sa majú použiť s verejným kľúčom v certifikáte, a hodnotu verejného bodu.

CSM_142 Dátový prvok Parametre domény musí obsahovať jeden z objektových identifikátorov uvedených v tabuľke 1, aby odkazoval na súbor štandardizovaných parametrov domény.

CSM_143 Dátový prvok verejný bod musí obsahovať verejný bod. Verejné body eliptickej krivky sa musia premeniť na oktetové reťazce, ako je špecifikované v [TR-03111]. Musí sa použiť nekomprimovaný kódovací formát. Pri obnove bodu eliptickej krivky z jeho zakódovaného formátu sa musia vždy vykonať overenia opísané v [TR-03111].

9.3.2.5 Referencia držiteľa certifikátu

CSM_144 Referencia držiteľa certifikátu je identifikátor pre verejný kľúč uvedený v certifikáte. Musí sa používať ako odkaz na verejný kľúč v iných certifikátoch.

CSM_145 V prípade certifikátov karty a certifikátov externých zariadení GNSS musí mať referencia držiteľa certifikátu dátový typ `ExtendedSerialNumber` uvedený v dodatku 1.

CSM_146 Pre jednotky vozidla výrobca pri žiadosti o certifikát môže, ale nemusí poznať špecifické sériové číslo výrobcu pre VU, pre ktorú je daný certifikát a príslušný súkromný kľúč určený. V prvom prípade musí mať referencia držiteľa certifikátu dátový typ `ExtendedSerialNumber` uvedený v dodatku 1. V druhom prípade musí mať referencia držiteľa certifikátu dátový typ `CertificateRequestID` uvedený v dodatku 1.

CSM_147 V prípade certifikátov ERCA a MSCA musí mať referencia držiteľa certifikátu dátový typ `CertificationAuthorityKID` uvedený v dodatku 1.

9.3.2.6 Dátum nadobudnutia účinnosti certifikátu

CSM_148 Dátum nadobudnutia účinnosti certifikátu musí označovať dátum a čas začiatku platnosti certifikátu. Dátumom nadobudnutia účinnosti certifikátu je dátum generácie certifikátu.

9.3.2.7 Dátum uplynutia platnosti certifikátu

CSM_149 Dátum uplynutia platnosti certifikátu musí označovať dátum a čas skončenia platnosti certifikátu.

9.3.2.8 Podpis certifikátu

CSM_150 Podpis na certifikáte sa musí realizovať na zakódovanej hlavnej časti certifikátu vrátane tagu a dĺžky hlavnej časti certifikátu. Algoritmus podpisu musí byť ECDSA, ako je uvedené v [DSS], s použitím hašovacieho algoritmu prepojeného s veľkosťou kľúča podpisovej autority, ako je uvedené v CSM_50. Formát podpisu musí byť nezašifrovaný, ako je uvedené v [TR-03111].

9.3.3 *Žiadosti o certifikáty*

CSM_151 Pri žiadosti o certifikát musí žiadateľ poslať certifikačnej autorite tieto údaje:

— identifikátor profilu požadovaného certifikátu

— očakávanú referenciu certifikačnej autority, ktorá sa má použiť na podpísanie certifikátu.

— verejný kľúč, ktorý sa má podpísať

CSM_152 Okrem údajov v CSM_151 musí MSCA v žiadosti o certifikát poslať ERCA tieto údaje, čo umožní ERCA vytvoriť referenciu držiteľa nového certifikátu MSCA:

— numerický kód štátu certifikačnej autority (dátový typ `NationNumeric` vymedzený v dodatku 1)

— alfanumerický kód štátu certifikačnej autority (dátový typ `NationAlpha` vymedzený v dodatku 1)

— 1-bajtové sériové číslo na rozlíšenie rôznych kľúčov certifikačnej autority, ak sa kľúče menia

— dvojbajtové pole s osobitnými doplňujúcimi informáciami certifikačnej autority

CSM_153 Okrem údajov v CSM_151 musí výrobca zariadení v žiadosti o certifikát poslať MSCA tieto údaje, čo umožní MSCA vytvoriť referenciu držiteľa nového certifikátu zariadenia:

— identifikátor typu zariadenia špecifický pre výrobcu

— ak je známe (pozri CSM_154), sériové číslo zariadenia jedinečné pre výrobcu, typ zariadenia a mesiac výroby. Inak jedinečný identifikátor žiadosti o certifikát.

— Mesiac a rok výroby zariadenia alebo žiadosti o certifikát.

Výrobca musí zabezpečiť, že tieto údaje sú správne a že certifikát získaný od MSCA sa vloží do určeného zariadenia.

CSM_154 V prípade VU výrobca pri žiadosti o certifikát môže, ale nemusí poznať špecifické sériové číslo výrobcu pre VU, pre ktorú je daný certifikát a príslušný súkromný kľúč určený. Ak je sériové číslo známe, musí ho výrobca VU poslať MSCA. Ak nie je známe, výrobca musí jedinečne identifikovať každú žiadosť o certifikát a poslať toto sériové číslo žiadosti o certifikát MSCA. Výsledný certifikát bude obsahovať sériové číslo žiadosti o certifikát. Po vložení certifikátu do konkrétnej VU musí výrobca oznámiť spojenie medzi sériovým číslom žiadosti o certifikát a identifikáciou VU autorite MSCA.

10. VZÁJOMNÁ AUTENTIFIKÁCIA VU-KARTA A ZABEZPEČENÉ SPRACOVANIE

10.1. **Všeobecné**

CSM_155 Na vysokej úrovni musí zabezpečená komunikácia medzi jednotkou vozidla a tachografovou kartou vychádzať z týchto krokov:

— Po prvé, každá strana musí preukázať druhej strane, že vlastní platný certifikát verejného kľúča, ktorý podpísala certifikačná autorita členského štátu. Certifikát verejného kľúča MSCA musí byť zas podpísaný európskou koreňovou certifikačnou autoritou. Tento krok sa nazýva overenie certifikačného reťazca a je podrobne opísaný v oddiele 10.2.

— Po druhé, jednotka vozidla musí karte preukázať, že má k dispozícii súkromný kľúč zodpovedajúci verejnému kľúču v predloženom certifikáte. Urobí tak podpisom náhodného čísla poslaného kartou. Karta overí podpis náhodného čísla. Ak je toto overenie úspešné, VU je autentifikovaná. Tento krok sa nazýva autentifikácia VU a je podrobne opísaný v oddiele 10.3.

— Po tretie, obidve strany nezávisle vypočítajú dva kľúče relácie AES asymetrickým algoritmom kľúčovej dohody. Jedným z týchto kľúčov relácie karta vytvára autentifikačný kód správy (MAC) na niektoré údaje zaslané VU. VU overuje MAC. Ak je toto overenie úspešné, karta je autentifikovaná. Tento krok sa nazýva autentifikácia karty a je podrobne opísaný v oddiele 10.4.

— Po štvrté, VU a karta musia používať dohodnuté kľúče relácie, aby sa zabezpečila dôvernosť, integrita a autenticita všetkých vymenených správ. Nazýva sa to zabezpečené spracovanie a je to podrobne opísané v oddiele 10.5.

CSM_156 Mechanizmus opísaný v CSM_155 sa spúšťa jednotkou vozidla vždy, keď je karta vložená do jedného z jej slotov.

10.2. **Vzájomné overovanie certifikačných reťazcov**

10.2.1 *Overovanie certifikačných reťazcov karty zo strany VU*

CSM_157 Jednotky vozidla musia na overovanie certifikačného reťazca tachografovej karty použiť protokol zobrazený na obrázku 4.

Poznámky k obrázku 4:

— Certifikáty karty a verejné kľúče uvedené na obrázku sú tie, ktoré sú určené na vzájomnú autentifikáciu. V oddiele 9.1.5 sa označujú ako Card_MA.

— Certifikáty Card.CA a verejné kľúče uvedené na obrázku sú certifikáty a kľúče určené na podpísanie certifikátov karty a je to uvedené v CAR certifikátu karty. V oddiele 9.1.3 sa označujú ako MSCA_Card.

— Certifikát Card.CA.EUR uvedený na obrázku je európsky koreňový certifikát, ktorý je uvedený v CAR certifikátu Card.CA.

— Certifikát Card.Link uvedený na obrázku je prípadný prepájací certifikát karty. Ako je uvedené v oddiele 9.1.2, je to prepájací certifikát pre nový európsky pár koreňových kľúčov vytvorený ERCA a podpísaný predchádzajúcim európskym súkromným kľúčom.

— Certifikát Card.Link.EUR je európsky koreňový certifikát, ktorý je uvedený v CAR certifikátu Card.Link.

CSM_158 Ako je znázornené na obrázku 4, overenie certifikačného reťazca karty sa musí začať po vložení karty. Jednotka vozidla musí prečítať referenciu držiteľa karty(`cardExtendedSerialNumber`) z EF ICC. VU musí kontrolovať, či kartu pozná, t. j., či úspešne overila certifikačný reťazec karty v minulosti a uložila ho do budúcnosti. Ak ju pozná a certifikát karty je stále platný, proces pokračuje overením certifikačného reťazca VU. Inak musí VU postupne z karty čítať certifikát MSCA_Card, ktorý sa ma použiť na overovanie certifikátu karty, certifikát Card.CA. EUR, ktorý sa má použiť na overovanie certifikátu MSCA_Card, a prípadne prepájací certifikát, pokým nenájde certifikát, ktorý pozná alebo môže overiť. Ak takýto certifikát nájde, VU tento certifikát použije na overenie základných certifikátov karty, ktoré VU prečítala z danej karty. Ak bude tento proces úspešný, pokračuje overením certifikačného reťazca VU. Ak nebude úspešný, VU musí kartu ignorovať.

Poznámka: Existujú tri spôsoby, ktorými môže VU certifikát Card.CA.EUR poznať:

— certifikát Card.CA.EUR je ten istý certifikát ako vlastný certifikát EUR jednotky vozidla;

— certifikát Card.CA.EUR predchádza vlastný certifikát EUR jednotky vozidla a VU už obsahovala tento certifikát v čase vydania (pozri CSM_81);

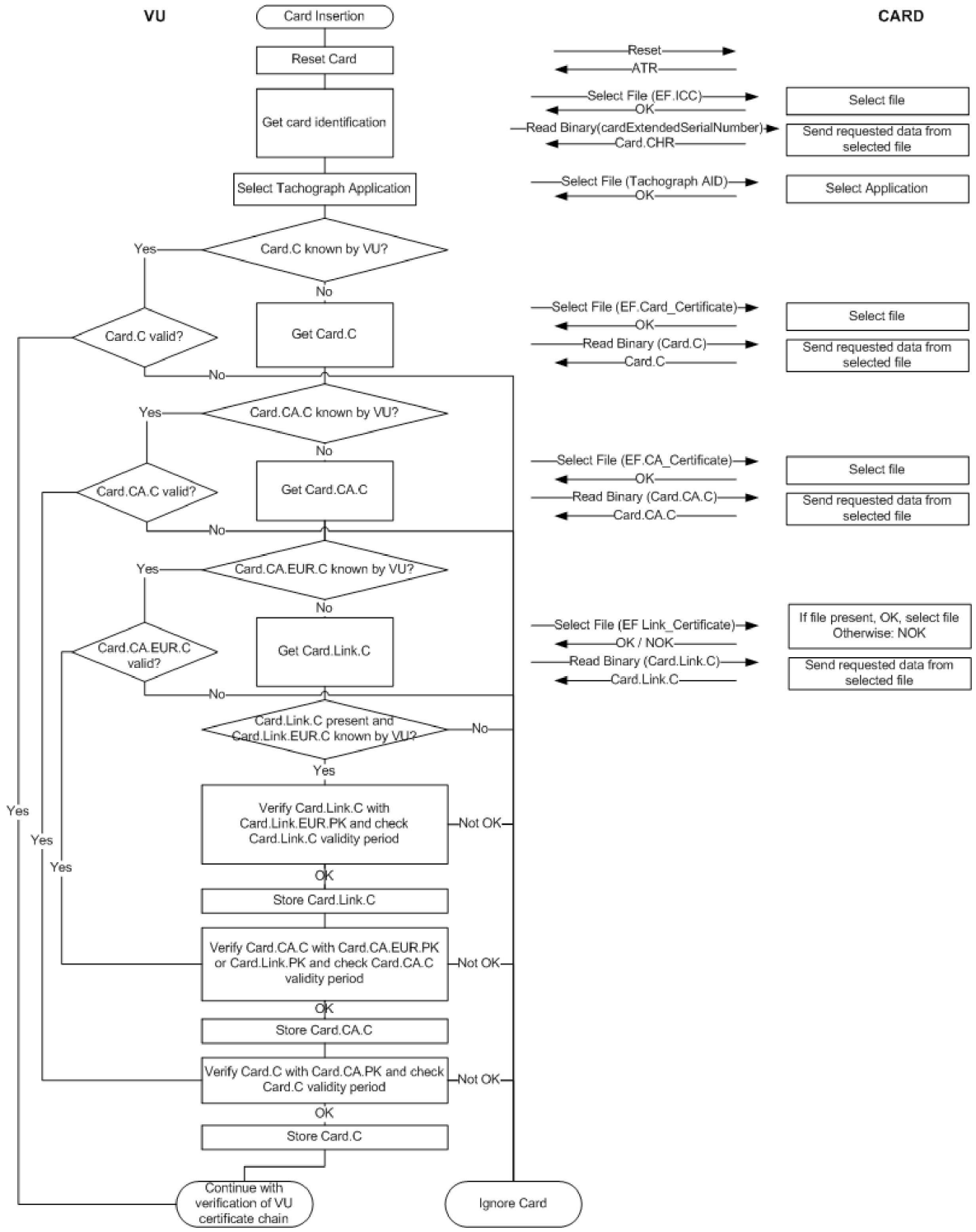
— certifikát Card.CA.EUR je nástupcom vlastného certifikátu EUR jednotky vozidla a VU získala prepájací certifikát v minulosti z inej tachografovej karty, overila ho a uložila do budúcnosti.

CSM_159 Ako sa uvádza v obrázku 4, keď VU overila autenticitu a platnosť predtým neznámeho certifikátu, môže uložiť tento certifikát do budúcnosti, aby keď sa s týmto certifikátom VU znova stretne nemusela znova overovať jeho autenticitu. Namiesto uloženia celého certifikátu si VU môže zvoliť, že uloží len obsah hlavnej časti certifikátu, ako je uvedené v oddiele 9.3.2.

CSM_160 VU musí overiť dočasnú platnosť každého certifikátu prečítaného z karty alebo uloženého v jej pamäti a zamietnuť certifikáty s uplynulou platnosťou. Na overenie dočasnej platnosti certifikátu predloženého kartou musí VU použiť svoje vstavané hodiny.

Obrázok 4

Protokol pre overovanie certifikačného reťazca karty jednotkou vozidla

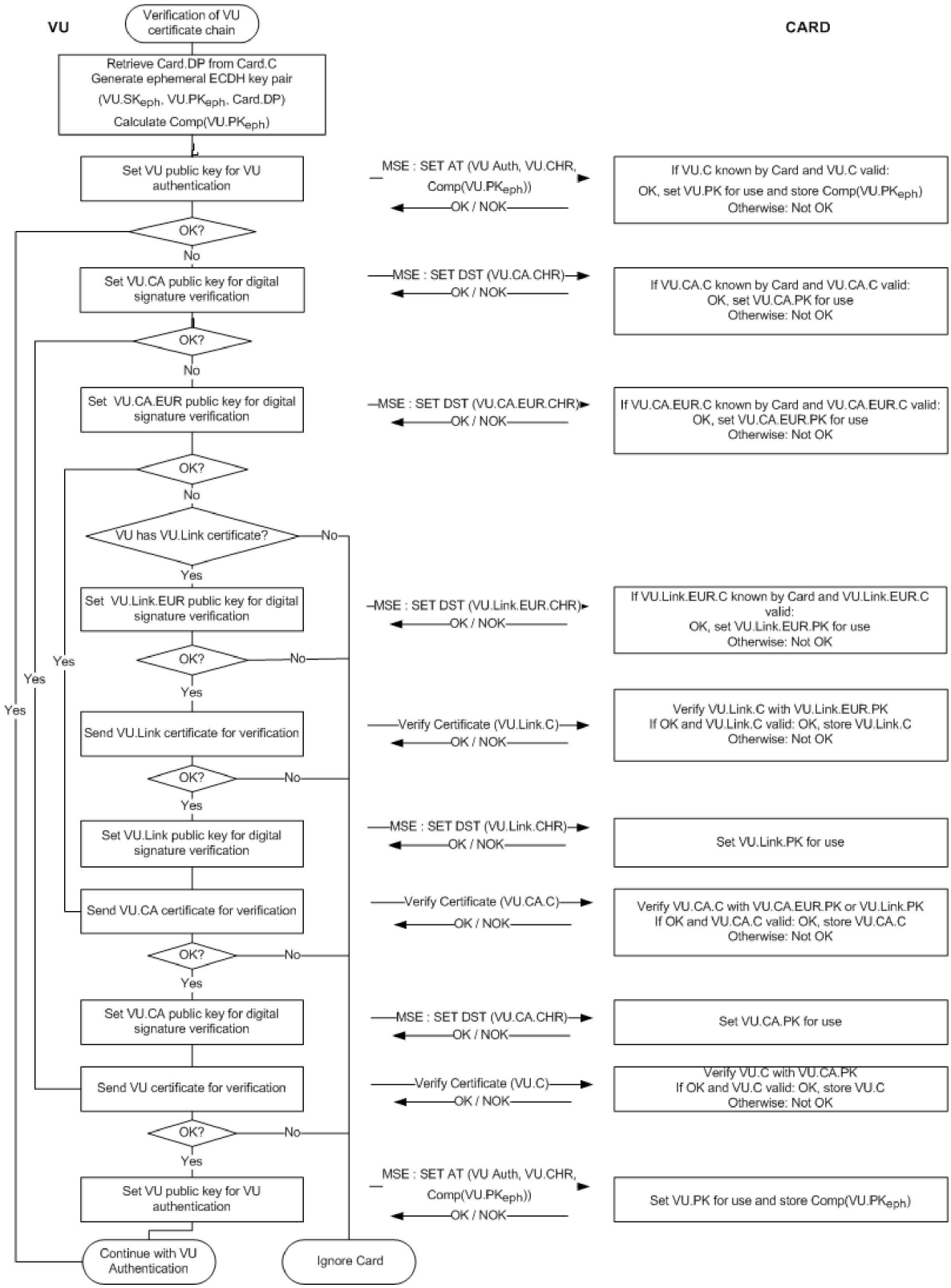


10.2.2 *Overovanie certifikačných reťazcov VU kartou*

CSM_161 Tachografové karty musia na overovanie certifikačného reťazca VU použiť protokol zobrazený na obrázku 5.

Obrázok 5

Protokol pre overovanie certifikačného reťazca VU kartou



Poznámky k obrázku 5:

— Certifikáty VU a verejné kľúče uvedené na obrázku sú tie, ktoré sú určené na vzájomnú autentifikáciu. V oddiele 9.1.4 sa označujú ako VU_MA.

— Certifikáty VU.CA a verejné kľúče uvedené na obrázku sú certifikáty a kľúče určené na podpísanie certifikátov VU a certifikátov externých zariadení GNSS. V oddiele 9.1.3 sa označujú ako MSCA_VU-EGF.

— Certifikát VU.CA.EUR uvedený na obrázku je európsky koreňový certifikát, ktorý je uvedený v CAR certifikátu VU.CA.

— Certifikát VU.Link uvedený na obrázku je prepájací certifikát VU, ak je prítomný. Ako je uvedené v oddiele 9.1.2, je to prepájací certifikát pre nový európsky pár koreňových kľúčov vytvorený ERCA a podpísaný predchádzajúcim európskym súkromným kľúčom.

— Certifikát VU.Link.EUR je európsky koreňový certifikát, ktorý je uvedený v CAR certifikátu VU.Link.

CSM_162 Ako je znázornené na obrázku 5, overenie certifikačného reťazca jednotky vozidla sa musí začať tým, že jednotka vozidla sa pokúsi nastaviť svoj vlastný verejný kľúč na použitie v tachografovej karte. Ak sa to podarí, znamená to, že karta v minulosti úspešne overila certifikačný reťazec VU a uložila certifikát VU do budúcnosti. V tomto prípade je certifikát VU nastavený na použitie a proces pokračuje autentifikáciou VU. Ak karta certifikát VU nepozná, VU musí postupne predložiť certifikát VU.CA, ktorý sa má použiť na overenie jej certifikátu VU, certifikát VU.CA.EUR, ktorý sa má použiť na overenie certifikátu VU.CA, a prípadne prepájací certifikát, s cieľom nájsť certifikát, ktorý karta pozná alebo môže overiť. Ak takýto certifikát nájde, karta musí tento certifikát použiť na overenie základných certifikátov VU, ktoré jej boli predložené. Ak bude toto overenie úspešné, VU musí nakoniec nastaviť svoj verejný kľúč, ktorý sa použije v tachografovej karte. Ak nebude úspešné, VU musí kartu ignorovať.

Poznámka: Existujú tri spôsoby, ako môže karta certifikát VU.CA.EUR poznať:

— certifikát VU.CA.EUR je totožný s vlastným certifikátom EUR karty;

— Certifikát VU.CA.EUR predchádza vlastný certifikát EUR karty a karta obsahovala tento certifikát už v čase vydania (pozri CSM_91);

— Certifikát VU.CA.EUR je nástupcom vlastného certifikátu EUR karty a karta získala prepájací certifikát v minulosti z inej jednotky vozidla, overila ho a uložila do budúcnosti.

CSM_163 VU musí použiť príkaz MSE: Set AT na nastavenie svojho verejného kľúča, ktorý sa použije v tachografovej karte. Ako je uvedené v dodatku 2, tento príkaz obsahuje označenie kryptografického mechanizmu, ktorý sa použije s kľúčom, ktorý je nastavený. Tento mechanizmus je „autentifikácia VU používajúca algoritmus ECDSA v kombinácii s hašovacím algoritmom prepojeným s veľkosťou kľúča kľúčového páru VU_MA jednotky vozidla, ako je uvedené v CSM_50“.

CSM_164 Príkaz MSE: Set AT obsahuje aj označenie efemérneho kľúčového páru, ktorý VU použije počas kľúčovej dohody relácie (pozri oddiel 10.4). Preto pred odoslaním príkazu MSE: Set AT musí VU vygenerovať efemérny kľúčový pár ECC. Na generovanie efemérneho kľúčového páru musí VU použiť štandardizované parametre domény uvedené v certifikáte karty. Efemérny kľúčový pár sa označuje ako ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). VU musí prijať x-ovú súradnicu efemérneho verejného bodu ECDH ako identifikáciu kľúča; To sa nazýva komprimované vyjadrenie verejného kľúča a označené ako Comp($VU.PK_{eph}$).

CSM_165 Ak je príkaz MSE: Set AT úspešný, karta nastaví uvedené VU.PK pre následné použitie počas autentifikácie vozidla a dočasne uložiť Comp($VU.PK_{eph}$). V prípade odoslania dvoch alebo viacerých úspešných príkazov MSE: Set AT pred vykonaním kľúčovej dohody relácie, karta musí uložiť len posledný prijatý Comp($VU.PK_{eph}$).

CSM_166 Karta musí overiť dočasnú platnosť každého certifikátu, ktorý VU predložila alebo naň odkazuje, uloženého v pamäti karty, a musí zamietnuť certifikáty s uplynulou platnosťou.

CSM_167 Na overenie dočasnej platnosti certifikátu, ktorý VU predložila, musí každá tachografová karta interne uložiť niektoré údaje, ktoré predstavujú aktuálny čas. Tieto údaje nesmie VU priamo aktualizovať. Pri vydaní musí byť aktuálny čas karty nastavený na dátum účinnosti certifikátu Card_MA karty. Karta musí aktualizovať svoj aktuálny čas, ak dátum účinnosti autentického certifikátu „platného zdroja času" predloženého VU je novší ako aktuálny čas karty. V takom prípade musí karta nastaviť svoj aktuálny čas na dátum účinnosti daného certifikátu. Karta ako platný zdroj času akceptuje len tieto certifikáty:

— Prepájacie certifikáty ERCA druhej generácie

— Certifikáty prepojenia MSCA druhej generácie

— Certifikáty VU druhej generácie vydané krajinou, ktorá vydala vlastný certifikát resp. certifikáty karty.

Poznámka: posledná požiadavka znamená, že karta musí byť schopná rozpoznať referenciu CAR certifikátu VU, t. j. certifikát MSCA_VU-EGF. Tá nebude rovnaká ako CAR jej vlastného certifikátu, ktorým je certifikát MSCA_card.

CSM_168 Ako sa uvádza v obrázku 5, keď karta overila autenticitu a platnosť predtým neznámeho certifikátu, môže uložiť tento certifikát do budúcnosti, aby keď sa s týmto certifikátom karta znova stretne nemusela znova overovať jeho autenticitu. Namiesto uloženia celého certifikátu si karta môže zvoliť, že uloží len obsah hlavnej časti certifikátu, ako je uvedené v bode 9.3.2.

10.3. **Autentifikácia VU**

CSM_169 Jednotky vozidla a karty musia používať na autentifikáciu VU pre kartu protokol autentifikácie VU zobrazený na obrázku 6. Autentifikácia VU umožňuje tachografovej karte výslovne overiť, že VU je autentická. Na to musí VU použiť svoj súkromný kľúč na podpis výzvy generovanej kartou.

CSM_170 VU k výzve karty v rámci podpisu pripojí referenciu držiteľa karty z certifikátu karty.

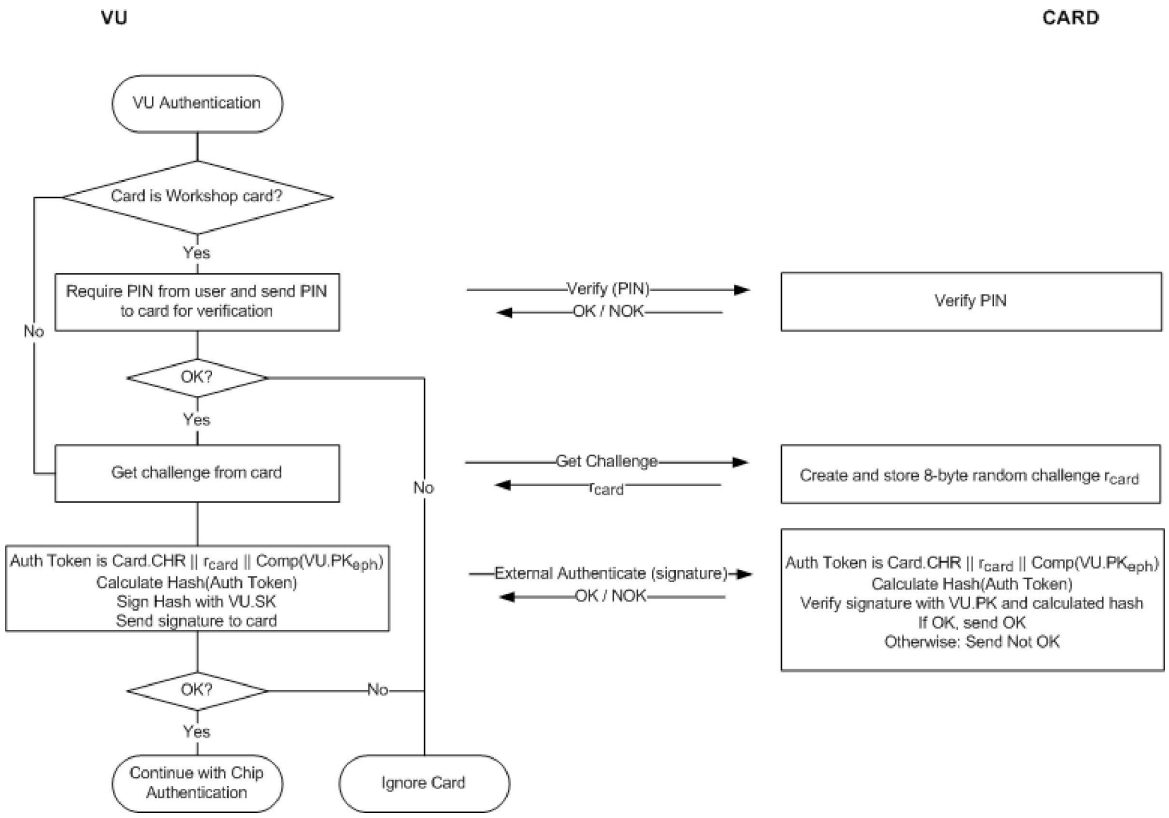
Poznámka: Tým sa zabezpečí, že karta, ktorej sa autentifikuje VU, je tá istá karta, ktorej certifikačný reťazec predtým VU overila.

CSM_171 VU musí v rámci podpisu pripojiť aj identifikátor efemérneho verejného kľúča Comp(VU.PK_{eph}), ktorý VU použije na nastavenie zabezpečeného spracovania počas procesu autentifikácie čipu uvedeného v oddiele 10.4.

Poznámka: To zabezpečuje, že VU, s ktorou karta komunikuje počas relácie zabezpečeného spracovania, je tá istá VU, ktorá bola overená kartou.

Obrázok 6

Protokol autentifikácie VU



CSM_172 Ak počas autentifikácie VU pošle VU viacnásobné príkazy GET CHALLENGE, karta musí vždy vrátiť novú 8-bajtovú náhodnú výzvu, ale uložiť len poslednú výzvu.

CSM_173 Algoritmus podpisovania použitý VU na autentifikáciu VU musí byť ECDSA, ako je uvedené v [DSS], použitím hašovacieho algoritmu prepojeného s veľkosťou kľúča kľúčového páru VU_MA jednotky vozidla, ako je uvedené v CSM_50. Formát podpisu musí byť nezašifrovaný, ako je uvedené v [TR-03111]. VU musí poslať výsledný podpis karte.

CSM_174 Po prijatí podpisu VU v príkaze EXTERNAL AUTHENTICATE, karta musí

— vypočítať autentifikačný znak zreťazením Card.CHR, výzvy karty r_{card} a identifikátora efemérneho verejného kľúča VU Comp(VU.PK_{eph}),

— vypočítať hash autentifikačného znaku pomocou hašovacieho algoritmu prepojeného s veľkosťou kľúča kľúčového páru VU_MA jednotky vozidla, ako je uvedené v CSM_50.

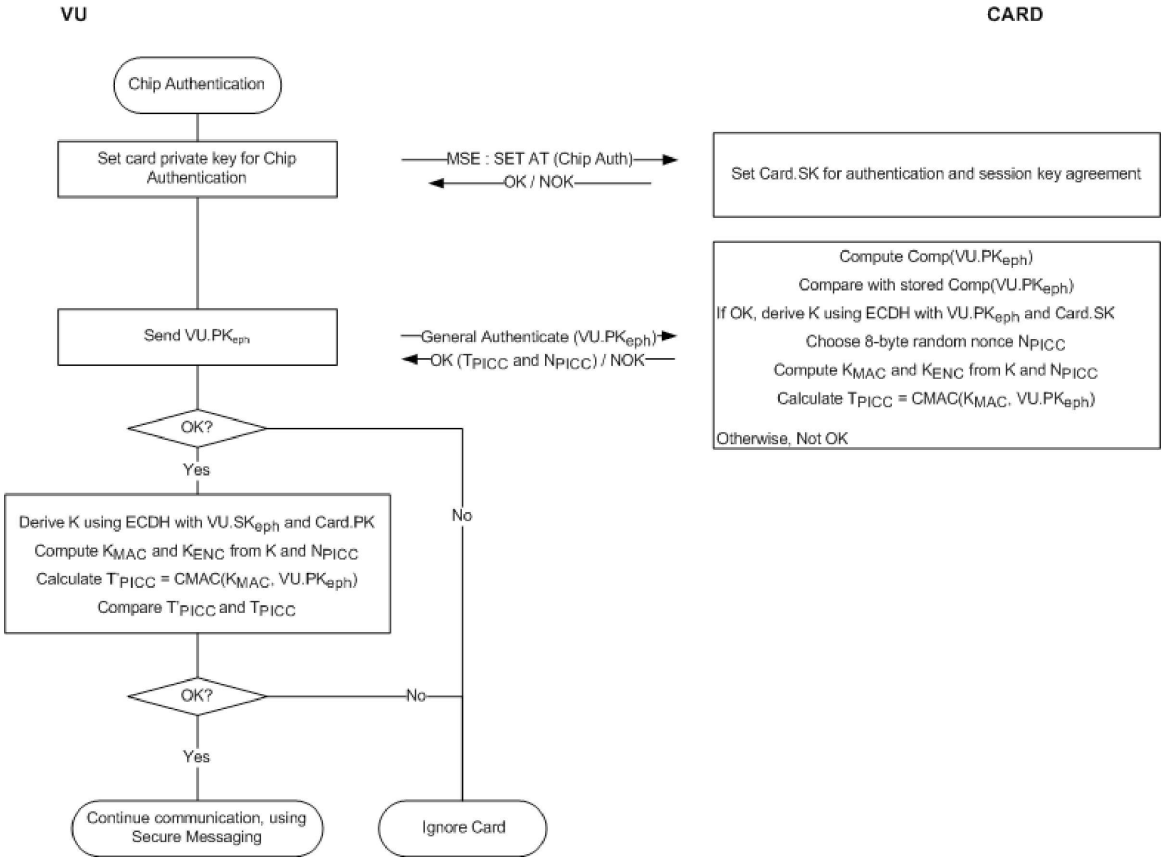
— overiť podpis VU pomocou algoritmu ECDSA v kombinácii s VU.PK a vypočítaným hashom.

10.4. Autentifikácia čipu a kľúčová dohoda relácie

CSM_175 Jednotky vozidla a karty musia používať na autentifikáciu karty pre VU protokol autentifikácie čipu zobrazený na obrázku 7. Autentifikácia čipu umožňuje jednotke vozidla výslovne overiť, že karta je autentická.

Obrázok 7

Autentifikácia čipu a kľúčová dohoda relácie



CSM_176 VU a karta musia vykonať tieto kroky:

1. Jednotka vozidla iniciuje proces autentifikácie čipu poslaním príkazu MSE: Set AT označujúceho „autentifikáciu čipu používajúcu algoritmus ECDH, čoho výsledkom je dĺžka kľúča relácie prepojená s dĺžkou kľúča kľúčového páru Card_MA karty, ako je uvedené v CSM_50“. VU musí určiť veľkosť kľúča kľúčový páru karty z certifikátu karty.

2. VU posiela verejný bod $VU.PK_{eph}$ jej efemérneho kľúčového páru karte. Ako je vysvetlené v CSM_164, VU vygenerovala tento efemérny kľúčový pár pred overovaním certifikačného reťazca VU. VU zaslala identifikátor efemérneho verejného kľúča $Comp(VU.PK_{eph})$ karte a karta ho uložila.

3. Karta vypočíta $Comp(VU.PK_{eph})$ z $VU.PK_{eph}$ a porovná ho s uloženou hodnotou $Comp(VU.PK_{eph})$.

4. Použitím algoritmu ECDH v kombinácii so statickým súkromným kľúčom karty a efemérnym verejným kľúčom VU karta vypočíta tajné K.

5. Karta náhodne vyberie 8-bajtovú jednorazovú hodnotu „nonce“ N_{PICC} a použije ju na odvodenie dvoch kľúčov relácie AES K_{MAC} a K_{ENC} z K. Pozri CSM_179.

6. Použitím K_{MAC} karta vypočíta autentifikačný znak na identifikátore efemérneho verejného kľúča VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Karta pošle N_{PICC} a T_{PICC} jednotke vozidla.

7. Použitím algoritmu ECDH v kombinácii so statickým verejným kľúčom karty a efemérnym súkromným kľúčom VU, VU vypočíta to isté tajné K, ako vypočítala karta v kroku 4.

8. VU odvodzuje kľúče relácie K_{MAC} a K_{ENC} z K a N_{PICC}; pozri CSM_179.

9. VU overuje autentifikačný znak T_{PICC}.

CSM_177 V uvedenom kroku 3 musí karta vypočítať Comp(VU.PKeph) ako x-ovú súradnicu verejného bodu vo VU.PKeph.

CSM_178 V uvedených krokoch 4 a 7 musia karta a jednotka vozidla použiť algoritmus ECKA-EG vymedzený v [TR-03111].

CSM_179 V uvedených krokoch 5 a 8 musia karta a jednotka vozidla použiť funkciu odvodenia kľúča na kľúče relácie AES vymedzenú v [TR-03111], s týmito spresneniami a zmenami:

— Hodnota počítadla pre K_{ENC} musí byť '00 00 00 01' a pre K_{MAC} '00 00 00 02'.

— Musí sa použiť nepovinná jednorazová hodnota „nonce" *r* a musí sa rovnať N_{PICC}.

— Na odvodenie 128-bitových kľúčov AES musí byť hašovací algoritmus, ktorý sa má použiť, SHA-256.

— Na odvodenie 192-bitových kľúčov AES musí byť hašovací algoritmus, ktorý sa má použiť, SHA-384.

— Na odvodenie 256-bitových kľúčov AES musí byť hašovací algoritmus, ktorý sa má použiť, SHA-512.

Dĺžka kľúčov relácie (t. j. dĺžka, na ktorú sa hash skráti) musí byť prepojená s veľkosťou kľúčového páru Card_MA, ako je uvedené v CSM_50.

CSM_180 V uvedených krokoch 6 a 9 musia karta a jednotka vozidla použiť algoritmus AES v režime CMAC, ako je uvedené v [SP 800-38B]. Dĺžka T_{PICC} musí byť prepojená s dĺžkou kľúčov relácie AES, ako je uvedené v CSM_50.

10.5. **Zabezpečené spracovanie správ**

10.5.1 *Všeobecné*

CSM_181 Všetky príkazy a odpovede vymieňané medzi jednotkou vozidla a tachografovou kartou po úspešnej autentifikácii čipu a až do konca relácie musia byť chránené zabezpečeným spracovaním.

CSM_182 Okrem čítania zo súboru s prístupovou podmienkou SM-R-ENC-MAC-G2 (pozri dodatok 2, oddiel 4) sa zabezpečené spracovanie musí použiť v režime iba na základe autentifikácie. V tomto režime sa na zaistenie autenticity a integrity správy pridá do všetkých príkazov a odpovedí kryptografický kontrolný súčet (alebo MAC).

CSM_183 Pri čítaní údajov zo súboru s prístupovou podmienkou SM-R-ENC-MAC-G2 sa musí použiť zabezpečené spracovanie v režime šifrovania a následnej autentifikácie, t. j. údaje odpovede sú najprv zašifrované na zaistenie dôvernosti správy, a potom sa z formátovaných šifrovaných údajov vypočíta MAC na zaistenie autenticity a integrity.

CSM_184 Zabezpečené spracovanie musí použiť AES, ako je definované v [AES] s kľúčmi relácie K_{MAC} a K_{ENC}, ktoré boli dohodnuté počas autentifikácia čipu.

CSM_185 Na zabránenie tzv. „replay" útokom sa ako počítadlo sekvencie odosielania (SSC) musí použiť celé číslo bez znamienka. Veľkosť SSC sa musí rovnať veľkosti bloku AES, t. j. 128 bitom. SSC musí byť vo formáte MSB-first (teda bajt najvyššieho rádu na prvom mieste). Keď sa začne zabezpečené spracovanie, počítadlo sekvencie odosielania sa začne od nuly ('00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'). SSC sa musí zvýšiť vždy pred generovaním príkazu alebo odpovede ADPU, t. j. keďže začiatočná hodnota SCC v relácii SM je 0, v prvom príkaze bude hodnota SSC 1. Hodnota SSC pre prvú odpoveď bude 2.

CSM_186 Na šifrovanie správ sa musí použiť K_{ENC} s AES v prevádzkovom režime reťazenia šifrovacieho bloku (CBC), ako je vymedzené v [ISO 10116], s parametrom prekladania *m* = 1 a inicializačným vektorom SV = E(K_{ENC}, SSC), t. j. aktuálna hodnota počítadla sekvencie odosielania zašifrovaná s K_{ENC}.

CSM_187 Na autentifikáciu správ sa musí použiť K_{MAC} s AES v režime CMAC, ako je uvedené v [SP 800-38B]. Dĺžka MAC musí byť prepojená s dĺžkou kľúčov relácie AES, ako je uvedené v CSM_50. Počítadlo sekvencie odosielania musí byť zahrnuté do MAC tak, že sa pripojí pred datagram, ktorý sa má autentifikovať.

10.5.2 *Štruktúra zabezpečeného spracovania správ*

CSM_188 Zabezpečené spracovanie musí využívať iba dátové objekty zabezpečeného spracovania (pozri [ISO 7816-4]], uvedené v tabuľke 5. V každej správe musia byť použité tieto dátové objekty v poradí uvedenom v tejto tabuľke.

Tabuľka 5

Dátové objekty zabezpečeného spracovania

Názov dátového objektu	Tag	Prítomnosť: povinný (M), podmienečný (C) alebo zakázaný (F) v	
		príkazoch	odpovediach
Nezašifrovaná hodnota nekódovaná v BER-TLV	'81'	C	C
Nezašifrovaná hodnota kódovaná v BER-TLV, ktorá ale neobsahuje dátové objekty SM	'B3'	C	C
Indikátor obsahu výplne, za ktorým nasleduje kryptogram, nezašifrovaná hodnota nekódovaná v BER-TLV	'87'	C	C
Chránené Le	'97'	C	F
Stav spracovania	'99'	F	M
Kryptografický kontrolný súčet	'8E'	M	M

Poznámka: Ako je uvedené v dodatku 2, tachografové karty môžu podporovať príkaz READ BINARY a UPDATE BINARY s nepárnym bajtom INS ('B1' resp. 'D7'). Tieto varianty príkazov sú potrebné na čítanie a aktualizáciu súborov s viac než 32 768 bajtmi. Ak sa takýto variant použije, namiesto objektu s tagom '81' sa musí použiť dátový objekt s tagom 'B3'. Pre viac informácií pozri dodatok 2.

CSM_189 Všetky dátové objekty SM musia byť zakódované DER TLV, ako je uvedené v [ISO 8825-1]. Výsledkom tohto kódovania je takáto štruktúra tag-dĺžka-hodnota (TLV):

Tag: Tag je kódovaný v jednom alebo dvoch oktetoch a určuje obsah.

Dĺžka: dĺžka je kódovaná ako celé číslo bez znamienka v jednom, dvoch alebo troch oktetoch, čoho výsledkom je maximálna dĺžka 65 535 oktetov. Musí sa použiť minimálny počet oktetov.

Hodnota: Hodnota je kódovaná v nula alebo viac oktetoch

CSM_190 APDU chránené zabezpečeným spracovaním sa vytvoria takto:

— Záhlavie príkazu musí byť zahrnuté do výpočtu MAC, preto sa pre bajt triedy CLA musí použiť hodnota '0C'.

— Ako je uvedené v dodatku 2, všetky bajty INS musia byť párne, s možnou výnimkou nepárnych bajtov INS v prípade príkazov READ BINARY a UPDATE BINARY.

— Skutočná hodnota Lc sa upraví na Lc' po uplatnení zabezpečeného spracovania.

— Dátové pole musí obsahovať dátové objekty SM.

— V chránenom príkaze APDU sa nový Le bajt musí nastaviť na '00'. V prípade potreby sa do dátového poľa zahrnie dátový objekt '97', s cieľom preniesť pôvodnú hodnotu Le.

CSM_191 Každý dátový objekt, ktorý sa má zašifrovať, musí byť vyplnený podľa normy [ISO 7816-4] s použitím indikátora obsahu výplne '01'. Na výpočet MAC musí byť každý dátový objekt v ADPU zároveň samostatne vyplnený podľa [ISO 7816-4].

Poznámka: Vyplnenie pre zabezpečené spracovanie sa vždy vykonáva vrstvou zabezpečeného spracovania, a nie algoritmami CMAC alebo CBC.

Zhrnutie a príklady

Príkaz ADPU s aplikovaným zabezpečeným spracovaním bude mať túto štruktúru, v závislosti od prípadu príslušného nezabezpečeného príkazu (DO je dátový objekt):

Prípad 1:	CLA INS P1 P2 || Lc' || DO '8E' || Le
Prípad 2:	CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le
Prípad 3 (párny bajt INS):	CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le
Prípad 3 (nepárny bajt INS):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le
Prípad 4 (párny bajt INS):	CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le
Prípad 4 (nepárny bajt INS):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

kde Le = '00' alebo '00 00' podľa toho, či sa používajú polia s krátkou dĺžkou alebo s rozšírenou dĺžkou; pozri [ISO 7816-4].

Odpoveď ADPU s aplikovaným zabezpečeným spracovaním bude mať túto štruktúru, v závislosti od prípadu príslušnej nezabezpečenej odpovede:

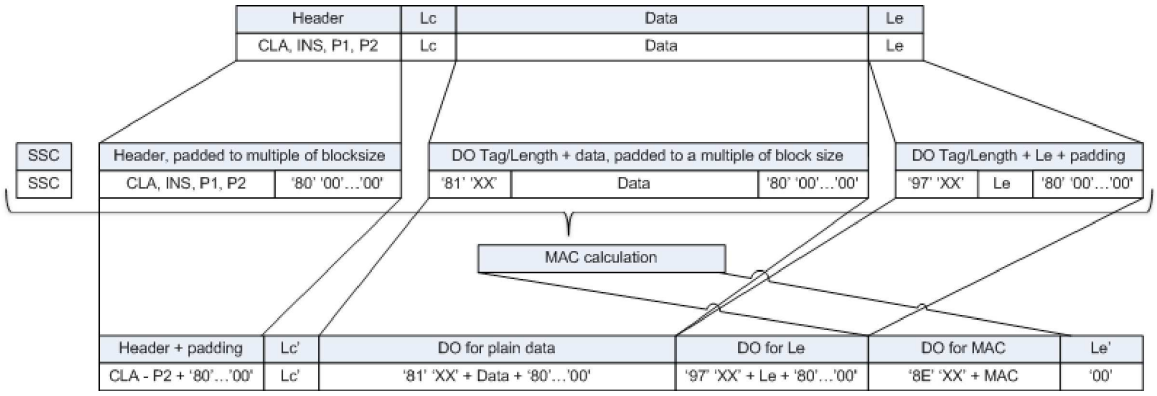
Prípad 1 alebo 3:	DO '99' || DO '8E' || SW1SW2
Prípad 2 alebo 4 (párny bajt INS) so zašifrovaním:	DO '81' || DO '99' || DO '8E' || SW1SW2
Prípad 2 alebo 4 (párny bajt INS) bez zašifrovania:	DO '87' || DO '99' || DO '8E' || SW1SW2
Prípad 2 alebo 4 (nepárny bajt INS) bez zašifrovania:	DO 'B3' || DO '99' || DO '8E' || SW1SW2

Poznámka: Prípad 2 alebo 4 (nepárny bajt INS) so šifrovaním sa nikdy nepoužíva v komunikácii medzi VU a kartou.

Ďalej sú uvedené tri príklady transformácií APDU pri príkazoch s párnym kódom INS. Obrázok 8 ukazuje autentifikovaný príkaz APDU prípadu 4, obrázok 9 ukazuje autentifikovanú odpoveď APDU prípadu 2/prípadu 4 a obrázok 10 ukazuje zašifrovanú a autentifikovanú odpoveď APDU prípadu 2/prípadu 4.

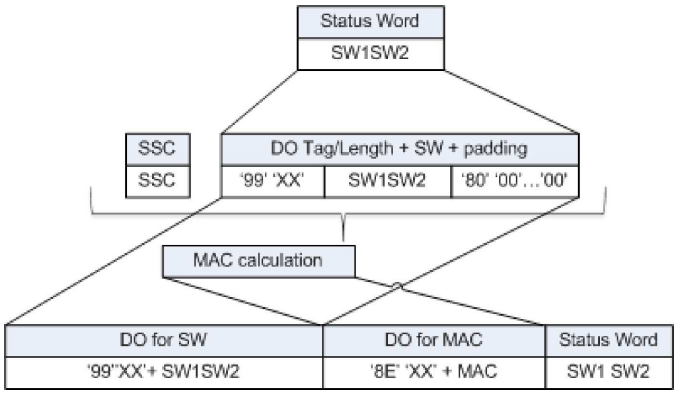
Obrázok 8

Transformácia autentifikovaného príkazu APDU prípadu 4



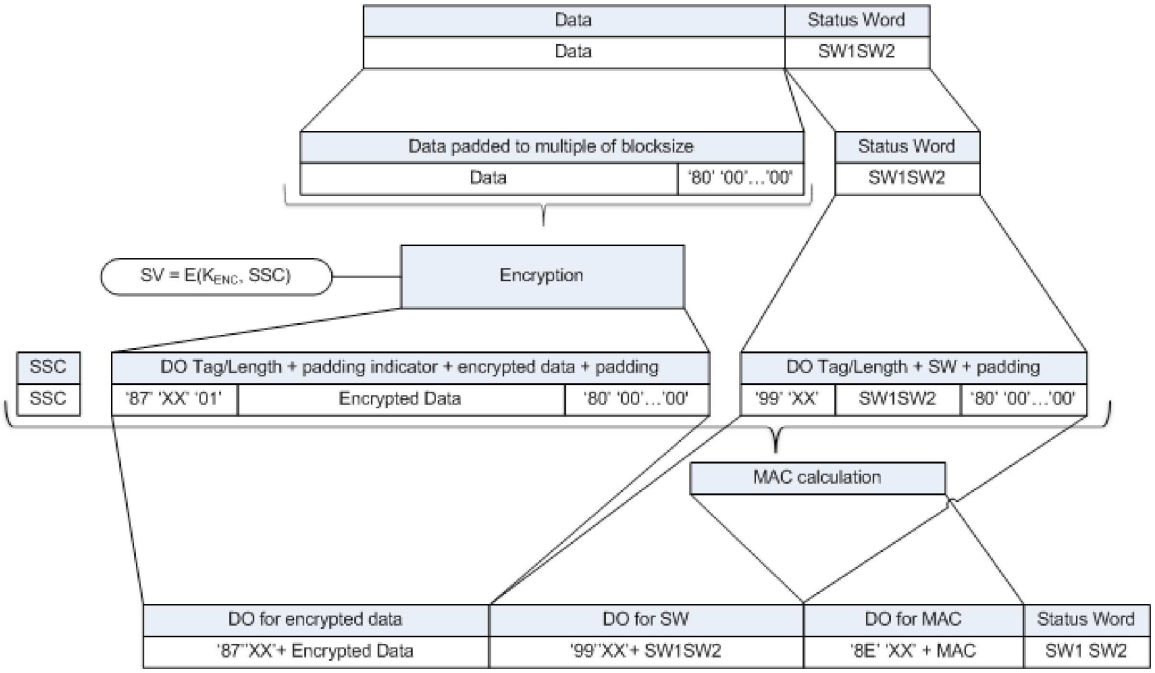
Obrázok 9

Transformácia autentifikovanej odpovede APDU prípadu 1/prípadu 3



Obrázok 10

Transformácia zašifrovanej a autentifikovanej odpovede ADPU prípadu 2/prípadu 4



10.5.3 *Zrušenie relácie zabezpečeného spracovania*

CSM_192 Jednotka vozidla musí zrušiť prebiehajúcu reláciu zabezpečeného spracovania, ak a len ak sa splní jedna z týchto podmienok:

— dostane nezašifrovanú odpoveď ADPU,

— v odpovedi ADPU zistí chybu zabezpečeného spracovania:

— Očakávaný dátový objekt zabezpečeného spracovania chýba, poradie dátových objektov je nesprávne alebo je zahrnutý neznámy dátový objekt.

— Dátový objekt zabezpečeného spracovania je nesprávny, napr. hodnota MAC je nesprávna, štruktúra TLV je nesprávna alebo indikátor výplne v tagu '87' nie je rovný '01'.

— karta pošle stavový bajt udávajúci, že zistila chybu SM (pozri CSM_194),

— dosiahol sa limit pre počet príkazov a súvisiacich odpovedí v rámci aktuálnej relácie. Pre danú VU musí byť tento limit vymedzený výrobcom, berúc do úvahy požiadavky zabezpečenia použitého hardvéru s maximálnou hodnotou 240 príkazov SM a súvisiacich odpovedí za reláciu.

CSM_193 Tachografová karta musí zrušiť prebiehajúcu reláciu zabezpečeného spracovania, ak a len ak sa splní jedna z týchto podmienok:

— dostane nezašifrovaný príkaz ADPU,

— v príkaze ADPU zistí chybu zabezpečeného spracovania:

— Očakávaný dátový objekt zabezpečeného spracovania chýba, poradie dátových objektov je nesprávne alebo je zahrnutý neznámy dátový objekt.

— Dátový objekt zabezpečeného spracovania je nesprávny, napr. hodnota MAC je nesprávna alebo štruktúra TLV je nesprávna.

— stratí napájanie alebo je resetovaná,

— VU zvolí aplikáciu na karte,

— VU začne proces autentifikácie VU,

— dosiahol sa limit pre počet príkazov a súvisiacich odpovedí v rámci aktuálnej relácie. Pre danú kartu musí byť tento limit vymedzený výrobcom, berúc do úvahy požiadavky zabezpečenia použitého hardvéru s maximálnou hodnotou 240 príkazov SM a súvisiacich odpovedí za reláciu.

CSM_194 Spracovanie chyby SM tachografovou kartou:

— Ak v príkaze APDU chýbajú niektoré očakávané dátové objekty zabezpečeného spracovania, poradie dátových objektov je nesprávne alebo sú zahrnuté neznáme dátové objekty, tachografová karta musí odpovedať stavovými bajtmi '69 87'.

— Ak je dátový objekt zabezpečeného spracovania v príkaze APDU nesprávny, tachografová karta musí odpovedať stavovými bajtmi '69 88'.

V takom prípade sa musia stavové bajty vrátiť bez SM.

CSM_195 Ak sa relácia zabezpečeného spracovania medzi VU a tachografovou kartou zruší, VU a tachografová karta musí

— bezpečne zničiť uložené kľúče relácie

— okamžite nadviazať novú reláciu zabezpečeného spracovania, ako je opísané v oddieloch 10.2 – 10.5.

CSM_196 Ak sa VU z akéhokoľvek dôvodu rozhodne reštartovať vzájomnú autentifikáciu s vloženou kartou, musí sa začať overovanie certifikačného reťazca karty, ako je opísané v oddiele 10.2, a nasleduje postup opísaný v oddieloch 10.2 – 10.5.

11. SPÁJANIE VU S EXTERNÝM ZARIADENÍM GNSS, VZÁJOMNÁ AUTENTIFIKÁCIA A ZABEZPEČENÉ SPRACOVANIE

11.1. **Všeobecné**

CSM_197 Externé zariadenie GNSS, ktoré používa VU na určovanie svojej polohy, môže byť interné (t. j. zabudované v puzdre VU a neoddeliteľné), alebo to môže byť externý modul. V prvom prípade netreba štandardizovať internú komunikáciu medzi zariadením GNSS a VU, a požiadavky tejto kapitoly sa neuplatňujú. V druhom prípade sa komunikácia medzi VU a externým zariadením GNSS musí štandardizovať a chrániť, ako je opísané v tejto kapitole.

CSM_198 Zabezpečená komunikácia medzi jednotkou vozidla a externým zariadením GNSS musí prebiehať rovnako, ako zabezpečená komunikácia medzi jednotkou vozidla a tachografovou kartou, pričom externé zariadenie GNSS (ďalej „EGF“), preberá úlohu karty. EGF musí spĺňať všetky požiadavky uvedené v kapitole 10 týkajúce sa tachografových kariet, berúc do úvahy odchýlky, objasnenia a doplnenia uvedené v tejto kapitole. Predovšetkým sa vzájomné overenia certifikačných reťazcov, autentifikácia VU a autentifikácia čipu musia vykonať tak, ako je opísané v oddieloch 11.3 a 11.4.

CSM_199 Komunikácia medzi jednotkou vozidla a EGF sa líši od komunikácie medzi jednotkou vozidla a kartou v tom, že jednotka vozidla a EGF musia byť raz spojené v dielni predtým, ako si VU a EGF môžu vymieňať údaje na báze GNSS počas bežnej prevádzky. Proces spájania je opísaný v oddiele 11.2.

CSM_200 Na komunikáciu medzi jednotkou vozidla a EGF sa musia použiť príkazy a odpovede ADPU vychádzajúce z [ISO 7816-4] a [ISO 7816-8]. Presná štruktúra týchto APDU je vymedzená v dodatku 2 tejto prílohy.

11.2. **Spájanie VU a externého zariadenia GNSS**

CSM_201 Jednotku vozidla a EGF vo vozidle musí spojiť dielňa. Počas bežnej prevádzky musia byť schopné komunikovať len spojená jednotka vozidla a EGF.

CSM_202 Spájanie jednotky vozidla a EGF musí byť možné len v prípade, ak je jednotka vozidla v režime kalibrácie. Spájanie musí začať jednotka vozidla.

CSM_203 Dielňa môže kedykoľvek opätovne spojiť jednotku vozidla s iným EGF alebo s tým istým EGF. Počas opätovného spojenia musí VU bezpečne zničiť existujúci certifikát EGF_MA vo svojej pamäti a uložiť certifikát EGF_MA toho EGF, s ktorým sa spája.

CSM_204 Dielňa môže kedykoľvek opätovne spojiť externé zariadenie GNSS s inou VU alebo s tou istou VU. Počas opätovného spojenia musí EGF bezpečne zničiť existujúci certifikát VU_MA vo svojej pamäti a uložiť certifikát VU_MA jednotky vozidla, s ktorou sa spája.

11.3. **Vzájomné overovanie certifikačných reťazcov**

11.3.1 *Všeobecné*

CSM_205 Vzájomné overovanie certifikačného reťazca medzi VU a EGF sa musí uskutočniť len počas spájania VU a EGF, ktoré vykonáva dielňa. Počas bežnej prevádzky spojených VU a EGF sa nesmú overovať žiadne certifikáty. Namiesto toho musia VU a EGF dôverovať certifikátom, ktoré uložili počas spojenia, po kontrole dočasnej platnosti týchto certifikátov. VU a EGF nesmie dôverovať žiadnym iným certifikátom, pokiaľ ide o ochranu komunikácie VU – EGF počas normálnej prevádzky.

11.3.2 *Počas spájania VU – EGF*

CSM_206 Počas spájania s EGF musí jednotka vozidla použiť protokol znázornený na obrázku 4 (oddiel 10.2.1) na overenie certifikačného reťazca externého zariadenia GNSS.

Poznámky k obrázku 4 v tomto kontexte:

— Kontrola prenosu údajov je mimo rozsahu pôsobnosti tohto dodatku. Avšak EGF nie je inteligentná karta, a VU teda pravdepodobne nepošle Reset na začatie komunikácie a neprijme ATR.

— Na vzájomnú autentifikáciu sa certifikáty a verejné kľúče karty uvedené na obrázku interpretujú ako certifikáty a verejné kľúče EGF. V oddiele 9.1.6 sa označujú ako EGF_MA.

— Na podpis certifikátov EGF sa certifikáty a verejné kľúče Card.CA uvedené na obrázku interpretujú ako certifikáty a verejné kľúče MSCA. V oddiele 9.1.3 sa označujú ako MSCA_VU-EGF.

— Certifikát Card.CA.EUR uvedený na obrázku sa interpretuje ako európsky koreňový certifikát, ktorý je uvedený v CAR certifikátu MSCA_VU-EGF.

— Certifikát Card.Link uvedený na obrázku sa interpretuje ako prepájací certifikát EGF, ak je prítomný. Ako je uvedené v oddiele 9.1.2, je to prepájací certifikát pre nový európsky pár koreňových kľúčov vytvorený ERCA a podpísaný predchádzajúcim európskym súkromným kľúčom.

— Certifikát Card.Link.EUR je európsky koreňový certifikát, ktorý je uvedený v CAR certifikátu Card.Link.

— Namiesto `cardExtendedSerialNumber`, musí VU z EF ICC čítať `sensorGNSSserialNumber`.

— Namiesto výberu AID tachografu musí VU vybrať AID EGF.

— „Ignorovať kartu“ sa interpretuje ako „ignorovať EGF“.

CSM_207 Po tom, ako jednotka vozidla overila certifikát EGF_MA, musí uložiť tento certifikát na použitie počas bežnej prevádzky; pozri oddiel 11.3.3.

CSM_208 Počas spájania s VU musí externé zariadenie GNSS použiť protokol znázornený na obrázku 5 (oddiel 10.2.2) na overenie certifikačného reťazca VU.

Poznámky k obrázku 5 v tomto kontexte:

— VU musí vygenerovať nový efemérny kľúčový pár pomocou parametrov domény v certifikáte EGF.

— Certifikáty VU a verejné kľúče uvedené na obrázku sú tie, ktoré sú určené na vzájomnú autentifikáciu. V oddiele 9.1.4 sa označujú ako VU_MA.

— Certifikáty VU.CA a verejné kľúče uvedené na obrázku sú certifikáty a kľúče určené na podpísanie certifikátov VU a certifikátov externých zariadení GNSS. V oddiele 9.1.3 sa označujú ako MSCA_VU-EGF.

— Certifikát VU.CA.EUR uvedený na obrázku je európsky koreňový certifikát, ktorý je uvedený v CAR certifikátu VU.CA.

— Certifikát VU.Link uvedený na obrázku je prepájací certifikát VU, ak je prítomný. Ako je uvedené v oddiele 9.1.2, je to prepájací certifikát pre nový európsky pár koreňových kľúčov vytvorený ERCA a podpísaný predchádzajúcim európskym súkromným kľúčom.

— Certifikát VU.Link.EUR je európsky koreňový certifikát, ktorý je uvedený v CAR certifikátu VU. Link.

CSM_209 Odchylne od požiadavky CSM_167, EGF musí použiť čas GNSS na overenie dočasnej platnosti akéhokoľvek predloženého certifikátu.

CSM_210 Po tom, ako externé zariadenie GNSS overilo certifikát VU_MA, musí uložiť tento certifikát na použitie počas bežnej prevádzky; pozri oddiel 11.3.3.

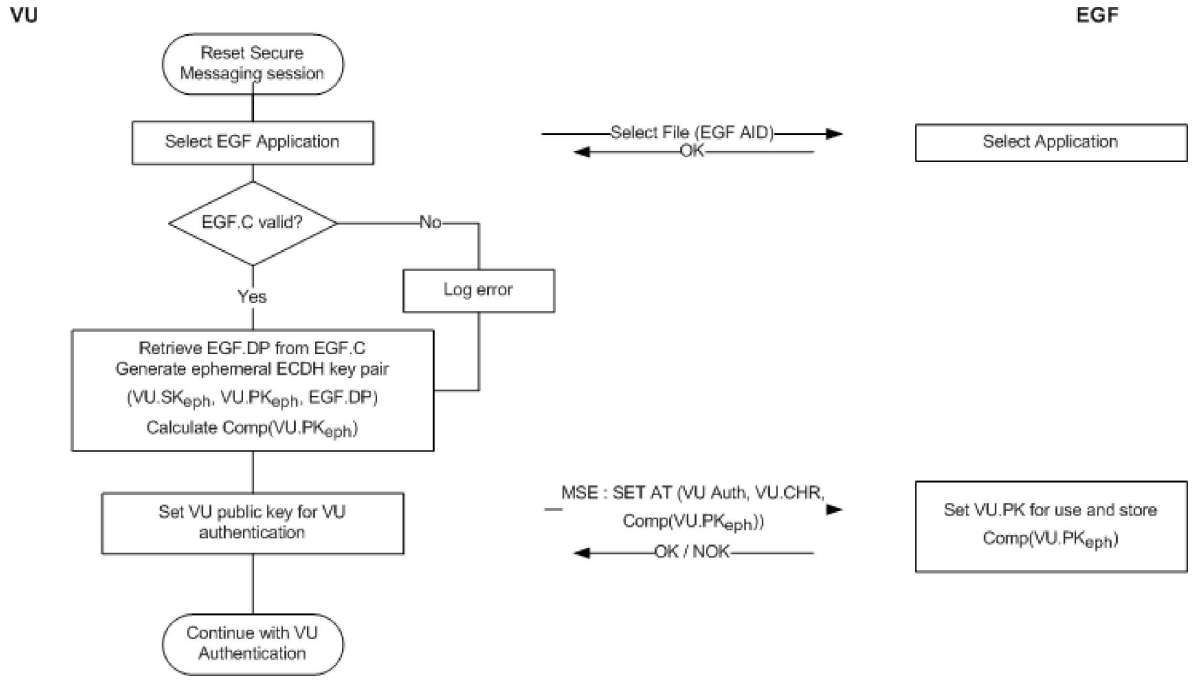
11.3.3 *Počas bežnej prevádzky*

CSM_211 Počas bežnej prevádzky musia jednotka vozidla a EGF na overovanie dočasnej platnosti certifikátov EGF_MA a VU_MA a na nastavenie verejného kľúča VU_MA pre následnú autentifikáciu VU použiť protokol zobrazený na obrázku 11. Počas bežnej prevádzky sa nesmie uskutočniť žiadne ďalšie vzájomné overenie certifikačných reťazcov.

Upozorňujeme, že obrázok 11 v podstate pozostáva z prvých krokov uvedených na obrázku 4 a obrázku 5. Opäť upozorňujeme, že keďže EGF nie je inteligentná karta, VU pravdepodobne nepošle Reset na začatie komunikácie a neprijme ATR. V každom prípade je to mimo rozsahu pôsobnosti tohto dodatku.

Obrázok 11

Vzájomné overovanie dočasnej platnosti certifikátov VU – EGF počas bežnej prevádzky



CSM_212 Ako je znázornené na obrázku 11, jednotka vozidla musí zaznamenať chybu v prípade, že certifikát EGF_MA už nie je platný. Avšak vzájomná autentifikácia, kľúčová dohoda a následná komunikácia prostredníctvom zabezpečeného spracovania musia pokračovať normálne.

11.4. Autentifikácia VU, autentifikácia čipu a kľúčová dohoda relácie

CSM_213 Autentifikácia VU, autentifikácia čipu a kľúčová dohoda relácie medzi VU a EGF sa uskutočňujú počas spájania a vždy, keď sa relácia zabezpečeného spracovania opätovne nadviaže počas bežnej prevádzky. VU a EGF musia vykonávať procesy opísané v oddieloch 10.3 a 10.4. Uplatňujú sa všetky požiadavky uvedené v týchto oddieloch.

11.5. Zabezpečené spracovanie správ

CSM_214 Všetky príkazy a odpovede vymieňané medzi jednotkou vozidla a externým zariadením GNSS po úspešnej autentifikácii čipu musia byť až do konca relácie chránené zabezpečeným spracovaním v režime iba na základe autentifikácie. Uplatňujú sa všetky požiadavky uvedené v oddiele 10.5.

CSM_215 Ak sa relácia zabezpečeného spracovania medzi VU a EGF zruší, VU musí okamžite vytvoriť novú reláciu zabezpečeného spracovania, ako je opísané v bode 11.3.3 a 11.4.

12. PÁROVANIE VU – SNÍMAČ POHYBU A KOMUNIKÁCIA

12.1. **Všeobecné**

CSM_216 Jednotka vozidla a snímač pohybu musia komunikovať pomocou protokolu rozhrania uvedeného v [ISO 16844-3] počas párovania a v bežnej prevádzke, so zmenami opísanými v tejto kapitole a v oddiele 9.2.1.

Poznámka: predpokladá sa, že čitatelia tejto kapitoly sú oboznámení s obsahom [ISO 16844-3].

12.2. **Párovanie VU – snímač pohybu pomocou rôznych generácií kľúča**

Ako je vysvetlené v oddiele 9.2.1, hlavný kľúč snímača pohybu a všetky súvisiace kľúče sa pravidelne nahrádzajú. Toto vedie k výskytu až troch kľúčov AES K_{M-WC} týkajúcich sa snímačov pohybu (nadväzných generácií) v dielenských kartách. Podobne sa v snímačoch pohybu môžu vyskytnúť až tri rôzne šifrovania údajov podľa AES (na základe nadväzných generácií hlavného kľúča K_M snímača pohybu). Jednotka vozidla obsahuje len jeden kľúč K_{M-VU} týkajúci sa snímača pohybu.

CSM_217 VU druhej generácie a snímač pohybu druhej generácie musia byť párované takto [porovnaj s tabuľkou 6 v (ISO 16844-3)]:

1. Dielenská karta druhej generácie sa vloží do VU a VU sa pripojí k snímaču pohybu.

2. VU prečíta všetky dostupné kľúče K_{M-WC} z dielenskej karty, skontroluje ich čísla verzií a vyberie ten, ktorého číslo verzie sa zhoduje s K_{M-VU} jednotky vozidla. Ak nie je zhodný kľúč K_{M-WC} v dielenskej karte prítomný, VU zruší párovací proces a zobrazí vhodné chybové hlásenie držiteľovi dielenskej karty.

3. VU vypočíta hlavný kľúč snímača pohybu K_M z K_{M-VU} a K_{M-WC}, a identifikačný kľúč K_{ID} z K_M, ako je uvedené v oddiele 9.2.1.

4. VU odošle pokyn na začatie párovacieho procesu so snímačom pohybu, ako je uvedené v [ISO 16844-3], a zašifruje sériové číslo, ktoré dostane od snímača pohybu s identifikačným kľúčom K_{ID}. VU odošle zašifrované sériové číslo späť snímaču pohybu.

5. Snímač pohybu priradí zašifrované sériové číslo postupne s každou šifrou sériového čísla, ktorými interne disponuje. Ak nájde zhodu, VU je autentifikovaná. Snímač pohybu zaznamená generáciu K_{ID} použitú jednotkou vozidla a vráti príslušnú zašifrovanú verziu svojho párovacieho kľúča; t. j. šifra, ktorá bola vytvorená pomocou tej istej generácie K_M.

6. VU dešifruje párovací kľúč pomocou K_M, vygeneruje kľúč relácie K_S, zašifruje ho párovacím kľúčom a pošle výsledok snímaču pohybu. Snímač pohybu dešifruje K_S.

7. VU zoradí párovacie informácie, ako je uvedené v [ISO 16844-3], zašifruje informácie párovacím kľúčom a pošle výsledok snímaču pohybu. Snímač pohybu dešifruje párovacie informácie.

8. Snímač pohybu zašifruje získané párovacie informácie prijatým K_S a vráti ich VU. VU overí, že párovacie informácie sú tie isté informácie, ktoré VU poslala snímaču pohybu v predchádzajúcom kroku. Tým sa preukáže, že snímač pohybu použil rovnaký K_S ako VU, a teda v kroku 5 poslal svoj párovací kľúč zašifrovaný správnou generáciou K_M. Preto je snímač pohybu overený.

Upozorňujeme, že kroky 2 a 5 sú odlišné od štandardného postupu v [ISO 16844-3]; ostatné kroky sú štandardné.

Príklad: Predpokladajme, že sa párovanie uskutočňuje v prvom roku platnosti certifikátu ERCA (3); pozri obrázok 2 v oddiele 9.2.1.2. Okrem toho

— Predpokladajme, že snímač pohybu bol vydaný v poslednom roku platnosti certifikátu ERCA (1). Preto bude obsahovať tieto kľúče a údaje:

  — N_S[1]: jeho sériové číslo zašifrované K_{ID} prvej generácie,

  — N_S[2]: jeho sériové číslo zašifrované K_{ID} druhej generácie,

  — N_S[3]: jeho sériové číslo zašifrované K_{ID} tretej generácie,

  — K_P[1]: jeho párovací kľúč prvej generácie ([1]), zašifrovaný K_M prvej generácie,

  — K_P[2]: jeho párovací kľúč druhej generácie, zašifrovaný K_M druhej generácie,

  — K_P[3]: jeho párovací kľúč tretej generácie, zašifrovaný K_M tretej generácie,

— Predpokladajme, že dielenská karta bola vydaná v prvom roku platnosti certifikátu ERCA (3). Preto bude obsahovať kľúč $K_{M\text{-}WC}$ druhej a tretej generácie.

— Predpokladajme, že VU je VU druhej generácie, ktorá obsahuje $K_{M\text{-}VU}$ druhej generácie.

V tomto prípade v krokoch 2 až 5 nastane toto:

— Krok 2: VU prečíta z dielenskej karty $K_{M\text{-}WC}$ druhej a tretej generácie a skontroluje čísla ich verzií.

— Krok 3: VU skombinuje $K_{M\text{-}WC}$ druhej generácie so svojím $K_{M\text{-}VU}$, aby vypočítala K_M a K_{ID}.

— Krok 4: VU zašifruje, prostredníctvom K_{ID}, sériové číslo, ktoré dostane od snímača pohybu.

— Krok 5: Snímač pohybu porovná získané údaje s N_S[1] a nenájde zhodu. Potom porovná dané údaje s N_S[2] a nájde zhodu. Z toho vyvodí, že VU je VU druhej generácie, a preto pošle späť K_P[2].

12.3. Párovanie VU – snímač pohybu a komunikácia pomocou AES

CSM_218 Ako sa uvádza v tabuľke 3 v oddiele 9.2.1, všetky kľúče, ktoré sa zúčastnia na párovaní (druhej generácie) jednotky vozidla a snímača pohybu a následnej komunikácii, musia byť kľúče AES, a nie kľúče TDES s dvojitou dĺžkou, ako je uvedené v [ISO 16844-3]. Tieto kľúče AES môžu mať dĺžku 128, 192 alebo 256 bitov. Keďže veľkosť blokov AES je 16 bajtov, dĺžka zašifrovanej správy musí byť násobkom 16 bajtov, v porovnaní s 8 bajtmi v prípade TDES. Okrem toho budú niektoré z týchto správ použité na prenos kľúčov AES, ktorých dĺžka môže byť 128, 192 alebo 256 bitov. Preto sa počet dátových bajtov na pokyn v tabuľke 5 normy [ISO 16844-3] zmení tak, ako zobrazené v tabuľke 6:

Tabuľka 6

Počet nezašifrovaných a zašifrovaných dátových bajtov na pokyn podľa [ISO 16844-3]

Pokyn	Požiadavka / odpoveď	Opis údajov	# dátových bajtov nezašifrovaného textu podľa [ISO 16844-3]	# dátových bajtov nezašifrovaného textu používajúcich kľúče AES	# zašifrovaných dátových bajtov pri používaní kľúčov AES s bitovou dĺžkou		
					128	192	256
10	požia-davka	autentifikačné údaje + číslo súboru	8	8	16	16	16

([1]) Upozorňujeme, že párovacie kľúče prvej, druhej a tretej generácie môžu byť v skutočnosti totožné, alebo to môžu byť rôzne kľúče s rôznymi dĺžkami, ako je vysvetlené v CSM_117.

Pokyn	Požiadavka / odpoveď	Opis údajov	# dátových bajtov nezašifrovaného textu podľa [ISO 16844-3]	# dátových bajtov nezašifrovaného textu používajúcich kľúče AES	# zašifrovaných dátových bajtov pri používaní kľúčov AES s bitovou dĺžkou		
					128	192	256
11	odpoveď	autentifikačné údaje + obsah súboru	16 alebo 32, v závislosti od súboru	16 alebo 32, v závislosti od súboru	16 / 32	16 / 32	16 / 32
41	požiadavka	sériové číslo MoS	8	8	16	16	16
41	odpoveď	párovací kľúč	16	16 / 24 / 32	16	32	32
42	požiadavka	kľúč relácie	16	16 / 24 / 32	16	32	32
43	požiadavka	párovacia informácia	24	24	32	32	32
50	odpoveď	párovacia informácia	24	24	32	32	32
70	požiadavka	Autentifikačné údaje	8	8	16	16	16
80	odpoveď	Hodnota počítadla MoS + autentifikačné údaje	8	8	16	16	16

CSM_219 Párovacie informácie, ktoré sú poslané v pokynoch 43 (žiadosť VU) a 50 (odpoveď MoS) musia byť zostavené tak, ako sa uvádza v oddiele 7.6.10 normy [ISO 16844-3], s výnimkou toho, že sa v schéme šifrovania párovacích údajov musí použiť algoritmus AES namiesto algoritmu TDES, následkom čoho budú dve šifrovania AES a prijatie výplne uvedenej v CSM_220, tak aby zodpovedala veľkosti bloku AES. Kľúč K'_P použitý na toto šifrovanie sa musí vygenerovať takto:

— Ak má párovací kľúč K_P dĺžku 16 bajtov: $K'_P = K_P \text{ XOR } (N_s||N_s)$

— Ak má párovací kľúč K_P dĺžku 24 bajtov: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s)$

— Ak má párovací kľúč K_P dĺžku 32 bajtov: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s||N_s)$

Kde N_s je 8 bajtové sériové číslo snímača pohybu.

CSM_220 Ak dátová dĺžka nezašifrovaného textu (používajúc kľúče AES) nie je násobkom 16 bajtov, musí sa použiť metóda výplne 2 vymedzená v [ISO 9797-1].

Poznámka: v [ISO 16844-3] je počet dátových bajtov nezašifrovaného textu vždy násobkom 8, takže vyplň nie je pri použití TDES potrebná. Vymedzenie údajov a správ v [ISO 16844-3] sa touto časťou tejto prílohy nemení, takže je potrebná výplň.

CSM_221 Pre pokyn 11 a v prípade, keď musí byť zašifrovaných viac ako jeden blok údajov, musí sa použiť prevádzkový režim reťazenia šifrovacieho bloku, ako je vymedzený v [ISO 10116], s parametrom prekladania $m = 1$. IV, ktorý sa má používať, musí byť

— Pre pokyn 11: 8-bajtový autentifikačný blok uvedený v oddiele 7.6.3.3 normy [ISO 16844-3], vyplnený pomocou metódy výplne 2 vymedzenej v [ISO 9797-1]; pozri aj oddiel 7.6.5 a 7.6.6 normy [ISO 16844-3].

— Pre všetky ostatné pokyny, v ktorých sa prenáša viac ako 16 bajtov, ako je uvedené v tabuľke 6: '00' {16}, t. j. šestnásť bajtov s binárnou hodnotu 0.

Poznámka: Ako je uvedené v oddiele 7.6.5 a 7.6.6 normy [ISO 16844-3], keď MoS zašifruje dátové súbory určené na zahrnutie do pokynu 11, autentifikačný blok je

— použitý ako inicializačný vektor pre šifrovanie súborov údajov v režime CBC, ako aj

— zašifrovaný a zahrnutý ako prvý blok v údajoch, ktoré sa posielajú VU.

12.4. **Párovanie VU – snímač pohybu v prípade rôznych generácií zariadenia**

CSM_222 Ako je vysvetlené v oddiele 9.2.1, snímač pohybu druhej generácie môže obsahovať šifrovanie párovacích údajov založené na TDES (ako je vymedzené v časti A tohto dodatku), ktoré umožňuje spárovanie snímača pohybu s VU prvej generácie. Ak tomu tak je, musia sa VU prvej generácie a snímač pohybu druhej generácie spárovať, ako je opísané v časti A tohto dodatku a v [ISO 16844-3]. Na proces párovania sa môže použiť dielenská karta buď prvej generácie alebo druhej generácie.

Poznámky:

— Nie je možné párovať VU druhej generácie so snímačom pohybu prvej generácie.

— Nie je možné použiť dielenskú kartu prvej generácie na spojenie VU druhej generácie so snímačom pohybu.

13. ZABEZPEČENIE DIAĽKOVEJ KOMUNIKÁCIE CEZ DSRC

13.1. **Všeobecné**

Ako je uvedené v dodatku 14, VU pravidelne generuje údaje diaľkového monitorovania tachografu (RTM) a posiela tieto údaje (internému alebo externému) diaľkovému komunikačnému zariadeniu (RCF). Diaľkové komunikačné zariadenie je zodpovedné za zasielanie týchto údajov prostredníctvom rozhrania DSRC opísaného v dodatku 14 diaľkovému snímaču. V dodatku 1 sa špecifikuje, že údaje RTM sú zreťazením týchto prvkov:

Zašifrovaný obsah tachografu zašifrovanie nezašifrovaného textu obsahu tachografu

Bezpečnostné údaje DRSC opísané ďalej

Formát nezašifrovaného textu obsahových údajov tachografu je uvedený v dodatku 1 a ďalej opísaný v dodatku 14. V tomto oddiele sa opisuje štruktúra bezpečnostných údajov DSRC; formálna špecifikácia je v dodatku 1.

CSM_223 Údaje nezašifrovaného textu `tachographPayload` oznámené jednotkou vozidla diaľkovému komunikačnému zariadeniu (ak RFC nie je súčasťou VU) alebo jednotkou vozidla diaľkovému snímaču cez rozhranie DSRC (ak je RFC súčasťou VU) musia byť chránené v režime šifrovania a následnej autentifikácie, t. j. obsahové údaje tachografu sú najprv zašifrované, aby sa zabezpečila dôvernosť správ, a následne sa vypočíta MAC na zabezpečenie autenticity a integrity údajov.

CSM_224 Bezpečnostné údaje DSRC musia pozostávať zo zreťazenia týchto dátových prvkov v tomto poradí; pozri tiež obrázok 12:

Aktuálny dátum a čas	Aktuálny dátum a čas VU (dátový typ `TimeReal`)
Počítadlo	3-bajtové počítadlo, pozri CSM_225

Sériové číslo VU	Sériové číslo VU (dátový typ `VuSerialNumber`)
Číslo verzie hlavného kľúča DRSC	1-bajtové číslo verzie hlavného kľúča DSRC, z ktorého boli odvodené kľúče DSRC určené pre VU, pozri oddiel 9.2.2.
MAC	MAC vypočítaný zo všetkých predchádzajúcich bajtov v údajoch RTM.

CSM_225 3-bajtové počítadlo v bezpečnostných údajoch DSRC musí byť vo formáte MSB-first (teda bajt najvyššieho rádu na prvom mieste). Keď VU prvýkrát vypočíta súbor údajov RTM po prijatí do výroby, musí nastaviť hodnotu počítadla na 0. VU musí zvýšiť hodnotu počítadla o 1 vždy predtým, ako vypočíta ďalší súbor údajov RTM.

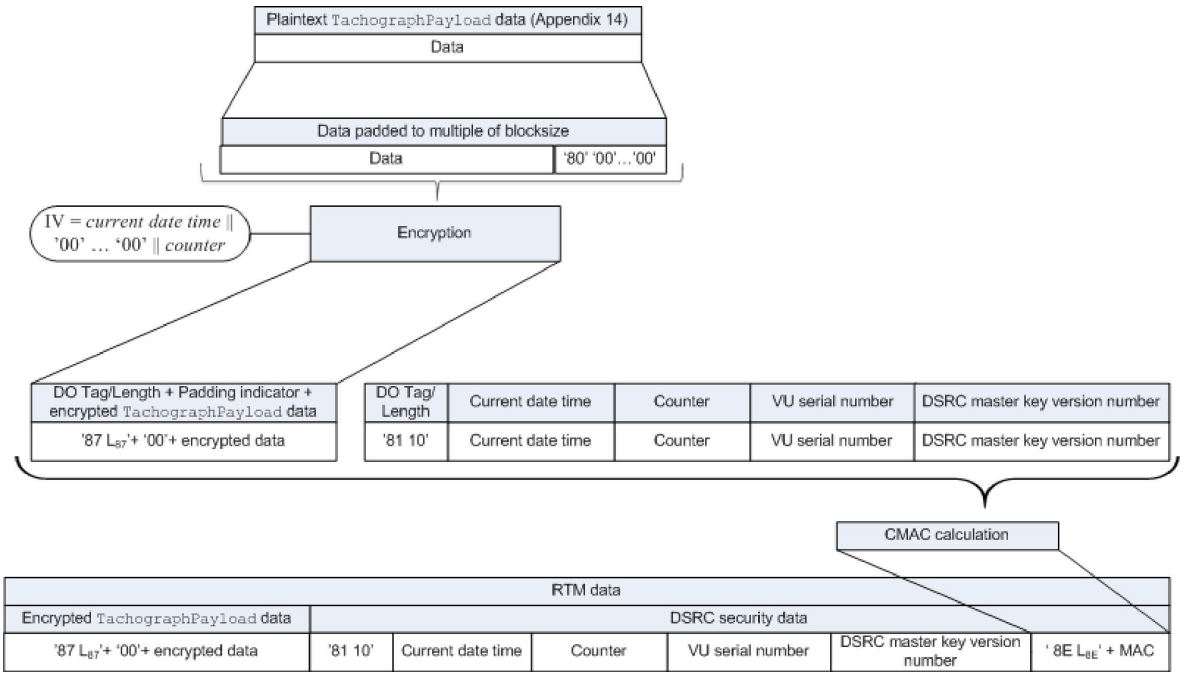
13.2. Šifrovanie obsahu tachografu a generácia MAC

CSM_226 Vzhľadom na dátový prvok nezašifrovaného textu s dátovým typom `TachographPayload` , ako je opísané v dodatku 14, VU musí zašifrovať tieto údaje, ako je znázornené na obrázku 12: kľúč DSRC jednotky vozidla na šifrovanie $K\_VU_{DSRC}\_ENC$ (pozri oddiel 9.2.2) sa musí používať s AES v prevádzkovom režime reťazenia šifrovacieho bloku (CBC), ako je vymedzené v [ISO 10116], s parametrom prekladania m = 1. Inicializačný vektor sa musí rovnať *IV = aktuálny dátum a čas || '00 00 00 00 00 00 00 00' || počítadlo*, kde *aktuálny čas a dátum* a *počítadlo* sú uvedené v CSM_224. Údaje, ktoré sa majú zašifrovať, musia byť vyplnené pomocou metódy vyplňovania 2, vymedzenej v [ISO 9797-1].

CSM_227 VU musí vypočítať MAC v bezpečnostných údajoch DSRC, ako je uvedené na obrázku 12: MAC sa musí vypočítať pre všetky predchádzajúce bajty v údajoch RTM, až do a vrátane čísla verzie hlavného kľúča DSRC, a vrátane tagov a dĺžok dátových objektov. VU musí použiť svoj kľúč DSRC na autenticitu $K\_VU_{DSRC}\_MAC$ (pozri oddiel 9.2.2) s algoritmom AES v režime CMAC, ako je uvedené v [SP 800-38B]. Dĺžka MAC musí byť prepojená s dĺžkou kľúčov DRSC určených pre VU, ako je uvedené v CSM_50.

Obrázok 12

Šifrovanie obsahu tachografu a generácia MAC



13.3. **Overovanie a dešifrovanie obsahu tachografu**

CSM_228 Ak diaľkový snímač získal údaje RTM z VU, musí poslať úplné údaje RTM kontrolnej karte v dátovom poli príkazu PROCESS DSRC MESSAGE, ako sa uvádza v dodatku 2. Potom:

1. Kontrolná karta musí skontrolovať číslo verzie hlavného kľúča DSRC v bezpečnostných údajoch DSRC. Ak kontrolná karta nepozná uvedený hlavný kľúč DSRC, vráti chybu uvedenú v dodatku 2 a zruší proces.

2. Kontrolná karta musí použiť uvedený hlavný kľúč DSRC v kombinácii so sériovým číslom VU v rámci bezpečnostných údajov DSRC na odvodenie kľúčov DSRC K_VU_{DSRC}_ENC a K_VU_{DSRC}_MAC pre danú VU, ako je uvedené v CSM_124.

3. Kontrolná karta musí použiť K_VU_{DSRC}_MAC na overenie MAC v bezpečnostných údajoch DSRC, ako sa uvádza v CSM_227. Ak je MAC nesprávny, kontrolná karta vráti chybu uvedenú v dodatku 2 a zruší proces.

4. Kontrolná karta musí použiť K_VU_{DSRC}_ENC na dešifrovanie zašifrovaného obsahu tachografu, ako sa uvádza v CSM_226. Kontrolná karta musí odstrániť výplň a vrátiť dešifrovaný obsah tachografu diaľkovému snímaču.

CSM_229 S cieľom zabrániť tzv. „replay“ útokom musí diaľkový snímač overiť aktuálnosť údajov RTM overením toho, či sa *aktuálny dátum a čas* v bezpečnostných údajoch DSRC príliš neodchyľuje od aktuálneho času diaľkového snímača.

Poznámky:

— To si vyžaduje, aby mal diaľkový snímač presný a spoľahlivý zdroj času.

— Keďže sa v dodatku 14 vyžaduje, aby VU vypočítala nový súbor údajov RTM každých 60 sekúnd a čas VU sa smie odchýliť 1 minútu od reálneho času, spodný limit pre aktuálnosť údajov RTM je 2 minúty. Skutočná aktuálnosť, ktorá sa má požadovať, tiež závisí od presnosti hodín diaľkového snímača.

CSM_230 Ak dielňa overí správne fungovanie funkcionality DSRC jednotky vozidla, musí poslať úplné údaje RTM prijaté z VU na dielenskú kartu v dátovom poli príkazu PROCESS DSRC MESSAGE, ako sa uvádza v dodatku 2. Dielenská karta musí vykonať všetky kontroly a opatrenia uvedené v CSM_228.

14. PODPIS SŤAHOVANIA ÚDAJOV A OVEROVANIE PODPISOV

14.1. **Všeobecné**

CSM_231 Inteligentné vyhradené zariadenie (IDE) musí uchovávať údaje prijaté z VU alebo karty počas jednej relácie sťahovania v jednom fyzickom dátovom súbore. Údaje sa môžu ukladať na ESM (externé pamäťové médium). Tento súbor obsahuje digitálne podpisy dátových blokov, ako je špecifikované v dodatku 7. Tento súbor musí obsahovať aj tieto certifikáty (pozri oddiel9.1):

— v prípade sťahovania z VU:

— certifikát VU_Sign

— certifikát MSCA_VU-EGF obsahujúci verejný kľúč, ktorý sa má použiť na overovanie certifikátu VU_Sign

— v prípade sťahovania z karty:

— certifikát Card_Sign

— certifikát MSCA_Card obsahujúci verejný kľúč, ktorý sa má použiť na overenie certifikátu Card_Sign

CSM_232 IDE tiež musí mať k dispozícii:

— ak používa na overenie podpisu kontrolnú kartu, ako je uvedené na obrázku 13. prepájací certifikát prepájajúci najnovší certifikát EUR s certifikátom EUR, ktorého obdobie platnosti ho priamo predchádza, pokiaľ existuje.

— ak samo overuje podpis: všetky platné európske koreňové certifikáty.

Poznámka: Metóda, ktorú IDE využíva na získanie týchto certifikátov, nie je uvedená v tomto dodatku.

14.2. **Generovanie podpisu**

CSM_233 Algoritmus podpisovania na vytvorenie digitálnych podpisov pre stiahnuté údaje musí byť ECDSA, ako je uvedené v [DSS], s použitím hašovacieho algoritmu prepojeného s veľkosťou kľúča VU alebo karty, ako je uvedené v CSM_50. Formát podpisu musí byť nezašifrovaný, ako je uvedené v [TR-03111].

14.3. **Overenie podpisu**

CSM_234 IDE môže podpis stiahnutých údajov overovať samo, alebo môže na tento účel použiť kontrolnú kartu. Ak použije kontrolnú kartu, overenie podpisu sa uskutočňuje tak, ako je uvedené na obrázku 13. Ak IDE overuje podpis samo, musí overiť autenticitu a platnosť všetkých certifikátov v certifikačnom reťazci v dátovom súbore, a overiť podpis údajov podľa podpisového systému vymedzeného v [DSS].

Poznámky k obrázku 13:

— Zariadenie, ktoré podpísalo údaje, ktoré sa majú analyzovať, je označené ako EQT.

— Certifikáty a verejné kľúče EQT uvedené na obrázku sú certifikáty a kľúče určené na podpísanie, t. j. VU_Sign alebo Card_Sign.

— Certifikáty a verejné kľúče EQT.CA uvedené na obrázku sú certifikáty a kľúče určené na podpísanie certifikátov VU, resp. karty.

— Certifikát EQT.CA.EUR uvedený na obrázku je európsky koreňový certifikát, ktorý je uvedený v CAR certifikátu EQT.CA.

— Certifikát EQT.Link uvedený na obrázku je prepájací certifikát EQT, ak je prítomný. Ako je uvedené v oddiele 9.1.2, je to prepájací certifikát pre nový európsky pár koreňových kľúčov vytvorený ERCA a podpísaný predchádzajúcim európskym súkromným kľúčom.

— Certifikát EQT.Link.EUR je európsky koreňový certifikát, ktorý je uvedený v CAR certifikátu EQT.Link.

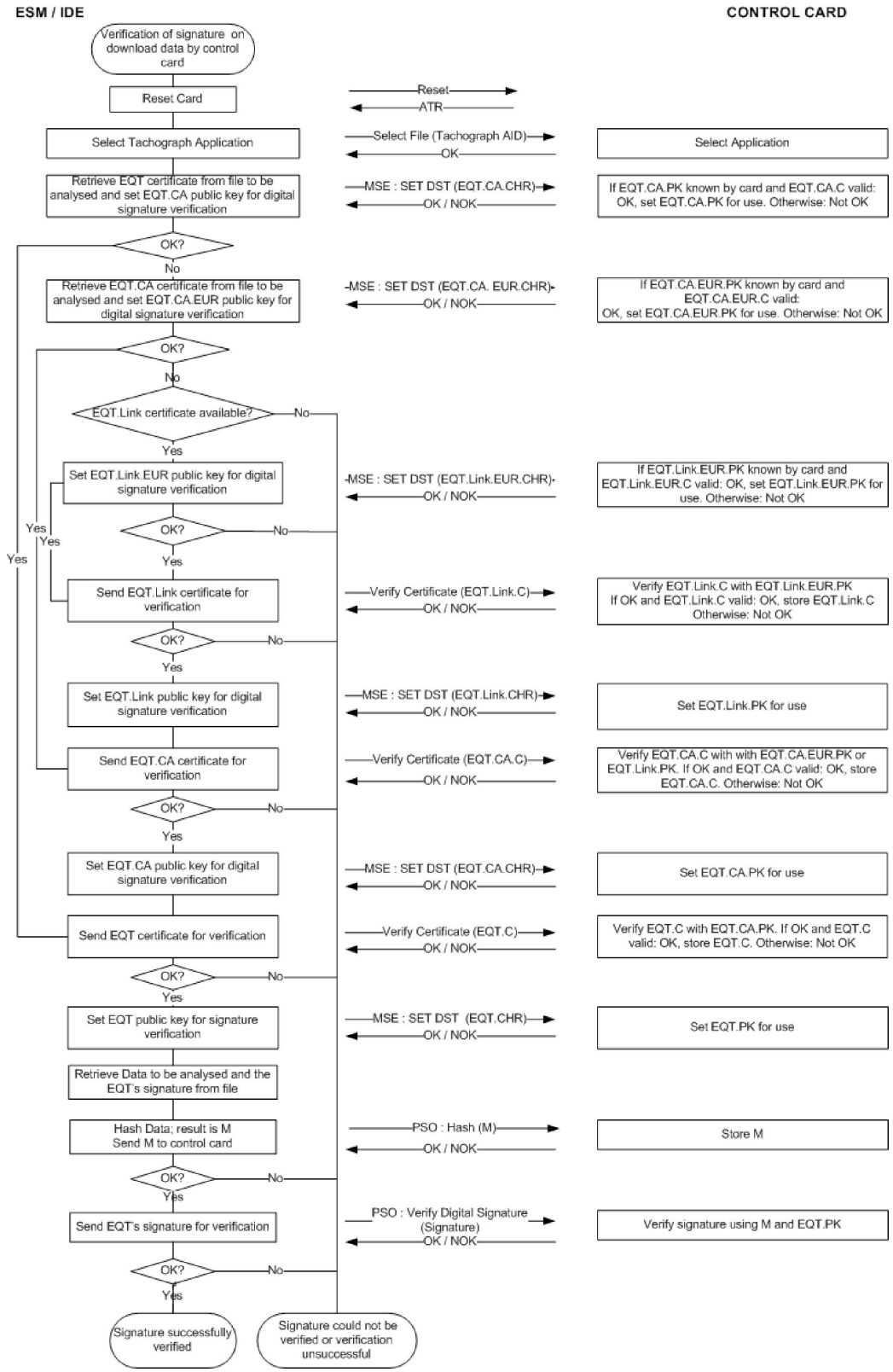
CSM_235 Na výpočet hash M poslaného kontrolnej karte v príkaze PSO:Hash musí IDE použiť hašovací algoritmus prepojený s veľkosťou kľúča VU alebo karty, z ktorých sú údaje stiahnuté, ako je uvedené v CSM_50.

CSM_236 Na overenie podpisu EQT musí kontrolná karta uplatniť podpisový systém vymedzený v [DSS].

Poznámka: Tento dokument neuvádza žiadne kroky, ktoré treba podniknúť, ak podpis stiahnutého dátového súboru nie je možné overiť alebo ak overenie nebolo úspešné.

Obrázok 13

Protokol na overenie podpisu stiahnutého dátového súboru



Dodatok 12

URČOVANIE POLOHY NA ZÁKLADE GLOBÁLNEHO NAVIGAČNÉHO SATELITNÉHO SYSTÉMU (GNSS)

OBSAH

1. ÚVOD 405

1.1. Rozsah pôsobnosti 405

1.2. Akronymy a notácie 405

2. ŠPECIFIKÁCIA PRIJÍMAČA GNSS 406

3. VETY NMEA 406

4. JEDNOTKA VOZIDLA S EXTERNÝM ZARIADENÍM GNSS 408

4.1. Konfigurácia 408

4.1.1 Hlavné komponenty a rozhrania 408

4.1.2 Stav externého zariadenia GNSS na konci výroby 408

4.2. Komunikácia medzi externým zariadením GNSS a jednotkou vozidla 409

4.2.1 Komunikačný protokol 409

4.2.2 Bezpečný prenos údajov GNSS 411

4.2.3 Štruktúra príkazu Read Record 412

4.3. Spojenie, vzájomná autentifikácia a kľúčová dohoda relácie externého zariadenia GNSS s jednotkou vozidla 413

4.4. Spracovanie chýb 413

4.4.1 Chyba komunikácie s externým zariadením GNSS 413

4.4.2 Porušenie fyzickej integrity externého zariadenia GNSS 413

4.4.3 Chýbajúce informácie o polohe od prijímača GNSS 413

4.4.4 Platnosť osvedčenia externého zariadenia GNSS sa skončila 414

5. JEDNOTKA VOZIDLA BEZ EXTERNÉHO ZARIADENIA GNSS 414

5.1. Konfigurácia 414

5.2. Spracovanie chýb 414

5.2.1 Chýbajúce informácie o polohe od prijímača GNSS 414

6. ČASOVÝ ROZPOR GNSS 414

7. NESÚLAD ÚDAJOV O POHYBE VOZIDLA 415

1. ÚVOD

V tomto dodatku sú stanovené technické požiadavky na údaje globálneho navigačného satelitného systému, ktoré využíva jednotka vozidla, vrátane protokolov, ktoré musia byť zavedené, aby bol zaručený bezpečný a správny dátový prenos údajov o polohe.

Uvedené požiadavky vychádzajú najmä z týchto článkov nariadenia (EÚ) č. 165/2014: „Článok 8 Zaznamenávanie polohy vozidla na určitých miestach dennej pracovnej doby“, „Článok 10 Rozhranie s inteligentnými dopravnými systémami“ a „Článok 11 Podrobné ustanovenia o inteligentnom tachografe“.

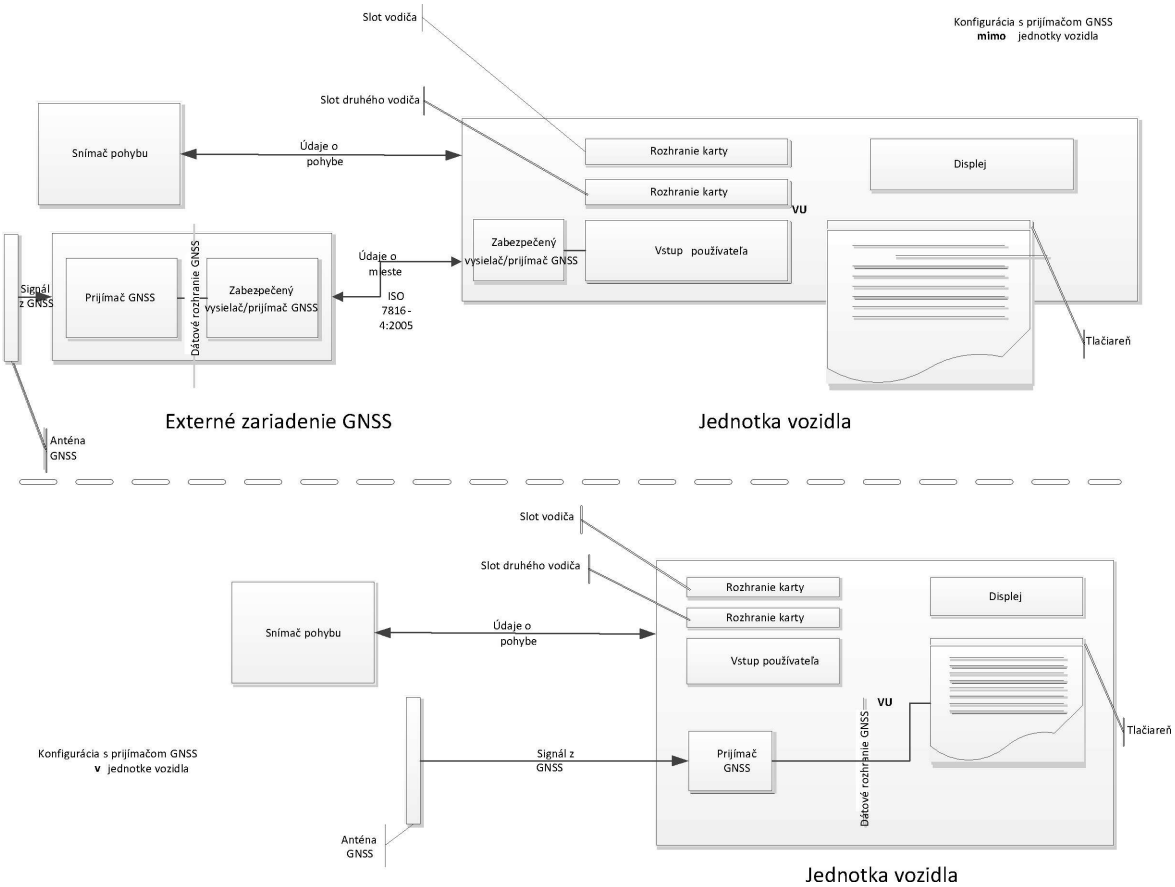
1.1. **Rozsah pôsobnosti**

GNS_1 Na to, aby sa mohol vykonávať článok 8, jednotka vozidla musí získavať údaje o polohe najmenej z jedného GNSS.

Jednotka vozidla môže, ale nemusí obsahovať externé zariadenie GNSS, ako je opísané na obrázku 1:

Obrázok 1

Rôzne konfigurácie prijímača GNSS



1.2. **Akronymy a notácie**

V tomto dodatku sa používajú tieto akronymy:

DOP Dilution of Precision (faktor zníženia presnosti)

EGF Elementary file GNSS Facility (základný súbor zariadenia GNSS)

EGNOS European Geostationary Navigation Overlay Service

GNSS Global Navigation Satellite System (globálny navigačný satelitný systém)

GSA GPS DOP and active satellites (faktor zníženia presnosti a aktívne satelity GPS)

HDOP Horizontal Dilution of Precision (faktor horizontálneho zníženia presnosti)

ICD Interface Control Document (dokument o kontrole rozhrania)

NMEA National Marine Electronics Association (Národná asociácia námornej elektroniky)

PDOP Position Dilution of Precision (faktor zníženia presnosti určenia polohy)

RMC Recommended Minimum Specific (odporúčané minimálne množstvo údajov)

SIS Signal in Space (vysielaný signál)

VDOP Vertical Dilution of Precision (faktor vertikálneho zníženia presnosti)

VU Vehicle Unit (jednotka vozidla – VU)

2. ŠPECIFIKÁCIA PRIJÍMAČA GNSS

Bez ohľadu na konfiguráciu inteligentného tachografu s externým zariadením GNSS alebo bez neho, nevyhnutným prvkom jeho účinnej prevádzky je poskytovanie presných a spoľahlivých informácií o polohe. Preto je vhodné požadovať kompatibilitu inteligentného tachografu so službami, ktoré poskytujú programy Galileo a European Geostationary Navigation Overlay Service (EGNOS), ako je stanovené v nariadení Európskeho parlamentu a Rady (EÚ) č. 1285/2013 ([1]). Systém vytvorený v rámci programu Galileo je nezávislý globálny satelitný navigačný systém a systém vytvorený v rámci programu EGNOS je regionálny satelitný navigačný systém, ktorý zvyšuje kvalitu signálu globálneho polohového systému.

GNS_2 Výrobcovia musia zabezpečiť, aby boli prijímače GNSS v inteligentných tachografoch kompatibilné so službami určovania polohy, ktoré poskytujú systémy Galileo a EGNOS. Výrobcovia sa môžu rozhodnúť, že okrem toho zabezpečia kompatibilitu aj s ďalšími satelitnými navigačnými systémami.

GNS_3 Prijímač GNSS musí byť schopný podporovať autentifikáciu verejne prístupnej služby (Open Service) systému Galileo, keď ju bude systém Galileo poskytovať a výrobcovia prijímačov GNSS podorovať. V prípade inteligentných tachografov zavedených na trh pred tým, ako sa to stane, ktoré nepodporujú autentifikáciu základnej služby systému Galileo, sa dodatočné vybavenie vyžadovať nebude.

3. VETY NMEA

V tomto oddiele sú opísané vety NMEA, ktoré sa používajú pri prevádzke inteligentného tachografu. Tento oddiel je platný pre konfiguráciu inteligentného tachografu s externým zariadením GNSS aj bez neho.

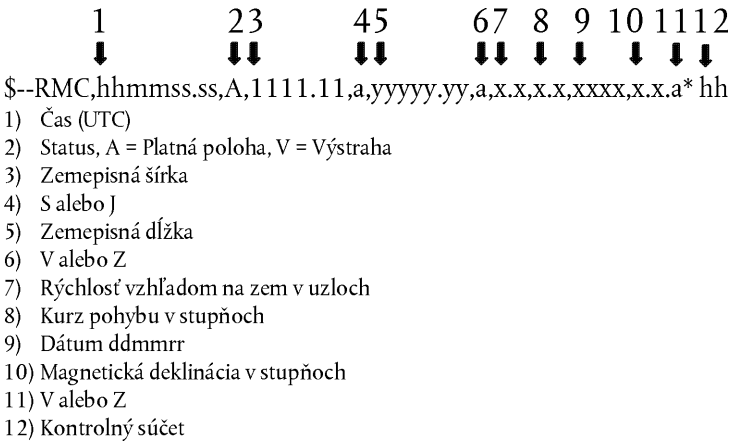
GNS_4 Údaje o polohe sú založené na vete NMEA o odporúčanom minimálnom množstve údajov (RMC) GNSS, ktorá obsahuje informácie o polohe (zemepisná šírka, zemepisná dĺžka), čas vo formáte UTC (koordinovaný svetový čas) (hhmmss.ss) a rýchlosť vzhľadom na zem v uzloch, ako aj doplnkové hodnoty.

Formát vety RMC je takýto (podľa normy NMEA V4.1):

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1285/2013 z 11. decembra 2013 o zriadení a využívaní európskych systémov satelitnej navigácie, ktorým sa ruší nariadenie Rady (ES) č. 876/2002 a nariadenie Európskeho parlamentu a Rady (ES) č. 683/2008 (Ú. v. EÚ L 347, 20.12.2013, s. 1).

Obrázok 2

Štruktúra vety RMC



Údaj o stave poskytuje informáciu, či je signál GNSS dostupný. Pokiaľ stav nenadobudne hodnotu A, prijímané údaje (napr. o čase alebo zemepisnej šírke/dĺžke) sa nemôžu použiť na zaznamenanie polohy vozidla v VU.

Rozlíšenie polohy je založené na už opísanom formáte vety RMC. Prvá časť polí 3 a 5 (prvé dve čísla) sa používa na vyjadrenie stupňov. Zvyšok sa používa na vyjadrenie minút s tromi desatinnými číslami. Rozlíšenie je teda 1/1 000 minúty alebo 1/60 000 stupňa (lebo jedna minúta je 1/60 stupňa).

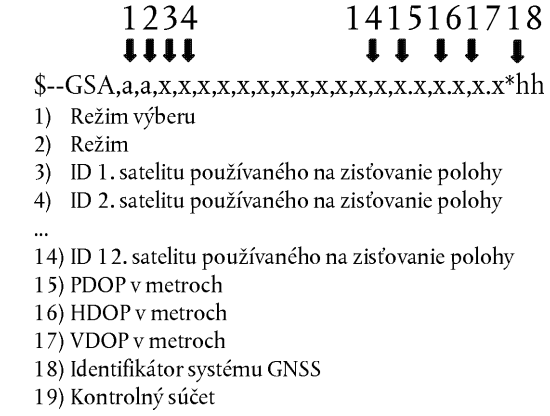
GNS_5 Jednotka vozidla má v databáze VU uloženú ako informáciu o polohe zemepisnú šírku a zemepisnú dĺžku s rozlíšením 1/10 minúty alebo 1/600 stupňa, ako je opísané v dodatku 1 pre typ zemepisných súradníc (GeoCoordinates).

Príkaz GSA (faktor zníženia presnosti a aktívne satelity GPS) môže VU použiť na určenie a zaznamenanie dostupnosti a presnosti signálu. Údaj HDOP sa používa predovšetkým na poskytnutie informácie o úrovni presnosti zaznamenaných údajov o polohe (pozri bod 4.2.2). Vo VU sa uloží hodnota HDOP (faktor horizontálneho zníženia presnosti) vypočítaná ako minimum hodnôt HDOP získaných z dostupných systémov GNSS.

Identifikátor (ID) systému GNSS označuje systémy GPS, Glonass, Galileo, Beidou alebo systém so satelitným rozšírením (SBAS).

Obrázok 3

Štruktúra vety GSA



Kde režim (2) poskytuje informáciu, či je zisťovanie polohy nedostupné (režim = 1), alebo je dostupné v 2D (režim = 2) alebo 3D (režim = 3).

GNS_6 Veta *GSA* sa ukladá s číslom záznamu „06“.

GNS_7 Maximálna veľkosť viet NMEA (napr. RMC, GSA alebo iných), ktorá sa môže použiť na dimenzovanie príkazu na čítanie záznamu, je 85 bajtov (pozri tabuľku 1).

4. JEDNOTKA VOZIDLA S EXTERNÝM ZARIADENÍM GNSS

4.1. **Konfigurácia**

4.1.1 *Hlavné komponenty a rozhrania*

V tejto konfigurácii je prijímač GNSS súčasťou externého zariadenia GNSS.

GNS_8 Externé zariadenie GNSS musí byť napájané cez osobitné rozhranie vozidla.

GNS_9 Externé zariadenie GNSS tvoria tieto komponenty (pozri obrázok 4):

a) komerčný prijímač GNSS na poskytovanie údajov o polohe prostredníctvom dátového rozhrania GNSS. Dátové rozhranie GNSS môže napríklad zodpovedať norme NMEA V4.10, podľa ktorej prijímač GNSS slúži ako vysielač a predáva vety NMEA zabezpečenému vysielaču/prijímaču (secure transceiver) GNSS na frekvencii 1 Hz pre vopred určený súbor viet NMEA, ktorý musí obsahovať prinajmenšom vety RMC a GSA. Zavedenie dátového rozhrania GNSS je vecou voľby výrobcu externého zariadenia GNSS;

b) jednotka vysielača/prijímača (zabezpečený vysielač/prijímač GNSS), zodpovedajúca norme ISO/IEC 7816-4:2013 (pozri bod 4.2.1), umožňujúca komunikáciu s jednotkou vozidla a podporu dátového rozhrania GNSS a prijímača GNSS. Jednotka je vybavená pamäťou na ukladanie identifikačných údajov prijímača GNSS a externého zariadenia GNSS;

c) systém ochranného krytu s funkciou zisťovania nedovolenej manipulácie, v ktorom je uzavretý prijímač GNSS aj zabezpečený vysielač/prijímač GNSS. Funkcia zisťovania nedovolenej manipulácie predstavuje uplatnenie opatrení na bezpečnostnú ochranu, ako sa vyžaduje v profile ochrany inteligentného tachografu;

d) anténa GNSS inštalovaná na vozidle a pripojená k prijímaču GNSS cez systém ochranného krytu.

GNS_10 Externé zariadenie GNSS má prinajmenšom tieto externé rozhrania:

a) rozhranie pre anténu GNSS inštalovanú na vozidle, ak sa používa externá anténa,

b) rozhranie pre jednotku vozidla.

GNS_11 Zabezpečený vysielač/prijímač VU v jednotke vozidla je druhým koncom zabezpečenej komunikácie so zabezpečeným vysielačom/prijímačom GNSS a musí zodpovedať norme ISO/IEC 7816-4:2013 pre pripojenie k externému zariadeniu GNSS.

GNS_12 Na fyzikálnej úrovni komunikácie s externým zariadením GNSS musí jednotka vozidla dodržiavať ISO/IEC 7816 – 12:2005 alebo inú normu, ktorá podporuje ISO/IEC 7816 – 4:2013. (pozri 4.2.1).

4.1.2 *Stav externého zariadenia GNSS na konci výroby*

GNS_13 Keď externé zariadenie GNSS opúšťa výrobný závod, v stálej pamäti zabezpečeného vysielača/prijímača GNSS sú uložené tieto hodnoty:

— kľúčový pár EGF_MA a zodpovedajúci certifikát,

— certifikát MSCA_VU-EGF obsahujúci verejný kľúč MSCA_VU-EGF.PK, ktorý sa používa na overenie certifikátu EGF_MA,

— certifikát EUR obsahujúci verejný kľúč EUR.PK, ktorý sa používa na overenie certifikátu MSCA_VU-EGF,

— certifikát EUR, ktorého platnosť priamo predchádza platnosti certifikátu EUR používaného na overenie certifikátu MSCA_VU-EGF, ak takýto certifikát existuje,

— prepájací certifikát prepájajúci tieto dva certifikáty EUR, ak existuje,

— rozšírené sériové číslo externého zariadenia GNSS,

— identifikátor operačného systému zariadenia GNSS,

— číslo typového schválenia externého zariadenia GNSS,

— identifikátor bezpečnostného prvku externého modulu GNSS.

4.2. **Komunikácia medzi externým zariadením GNSS a jednotkou vozidla**

4.2.1 *Komunikačný protokol*

GNS_14 Komunikačný protokol medzi externým zariadením GNSS a jednotkou vozidla musí podporovať tri funkcie:

1. zhromažďovanie a distribúcia údajov GNSS (napr. o polohe, časovaní, rýchlosti);

2. zhromažďovanie konfiguračných údajov o externom zariadení GNSS;

3. riadiaci protokol na podporu spojenia, vzájomnej autentifikácie a kľúčovej dohody relácie medzi externým zariadením GNSS a VU.

GNS_15 Komunikačný protokol musí byť založený na norme ISO/IEC 7816-4:2013 so zabezpečeným vysielačom/prijímačom VU, ktorý bude plniť úlohu hlavnej jednotky („master“) a zabezpečený vysielač/prijímač GNSS bude podriadený („slave“). Fyzické pripojenie externého zariadenia GNSS k jednotke vozidla je založené na norme ISO/IEC 7816-12:2005 alebo na inej norme, ktorá podporuje ISO/IEC 7816-4:2013.

GNS_16 V komunikačnom protokole sa nepodporujú polia so zväčšenou dĺžkou.

GNS_17 Komunikačný protokol podľa normy ISO 7816 (*-4:2013 aj *-12:2005) medzi externým zariadením GNSS a jednotkou vozidla je nastavený na T = 1.

GNS_18 Pokiaľ ide o funkcie 1) zhromažďovanie a distribúcia údajov GNSS, 2) zhromažďovanie konfiguračných údajov o externom zariadení GNSS a 3) riadiaci protokol, zabezpečený vysielač/prijímač GNSS simuluje inteligentnú kartu so štruktúrou systému súborov, ktorú tvorí hlavný súbor (Master File – MF), súbor s adresárom (Directory File – DF) s aplikačným identifikátorom uvedeným v dodatku 1 kapitole 6.2 („FF 44 54 45 47 4D“) a s tromi elementárnymi súbormi (Elementary File – EF) obsahujúcimi certifikáty a jeden samostatný elementárny súbor (EF.EGF) s identifikátorom súboru rovným „2F2F“, ako je opísané v tabuľke 1.

GNS_19 Zabezpečený vysielač/prijímač GNSS ukladá údaje prichádzajúce z prijímača GNSS a konfiguráciu do súboru EF.EGF. Je to lineárny záznamový súbor variabilnej dĺžky s identifikátorom rovným „2F2F“ v hexadecimálnom formáte.

GNS_20 Zabezpečený vysielač/prijímač GNSS používa pamäť na ukladanie údajov so schopnosťou vykonať najmenej 20 miliónov cyklov zapisovania/čítania. Okrem tohto aspektu je vnútorné usporiadanie a realizácia zabezpečeného vysielača/prijímača GNSS vecou výrobcu.

Prehľad čísel záznamov a údajov je uvedený v tabuľke 1. Všimnite si, že sú tam uvedené štyri vety GSA pre štyri satelitné systémy a systém so satelitným rozšírením (SBAS).

GNS_21 Štruktúra súboru je uvedená v tabuľke 1. Podmienky prístupu (ALW, NEV, SM-MAC) nájdete v dodatku 2 kapitole 3.5.

Tabuľka 1

Štruktúra súboru

		Podmienky prístupu		
Súbor	ID súboru	Čítať	Aktualizovať	Šifrované
MF	3F00			
EF.ICC	0002	ALW	NEV (zo strany VU)	Nie
DF zariadenia GNSS	0501	ALW	NEV	Nie
EF EGF_MACertificate	C100	ALW	NEV	Nie
EF CA_Certificate	C108	ALW	NEV	Nie
EF Link_Certificate	C109	ALW	NEV	Nie
EF.EGF	2F2F	SM-MAC	NEV (zo strany VU)	Nie

Súbor/Dátový prvok	Č. záznamu	Veľkosť (bajty)		Predvolené hodnoty
		Min	Max	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF zariadenia 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				
Veta RMC NMEA	‘01’	85	85	
1. veta GSA NMEA	‘02’	85	85	
2. veta GSA NMEA	‘03’	85	85	

Súbor/Dátový prvok	Č. záznamu	Veľkosť (bajty)		Predvolené hodnoty
		Min	Max	
3. veta GSA NMEA	'04'	85	85	
4. veta GSA NMEA	'05'	85	85	
5. veta GSA NMEA	'06'	85	85	
rozšírené sériové číslo externého zariadenia GNSS vymedzené v dodatku 1 ako SensorGNSSSerialNumber.	'07'	8	8	
identifikátor operačného systému zabezpečeného vysielača/prijímača GNSS, vymedzený v dodatku 1 ako SensorOSIdentifier.	'08'	2	2	
Číslo typového schválenia externého zariadenia GNSS, vymedzené v dodatku 1 ako SensorExternalGNSSApprovalNumber.	'09'	16	16	
Identifikátor bezpečnostného komponentu externého zariadenia GNSS, vymedzený v dodatku 1 ako SensorExternalGNSSSCIdentifier.	'10'	8	8	
RFU – Vyhradené na budúce použitie	Od '11' do 'FD'			

4.2.2 *Bezpečný prenos údajov GNSS*

GNS_22 Bezpečný prenos údajov GNSS o polohe je možný iba za týchto podmienok:

1. Proces spojenia bol dokončený, ako je opísané v dodatku 11. Spoločné bezpečnostné mechanizmy.

2. Pravidelná vzájomná autentifikácia a kľúčová dohoda relácie medzi VU a externým GNSS, tiež opísané v dodatku 11. Spoločné bezpečnostné mechanizmy boli realizované s uvedenou frekvenciou.

GNS_23 Každých T sekúnd, kde T je hodnota nižšia alebo rovná 10, kým sa neuskutoční spojenie alebo vzájomná autentifikácia a kľúčová dohoda relácie, VU požaduje od externého zariadenia GNSS informácie o polohe na základe tohto toku:

1. VU požaduje od externého zariadenia GNSS informácie o mieste spolu s údajmi o faktore zníženia presnosti (z vety GSA NMEA). Zabezpečený vysielač/prijímač VU používa príkaz SELECT a READ RECORD(S) (vybrať a čítať záznam/záznamy) podľa normy ISO/IEC 7816-4:2013 v režime zabezpečeného spracovania iba na základe autentifikácie, ako je opísané v dodatku 11 oddiele 11.5, s identifikátorom súboru „2F2F" a číslom záznamu (RECORD) rovným „01" pre vetu RMC NMEA a „02", „03", „04", „05", „06" pre vetu GSA NMEA.

2. Posledný prijatý údaj o polohe sa uloží v EF s identifikátorom „2F2F" a záznamy opísané v tabuľke 1 v zabezpečenom vysielači/prijímači GNSS, keď zabezpečený vysielač/prijímač GNSS dostáva údaje NMEA s frekvenciou najmenej 1 Hz od prijímača GNSS prostredníctvom dátového rozhrania GNSS.

3. Zabezpečený vysielač/prijímač GNSS posiela odpoveď zabezpečenému vysielaču/prijímaču VU pomocou správy s odpoveďou APDU v režime zabezpečeného spracovania iba na základe autentifikácie, ako je opísané v dodatku 11 oddiele 11.5.

4. Zabezpečený vysielač/prijímač VU skontroluje autenticitu a integritu prijatej odpovede. V prípade kladného výsledku sa údaje o polohe presunú do procesora VU prostredníctvom dátového rozhrania GNSS.

5. Procesor VU skontroluje prijaté údaje tak, že z vety RMC NMEA vyberie informácie (napr. o zemepisnej šírke, zemepisnej dĺžke, čase). Veta RMC NMEA obsahuje informácie, ak je príslušná pozícia platná. Ak táto pozícia nie je platná, údaje o polohe ešte nie sú dostupné a nemôžu sa použiť na zaznamenanie polohy vozidla. Ak je pozícia platná, procesor VU vyberie aj hodnoty faktora HDOP z viet GSA NMEA a vypočíta priemernú hodnotu pre dostupné satelitné systémy (t. j. keď je zisťovanie polohy dostupné).

6. Procesor VU ukladá prijaté a spracované informácie, ako sú zemepisná šírka, zemepisná dĺžka, čas a rýchlosť, v VU vo formáte vymedzenom v dátovom slovníku v dodatku 1 ako zemepisné súradnice (GeoCoordinates), spolu s hodnotou faktora HDOP vypočítanou ako minimum hodnôt HDOP získaných z dostupných systémov GNSS.

4.2.3 *Štruktúra príkazu Read Record*

V tomto oddiele je podrobne opísaná štruktúra príkazu Read Record. Pridáva sa zabezpečené spracovanie správ (v režime iba na základe autentifikácie), ako je opísané v dodatku 11 Spoločné bezpečnostné mechanizmy.

GNS_24 Príkaz podporuje režim zabezpečeného spracovania správ iba na základe autentifikácie, pozri dodatok 11.

GNS_25 Príkazová správa

Bajt	Dĺžka	Hodnota	Opis
CLA	1	'0Ch'	Požaduje sa zabezpečené spracovanie správ.
INS	1	'B2h'	Read Record
P1	1	'XXh'	Číslo záznamu ('00' označuje aktuálny záznam)
P2	1	'04h'	Čítať záznam s číslom záznamu uvedeným v P1
Le	1	'XXh'	Očakávaná dĺžka údajov. Počet bajtov, ktoré sa majú čítať.

GNS_26 Záznam uvedený v P1 sa stáva aktuálnym záznamom.

Bajt	Dĺžka	Hodnota	Opis
#1-#X	X	'XX..XXh'	Prečítané údaje
SW	2	'XXXXh'	Slová označujúce stav (SW1, SW2)

— Ak je príkaz úspešný, zabezpečený vysielač/prijímač GNSS posiela odpoveď „**9000**".

— Ak aktuálny súbor nie je záznamovo orientovaný, zabezpečený vysielač/prijímač GNSS posiela odpoveď„**6981**".

— Ak sa príkaz použije s P1 = „00", ale neexistuje aktuálny EF, zabezpečený vysielač/prijímač GNSS posiela odpoveď „**6986**" (príkaz nie je povolený).

— Ak sa záznam nenájde, zabezpečený vysielač/prijímač GNSS posiela odpoveď „**6A 83**".

— Ak externé zariadenie GNSS zistí nedovolenú manipuláciu, posiela ako odpoveď stavové slová „**66 90**".

GNS_27 Zabezpečený vysielač/prijímač GNSS podporuje tieto príkazy tachografu druhej generácie uvedené v dodatku 2:

Príkaz	Odkaz
Select	Dodatok 2 kapitola 3.5.1
Read Binary	Dodatok 2 kapitola 3.5.2
Get Challenge	Dodatok 2 kapitola 3.5.4
PSO: Verify Certificate	Dodatok 2 kapitola 3.5.7
External Authenticate	Dodatok 2 kapitola 3.5.9
General Authenticate	Dodatok 2 kapitola 3.5.10
MSE:SET	Dodatok 2 kapitola 3.5.11

4.3. **Spojenie, vzájomná autentifikácia a kľúčová dohoda relácie externého zariadenia GNSS s jednotkou vozidla**

Spojenie, vzájomná autentifikácia a kľúčová dohoda relácie externého zariadenia GNSS s jednotkou vozidla sú opísané v dodatku 11. Spoločné bezpečnostné mechanizmy, kapitola 11.

4.4. **Spracovanie chýb**

V tomto oddiele je opísané, ako sa v VU riešia a zaznamenávajú prípadné chybové situácie externého zariadenia GNSS.

4.4.1 *Chyba komunikácie s externým zariadením GNSS*

GNS_28 Ak VU nie je schopná komunikovať s pripojeným externým zariadením GNSS nepretržite dlhšie ako 20 minút, VU generuje a zaznamená udalosť typu EventFaultType s hodnotou enum „53“H *External GNSS communication fault* (externá porucha komunikácie GNSS) a s časovou značkou nastavenou na aktuálny čas. Udalosť sa generuje, iba ak sú splnené tieto dve podmienky: a) inteligentný tachograf nie je v režime kalibrácie a b) vozidlo sa pohybuje. V tejto súvislosti sa komunikačná chyba objaví vtedy, keď zabezpečený vysielač/prijímač VU nedostane správu s odpoveďou na správu s požiadavkou, ako je opísané v bode 4.2.

4.4.2 *Porušenie fyzickej integrity externého zariadenia GNSS*

GNS_29 Ak bolo externé zariadenie GNSS porušené, zabezpečený vysielač/prijímač GNSS vymaže celú svoju pamäť vrátane kryptografických materiálov. Ako je opísané v GNS_25 a GNS_26, VU zistí nedovolenú manipuláciu, ak stav odpovede je „6690“. VU potom vygeneruje udalosť typu EventFaultType enum „55“H *Tamper detection of GNSS* (zistená manipulácia GNSS).

4.4.3 *Chýbajúce informácie o polohe od prijímača GNSS*

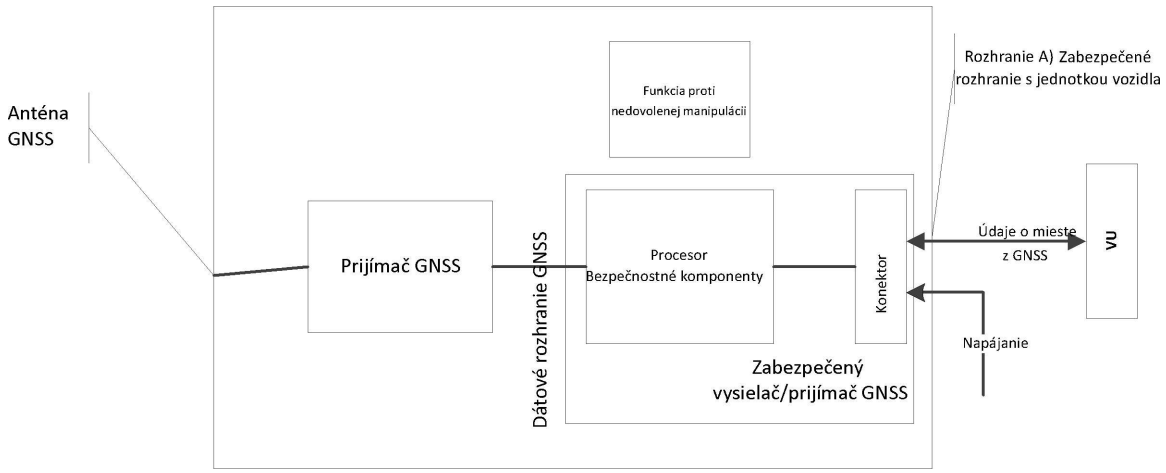
GNS_30 Ak zabezpečený vysielač/prijímač GNSS nedostane údaje od prijímača GNSS nepretržite dlhšie ako tri hodiny, zabezpečený vysielač/prijímač GNSS vygeneruje správu s odpoveďou na príkaz READ RECORD s číslom záznamu (RECORD) rovným „01“ a s dátovým poľom 12 bajtov – všetky nastavené na 0xFF. Po prijatí správy s odpoveďou s touto hodnotou dátového poľa VU vygeneruje a zaznamená udalosť typu EventFaultType enum „52“H *External GNSS receiver fault* (externá porucha prijímača GNSS) s časovou pečiatkou nastavenou na aktuálny čas, iba ak sú splnené tieto dve podmienky: a) inteligentný tachograf nie je v režime kalibrácie a b) vozidlo sa pohybuje.

4.4.1 *Platnosť osvedčenia externého zariadenia GNSS sa skončila*

GNS_31 Ak VU zistí, že certifikát externého zariadenia GNSS, ktorý sa používal na vzájomnú autentifikáciu, už nie je platný, VU vygeneruje a zaznamená chybu záznamového zariadenia typu EventFaultType enum „56“*H External GNSS facility certificate expired (platnosť certifikátu externého zariadenia GNSS sa skončila)* a s časovou pečiatkou nastavenou na aktuálny čas. VU naďalej používa údaje o polohe prijaté od GNSS.

Obrázok 4

Schéma externého zariadenia GNSS



5. JEDNOTKA VOZIDLA BEZ EXTERNÉHO ZARIADENIA GNSS

5.1. **Konfigurácia**

V tejto konfigurácii je prijímač GNSS inštalovaný vo vnútri jednotky vozidla, ako je opísané na obrázku 1.

GNS_32 Prijímač GNSS slúži ako vysielač a odovzdáva vety NMEA procesoru VU, ktorý funguje ako prijímač na frekvencii 1/10 Hz alebo vyššej, pre vopred určený súbor viet NMEA, ktorý musí obsahovať prinajmenšom vety RMC a GSA.

GNS_33 Externá anténa GNSS inštalovaná na vozidle alebo interná anténa GNSS je pripojená k VU.

5.2. **Spracovanie chýb**

5.2.1 *Chýbajúce informácie o polohe od prijímača GNSS*

GNS_34 Ak VU nedostane údaje od prijímača GNSS nepretržite dlhšie ako tri hodiny, VU vyvolá a zaznamená udalosť typu EventFaultType s hodnotou enum „51“H *Internal GNSS receiver fault* (interná porucha prijímača GNSS) s časovou pečiatkou nastavenou na aktuálny čas, iba ak sú splnené tieto dve podmienky: a) inteligentný tachograf nie je v režime kalibrácie a b) vozidlo sa pohybuje.

6. ČASOVÝ ROZPOR GNSS

Ak VU zistí odchýlku väčšiu ako 1 minúta medzi časom určeným funkciou merania času jednotky vozidla a časom pochádzajúcim z prijímača GNSS, VU zaznamená udalosť typu EventFaultType enum *„'0B'H Time conflict (GNSS versus VU internal clock)* [časový konflikt (GNSS verzus vstavané hodiny VU)]. Táto udalosť sa zaznamená spolu s časom vstavaných hodín jednotky vozidla a sprevádza ju automatická úprava času. Po vyvolaní udalosti časového konfliktu nebude VU kontrolovať časovú odchýlku nasledujúcich 12 hodín. Táto udalosť nebude vyvolaná v prípadoch, keď prijímač GNSS nemohol zachytiť platný signál GNSS počas uplynulých 30 dní. Automatické nastavenie času sa však vykoná, keď budú opäť dostupné informácie o polohe z prijímača GNSS.

7. NESÚLAD ÚDAJOV O POHYBE VOZIDLA

GNS_35 VU musí iniciovať a zaznamenať udalosť „nesúlad údajov o pohybe vozidla“ (pozri požiadavku 84 v tejto prílohe) s časovou pečiatkou rovnajúcou sa aktuálnemu času, ak informácie o pohybe vypočítané zo snímača pohybu sú v rozpore s údajmi o pohybe vypočítanými z interného prijímača GNSS alebo externého zariadenia GNSS. Na odhalenie takýchto rozporov sa použije medián rozdielov rýchlosti medzi týmito zdrojmi, ako sa uvádza ďalej:

— každých maximálne 10 sekúnd sa vypočíta absolútna hodnota rozdielu medzi rýchlosťou vozidla odhadnutou z GNSS a rýchlosťou odhadnutou zo snímača pohybu,

— na výpočet mediánu sa použijú všetky vypočítané hodnoty v časovom okne obsahujúcom posledných päť minút pohybu,

— medián sa vypočíta ako priemer 80 % hodnôt, ktoré zostanú po eliminácii najvyšších absolútnych hodnôt (tzv. outliers).

Udalosť nesúlad údajov o pohybe vozidla sa spustí, ak je medián počas piatich neprerušených minút pohybu vozidla vyšší ako 10 km/h. Aby sa zabezpečila spoľahlivejšia detekcia manipulácie s tachografom, môžu sa prípadne použiť iné nezávislé zdroje detekcie pohybu vozidla. (*Poznámka:* použitie mediánu za posledných 5 minút má za cieľ obmedziť riziko zahrnutia odľahlých a prechodných hodnôt). Táto udalosť sa nespustí za týchto podmienok: a) počas prepravy vozidla trajektom alebo vlakom, b) keď nie sú dostupné informácie o polohe z prijímača GNSS a c) počas režimu kalibrácie.

Dodatok 13

ROZHRANIE ITS

OBSAH

1. ÚVOD 416

2. ROZSAH PÔSOBNOSTI 416

2.1. Akronymy, vymedzenia pojmov a notácie 417

3. ODKAZOVANÉ NARIADENIA A NORMY 418

4. PRINCÍP ČINNOSTI ROZHRANIA 418

4.1. Predbežné podmienky prenosu údajov cez rozhranie ITS 418

4.1.1 Údaje poskytované prostredníctvom rozhrania ITS 418

4.1.2 Obsah údajov 418

4.1.3 Aplikácie ITS 418

4.2. Komunikačná technológia 419

4.3. Autorizácia PIN kódom 419

4.4. Formát správy 421

4.5. Súhlas vodiča 425

4.6. Získavanie bežných údajov 426

4.7. Získavanie osobných údajov 426

4.8. Získavanie údajov o udalostiach a poruchách 426

1. ÚVOD

V tomto dodatku sú špecifikované konštrukcie a postupy, ktoré je potrebné dodržiavať s cieľom zaviesť rozhranie s inteligentnými dopravnými systémami (ITS), ako sa to požaduje v článku 10 nariadenia (EÚ) č. 165/2014 (ďalej len „*nariadenie*“).

V *nariadení* sa uvádza, že tachografy vozidiel môžu byť vybavené štandardizovaným rozhraním, ktoré umožňuje externému zariadeniu používať v prevádzkovom režime údaje zaznamenané alebo vytvorené tachografom, ak sú splnené tieto podmienky:

a) rozhranie nemá vplyv na autenticitu a integritu údajov tachografu;

b) rozhranie je v súlade s podrobnými ustanoveniami uvedenými v článku 11 nariadenia;

c) externé zariadenie pripojené k rozhraniu získa prístup k osobným údajom vrátane údajov o geografickej polohe až po overiteľnom súhlase vodiča, ktorého sa tieto údaje týkajú.

2. ROZSAH PÔSOBNOSTI

Rozsahom pôsobnosti tohto dodatku je určiť, ako aplikácie zavedené vo externých zariadeniach môžu cez pripojenie Bluetooth® získať údaje (ďalej len „*údaje*“) z tachografu.

Údaje dostupné cez toto rozhranie sú opísané v prílohe 1 k tomuto dokumentu. Toto rozhranie nevylučuje zavedenie ďalších rozhraní (napr. cez CANbus) na prenos údajov z VU k iným procesorom vozidla.

V tomto dodatku sú špecifikované:

— *údaje* dostupné prostredníctvom rozhrania ITS,

— profil Bluetooth®, ktorý sa používa na prenos údajov,

— postupy dopytu a sťahovania a postupnosť operácií,

— mechanizmus párovania tachografu s externým zariadením,

— mechanizmus vyjadrovania súhlasu dostupný vodičovi.

Na účely spresnenia v tomto dodatku nie sú špecifikované:

— vykonávanie a riadenie získavania *údajov* v rámci VU (ktoré je špecifikované na inom mieste v *nariadení* alebo je funkciou konštrukcie zariadenia),

— forma prezentácie získaných údajov aplikácii zavedenej vo externom zariadení,

— ustanovenia o zabezpečení údajov nad rámec toho, čo poskytuje systém Bluetooth® (ako napríklad šifrovanie), týkajúce sa obsahu *údajov* (ktoré sú špecifikované na inom mieste v *nariadení* (dodatok 10 Spoločné bezpečnostné mechanizmy).

— protokoly Bluetooth®, ktoré používa rozhranie ITS.

2.1. **Akronymy, vymedzenia pojmov a notácie**

V tomto dodatku sa používajú tieto akronymy a vymedzenia pojmov špecifické pre tento dodatok:

Komunikácia	Výmena informácií/údajov medzi hlavnou (master) jednotkou (t. j. tachografom) a externou jednotkou prostredníctvom rozhrania ITS cez Bluetooth®.
Údaje	Súbory údajov, ako sú špecifikované v prílohe 1.
Nariadenie	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 165/2014 zo 4. februára 2014 o tachografoch v cestnej doprave, ktorým sa ruší nariadenie Rady (EHS) č. 3821/85 o záznamovom zariadení v cestnej doprave a mení nariadenie Európskeho parlamentu a Rady (ES) č. 561/2006 o harmonizácii niektorých právnych predpisov v sociálnej oblasti, ktoré sa týkajú cestnej dopravy,
BR	Basic Rate (základná rýchlosť)
EDR	Enhanced Data Rate (vyššia rýchlosť prenosu údajov)
GNSS	Global Navigation Satellite System (globálny navigačný satelitný systém)
IRK	Identity Resolution Key (kľúč rozlišovania identity)
ITS	Intelligent Transport System (inteligentný dopravný systém – ITS)
LE	Low Energy (nízkoenergetické)
PIN	Personal Identification Number (osobné identifikačné číslo)
PUC	Personal Unblocking Code (osobný odblokovací kód)
SID	Service Identifier (identifikátor služby)
SPP	Serial Port Profile (profil sériového portu)
SSP	Secure Simple Pairing (bezpečné jednoduché párovanie)
TRTP	Transfer Request Parameter (parameter prenosu požiadavky)
TREP	Transfer Response Parameter (parameter prenosu odpovede)
VU	Vehicle Unit (jednotka vozidla – VU)

3. ODKAZOVANÉ NARIADENIA A NORMY

Špecifikácia uvedená v tomto dodatku odkazuje na tieto nariadenia a normy alebo ich časti a závisí od nich. V ustanoveniach tohto dodatku sú uvedené príslušné normy alebo ich príslušné časti. V prípade akýchkoľvek nezrovnalostí majú prednosť ustanovenia tohto dodatku.

V tomto dodatku sa odkazuje na tieto nariadenia a normy:

— Nariadenie Európskeho parlamentu a Rady (EÚ) č. 165/2014 zo 4. februára 2014 o tachografoch v cestnej doprave, ktorým sa ruší nariadenie Rady (EHS) č. 3821/85 o záznamovom zariadení v cestnej doprave a mení nariadenie Európskeho parlamentu a Rady (ES) č. 561/2006 o harmonizácii niektorých právnych predpisov v sociálnej oblasti, ktoré sa týkajú cestnej dopravy.

— Nariadenie Európskeho parlamentu a Rady (ES) č. 561/2006 z 15. marca 2006 o harmonizácii niektorých právnych predpisov v sociálnej oblasti, ktoré sa týkajú cestnej dopravy, ktorým sa menia a dopĺňajú nariadenia Rady (EHS) č. 3821/85 a (ES) č. 2135/98 a zrušuje nariadenie Rady (EHS) č. 3820/85.

— ISO 16844 – 4: Cestné vozidlá. Tachografové systémy. Časť 4: Rozhranie CAN

— ISO 16844 – 7: Cestné vozidlá. Tachografové systémy. Časť 7: Parametre

— Bluetooth® – Serial Port Profile – V1.2

— Bluetooth® – Základná verzia 4.2,

— NMEA 0183 V4.1 protocol

4. PRINCÍP ČINNOSTI ROZHRANIA

4.1. **Predbežné podmienky prenosu údajov cez rozhranie ITS**

Za aktualizáciu a uchovávanie údajov, ktoré sa majú uložiť do VU, zodpovedá samotná VU, bez akéhokoľvek zásahu rozhrania ITS. Prostriedky, ktorými sa to dosahuje, sú vnútornou vecou VU a sú špecifikované na inom mieste v *nariadení* a nie sú špecifikované v tomto dodatku.

4.1.1 *Údaje poskytované prostredníctvom rozhrania ITS*

Za aktualizáciu údajov, ktoré sa majú poskytovať prostredníctvom rozhrania ITS na frekvencii určenej v rámci postupov VU, zodpovedá samotná VU, bez akéhokoľvek zásahu rozhrania ITS. Údaje VU sa používajú ako základ na vytváranie a aktualizáciu *údajov*, pričom prostriedky, ktorými sa to dosahuje, sú špecifikované na inom mieste v *nariadení*, alebo ak takáto špecifikácia neexistuje, sú funkciou konštrukcie zariadenia a nie sú špecifikované v tomto dodatku.

4.1.2 *Obsah údajov*

Obsah *údajov* je špecifikovaný v prílohe 1 k tomuto dodatku.

4.1.3 *Aplikácie ITS*

Aplikácie ITS budú využívať údaje sprístupnené prostredníctvom rozhrania ITS napríklad na optimalizáciu riadenia činnosti vodiča, pri dodržiavaní ustanovení nariadenia, na zisťovanie možných porúch tachografu alebo na používanie údajov GNSS. Špecifikácia aplikácií nepatrí do rozsahu pôsobnosti tohto dodatku.

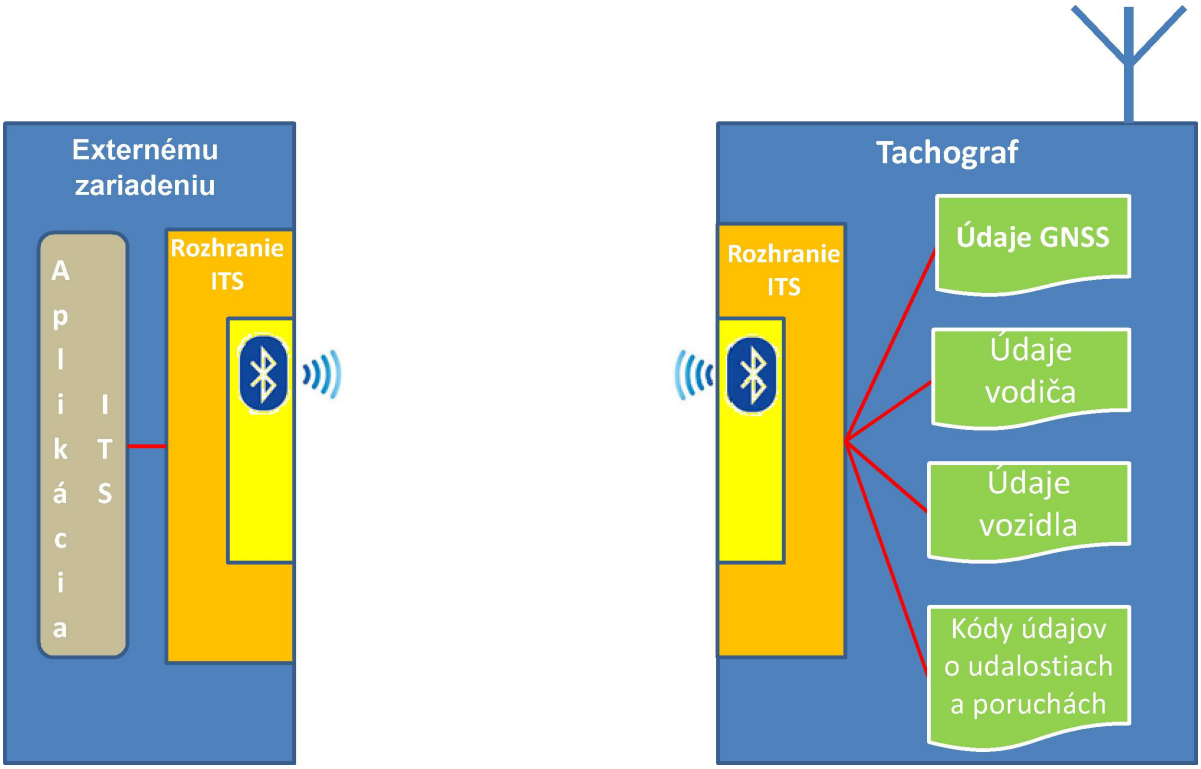
4.2. **Komunikačná technológia**

Výmena *údajov* použitím rozhrania ITS sa vykonáva cez rozhranie kompatibilné s rozhraním Bluetooth®, verzia 4.2 alebo novšia. Rozhranie Bluetooth® pracuje v nelicencovanom pásme vyhradenom na priemyselné, vedecké a lekárske ciele (industrial, scientific and medical – ISM) 2,4 – 2,485 GHz. Rozhranie Bluetooth® 4.2 ponúka zlepšené mechanizmy zaistenia súkromia a bezpečnosti a zvyšuje rýchlosť a spoľahlivosť prenosu údajov. Na účely tejto špecifikácie sa používa rádiové rozhranie Bluetooth® triedy 2 s rozsahom do desiatich metrov. Viac informácií o rozhraní Bluetooth® 4.2 je k dispozícii na webovom sídle www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Komunikácia sa vytvára pomocou komunikačného zariadenia po dokončení procesu párovania autorizovaným zariadením. Rozhranie Bluetooth® využíva model „master/slave“ na riadenie, kedy a kam môžu zariadenia posielať údaje. Tachograf bude plniť úlohu hlavnej („master“) jednotky, zatiaľ čo externé zariadenie bude podriadené („slave“).

Keď sa externé zariadenie prvýkrát dostane do dosahu VU, môže sa začať proces párovania Bluetooth® (pozri aj prílohu 2). Zariadenia si vymenia svoje adresy, názvy, profily a spoločný tajný kľúč, čo im umožňuje spojiť sa, kedykoľvek sa v budúcnosti stretnú. Po dokončení tohto kroku je externé zariadenie dôveryhodné a je pripravené začať s požiadavkami na stiahnutie údajov z tachografu. Nepredpokladá sa pridávanie kódovacích mechanizmov nad rámec toho, čo poskytuje systém Bluetooth®. Ak je však potrebné doplniť bezpečnostné mechanizmy, vykoná sa to v súlade s dodatkom 10 Spoločné bezpečnostné mechanizmy.

Celkový princíp komunikácie je opísaný na tomto obrázku.



Na prenos údajov z VU k externému zariadeniu sa používa profil SPP (Serial Port Profile) Bluetooth®.

4.3. **Autorizácia PIN kódom**

Z bezpečnostných dôvodov musí mať VU posilnený systém autorizácie PIN kódom, oddelený od párovania systému Bluetooth. Každá VU musí byť schopná generovať PIN kódy na účely autentifikácie, pozostávajúce najmenej zo štyroch číslic. Pri každom párovaní s VU musí externé zariadenie pred prijatím akýchkoľvek údajov poskytnúť správny PIN kód.

Po zadaní správneho PIN kódu sa zariadenie zaradí do zoznamu povolených zariadení. Zoznam povolených zariadení musí mať priestor najmenej pre 64 zariadení spárovaných s konkrétnou VU.

Ak zariadenie zadá nesprávny PIN kód trikrát za sebou, dočasne sa zaradí do zoznamu nepovolených zariadení. Kým je zariadenie zaradené do zoznamu nepovolených zariadení, každý ďalší pokus o spojenie bude odmietnutý. Ak zariadenie opäť zadá nesprávny PIN kód trikrát za sebou, trvanie zákazu sa predĺži (pozri tabuľku 1). Po zadaní správneho PIN kódu sa dĺžka trvania zákazu a počet pokusov vynuluje. Obrázok 1 v prílohe 2 predstavuje sekvenčný diagram pokusu o potvrdenie platnosti PIN kódu.

Tabuľka 1

Trvanie zákazu v závislosti od počtu po sebe idúcich nesprávnych zadaní PIN kódu

Počet po sebe idúcich nesprávnych zadaní	Trvanie zákazu
3	30 sekúnd
6	5 minút
9	1 hodina
12	24 hodín
15	natrvalo

Ak zariadenie zadá nesprávny PIN kód pätnásťkrát za sebou (5 × 3), zaradí sa do zoznamu nepovolených jednotiek ITS natrvalo. Tento trvalý zákaz sa zruší iba zadaním správneho PUC kódu.

PUC kód pozostáva z ôsmich číslic a poskytuje ho výrobca pri dodaní VU. Ak dôjde k zadaniu nesprávneho PUC kódu desaťkrát za sebou, zaradí sa do zoznamu nepovolených jednotiek ITS bez možnosti zrušenia.

Výrobca môže poskytnúť možnosť zmeniť PIN kód priamo prostredníctvom VU, ale PUC kód nesmie byť meniteľný. Zmena PIN kódu, ak je možná, si vyžaduje zadanie platného PIN kódu priamo do VU.

Okrem toho všetky zariadenia zaradené do zoznamu povolených zariadení budú na tomto zozname, až kým ich používateľ ručne nevyradí (napr. cez rozhranie človek – stroj VU alebo iným spôsobom). Takto sa môžu zo zoznamu povolených zariadení vyradiť stratené alebo ukradnuté jednotky ITS. Aj v prípade, že jednotka ITS opustí zónu pripojenia Bluetooth na viac ako 24 hodín, automaticky sa vyradí zo zoznamu povolených zariadení VU a pri opätovnom pripájaní musí znovu zadať správny PIN kód.

Formát správ prenášaných medzi rozhraním VU a samotnou VU nie je určený, ale ponecháva sa na voľné uváženie výrobcu. Tento výrobca však musí zabezpečiť, aby bol formát správ prenášaných medzi jednotkou ITS a rozhraním VU uznávaný (pozri špecifikácie ASN.1).

Každá požiadavka na prenos údajov bude preto pred akýmkoľvek spracovaním podrobená riadnemu overovaniu oprávnenia odosielateľa. Obrázok 2 v prílohe 2 predstavuje sekvenčný diagram tohto postupu. Každé zariadenie zaradené do zoznamu nepovolených zariadení dostane automatické odmietnutie. Každé zariadenie nezaradené do zoznamu nepovolených zariadení ani do zoznamu povolených zariadení dostane požiadavku na zadanie PIN kódu, ktorú musí splniť pred opätovným odoslaním svojej požiadavky na prenos údajov.

4.4. **Formát správy**

Všetky správy vymieňané medzi jednotkou ITS a rozhraním VU sú formátované so štruktúrou pozostávajúcou z troch častí: záhlavie pozostávajúce z cieľového bajtu (TGT), zo zdrojového bajtu (SRC) a z dĺžkového bajtu (LEN).

Dátové pole pozostávajúce z bajtu identifikátora služby (SID) a variabilného počtu dátových bajtov (maximálne 255).

Bajt kontrolného súčtu je jednobajtový súčet modulov 256 všetkých bajtov správy, okrem samotného CS.

Správa musí byť vo formáte Big Endian.

Tabuľka 2

Všeobecný formát správy

Záhlavie			Dátové pole					Kontrolný súčet
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 bajty			Maximálne 255 bajtov					1 bajt

Záhlavie

TGT a SRC: identifikátor (ID) cieľového (TGT) a zdrojového (SRC) zariadenia správy. Predvolená hodnota ID rozhrania VU je „EE“. Hodnota ID sa nemôže meniť. Jednotka ITS používa pre svoju prvú správu komunikačnej relácie predvolenú hodnotu ID „A0“. Rozhranie VU potom pridelí jednotke ITS jedinečný ID a informuje ju o tomto ID pre budúce správy počas relácie.

Bajt LEN zohľadňuje iba časť „DATA“ dátového poľa (pozri tabuľku 2), pričom prvé štyri bajty sú implicitné.

Rozhranie VU potvrdí autenticitu odosielateľa správy krížovou kontrolou svojho zoznamu ID a údajov Bluetooth, teda kontrolou, či jednotka ITS zodpovedajúca zadanému ID je momentálne v dosahu pripojenia Bluetooth.

Dátové pole

Dátové pole okrem identifikátora služby (SID) obsahuje aj ďalšie parametre: parameter prenosu požiadavky (TRTP) a bajty počítadla.

Ak sú údaje, ktoré sa majú prenášať, dlhšie než disponibilné miesto v jednej správe, rozdelia sa na viaceré čiastkové správy. Každá čiastková správa musí mať rovnaké záhlavie a SID, ale bude obsahovať dvojbajtové počítadlo, aktuálny údaj počítadla (Counter Current – CC) a maximálny údaj počítadla (Counter Max – CM), na označenie čísla čiastkovej správy. S cieľom umožniť kontrolu chýb a zrušenie potvrdzuje prijímajúce zariadenie každú čiastkovú správu. Prijímajúce zariadenie môže prijať čiastkovú správu, požiadať o jej nový prenos, ako aj požadovať od odosielajúceho zariadenia, aby znovu začalo alebo zrušilo prenos.

Ak sa bajty CC a CM nepoužívajú, dostanú hodnotu 0xFF.

Napríklad táto správa

HEADER	SID	TRTP	CC	CM	DATA	CS
3 bajty	Dlhšia než 255 bajtov					1 bajt

sa prenáša takto:

HEADER	SID	TRTP	01	n	DATA	CS
3 bajty	255 bajty					1 bajt

HEADER	SID	TRTP	02	n	DATA	CS
3 bajty	255 bajty					1 bajt

…

HEADER	SID	TRTP	N	N	DATA	CS
3 bajty	Maximálne 255 bajtov					1 bajt

Tabuľka 3 obsahuje správy, ktoré sú schopné vymieňať si VU a jednotka ITS. Obsah každého parametra je uvedený v hexadecimálnom tvare. V tabuľke nie sú z dôvodu prehľadnosti zastúpené bajty CC a CM. Ich úplný formát je uvedený vyššie.

Tabuľka 3

Podrobný obsah správy

Správa	Záhlavie			DATA			Kontrolný súčet
	TGT	SRC	LEN	SID	TRTP	DATA	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (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	Čas	
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		

Správa	Záhlavie			DATA			Kontrolný súčet
	TGT	SRC	LEN	SID	TRTP	DATA	
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Údaje	
DataUnavailable							
Žiadne údaje nie sú k dispozícii	*ITSID*	EE	02	0A	TREP	10	
Osobné údaje sa nezdieľajú	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Všeobecné odmietnutie	*ITSID*	EE	02	0 B	SID Req	10	
Služba nie je podporovaná	*ITSID*	EE	02	0 B	SID Req	11	
Subfunkcia nie je podporovaná	*ITSID*	EE	02	0 B	SID Req	12	
Nesprávna dĺžka správy	*ITSID*	EE	02	0 B	SID Req	13	
Nesprávne podmienky alebo sekvenčná chyba požiadavky	*ITSID*	EE	02	0 B	SID Req	22	
Požiadavka mimo rozsahu	*ITSID*	EE	02	0 B	SID Req	31	
Odpoveď nasleduje	*ITSID*	EE	02	0 B	SID Req	78	
Nezhoda ITSID	*ITSID*	EE	02	0 B	SID Req	FC	
ITSID sa nenašiel	*ITSID*	EE	02	0 B	SID Req	FB	

RequestPIN (SID 01)

Túto správu vydáva rozhranie VU, ak požiadavku na prenos akýchkoľvek údajov posiela jednotka ITS, ktorá nie je zaradená do zoznamu nepovolených zariadení ani do zoznamu povolených zariadení.

SendITSID (SID 02)

Túto správu vydáva rozhranie VU vždy, keď požiadavku posiela nové zariadenie. Zariadenie používa predvolenú hodnotu ID „A0“, pokiaľ nedostane pridelený jedinečný ID pre komunikačnú reláciu.

SendPIN (SID 03)

Túto správu vydáva jednotka ITS, aby ju rozhranie VU zaradilo do zoznamu povolených zariadení. Obsahom tejto správy je kód 4 INTEGER 0 až 9.

PairingResult (SID 04)

Túto správu vydáva rozhranie VU na informovanie jednotky ITS, či PIN kód, ktorý jednotka odoslala, bol správny. Obsahom tejto správy je BOOLEAN s hodnotou „True“, ak bol PIN kód správny, a „False“ v opačnom prípade.

SendPUC (SID 05)

Túto správu vydáva jednotka ITS, aby rozhranie VU zrušilo sankciu zaradenia do zoznamu nepovolených zariadení. Obsahom tejto správy je kód 8 INTEGER 0 až 9.

BanLiftingResult (SID 06)

Túto správu vydáva rozhranie VU na informovanie jednotky ITS, či PUC kód, ktorý jednotka odoslala, bol správny. Obsahom tejto správy je BOOLEAN s hodnotou „True“, ak bol PUC kód správny, a „False“ v opačnom prípade.

RequestRejected (SID 07)

Túto správu vydáva rozhranie VU ako odpoveď na akúkoľvek správu jednotky ITS zaradenej do zoznamu nepovolených zariadení, s výnimkou správy „SendPUC“. Správa obsahuje zostávajúci čas, dokedy bude jednotka ITS zaradená do zoznamu nepovolených zariadení, pri dodržaní formátu sekvencie „Time“, ako je vymedzený v prílohe 3.

RequestData (SID 08)

Túto správu vydáva jednotka ITS ako požiadavku na sprístupnenie údajov. Jednobajtový parameter prenosu požiadavky (TRTP) udáva typ požadovaných údajov. Existuje viacero typov údajov:

— standardTachData (TRTP 01): údaje dostupné z tachografu klasifikované ako nie osobné,

— personalTachData (TRTP 02): údaje dostupné z tachografu klasifikované ako osobné,

— gnssData (TRTP 03): údaje GNSS, vždy osobné,

— standardEventData (TRTP 04): zaznamenané údaje o udalosti klasifikované ako nie osobné,

— personalEventData (TRTP 05): zaznamenané údaje o udalosti klasifikované ako osobné,

— standardFaultData (TRTP 06): zaznamenané poruchy klasifikované ako nie osobné,

— manufacturerData (TRTP 07). údaje sprístupnené výrobcom.

Viac informácií o obsahu každého typu údajov nájdete v prílohe 3 k tomuto dodatku.

Viac informácií o formáte a obsahu údajov GNSS nájdete v dodatku 12.

Viac informácií týkajúcich sa kódu údajov o udalosti a porúch nájdete v prílohách IB a IC.

ResquestAccepted (SID 09)

Túto správu vydáva rozhranie VU, ak bola správa „RequestData“ jednotky ITS prijatá. Táto správa obsahuje jednobajtový parameter TREP, čo je bajt TRTP súvisiacej správy „RequestData“, a všetky údaje požadovaného typu.

DataUnavailable (SID 0A)

Túto správu vydáva rozhranie VU, ak z určitých dôvodov nie sú požadované údaje k dispozícii, aby sa mohli poslať jednotke ITS zaradenej do zoznamu povolených zariadení. Táto správa obsahuje jednobajtový parameter TREP, čo je parameter TRTP požadovaných údajov, a jednobajtový kód chýb špecifikovaný v tabuľke 3. K dispozícii sú tieto kódy:

— Žiadne údaje nie sú k dispozícii (10): rozhranie VU sa z nešpecifikovaných dôvodov nemôže dostať k údajom VU,

— Osobné údaje sa nezdieľajú (11): jednotka ITS sa pokúša opäť získať osobné údaje, ktoré sa nezdieľajú.

NegativeAnswer (SID 0B)

Túto správu vydáva rozhranie VU, ak požiadavku nemožno vybaviť z iného dôvodu, než je nedostupnosť údajov. Táto správa je spravidla dôsledkom nesprávneho formátu požiadavky (dĺžka, SID, ITSID…), ale nie je obmedzená výlučne na tento prípad. TRTP v dátovom poli obsahuje SID požiadavky. Dátové pole obsahuje kód označujúci dôvod zápornej odpovede. K dispozícii sú tieto kódy:

— Všeobecné odmietnutie (kód: 10)

— Tento krok nie je možné vykonať z dôvodu, ktorý nie je uvedený v ďalšej časti ani v oddiele (zadaj číslo oddielu *DataUnavailable*).

— Služba nie je podporovaná (kód: 11)

— SID požiadavky je nezrozumiteľný.

— Subfunkcia nie je podporovaná (kód: 12)

— Parameter požiadavky TRTP je nezrozumiteľný. Môže napríklad chýbať alebo jeho hodnota leží mimo prípustných hodnôt.

— Nesprávna dĺžka správy (kód: 13)

— Dĺžka prijatej správy je nesprávna (nezhoda medzi bajtom LEN a skutočnou dĺžkou správy).

— Nesprávne podmienky alebo sekvenčná chyba požiadavky (kód: 22)

— Požadovaná služba nie je aktívna alebo sekvencia správ s požiadavkami nie je správna.

— Požiadavka mimo rozsahu (kód: 33)

— Záznam o parametri požiadavky (dátové pole) nie je platný.

— Odpoveď nasleduje (kód: 78)

— Požadovaná činnosť sa nemôže dokončiť načas a VU nie je pripravená na prijatie ďalšej požiadavky.

— Nezhoda *ITSID* (kód: FB)

— Zdrojový bajt SRC *ITSID* po porovnaní s informáciami systému Bluetooth nie je v súlade s pripojeným zariadením.

— *ITSID* sa nenašiel (kód: FC)

— Zdrojový bajt SRC ITSID nie je spojený so žiadnym zariadením.

V riadkoch 1 – 72 (**FormatMessageModule**) kódu ASN.1 v prílohe 3 sú špecifikované formáty správ, ako je uvedené v tabuľke 3. Viac podrobností o obsahu správ je uvedených v ďalšej časti.

4.5. **Súhlas vodiča**

Všetky dostupné údaje sa klasifikujú buď ako bežné, alebo ako osobné. Osobné údaje sa sprístupnia, iba ak s tým vyjadrí súhlas vodič, ktorý tak súhlasí s tým, aby osobné údaje z tachografu opustili sieť vozidla a použili sa pre aplikácie tretej strany.

Vodič vyjadrí svoj súhlas, keď pri prvom vložení danej karty vodiča alebo dielenskej karty, zatiaľ pre jednotku vozidla neznámej, držiteľ karty dostane výzvu, aby vyjadril svoj súhlas s odoslaním osobných údajov, súvisiacich s tachografom, prostredníctvom voliteľného rozhrania ITS (pozri aj odsek 3.6.2 prílohy I C).

Stav súhlasu (aktivovaný/deaktivovaný) sa zaznamená v pamäti tachografu.

V prípade viacerých vodičov sa s rozhraním ITS môžu zdieľať len osobné údaje o vodičoch, ktorí na to dali svoj súhlas. Ak sú vo vozidle napríklad dvaja vodiči a iba prvý vodič súhlasí so zdieľaním svojich osobných údajov, osobné údaje týkajúce sa druhého vodiča nesmú byť zdieľané.

4.6. **Získavanie bežných údajov**

Obrázok 3 v prílohe 2 predstavuje sekvenčný diagram platnej požiadavky, ktorú poslala jednotka ITS, aby získala prístup k štandardným údajom. Jednotka ITS je riadne zaradená do zoznamu povolených zariadení a nepožaduje osobné údaje, preto nie je potrebné ďalšie overovanie. V diagramoch sa predpokladá, že už boli riadne vykonané postupy zobrazené na obrázku 2 v prílohe 2. Tie sa môžu dosadiť namiesto sivého okienka *REQUEST TREATMENT* na obrázku 2.

Spomedzi dostupných údajov sa za bežné považujú:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Získavanie osobných údajov**

Obrázok 4 v prílohe 2 predstavuje sekvenčný diagram spracovania požiadavky na osobné údaje. Ako už bolo uvedené, rozhranie VU odošle osobné údaje, iba ak vodič vyslovene súhlasil (pozri aj oddiel 4.5). V opačnom prípade sa požiadavka musí automaticky odmietnuť.

Spomedzi dostupných údajov sa za osobné považujú:

— personalTachData (TRTP 02),

— gnssData (TRTP 03),

— personalEventData (TRTP 05),

— manufacturerData (TRTP 07).

4.8. **Získavanie údajov o udalostiach a poruchách**

Jednotky ITS môžu požadovať údaje o udalostiach uvedených v zozname všetkých neočakávaných udalostí. Tieto údaje sa považujú buď za bežné, alebo za osobné (pozri prílohu 3). Obsah každej udalosti zodpovedá dokumentácii uvedenej v prílohe 1 k tomuto dodatku.

PRÍLOHA 1

ZOZNAM ÚDAJOV DOSTUPNÝCH PROSTREDNÍCTVOM ROZHRANIA ITS

Data	Source	Data classification (personal/ not personal)
VehicleIdentificationNumber	Vehicle Unit	**not personal**
CalibrationDate	Vehicle Unit	**not personal**
TachographVehicleSpeed speed instant t	Vehicle Unit	personal
Driver1WorkingState Selector driver	Vehicle Unit	personal
Driver2WorkingState	Vehicle Unit	personal
DriveRecognize Speed Threshold detected	Vehicle Unit	**not personal**
Driver1TimeRelatedStates Weekly day time	Driver Card	personal
Driver2TimeRelatedStates	Driver Card	personal
DriverCardDriver1	Vehicle Unit	**not personal**
DriverCardDriver2	Vehicle unit	**not personal**
OverSpeed	Vehicle Unit	personal
TimeDate	Vehicle Unit	**not personal**
HighResolutionTotalVehicleDistance	Vehicle Unit	**not personal**
ServiceComponentIdentification	Vehicle Unit	**not personal**
ServiceDelayCalendarTimeBased	Vehicle Unit	**not personal**
Driver1Identification	Driver Card	personal
Driver2Identification	Driver Card	personal
NextCalibrationDate	Vehicle Unit	**not personal**
Driver1ContinuousDrivingTime	Driver Card	personal
Driver2ContinuousDrivingTime	Driver Card	personal
Driver1CumulativeBreakTime	Driver Card	personal
Driver2CumulativeBreakTime	Driver Card	personal
Driver1CurrentDurationOfSelectedActivity	Driver Card	personal
Driver2CurrentDurationOfSelectedActivity	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
SpeedAuthorised	Vehicle Unit	**not personal**
TachographCardSlot1	Driver Card	**not personal**
TachographCardSlot2	Driver Card	**not personal**
Driver1Name	Driver Card	personal
Driver2Name	Driver Card	personal
OutOfScopeCondition	Vehicle Unit	**not personal**
ModeOfOperation	Vehicle Unit	**not personal**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
EngineSpeed	Vehicle Unit	personal
RegisteringMemberState	Vehicle Unit	**not personal**
VehicleRegistrationNumber	Vehicle Unit	**not personal**
Driver1EndOfLastDailyRestPeriod	Driver Card	personal
Driver2EndOfLastDailyRestPeriod	Driver Card	personal
Driver1EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver1EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver1CurrentDailyDrivingTime	Driver Card	personal
Driver2CurrentDailyDrivingTime	Driver Card	personal
Driver1CurrentWeeklyDrivingTime	Driver Card	personal
Driver2CurrentWeeklyDrivingTime	Driver Card	personal
Driver1TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver1CardExpiryDate	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
Driver2CardExpiryDate	Driver Card	personal
Driver1CardNextMandatoryDownloadDate	Driver Card	personal
Driver2CardNextMandatoryDownloadDate	Driver Card	personal
TachographNextMandatoryDownloadDate	Vehicle Unit	**not personal**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Driver Card	personal
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Driver Card	personal
Driver1CumulativeUninterruptedRestTime	Driver Card	personal
Driver2CumulativeUninterruptedRestTime	Driver Card	personal
Driver1MinimumDailyRest	Driver Card	personal
Driver2MinimumDailyRest	Driver Card	personal
Driver1MinimumWeeklyRest	Driver Card	personal
Driver2MinimumWeeklyRest	Driver Card	personal
Driver1MaximumDailyPeriod	Driver Card	personal
Driver2MaximumDailyPeriod	Driver Card	personal
Driver1MaximumDailyDrivingTime	Driver Card	personal
Driver2MaximumDailyDrivingTime	Driver Card	personal
Driver1NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver2NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver1RemainingCurrentDrivingTime	Driver Card	personal
Driver2RemainingCurrentDrivingTime	Driver Card	personal
GNSS position	Vehicle Unit	personal

2) SÚVISLÉ ÚDAJE GNSS DOSTUPNÉ PO SÚHLASE VODIČA

Pozri dodatok 12 – GNSS.

3) KÓDY UDALOSTÍ DOSTUPNÉ BEZ SÚHLASU VODIČA

Udalosť	Pravidlá uloženia	Údaje, ktoré sa zaznamenajú o každej udalosti
Vloženie neplatnej karty	— 10 posledných udalostí.	— dátum a čas udalosti, — typ, číslo, vydávajúci členský štát a generácia karty(-iet), ktorá(-é) spôsobila(-i) udalosť, — počet podobných udalostí v daný deň.
Konflikt karty	— 10 posledných udalostí.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ, číslo, vydávajúci členský štát a generácia dvoch kariet, ktoré spôsobili rozpor.
Nesprávne uzavretá posledná relácia karty	— 10 posledných udalostí.	— dátum a čas vloženia karty, — typ, číslo, vydávajúci členský štát a generácia karty, — údaje čítané z karty počas poslednej relácie: — dátum a čas vloženia karty, — VRN, členský štát evidencie a generácia VU.
Prerušenie napájania (2)	— najdlhšia udalosť počas každého z 10 posledných dní jej výskytu, — 5 najdlhších udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ, číslo, vydávajúci členský štát a generácia všetkých kariet vložených na začiatku a/alebo na konci udalosti, — počet podobných udalostí v daný deň.
Chyba komunikácie s diaľkovým komunikačným zariadením	— najdlhšia udalosť počas každého z 10 posledných dní jej výskytu, — 5 najdlhších udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ, číslo, vydávajúci členský štát a generácia všetkých kariet vložených na začiatku a/alebo na konci udalosti, — počet podobných udalostí v daný deň.
Chýbajúce informácie o polohe z prijímača GNSS	— najdhšia udalosť počas každého z 10 posledných dní jej výskytu, — 5 najdlhších udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ, číslo, vydávajúci členský štát a generácia všetkých kariet vložených na začiatku a/alebo na konci udalosti, — počet podobných udalostí v daný deň.
Chyba údajov o pohybe	— najdlhšia udalosť počas každého z 10 posledných dní jej výskytu, — 5 najdlhších udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ, číslo, vydávajúci členský štát a generácia všetkých kariet vložených na začiatku a/alebo na konci udalosti, — počet podobných udalostí v daný deň.

Udalosť	Pravidlá uloženia	Údaje, ktoré sa zaznamenajú o každej udalosti
Nesúlad údajov o pohybe vozidla	— najdlhšia udalosť počas každého z 10 posledných dní jej výskytu, — 5 najdlhších udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ, číslo, vydávajúci členský štát a generácia všetkých kariet vložených na začiatku a/alebo na konci udalosti, — počet podobných udalostí v daný deň.
Pokus o narušenie zabezpečenia	10 posledných udalostí z každého typu udalosti.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti (ak je to relevantné), — typ, číslo, vydávajúci členský štát a generácia všetkých kariet vložených na začiatku a/alebo na konci udalosti, — typ udalosti.
Časový konflikt	— najdlhšia udalosť počas každého z 10 posledných dní jej výskytu, — 5 najdlhších udalostí počas posledných 365 dní.	— dátum a čas záznamového zariadenia, — dátum a čas GNSS, — typ, číslo, vydávajúci členský štát a generácia všetkých kariet vložených na začiatku a/alebo na konci udalosti, — počet podobných udalostí v daný deň.

4) KÓDY UDALOSTÍ DOSTUPNÉ SO SÚHLASOM VODIČA

Udalosť	Pravidlá uloženia	Údaje, ktoré sa zaznamenajú o každej udalosti
Jazda bez príslušnej karty	— najdlhšia udalosť počas každého z 10 posledných dní jej výskytu, — 5 najdlhších udalostí počas posledných 365 dní.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — typ, číslo, vydávajúci členský štát a generácia všetkých kariet vložených na začiatku a/alebo na konci udalosti, — počet podobných udalostí v daný deň.
Vloženie karty za jazdy	— posledná udalosť počas každého z 10 posledných dní jej výskytu.	— dátum a čas udalosti, — typ, číslo, vydávajúci členský štát a generácia karty, — počet podobných udalostí v daný deň.
Prekročenie rýchlosti (1)	— najzávažnejšia udalosť počas každého z 10 posledných dní jej výskytu (t. j. udalosť s najvyššou priemernou rýchlosťou), — 5 najzávažnejších udalostí počas posledných 365 dní, — prvá udalosť, ktorá sa vyskytla po poslednej kalibrácii.	— dátum a čas začiatku udalosti, — dátum a čas konca udalosti, — maximálna rýchlosť nameraná počas udalosti, — aritmetický priemer rýchlosti nameranej počas udalosti, — typ, číslo, vydávajúci členský štát a generácia karty vodiča (ak je to použiteľné), — počet podobných udalostí v daný deň.

5) KÓDY ÚDAJOV O PORUCHÁCH DOSTUPNÉ BEZ SÚHLASU VODIČA

Porucha	Pravidlá uloženia	Údaje, ktoré sa zaznamenajú o každej poruche
Porucha karty	— 10 posledných porúch karty vodiča.	— dátum a čas začiatku poruchy, — dátum a čas konca poruchy, — typ, číslo, vydávajúci členský štát a generácia karty(-iet).
Porucha záznamového zariadenia	— 10 posledných porúch z každého typu poruchy, — prvá porucha, ktorá sa vyskytla po poslednej kalibrácii.	— dátum a čas začiatku poruchy, — dátum a čas konca poruchy, — typ poruchy, — typ, číslo, vydávajúci členský štát a generácia všetkých kariet vložených na začiatku a/alebo na konci poruchy.

Táto porucha vznikne pri každom uvedenom zlyhaní, ak zariadenie nie je v režime kalibrácie:

— vnútorná porucha VU,

— porucha tlače,

— porucha zobrazenia

— porucha sťahovania,

— porucha snímača,

— porucha prijímača GNSS alebo externého zariadenia GNSS,

— porucha diaľkového komunikačného zariadenia.

6) UDALOSTI A PORUCHY BEZ SÚHLASU VODIČA ŠPECIFIKOVANÉ VÝROBCOM

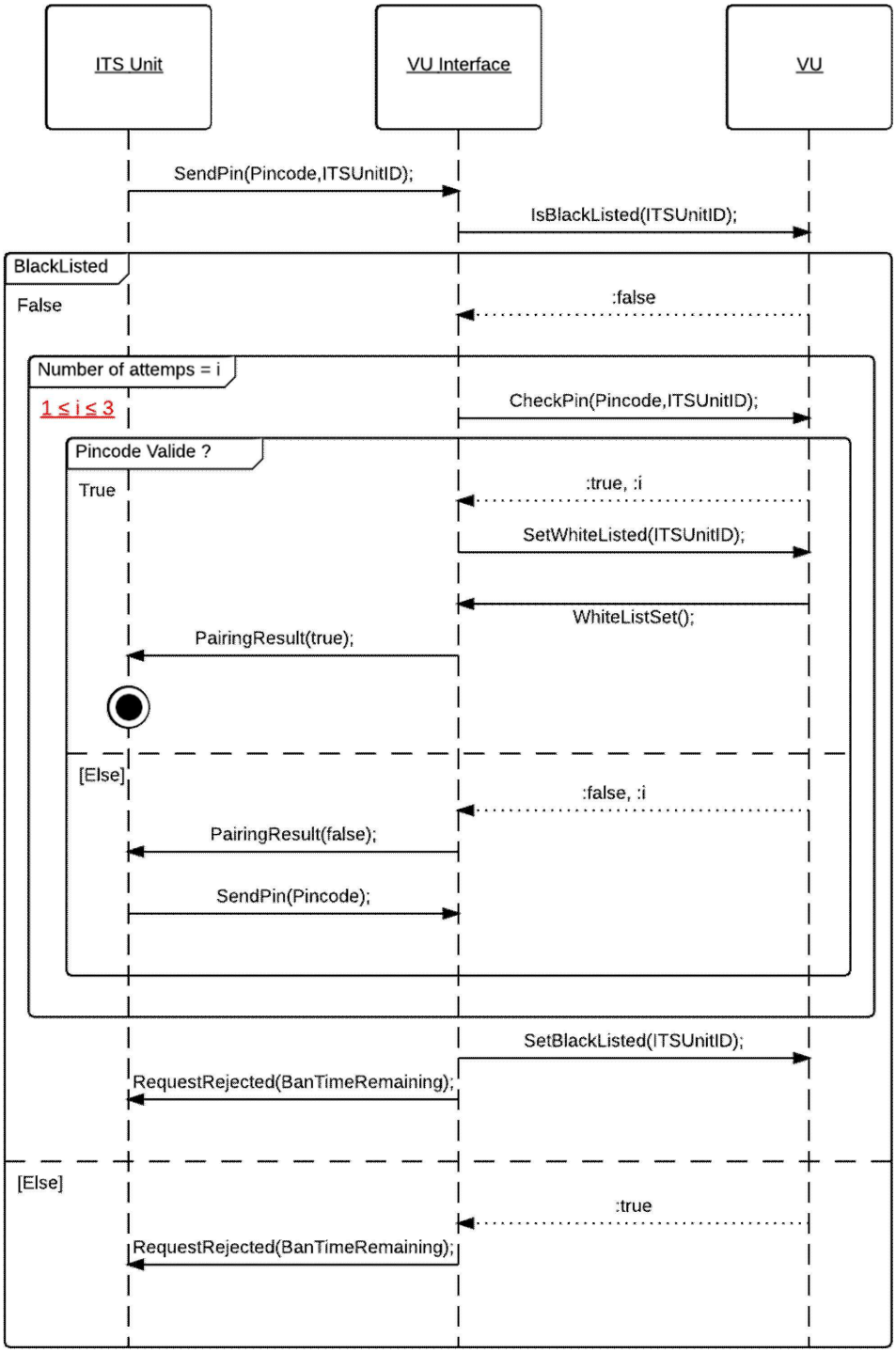
Udalosť alebo porucha	Pravidlá uloženia	Údaje, ktoré sa zaznamenajú o každej udalosti
Určí výrobca	Určí výrobca	Určí výrobca

PRÍLOHA 2

SEKVENČNÉ DIAGRAMY VÝMENY SPRÁV S JEDNOTKOU ITS

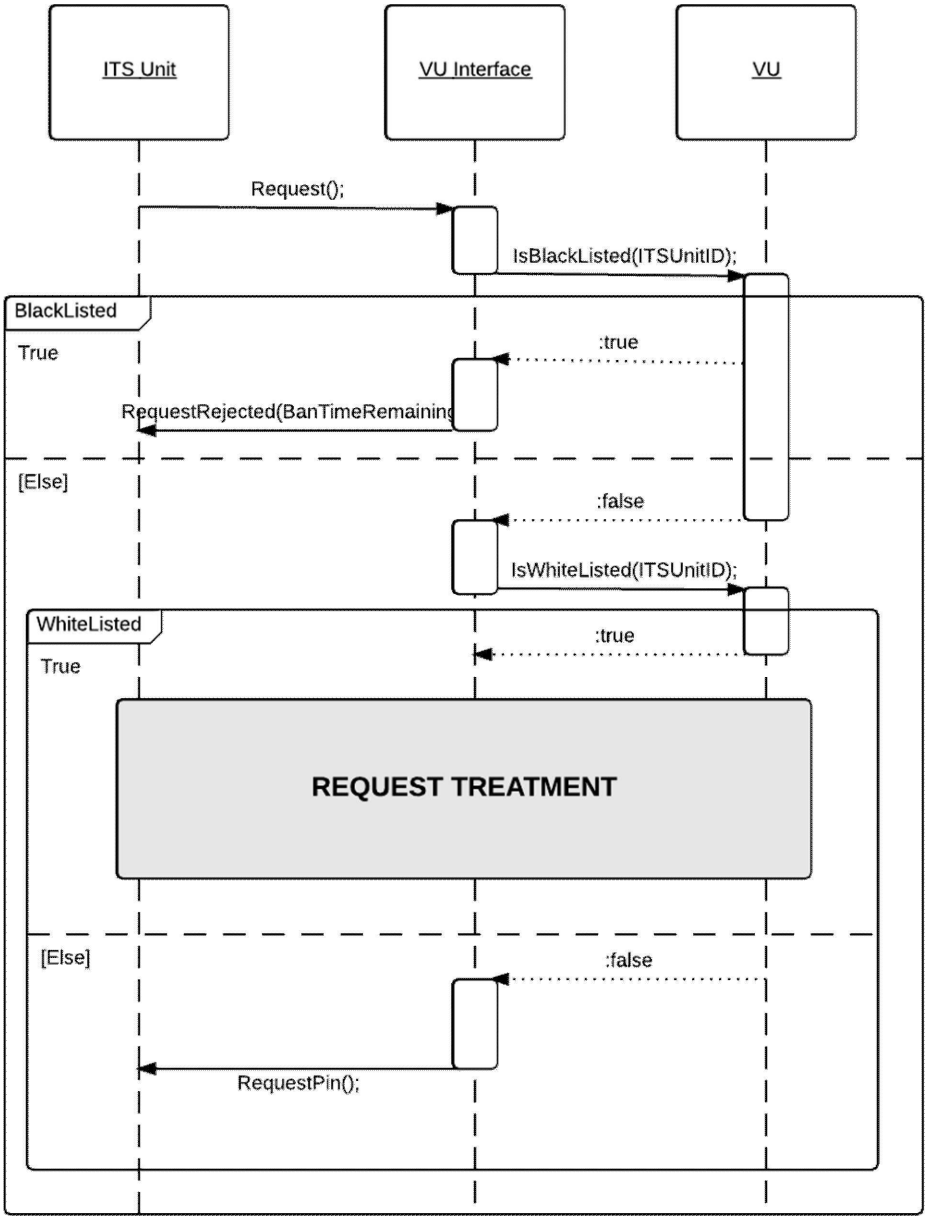
Obrázok 1

Sekvenčný diagram pokusu o potvrdenie platnosti PIN kódu



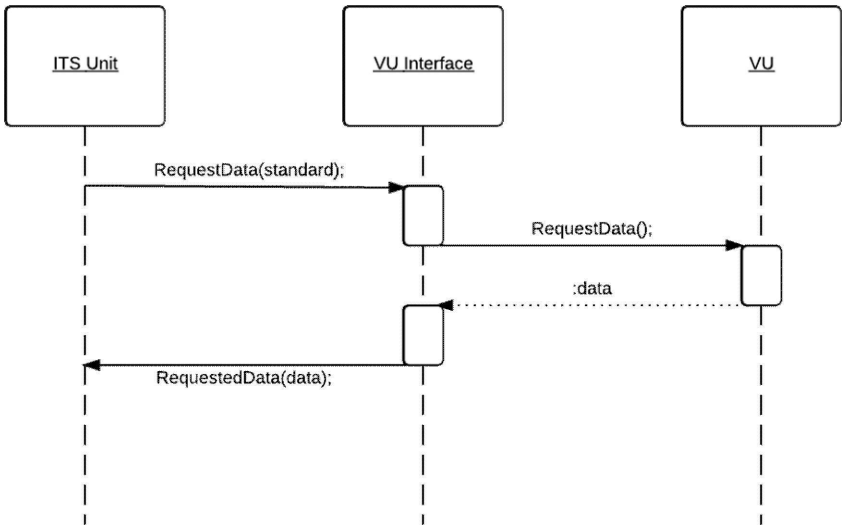
Obrázok 2

Sekvenčný diagram overovania platnosti povolenia jednotky ITS



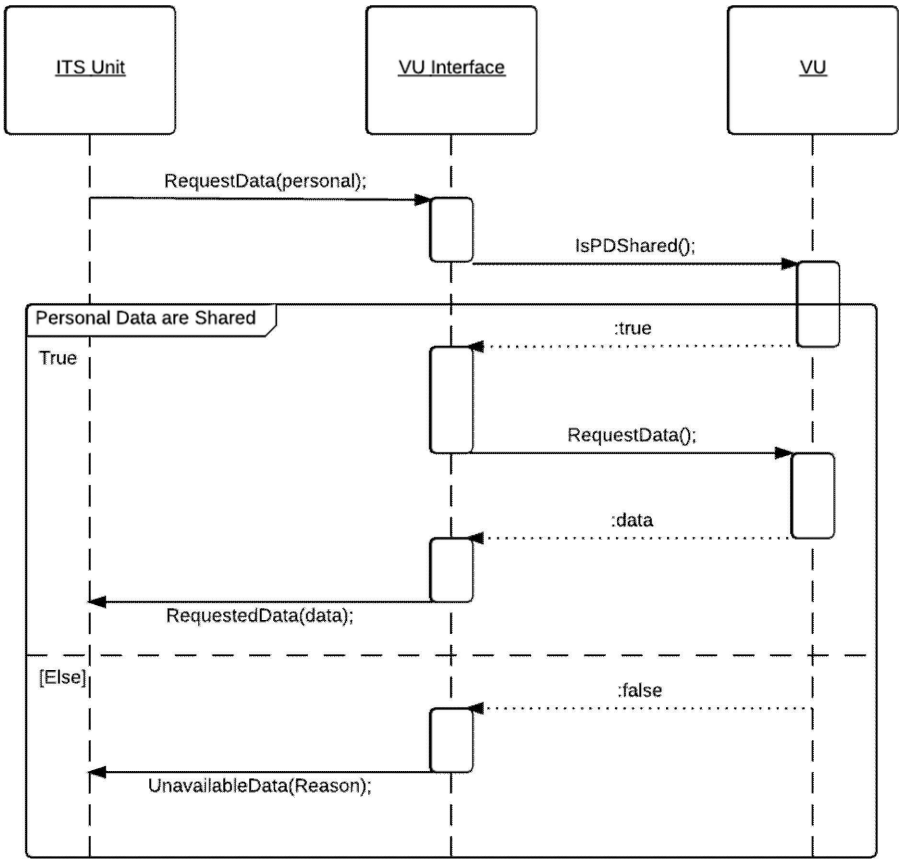
Obrázok 3

Sekvenčný diagram spracovania požiadavky na údaje klasifikované ako nie osobné (po zadaní správneho PIN kódu)



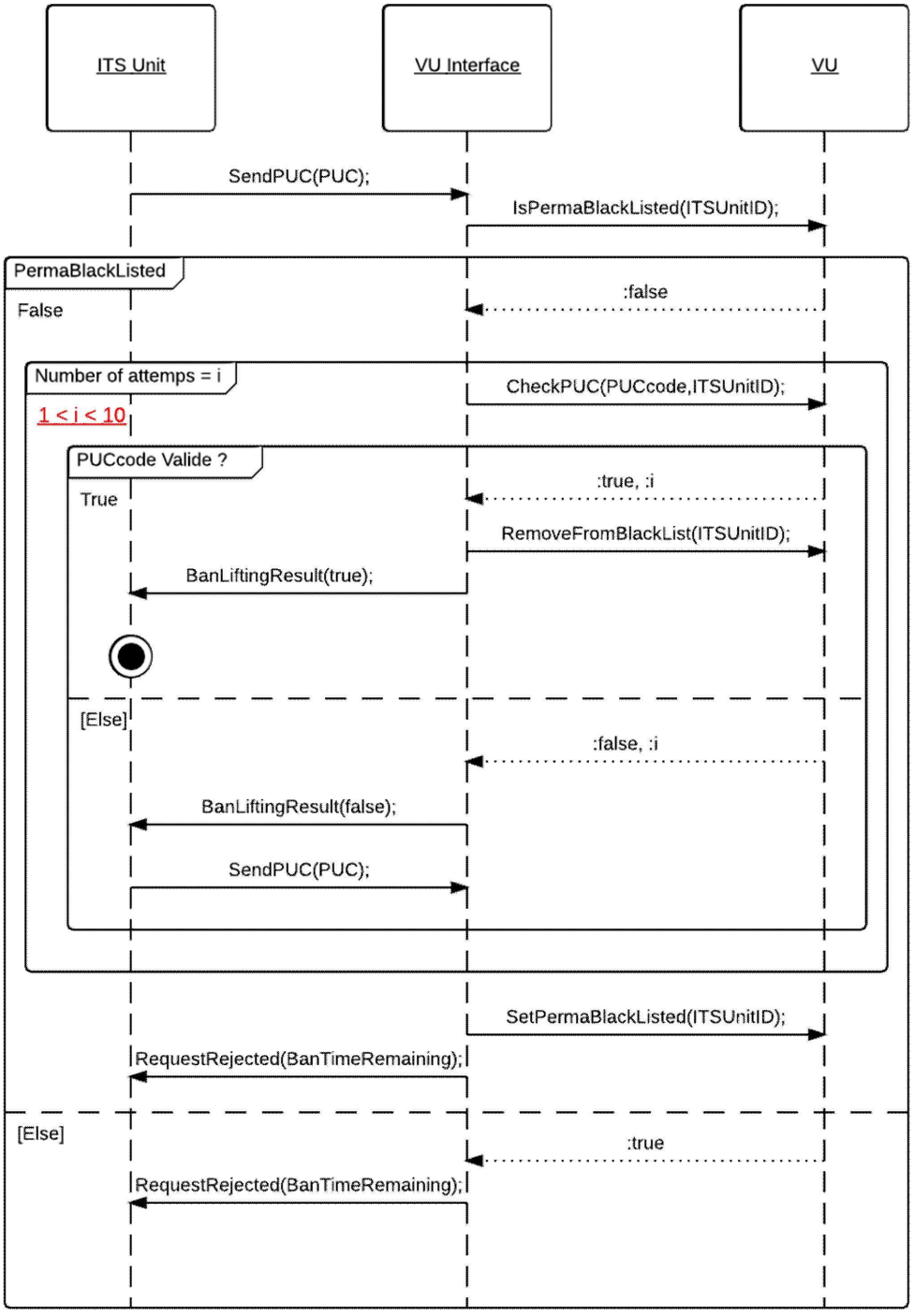
Obrázok 4

Sekvenčný diagram spracovania požiadavky na údaje klasifikované ako osobné (po zadaní správneho PIN kódu)



Obrázok 5

Sekvenčný diagram pokusu o potvrdenie platnosti PUC kódu



PRÍLOHA 3

ŠPECIFIKÁCIE 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
```

Dodatok 14

FUNKCIA DIAĽKOVEJ KOMUNIKÁCIE

OBSAH

1 ÚVOD ... 450

2 ROZSAH PÔSOBNOSTI ... 451

3 SKRATKY, VYMEDZENIA POJMOV A NOTÁCIE ... 452

4 PREVÁDZKOVÉ SCENÁRE ... 454

4.1 Prehľad ... 454

4.1.1 Predpoklady na prenos údajov prostredníctvom rozhrania DSRC 5,8 GHz ... 454

4.1.2 Profil 1a: prostredníctvom ručného snímača komunikačného zariadenia na diaľkovú včasnú detekciu alebo snímača dočasne inštalovaného a zacieleného pri ceste ... 455

4.1.3 Profil 1b: prostredníctvom snímača komunikačného zariadenia na diaľkovú včasnú detekciu (REDCR) inštalovaného a ovládaného vo vozidle ... 456

4.2 Zabezpečenie a integrita ... 456

5 TECHNICKÉ RIEŠENIE A PROTOKOLY DIAĽKOVEJ KOMUNIKÁCIE ... 456

5.1 Technické riešenie ... 456

5.2 Pracovný postup ... 459

5.2.1 Operácie ... 459

5.2.2 Výklad údajov získaných prostredníctvom komunikácie DSRC ... 461

5.3 Parametre fyzického rozhrania DSRC pre diaľkovú komunikáciu ... 461

5.3.1 Obmedzenia na umiestnenie ... 461

5.3.2 Parametre zostupného (downlink) a vzostupného (uplink) prepojenia ... 461

5.3.3 Konštrukcia antény ... 466

5.4 Požiadavky na protokol DSRC pre RTM ... 466

5.4.1 Prehľad ... 466

5.4.2 Príkazy ... 469

5.4.3 Postupnosť príkazov snímania ... 469

5.4.4 Štruktúry údajov ... 470

5.4.5 Prvky RtmData, vykonávané činnosti a vymedzenie pojmov ... 472

5.4.6 Mechanizmus prenosu údajov ... 476

5.4.7 Podrobný opis transakcií DSRC ... 476

5.4.8 Opis skúšobnej transakcie DSRC ... 486

5.5 Podpora smernice 2015/71/ES ... 490

5.5.1 Prehľad ... 490

5.5.2 Príkazy 490

5.5.3 Postupnosť príkazov snímania 490

5.5.4 Štruktúry údajov 490

5.5.5 Modul ASN.1 pre transakciu OWS DSRC 491

5.5.6 Prvky OwsData, vykonávané činnosti a vymedzenie pojmov 492

5.5.7 Mechanizmy prenosu údajov 492

5.6 Prenos údajov medzi DSRC – VU a VU 492

5.6.1 Fyzické prepojenie a rozhrania 492

5.6.2 Aplikačný protokol 493

5.7 Spracovanie chýb 494

5.7.1 Zaznamenávanie a oznamovanie údajov v DSRC – VU 494

5.7.2 Chyby bezdrôtovej komunikácie 494

6 UVEDENIE DO PREVÁDZKY A PRAVIDELNÉ KONTROLNÉ SKÚŠKY FUNKCIE DIAĽKOVEJ KOMUNIKÁCIE 496

6.1 Všeobecné 496

6.2 ECHO 496

6.3 Skúšky na potvrdenie zabezpečeného obsahu údajov 496

1 ÚVOD

V tomto dodatku sú špecifikované technické riešenia a postupy na výkon funkcie diaľkovej komunikácie (ďalej len „komunikácia“), ako sa to požaduje v článku 9 nariadenia (EÚ) č. 165/2014 (ďalej len „nariadenie“).

DSC_1 Podľa nariadenia (EÚ) č. 165/2014 musí byť tachograf vybavený funkciou diaľkovej komunikácie, ktorá umožní zástupcom príslušných kontrolných orgánov snímanie informácií z tachografov prechádzajúcich vozidiel pomocou diaľkového snímacieho zariadenia (snímač komunikačného zariadenia na diaľkovú včasnú detekciu – REDCR), konkrétne snímacieho zariadenia s bezdrôtovým spojením prostredníctvom rozhraní vyhradenej komunikácie krátkeho dosahu (DSRC) CEN 5,8 GHz.

Dôležité je pochopiť, že táto funkcia má slúžiť iba ako predbežný filter pre výber vozidiel na dôkladnejšiu kontrolu a nenahrádza formálny postup inšpekcie podľa ustanovení nariadenia (EÚ) č. 165/2014. V odôvodnení 9 tohto nariadenia sa uvádza, že diaľková komunikácia medzi tachografom a kontrolnými orgánmi na účely cestnej kontroly uľahčuje cielené cestné kontroly.

DSC_2 *Údaje* sa vymieňajú *komunikáciou*, ktorá predstavuje bezdrôtový styk s použitím bezdrôtovej komunikácie DSRC 5,8 GHz v súlade s týmto dodatkom a testovaných porovnávaním s príslušnými parametrami normy 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 *Komunikácia* s komunikačným zariadením sa nadviaže iba po vyslaní požiadavky zo zariadenia príslušného kontrolného orgánu s použitím rádiokomunikačných prostriedkov spĺňajúcich príslušné požiadavky (*snímač komunikačného zariadenia na diaľkovú včasnú detekciu (REDCR)*).

DSC_4 *Údaje* musia byť zabezpečené, aby zaručovali integritu.

DSC_5 Prístup k preneseným *údajom* majú iba príslušné kontrolné orgány oprávnené kontrolovať porušovanie nariadenia (ES) č. 561/2006 a nariadenia (EÚ) č. 165/2014 a dielne, pokiaľ je to potrebné na overenie správneho fungovania tachografu.

DSC_6 V rámci *komunikácie* sa vymieňajú iba *údaje* potrebné na cielenie cestných kontrol vozidiel s potenciálne zmanipulovaným alebo zneužitým tachografom.

DSC_7 Integrita a zabezpečenie *údajov* sa dosahuje zabezpečením *údajov* v jednotke vozidla (VU) a prenášaním iba zabezpečených obsahových *údajov* a údajov týkajúcich sa zabezpečenia (pozri 5.4.4) prostredníctvom média diaľkovej komunikácie DSRC 5,8 GHz, čo znamená, že iba oprávnené osoby z príslušných kontrolných orgánov majú prostriedky na preskúmanie údajov prenesených v rámci *komunikácie* a na overenie ich antenticity. Pozri dodatok 11 Spoločné mechanizmy zabezpečenia.

DSC_8 *Údaje* musia obsahovať časovú pečiatku udávajúcu čas ich poslednej aktualizácie.

DSC_9 S obsahom bezpečnostných údajov môžu byť oboznámené iba príslušné kontrolné orgány v rámci kontroly a strany, s ktorými si tieto orgány vymieňajú dané informácie, a netýkajú sa ho ustanovenia pre *komunikáciu* uvedené v tomto dodatku, s výnimkou prípadu, keď sa v ustanovení pre *komunikáciu* požaduje prenos balíka bezpečnostných údajov s každým balíkom obsahových údajov.

DSC_10 Rovnaká architektúra a zariadenie sa musí dať použiť na získavanie údajov v rámci iných koncepcií (napríklad palubné váženie), s použitím štruktúry stanovenej v tomto dodatku.

DSC_11 Na spresnenie, v súlade s ustanoveniami nariadenia (EÚ) č. 165/2014 (článok 7), sa v rámci *komunikácie* neprenášajú údaje týkajúce sa totožnosti vodiča.

2 ROZSAH PÔSOBNOSTI

Týmto dodatkom sa určuje, ako zástupcovia príslušných kontrolných orgánov používajú špecifikovanú bezdrôtovú komunikáciu DSRC 5,8 GHz na diaľkové získavanie údajov z cieľového vozidla, na základe ktorých sa môže zistiť, že cieľové vozidlo potenciálne porušuje nariadenie (EÚ) č. 165/2014 a malo by sa zvážiť jeho zastavenie na účely ďalšieho preskúmania (ďalej len „*údaje*“).

V nariadení (EÚ) č. 165/2014 sa požaduje, aby sa zber údajov obmedzil len na tie údaje, na základe ktorých sa môže zistiť potenciálne porušenie v zmysle článku 9 nariadenia (EÚ) č. 165/2014.

V rámci tohto scenára je čas určený na komunikáciu obmedzený, pretože *komunikácia* je cielená a má krátky dosah. Príslušné kontrolné orgány môžu komunikačné prostriedky určené na diaľkové monitorovanie tachografu (RTM) používať aj na iné účely (napríklad v súvislosti s maximálnou hmotnosťou a rozmermi ťažkých nákladných vozidiel podľa smernice 2015/719/EÚ), pričom takéto operácie sa môžu vykonávať samostatne alebo nadväzne, podľa rozhodnutia príslušných kontrolných orgánov.

V tomto dodatku sú špecifikované:

— komunikačné zariadenia, postupy a protokoly, ktoré sa musia používať na *komunikáciu*,

— normy a právne predpisy, ktoré musia spĺňať rádiokomunikačné zariadenia,

— prezentácia *údajov komunikačnému* zariadeniu,

— postupy dopytu a sťahovania a postupnosť operácií,

— *údaje*, ktoré sa majú prenášať,

— potenciálny výklad významu *údajov* prenášaných v rámci *komunikácie*,

— ustanovenia o bezpečnostných údajoch v rámci *komunikácie*,

— dostupnosť *údajov* príslušným kontrolným orgánom,

— ako môže *snímač komunikačného zariadenia na diaľkovú včasnú detekciu* požadovať rôzne koncepcie údajov o náklade a vozovom parku.

Na spresnenie, v tomto dodatku nie sú špecifikované:

— vykonávanie a riadenie získavania *údajov* v rámci VU (ktoré vyplynie z technického riešenia produktov, ak sa na inom mieste v nariadení (EÚ) č. 165/2014 nestanovuje inak),

— forma prezentácie získaných údajov zástupcom príslušných kontrolných orgánov, ani kritériá, ktoré používajú príslušné kontrolné orgány pri rozhodovaní o tom, ktoré vozidlo zastaviť (to vyplynie z technického riešenia produktov, ak sa nestanovuje inak na inom mieste v nariadení (EÚ) č. 165/2014 alebo v politickom rozhodnutí príslušných kontrolných orgánov). Na spresnenie: *komunikáciou* sa *údaje* sprístupňujú príslušným kontrolným orgánom, iba aby mohli tieto orgány prijímať informované rozhodnutia,

— opatrenia na zaistenie zabezpečenia údajov (ako je šifrovanie) týkajúce sa obsahu *údajov* (ktoré sa stanovia v dodatku 11 Spoločné mechanizmy zabezpečenia).

— podrobnosti o prípadných iných koncepciách údajov než RTM, ktoré sa dajú získať s použitím rovnakej architektúry a zariadenia,

— podrobnosti správania a riadenia medzi VU a DSRC – VU, ani správania v rámci DSRC – VU (okrem poskytovania *údajov* na základe požiadavky zo snímača REDCR).

3 SKRATKY, VYMEDZENIA POJMOV A NOTÁCIE

V tomto dodatku sa používajú tieto osobitné skratky a vymedzenia pojmov:

anténa	elektrické zariadenie, ktoré premieňa elektrickú energiu na rádiové vlny a naopak, pričom sa používa v kombinácii s rádiovým vysielačom alebo prijímačom. Počas prevádzky rádiový vysielač dodáva elektrický prúd kmitajúci s rádiovou frekvenciou na svorky antény a anténa vyžaruje energiu z tohto prúdu ako elektromagnetické vlny (rádiové vlny). Pri prijímaní signálu anténa zachytáva určitú časť energie elektromagnetickej vlny a na jej svorkách tým vzniká nízke napätie, ktoré sa zosilňuje v prijímači,
komunikácia	výmena informácií/údajov medzi DSRC – REDCR a DSRC – VU vo vzťahu master/slave (hlavná/podriadená jednotka) podľa oddielu 5 na účely získania údajov,
údaje	zabezpečené údaje stanoveného formátu (pozri 5.4.4), o ktoré požiadal snímač *DSRC – REDCR* a ktoré mu boli poskytnuté z jednotky *DSRC – VU* spojením DSRC 5,8 GHz podľa oddielu 5 nižšie,
nariadenie (EÚ) č. 165/2014	nariadenie Európskeho parlamentu a Rady (EÚ) č. 165/2014 zo 4. februára 2014 o tachografoch v cestnej doprave, ktorým sa ruší nariadenie Rady (EHS) č. 3821/85 o záznamovom zariadení v cestnej doprave a mení nariadenie Európskeho parlamentu a Rady (ES) č. 561/2006 o harmonizácii niektorých právnych predpisov v sociálnej oblasti, ktoré sa týkajú cestnej dopravy,
AID	Application Identifier (identifikátor aplikácie)
BLE	Bluetooth Low Energy (nízkoenergetický systém Bluetooth)
BST	Beacon Service Table (tabuľka prevádzkových režimov majáka)

CIWD	Card insertion while driving (vloženie karty počas jazdy)
CRC	cyclic redundancy check (kontrola cyklickým kódom)
DSC (n)	identifikátor požiadavky na osobitný dodatok k DSRC
DSRC	Dedicated Short Range Communication (vyhradená komunikácia krátkeho dosahu)
DSRC-REDCR	DSRC – Remote Early Detection Communication Reader (snímač komunikačného zariadenia na diaľkovú včasnú detekciu)
DSRC-VU	DSRC – Vehicle Unit (jednotka vozidla). Ide o „zariadenie na diaľkovú včasnú detekciu“ vymedzené v prílohe 1C.
DWVC	Driving without valid card (jazda bez platnej karty)
EID	Element Identifier (identifikátor prvku)
LLC	Logical Link Control (riadenie logického spojenia)
LPDU	LLC Protocol Data Unit (protokolová dátová jednotka LLC)
OWS	Onboard Weighing System (palubný vážiaci systém)
PDU	Protocol Data Unit (protokolová dátová jednotka)
REDCR	Remote early detection communication reader (snímač komunikačného zariadenia na diaľkovú včasnú detekciu). Ide o „snímač komunikačného zariadenia na diaľkovú včasnú detekciu“ vymedzený v prílohe 1C
RTM	Remote Tachograph Monitoring (diaľkové monitorovanie tachografu)
SM-REDCR	Security Module – Remote early detection communication reader (modul zabezpečenia – snímač komunikačného zariadenia na diaľkovú včasnú detekciu)
TARV	Telematics Applications for Regulated Vehicles (telematické aplikácie pre regulované vozidlá) (súbor noriem ISO 15638)
VU	Vehicle Unit (jednotka vozidla)
VUPM	Vehicle Unit Payload Memory (pamäť jednotky vozidla pre obsahové údaje)
VUSM	Vehicle Unit Security Module (modul zabezpečenia jednotky vozidla)
VST	Vehicle Service Table (tabuľka jednotky vozidla)
WIM	Weigh in motion (váženie za pohybu)
WOB	Weigh on board (palubné váženie)

Špecifikácia uvedená v tomto dodatku odkazuje na nasledujúce nariadenia a normy alebo ich časti a vychádza z nich. V ustanoveniach tohto dodatku sú uvedené príslušné normy alebo ich príslušné časti. V prípade akýchkoľvek nezrovnalostí majú prednosť ustanovenia tohto dodatku. V prípade akýchkoľvek nezrovnalostí, ak v tomto dodatku nie je jednoznačne určená žiadna špecifikácia, prednosť má prevádzka podľa normy ERC 70-03 (overí sa porovnaním s príslušnými parametrami normy EN 300 674-1) a ďalej v zostupnom poradí podľa noriem EN 12795, EN 12253 EN 12834 a EN 13372, 6.2, 6.3, 6.4 a 7.1.

V dodatku sa odkazuje na tieto nariadenia a normy:

1. Nariadenie Európskeho parlamentu a Rady (EÚ) č. 165/2014 zo 4. februára 2014 o tachografoch v cestnej doprave, ktorým sa ruší nariadenie Rady (EHS) č. 3821/85 o záznamovom zariadení v cestnej doprave a mení nariadenie Európskeho parlamentu a Rady (ES) č. 561/2006 o harmonizácii niektorých právnych predpisov v sociálnej oblasti, ktoré sa týkajú cestnej dopravy.

2. Nariadenie Európskeho parlamentu a Rady (ES) č. 561/2006 z 15. marca 2006 o harmonizácii niektorých právnych predpisov v sociálnej oblasti, ktoré sa týkajú cestnej dopravy, ktorým sa menia a dopĺňajú nariadenia Rady (EHS) č. 3821/85 a (ES) č. 2135/98 a zrušuje nariadenie Rady (EHS) č. 3820/85 (Text s významom pre EHP).

3. ERC 70-03 CEPT: odporúčanie ECC 70-03: týkajúce sa používania zariadení s krátkym dosahom.

4. ISO 15638 Inteligentné dopravné systémy – Rámec pre kooperatívne telematické aplikácie pre reguláciu komerčných nákladných vozidiel (TARV).

5. EN 300 674-1 Elektromagnetická kompatibilita a záležitosti rádiového spektra (ERM), Telematika v cestnej doprave a prevádzke (RTTT), Vysielacie zariadenia účelových komunikácií na krátku vzdialenosť (DSRC) (500 kbit/s, 250 kbit/s) pracujúce v pásme ISM 5,8 GHz pre priemyselné, vedecké a zdravotnícke zariadenia, časť 1: Všeobecné charakteristiky a skúšobné metódy pre cestné jednotky (RSU) a palubné jednotky (OBU).

6. EN 12253 Telematika v cestnej doprave a preprave. Vyhradená komunikácia krátkeho dosahu pomocou majákového vozidla. Fyzikálna úroveň na báze nosiča 5,8 GHz.

7. EN 12795 Telematika v cestnej doprave a preprave. Jednoúčelová komunikácia s krátkym dosahom. Vrstva údajového spojenia. Stredný prístup a kontrola logického spojenia.

8. EN 12834 Telematika v cestnej doprave a preprave. Jednoúčelová komunikácia s krátkym dosahom. Aplikačná úroveň.

9. EN 13372 Telematika v cestnej doprave a preprave. Vyhradená komunikácia krátkeho dosahu. Profily na použitie v RTTT.

10. ISO 14906 Elektronické zhromažďovanie poplatkov. Stanovenie použiteľných rozhraní pre vyhradenú komunikáciu krátkeho dosahu.

4 PREVÁDZKOVÉ SCENÁRE

4.1 **Prehľad**

V nariadení (EÚ) č. 165/2014 sú stanovené konkrétne a kontrolované scenáre, v rámci ktorých sa má používať *komunikácia*.

Podporované sú tieto scenáre:

„Komunikačný profil č. 1: Cestná kontrola, pri ktorej sa používa bezdrôtová komunikácia krátkeho dosahu prostredníctvom snímača komunikačného zariadenia na diaľkovú včasnú detekciu a ktorá je podnetom na fyzickú cestnú kontrolu (master/slave – hlavná/podriadená jednotka)

Profil snímača 1a: prostredníctvom ručného snímača komunikačného zariadenia na diaľkovú včasnú detekciu alebo snímača dočasne inštalovaného a zacieleného pri ceste

Profil snímača 1b: prostredníctvom snímača komunikačného zariadenia na diaľkovú včasnú detekciu inštalovaného a ovládaného vo vozidle“.

4.1.1 *Predpoklady na prenos údajov prostredníctvom rozhrania DSRC 5,8 GHz*

POZNÁMKA: Pre pochopenie kontextu predpokladov pozri obrázok 14.3.

4.1.1.1 Údaje uchovávané vo VU

DSC_12 VU zodpovedá za aktualizáciu údajov každých 60 sekúnd a ich uchovávanie vo VU bez akéhokoľvek zásahu komunikačnej funkcie DSRC. Prostriedky, ktorými sa to dosahuje, závisia od VU, sú stanovené v nariadení (EÚ) č. 165/2014, prílohe 1 C, oddiele 3.19 „*Diaľková komunikácia pre cielené cestné kontroly*“ a nestanovujú sa v tomto dodatku.

4.1.1.2 Údaje poskytované zariadeniu DSRC – VU

DSC_13 VU zodpovedá za aktualizáciu údajov DSRC tachografu (*údaje*) pri každej aktualizácii údajov uložených vo VU v intervale stanovenom v bode 4.1.1.1 (DSC_12), bez akéhokoľvek zásahu komunikačnej funkcie DSRC.

DSC_14 Údaje VU sa používajú ako základ pre zhromažďovanie a aktualizáciu *údajov*, pričom prostriedky, ktorými sa to dosahuje, sú stanovené v prílohe 1 C, oddiele 3.19 *„Diaľková komunikácia pre cielené cestné kontroly“*, alebo ak neexistuje žiadna taká špecifikácia, vyplývajú z technického riešenia zariadenia a nestanovujú sa v tomto dodatku. Technické riešenie prepojenia medzi zariadením DSRC – VU a VU je uvedené v oddiele 5.6.

4.1.1.3 Obsah údajov

DSC_15 Obsah a formát *údajov* musia byť také, aby po dekódovaní boli štruktúrované a sprístupnené vo forme a formáte podľa bodu 5.4.4 tohto dodatku (Štruktúry údajov).

4.1.1.4 Prezentácia údajov

DSC_16 *Údaje*, ktoré sa v súlade s postupmi stanovenými v bode 4.1.1.1 často aktualizujú, sa pred prezentáciou zariadeniu *DSRC – VU* zabezpečia a prezentujú sa ako zabezpečená hodnota koncepcie údajov na dočasné uloženie v *DSRC – VU* ako aktuálna verzia *údajov*. Tieto údaje sa prenášajú z modulu *VUSM* do pamäte *VUPM* ako funkcie DSRC. *VUSM* a *VUPM* sú funkcie a nemusia nevyhnutne byť fyzickými objektmi. Forma fyzickej konkretizácie vykonávania týchto funkcií je vecou technického riešenia zariadenia, pokiaľ sa nešpecifikuje na inom mieste v nariadení (EÚ) č. 165/2014.

4.1.1.5 Bezpečnostné údaje

DSC_17 Bezpečnostné údaje (*securityData*), ktoré predstavujú údaje požadované snímačom *REDCR* na doplnenie jeho schopnosti dešifrovať *údaje*, sa dodajú v súlade s dodatkom 11 Spoločné mechanizmy zabezpečenia a prezentujú sa ako hodnota koncepcie údajov na dočasné uloženie v *DSRC – VU* ako aktuálna verzia *securityData* vo forme stanovenej v odseku 5.4.4 tohto dodatku.

4.1.1.6 Údaje VUPM dostupné na prenos prostredníctvom rozhrania DSRC

DSC_18 Koncepcia údajov, ktorá musí byť vždy dostupná v pamäti VUPM ako funkcii DSRC na okamžitý prenos na základe požiadavky snímača *REDCR*, je stanovená v odseku 5.4.4 pre úplné špecifikácie modulu ASN.1.

Všeobecný prehľad komunikačného profilu 1

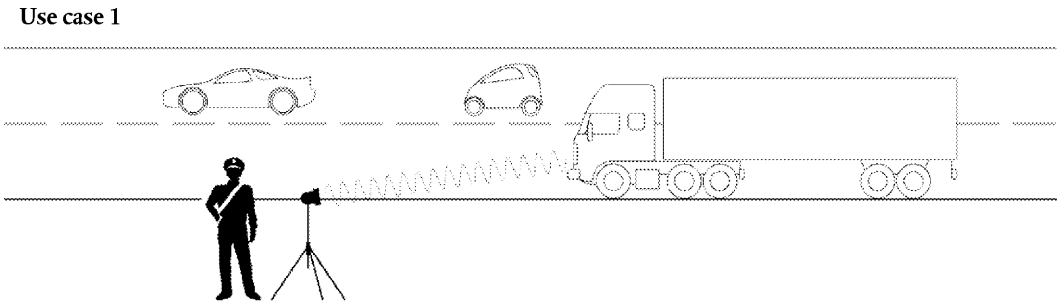
Tento profil zahŕňa prípad použitia, keď zástupca príslušného kontrolného orgánu používa diaľkovú komunikáciu krátkeho dosahu prostredníctvom snímača komunikačného zariadenia na diaľkovú včasnú detekciu (rozhrania DSRC 5,8 GHz pracujúce v súlade s odporúčaním ERC 70-03 a testované porovnávaním s príslušnými parametrami normy EN 300 674-1 v súlade s oddielom 5) (*REDCR*) na diaľkovú identifikáciu vozidla, ktoré potenciálne porušuje nariadenie (EÚ) č. 165/2014. Zástupca príslušného kontrolného orgánu, ktorý riadi snímanie, po identifikácii rozhodne, či by sa vozidlo malo zastaviť.

4.1.2 *Profil 1a: prostredníctvom ručného snímača komunikačného zariadenia na diaľkovú včasnú detekciu alebo snímača dočasne inštalovaného a zacieleného pri ceste*

V tomto prípade použitia sa zástupca príslušného kontrolného orgánu nachádza pri ceste a zacieli ručný, stojanový alebo iný prenosný snímač *REDCR* z okraja cesty na stred čelného skla cieľového vozidla. Snímanie sa vykonáva prostredníctvom rozhraní DSRC 5,8 GHz pracujúcich v súlade s odporúčaním ERC 70-03 a testovaných porovnávaním s príslušnými parametrami normy EN 300 674-1 v súlade s odsekom 5. Pozri obrázok 14.1 (prípad použitia 1).

Obrázok 14.1

Snímanie z okraja cesty prostredníctvom DSRC 5,8 GHz



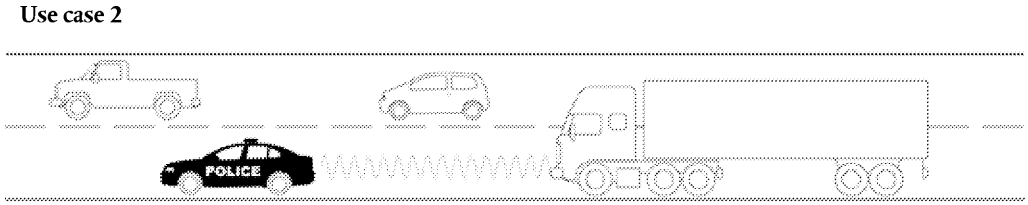
REDCR pri ceste

4.1.3 *Profil 1b: prostredníctvom snímača komunikačného zariadenia na diaľkovú včasnú detekciu (REDCR) inštalovaného a ovládaného vo vozidle*

V tomto prípade použitia sa zástupca príslušného kontrolného orgánu nachádza v pohybujúcom sa vozidle a buď zacieli prenosný ručný snímač *REDCR* z vozidla na stred čelného skla cieľového vozidla, alebo je snímač *REDCR* upevnený vo vozidle, prípadne na ňom tak, aby bol zacielený na stred čelného skla cieľového vozidla, keď je vozidlo so snímačom komunikačného zariadenia na diaľkovú včasnú detekciu v určitej pozícii voči cieľovému vozidlu (napríklad priamo pred ním v dopravnom prúde). Snímanie sa vykonáva prostredníctvom rozhraní DSRC 5,8 GHz pracujúcich v súlade s odporúčaním ERC 70-03 a testovaných porovnávaním s príslušnými parametrami normy EN 300 674-1 v súlade s odsekom 5. Pozri obrázok 14.2 (prípad použitia 2).

Obrázok 14.2

Snímanie z vozidla prostredníctvom DSRC 5,8 GHz



Mobilný REDCR

4.2 **Zabezpečenie a integrita**

Aby bolo možné overiť autenticitu a integritu údajov sťahovaných prostredníctvom diaľkovej komunikácie, zabezpečené *údaje* sa overujú a dekódujú v súlade s dodatkom 11 Spoločné mechanizmy zabezpečenia.

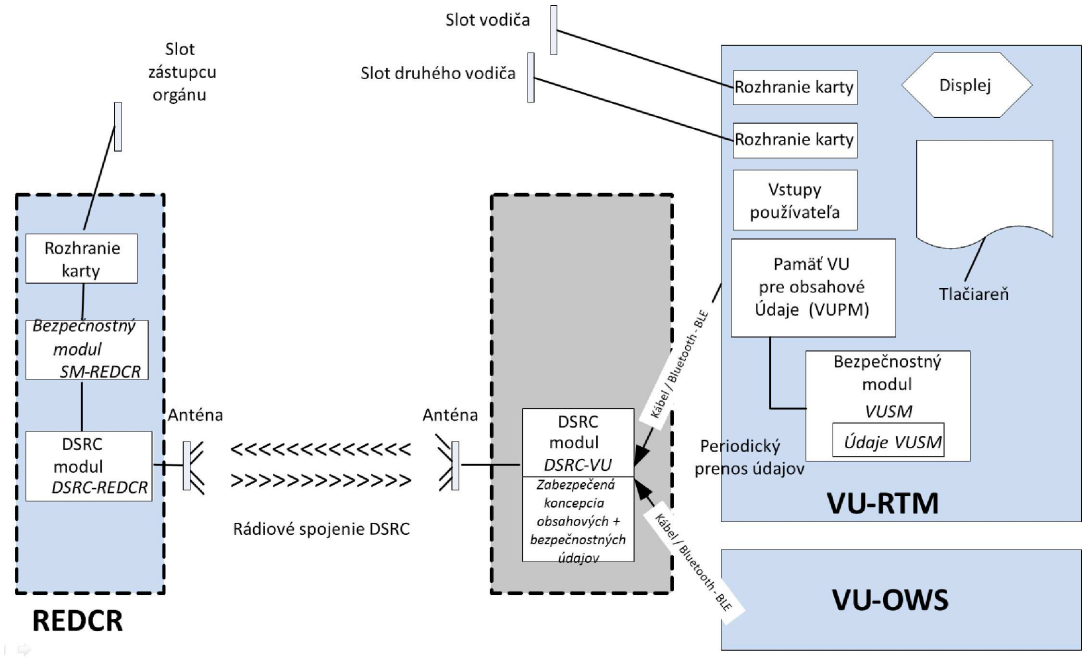
5 TECHNICKÉ RIEŠENIE A PROTOKOLY DIAĽKOVEJ KOMUNIKÁCIE

5.1 **Technické riešenie**

Technické riešenie funkcie diaľkovej komunikácie inteligentného tachografu je znázornené na obrázku 14.3.

Obrázok 14.3

Technické riešenie funkcie diaľkovej komunikácie



DSC_19 Vo VU sú umiestnené tieto funkcie:

— Modul zabezpečenia (*VUSM*). Táto funkcia vo VU je zodpovedná za zabezpečenie *údajov*, ktoré sa majú prostredníctvom diaľkovej komunikácie prenášať z DSRC – VU k zástupcovi príslušného kontrolného orgánu.

— Zabezpečené údaje sa uchovávajú v pamäti VUSM. V intervaloch stanovených v bode 4.1.1.1 (DSC_12) VU kóduje a dopĺňa údaje v rámci koncepcie RTMdata (ktorá zahŕňa hodnoty koncepcie obsahových a bezpečnostných údajov určené v ďalšej časti tohto dodatku) uchovávané v pamäti DSRC – VU. Prevádzka modulu zabezpečenia je vymedzená dodatku 11 Spoločné mechanizmy zabezpečenia a je mimo rozsahu pôsobnosti tohto dodatku – s výnimkou požiadavky poskytovať aktualizáciu komunikačnému zariadeniu VU pri každej zmene údajov v module VUSM.

— Komunikácia medzi VU a DSRC – VU môže mať podobu drôtovej komunikácie alebo komunikácie prostredníctvom nízkoenergetického systému Bluetooth (BLE) a zariadenie DSRC – VU môže byť fyzicky umiestnené ako integrálna súčasť antény na čelnom skle vozidla, vo vnútri VU alebo niekde medzi týmito polohami.

— Zariadenie DSRC – VU musí mať neustále k dispozícii spoľahlivý zdroj napájania. Spôsob napájania je otázkou technického riešenia.

— Zariadenie DSRC – VU musí byť vybavené stálou energeticky nezávislou pamäťou, aby sa údaje v DSRC – VU zachovali, aj keď je zapaľovanie vozidla vypnuté.

— Ak sa komunikácia medzi VU a DSRC – VU vykonáva prostredníctvom systému BLE a napájacím zdrojom je nenabíjateľná batéria, napájací zdroj DRSC – VU sa musí vymeniť pri každej pravidelnej inšpekcii a výrobca zariadenia DSRC – VU je zodpovedný za zaistenie vhodného napájacieho zdroja, ktorý vydrží od jednej pravidelnej inšpekcie do ďalšej, aby tak mal snímač REDCR počas celého uvedeného obdobia zabezpečený normálny prístup k údajom bez zlyhania alebo prerušenia.

— Zariadenie VU RTM „obsahová pamäť“ (*VUPM*). Táto funkcia vo VU je zodpovedná za poskytovanie a aktualizáciu *údajov*. Obsah *údajov*. („TachographPayload“) je vymedzený nižšie v odsekoch 5.4.4 a 5.4.5 a aktualizuje sa v intervale stanovenom v bode 4.1.1.1 (DSC_12).

— DSRC – VU. Ide o funkciu zariadenia, ktoré je súčasťou antény alebo je k nej pripojené a komunikuje s VU prostredníctvom drôtového alebo bezdrôtového (BLE) pripojenia, sú v ňom uložené aktuálne údaje (*VUPM-data*) a riadi odpoveď na snímanie prostredníctvom média DSRC 5,8 GHz. Odpojenie zariadenia DRSC alebo manipulovanie jeho funkčnosti počas bežnej prevádzky vozidla sa považuje za porušenie nariadenia (EÚ) č. 165/2014.

— Modul zabezpečenia (REDCR) (SM – REDCR) je funkcia, ktorá sa používa na dekódovanie a kontrolu integrity údajov odchádzajúcich z VU. Prostriedky, ktorými sa to dosahuje, sú určené v dodatku 11 – Spoločné mechanizmy zabezpečenia – a nie sú vymedzené v tomto dodatku.

— Zariadenie funkcie DSRC (REDCR) (*DSRC – REDCR*) pozostáva z vysielača/prijímača 5,8 GHz a príslušného firmvéru a softvéru, ktorý riadi *komunikáciu* s *DSRC – VU* podľa tohto dodatku.

— Zariadenie *DSRC – REDCR* sníma *DSRC – VU* cieľového vozidla a prostredníctvom spojenia DSRC získava *údaje* (aktuálne údaje *VUPM-data* cieľového vozidla), ktoré spracováva a ukladá do svojej pamäte *SM – REDCR*.

— Anténa DSRC – VU sa umiestni tak, aby sa optimalizovala komunikácia DSRC medzi vozidlom a anténou na okraji cesty (vo všeobecnosti uprostred alebo blízko stredu čelného skla vozidla …). Pre ľahké vozidlá je vhodná inštalácia vo vrchnej časti čelného skla.

— Pred anténou alebo blízko nej sa nesmú nachádzať žiadne kovové predmety (napr. menovky, nálepky, pásy antireflexných (tónovaných) fólií, slnečné clony, stierače v pokoji), ktoré by mohli rušiť komunikáciu.

— Anténa musí byť upevnená tak, aby jej os bola zhruba rovnobežná s povrchom vozovky.

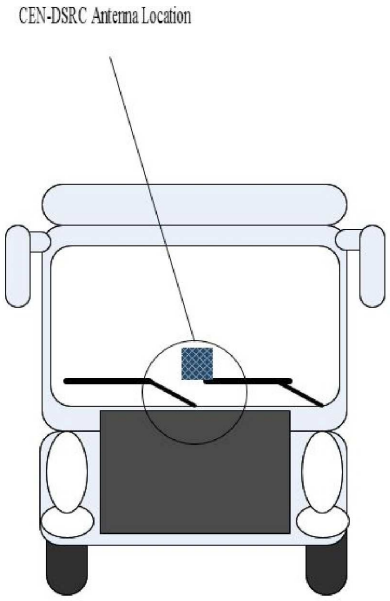
DSC_20 Anténa a komunikácia pracuje v rámci odporúčania ERC 70-03 a testuje sa porovnávaním s príslušnými parametrami normy EN 300 674-1 v súlade s odsekom 5. Anténa a komunikácia môžu uplatňovať techniky na zmiernenie rizika bezdrôtovej intereferencie uvedené v správe ECC 228, napr. pomocou filtrov pri komunikácii CEN DSRC 5.8 GHz.

DSC_21 Anténa DSRC musí byť pripojená k zariadeniu DSRC – VU buď priamo v rámci modulu upevneného na čelné sklo alebo v jeho blízkosti, alebo prostredníctvom vyhradeného kábla skonštruovaného tak, aby sa sťažilo jeho neoprávnené odpojenie. Odpojenie antény alebo manipulovanie jej funkčnosti sa považuje za porušenie nariadenia (EÚ) č. 165/2014. Úmyselné maskovanie alebo iné nežiaduce ovplyvňovanie prevádzkovej výkonnosti antény sa považuje za porušenie nariadenia (EÚ) č. 165/2014.

DSC_22 Tvar antény nie je vymedzený a je otázkou komerčného rozhodnutia, pokiaľ namontované zariadenie DSRC – VU spĺňa požiadavky súladu stanovené v oddiele 5 nižšie. Anténa sa umiestni tak, ako sa uvádza v bode DSC_19 a ako je znázornené na obrázku 14.4 (kružnica) a umožňuje efektívne použitie podľa bodov 4.1.2 a 4.1.3.

Obrázok 14.4

Príklad umiestnenia antény DSRC 5,8 GHz na čelnom skle regulovaných vozidiel



Tvar snímača *REDCR* a jeho antény sa môže meniť podľa podmienok snímania (snímač upevnený na stojane, držaný v ruke, upevnený vo vozidle atď.) a podľa prevádzkového postupu, ktorý používa zástupca príslušného kontrolného orgánu.

Na prezentáciu výsledkov funkcie diaľkovej komunikácie zástupcovi príslušného kontrolného orgánu sa používa funkcia zobrazenia a/alebo upozornenia. Výsledok sa môže zobraziť na monitore, ako tlačený výstup, ako zvukový signál alebo ako ich kombinácia. Forma zobrazenia a/alebo upozornenia je vecou požiadaviek zástupcov príslušných kontrolných orgánov a technického riešenia zariadenia a nie je špecifikovaná v tomto dodatku.

DSC_23 Konštrukcia a tvar snímača *REDCR* sú vecou komerčných návrhov v súlade s odporúčaním ERC 70-03, ako aj s konštrukčnými a prevádzkovými špecifikáciami podľa tohto dodatku (odsek 5.3.2), takže poskytujú trhu maximálnu flexibilitu, aby sa navrhovali a poskytovali zariadenia spĺňajúce osobitné potreby jednotlivých príslušných kontrolných orgánov.

DSC_24 Konštrukcia a tvar zariadenia *DSRC – VU* a jeho umiestnenie vnútri alebo mimo VU sú vecou komerčných návrhov v súlade s odporúčaním ERC 70-03 a s konštrukčnými a prevádzkovými špecifikáciami stanovenými v tomto dodatku (odsek 5.3.2) a v tomto oddiele (5.1).

DSC_25 Zariadenie *DSRC – VU* však musí byť primerane schopné prijímať hodnoty koncepcie údajov od ostatných inteligentných zariadení vozidla prostredníctvom otvorených prepojení a protokolov zodpovedajúcich normám odvetvia (napríklad od zariadenia na palubné váženie), pokiaľ sa takéto koncepcie údajov identifikujú pomocou jedinečných a známych identifikátorov aplikácií alebo názvov súborov; pokyny na používanie takých protokolov musia byť sprístupnené Európskej komisii a bezplatne dostupné výrobcom príslušných zariadení.

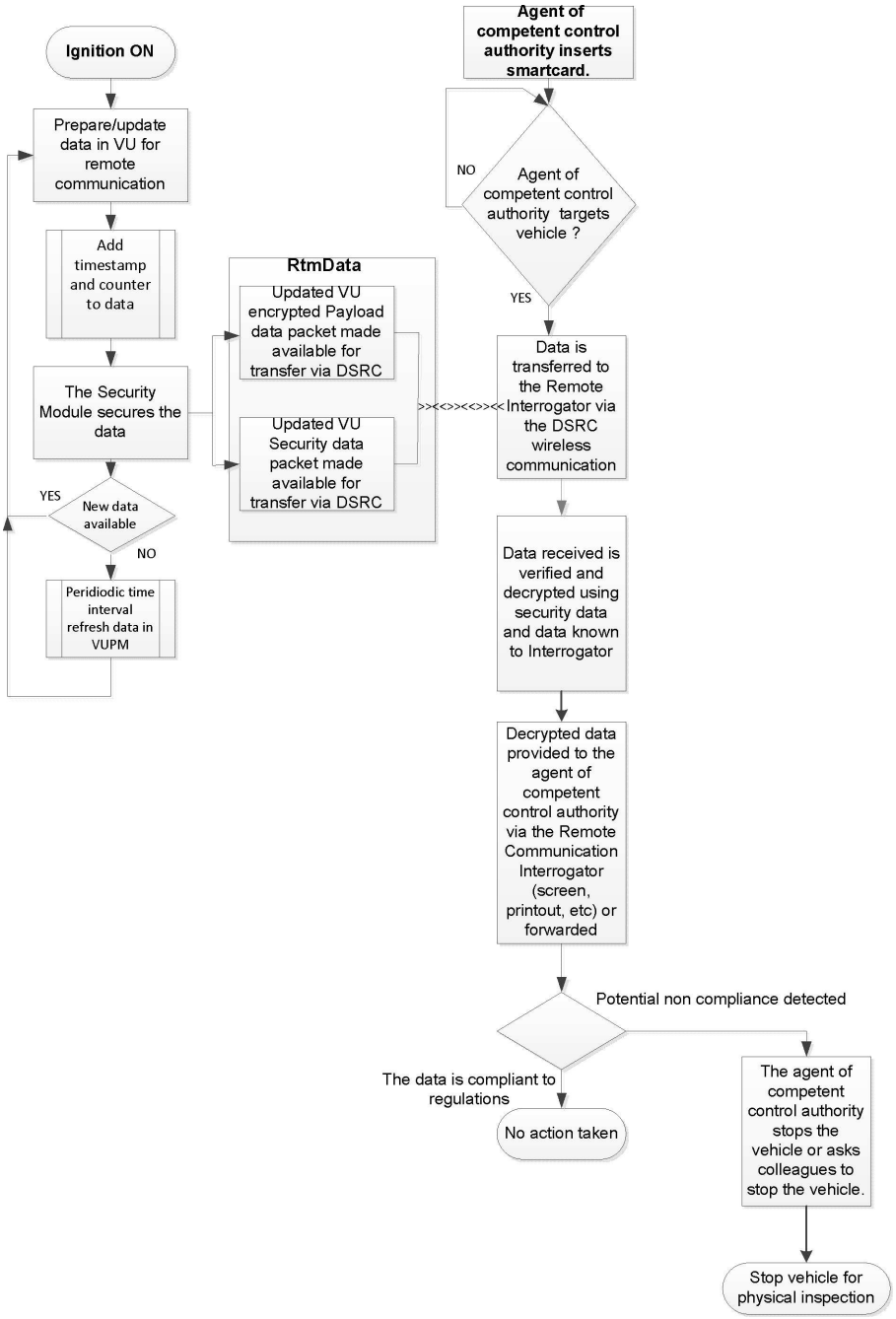
5.2 **Pracovný postup**

5.2.1 *Operácie*

Pracovný postup operácií je znázornený na obrázku 14.5.

Obrázok 14.5

Pracovný postup pre funkciu diaľkovej komunikácie



Tu sú opísané jednotlivé kroky:

a) Keď je vozidlo v prevádzke (zapaľovanie je zapnuté – „ON“), tachograf poskytuje údaje funkcii VU. Funkcia VU pripravuje *údaje* pre funkciu diaľkovej komunikácie (zakódované) a aktualizuje údaje *VUPM* uložené v pamäti zariadenia *DSRC – VU* (ako je stanovené v bodoch 4.1.1.1 a 4.1.1.2). Získané *údaje* sa formátujú podľa odsekov 5.4.4 a 5.4.5.

b) Vždy, keď sa *údaje* aktualizujú, aktualizuje sa aj časová pečiatka uvedená v koncepcii bezpečnostných údajov.

c) Funkciou *VUSM* sa údaje zabezpečujú v súlade s postupmi stanovenými v dodatku 11.

d) Vždy, keď sa *údaje* aktualizujú (pozri body 4.1.1.1 a 4.1.1.2), prenesú sa do zariadenia *DSRC – VU*, kde nahradia všetky predchádzajúce údaje, aby bolo možné zakaždým poskytnúť aktualizované údaje (*údaje*) v prípade ich snímania prostredníctvom snímača *REDCR*. Keď VU poskytuje *údaje* zariadeniu DSRC – VU, je možné ich identifikovať na základe názvu súboru *RTMData* alebo identifikátormi ApplicationID a Attribute.

e) Ak chce zástupca príslušného kontrolného orgánu zacieliť vozidlo a získať z cieľového vozidla *údaje*, najskôr musí vložiť svoju inteligentnú kartu do snímača *REDCR*, aby sa aktivovala *komunikácia* a zariadenie *SM – REDCR* mohlo overiť autenticitu karty a dekódovať údaje.

f) Zástupca príslušného kontrolného orgánu potom zacieli vozidlo a prostredníctvom diaľkovej komunikácie si vyžiada údaje. Snímač *REDCR* nadviaže reláciu rozhrania DSRC 5,8 GHz so zariadením *DSRC – VU* cieľového vozidla a požiada o *údaje*. *Údaje* sa prenášajú do snímača *REDCR* systémom bezdrôtovej komunikácie ako atribút DSRC s využitím aplikačnej služby GET v zmysle oddielu 5.4. Tento atribút obsahuje šifrované hodnoty obsahových údajov a bezpečnostných údajov DSRC.

g) Zariadenie *REDCR* údaje analyzuje a poskytuje ich zástupcovi príslušného kontrolného orgánu.

h) Zástupca príslušného kontrolného orgánu používa údaje pri rozhodovaní, či zastaviť vozidlo na dôkladnú kontrolu alebo nie, prípadne či požiadať iného zástupcu príslušného kontrolného orgánu, aby vozidlo zastavil.

5.2.2 *Výklad údajov získaných prostredníctvom komunikácie DSRC*

DSC_26 Údaje získané prostredníctvom rozhrania 5,8 GHz majú výlučne zmysel a význam vymedzený v odsekoch 5.4.4 a 5.4.5 nižšie a treba ich chápať v rámci tam stanovených cieľov. V súlade s ustanoveniami nariadenia (EÚ) č. 165/2014 sa *údaje* použijú iba na poskytnutie relevantných informácií príslušnému kontrolnému orgánu ako pomoc pri rozhodovaní o tom, ktoré vozidlo zastaviť na fyzickú kontrolu, a v súlade s článkom 9 nariadenia (EÚ) č. 165/2014 sa musia následne vymazať.

5.3 **Parametre fyzického rozhrania DSRC pre diaľkovú komunikáciu**

5.3.1 *Obmedzenia na umiestnenie*

DSC_27 Diaľkové snímanie vozidiel prostredníctvom rozhrania DSRC 5,8 GHz by sa nemalo používať v okruhu 200 metrov od funkčného portálu DSRC 5,8 GHz.

5.3.2 *Parametre zostupného (downlink) a vzostupného (uplink) prepojenia*

DSC_28 Zariadenie používané na diaľkové monitorovanie tachografu musí zodpovedať odporúčaniu ERC 70-03 a parametrom stanoveným v tabuľkách 14.1 a 14.2 a pracovať v súlade s nimi.

DSC_29 Aby sa zaistila kompatibilita s prevádzkovými parametrami ďalších normovaných systémov DSRC 5,8 GHz, zariadenie používané na diaľkové monitorovanie tachografu musí navyše zodpovedať parametrom uvedeným v normách EN 12253 a EN 13372.

Ide o:

Tabuľka 14.1

Parametre zostupného prepojenia (downlink)

Číslo položky	Parameter	Hodnota (hodnoty)	Poznámka
D1	Frekvencie nosiča zostupného prepojenia	Snímač REDCR môže použiť štyri alternatívy: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	V súlade s ERC 70-03. Frekvencie nosiča môže zvoliť realizátor cestného systému a nemusia byť známe zariadeniu DSRC – VU. (V súlade s normami EN 12253, EN 13372)
D1a (*)	Tolerancia frekvencií nosiča	do ±5 ppm	(V súlade s normou EN 12253)
D2 (*)	Spektrálna maska vysielača pri ceste – RSU (REDCR)	V súlade s ERC 70-03. REDCR musí zodpovedať triedam B a C podľa normy EN 12253. Žiadne iné osobitné požiadavky v rámci tejto prílohy.	Parameter používaný na kontrolu rušenia medzi snímačmi vo vzájomnej blízkosti (podľa noriem EN 12253 a EN 13372).
D3	Minimálny frekvenčný rozsah palubnej jednotky – OBU (DSRC – VU)	5,795 – 5,815 GHz	(V súlade s normou EN 12253)
D4 (*)	Maximálny výkon EIRP	V súlade s odporúčaním ERC 70-03 (bez licencie) a s vnútroštátnymi právnymi predpismi Maximálne + 33 dBm	(V súlade s normou EN 12253)
D4a	Uhlová maska výkonu EIRP	Podľa deklarovanej a uverejnenej špecifikácie konštruktéra snímača	(V súlade s normou EN 12253)
D5	Polarizácia	Kruhová ľavotočivá	(V súlade s normou EN 12253)
D5a	Diagonálna polarizácia	XPD: V osi: (REDCR) RSU t ≥15 dB (DSRC-VU) OBU r ≥10 dB V oblasti −3 dB: (REDCR) RSU t ≥10 dB (DSRC-VU) OBU r ≥6 dB	(V súlade s normou EN 12253)
D6 (*)	Modulácia	Dvojúrovňová amplitúdová modulácia	(V súlade s normou EN 12253)
D6a (*)	Modulačný index	0,5 … 0,9	(V súlade s normou EN 12253)

Číslo položky	Parameter	Hodnota (hodnoty)	Poznámka
D6b	Diagram oka	≥ 90 % (čas) / ≥ 85 % (amplitúda)	
D7 (*)	Kódovanie údajov	FM0 Bit „1“ má prechod iba na začiatku a na konci bitového intervalu. Bit „0“ má doplnkový prechod v strede bitového intervalu v porovnaní s bitom „1“.	(V súlade s normou EN 12253)
D8 (*)	Bitová rýchlosť	500 kBit/s	(V súlade s normou EN 12253)
D8a	Tolerancia bitových hodín	Lepšia ako ±100 ppm.	(V súlade s normou EN 12253)
D9 (*)	Bitová chybovosť (BER) pre komunikáciu	≤ 10^{-6}, keď dopadajúci výkon na OBU (DSRC – VU) je v rozmedzí stanovenom v bodoch [D11a až D11b].	(V súlade s normou EN 12253)
D10	Spúšťací signál pre OBU (DSRC-VU)	OBU (DSRC-VU) sa musí spustiť po prijatí akéhokoľvek rámca s najmenej 11 oktetmi (vrátane preambuly).	Nie je potrebný žiadny osobitný vzor spúšťania. DSRC – VU sa môže spustiť aj po prijatí rámca s menej než 11 oktetmi. (V súlade s normou EN 12253)
D10a	Maximálny čas začiatku	≤ 5 ms	(V súlade s normou EN 12253)
D11	Komunikačná zóna	Priestorová oblasť, v ktorej sa dosahuje hodnota BER podľa bodu D9a.	(V súlade s normou EN 12253)
D11a (*)	Hraničná hodnota výkonu pre komunikáciu (horná).	– 24dBm	(V súlade s normou EN 12253)
D11b (*)	Hraničná hodnota výkonu pre komunikáciu (spodná).	Dopadajúci výkon: – 43 dBm (v osi) – 41 dBm (pod uhlom – 45° až + 45° zodpovedajúcim rovine rovnobežnej s povrchom vozovky, keď sa DSRC – VU neskôr inštaluje vo vozidle (azimut))	(V súlade s normou EN 12253) Rozšírená požiadavka na horizontálne uhly do ±45° vzhľadom na možnosti použitia určené v tejto prílohe.
D12 (*)	Vypínacia hladina výkonu pre (DSRC-VU)	– 60 dBm	(V súlade s normou EN 12253)
D13	Preambula	Preambula je povinná.	(V súlade s normou EN 12253)
D13a	Dĺžka a vzor preambuly	16 bitov ±1 bit v prípade bitov FM0 kódovaných ako „1“	(V súlade s normou EN 12253)

Číslo položky	Parameter	Hodnota (hodnoty)	Poznámka
D13b	Tvar signálu preambuly	Striedavá postupnosť nízkej a vysokej úrovne s dĺžkou trvania pulzu 2 µs. Tolerancia je uvedená v bode D8a.	(V súlade s normou EN 12253)
D13c	Koncové bity	RSU (REDCR) má povolené vyslať najviac 8 bitov po príznaku ukončenia (end flag). OBU (DSRC-VU) nemusí tieto dodatočné bity zohľadniť.	(V súlade s normou EN 12253)

(*) – Parametre zostupného prepojenia, ktoré podliehajú skúške zhody v súlade s príslušnou skúškou parametrov uvedenou v norme EN 300 674-1.

Tabuľka 14.2

Parametre vzostupného prepojenia (uplink)

Číslo položky	Parameter	Hodnota (hodnoty)	Poznámka
U1 (*)	Frekvencie pomocného nosiča	OBU (DSRC – VU) musí podporovať 1,5 MHz a 2,0 MHz RSU (REDCR) musí podporovať 1,5 MHz alebo 2,0 MHz alebo obe. U1-0: 1,5 MHz U1-1: 2,0 MHz	Voľba frekvencie pomocného nosiča (1,5 MHz alebo 2,0 MHz) závisí od zvoleného profilu podľa normy EN 13372.
U1a (*)	Tolerancia frekvencií pomocného nosiča	do ± 0,1 %	(V súlade s normou EN 12253)
U1b	Použitie postranných pásiem	Rovnaké údaje na oboch stranách.	(V súlade s normou EN 12253)
U2 (*)	Spektrálna maska vysielača OBU (DSRC-VU)	Podľa normy EN 12253. 1) Výkon mimo pásma: pozri normu ETSI EN 300674-1 2) Výkon v pásme: [U4a] dBm pri 500 kHz 3) Emisia v akomkoľvek inom kanáli vzostupného prepojenia: U2(3)-1 = – 35 dBm pri 500 kHz	(V súlade s normou EN 12253)
U4a (*)	Maximálny výkon EIRP v jednom postrannom pásme (v osi)	Dve možnosti: U4a-0: – 14 dBm U4a-1: – 21 dBm	Podľa deklarovanej a uverejnenej špecifikácie konštruktéra zariadenia.
U4b (*)	Maximálny výkon EIRP v jednom postrannom pásme (35°)	Dve možnosti: — neuplatňuje sa — – 17 dBm	Podľa deklarovanej a uverejnenej špecifikácie konštruktéra zariadenia.
U5	Polarizácia	Kruhová ľavotočivá	(V súlade s normou EN 12253)

Číslo položky	Parameter	Hodnota (hodnoty)	Poznámka
U5a	Diagonálna polarizácia	XPD: V osi: (REDCR) RSU r ≥15 dB (DSRC-VU) OBU t ≥10 dB Pri – 3 dB: (REDCR) RSU r ≥10 dB (DSRC-VU) OBU t ≥6 dB	(V súlade s normou EN 12253)
U6	Modulácia pomocného nosiča	2-PSK Zakódované údaje zosynchronizované s pomocným nosičom: Prechody zakódovaných údajov sa zhodujú s prechodmi pomocného nosiča.	(V súlade s normou EN 12253)
U6b	Pracovný cyklus	Pracovný cyklus: 50 % ± α, α ≤ 5 %	(V súlade s normou EN 12253)
U6c	Modulácia nosiča	Multiplikácia modulovaného pomocného nosiča s nosičom.	(V súlade s normou EN 12253)
U7 (*)	Kódovanie údajov	NRZI (Žiadny prechod na začiatku bitu „1“, prechod na začiatku bitu „0“, žiadny prechod v rámci bitu)	(V súlade s normou EN 12253)
U8 (*)	Bitová rýchlosť	250 kbit/s	(V súlade s normou EN 12253)
U8a	Tolerancia bitových hodín	do ± 1 000 ppm	(V súlade s normou EN 12253)
U9	Bitová chybovosť (BER) pri komunikácii	$\leq 10^{-6}$	(V súlade s normou EN 12253)
U11	Komunikačná zóna	Priestorová oblasť, v ktorej je zariadenie DSRC – VU umiestnené tak, že jeho vysielanie prijíma snímač REDCR s hodnotou BER nižšou, než sa uvádza v bode U9a.	(V súlade s normou EN 12253)
U12a (*)	Konverzný zisk (spodná hranica)	1 dB pre každé postranné pásmo Rozsah uhlov: Kruhovo symetrický medzi osou a ± 35° a	
		v rozsahu – 45° až + 45° zodpovedajúci rovine rovnobežnej s povrchom vozovky, keď sa DSRC – VU neskôr inštaluje vo vozidle (azimut))	Vyšší než stanovený rozsah hodnôt pre horizontálne uhly do ± 45° vzhľadom na možnosti použitia určené v tejto prílohe.
U12b (*)	Konverzný zisk (horná hranica)	10 dB pre každé postranné pásmo	Nižší, než je špecifikovaný rozsah hodnôt pre každé postranné pásmo v rámci kruhového kužeľa okolo osi s počiatočným uhlom ± 45°
U13	Preambula	Preambula je povinná.	(V súlade s normou EN 12253)

Číslo položky	Parameter	Hodnota (hodnoty)	Poznámka
U13a	Dĺžka a vzor preambuly	32 až 36 µs modulované len s pomocným nosičom, potom 8 bitov NRZI kódovaných „0“.	(V súlade s normou EN 12253)
U13b	Koncové bity	DSRC – VU smie vyslať najviac 8 bitov po príznaku ukončenia. RSU (REDCR) nemusí tieto dodatočné bity zohľadniť.	(V súlade s normou EN 12253)

(*) Parametre vzostupného prepojenia, ktoré podliehajú skúške zhody v súlade s príslušnou skúškou parametrov uvedenou v norme EN 300 674-1.

5.3.3 *Konštrukcia antény*

5.3.3.1 Anténa REDCR

DSC_30 Konštrukcia antény snímača *REDCR* je vecou komerčných návrhov v súlade s obmedzeniami stanovenými v odseku 5.3.2 a je uspôsobená tak, aby optimalizovala snímaciu výkonnosť zariadenia *DSRC – REDCR* vzhľadom na konkrétne účely a prevádzkové podmienky, na ktoré bol snímač *REDCR* navrhnutý.

5.3.3.2 Anténa VU

DSC_31 Konštrukcia antény snímača *DSRC-VU* je vecou komerčných návrhov v súlade s obmedzeniami stanovenými v odseku 5.3.2 a je uspôsobená tak, aby optimalizovala snímaciu výkonnosť zariadenia *DSRC – REDCR* vzhľadom na konkrétne účely a prevádzkové podmienky, na ktoré bol snímač *REDCR* navrhnutý.

DSC_32 Anténa VU musí byť upevnená na čelné sklo vozidla alebo v jeho blízkosti, ako je špecifikované v oddiele 5.1.

DSC_33 V skúšobnom prostredí v dielni (pozri oddiel 6.3) sa musí anténa DSRC – VU upevnená podľa oddielu 5.1 vyššie úspešne spojiť so štandardným skúšobným komunikačným zariadením a úspešne vykonať transakciu RTM podľa tohto dodatku na vzdialenosť 2 až 10 metrov viac ako 99 % času, s priemerom vyše 1 000 snímaní.

5.4 **Požiadavky na protokol DSRC pre RTM**

5.4.1 *Prehľad*

DSC_34 Transakčný protokol na sťahovanie *údajov* prostredníctvom spojenia s rozhraním DSRC 5,8 GHz prebieha podľa nasledovných krokov. V tomto oddiele sa opisuje transakčný tok v ideálnych podmienkach bez retransmisie alebo prerušení komunikácie.

POZNÁMKA Účelom inicializačnej fázy (1. krok) je pripraviť komunikáciu medzi snímačom *REDCR* a DSRC – VU, ktoré vstúpili do transakčnej zóny DSRC 5,8 GHz (master/slave – hlavná/podriadená jednotka), ale ešte nezačali komunikáciu so snímačom *REDCR*, a oznámiť aplikačné procesy.

— **1. krok** Inicializácia. Snímač *REDCR* posiela dátový rámec obsahujúci „tabuľku prevádzkových režimov majáka“ (BST), ktorá zahŕňa identifikátory aplikácie (AID) na zozname podporovaných služieb. V aplikácii RTM to bude jednoducho služba s hodnotou AID = 2 (Freight&Fleet). Zariadenie *DSRC – VU* vyhodnotí prijatú tabuľku BST a odpovie (pozri v ďalšej časti) zoznamom podporovaných aplikácií v rámci domény Freight&Fleet, alebo neodpovie, ak žiadna aplikácia nie je podporovaná. Ak snímač *REDCR* neponúka hodnotu AID = 2, zariadenie DSRC – VU snímaču REDCR neodpovie.

— **2. krok** Zariadenie *DSRC – VU* posiela rámec s požiadavkou na pridelenie súkromného okna.

— **3. krok** Snímač *REDCR* posiela rámec s pridelením súkromného okna.

— **4. krok** Zariadenie *DSRC – VU* použije pridelené súkromné okno na odoslanie rámca obsahujúceho tabuľku jednotky vozidla (VST). Táto tabuľka VST obsahuje zoznam všetkých jednotlivých konkretizácií aplikácie, ktoré toto zariadenie *DSRC – VU* podporuje v rámci AID = 2. Rôzne konkretizácie sa identifikujú pomocou jedinečne generovaných identifikátorov prvku (EID), z ktorých každý je spojený s hodnotou parametra Application Context Mark (kontextová značka aplikácie) označujúcou podporovanú aplikáciu a normu.

— **5. krok** Snímač *REDCR* ďalej analyzuje ponúkanú tabuľku VST a buď ukončí spojenie (RELEASE), keďže ho nezaujíma nič z ponuky VST (t. j. dostáva VST od zariadenia *DSRC – VU*, ktoré nepodporuje transakciu RTM), alebo, ak dostane vhodnú tabuľku VST, začne konkretizáciu aplikácie.

— **6. krok** Aby to snímač *REDCR* dosiahol, vyšle rámec obsahujúci príkaz na získanie údajov RTM, ktorý identifikuje konkretizáciu aplikácie RTM špecifikovaním identifikátora zodpovedajúceho konkretizácii aplikácie RTM (ktorý DSRC – VU uvádza v tabuľke VST) a pridelí súkromné okno.

— **7. krok** Zariadenie *DSRC – VU* použije novo pridelené súkromné okno na odoslanie rámca obsahujúceho požadovaný identifikátor zodpovedajúci konkretizácii aplikácie RTM podľa tabuľky VST, a následne atribút *RtmData* (obsahový + bezpečnostný prvok).

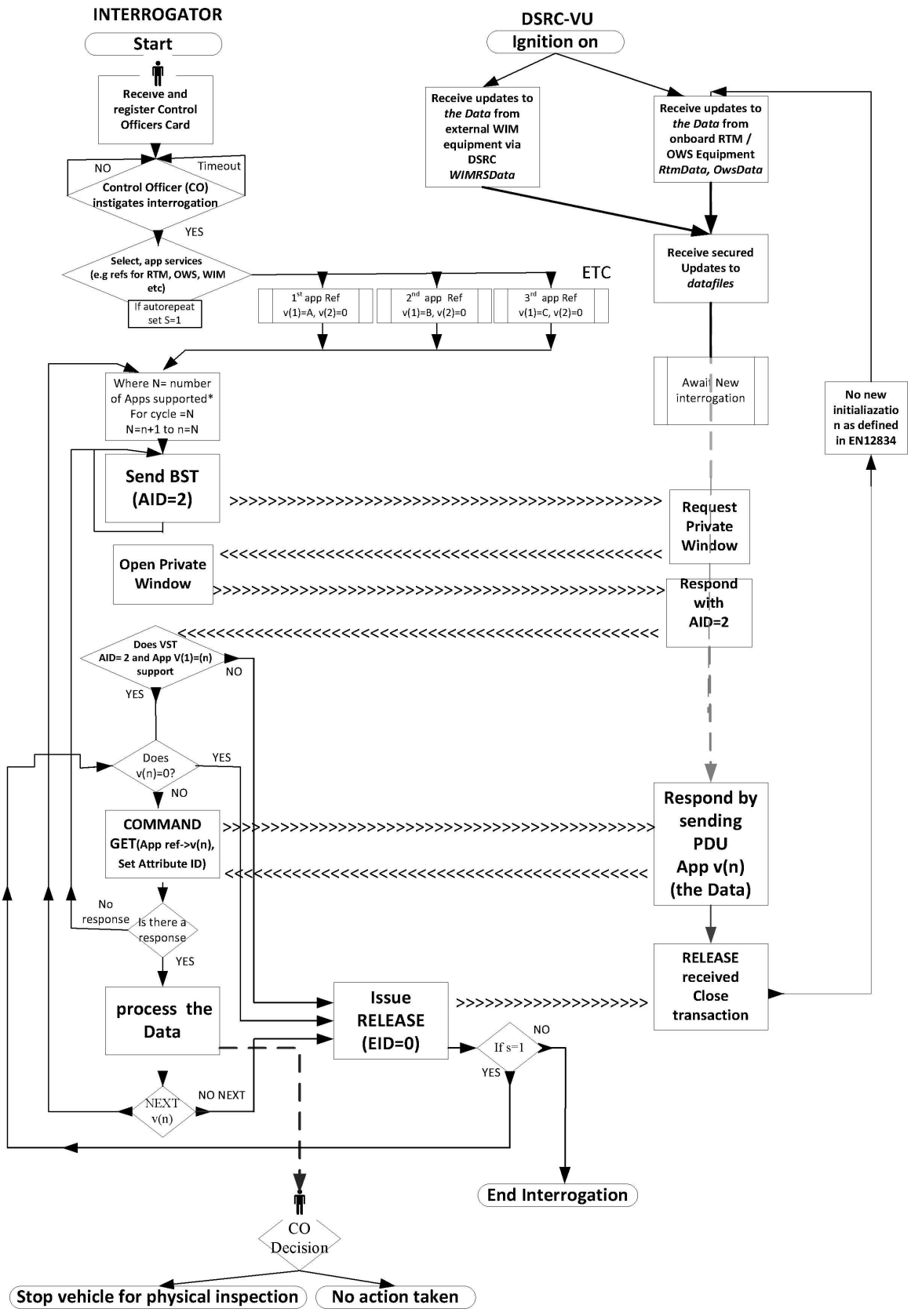
— **8. krok** Ak sa požadujú viaceré služby, hodnota „n“ sa zmení na referenčné číslo nasledujúcej služby a postup sa opakuje.

— **9. krok** Snímač *REDCR* potvrdí prijatie údajov zaslaním rámca obsahujúceho príkaz RELEASE zariadeniu *DSRC – VU*, aby sa relácia ukončila ALEBO, ak sa mu nepodarilo validovať úspešné prijatie LPDU, vráti sa ku 6. kroku.

Grafické znázornenie transakčného protokolu je uvedené na obrázku 14.6.

Obrázok 14.6

Schéma postupu aplikácie RTM s použitím DSRC 5,8 GHz



5.4.2 *Príkazy*

DSC_35 Tieto príkazy sú jedinými funkciami, ktoré sa používajú v transakčnej fáze aplikácie RTM:

— **INITIALISATION.request**: Príkaz vydaný snímačom REDCR vo forme vysielania s vymedzením aplikácií, ktoré REDCR podporuje.

— **INITIALISATION.response**: Odpoveď zariadenia DSRC – VU potvrdzujúca pripojenie a obsahujúca zoznam podporovaných inštancií aplikácií s charakteristikami a informáciami, ako k nim pristupovať (EID).

— **GET.request**: Príkaz vydaný snímačom *REDCR* zariadeniu *DSRC – VU*, ktorým sa špecifikuje konkretizácia aplikácie na základe stanoveného identifikátora EID podľa prijatej tabuľky VST, a dáva sa pokyn zariadeniu *DSRC – VU*, aby odoslalo zvolené atribúty s *údajmi*. Cieľom príkazu GET je, aby snímač *REDCR* získal *údaje* od zariadenia *DSRC – VU*.

— **GET.response**: Odpoveď zariadenia DSRC – VU, ktorá obsahuje požadované *údaje*.

— **ACTION.request ECHO**: Príkaz zariadeniu *DSRC – VU*, aby odoslalo údaje z *DSRC – VU* naspäť snímaču *REDCR*. Cieľom príkazu ECHO je umožniť dielňam alebo skúšobným zariadeniam pre typové schvaľovanie preskúšať, či spojenie DSRC funguje, bez potreby prístupu k oprávneniam zabezpečenia.

— **ACTION**.response ECHO: Odpoveď zariadenia DSRC – VU na príkaz ECHO.

— **EVENT_REPORT.request** RELEASE: Príkaz, ktorým sa dáva pokyn zariadeniu *DSRC – VU*, že transakcia sa skončila. Cieľom príkazu RELEASE je ukončiť reláciu so zariadením *DSRC – VU*. Zariadenie *DSRC – VU* po prijatí príkazu RELEASE nesmie odpovedať na žiadne ďalšie snímanie v rámci aktuálneho spojenia. Upozorňujeme, že podľa normy EN 12834 sa zariadenie DSRC – VU nepripojí dvakrát k tomu istému snímaču, pokiaľ nebude mimo komunikačnej zóny počas 255 sekúnd alebo sa na snímači nezmení identifikátor majáka.

5.4.3 *Postupnosť príkazov snímania*

DSC_36 Z hľadiska postupnosti príkazov a odpovedí sa transakcia opisuje takto:

Krok	Odosielateľ		Príjemca	Opis	Činnosť
1	REDCR	>	DSRC-VU	Inicializácia komunikačného spojenia – Požiadavka	Snímač REDCR odosiela tabuľku BST.
2	*DSRC-VU*	>	*REDCR*	*Inicializácia komunikačného spojenia – Odpoveď*	*Ak tabuľka BST podporuje AID=2, DSRC – VU si vyžiada súkromné okno*
3	REDCR	>	DSRC-VU	Poskytne súkromné okno.	Posiela rámec s pridelením súkromného okna.
4	*DSRC-VU*	>	*REDCR*	*Posiela tabuľku VST.*	*Posiela rámec obsahujúci VST.*
5	REDCR	>	DSRC-VU	Posiela príkaz GET.request na údaje v atribúte pre konkrétny identifikátor EID.	
6	*DSRC-VU*	>	*REDCR*	*Posiela príkaz GET.response s požadovaným atribútom pre konkrétny EID.*	*Posiela atribút (RTMData, OWSData...) s údajmi pre konkrétny EID.*

Krok	Odosielateľ		Príjemca	Opis	Činnosť
7	REDCR	>	DSRC-VU	Posiela príkaz GET.request na údaje v inom atribúte (v prípade potreby).	
8	*DSRC-VU*	>	*REDCR*	*Posiela príkaz GET.response s požadovaným atribútom.*	*Posiela atribút s údajmi pre konkrétny EID.*
9	REDCR	>	DSRC-VU	Potvrdzuje úspešné prijatie údajov.	Posiela príkaz RELEASE, ktorým sa ukončí transakcia.
10	*DSRC-VU*			*Ukončuje transakciu.*	

Príklad postupnosti transakcie a obsahu vymieňaných rámcov je uvedený v odsekoch 5.4.7 a 5.4.8.

5.4.4 *Štruktúry údajov*

DSC_37 Sémantická štruktúra *údajov* prenášaných prostredníctvom rozhrania DSRC 5,8 GHz musí byť v súlade s týmto dodatkom. Spôsob, akým sú tieto údaje štruktúrované, je špecifikovaný v tomto odseku.

DSC_38 Obsahové údaje (údaje RTM) pozostávajú zo zreťazenia:

1. údajov EncryptedTachographPayload, ktoré sú kódovaním údajov TachographPayload vymedzeným v ASN.1 oddiele 5.4.5. Spôsob kódovania je opísaný v dodatku 11;

2. údajov DSRCSecurityData špecifikovaných v dodatku 11.

DSC_39 Údaje RTM Data sa označujú ako atribút RTM = 1 a prenášajú sa v kontajneri RTM = 10.

DSC_40 Kontextová značka RTM identifikuje podporovanú časť normy zo súboru noriem TARV (RTM zodpovedá časti 9),

Modul ASN.1 pre údaje DSRC v rámci aplikácie RTM je vymedzený takto:

```
   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 *Prvky RtmData, vykonávané činnosti a vymedzenie pojmov*

DSC_41 Hodnoty údajov, ktoré sa majú vypočítať vo VU a použiť na aktualizáciu zabezpečených údajov v DSRC – VU, sa vypočítajú podľa pravidiel uvedených v tabuľke 14.3:

Tabuľka 14.3

Prvky RtmData, vykonávané činnosti a vymedzenie pojmov

(1) Dátový prvok RTM	(2) Činnosť vykonávaná VU		(3) Vymedzenie údajov podľa ASN.1
RTM1 **Evidenčné číslo vozidla**	VU určí hodnotu dátového prvku RTM1 *tp15638VehicleRegistrationPlate* zo zaznamenanej hodnoty dátového typu *VehicleRegistrationIdentification* v zmysle dodatku 1 *VehicleRegistrationIdentification*	Evidenčné číslo vozidla ako reťazec znakov	tp15638VehicleRegstrationPlate LPN, --Evidenčné číslo vozidla importované z normy ISO 14906 s obmedzením špecifikovaným v norme EN 15509, ktorá je postupnosťou (SEQUENCE) pozostávajúcou z kódu krajiny, nasledovaného abecedným indikátorom a samotným evidenčným číslom, ktoré má vždy 14 oktetov (doplnených nulami), aby dĺžka typu LPN podľa normy EN 15509 bola vždy 17 oktetov, z ktorých 14 predstavuje „skutočné“ evidenčné číslo.

(1) Dátový prvok RTM	(2) Činnosť vykonávaná VU		(3) Vymedzenie údajov podľa ASN.1
RTM2 **Udalosť – prekročenie povolenej rýchlosti**	VU vygeneruje booleovskú hodnotu pre dátový prvok RTM2 tp15638SpeedingEvent. VU vypočíta hodnotu tp15638SpeedingEvent z počtu udalostí prekročenia rýchlosti (Over Speeding Events) zaznamenaných vo VU v priebehu uplynulých 10 dní výskytu podľa prílohy 1C. Ak počas uplynulých 10 dní výskytu došlo aspoň k jednej udalosti tp15638SpeedingEvent, hodnota tp15638SpeedingEvent sa nastaví na hodnotu TRUE. INAK (ELSE), ak sa počas uplynulých 10 dní výskytu nezaznamenali žiadne udalosti, hodnota tp15638SpeedingEvent sa nastaví na hodnotu FALSE.	1 (TRUE) – znamená nezrovnalosti týkajúce sa rýchlosti v priebehu uplynulých 10 dní výskytu.	`tp15638speedingEvent BOOLEAN,`
RTM3 **Jazda bez platnej karty**	VU vygeneruje booleovskú hodnotu pre dátový prvok RTM3 tp15638DrivingWithoutValidCard. VU priradí premennej tp15638DrivingWithoutValidCard hodnotu TRUE, ak sa v údajoch VU počas uplynulých 10 dní výskytu zaznamenala aspoň jedna udalosť typu „vedenie vozidla bez príslušnej karty“ podľa prílohy 1C. INAK (ELSE), ak sa počas uplynulých 10 dní výskytu nezaznamenali žiadne udalosti, premenná tp15638DrivingWithoutValidCard sa nastaví na hodnotu FALSE.	1 (TRUE) = označuje použitie neplatnej karty.	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Platná karta vodiča**	VU vygeneruje booleovskú hodnotu pre dátový prvok RTM4 tp15638DriverCard na základe údajov uložených vo VU a vymedzených v dodatku 1. Ak nie je prítomná žiadna platná karta vodiča, VU nastaví premennú na hodnotu TRUE. INAK (ELSE), ak je prítomná platná karta vodiča, VU nastaví premennú na hodnotu FALSE.	0 (FALSE) = znamená platnú kartu vodiča	`tp15638DriverCard BOOLEAN,`
RTM5 **Vloženie karty počas jazdy**	VU vygeneruje booleovskú hodnotu pre dátový prvok RTM5. VU priradí premennej tp15638CardInsertion hodnotu TRUE, ak sa v údajoch VU zaznamenala v priebehu uplynulých 10 dní výskytu aspoň jedna udalosť typu „Vloženie karty počas vedenia vozidla“ v zmysle prílohy 1C. INAK (ELSE), ak sa počas uplynulých 10 dní výskytu nezaznamenali žiadne takéto udalosti, premenná tp15638CardInsertion sa nastaví na hodnotu FALSE.	1 (TRUE) = označuje vloženie karty počas jazdy v priebehu uplynulých 10 dní výskytu.	`tp15638CardInsertion BOOLEAN,`
RTM6 **Chyba údajov o pohybe**	VU vygeneruje booleovskú hodnotu pre dátový prvok RTM6. VU priradí premennej tp15638MotionDataError hodnotu TRUE, ak sa v údajoch VU zaznamenala v priebehu uplynulých 10 dní výskytu aspoň jedna udalosť typu „chyba údajov o pohybe“ v zmysle prílohy 1C. INAK (ELSE), ak sa počas uplynulých 10 dní výskytu nezaznamenali žiadne takéto udalosti, premenná tp15638MotionDataError sa nastaví na hodnotu FALSE.	1 (TRUE) = označuje chybu údajov o pohybe počas uplynulých 10 dní výskytu.	`tp15638motionDataError BOOLEAN,`

(1) Dátový prvok RTM	(2) Činnosť vykonávaná VU		(3) Vymedzenie údajov podľa ASN.1
RTM7 **Nesúlad údajov o pohybe vozidla**	VU vygeneruje booleovskú hodnotu pre dátový prvok RTM7. VU priradí premennej tp15638vehicleMotionConflict hodnotu TRUE, ak sa v údajoch VU zaznamenala v priebehu uplynulých 10 dní výskytu aspoň jedna udalosť typu „nesúlad údajov o pohybe vozidla“ (hodnota ‘0A’H). INAK (ELSE), ak sa počas uplynulých 10 dní výskytu nezaznamenali žiadne udalosti, premenná tp15638vehicleMotionConflict sa nastaví na hodnotu FALSE.	1 (TRUE) = označuje nesúlad údajov o pohybe počas uplynulých 10 dní výskytu.	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Druhá karta vodiča**	VU vygeneruje booleovskú hodnotu pre dátový prvok RTM8 na základe prílohy 1C („údaje o činnosti vodiča“ posádka (CREW) a druhý vodič (CO-DRIVER)). Ak je prítomná druhá platná karta vodiča, VU nastaví premennú na hodnotu TRUE. INAK (ELSE), ak druhá platná karta vodiča nie je prítomná, VU nastaví premennú na hodnotu FALSE.	1 (TRUE) = označuje vloženú druhú kartu vodiča.	`tp156382ndDriverCard` `BOOLEAN,`
RTM9 **Aktuálna činnosť**	VU vygeneruje booleovskú hodnotu pre dátový prvok RTM9. Ak sa aktuálna činnosť zaznamená vo VU ako akákoľvek iná činnosť než „jazda“ (DRIVING) v zmysle prílohy 1C, VU nastaví premennú na hodnotu TRUE. INAK (ELSE), ak sa aktuálna činnosť zaznamená vo VU ako „jazda“ (DRIVING), VU nastaví premennú na hodnotu FALSE.	1 (TRUE) = zvolená iná činnosť, 0 (FALSE) = zvolená jazda	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Posledná relácia ukončená**	VU vygeneruje booleovskú hodnotu pre dátový prvok RTM10. Ak posledná relácia karty nebola správne ukončená v zmysle prílohy 1C, VU nastaví premennú na hodnotu TRUE. INAK (ELSE), ak posledná relácia karty bola ukončená správne, VU nastaví premennú na hodnotu FALSE.	1 (TRUE) = nesprávne ukončenie 0 (FALSE) = správne ukončenie	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Prerušenie napájania**	VU vygeneruje celočíselnú hodnotu pre dátový prvok RTM11. VU priradí premennej tp15638PowerSupplyInterruption hodnotu rovnajúcu sa najdlhšiemu prerušeniu dodávky energie podľa článku 9 nariadenia (EÚ) č. 165/2014 typu „prerušenie napájania“ v zmysle prílohy 1C. INAK (ELSE), ak počas uplynulých 10 dní výskytu nedošlo k prerušeniu napájania, premenná sa nastaví na hodnotu 0.	— Počet prerušení napájania počas uplynulých 10 dní výskytu	`tp15638powerSupplyInterruption` `celé číslo – INTEGER (0..127),`

(1) Dátový prvok RTM	(2) Činnosť vykonávaná VU		(3) Vymedzenie údajov podľa ASN.1
RTM12 **Porucha snímača**	VU vygeneruje celočíselnú hodnotu pre dátový prvok RTM12. VU priradí premennej sensorFault hodnotu: — 1 ak sa počas uplynulých 10 dní zaznamenala udalosť typu '35'H porucha snímača, — 2 ak sa počas uplynulých 10 dní zaznamenala udalosť typu porucha prijímača GNSS (interná či externá s hodnotami enum '51'H alebo '52'H) — 3 ak sa počas uplynulých 10 dní výskytu zaznamenala udalosť typu '53'H „External GNSS communication fault" (externá porucha komunikácie GNSS) — -4 ak sa počas uplynulých 10 dní výskytu zaznamenala porucha snímača aj prijímača GNSS — -5 ak sa počas uplynulých 10 dní výskytu zaznamenala porucha snímača aj externá porucha komunikácie GNSS — -6 ak sa počas uplynulých 10 dní výskytu zaznamenala porucha prijímača GNSS aj externá porucha komunikácie GNSS — -7 ak sa počas uplynulých 10 dní výskytu zaznamenali všetky tri poruchy. INAK (ELSE) sa priradí hodnota 0, ak sa počas uplynulých 10 dní výskytu nezaznamenali žiadne udalosti.	— Porucha snímača – jeden oktet podľa slovníka údajov	`tp15638SensorFault celé číslo – INTEGER (0..255),`
RTM13 **Úprava času**	VU generuje celé číslo (timeReal z dodatku 1) pre dátový prvok RTM13 na základe prítomnosti údajov o úprave času v zmysle prílohy 1C. VU priradí hodnotu času, kedy došlo k poslednej udalosti úpravy času. INAK (ELSE), ak v údajoch VU neexistuje žiadna udalosť Time Adjustment (úprava času) v zmysle prílohy 1C, VU nastaví hodnotu 0	Čas poslednej úpravy času	`tp15638TimeAdjustment` `celé číslo – INTEGER(0..4294967295),`
RTM14 **Pokus o narušenie zabezpečenia**	VU generuje celé číslo (timeReal z dodatku 1) pre dátový prvok RTM14 na základe prítomnosti udalosti „Security breach attempt" (pokus o narušenie zabezpečenia) v zmysle prílohy 1C. VU nastaví hodnotu času posledného pokusu o narušenie zabezpečenia, ktorý VU zaznamenala. INAK (ELSE), ak v údajoch VU nie je zaznamenaný žiaden pokus o narušenie zabezpečenia v zmysle prílohy 1C, nastaví hodnotu 0x00FF.	Čas posledného pokusu o narušenie — predvolená hodnota = 0x00FF	`tp15638LatestBreachAttempt` `celé číslo – INTEGER(0..4294967295),`
RTM15 **Posledná kalibrácia**	VU generuje celé číslo (timeReal z dodatku 1) pre dátový prvok RTM15 na základe prítomnosti údajov o poslednej kalibrácii v zmysle prílohy 1C. VU nastaví hodnotu času posledných dvoch kalibrácií (RTM15 a RTM16), ktoré sú nastavené vo VuCalibrationData v zmysle dodatku 1. VU nastaví hodnotu pre RTM15 na timeReal posledného záznamu o kalibrácii.	Údaje o čase poslednej kalibrácie	`tp15638LastCalibrationData` `celé číslo – INTEGER(0..4294967295),`

(1) Dátový prvok RTM	(2) Činnosť vykonávaná VU		(3) Vymedzenie údajov podľa ASN.1
RTM16 **Predchádzajúca kalibrácia**	VU generuje celé číslo (timeReal z dodatku 1) pre dátový prvok RTM16 podľa záznamu o kalibrácii predchádzajúcej poslednú kalibráciu INAK (ELSE), ak k žiadnej predchádzajúcej kalibrácii nedošlo, VU nastaví hodnotu RTM16 na 0.	Údaje o čase predchádzajúcej kalibrácie	`tp15638PrevCalibrationData` `celé číslo – INTEGER(0..4294967295),`
RTM17 **Dátum pripojenia tachografu**	VU vygeneruje pre dátový prvok RTM17 celočíselnú hodnotu (timeReal z dodatku 1). VU nastaví hodnotu času prvej inštalácie VU. VU tieto údaje extrahuje z VuCalibrationData (dodatok 1) z vuCalibrationRecords, pričom CalibrationPurpose sa rovná: '03'H	Dátum pripojenia tachografu	`tp15638DateTachoConnected` `celé číslo – INTEGER(0..4294967295),`
RTM18 **Aktuálna rýchlosť**	VU vygeneruje celočíselnú hodnotu pre dátový prvok RTM18. VU nastaví hodnotu pre RTM18 na poslednú aktuálnu zaznamenanú rýchlosť v čase poslednej aktualizácie RtmData.	Posledná aktuálna zaznamenaná rýchlosť	`tp15638CurrentSpeed` `celé číslo – INTEGER (0..255),`
RTM19 **Časová pečiatka**	VU vygeneruje pre dátový prvok RTM19 celočíselnú hodnotu (timeReal z dodatku 1). VU nastaví hodnotu pre RTM19 na čas poslednej aktualizácie RtmData.	Časová pečiatka aktuálneho záznamu TachographPayload	`tp15638Timestamp` `celé číslo – INTEGER(0..4294967295),`

5.4.6 *Mechanizmus prenosu údajov*

DSC_42 Už vymedzené obsahové údaje si vyžiada snímač REDCR po inicializačnej fáze a následne ich zariadenie *DSRC – VU* vysiela v pridelenom okne. Snímač REDCR použije na získanie údajov príkaz GET.

DSC_43 Pre všetky výmeny DSRC musia byť údaje zakódované podľa pravidiel zhusteného kódovania (Packed Encoding Rules – PER).

5.4.7 *Podrobný opis transakcií DSRC*

DSC_44 Inicializácia sa vykonáva podľa odsekov DSC_44 – DSC_48 a tabuliek 14.4 – 14.9. V inicializačnej fáze snímač REDCR začína posielať rámec obsahujúci tabuľku prevádzkových režimov majáka (BST) podľa noriem EN 12834 a EN 13372, oddielov 6.2, 6.3, 6.4 a 7.1, s nastaveniami podľa nasledovnej tabuľky 14.4.

Tabuľka 14.4

Inicializácia – nastavenia rámca BST

Pole	Nastavenia
Identifikátor spojenia	Vysielacia adresa
Identifikátor majáka (BeaconId)	Podľa normy EN 12834
Čas	Podľa normy EN 12834
Profil	Bez rozšírenia, použije sa 0 alebo 1
MandApplications	Bez rozšírenia, identifikátor EID neprítomný, parameter neprítomný, AID = 2 Freight&Fleet
NonMandApplications	Neprítomné
ProfileList	Bez rozšírenia, počet profilov na zozname = 0
Záhlavie fragmentácie	Bez fragmentácie
Nastavenia vrstvy 2	PDU príkazu, príkaz UI

Praktický príklad nastavení špecifikovaných v tabuľke 14.4 s označením bitového kódovania je uvedený v tabuľke 14.5.

Tabuľka 14.5

Inicializácia – príklad obsahu rámca BST

Oktet č.	Atribút/pole	Bity v oktete	Opis
1	FLAG	0111 1110	Príznak začiatku
2	Broadcast ID	1111 1111	Vysielacia adresa
3	MAC Control Field	1010 0000	PDU príkazu
4	LLC Control field	0000 0011	Príkaz UI
5	Fragmentation header	1xxx x001	Bez fragmentácie

Oktet č.	Atribút/pole	Bity v oktete	Opis
6	BST	1000	Požiadavka inicializácie
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	aplikácie NonMand neprítomné
		xxx	Identifikátor výrobcu
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27-bitový identifikátor dostupný výrobcovi
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32-bitový UNIX v reálnom čase
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,…)	0000 0000	Bez rozšírenia. Príklad profilu 0
17	MandApplications SEQUENCE (SIZE(0..127, …)) OF {	0000 0001	Bez rozšírenia. Počet mandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	Identifikátor EID neprítomný
	OPTION indicator	0	Parameter neprítomný
	AID DSRCApplicationEntityID } }	00 0010	Bez rozšírenia. AID= 2 Freight&Fleet

Oktet č.	Atribút/pole	Bity v oktete	Opis
19	ProfileList SEQUENCE (0..127,…) OF Profile }	0000 0000	Bez rozšírenia, počet profilov na zozname = 0
20	FCS	xxxx xxxx	Kontrolný súčet rámca
21		xxxx xxxx	
22	Flag	0111 1110	Príznak ukončenia

DSC_45 Zariadenie *DSRC – VU* po prijatí tabuľky BST požaduje pridelenie súkromného okna, ako je špecifikované v normách EN 12795 a EN 13372, 7.1.1, bez konkrétnych nastavení RTM. V tabuľke 14.6 je uvedený príklad bitového kódovania.

Tabuľka 14.6

Inicializácia – obsah rámca požiadavky na pridelenie súkromného okna

Oktet č.	Atribút/pole	Bity v oktete	Opis
1	FLAG	0111 1110	Príznak začiatku
2	Private LID	xxxx xxxx	Adresa spojenia konkrétneho DSRC – VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Požiadavka na súkromné okno
7	FCS	xxxx xxxx	Kontrolný súčet rámca
8		xxxx xxxx	
9	Flag	0111 1110	Príznak ukončenia

DSC_46 Snímač REDCR potom odpovedá pridelením súkromného okna, ako je špecifikované v normách EN 12795 a EN 13372, 7.1.1, bez konkrétnych nastavení RTM.

V tabuľke 14.7 je uvedený príklad bitového kódovania.

Tabuľka 14.7

Inicializácia – obsah rámca pridelenia súkromného okna

Oktet č.	Atribút/pole	Bity v oktete	Opis
1	FLAG	0111 1110	Príznak začiatku
2	Private LID	xxxx xxxx	Adresa spojenia konkrétneho DSRC – VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Pridelenie súkromného okna
7	FCS	xxxx xxxx	Kontrolný súčet rámca
8		xxxx xxxx	
9	Flag	0111 1110	Príznak ukončenia

DSC_47 Zariadenie *DSRC – VU* po prijatí pridelenia súkromného okna posiela svoju tabuľku jednotky vozidla (VST), ako je vymedzené v normách EN 12834 a EN 13372 a oddieloch 6.2, 6.3, 6.4 a 7.1, s nastaveniami podľa tabuľky 14.8, s použitím prideleného prenosového okna.

Tabuľka 14.8

Inicializácia – nastavenia rámca VST

Pole	Nastavenia
Private LID	Podľa normy EN 12834
Parametre tabuľky VST	Fill=0, potom pre každú podporovanú aplikáciu: Identifikátor EID prítomný, parameter prítomný, AID = 2, identifikátor EID, ako ho vygeneruje palubná jednotka (OBU)
Paramter	Bez rozšírenia, obsahuje kontextovú značku RTM
ObeConfiguration	Nepovinné pole ObeStatus môže byť prítomné, ale REDCR ho nepoužije
Fragmentation header	Bez fragmentácie
Nastavenia vrstvy 2	PDU príkazu, príkaz UI

DSC_48 Zariadenie *DSRC – VU* musí podporovať aplikáciu „Nákladná doprava a vozový park“ („Freight and Fleet“) s identifikátorom aplikácie „2“. Podporované môžu byť aj iné identifikátory aplikácie, ale nie sú prítomné v tejto tabuľke VST, keďže tabuľka BST požaduje iba AID = 2. Pole „Aplikácie“ obsahuje zoznam podporovaných inštancií aplikácií v zariadení *DSRC – VU*. Pre každú konkretizáciu podporovanej aplikácie sa uvedie odkaz na príslušnú normu, vytvorený z kontextovej značky RTM, ktorá pozostáva z identifikátora objektu (OBJECT IDENTIFIER) predstavujúceho súvisiacu normu, jej časť (9 pre RTM) a prípadne jej verziu a z identifikátora prvku (EID), ktorý je generovaný zariadením DSRC – VU a súvisí s danou inštanciou aplikácie.

Praktický príklad nastavení špecifikovaných v tabuľke 14.8 s označením bitového kódovania je uvedený v tabuľke 14.9.

Tabuľka 14.9

Inicializácia – príklad obsahu rámca VST

Oktet č.	Atribút/pole	Bity v oktete	Opis
1	FLAG	0111 1110	Príznak začiatku
2	Private LID	xxxx xxxx	Adresa spojenia konkrétneho DSRC – VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	PDU príkazu
7	LLC Control field	0000 0011	Príkaz UI
8	Fragmentation header	1xxx x001	Bez fragmentácie
9	VST SEQUENCE {	1001	Odpoveď inicializácie
	Fill BIT STRING (SIZE(4))	0000	Nepoužité a nastavené na 0.
10	Profile INTEGER (0..127,…) Applications SEQUENCE OF {	0000 0000	Bez rozšírenia. Príklad profilu 0
11		0000 0001	Bez rozšírenia, 1 aplikácia
12	SEQUENCE {		
	OPTION indicator	1	Identifikátor EID prítomný
	OPTION indicator	1	Parameter prítomný
	AID DSRCApplicationEntityID	00 0010	Bez rozšírenia. AID= 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Vymedzené v OBU, identifikuje inštanciu aplikácie.

Oktet č.	Atribút/pole	Bity v oktete	Opis
14	Parameter Container {	0000 0010	Bez rozšírenia, voľba kontajnera = 02, oktetový reťazec
15		0000 1000	Bez rozšírenia, dĺžka kontextovej značky RTM = 8
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	Identifikátor objektu podporovanej normy, časti a verzie. Príklad: ISO (1) norma (0) TARV (15638) časť 9 (9) verzia 1 (1). Prvý oktet 06H je identifikátor objektu, druhý oktet 06H je jeho dĺžka. Nasledujúcich 6 oktetov kóduje príklad identifikátora objektu Upozorňujeme, že je prítomný iba jeden prvok sekvencie (voliteľný prvok RtmCommProfile sa vynecháva)
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 neprítomný
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Identifikátor výrobcu DSRC – VU podľa registra v ISO 14816
27		xxxx xxxx	
28	FCS	xxxx xxxx	Kontrolný súčet rámca
29		xxxx xxxx	
30	Flag	0111 1110	Príznak ukončenia

DCS_49 Snímač REDCR potom zosníma údaje vyslaním príkazu GET, ktorý zodpovedá príkazu GET vymedzenému v norme EN 13372, oddieloch 6.2, 6.3, 6.4 a v norme EN 12834, s nastaveniami, ako sú špecifikované v tabuľke 14.10.

Tabuľka 14.10

Prezentácia – nastavenia rámca požiadavky GET

Pole	Nastavenia
Invoker Identifier (IID)	Neprítomný
Link Identifier (LID)	Adresa spojenia konkrétneho DSRC – VU
Chaining	Nie

Pole	Nastavenia
Element Identifier (EID)	Podľa VST. Bez rozšírenia
Access Credentials	Nie
AttributeIdList	Bez rozšírenia, 1 atribút, AttributeID = 1 (RtmData)
Fragmentation	Nie
Layer2 settings	PDU príkazu, pollovaný (polled) príkaz ACn

V tabuľke 14.11 je uvedený príklad čítania údajov RTM.

Tabuľka 14.11

Prezentácia – príklad rámca požiadavky GET

Oktet č.	Atribút/pole	Bity v oktete	Opis
1	FLAG	0111 1110	Príznak začiatku
2	Private LID	xxxx xxxx	Adresa spojenia konkrétneho DSRC – VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU príkazu
7	LLC Control field	n111 0111	Pollovaný príkaz ACn, n-bitový
8	Fragmentation header	1xxx x001	Bez fragmentácie
9	Get.request SEQUENCE {	0110	Požiadavka Get
	OPTION indicator	0	Prístupové oprávnenia neprítomné
	OPTION indicator	0	Identifikátor IID neprítomný
	OPTION indicator	1	AttributeIdList prítomný
	Fill BIT STRING(SIZE(1))	0	Nastavené na 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	EID inštancie aplikácie RTM podľa VST. Bez rozšírenia
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Bez rozšírenia, počet atribútov = 1
12		0000 0001	AttributeId=1, RtmData. Bez rozšírenia

Oktet č.	Atribút/pole	Bity v oktete	Opis
13	FCS	xxxx xxxx	Kontrolný súčet rámca
14		xxxx xxxx	
15	Flag	0111 1110	Príznak ukončenia

DSC_50 Zariadenie *DSRC – VU* po prijatí požiadavky GET posiela odpoveď GET s požadovanými údajmi, ktorá zodpovedá odpovedi GET vymedzenej v norme EN 13372, oddiele 6.2, 6.3, 6.4 a v norme EN 12834, s nastaveniami, ako sú špecifikované v tabuľke 14.12.

Tabuľka 14.12

Prezentácia – nastavenia rámca odpovede GET

Pole	Nastavenia
Invoker Identifier (IID)	Neprítomný
Link Identifier (LID)	Podľa normy EN 12834
Chaining	Nie
Element Identifier (EID)	Podľa VST.
Access Credentials	Nie
Fragmentation	Nie
Layer2 settings	PDU odpovede, odpoveď dostupná a príkaz akceptovaný, príkaz ACn

V tabuľke 14.13 je uvedený príklad čítania údajov RTM.

Tabuľka 14.13

Prezentácia – príklad obsahu rámca odpovede

Oktet č.	Atribút/pole	Bity v oktete	Opis
1	FLAG	0111 1110	Príznak začiatku
2	Private LID	xxxx xxxx	Adresa spojenia konkrétneho DSRC – VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	

Oktet č.	Atribút/pole	Bity v oktete	Opis
6	MAC Control field	1101 0000	PDU odpovede
7	LLC Control field	n111 0111	Odpoveď dostupná, príkaz ACn n-bitový
8	LLC Status field	0000 0000	Odpoveď dostupná a príkaz akceptovaný
9	Fragmentation header	1xxx x001	Bez fragmentácie
10	Get.response SEQUENCE {	0111	Odpoveď Get
	OPTION indicator	0	Identifikátor IID neprítomný
	OPTION indicator	1	Zoznam atribútov prítomný
	OPTION indicator	0	Stav návratu neprítomný
	Fill BIT STRING(SIZE(1))	0	Nepoužíva sa
11	EID INTEGER(0..127,…)	xxxx xxxx	Odpoveď inštancie aplikácie RTM. Bez rozšírenia,
12	AttributeList SEQUENCE OF {	0000 0001	Bez rozšírenia, počet atribútov = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Bez rozšírenia, AttributeId=1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Bez rozšírenia, voľba kontajnera = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Kontrolný súčet rámca
n+2		xxxx xxxx	
n+3	Flag	0111 1110	Príznak ukončenia

DSC_51 Snímač REDCR potom ukončí spojenie vydaním EVENT_REPORT, RELEASE v súlade s normou EN 13372, oddielom 6.2, 6.3, 6.4 a normou EN 12834 oddielom 7.3.8, bez konkrétnych nastavení RTM. V tabuľke 14.14 je uvedený príklad bitového kódovania príkazu RELEASE.

Tabuľka 14.14

Ukončenie. Obsah rámca EVENT_REPORT Release

Oktet č.	Atribút/pole	Bity v oktete	Opis
1	FLAG	0111 1110	Príznak začiatku
2	Private LID	xxxx xxxx	Adresa spojenia konkrétneho DSRC – VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1000 s000	Rámec obsahuje LPDU príkazu
7	LLC Control field	0000 0011	Príkaz UI
8	Fragmentation header	1xxx x001	Bez fragmentácie
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Prístupové oprávnenia neprítomné
	OPTION indicator	0	Parameter udalosti neprítomný
	OPTION indicator	0	Identifikátor IID neprítomný
	Mode BOOLEAN	0	Neočakáva sa odpoveď
10	EID INTEGER (0..127,…)	0000 0000	Bez rozšírenia, EID = 0 (systém)
11	EventType INTEGER (0..127,…) }	0000 0000	Typ udalosti 0 = Odpojenie (Release)
12	FCS	xxxx xxxx	Kontrolný súčet rámca
13		xxxx xxxx	
14	Flag	0111 1110	Príznak ukončenia

DSC_52 Od zariadenia *DSRC – VU* sa neočakáva žiadna odpoveď na príkaz Release. Komunikácia sa potom ukončí.

5.4.8 *Opis skúšobnej transakcie DSRC*

DSC_53 Úplné skúšky, ktoré zahŕňajú zabezpečenie údajov, musia vykonávať v súlade s dodatkom 11 Spoločné mechanizmy zabezpečenia oprávnené osoby s prístupom k postupom zabezpečenia, s použitím bežného príkazu GET opísaného vyššie.

DSC_54 Uvedenie do prevádzky a pravidelné kontrolné skúšky, ktoré si vyžadujú dekódovanie a porozumenie obsahu dekódovaných údajov, sa musia vykonávať v súlade s dodatkom 11 Spoločné mechanizmy zabezpečenia a dodatkom 9 – Typové schválenie – zoznam minimálne požadovaných skúšok.

Základná komunikácia DSRC sa však môže skúšať príkazom ECHO. Takéto skúšky sa môžu vyžadovať pri uvedení do prevádzky, pri pravidelnej kontrole alebo na požiadanie príslušného kontrolného orgánu, prípadne na základe požiadaviek nariadenia (EÚ) č. 165/2014 (pozri oddiel 6 nižšie).

DSC_55 Na vykonanie tejto základnej skúšky komunikácie vydá snímač REDCR príkaz ECHO počas relácie, t. j. po úspešnom ukončení inicializačnej fázy. Postupnosť interakcií je tak podobná ako pri snímaní:

— 1. krok Snímač *REDCR* posiela tabuľku prevádzkových režimov majáka (BST), ktorá zahŕňa identifikátory aplikácie (AID) na zozname podporovaných služieb. V aplikáciách RTM to bude jednoducho služba s hodnotou AID = 2.

Zariadenie *DSRC – VU* vyhodnotí prijatú tabuľku BST a ak zistí, že BST požaduje Freight&Fleet (AID = 2), odpovie. Ak snímač *REDCR* neponúka hodnotu AID = 2, zariadenie *DSRC – VU* ukončí transakciu so snímačom *REDCR*.

— 2. krok Zariadenie *DSRC – VU* posiela požiadavku na pridelenie súkromného okna.

— 3. krok Snímač REDCR posiela pridelenie súkromného okna.

— 4. krok Zariadenie *DSRC – VU* použije pridelené súkromné okno na odoslanie svojej tabuľky jednotky vozidla (VST). Táto tabuľka VST obsahuje zoznam všetkých jednotlivých konkretizácií aplikácie, ktoré toto zariadenie *DSRC – VU* podporuje v rámci AID = 2. Rôzne konkretizácie sa identifikujú pomocou jedinečných identifikátorov EID, z ktorých každý je spojený s hodnotou parametra označujúcou podporovanú inštanciu aplikácie.

— 5. krok Snímač *REDCR* ďalej analyzuje ponúkanú tabuľku VST a buď ukončí spojenie (RELEASE), keďže ho nezaujíma nič z ponuky VST (t. j. dostáva VST od zariadenia *DSRC – VU*, ktoré nie je RTM VU), alebo, ak dostane vhodnú tabuľku VST, začne konkretizáciu aplikácie.

— 6. krok Snímač *REDCR* vydá príkaz (ECHO) konkrétnemu zariadeniu *DSRC – VU* a pridelí súkromné okno.

— 7. krok Zariadenie *DSRC – VU* použije novo pridelené súkromné okno na odoslanie rámca odpovede na príkaz ECHO.

V nasledujúcich tabuľkách sú uvedené praktické príklady relácie výmeny ECHO.

DSC_56 Inicializácia sa vykonáva podľa 5.4.7 (DSC_44 – DSC_48) a tabuliek 14.4 – 14.9

DSC_57 Snímač REDCR potom vydá príkaz ACTION, ECHO podľa normy ISO 14906 so 100 oktetmi údajov a bez konkrétnych nastavení pre RTM. V tabuľke 14.15 je uvedený obsah rámca odoslaného snímačom REDCR.

Tabuľka 14.15

Príklad rámca požiadavky ACTION, ECHO

Oktet č.	Atribút/pole	Bity v oktete	Opis
1	FLAG	0111 1110	Príznak začiatku
2	Private LID	xxxx xxxx	Adresa spojenia konkrétneho DSRC – VU
3		xxxx xxxx	

Oktet č.	Atribút/pole	Bity v oktete	Opis
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU príkazu
7	LLC Control field	n111 0111	Pollovaný príkaz ACn, n-bitový
8	Fragmentation header	1xxx x001	Bez fragmentácie
9	ACTION.request SEQUENCE {	0000	Činnosť – požiadavka (ECHO)
	OPTION indicator	0	Prístupové oprávnenia neprítomné
	OPTION indicator	1	Parameter činnosti prítomný
	OPTION indicator	0	Identifikátor IID neprítomný
	Mode BOOLEAN	1	Očakáva sa odpoveď.
10	EID INTEGER (0..127,…)	0000 0000	Bez rozšírenia, EID = 0 (systém)
11	ActionType INTEGER (0..127,…)	0000 1111	Bez rozšírenia, požiadavka na typ činnosti ECHO
12	ActionParameter CONTAINER {	0000 0010	Bez rozšírenia, voľba kontajnera = 2
13		0110 0100	Bez rozšírenia. Dĺžka reťazca = 100 oktetov
14		xxxx xxxx	Údaje, ktoré sa majú odraziť
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Kontrolný súčet rámca
115		xxxx xxxx	
116	Flag	0111 1110	Príznak ukončenia

DSC_58 Zariadenie *DSRC – VU* po prijatí požiadavky ECHO posiela odpoveď ECHO so 100 oktetmi údajov, ktorá odráža prijatý príkaz, podľa normy ISO 14906, bez konkrétnych nastavení RTM. V tabuľke 14.16 je uvedený príklad kódovania na bitovej úrovni.

Tabuľka 14.16

Príklad rámca odpovede ACTION, ECHO

Oktet č.	Atribút/pole	Bity v oktete	Opis
1	FLAG	0111 1110	Príznak začiatku
2	Private LID	xxxx xxxx	Adresa spojenia konkrétnej VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU odpovede
7	LLC Control field	n111 0111	Príkaz ACn, n-bitový
8	LLC status field	0000 0000	Odpoveď dostupná
9	Fragmentation header	1xxx x001	Bez fragmentácie
10	ACTION.response SEQUENCE {	0001	Činnosť – odpoveď (ECHO)
	OPTION indicator	0	Identifikátor IID neprítomný
	OPTION indicator	1	Parameter odpovede prítomný
	OPTION indicator	0	Stav návratu neprítomný
	Fill BIT STRING (SIZE (1))	0	Nepoužíva sa
11	EID INTEGER (0..127,…)	0000 0000	Bez rozšírenia, EID = 0 (systém)
12	ResponseParameter CONTAINER {	0000 0010	Bez rozšírenia, voľba kontajnera = 2
13		0110 0100	Bez rozšírenia. Dĺžka reťazca = 100 oktetov
14		xxxx xxxx	Odrazené údaje
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Kontrolný súčet rámca
115		xxxx xxxx	
116	Flag	0111 1110	Príznak ukončenia

5.5 **Podpora smernice 2015/71/ES**

5.5.1 *Prehľad*

DSC_59 V záujme podpory smernice 2015/719/EÚ o maximálnej hmotnosti a najväčších rozmeroch ťažkých nákladných vozidiel bude transakčný protokol na sťahovanie údajov palubného vážiaceho systému (OWS) prostredníctvom spojenia s rozhraním DSRC 5,8 GHz rovnaký ako protokol používaný pre údaje aplikácie RTM (pozri 5.4.1) –jediným rozdielom je, že identifikátor objektu, ktorý súvisí s normou TARV, sa bude týkať normy ISO 15638 (TARV) časti 20 súvisiacej s WOB/OWS.

5.5.2 *Príkazy*

DSC_60 Príkazy používané na transakciu OWS budú rovnaké ako príkazy používané na transakciu RTM.

5.5.3 *Postupnosť príkazov snímania*

DSC_61 Postupnosť príkazov snímania údajov OWS bude rovnaká ako pri údajoch RTM.

5.5.4 *Štruktúry údajov*

DSC_62 Obsah (údaje OWS) pozostáva zo zreťazenia

1. údajov EncryptedOwsPayload, ktoré sú kódovaním údajov OwsPayload vymedzených v ASN.1 oddiele 5.5.5. Spôsob kódovania je rovnaký ako spôsob prijatý pre RtmData, ktorý je špecifikovaný v dodatku 11,

2. údajov DSRCSecurityData vypočítaných podľa rovnakých algoritmov, aké boli prijaté pre RtmData, ktoré sú špecifikované v dodatku 11.

5.5.5 *Modul ASN.1 pre transakciu OWS DSRC*

DSC_63. Modul ASN.1 pre údaje DSRC v rámci aplikácie RTM je vymedzený takto:

```
   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 *Prvky OwsData, vykonávané činnosti a vymedzenie pojmov*

Prvky OwsData sú vymedzené tak, aby podporovali smernicu 2015/719/EÚ o maximálnej hmotnosti a najväčších rozmeroch ťažkých nákladných vozidiel. Ich význam je:

— recordedWeight predstavuje celkovú nameranú hmotnosť ťažkého nákladného vozidla s rozlíšením 10 kg, ako je vymedzené v norme EN ISO 14906. Napríklad hodnota 2 500 predstavuje hmotnosť 25 ton.

— axlesConfiguration predstavuje konfiguráciu ťažkého nákladného vozidla podľa počtu náprav. Konfigurácia je vymedzená s bitovou maskou 20 bitov (prevzatou z normy EN ISO 14906).

Bitová maska 2 bity predstavuje konfiguráciu nápravy v tomto formáte:

— Hodnota 00B znamená, že hodnota je „nedostupná“, pretože vozidlo nemá vybavenie na získanie hmotnosti na danej náprave.

— Hodnota 01B znamená, že daná náprava nie je prítomná.

— Hodnota 10B znamená, že náprava je prítomná a že hmotnosť sa vypočítala, získala a poskytla v poli axlesRecordedWeight.

— Hodnota 11B je vyhradená na budúce použitie.

Posledné 4 bity sú vyhradené na budúce použitie (RFU).

Počet náprav										
Počet náprav na ťahači			Počet náprav na prípojnom vozidle							
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 bity)

— axlesRecordedWeight predstavuje zaznamenanú špecifickú hmotnosť na každú nápravu s rozlíšením 10 kg. Na každú nápravu sa použijú dva oktety. Napríklad hodnota 150 predstavuje hmotnosť 1 500 kg.

Ostatné dátové typy sú vymedzené v odseku 5.4.5.

5.5.7 *Mechanizmy prenosu údajov*

DSC_64 Mechanizmus prenosu údajov medzi snímačom a zariadením DSRC vo vozidle je rovnaký pre údaje OWS ako pre údaje RTM (pozri 5.4.6).

DSC_65 Prenos údajov medzi platformou na zhromažďovanie údajov o maximálnej hmotnosti a zariadením DSRC vo vozidle je založený na fyzickom prepojení a na rozhraniach a protokoloch vymedzených v oddiele 5.6.

5.6 **Prenos údajov medzi DSRC – VU a VU**

5.6.1 *Fyzické prepojenie a rozhrania*

DSC_66 Prepojenie medzi *VU* a zariadením *DSRC – VU* sa môže zabezpečiť buď fyzickým káblom, alebo bezdrôtovou komunikáciou krátkeho dosahu založenou na systéme Bluetooth v4.0 BLE.

DSC_67 Bez ohľadu na voľbu fyzického prepojenia a rozhrania musia byť splnené tieto požiadavky:

DSC_68 a) Aby sa dali VU a zariadenia DSRC – VU, alebo aj rôzne šarže DSRC – VU kupovať od rôznych dodávateľov, prepojenie medzi VU a zariadením DSRC – VU musí byť otvoreným štandardným prepojením. VU sa so zariadením DSRC – VU prepojí niektorou z týchto možností:

i) pomocou pevného kábla dĺžky aspoň 2 metre so schváleným priamym 11-pólovým zástrčkovým konektorom DIN 41612 H11 zo strany zariadenia DSRC – VU, ktorý sa zasunie do podobného schváleného zásuvkového konektora ISO/DIN zo strany zariadenia VU;

ii) prostredníctvom nízkoenergetického systému Bluetooth (BLE);

iii) pomocou štandardného prepojenia podľa noriem ISO 11898 alebo SAE J1939;

DSC_69 b) vymedzenie rozhraní a prepojenia medzi VU a zariadením DSRC – VU musí podporovať príkazy aplikačného protokolu stanovené v odseku 5.6.2 a

DSC_70 c) VU a zariadenie DSRC – VU musia podporovať prenos údajov prepojením z hľadiska prevádzkovej výkonnosti aj napájania.

5.6.2 *Aplikačný protokol*

DSC_71 Aplikačný protokol medzi zariadením diaľkovej komunikácie VU a zariadením DSRC – VU je zodpovedný za pravidelný prenos údajov diaľkovej komunikácie z VU do DSRC.

DSC_72 Vymedzené sú tieto základné príkazy:

1. Inicializácia komunikačného spojenia – Požiadavka
2. Inicializácia komunikačného spojenia – Odpoveď
3. Poslať údaje s identifikátorom aplikácie RTM a obsahom vymedzeným údajmi RTM
4. Potvrdenie údajov
5. Ukončenie komunikačného spojenia – Požiadavka
6. Ukončenie komunikačného spojenia – Odpoveď

DSC_73 V ASN1.0 môžu byť uvedené príkazy vymedzené ako:

```
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 Opis príkazov a parametrov:

— RCDT-Communication Link Initialization – Request sa používa na inicializáciu komunikačného spojenia. Príkaz posiela VU zariadeniu DSRC – VU. VU nastaví identifikátor LinkIdentifier a oznámi ho zariadeniu DSRC – VU, aby bolo možné sledovať konkrétne komunikačné spojenie.

(Poznámka: ide o podporu budúcich spojení a iných aplikácií/modulov, ako je napríklad palubné váženie).

— RCDT-Communication Link Initialization – Response používa zariadenie DSRC – VU na poskytnutie odpovede na požiadavku inicializácie komunikačného spojenia. Príkaz posiela zariadenie DSRC – VU zariadeniu VU. Príkaz poskytuje výsledok inicializácie ako odpoveď = 1 (úspešné) alebo = 0 (neúspešné).

DSC_75 Inicializácia komunikačného spojenia sa vykoná až po inštalácii, kalibrácii a po spustení motora/VU.

— RCDT-Send Data používa VU na odoslanie podpísaných údajov RCDTData (t. j. *údajov diaľkovej komunikácie*) zariadeniu DSRC – VU. Údaje sa posielajú každých 60 sekúnd. Parameter DataTransactionId identifikuje konkrétny prenos údajov. Používa sa aj identifikátor LinkIdentifier na zabezpečenie správnosti príslušného spojenia.

— RCDT-Data Acknowledgment posiela zariadenie DSRC – VU ako spätnú väzbu pre VU o prijatí údajov odoslaných príkazom RCDT-Send Data , ktorý identifikuje parameter DataTransactionId. Parameter odpovede je = 1 (úspešné) alebo = 0 (neúspešné). Ak VU dostane viac ako tri odpovede rovné 0 alebo ak VU nedostane potvrdenie RCDT-Data Acknowledgment pre určité už odoslané údaje RCDT-Send Data s konkrétnym parametrom DataTransactionId, vygeneruje a zaznamená udalosť.

— RCDT-Communication Link Termination request posiela VU zariadeniu DSRC – VU na ukončenie spojenia pre konkrétny identifikátor LinkIdentifier.

DSC_76 Pri reštartovaní zariadenia DSRC – VU alebo VU by sa mali prerušiť všetky existujúce komunikačné spojenia, keďže v dôsledku náhleho vypnutia VU by mohli spojenia zostať neukončené.

— RCDT-Communication Link Termination – Response posiela zariadenie DSRC – VU zariadeniu VU na potvrdenie požiadavky VU na ukončenie spojenia pre konkrétny identifikátor LinkIdentifier.

5.7 **Spracovanie chýb**

5.7.1 *Zaznamenávanie a oznamovanie údajov v DSRC – VU*

DSC_77 Už zabezpečené *údaje* sa poskytujú zariadeniu *DSRC – VU* prostredníctvom funkcie modulu zabezpečenia (*VUSM*). Modul *VUSM* overuje, či sa údaje zaznamenali v zariadení *DSRC – VU* správne. Zaznamenávanie a hlásenie prípadných chýb v prenose údajov z *VU* do pamäte zariadenia *DSRC – VU* sa zaznamená ako typ EventFaultType s hodnotou enum nastavenou na '62'H Chyba komunikácie diaľkového komunikačného zariadenia, spolu s časovou pečiatkou.

DSC_78 *VU* uchová súbor s jedinečným názvom, ktorý kontrolóri ľahko identifikujú na účely zaznamenania „interných komunikačných porúch VU".

DSC_79 Ak sa pamäť VUPM pokúša získať údaje VU z modulu zabezpečenia (aby ich poskytla VU-DSRC), ale neúspešne, zaznamená poruchu ako typ EventFaultType s hodnotou enum nastavenou na *'62'H Chyba komunikácie diaľkového komunikačného zariadenia*, spolu s časovou pečiatkou. Zlyhanie komunikácie sa zaznamená, ak správa RCDT Data Acknowledgment k príslušnému príkazu RCDT Send Data (t. j. Správy Send Data a Acknowledgment s rovnakým DataTransactionId) nie je prijatá viac ako trikrát po sebe.

5.7.2 *Chyby bezdrôtovej komunikácie*

DSC_80 Spracovanie chýb komunikácie musí byť v súlade so súvisiacimi normami DSRC, konkrétne EN 300 674-1, EN 12253, EN 12795, EN 12834 a príslušnými parametrami normy EN 13372.

5.7.2.1 *Chyby kódovania a podpisu*

DSC_81 Chyby kódovania a podpisu sa spracúvajú podľa dodatku 11 Spoločné mechanizmy zabezpečenia a nevyskytujú sa v žiadnych chybových správach súvisiacich s prenosom údajov DSRC.

5.7.2.2 *Zaznamenávanie chýb*

Médium DSRC je dynamická bezdrôtová komunikácia v prostredí s nestálymi atmosférickými a interferenčnými podmienkami, predovšetkým v kombináciách prenosných snímačov REDCR a pohybujúcich sa vozidiel, ktoré táto aplikácia zahŕňa. Preto je dôležité vymedziť rozdiel medzi „zlyhaním snímania“ a „chybou“. V prípade transakcie prostredníctvom bezdrôtového rozhrania je zlyhanie snímania bežné a zväčša sa rieši opakovaným pokusom, t. j. opätovné vysielanie tabuľky BST a opakovaný pokus o vykonanie sekvencie, čo vo väčšine prípadov vedie k úspešnému nadviazaniu komunikácie a prenosu údajov, pokiaľ sa cieľové vozidlo v čase potrebnom na opätovné vysielanie nepresunie mimo dosah. („Úspešné snímanie“ si môže vyžadovať viacero opakovaných pokusov.)

Príčinou zlyhania snímania môže byť nesprávne spárovanie antén (zlyhanie „zacielenia“); tienenie niektorej z antén – to môže byť úmyselné, ale aj zavinené fyzickou prítomnosťou iného vozidla; rušenie rádiových vĺn, predovšetkým od WIFI cca 5,8 GHz alebo iných verejných prostriedkov bezdrôtovej komunikácie, radarové rušenie alebo nepriaznivé atmosférické podmienky (napr. počas búrky); alebo jednoducho presun vozidla mimo dosah komunikácie DSRC. Jednotlivé prípady zlyhaní snímania sa z princípu nemôžu zaznamenať, jednoducho preto, že ku komunikácii nedošlo.

Ak sa však zástupca príslušného kontrolného orgánu zameria na určité vozidlo a pokúša sa snímať jeho zariadenie *DSRC – VU*, ale nedôjde k úspešnému prenosu údajov, toto zlyhanie by mohlo byť dôsledkom úmyselnej manipulácie, a preto zástupca príslušného kontrolného orgánu potrebuje prostriedok na zaznamenanie zlyhania a upozornenie kolegov na ďalších stanovištiach, že môže ísť o porušenie predpisov. Kolegovia môžu potom vozidlo zastaviť a vykonať fyzickú kontrolu. Keďže však nedošlo k úspešnej komunikácii, DSRC-VU nemôže poskytnúť o zlyhaní údaje. Takého hlásenie musí preto vychádzať z technického riešenia zariadenia REDCR.

„Zlyhanie snímania“ je technicky odlišné od „chyby“. „Chyba“ v tejto súvislosti znamená získanie nesprávnej hodnoty.

Údaje prenášané do zariadenia *DSRC – VU* sa poskytujú už zabezpečené, preto musia byť overené poskytovateľom údajov (pozri oddiel 5.4).

Údaje následne prenášané prostredníctvom bezdrôtového rozhrania podliehajú kontrole cyklickým kódom (CRC) na komunikačnej úrovni. Ak kontrola CRC údaje potvrdí, potom sú správne. Ak kontrola CRC údaje nepotvrdí, opätovne sa vysielajú. Pravdepodobnosť, že nesprávne údaje by mohli úspešne prejsť kontrolou CRC, je štatisticky taká nízka, že ju možno zanedbať.

Ak kontrola CRC údaje nepotvrdí a nie je čas na opätovné vysielanie a prijímanie správnych údajov, výsledkom nebude chyba, ale výskyt osobitného typu zlyhania snímania.

Jediným zmysluplným údajom o „zlyhaní“, ktorý sa dá zaznamenať, je počet prípadov úspešného spustenia transakcie, ktoré neviedlo k úspešnému prenosu údajov do snímača REDCR.

DSC_82 Snímač *REDCR* preto zaznamená s časovou pečiatkou počet prípadov, keď „inicializačná“ fáza snímania DSRC bola úspešná, ale transakcia bola ukončená skôr, než snímač REDCR úspešne získal *údaje*. Tieto údaje sú k dispozícii zástupcovi príslušného kontrolného orgánu a ukladajú sa do pamäte zariadenia REDCR. Prostriedky na dosiahnutie tohto cieľa sú vecou technického riešenia zariadenia alebo špecifikácie príslušného kontrolného orgánu.

Jediným zmysluplným údajom o „chybe“, ktorý sa dá zaznamenať, je počet prípadov, keď snímač REDCR nedokázal dekódovať prijaté *údaje*. Treba však poznamenať, že tento údaj sa týka iba účinnosti softvéru snímača REDCR. Môže sa stať, že údaje sa technicky dekódujú, ale nebudú dávať sémantický zmysel.

DSC_83 Snímač *REDCR* preto zaznamená s časovou pečiatkou počet prípadov, keď sa neúspešne pokúšal dešifrovať údaje získané prostredníctvom rozhrania DSRC.

6 UVEDENIE DO PREVÁDZKY A PRAVIDELNÉ KONTROLNÉ SKÚŠKY FUNKCIE DIAĽKOVEJ KOMUNIKÁCIE

6.1 **Všeobecné**

DSC_84 Pre funkciu diaľkovej komunikácie sa počíta s dvoma typmi skúšok:

1) Skúška ECHO na overenie komunikačného kanála *DSRC-REDCR* >>-:-<*DSRC-VU wireless*.
2) Skúška zabezpečenia celého systému, aby sa zaistilo, že dielenská karta má prístup k obsahu zakódovaných a podpísaných údajov, ktoré boli vytvorené vo VU a prenášané bezdrôtovým komunikačným kanálom.

6.2 **ECHO**

Tento oddiel obsahuje ustanovenia konkrétne určené na preskúšanie, či je kanál *DSRC-REDCR* >>-:-<*DSRC-VU* funkčne aktívny.

Cieľom príkazu ECHO je umožniť dielňam alebo skúšobným zariadeniam pre typové schvaľovanie preskúšať, či spojenie DSRC funguje, bez potreby prístupu k oprávneniam zabezpečenia. Skúšobné zariadenie preto musí byť schopné iba inicializovať komunikáciu DSRC (odoslaním tabuľky BST s hodnotou AID = 2) a potom poslať príkaz ECHO; ak DSRC funguje, skúšobné zariadenie dostane odpoveď na príkaz ECHO. Podrobnosti sú uvedené v odseku 5.4.8. Ak túto odpoveď prijme správne, spojenie DSRC (*DSRC-REDCR* >>-:-<*DSRC-VU*) sa môže hodnotiť ako správne fungujúce.

6.3 **Skúšky na potvrdenie zabezpečeného obsahu údajov**

DSC_85 Táto skúška sa vykonáva na potvrdenie zabezpečenia toku údajov v celom systéme. Na takúto skúšku je potrebný skúšobný snímač DSRC. Skúšobný snímač DSRC vykonáva rovnaké funkcie a je vyhotovený s rovnakými špecifikáciami ako snímač, ktorý používajú kontrolné orgány, s tým rozdielom, že na overenie používateľa skúšobného snímača DSRC sa používa dielenská karta namiesto kontrolnej karty. Skúška sa môže vykonať po počiatočnej aktivácii inteligentného tachografu alebo na konci postupu kalibrácie. Jednotka vozidla po aktivácii vygeneruje a oznámi DSRC-VU zabezpečené údaje včasnej detekcie.

DSC_86 Pracovník dielne musí umiestniť skúšobný snímač DSRC pred vozidlo do vzdialenosti 2 až 10 metrov.

DSC_87 Potom pracovník dielne vloží dielenskú kartu do skúšobného snímača DSRC, čím požiada jednotku vozidla o snímanie údajov včasnej detekcie. Po úspešnom snímaní pracovník dielne otvorí prijaté údaje a uistí sa, že bola úspešne overená ich integrita a boli dekódované.

Dodatok 15

PRECHOD: RIADENIE KOEXISTENCIE JEDNOTLIVÝCH GENERÁCIÍ ZARIADENIA

OBSAH

1. VYMEDZENIE POJMOV 497

2. VŠEOBECNÉ USTANOVENIA 497

2.1. Prehľad prechodu 497

2.2. Interoperabilita medzi VU a kartami 498

2.3. Interoperabilita medzi jednotkou vozidla a snímačom pohybu 498

2.4. Interoperabilita medzi jednotkou vozidla, tachografovými kartami a zariadením na sťahovanie údajov 498

2.4.1 Priame sťahovanie z karty prostredníctvom inteligentného vyhradeného zariadenia 498

2.4.2 Sťahovanie z karty prostredníctvom jednotky vozidla 499

2.4.3 Sťahovanie z jednotky vozidla 499

2.5. Interoperabilita medzi jednotkou vozidla a kalibračným zariadením 499

3. ZÁKLADNÉ OPATRENIA POČAS OBDOBIA PRED TERMÍNOM ZAVEDENIA 499

4. USTANOVENIA NA OBDOBIE PO TERMÍNE ZAVEDENIA 499

1. VYMEDZENIE POJMOV

Na účely tohto dodatku sa používa toto vymedzenie pojmov:

systém inteligentného tachografu: podľa vymedzenia v tejto prílohe (kapitola 1: vymedzenie bbb),

systém tachografu prvej generácie: podľa vymedzenia v tomto nariadení (článok 2: vymedzenie v bode 1);

systém tachografu druhej generácie: podľa vymedzenia v tomto nariadení (článok 2: vymedzenie v bode 7);

termín zavedenia: podľa vymedzenia v tejto prílohe (kapitola 1: pojem ccc),

inteligentné vyhradené zariadenie (Inteligent Dedicated Equipment – IDE): zariadenie používané na sťahovanie údajov, ako je vymedzené v dodatku 7 tejto prílohy.

2. VŠEOBECNÉ USTANOVENIA

2.1. **Prehľad prechodu**

V preambule tejto prílohy je uvedený prehľad prechodu medzi tachografovými systémami prvej a druhej generácie.

Na doplnenie k ustanoveniam tejto preambuly:

— snímače pohybu prvej generácie nebudú interoperabilné s jednotkami vozidla druhej generácie,

— inštalácia snímačov pohybu druhej generácie do vozidiel sa začne v rovnakom čase ako inštalácia jednotiek vozidla druhej generácie,

— zariadenia na sťahovanie údajov a kalibráciu sa budú musieť vyvíjať tak, aby podporovali používanie obidvoch generácií záznamových zariadení a tachografových kariet.

2.2. **Interoperabilita medzi VU a kartami**

Je zrejmé, že tachografové karty prvej generácie sú interoperabilné s jednotkami vozidla prvej generácie (v súlade s prílohou 1B k tomuto nariadeniu), zatiaľ čo tachografové karty druhej generácie sú interoperabilné s jednotkami vozidla druhej generácie (v súlade s prílohou 1C k tomuto nariadeniu). Okrem toho sa uplatňujú tieto požiadavky:

MIG_001 Okrem toho, čo je stanovené v požiadavkách MIG_004 a MIG_005, tachografové karty prvej generácie sa až do skončenia svojej platnosti môžu naďalej používať v jednotkách vozidla druhej generácie. Držitelia však môžu požiadať o ich nahradenie tachografovými kartami druhej generácie, hneď ako budú dostupné.

MIG_002 Jednotky vozidla druhej generácie musia byť schopné používať každú vloženú platnú kartu vodiča, kontrolnú kartu a podnikovú kartu prvej generácie.

MIG_003 Táto schopnosť sa môže v takýchto jednotkách vozidla v dielni raz a navždy eliminovať tak, že tachografové karty prvej generácie sa už viac nebudú akceptovať. To bude možné realizovať až keď Európska komisia zavedie postup umožňujúci požiadať dielne o vykonanie tohto zásahu, napríklad počas každej pravidelnej kontroly tachografu.

MIG_004 Jednotky vozidla druhej generácie musia byť schopné používať iba dielenské karty druhej generácie.

MIG_005 Jednotky vozidla druhej generácie pri určovaní prevádzkového režimu berú do úvahy iba typy vložených platných kariet, bez ohľadu na ich generáciu.

MIG_006 Každá platná tachografová karta druhej generácie sa musí dať použiť v jednotkách vozidla prvej generácie presne rovnakým spôsobom ako tachografová karta druhej generácie toho istého typu.

2.3. **Interoperabilita medzi jednotkou vozidla a snímačom pohybu**

Je zrejmé, že snímače pohybu prvej generácie sú interoperabilné s jednotkami vozidla prvej generácie, zatiaľ čo snímače pohybu druhej generácie sú interoperabilné s jednotkami vozidla druhej generácie. Okrem toho sa uplatňujú tieto požiadavky:

MIG_007 Jednotky vozidla druhej generácie sa nebudú môcť spájať a používať so snímačmi pohybu prvej generácie.

MIG_008 Snímače pohybu druhej generácie sa môžu spájať a používať buď iba s jednotkami vozidla druhej generácie, alebo s jednotkami vozidla obidvoch generácií.

2.4. **Interoperabilita medzi jednotkou vozidla, tachografovými kartami a zariadením na sťahovanie údajov**

MIG_009 Zariadenie na sťahovanie údajov sa môže používať buď iba s jednotkami vozidla a tachografovými kartami jednej generácie, alebo obidvoch generácií.

2.4.1 *Priame sťahovanie z karty prostredníctvom inteligentného vyhradeného zariadenia*

MIG_010 Údaje sa prostredníctvom inteligentného vyhradeného zariadenia (IDE) sťahujú z tachografových kariet jednej generácie, vložených do svojich čítacích zariadení, s použitím bezpečnostných mechanizmov a protokolov sťahovania údajov tejto generácie, pričom sťahované údaje musia mať formát určený pre danú generáciu.

MIG_011 S cieľom umožniť kontrolu vodičov aj kontrolnými orgánmi mimo EÚ musí byť možné stiahnuť údaje z kariet vodiča (a dielenských kariet) druhej generácie presne rovnakým spôsobom ako z kariet vodiča (a dielenských kariet) prvej generácie. Také sťahovanie musí zahŕňať:

— nepodpísané elementárne súbory `IC` a `ICC`,

— nepodpísané EF (prvej generácie) `Card_Certificate` a `CA_Certificate`,

— ďalšie aplikačné dátové EF [v rámci vyhradeného súboru (DF) TACHO], ktoré si vyžaduje protokol sťahovania údajov z karty prvej generácie. Tieto informácie musia byť zabezpečené digitálnym podpisom v súlade s bezpečnostnými mechanizmami prvej generácie.

Takéto sťahovanie nezahŕňa aplikačné dátové EF prítomné iba na kartách vodiča (a dielenských kartách) druhej generácie (aplikačné dátové EF v rámci DF TACHO_G2).

2.4.2 *Sťahovanie z karty prostredníctvom jednotky vozidla*

MIG_012 Z karty druhej generácie vloženej v jednotke vozidla prvej generácie sa údaje sťahujú s použitím protokolu sťahovania údajov prvej generácie. Karta musí odpovedať na príkazy jednotky vozidla presne rovnakým spôsobom ako karta prvej generácie a sťahované údaje musia mať rovnaký formát ako údaje sťahované z karty prvej generácie.

MIG_013 Z karty prvej generácie vloženej v jednotke vozidla druhej generácie sa údaje sťahujú s použitím protokolu sťahovania údajov vymedzeného v dodatku 7 tejto prílohy. Jednotka vozidla musí posielať príkazy karte presne rovnakým spôsobom ako jednotka vozidla prvej generácie a sťahované údaje musia zachovávať formát určený pre karty prvej generácie.

2.4.3 *Sťahovanie z jednotky vozidla*

MIG_014 Z jednotiek vozidla druhej generácie sa údaje sťahujú s použitím bezpečnostných mechanizmov druhej generácie a protokolu sťahovania údajov špecifikovaného v dodatku 7 tejto prílohy.

MIG_015 S cieľom umožniť kontrolu vodičov aj kontrolnými orgánmi mimo EÚ a sťahovanie údajov z jednotiek vozidla aj v dielňach mimo EÚ sa môže poskytnúť voliteľná možnosť sťahovať údaje z jednotiek vozidla druhej generácie s použitím bezpečnostných mechanizmov prvej generácie a protokolu sťahovania údajov prvej generácie. Sťahované údaje musia mať rovnaký formát ako údaje sťahované z jednotky vozidla prvej generácie. Táto možnosť sa môže zvoliť prostredníctvom príkazov v menu.

2.5. **Interoperabilita medzi jednotkou vozidla a kalibračným zariadením**

MIG_016 Kalibračné zariadenie musí byť schopné vykonať kalibráciu všetkých generácií tachografu s použitím kalibračného protokolu príslušnej generácie. Kalibračné zariadenie sa môže používať buď pre tachograf jednej generácie, alebo obidvoch generácií.

3. ZÁKLADNÉ OPATRENIA POČAS OBDOBIA PRED TERMÍNOM ZAVEDENIA

MIG_017 Skúšobné kľúče a osvedčenia musia mať výrobcovia k dispozícii najneskôr **30 mesiacov** pred termínom zavedenia.

MIG_018 Skúšky interoperability musia byť pripravené, ak o ne výrobcovia požiadajú, najneskôr **15 mesiacov** pred termínom zavedenia.

MIG_019 Úradné kľúče a osvedčenia musia mať výrobcovia k dispozícii najneskôr **12 mesiacov** pred termínom zavedenia.

MIG_020 Členské štáty musia byť schopné vydať dielenské karty druhej generácie najneskôr **tri mesiace** pred termínom zavedenia.

MIG_021 Členské štáty musia byť schopné vydať všetky typy tachografových kariet druhej generácie najneskôr **jeden mesiac pred termínom zavedenia.**

4. USTANOVENIA NA OBDOBIE PO TERMÍNE ZAVEDENIA

MIG_022 Po termíne zavedenia musia členské štáty vydávať už iba tachografové karty druhej generácie.

MIG_023 Výrobcovia jednotiek vozidla/snímačov pohybu majú povolené vyrábať jednotky vozidla/snímače pohybu prvej generácie tak dlho, kým sa budú používať v praxi, aby bolo možné vymieňať nesprávne fungujúce komponenty.

MIG_024 Výrobcovia jednotiek vozidla/snímačov pohybu môžu požiadať o zachovanie typového schválenia jednotiek vozidla/snímačov pohybu prvej generácie tých typov, ktoré už mali udelené typové schválenie, a toto zachovanie sa im umožní.

Dodatok 16

ADAPTÉR PRE VOZIDLÁ KATEGÓRIÍ M1 A N1

OBSAH

1. SKRATKY A REFERENČNÉ DOKUMENTY 501
1.1. Skratky 501
1.2. Referenčné normy 501
2. VŠEOBECNÉ CHARAKTERISTICKY A FUNKCIE ADAPTÉRA3 502
2.1. Všeobecný opis adaptéra 502
2.2. Funkcie 502
2.3. Zabezpečenie 502
3. POŽIADAVKY NA ZÁZNAMOVÉ ZARIADENIE PO NAMONTOVANÍ ADAPTÉRA 502
4. KONŠTRUKČNÉ A FUNKČNÉ POŽIADAVKY NA ADAPTÉR 503
4.1. Prepojenie a úprava vstupných impulzov rýchlosti 503
4.2. Prívod vstupných impulzov do vstavaného snímača pohybu 503
4.3. Vstavaný snímač pohybu 503
4.4. Požiadavky na zabezpečenie 503
4.5. Výkonnostné parametre 504
4.6. Materiály 504
4.7. Označenia 504
5. MONTÁŽ ZÁZNAMOVÉHO ZARIADENIA PRI POUŽITÍ ADAPTÉRA 504
5.1. Montáž 504
5.2. Plombovanie 505
6. KONTROLY, INŠPEKCIE A OPRAVY 505
6.1. Pravidelné kontroly 505
7. TYPOVÉ SCHVÁLENIE ZÁZNAMOVÉHO ZARIADENIA PRI POUŽITÍ ADAPTÉRA 505
7.1. Všeobecne 505
7.2. Osvedčenie funkčnosti 506

1. SKRATKY A REFERENČNÉ DOKUMENTY

1.1. **Skratky**

TBD určí sa neskôr

VU jednotka vozidla

1.2. **Referenčné normy**

ISO16844-3 Cestné vozidlá. Tachografové systémy. Časť 3: Rozhranie snímača pohybu

2. VŠEOBECNÉ CHARAKTERISTICKY A FUNKCIE ADAPTÉRA

2.1. **Všeobecný opis adaptéra**

ADA_001 Adaptér musí pripojenej VU poskytnúť zabezpečené údaje o pohybe, ktoré neustále udávajú rýchlosť vozidla a prejdenú vzdialenosť.

Adaptér je určený len pre vozidlá, ktoré musia byť vybavené záznamovým zariadením podľa tohto nariadenia.

Montuje a používa sa iba v typoch vozidiel vymedzených v bode yy) („adaptér“) v prílohe 1C, ak nie je mechanicky možné namontovať žiaden iný typ existujúceho snímača pohybu, ktorý je inak v súlade s ustanoveniami tejto prílohy a jej dodatkov 1 až 16.

Adaptér sa nesmie mechanicky prepojiť s pohyblivou časťou vozidla; pripojí sa k impulzom rýchlosti a vzdialenosti, ktoré vytvárajú integrované senzory alebo alternatívne rozhrania.

ADA_002 Typovo schválený snímač pohybu (podľa ustanovení tejto prílohy 1C, oddielu 8 – Typové schválenie záznamového zariadenia a tachografových kariet) sa pripevní k puzdru adaptéra, ktoré zahŕňa aj zariadenie na konverziu impulzov, ktoré privádza vstupné impulzy do vstavaného snímača pohybu. Vstavaný snímač pohybu musí byť pripojený k VU, aby rozhranie medzi VU a adaptérom spĺňalo požiadavky normy ISO16844-3.

2.2. **Funkcie**

ADA_003 Adaptér musí zabezpečovať tieto funkcie:

— prepojenie a úprava vstupných impulzov rýchlosti,

— prívod vstupných impulzov do vstavaného snímača pohybu,

— všetky funkcie vstavaného snímača pohybu poskytujúce zabezpečené údaje o pohybe jednotke vozidla.

2.3. **Zabezpečenie**

ADA_004 Adaptér nepodlieha certifikácii zabezpečenia podľa požiadavky na všeobecné zabezpečenie snímača pohybu v zmysle dodatku 10 k tejto prílohe. Namiesto toho sa uplatňujú požiadavky na zabezpečenie uvedené v oddiele 4.4 tohto dodatku.

3. POŽIADAVKY NA ZÁZNAMOVÉ ZARIADENIE PO NAMONTOVANÍ ADAPTÉRA

Požiadavky v nasledujúcich kapitolách určujú, ako sa majú chápať požiadavky tejto prílohy pri používaní adaptéra. Príslušné čísla požiadaviek prílohy 1C sa uvádzajú v zátvorkách.

ADA_005 Záznamové zariadenie každého vozidla vybaveného adaptérom musí spĺňať všetky ustanovenia tejto prílohy, pokiaľ nie je v tomto dodatku uvedené inak.

ADA_006 Po namontovaní adaptéra zahŕňa záznamové zariadenie káble, adaptér (vrátane snímača pohybu) a VU [01].

ADA_007 Zisťovanie udalostí a/alebo porúch fungovania záznamového zariadenia sa upravuje takto:

— udalosť „prerušenie napájania“ spúšťa VU, ak nie je v režime kalibrácie, v prípade akéhokoľvek prerušenia napájania vstavaného snímača pohybu trvajúceho dlhšie ako 200 milisekúnd [79]

— udalosť „chyba údajov o pohybe“ spúšťa VU v prípade prerušenia normálneho toku údajov medzi vstavaným snímačom pohybu a VU a/alebo pri chybe integrity alebo autentifikácie údajov počas výmeny údajov medzi vstavaným snímačom pohybu a VU [83]

— udalosť „pokus o narušenie zabezpečenia“ spúšťa VU pri akejkoľvek inej udalosti ovplyvňujúcej zabezpečenie vstavaného snímača pohybu, ak nie je v režime kalibrácie [85]

— „Poruchu záznamového zariadenia“ spúšťa VU, ak nie je v režime kalibrácie, pri akejkoľvek poruche vstavaného snímača pohybu [88].

ADA_008 Poruchy adaptéra, ktoré dokáže záznamové zariadenie zistiť, súvisia so vstavaným snímačom pohybu [88].

ADA_009 Funkcia kalibrácie VU umožní automaticky spárovať vstavaný snímač pohybu s VU [202, 204].

4. KONŠTRUKČNÉ A FUNKČNÉ POŽIADAVKY NA ADAPTÉR

4.1. **Prepojenie a úprava vstupných impulzov rýchlosti**

ADA_011 Rozhranie vstupu adaptéra musí prijímať frekvenčné impulzy predstavujúce rýchlosť vozidla a prejdenú vzdialenosť. Elektrické charakteristiky vstupných impulzov: *Určí neskôr výrobca*. Úpravy dostupné len výrobcovi adaptéra a schválenej dielni vykonávajúcej montáž adaptéra musia podľa potreby umožňovať správne prepojenie vstupu adaptéra s vozidlom.

ADA_012 Rozhranie vstupu adaptéra musí podľa potreby umožniť násobenie alebo delenie frekvenčných impulzov vstupných impulzov rýchlosti určeným faktorom s cieľom upraviť signál na hodnotu v rozsahu faktora k definovanú v tejto prílohe (4 000 až 25 000 impulzov/km). Určený faktor môže naprogramovať iba výrobca adaptéra a schválená dielňa vykonávajúca montáž adaptéra.

4.2. **Prívod vstupných impulzov do vstavaného snímača pohybu**

ADA_013 Vstupné impulzy, ktoré sa môžu upraviť podľa uvedených ustanovení, sa privádzajú do vstavaného snímača pohybu tak, aby snímač pohybu zistil každý vstupný impulz.

4.3. **Vstavaný snímač pohybu**

ADA_014 Vstavaný snímač pohybu stimulujú privádzané impulzy, a tak môže vytvárať údaje o pohybe presne zodpovedajúce pohybu vozidla, ako keby bol mechanicky prepojený s pohyblivou časťou vozidla.

ADA_015 Identifikačné údaje vstavaného snímača pohybu použije VU na identifikáciu adaptéra [95].

ADA_016 Údaje o montáži uložené vo vstavanom snímači pohybu sa považujú za údaje o montáži adaptéra [122].

4.4. **Požiadavky na zabezpečenie**

ADA_017 Puzdro adaptéra musí byť navrhnuté tak, aby sa nedalo otvoriť. Zaplombuje sa, aby sa dali ľahko zistiť pokusy o fyzickú manipuláciu (napr. vizuálnou kontrolou, pozri ADA_035). Plomba musí spĺňať rovnaké požiadavky, ako plomby snímačov pohybu [398 až 406].

ADA_018 Vstavaný snímač pohybu sa nesmie dať z adaptéra odstrániť bez porušenia plomby (plomb) puzdra adaptéra alebo rozlomenia plomby medzi snímačom a puzdrom adaptéra (pozri ADA_034).

ADA_019 Adaptér musí zabezpečiť, aby sa údaje o pohybe dali spracúvať a odvodzovať len zo vstupu adaptéra.

4.5. **Výkonnostné parametre**

ADA_020 Adaptér musí byť plne funkčný v teplotnom rozsahu stanovenom výrobcom.

ADA_021 Adaptér musí byť plne funkčný v rozsahu vlhkosti 10 až 90 % [214].

ADA_022 Adaptér musí byť chránený proti prepätiu, zmene polarity napájania a skratom [216].

ADA_023 Adaptér musí buď:

— reagovať na magnetické pole, ktoré ruší snímanie pohybu vozidla. Za takýchto okolností jednotka vozidla zaznamená a uloží poruchu snímača [88]; alebo,

— mať snímací prvok, ktorý je chránený pred magnetickými poľami alebo je voči nim imúnny [217].

ADA_024 Adaptér musí zodpovedať predpisu EHK OSN R10 z hľadiska elektromagnetickej kompatibility a musí byť chránený pred elektrostatickými výbojmi a kolísaním napätia [218].

4.6. **Materiály**

ADA_025 Adaptér musí spĺňať stupeň ochrany *(určí neskôr výrobca v závislosti od miesta montáže)* [220, 221].

ADA_026 Puzdro adaptéra musí byť žlté.

4.7. **Označenia**

ADA_027 Na adaptér sa upevní popisný štítok s týmito údajmi:

— názov a adresa výrobcu adaptéra,

— výrobcovo číslo dielu a rok výroby adaptéra,

— schvaľovacia značka typu adaptéra alebo typu záznamového zariadenia vrátane adaptéra,

— dátum montáže adaptéra,

— identifikačné číslo vozidla, na ktoré bol adaptér namontovaný.

ADA_028 Popisný štítok musí obsahovať aj tieto údaje (ak sa nedajú prečítať priamo z vonkajšej strany vstavaného snímača pohybu):

— názov výrobcu vstavaného snímača pohybu,

— výrobcovo číslo dielu a rok výroby vstavaného snímača pohybu,

— schvaľovacia značka vstavaného snímača pohybu.

5. MONTÁŽ ZÁZNAMOVÉHO ZARIADENIA PRI POUŽITÍ ADAPTÉRA

5.1. **Montáž**

ADA_029 Adaptéry určené na montáž vo vozidle inštalujú iba výrobcovia vozidiel alebo schválené dielne oprávnené montovať, aktivovať a kalibrovať digitálne a inteligentné tachografy.

ADA_030 Takáto schválená dielňa musí pri montáži adaptéra upraviť vstupné rozhranie a zvoliť pomer delenia vstupného signálu (podľa potreby).

ADA_031 Takáto schválená dielňa musí pri montáži adaptéra zaplombovať jeho puzdro.

ADA_032 Adaptér sa umiestni čo najbližšie k tej časti vozidla, z ktorej pochádzajú vstupné impulzy.

ADA_033 Napájacie káble adaptéra musia byť červené (kladné napájanie) a čierne (uzemnenie).

5.2. **Plombovanie**

ADA_034 Uplatňujú sa tieto požiadavky na zaplombovanie:

— puzdro adaptéra musí byť zaplombované (pozri ADA_017),

— puzdro vstavaného snímača musí byť plombou spojené s puzdrom adaptéra, ak snímač možno oddeliť od puzdra adaptéra bez narušenia plomby (plomb) puzdra adaptéra (pozri ADA_018),

— puzdro adaptéra musí byť plombou spojené s vozidlom,

— spojenie medzi adaptérom a zariadením, ktoré dodáva vstupné impulzy, musí byť primerane podľa možností zaplombované na oboch koncoch.

6. KONTROLY, INŠPEKCIE A OPRAVY

6.1. **Pravidelné kontroly**

ADA_035 Pri použití adaptéra musí každá pravidelná kontrola (pravidelné kontroly v zmysle dodržania požiadaviek [409] až [413] prílohy 1C) záznamového zariadenia zahŕňať overenie týchto prvkov:

— či má adaptér náležité označenia typového schválenia,

— či sú plomby a spoje adaptéra nedotknuté,

— či je adaptér namontovaný v súlade s montážnym štítkom,

— či je adaptér namontovaný podľa pokynov výrobcu adaptéra a/alebo vozidla,

— či je montáž adaptéra pre kontrolované vozidlo povolená.

ADA_036 Tieto kontroly zahŕňajú kalibráciu a náhradu všetkých plomb bez ohľadu na ich stav.

7. TYPOVÉ SCHVÁLENIE ZÁZNAMOVÉHO ZARIADENIA PRI POUŽITÍ ADAPTÉRA

7.1. **Všeobecne**

ADA_037 Záznamové zariadenie sa predkladá na typové schválenie celé vrátane adaptéra [425].

ADA_038 Každý adaptér možno predložiť na typové schválenie samostatne alebo ako súčasť záznamového zariadenia.

ADA_039 Takéto typové schválenie musí zahŕňať funkčné skúšky, ktorým podlieha aj adaptér. Kladné výsledky každej z týchto skúšok sa doložia príslušným osvedčením [426].

7.2. **Osvedčenie funkčnosti**

ADA_040 Osvedčenie funkčnosti adaptéra alebo záznamového zariadenia vrátane adaptéra sa doručí výrobcovi adaptéra až po úspešnom vykonaní všetkých funkčných skúšok v tomto minimálnom rozsahu.

Č.	Skúška	Opis	Súvisiace požiadavky
1.	**Administratívne preskúmanie**		
1.1	Dokumentácia	Správnosť dokumentácie k adaptéru	
2.	**Vizuálna kontrola**		
2.1.	Zhoda adaptéra s dokumentáciou		
2.2.	Identifikácia/označenia adaptéra		ADA_027, ADA_028
2.3	Materiály adaptéra		[219] až [223] ADA_026
2.4.	Plombovanie		ADA_017, ADA_018, ADA_034
3.	**Funkčné skúšky**		
3.1	Privádzanie impulzov rýchlosti do vstavaného senzora pohybu		ADA_013
3.2	Prepojenie a úprava vstupných impulzov rýchlosti		ADA_011, ADA_012
3.3	Presnosť merania pohybu		[30] až [35], [217]
4.	**Skúšanie vplyvu prostredia**		
4.1	Výsledky výrobcových skúšok	Výsledky výrobcových skúšok vplyvu prostredia	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Elektromagnetická kompatibilita (EMC)**		
5.1	Vyžarované emisie a citlivosť	Overenie zhody so smernicou 2006/28/ES	ADA_024
5.2	Výsledky výrobcových skúšok	Výsledky výrobcových skúšok vplyvu prostredia	ADA_024