Službeni list Europske unije

L 139

Svezak 59.

Hrvatsko izdanje

Zakonodavstvo

26. svibnja 2016.

Sadržaj

II. *Nezakonodavni akti*

UREDBE

★ **Provedbena uredba Komisije (EU) 2016/799 od 18. ožujka 2016. o provedbi Uredbe (EU) br. 165/2014 Europskog parlamenta i Vijeća o utvrđivanju tehničkih zahtjeva za izradu, ispitivanje, ugradnju, rad i popravak tahografa i njihovih sastavnih dijelova** [1] 1

[1] Tekst značajan za EGP

HR

Akti čiji su naslovi tiskani običnim slovima jesu oni koji se odnose na svakodnevno upravljanje poljoprivrednim pitanjima, a općenito vrijede ograničeno razdoblje.

Naslovi svih drugih akata tiskani su masnim slovima, a prethodi im zvjezdica.

II.

(Nezakonodavni akti)

UREDBE

PROVEDBENA UREDBA KOMISIJE (EU) 2016/799

od 18. ožujka 2016.

o provedbi Uredbe (EU) br. 165/2014 Europskog parlamenta i Vijeća o utvrđivanju tehničkih zahtjeva za izradu, ispitivanje, ugradnju, rad i popravak tahografa i njihovih sastavnih dijelova

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) br. 165/2014 Europskog parlamenta i Vijeća od 4. veljače 2014. o tahografima u cestovnom prometu ([1]), a posebno njezin članak 11. i članak 12. stavak 7.,

budući da:

(1) Uredbom (EU) br. 165/2014 uvedeni su digitalni tahografi druge generacije, takozvani pametni tahografi, koji su povezani s globalnim satelitskim navigacijskim sustavom („GNSS"), komunikacijskim uređajem za rano otkrivanje na daljinu i sučeljem s inteligentnim prijevoznim sustavima. Potrebno je utvrditi specifikacije u pogledu tehničkih zahtjeva za izradu pametnih tahografa.

(2) Uređaj za rano otkrivanje na daljinu uspostavljen je na temelju članka 9. stavka 4. Uredbe (EU) br. 165/2014 te bi se njime službenicima za kontrolu na cesti trebalo slati podatke s digitalnog tahografa i informacije koje se odnose na masu i masu po osovini cjelokupne kombinacije vozila (traktora i prikolice ili poluprikolice) u skladu s Direktivom 96/53/EZ Europskog parlamenta i Vijeća ([2]). Time bi se trebalo nadzornim tijelima omogućiti učinkovitu i brzu provjeru vozila, s manje elektroničkih uređaja u kabini vozila.

(3) U skladu s Direktivom 96/53/EZ u uređaju za rano otkrivanje na daljinu trebalo bi upotrebljavati norme Europskog odbora za normizaciju u pogledu komunikacijskog sustava kratkog dometa ([3]) navedene u toj Direktivi, u frekvencijskom pojasu od 5 795 do 5 805 MHz. Budući da se taj frekvencijski pojas upotrebljava i za elektroničku naplatu cestarine te kako bi se izbjegle interferencije između aplikacija za naplatu cestarine i kontrolu, službenici za kontrolu ne bi trebali upotrebljavati uređaj za rano otkrivanje na daljinu u blizini naplatnih postaja.

(4) Uz pametni tahograf trebalo bi uvesti nove sigurnosne mehanizme za održavanje razine sigurnosti digitalnog tahografa radi rješavanja trenutačnih sigurnosnih nedostataka. Jedan je od tih nedostataka nepostojanje datuma isteka digitalnih certifikata. Radi usklađivanja s najboljim praksama u pogledu sigurnosti preporučuje se da bi trebalo izbjegavati upotrebu digitalnih certifikata bez datuma isteka. Uobičajeno bi razdoblje valjanosti jedinica u vozilu trebalo iznositi 15 godina, počevši od datuma izdavanja digitalnih certifikata jedinice u vozilu. Nakon isteka tog razdoblja valjanosti trebalo bi zamijeniti jedinice u vozilu.

([1]) SL L 60, 28.2.2014., str. 1.
([2]) Direktiva Vijeća 96/53/EZ od 25. srpnja 1996. o utvrđivanju najvećih dopuštenih dimenzija u unutarnjem i međunarodnom prometu te najveće dopuštene mase u međunarodnom prometu za određena cestovna vozila koja prometuju unutar Zajednice (SL L 235, 17.9.1996., str. 59.).
([3]) Norme u pogledu komunikacijskog sustava kratkog dometa Europskog odbora za normizaciju (CEN): EN 12253, EN 12795, EN 12834, EN 13372 i ISO 14906.

(5) Pružanje sigurnih i pouzdanih informacija o pozicioniranju ključan je dio učinkovitog rada pametnih tahografa. Stoga je primjereno osigurati njihovu sukladnost s uslugama dodane vrijednosti koje pruža program Galileo kako je utvrđeno u Uredbi (EU) br. 1285/2013 Europskog parlamenta i Vijeća ([1]) radi poboljšanja razine sigurnosti pametnog tahografa.

(6) U skladu s člankom 8. stavkom 1., člankom 9. stavkom 1. te člankom 10. stavcima 1. i 2. Uredbe (EU) br. 165/2014 sigurnosni mehanizmi uvedeni tom Uredbom trebali bi se primjenjivati 36 mjeseci nakon stupanja na snagu potrebnih provedbenih akata kako bi se proizvođačima omogućilo da razviju novu generaciju pametnih tahografa te da dobiju certifikate o homologaciji od nadležnih tijela.

(7) U skladu s Uredbom (EU) br. 165/2014 vozila koja se prvi put registriraju u državi članici 36 mjeseci nakon stupanja na snagu te Uredbe Komisije trebala bi biti opremljena pametnim tahografom u skladu sa zahtjevima te Uredbe Komisije. U svakom bi slučaju sva vozila koja prometuju u državi članici koja nije država članica njihove registracije trebala biti opremljena sukladnim pametnim tahografom 15 godina nakon datuma primjene tih zahtjeva.

(8) Uredbom Komisije (EZ) br. 68/2009 ([2]) tijekom prijelaznog razdoblja koje je završilo 31. prosinca 2013. bila je omogućena upotreba adaptera radi omogućivanja ugradnje tahografa u vozila tipa M1 i N1. Zbog tehničkih poteškoća povezanih s pronalaskom alternativnog rješenja za upotrebu adaptera stručnjaci iz automobilske industrije i industrije tahografa u suradnji s Komisijom zaključili su da nema izvedivog alternativnog rješenja za adapter koje ne bi prouzročilo znatne troškove industriji, a to bi bilo neproporcionalno veličini tržišta. Stoga bi trebalo dopustiti upotrebu adaptera u vozilima tipa M1 i N1 bez vremenskog ograničenja.

(9) Mjere predviđene ovom Uredbom u skladu su s mišljenjem Odbora iz članka 42. stavka 3. Uredbe (EU) br. 165/2014.,

DONIJELA JE OVU UREDBU:

Članak 1.

Predmet i područje primjene

1. Ovom se Uredbom utvrđuju odredbe potrebne za ujednačenu primjenu sljedećih aspekata u pogledu tahografa:

(a) bilježenje položaja vozila na određenim mjestima tijekom dnevnog radnog vremena vozača;

(b) daljinsko rano otkrivanje moguće manipulacije ili zloupotrebe pametnih tahografa;

(c) povezanost s inteligentnim prijevoznim sustavima;

(d) administrativni i tehnički zahtjevi za postupke za homologaciju tahografa, uključujući sigurnosne mehanizme.

2. Izrada, ispitivanje, ugradnja, pregled, rad i popravak pametnih tahografa i njihovih sastavnih dijelova moraju biti u skladu s tehničkim zahtjevima utvrđenima u Prilogu I.C ovoj Uredbi.

3. U pogledu izrade, ispitivanja, ugradnje, pregleda, rada i popravaka tahografi koji nisu pametni tahografi moraju i dalje ispunjavati zahtjeve iz Priloga I. ili Priloga I.B Uredbi Vijeća (EEZ) br. 3821/85 ([3]), kako je primjenjivo.

([1]) Uredba (EU) br. 1285/2013 Europskog parlamenta i Vijeća od 11. prosinca 2013. o provedbi i uporabi europskih sustava za satelitsku navigaciju i stavljanju izvan snage Uredbe Vijeća (EZ) br. 876/2002 i Uredbe (EZ) br. 683/2008 Europskog parlamenta i Vijeća (SL L 347, 20.12.2013., str. 1.).

([2]) Uredba Komisije (EZ) br. 68/2009 od 23. siječnja 2009. o devetoj prilagodbi tehničkom napretku Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u cestovnom prometu (SL L 21, 24.1.2009., str. 3.).

([3]) Uredba Vijeća (EEZ) br. 3821/85 od 20. prosinca 1985. o tahografu u cestovnom prometu (SL L 370, 31.12.1985., str. 8.).

4. U skladu s člankom 10.d Direktive 96/53/EZ uređaj za rano otkrivanje na daljinu šalje i podatke o masi dobivene iz unutarnjih sustava za vaganje u vozilu, u svrhu ranog otkrivanja prijevare.

Članak 2.

Definicije

Za potrebe ove Uredbe primjenjuju se definicije iz članka 2. Uredbe (EU) br. 165/2014.

Osim toga, primjenjuju se i sljedeće definicije:

(1) „digitalni tahograf" ili „tahograf prve generacije" znači digitalni tahograf koji nije pametni tahograf;

(2) „vanjski uređaj GNSS-a" znači uređaj koji sadržava prijamnik GNSS-a kad jedinica u vozilu nije samostalna te ostale sastavne dijelove potrebne za zaštitu prijenosa podataka o položaju ostatku jedinice u vozilu;

(3) „opisna mapa" znači cjelokupna mapa, u elektroničkom ili fizičkom obliku, koja sadržava sve informacije koje je proizvođač ili njegov zastupnik dostavio homologacijskom tijelu u svrhu homologacije tahografa ili nekog njegova sastavnog dijela, uključujući certifikate navedene u članku 12. stavku 3. Uredbe (EU) br. 165/2014, obavljena ispitivanja definirana u Prilogu I.C ovoj Uredbi te nacrte, fotografije i druge relevantne dokumente;

(4) „opisna dokumentacija" znači opisna mapa, u elektroničkom ili fizičkom obliku, kojoj su priloženi svi drugi dokumenti koje je homologacijsko tijelo dodalo opisnoj mapi tijekom provođenja svojih djelatnosti, uključujući certifikat o EZ homologaciji tahografa ili nekog njegova sastavnog dijela;

(5) „kazalo opisne dokumentacije" znači dokument u kojem je naveden i brojevima označen sadržaj opisne dokumentacije te u kojem su utvrđeni svi relevantni dijelovi te dokumentacije. U formatu tog dokumenta razlikuju se uzastopni koraci u postupku EZ homologacije, uključujući datume svih revizija i ažuriranja opisne dokumentacije;

(6) „uređaj za rano otkrivanje na daljinu" znači oprema jedinice u vozilu koja se upotrebljava za provedbu ciljanih provjera na cesti;

(7) „pametni tahograf" ili „tahograf druge generacije" znači digitalni tahograf koji je u skladu s člancima 8., 9. i 10. Uredbe (EU) br. 165/2014 te s Prilogom I.C ovoj Uredbi;

(8) „sastavni dio tahografa" ili „sastavni dio" znači bilo koji od sljedećih elemenata: jedinica u vozilu, senzor kretanja, tahografska kartica, tahografski listić, vanjski uređaj GNSS-a i uređaj za rano otkrivanje na daljinu;

(9) „homologacijsko tijelo" znači tijelo države članice nadležno za provedbu homologacije tahografa ili njegovih sastavnih dijelova, postupka ovlaštenja, izdavanja i, prema potrebi, povlačenja certifikata o homologaciji, koje djeluje u svojstvu kontaktne točke za homologacijska tijela drugih država članica te osigurava da proizvođači ispunjuju svoje obveze u pogledu sukladnosti sa zahtjevima iz ove Uredbe.

Članak 3.

Usluge koje se temelje na lokaciji

1. Proizvođači osiguravaju sukladnost pametnih tahografa s uslugama pozicioniranja koje pružaju sustav Galileo i Europski geostacionarni navigacijski sustav („EGNOS").

2. Uz sustave navedene u stavku 1. proizvođači mogu odlučiti osigurati sukladnost i s drugim satelitskim navigacijskim sustavima.

Članak 4.

Postupci za homologaciju tahografa i sastavnih dijelova tahografa

1. Proizvođač ili njegov zastupnik predaje zahtjev za homologaciju tahografa ili njegovih sastavnih dijelova ili skupine sastavnih dijelova homologacijskim tijelima koja određuju države članice. Zahtjev se sastoji od opisne mape koja sadržava informacije o svakom predmetnom dijelu uključujući, prema potrebi, certifikate o homologaciji drugih sastavnih dijelova potrebnih za upotpunjivanje tahografa te sve druge relevantne dokumente.

2. Država članica odobrava homologaciju tahografu, njegovu sastavnom dijelu ili skupini sastavnih dijelova koji su sukladni s administrativnim i tehničkim zahtjevima navedenima u članku 1. stavku 2. ili 3., kako je primjenjivo. U tom slučaju homologacijsko tijelo podnositelju zahtjeva izdaje certifikat o homologaciji koji je sukladan predlošku utvrđenom u Prilogu II. ovoj Uredbi.

3. Homologacijsko tijelo može zatražiti od proizvođača ili njegova zastupnika da dostavi dodatne informacije.

4. Proizvođač ili njegov zastupnik homologacijskim tijelima i tijelima nadležnima za izdavanje certifikata iz članka 12. stavka 3. Uredbe (EU) br. 165/2014 stavlja na raspolaganje onoliko tahografa ili sastavnih dijelova tahografa koliko je potrebno za uspješnu provedbu postupka homologacije.

5. Ako proizvođač ili njegov zastupnik zatraži homologaciju određenih sastavnih dijelova ili skupina sastavnih dijelova tahografa, homologacijskim tijelima dostavlja druge sastavne dijelove koji su već homologirani i druge dijelove potrebne za izradu potpunog tahografa, kako bi ta tijela mogla provesti potrebna ispitivanja.

Članak 5.

Izmjene homologacije

1. Proizvođač ili njegov zastupnik bez odlaganja izvješćuje homologacijska tijela koja su odobrila prvotnu homologaciju o svim izmjenama softvera ili hardvera tahografa ili vrste materijala upotrijebljenih u njegovoj proizvodnji koje se unose u opisnu dokumentaciju te dostavlja zahtjev za izmjenu homologacije.

2. Homologacijska tijela mogu revidirati ili proširiti postojeću homologaciju ili izdati novu homologaciju u skladu s vrstom i značajkama izmjena.

„Revizija” se provodi ako homologacijsko tijelo smatra da su izmjene softvera ili hardvera tahografa ili vrste materijala upotrijebljenih u njegovoj proizvodnji neznatne. U tom slučaju homologacijsko tijelo izdaje revidirane dokumente iz opisne dokumentacije u kojima je navedena vrsta provedenih izmjena i datum njihova odobrenja. Ažurirana verzija opisne dokumentacije u pročišćenom obliku uz detaljne opise provedenih izmjena dovoljna je za ispunjenje tog zahtjeva.

„Proširenje” se provodi ako homologacijsko tijelo smatra da su izmjene softvera ili hardvera tahografa ili vrste materijala upotrijebljenih u njegovoj proizvodnji znatne. U tom slučaju može zatražiti provođenje novih ispitivanja i o tome izvijestiti proizvođača ili njegova zastupnika. Pokažu li se ta ispitivanja zadovoljavajućima, homologacijsko tijelo izdaje revidirani certifikat o homologaciji koji sadržava broj koji se odnosi na dodijeljeno proširenje. U certifikatu o homologaciji navodi se razlog proširenja i datum njegova izdavanja.

3. U kazalu opisne dokumentacije navodi se datum najnovijeg proširenja ili revizije homologacije ili datum najnovije konsolidacije ažurirane verzije homologacije.

4. Nova homologacija potrebna je ako bi zbog zatraženih izmjena homologiranog tahografa ili njegovih dijelova došlo do izdavanja novog certifikata o sigurnosti ili interoperabilnosti.

Članak 6.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Primjenjuje se od 2. ožujka 2016.

Međutim, prilozi se primjenjuju od 2. ožujka 2019. uz iznimku Dodatka 16. koji se primjenjuje od 2. ožujka 2016.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 18. ožujka 2016.

Za Komisiju
Predsjednik
Jean-Claude JUNCKER

PRILOG I.C

Zahtjevi u pogledu izrade, ispitivanja, ugradnje i pregleda

UVOD 12

1 DEFINICIJE 13

2 OPĆA OBILJEŽJA I FUNKCIJE UREĐAJA ZA BILJEŽENJE PODATAKA 19

2.1 Opća obilježja 19

2.2 Funkcije 20

2.3 Načini rada 21

2.4 Sigurnost 22

3 ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNOSTI UREĐAJA ZA BILJEŽENJE PODATAKA 22

3.1 Praćenje umetanja i uklanjanja kartica 22

3.2 Mjerenje brzine, položaja i prijeđenog puta 23

3.2.1 Mjerenje prijeđene udaljenosti 23

3.2.2 Mjerenje brzine 23

3.2.3 Mjerenje položaja 24

3.3 Mjerenje vremena 24

3.4 Praćenje aktivnosti vozača 24

3.5 Praćenje statusa vožnje 25

3.6 Unosi vozača 25

3.6.1 Unos mjesta početka i/ili kraja dnevnog radnog vremena 25

3.6.2 Ručni unos aktivnosti vozača i suglasnost vozača u pogledu sučelja ITS-a 25

3.6.3 Unos posebnih stanja 27

3.7 Upravljanje blokadama poduzeća 27

3.8 Praćenje aktivnosti nadzora 28

3.9 Prepoznavanje događaja i/ili kvarova 28

3.9.1 Događaj „umetanje nevažeće kartice” 28

3.9.2 Događaj „konflikt kartica” 28

3.9.3 Događaj „vremensko preklapanje” 28

3.9.4 Događaj „vožnja bez odgovarajuće kartice” 29

3.9.5 Događaj „umetanje kartice tijekom vožnje” 29

3.9.6 Događaj „neispravno zatvaranje posljednje razmjene podataka s karticom” 29

3.9.7 Događaj „prekoračenje brzine” 29

3.9.8 Događaj „prekid napajanja” 29

3.9.9 Događaj „greška u komunikaciji s uređajem za komunikaciju na daljinu” 29

3.9.10 Događaj „izostanak podataka o položaju iz prijamnika GNSS-a” 29

3.9.11	Događaj „greška u komunikaciji s vanjskim uređajem GNSS-a”	30
3.9.12	Događaj „greška u podatcima o kretanju”	30
3.9.13	Događaj „konflikt u kretanju vozila”	30
3.9.14	Događaj „pokušaj povrede sigurnosti”	30
3.9.15	Događaj „vremenski konflikt”	30
3.9.16	Kvar „kartica”	30
3.9.17	Kvar „uređaj za bilježenje podataka”	30
3.10	Ugrađena ispitivanja i samoispitivanja	31
3.11	Čitanje iz podatkovne memorije	31
3.12	Bilježenje i pohrana u podatkovnoj memoriji	31
3.12.1	Identifikacijski podatci o uređaju	32
3.12.1.1	Identifikacijski podatci jedinice u vozilu	32
3.12.1.2	Identifikacijski podatci senzora kretanja	32
3.12.1.3	Identifikacijski podatci globalnih satelitskih navigacijskih sustava	33
3.12.2	Ključevi i certifikati	33
3.12.3	Podatci o umetanju i uklanjanju kartice vozača ili kartice radionice	33
3.12.4	Podatci o aktivnosti vozača	34
3.12.5	Mjesta i položaji početka i završetka dnevnog radnog vremena i/ili dostizanja tri sata neprekidnog vremena vožnje	34
3.12.6	Stanje brojača prijeđenih kilometara	35
3.12.7	Detaljni podatci o brzini	35
3.12.8	Podatci o događajima	35
3.12.9	Podatci o kvarovima	37
3.12.10	Podatci o kalibraciji	38
3.12.11	Podatci o prilagodbi vremena	39
3.12.12	Podatci o aktivnostima nadzora	39
3.12.13	Podatci o blokadama poduzeća	39
3.12.14	Podatci o aktivnostima preuzimanja podataka	39
3.12.15	Podatci o posebnim stanjima	40
3.12.16	Podatci o tahografskoj kartici	40
3.13	Očitavanje podataka s tahografskih kartica	40
3.14	Bilježenje i pohrana podataka na tahografske kartice	40
3.14.1	Bilježenje i pohrana podataka na tahografske kartice prve generacije	40
3.14.2	Bilježenje i pohrana podataka na tahografske kartice druge generacije	41
3.15	Prikaz	41
3.15.1	Standardni prikaz	42

3.15.2	Prikaz upozorenja	43
3.15.3	Pristup izbornicima	43
3.15.4	Ostali prikazi	43
3.16	Ispis	43
3.17	Upozorenja	44
3.18	Preuzimanje podataka na vanjske medije	45
3.19	Komunikacija na daljinu za ciljane provjere na cesti	45
3.20	Izlazni podatci za dodatne vanjske uređaje	46
3.21	Kalibracija	47
3.22	Provjera kalibracije na cesti	47
3.23	Prilagodba vremena	48
3.24	Karakteristike radnog učinka	48
3.25	Materijali	48
3.26	Oznake	49
4	ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNOSTI TAHOGRAFSKIH KARTICA	49
4.1	Vidljivi podatci	49
4.2	Sigurnost	52
4.3	Norme	53
4.4	Specifikacije okruženja i elektrotehničke specifikacije	53
4.5	Pohrana podataka	53
4.5.1	Elementarne datoteke za identifikaciju i upravljanje karticama	54
4.5.2	Identifikacija IC kartice	54
4.5.2.1	Identifikacija čipa	54
4.5.2.2	DIR (prisutan samo na tahografskim karticama druge generacije)	54
4.5.2.3	Podatci ATR-a (uvjetno, prisutno samo na tahografskim karticama druge generacije)	54
4.5.2.4	Podatci proširene veličine (uvjetno, prisutno samo na tahografskim karticama druge generacije)	55
4.5.3	Kartica vozača	55
4.5.3.1	Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)	55
4.5.3.1.1	Identifikacija aplikacije	55
4.5.3.1.2	Ključevi i certifikati	55
4.5.3.1.3	Identifikacija kartice	55
4.5.3.1.4	Identifikacija nositelja kartice	55
4.5.3.1.5	Preuzimanje podataka s kartice	55
4.5.3.1.6	Podatci o vozačkoj dozvoli	55
4.5.3.1.7	Podatci o događajima	56

4.5.3.1.8 Podatci o kvarovima ... 56
4.5.3.1.9 Podatci o aktivnosti vozača ... 57
4.5.3.1.10 Podatci o upotrijebljenim vozilima ... 57
4.5.3.1.11 Mjesta početka i/ili završetka dnevnog radnog vremena ... 58
4.5.3.1.12 Podatci o upotrebi kartice ... 58
4.5.3.1.13 Podatci o aktivnostima nadzora ... 58
4.5.3.1.14 Podatci o posebnim stanjima ... 58
4.5.3.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije) ... 59
4.5.3.2.1 Identifikacija aplikacije ... 59
4.5.3.2.2 Ključevi i certifikati ... 59
4.5.3.2.3 Identifikacija kartice ... 59
4.5.3.2.4 Identifikacija nositelja kartice ... 59
4.5.3.2.5 Preuzimanje podataka s kartice ... 59
4.5.3.2.6 Podatci o vozačkoj dozvoli ... 59
4.5.3.2.7 Podatci o događajima ... 59
4.5.3.2.8 Podatci o kvarovima ... 60
4.5.3.2.9 Podatci o aktivnosti vozača ... 61
4.5.3.2.10 Podatci o upotrijebljenim vozilima ... 61
4.5.3.2.11 Mjesta i položaji početka i/ili završetka dnevnog radnog vremena ... 62
4.5.3.2.12 Podatci o upotrebi kartice ... 62
4.5.3.2.13 Podatci o aktivnostima nadzora ... 62
4.5.3.2.14 Podatci o posebnim stanjima ... 63
4.5.3.2.15 Podatci o upotrijebljenoj jedinici u vozilu ... 63
4.5.3.2.16 Podatci o mjestima na kojima se dostižu tri sata neprekidne vožnje ... 63
4.5.4 Kartica radionice ... 63
4.5.4.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije) ... 63
4.5.4.1.1 Identifikacija aplikacije ... 63
4.5.4.1.2 Ključevi i certifikati ... 63
4.5.4.1.3 Identifikacija kartice ... 64
4.5.4.1.4 Identifikacija nositelja kartice ... 64
4.5.4.1.5 Preuzimanje podataka s kartice ... 64
4.5.4.1.6 Podatci o kalibraciji i prilagodbi vremena ... 64

4.5.4.1.7 Podatci o događajima i kvarovima 65
4.5.4.1.8 Podatci o aktivnosti vozača 65
4.5.4.1.9 Podatci o upotrijebljenim vozilima 65
4.5.4.1.10 Podatci o početku i/ili završetku dnevnog radnog vremena 65
4.5.4.1.11 Podatci o upotrebi kartice 65
4.5.4.1.12 Podatci o aktivnostima nadzora 65
4.5.4.1.13 Podatci o posebnim stanjima 65
4.5.4.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije) 65
4.5.4.2.1 Identifikacija aplikacije 65
4.5.4.2.2 Ključevi i certifikati 66
4.5.4.2.3 Identifikacija kartice 66
4.5.4.2.4 Identifikacija nositelja kartice 66
4.5.4.2.5 Preuzimanje podataka s kartice 66
4.5.4.2.6 Podatci o kalibraciji i prilagodbi vremena 66
4.5.4.2.7 Podatci o događajima i kvarovima 67
4.5.4.2.8 Podatci o aktivnosti vozača 67
4.5.4.2.9 Podatci o upotrijebljenim vozilima 67
4.5.4.2.10 Podatci o početku i/ili završetku dnevnog radnog vremena 67
4.5.4.2.11 Podatci o upotrebi kartice 67
4.5.4.2.12 Podatci o aktivnostima nadzora 67
4.5.4.2.13 Podatci o upotrijebljenoj jedinici u vozilu 67
4.5.4.2.14 Podatci o mjestima na kojima se dostižu tri sata neprekidne vožnje 68
4.5.4.2.15 Podatci o posebnim stanjima 68
4.5.5 Kontrolna kartica 68
4.5.5.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije) 68
4.5.5.1.1 Identifikacija aplikacije 68
4.5.5.1.2 Ključevi i certifikati 68
4.5.5.1.3 Identifikacija kartice 68
4.5.5.1.4 Identifikacija nositelja kartice 68
4.5.5.1.5 Podatci o aktivnostima nadzora 69
4.5.5.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije) 69
4.5.5.2.1 Identifikacija aplikacije 69
4.5.5.2.2 Ključevi i certifikati 69

4.5.5.2.3	Identifikacija kartice	69
4.5.5.2.4	Identifikacija nositelja kartice	69
4.5.5.2.5	Podatci o aktivnostima nadzora	70
4.5.6	Kartica poduzeća	70
4.5.6.1	Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)	70
4.5.6.1.1	Identifikacija aplikacije	70
4.5.6.1.2	Ključevi i certifikati	70
4.5.6.1.3	Identifikacija kartice	70
4.5.6.1.4	Identifikacija nositelja kartice	70
4.5.6.1.5	Podatci o aktivnostima poduzeća	70
4.5.6.2	Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)	71
4.5.6.2.1	Identifikacija aplikacije	71
4.5.6.2.2	Ključevi i certifikati	71
4.5.6.2.3	Identifikacija kartice	71
4.5.6.2.4	Identifikacija nositelja kartice	71
4.5.6.2.5	Podatci o aktivnostima poduzeća	71
5	UGRADNJA UREĐAJA ZA BILJEŽENJE PODATAKA	72
5.1	Ugradnja	72
5.2	Tipska pločica	73
5.3	Plombiranje	74
6	PROVJERE, PREGLEDI I POPRAVCI	74
6.1	Ovlaštenje instalatera, radionica i proizvođača vozila	74
6.2	Provjera novih ili popravljenih uređaja	75
6.3	Pregled pri ugradnji	75
6.4	Periodični pregledi	75
6.5	Mjerenje grešaka	76
6.6	Popravci	76
7	IZDAVANJE KARTICA	76
8	HOMOLOGACIJA UREĐAJA ZA BILJEŽENJE PODATAKA I TAHOGRAFSKIH KARTICA	77
8.1	Opći zahtjevi	77
8.2	Certifikat o sigurnosti	78
8.3	Certifikat o ispravnosti	78
8.4	Certifikat o interoperabilnosti	78
8.5	Certifikat o homologaciji	79
8.6	Izvanredni postupak: prvi certifikati o interoperabilnosti za uređaje za bilježenje podataka i tahografske kartice druge generacije	80

UVOD

Sustav digitalnog tahografa prve generacije upotrebljava se od 1. svibnja 2006. U prijevozu unutar zemlje može se upotrebljavati do isteka njegova životnog ciklusa. U međunarodnom prijevozu sva se vozila 15 godina nakon stupanja na snagu ove Uredbe Komisije moraju opremiti drugom generacijom pametnih tahografa koja je u skladu s tahografima uvedenima ovom Uredbom.

Ovaj Prilog sadržava zahtjeve u pogledu uređaja za bilježenje podataka i tahografskih kartica druge generacije. Od datuma njegova uvođenja u vozila koja se prvi put registriraju ugrađuju se uređaji za bilježenje podataka druge generacije te se izdaju tahografske kartice druge generacije.

Kako bi se poticalo nesmetano uvođenje sustava tahografa druge generacije,

— tahografske kartice druge generacije osmišljene su tako da se mogu upotrebljavati i u jedinicama u vozilima prve generacije;

— zamjena valjanih tahografskih kartica prve generacije ne zahtijeva se na datum uvođenja.

Time će se vozačima omogućiti da zadrže vlastitu jedinstvenu karticu vozača te da je upotrebljavaju za oba sustava.

Međutim, uređaj za bilježenje podataka druge generacije kalibrira se samo upotrebom kartica radionice druge generacije.

Ovaj Prilog sadržava sve zahtjeve koji se odnose na interoperabilnost sustava tahografa prve i druge generacije.

Dodatak 15. sadržava dodatne pojedinosti o načinu upravljanja supostojanjem dvaju sustava.

Popis dodataka

Dodatak 1.: RJEČNIK S PODATCIMA

Dodatak 2.: SPECIFIKACIJE TAHOGRAFSKE KARTICE

Dodatak 3.: PIKTOGRAMI

Dodatak 4.: ISPISI

Dodatak 5.: PRIKAZ

Dodatak 6.: PREDNJI PRIKLJUČAK ZA KALIBRACIJU I PREUZIMANJE PODATAKA

Dodatak 7.: PROTOKOLI PREUZIMANJA PODATAKA

Dodatak 8.: PROTOKOL KALIBRACIJE

Dodatak 9.: HOMOLOGACIJA I POPIS OBVEZNIH ISPITIVANJA

Dodatak 10.: SIGURNOSNI ZAHTJEVI

Dodatak 11.: ZAJEDNIČKI SIGURNOSNI MEHANIZMI

Dodatak 12.: UTVRĐIVANJE POLOŽAJA NA TEMELJU GLOBALNOG SATELITSKOG NAVIGACIJSKOG SUSTAVA (GNSS)

Dodatak 13.: ITS SUČELJE

Dodatak 14.: FUNKCIJA KOMUNIKACIJE NA DALJINU

Dodatak 15.: MIGRACIJA: UPRAVLJANJE ISTODOBNIM POSTOJANJEM VIŠE GENERACIJA OPREME

Dodatak 16.: ADAPTER ZA VOZILA KATEGORIJE M1 I N1

1 DEFINICIJE

U ovom Prilogu:

a) „aktiviranje” znači:

faza u kojoj je tahograf u potpunosti operativan i provodi sve funkcije, uključujući sigurnosne funkcije, upotrebom kartice radionice;

b) „autentifikacija” znači:

funkcija namijenjena utvrđivanju i provjeri identiteta;

c) „autentičnost” znači:

obilježje da informacija dolazi od izvora čiji je identitet moguće provjeriti;

d) „ugrađeno ispitivanje (BIT)” znači:

ispitivanja koja se provode na zahtjev i koja aktivira operater ili se aktiviraju vanjskom opremom;

e) „kalendarski dan” znači:

dan koji traje od 00:00 sati do 24:00 sata. Svi kalendarski dani odnose se na koordinirano svjetsko vrijeme (UTC);

f) „kalibracija” pametnog tahografa znači:

ažuriranje ili potvrda parametara vozila koje treba sačuvati u podatkovnoj memoriji. Parametri vozila uključuju identifikaciju vozila (VIN, VRN i država registracije) i karakteristike vozila (w, k, l, veličina guma, podešavanje uređaja za ograničavanje brzine (prema potrebi), trenutačno vrijeme po UTC-u, trenutačno stanje na brojaču kilometara); tijekom kalibracije uređaja za bilježenje podataka u podatkovnoj memoriji pohranjuju se i tipovi i identifikatori svih postavljenih plombi koje su važne za homologaciju;

svako ažuriranje ili potvrđivanje samo vremena po UTC-u smatra se prilagodbom vremena, a ne kalibracijom, pod uvjetom da se time ne proturječi zahtjevu 409;

za kalibriranje uređaja za bilježenje podataka potrebna je kartica radionice;

g) „broj kartice” znači:

broj od 16 alfanumeričkih znakova kojim se na jedinstven način identificira tahografska kartica unutar neke države članice. Broj kartice uključuje indeks rednog broja kartice (prema potrebi), indeks zamjene kartice i indeks obnavljanja kartice;

kartica se tako na jedinstven način identificira oznakom države članice izdavateljice i brojem kartice;

h) „indeks rednog broja kartice” znači:

14. alfanumerički znak broja kartice koji se upotrebljava za razlikovanje različitih kartica izdanih poduzeću, radionici ili nadzornom tijelu koje ima pravo na više tahografskih kartica. Poduzeće, radionica ili nadzorno tijelo na jedinstven se način identificira s pomoću prvih 13 znamenaka broja kartice;

i) „indeks obnavljanja kartice” znači:

16. alfanumerički znak broja kartice koji se uvećava pri svakom obnavljanju tahografske kartice;

j) „indeks zamjene kartice” znači:

15. alfanumerički znak broja kartice koji se uvećava pri svakoj zamjeni tahografske kartice;

k) „karakteristični koeficijent vozila” znači:

brojčana veličina koja navodi vrijednost izlaznog signala koji nastaje na priključnom mjestu uređaja za bilježenje podataka i vozila (na mjenjaču ili osovini kotača) dok vozilo prelazi put od jednog kilometra u standardnim uvjetima ispitivanja kako je definirano u zahtjevu 414. Karakteristični koeficijent izražava se u impulsima po kilometru (w = … imp/km);

l) „kartica poduzeća” znači:

tahografska kartica koju ovlaštena tijela u državi članici izdaju prijevoznom poduzeću koje upravlja vozilima u koja je ugrađen tahograf, a koja služi za identifikaciju prijevoznog poduzeća te omogućuje prikazivanje, preuzimanje i ispisivanje podataka pohranjenih u tahografu koje je prijevozno poduzeće zaključalo;

m) „konstanta uređaja za bilježenje podataka” znači:

brojčana veličina koja navodi vrijednost ulaznog signala potrebnog za pokazivanje i bilježenje duljine prijeđenog puta od jednog kilometra; ta se konstanta izražava u impulsima po kilometru (k = … imp/km)

n) „neprekidno vrijeme vožnje” izračunava se u uređaju za bilježenje podataka kao ([1]):

neprekidno vrijeme vožnje izračunava se kao trenutačno akumulirano vrijeme vožnje određenog vozača od završetka posljednjeg razdoblja DOSTUPNOSTI ili STANKE/ODMORA ili NEPOZNATO ([2]) u trajanju od najmanje 45 minuta (navedeno razdoblje može biti podijeljeno u skladu s Uredbom (EZ) br. 561/2006 Europskog parlamenta i Vijeća ([3])). U navedenom se izračunu prema potrebi uzimaju u obzir prethodne aktivnosti pohranjene na kartici vozača. Ako vozač nije umetnuo svoju karticu, izračun se temelji na zapisima iz podatkovne memorije koji se odnose na tekuće razdoblje u kojem kartica nije bila umetnuta u odgovarajući utor za kartice;

o) „kontrolna kartica” znači:

tahografska kartica koju ovlaštena tijela u državi članici izdaju nacionalnom nadležnom nadzornom tijelu, a koja služi za identifikaciju nadzornog tijela i, prema potrebi, službenika za kontrolu te koja omogućuje pristup podatcima pohranjenima u podatkovnoj memoriji, kartici vozača ili, prema potrebi, karticama radionice, u svrhu njihova čitanja, ispisivanja i/ili preuzimanja.

Osim toga, omogućuje pristup funkciji provjere kalibracije na cesti i podatcima na čitaču komunikacije ranog otkrivanja na daljinu;

p) „kumulativno vrijeme stanki” izračunava se u uređaju za bilježenje podataka kao ([1]):

kumulativno vrijeme stanki od vremena vožnje izračunava se kao trenutačno akumulirano vrijeme DOSTUPNOSTI ili STANKE/ODMORA ili NEPOZNATO ([2]) u trajanju od najmanje 15 minuta za pojedinog vozača, od završetka posljednjeg razdoblja njegove DOSTUPNOSTI ili STANKE/ODMORA ili NEPOZNATO ([2]) u trajanju od najmanje 45 minuta (to razdoblje može biti podijeljeno u skladu s Uredbom (EZ) br. 561/2006).

U navedenom se izračunu prema potrebi uzimaju u obzir prethodne aktivnosti pohranjene na kartici vozača. Nepoznata razdoblja negativnog vremenskog izračuna (početak nepoznatog razdoblja vremenski je kasniji od završetka nepoznatog razdoblja) zbog vremenskih preklapanja između dvaju različitih uređaja za bilježenje podataka ne uzimaju se u obzir za izračun.

Ako vozač nije umetnuo svoju karticu, izračun se temelji na zapisima iz podatkovne memorije koji se odnose na tekuće razdoblje u kojem kartica nije bila umetnuta u odgovarajući utor za kartice;

([1]) Ovaj način izračuna neprekidnog vremena vožnje i kumulativnog vremena stanki služi uređaju za bilježenje podataka za izračun upozorenja o neprekidnom vremenu vožnje. Time se ne dovodi u pitanje pravno tumačenje navedenih vremena. Alternativni načini izračuna neprekidnog vremena vožnje i kumulativnog vremena stanki mogu se upotrijebiti za zamjenu tih definicija ako su postale zastarjele ažuriranjem u drugim odgovarajućim zakonima.

([2]) Razdoblja NEPOZNATO odnose se na razdoblja kada kartica vozača nije bila umetnuta u uređaj za bilježenje podataka i za koja nisu ručno upisivani podatci o aktivnostima vozača.

([3]) Uredba (EZ) br. 561/2006 Europskog parlamenta i Vijeća od 15. ožujka 2006. o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na cestovni promet i o izmjeni uredbi Vijeća (EEZ) br. 3821/85 i (EZ) br. 2135/98 te o stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3820/85 (SL L 102, 11.4.2006., str. 1.).

q) „podatkovna memorija” znači:

elektroničko sredstvo za pohranjivanje podataka ugrađeno u uređaj za bilježenje podataka;

r) „digitalni potpis” znači:

podatci stavljeni na blok podataka ili kriptografska pretvorba bloka podataka koja omogućuje primatelju bloka podataka dokazivanje autentičnosti i integriteta bloka podataka;

s) „preuzimanje podataka” znači:

kopiranje, zajedno s digitalnim potpisom, dijela ili čitavog skupa datoteka zabilježenih u podatkovnoj memoriji jedinice u vozilu ili u memoriji tahografske kartice pod uvjetom da taj proces ne mijenja niti briše pohranjene podatke.

Proizvođači jedinica pametnih tahografa u vozilu i proizvođači opreme oblikovane i namijenjene za preuzimanje datoteka moraju poduzeti sve razumne mjere da osiguraju da prijevozna poduzeća ili vozači mogu preuzeti te podatke uz minimalnu odgodu.

Preuzimanje datoteke s detaljnim podatcima o brzini ne mora biti potrebno za utvrđivanje sukladnosti s Uredbom (EZ) br. 561/2006, no može se upotrijebiti za druge potrebe, kao što je istraživanje nesreća;

t) „kartica vozača” znači:

tahografska kartica koju ovlaštena tijela u državi članici izdaju pojedinom vozaču, a koja služi za identifikaciju vozača te omogućuje pohranu podataka o aktivnosti vozača;

u) „djelatni opseg kotača” znači:

srednja vrijednost prijeđenog puta pogonskog kotača kod punog okretaja. Mjerenje tog puta mora se obavljati u standardnim uvjetima ispitivanja, kako je definirano u zahtjevu 414, i izražava se u obliku „l = … mm”. Proizvođači vozila mogu nadomjestiti mjerenje tog puta teoretskim izračunom u kojem se uzima u obzir raspored opterećenja po osovinama za nenatovareno vozilo u stanju spremnom za vožnju ([1]). Metode takvog teoretskog izračuna odobrava nadležno tijelo države članice i mogu se poduzeti samo prije aktivacije tahografa;

v) „događaj” znači:

neuobičajeno djelovanje koje otkrije pametni tahograf, a koje može biti rezultat pokušaja prijevare;

w) „vanjski uređaj GNSS-a” znači:

uređaj koji sadržava prijamnik GNSS-a kad jedinica u vozilu nije samostalna te ostale sastavne dijelove potrebne za zaštitu prijenosa podataka o položaju drugim dijelovima jedinice u vozilu;

x) „kvar” znači:

neuobičajeno djelovanje koje otkrije pametni tahograf, a koje može biti rezultat nepravilnosti ili greške na uređaju;

y) „prijamnik GNSS-a” znači:

elektronički uređaj koji prima i digitalno obrađuje signale iz jednoga globalnog satelitskog navigacijskog sustava ili više njih (eng. *Global Navigation Satellite System*, GNSS) radi pružanja informacija o položaju, brzini i vremenu;

z) „ugradnja” znači:

postavljanje tahografa u vozilo;

([1]) Uredba Komisije (EU) br. 1230/2012 od 12. prosinca 2012. o provedbi Uredbe (EZ) br. 661/2009 Europskog parlamenta i Vijeća o zahtjevima za homologaciju tipa za mase i dimenzije vozila i njihovih prikolica te o izmjeni Direktive 2007/46/EZ Europskog parlamenta i Vijeća (SL L 353, 21.12.2012.,str. 31.), kako je zadnji put izmijenjena.

aa) „interoperabilnost” znači:

sposobnost sustava i temeljnih poslovnih procesa da razmjenjuju podatke i dijele informacije;

bb) „sučelje” znači:

veza između sustava koja im omogućuje međusobno povezivanje i interakciju;

cc) „položaj” znači:

geografske koordinate vozila u određenom trenutku;

dd) „senzor kretanja” znači:

dio tahografa na kojem se prikazuje signalna oznaka brzine vozila i/ili duljine prijeđenoga puta vozila;

ee) „nevažeća kartica” znači:

kartica za koju se otkrije da je neispravna ili čija početna autentifikacija nije uspjela ili čiji datum početka važenja još nije dosegnut ili čiji je datum isteka prošao;

ff) „otvorena norma” znači:

norma iz dokumenta o specifikaciji normi koja je dostupna besplatno ili uz nominalnu naplatu i može se kopirati, dijeliti ili upotrebljavati bez naknade ili uz nominalnu naknadu;

gg) „izvan područja primjene” znači:

okolnosti u kojima uređaj za bilježenje podataka nije potrebno upotrebljavati u skladu s odredbama Uredbe (EZ) br. 561/2006.

hh) „prekoračenje brzine” znači:

prekoračenje dopuštene brzine vozila koja se utvrđuje u bilo kojem razdoblju duljem od 60 sekundi, tijekom kojeg izmjerena brzina vozila prelazi graničnu brzinu podešenu uređajem za ograničenje brzine, a utvrđenu Direktivom Vijeća 92/6/EEZ ([1]), kako je zadnje izmijenjena;

ii) „periodični pregled” znači:

skup postupaka koji se obavljaju za provjeru radi li tahograf pravilno, odgovaraju li njegove postavke parametrima vozila i jesu li uređaji za manipulaciju spojeni na tahograf;

jj) „pisač” znači:

sastavni dio uređaja za bilježenje podataka koji daje ispis pohranjenih podataka;

kk) „komunikacija ranog otkrivanja na daljinu” znači:

komunikacija između uređaja za rano otkrivanje na daljinu i čitača komunikacije ranog otkrivanja na daljinu tijekom ciljanih provjera na cesti u cilju daljinskog otkrivanja moguće manipulacije ili zloupotrebe uređaja za bilježenje podataka;

ll) „uređaj za komunikaciju na daljinu” znači:

uređaj jedinice u vozilu koji se upotrebljava za provođenje ciljanih provjera na cesti;

([1]) Direktiva Vijeća 92/6/EEZ od 10. veljače 1992. o ugradnji i uporabi uređaja za ograničenje brzine za određene kategorije motornih vozila u Zajednici (SL L 57, 2.3.1992., str. 27.).

mm) „čitač komunikacije ranog otkrivanja na daljinu” znači:

sustav koji upotrebljavaju službenici za kontrolu za ciljane provjere na cesti;

nn) „obnavljanje” znači:

izdavanje nove tahografske kartice kad postojećoj kartici istekne valjanost ili kad postane neispravna pa je vraćena tijelu koje ju je izdalo. Obnavljanje uvijek podrazumijeva sigurnost da ne postoje dvije važeće kartice;

oo) „popravak” znači:

bilo kakav popravak senzora kretanja, jedinice u vozilu ili kabela koji zahtijeva isključivanje s napajanja ili isključivanje s drugih sastavnih dijelova tahografa ili otvaranje senzora kretanja ili jedinice u vozilu;

pp) „zamjena kartice” znači:

izdavanje tahografske kartice kao zamjene za postojeću karticu čiji su gubitak, krađa ili neispravnost prijavljeni, a nije vraćena tijelu koje ju je izdalo. Zamjena uvijek podrazumijeva rizik da mogu istodobno postojati dvije važeće kartice;

qq) „sigurnosno certificiranje” znači:

postupak kojim certifikacijsko tijelo koje je primijenilo zajednička mjerila tijekom certifikacije potvrđuje da uređaj za bilježenje podataka (ili njegov sastavni dio) ili tahografska kartica koja se ispituje zadovoljava sigurnosne zahtjeve utvrđene u odgovarajućim profilima zaštite;

rr) „samoispitivanje” znači:

ispitivanja koja uređaj za bilježenje podataka provodi ciklički i automatski radi otkrivanja kvarova;

ss) „izmjereno vrijeme” znači:

trajni digitalni zapis koordiniranog svjetskog datuma i vremena (UTC);

tt) „prilagodba vremena” znači:

automatska prilagodba trenutačnog vremena u redovnim intervalima i s maksimalnim odstupanjem od jedne minute ili prilagodba koja se provodi tijekom kalibracije;

uu) „veličina gume” znači:

oznaka dimenzije guma (vanjskih pogonskih kotača) u skladu s Direktivom Vijeća 92/23/EEZ ([1]), kako je zadnje izmijenjena;

vv) „identifikacija vozila” znači

brojevi kojima se identificira vozilo: registracijski broj vozila (eng. *Vehicle Registration Number*, VRN) s oznakom države članice u kojoj je vozilo registrirano i identifikacijski broj vozila (eng. *Vehicle Identification Number*, VIN) ([2]);

ww) za potrebe izračunavanja u uređaju za bilježenje podataka „tjedan” znači:

razdoblje između 00:00 sati UTC u ponedjeljak i 24:00 sata UTC u nedjelju;

([1]) Direktiva Vijeća 92/23/EEZ od 31. ožujka 1992. o gumama za motorna vozila i njihove prikolice i o njihovoj ugradbi (SL L 129, 14.5.1992., str. 95.).

([2]) Direktiva Vijeća 76/114/EEZ od 18. prosinca 1975. o usklađivanju zakonodavstava država članica u odnosu na propisane pločice i natpise za motorna vozila i njihove prikolice te na njihov položaj i način pričvršćivanja (SL L 24, 30.1.1976., str. 1.).

xx) „kartica radionice” znači:

tahografska kartica koju su ovlaštena tijela u državi članici izdala ovlaštenom osoblju proizvođača tahografa, instalatera, proizvođača vozila ili radionice koje je država članica odobrila, a koja služi za identifikaciju nositelja kartice te omogućuje ispitivanje, kalibraciju i aktiviranje tahografa i/ili preuzimanje podataka iz njih;

yy) „adapter” znači:

uređaj koji stalno daje signal brzine vozila i/ili prijeđene udaljenosti, osim onoga koji se upotrebljava za neovisno otkrivanje kretanja, te koji se:

— ugrađuje i upotrebljava samo u vozilima tipa M1 i N1 (kako je definirano u Prilogu II. Direktivi 2007/46/EZ Europskog parlamenta i Vijeća ([1]), kako je zadnje izmijenjena) koja su stavljena u upotrebu nakon 1. svibnja 2006.,

— ugrađuje kada nije mehanički moguće ugraditi bilo kakvu drugu vrstu postojećeg senzora kretanja, koji je inače usklađen s odredbama ovog Priloga i njegovih dodataka od 1. do 15.,

— ugrađuje između jedinice u vozilu i ondje gdje ugrađeni senzori ili alternativna sučelja proizvode impulse brzine/udaljenosti.

— Gledano iz jedinice u vozilu, ponašanje adaptera jednako je kao da je senzor kretanja, sukladan odredbama ovog Priloga i njegovih dodataka od 1. do 16., spojen na jedinicu u vozilu.

Upotrebom takvog adaptera u prethodno opisanim vozilima omogućuju se ugradnja i ispravna upotreba jedinice u vozilu koja je u skladu sa svim zahtjevima ovog Priloga.

Za ta vozila, pametni tahograf sastavljen je od kabela, adaptera i jedinice u vozilu;

zz) „integritet podataka” znači:

točnost i dosljednost pohranjenih podataka, na koje upućuje nedostatak bilo kakvih promjena podataka između dvaju ažuriranja podatkovnog zapisa. Integritet podrazumijeva da su podatci točna preslika izvorne verzije, npr. da nisu postali neispravni u procesu njihova zapisivanja na tahografsku karticu ili namjensku opremu ili njihova čitanja s nje, ili tijekom prijenosa bilo kakvim komunikacijskim kanalom;

aaa) „zaštita podataka” znači:

ukupne tehničke mjere koje su poduzete kako bi se osigurala ispravna provedba načela utvrđenih u Direktivi br. 95/46/EZ Europskog parlamenta i Vijeća ([2]) te načela utvrđenih u Direktivi 2002/58/EZ Europskog parlamenta i Vijeća ([3]);

bbb) „sustav pametnog tahografa” znači:

uređaj za bilježenje podataka, tahografske kartice i skup svih uređaja koji su s njima izravno ili neizravno povezani tijekom njihove izrade, ugradnje, upotrebe, ispitivanja i nadzora, kao što su kartice, čitač komunikacije na daljinu i svi ostali uređaji za preuzimanje podataka, analizu podataka, kalibraciju, generiranje sigurnosnih elemenata, upravljanje njima ili njihovo uvođenje itd.

ccc) „datum uvođenja” znači:

36 mjeseci nakon stupanja na snagu detaljnih odredbi iz članka 11. Uredbe (EU) br. 165/2014 Europskog parlamenta i Vijeća ([4]).

([1]) Direktiva 2007/46/EZ Europskog parlamenta i Vijeća od 5. rujna 2007. o uspostavi okvira za homologaciju motornih vozila i njihovih prikolica te sustava, sastavnih dijelova i zasebnih tehničkih jedinica namijenjenih za takva vozila (Okvirna direktiva) (SL L 263, 9.10.2007., str. 1.).

([2]) Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL L 281, 23.11.1995., str. 31.).

([3]) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (SL L 201, 31.7.2002., str. 37.).

([4]) Uredba (EU) br. 165/2014 Europskog parlamenta i Vijeća od 4. veljače 2014. o tahografima u cestovnom prometu, stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u cestovnom prometu i izmjeni Uredbe (EZ) br. 561/2006 Europskog parlamenta i Vijeća o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na cestovni promet (SL L 60, 28.2.2014., str. 1.).

To je datum:

— *nakon kojeg se u vozila koja se prvi put registriraju ugrađuje tahograf koji je povezan s uslugom pozicioniranja na temelju satelitskog navigacijskog sustava,*

— *nakon kojeg vozila koja se prvi put registriraju mogu dostavljati podatke za ciljane provjere na cesti nadležnim nadzornim tijelima dok je vozilo u pokretu*

— *i nakon kojeg vozila koja se prvi put registriraju mogu biti opremljena standardiziranim sučeljima putem kojih podatke koje je tahograf zabilježio ili generirao može na operativan način upotrebljavati vanjski uređaj;*

ddd) „profil zaštite" znači:

dokument koji se upotrebljava kao dio postupka certificiranja u skladu sa zajedničkim mjerilima i omogućuje provedbu neovisnih specifikacija zahtjeva u pogledu osiguravanja informatičke sigurnosti;

eee) „točnost GNSS-a":

u kontekstu bilježenja položaja na temelju globalnog satelitskog navigacijskog sustava (GNSS) tahografima, znači vrijednost horizontalnog slabljenja preciznosti (eng. *Horizontal Dilution of Precision*, HDOP) izračunanu kao minimalne vrijednosti HDOP prikupljene na raspoloživim sustavima GNSS-a.

2 OPĆA OBILJEŽJA I FUNKCIJE UREĐAJA ZA BILJEŽENJE PODATAKA

2.1 **Opća obilježja**

Svrha uređaja za bilježenje podataka je bilježenje, pohrana, prikaz, ispis i generiranje podataka o aktivnostima vozača.

Vozilo opremljeno uređajem za bilježenje podataka u skladu s odredbama ovog Priloga mora imati pokazivač brzine i brojač kilometara. Te funkcije mogu biti ugrađene u uređaj za bilježenje podataka.

01) Uređaj za bilježenje podataka sastoji se od kabela, senzora kretanja i jedinice u vozilu.

02) Sučelje između senzora kretanja i jedinica u vozilu u skladu je sa zahtjevima navedenima u Dodatku 11.

03) Jedinica u vozilu povezana je na globalni satelitski navigacijski sustav ili više njih, kako je određeno u Dodatku 12.

04) Jedinica u vozilu komunicira s čitačima komunikacije ranog otkrivanja na daljinu, kako je utvrđeno u Dodatku 14.

05) Jedinica u vozilu može uključivati sučelje ITS-a koje je određeno u Dodatku 13.

Uređaj za bilježenje podataka može se spojiti na druge uređaje preko dodatnih sučelja i/ili preko neobaveznog sučelja ITS-a.

06) Nijednim priključivanjem ili spajanjem neke funkcije, jednog uređaja ili više njih, bili oni odobreni ili ne, na uređaj za bilježenje podataka ne smije se ometati ili moći ometati pravilan i siguran rad uređaja za bilježenje podataka i odredbi ove Uredbe.

Korisnici uređaja za bilježenje podataka identificiraju se s pomoću tahografskih kartica.

07) Uređajem za bilježenje podataka daje se pravo selektivnog pristupa podatcima i funkcijama u skladu s vrstom i/ili identitetom korisnika.

Uređaj za bilježenje podataka bilježi i pohranjuje podatke u podatkovnu memoriju, uređaj za komunikaciju na daljinu i na tahografske kartice.

To se provodi u skladu s Direktivom 95/46/EZ od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka ([1]), s Direktivom 2002/58/EZ od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija ([2]) te u skladu s člankom 7. Uredbe (EU) br. 165/2014.

2.2 **Funkcije**

08) Uređaj za bilježenje podataka osigurava sljedeće funkcije:

— praćenje umetanja i uklanjanja kartice,

— mjerenje brzine, prijeđenog puta i položaja,

— mjerenje vremena,

— praćenje aktivnosti vozača,

— praćenje statusa vožnje,

— ručne unose vozača:

  — unos mjesta početka i/ili završetka dnevnog radnog vremena,

  — ručni unos aktivnosti vozača,

  — unos posebnih uvjeta,

— upravljanje blokadama poduzeća,

— praćenje aktivnosti nadzora,

— otkrivanje događaja i/ili kvarova,

— ugrađena ispitivanja i samoispitivanja,

— čitanje iz podatkovne memorije,

— bilježenje i pohrana u podatkovnoj memoriji,

— čitanje s tahografskih kartica,

— bilježenje i pohrana na tahografske kartice,

— prikaz,

— ispis,

— upozoravanje,

— preuzimanje podataka na vanjske medije,

— daljinsku komunikaciju za ciljane provjere na cesti,

— izlaz podataka na dodatne uređaje,

— kalibraciju,

— provjeru kalibracije na cesti,

— prilagodbu vremena.

([1]) SL L 281, 23.11.1995., str. 31.
([2]) SL L 201, 31.7.2002., str. 37.

2.3 **Načini rada**

09) Uređaj za bilježenje podataka mora ima četiri načina rada:

— operativni način,

— kontrolni način,

— kalibracijski način,

— način rada poduzeća.

10) Uređaj za bilježenje podataka prebacuje se na sljedeći način rada u skladu s umetnutim valjanim tahografskim karticama u uređaje s kartičnim sučeljem. Za određivanje načina rada nije važna generacija tahografske kartice ako je umetnuta kartica valjana. Kartica radionice prve generacije uvijek se smatra nevažećom ako je umetnuta u jedinicu u vozilu druge generacije.

Način rada		Utor vozača				
		Bez kartice	Kartica vozača	Kontrolna kartica	Kartica radionice	Kartica poduzeća
Utor suvozača	Bez kartice	Operativni	Operativni	Kontrolni	Kalibracijski	Poduzeće
	Kartica vozača	Operativni	Operativni	Kontrolni	Kalibracijski	Poduzeće
	Kontrolna kartica	Kontrolni	Kontrolni	Kontrolni (*)	Operativni	Operativni
	Kartica radionice	Kalibracijski	Kalibracijski	Operativni	Kalibracijski (*)	Operativni
	Kartica poduzeća	Poduzeće	Poduzeće	Operativni	Operativni	Poduzeće (*)

(*) U tim situacijama uređaj za bilježenje podataka upotrebljava samo tahografsku karticu umetnutu u utor vozača.

11) Uređaj za bilježenje podataka zanemaruje umetnute nevažeće kartice, osim prikaza, ispisa ili preuzimanja podataka s istekle kartice, što mora biti omogućeno.

12) Sve funkcije navedene pod točkom 2.2. moraju raditi u svim načinima rada, uz sljedeće iznimke:

— funkcija kalibracije dostupna je samo u kalibracijskom načinu rada,

— funkcija provjere kalibracije na cesti dostupna je samo u kontrolnom načinu rada,

— funkcija upravljanja blokadama poduzeća dostupna je samo u načinu rada poduzeća,

— funkcija praćenja aktivnosti nadzora radi samo u kontrolnom načinu rada,

— funkcija preuzimanja podataka nije dostupna u operativnom načinu rada (osim kako je predviđeno u zahtjevu 193) osim preuzimanja podataka s kartice vozača kad nijedna druga kartica nije umetnuta u jedinicu u vozilu.

13) Uređaj za bilježenje podataka može prenijeti sve podatke na zaslon, pisač ili vanjska sučelja uz sljedeće iznimke:

— u operativnom načinu rada svi osobni identifikacijski podatci (prezime i ime(na)) koji ne odgovaraju umetnutoj tahografskoj kartici ostaju nevidljivi, a svaki broj kartice koji ne odgovara umetnutoj tahografskoj kartici ostaje djelomično nevidljiv (nevidljiva je svaka neparna znamenka slijeva nadesno),

— u načinu rada poduzeća, podatci o vozaču (zahtjevi 102, 105 i 108) mogu se prenijeti samo za razdoblja u kojima nema blokade ili za razdoblja koja nije blokiralo neko drugo poduzeće(koje se identificira s pomoću prvih 13 znamenaka broja kartice poduzeća),

— kad u uređaj za bilježenje podataka nije umetnuta kartica, podatci o vozaču mogu se prenijeti samo za tekući dan i prethodnih osam kalendarskih dana,

— osobni podatci iz jedinice u vozilu ne prenose se preko sučelja ITS-a jedinice u vozilu bez provjere pristanka vozača na kojeg se podatci odnose,

— jedinice u vozilu imaju rok valjanosti tijekom redovnog rada od 15 godina, počevši od datuma izdavanja certifikata za jedinice u vozilu, ali se jedinice u vozilu mogu upotrebljavati dodatna 3 mjeseca samo u svrhu preuzimanja podataka.

2.4 **Sigurnost**

Cilj je sigurnosti sustava zaštititi podatkovnu memoriju sprečavanjem neovlaštena pristupa i manipuliranja podatcima te otkrivanjem svakog takvog pokušaja, zaštititi integritet i autentičnost podataka koji se razmjenjuju između senzora kretanja i jedinice u vozilu, zaštititi integritet i autentičnost podataka koji se razmjenjuju između uređaja za bilježenje podataka i tahografskih kartica, zaštititi integritet i autentičnost podataka koji se razmjenjuju između uređaja za bilježenje podataka i vanjskog uređaja GNSS-a, zaštititi povjerljivost, integritet i autentičnost podataka koji se razmjenjuju komunikacijom ranog otkrivanja na daljinu u svrhu nadzora te provjeriti integritet i autentičnost preuzetih podataka.

14) Kako bi se postigla sigurnost sustava, sljedeći sastavni dijelovi moraju zadovoljavati sigurnosne zahtjeve utvrđene u njihovim profilima zaštite, kako se zahtijeva u Dodatku 10.:

— jedinica u vozilu,

— tahografska kartica,

— senzor kretanja,

— vanjski uređaj GNSS-a (ovaj je profil nužan i primjenjiv samo za vanjsku verziju GNSS-a).

3 ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNOSTI UREĐAJA ZA BILJEŽENJE PODATAKA

3.1 **Praćenje umetanja i uklanjanja kartica**

15) Uređaj za bilježenje podataka nadzire uređaje s kartičnim sučeljem tako da registrira umetanje i uklanjanje kartice.

16) Pri umetanju kartice uređaj za bilježenje podataka otkriva je li umetnuta kartica važeća tahografska kartica i u tom slučaju identificira vrstu kartice i generaciju kartice.

Ako je u uređaj za bilježenje podataka već umetnuta kartica s istim brojem kartice i većim indeksom obnavljanja, kartica se označava kao nevažeća.

Ako je u uređaj za bilježenje podataka već umetnuta kartica s istim brojem kartice i indeksom ponovnog izdavanja, ali s većim indeksom zamjene kartice, kartica se označava kao nevažeća.

17) Uređaj za bilježenje podataka tahografske kartice prve generacije smatra nevažećima nakon što radionica onemogući upotrebu tahografskih kartica prve generacije u skladu s Dodatkom 15. (zahtjev MIG003).

18) Kartice radionice prve generacije koje su umetnute u uređaj za bilježenje podataka druge generacije smatraju se nevažećima.

19) Uređaj za bilježenje podataka mora biti osmišljen tako da se tahografske kartice blokiraju u tom položaju pri pravilnom umetanju u uređaje s kartičnim sučeljem.

20) Tahografske kartice mogu se deblokirati samo kad je vozilo zaustavljeno i nakon što su odgovarajući podatci pohranjeni na kartice. Za deblokiranje kartice potrebna je aktivnost korisnika.

3.2 **Mjerenje brzine, položaja i prijeđenog puta**

21) Senzor kretanja (koji može biti ugrađen u adapter) glavni je izvor za mjerenje brzine i prijeđenog puta.

22) Ta funkcija mora neprekidno mjeriti i dati stanje brojača kilometara koje odgovara ukupnoj udaljenosti koju je vozilo prešlo upotrebom impulsa koje šalje senzor kretanja.

23) Ta funkcija mora neprekidno mjeriti i dati brzinu vozila upotrebom impulsa koje šalje senzor kretanja.

24) Funkcija mjerenja brzine daje informaciju i kreće li se vozilo ili stoji. Smatra se da se vozilo kreće čim funkcija utvrdi više od 1 imp/sek u trajanju od najmanje 5 sekundi na senzoru kretanja; u protivnom se smatra da vozilo stoji.

25) Uređaji za prikaz brzine (brzinomjer) i ukupno prijeđene udaljenosti (brojač kilometara) ugrađeni na svako vozilo opremljeno uređajem za bilježenje podataka koji je sukladan odredbama ove Uredbe moraju udovoljavati zahtjevima u pogledu najvećih dopuštenih odstupanja (vidjeti točke 3.2.1. i 3.2.2.) utvrđenima u ovom Prilogu.

26) Za otkrivanje manipulacije podatcima o kretanju vozila, podatci iz senzora kretanja potvrđuju se podatcima o kretanju vozila iz prijamnika GNSS-a i, prema potrebi, iz drugih izvora koji su neovisni o senzoru kretanja.

27) Ta funkcija mjeri položaj vozila kako bi se omogućilo automatsko bilježenje:

— položaja na kojima vozač i/ili suvozač počinju svoje dnevno radno vrijeme;

— položaja na kojima neprekidno vrijeme vožnje vozača dostiže višekratnik tri sata;

— položaja na kojima vozač i/ili suvozač završavaju svoje dnevno radno vrijeme.

3.2.1 *Mjerenje prijeđene udaljenosti*

28) Prijeđena udaljenost može se mjeriti:

— tako da se zbraja kretanje unaprijed i unatrag, ili

— samo pri kretanju vozila unaprijed.

29) Uređaj za bilježenje podataka mjeri udaljenost od 0 do 9 999 999,9 km.

30) Udaljenost mora biti u granicama sljedećih odstupanja (na najmanjoj udaljenosti od 1 000 m):

— ± 1 % prije ugradnje,

— ± 2 % pri ugradnji i periodičnom pregledu,

— ± 4 % tijekom upotrebe.

31) Udaljenost mora imati razlučivost jednaku ili veću od 0,1 km.

3.2.2 *Mjerenje brzine*

32) Uređaj za bilježenje podataka mjeri brzinu od 0 do 220 km/h.

33) Kako bi se osiguralo najveće dopušteno odstupanje prikazane brzine od ± 6 km/h tijekom upotrebe, a s obzirom na:

— dopušteno odstupanje od ± 2 km/h za ulazna odstupanja (trošenje guma, …),

— dopušteno odstupanje od ± 1 km/h za mjerenja izvršena tijekom ugradnje ili periodičnih pregleda,

za brzine između 20 i 180 km/h i za karakteristične koeficijente vozila između 4 000 i 25 000 imp/km uređaj za bilježenje podataka mjeri brzinu uz dopušteno odstupanje od ± 1 km/h (pri konstantnoj brzini).

Napomena: Razlučivost pohrane podataka ima dodatno dopušteno odstupanje od ± 0,5 km/h za brzinu koju pohranjuje uređaj za bilježenje podataka.

34) Brzina se mora mjeriti ispravno unutar uobičajenih dopuštenih odstupanja u roku od 2 sekunde od završetka promjene brzine kad se brzina mijenjala do 2 m/s^2.

35) Mjerenje brzine mora imati razlučivost jednaku ili bolju od 1 km/h.

3.2.3 *Mjerenje položaja*

36) Uređaj za bilježenje podataka mjeri apsolutni položaj vozila upotrebom prijamnika GNSS-a.

37) Apsolutni položaj mjeri se u koordinatama zemljopisne širine i dužine u stupnjevima i minutama, uz razlučivost od 1/10 minute.

3.3 **Mjerenje vremena**

38) Funkcija mjerenja vremena mora trajno mjeriti i digitalno iskazivati datum i vrijeme po UTC-u.

39) Pri datiranju podataka u uređaju za bilježenje podataka (zapisi, razmjena podataka) i za sve ispise navedene u Dodatku 4. „Ispisi" upotrebljavaju se datum i vrijeme po UTC-u.

40) Za prikaz lokalnog vremena mora biti moguće mijenjati prikaz razlike vremena u polusatnim koracima. Drugi pomaci, osim negativnih ili pozitivnih višekratnika pola sata, nisu dozvoljeni;

41) Odstupanje vremena može biti unutar vrijednosti od ± 2 sekunde po danu u uvjetima homologacije, ako nema prilagodbe vremena.

42) Vrijeme koje se mjeri mora imati razlučivost bolju od 1 sekunde ili jednaku.

43) Na mjerenje vremena ne smije utjecati prekid vanjskog napajanja kraći od 12 mjeseci u uvjetima homologacije.

3.4 **Praćenje aktivnosti vozača**

44) Ova funkcija mora neprekidno i odvojeno pratiti aktivnosti jednog vozača i jednog suvozača.

45) Aktivnosti vozača su VOŽNJA, RAD, DOSTUPNOST ili STANKA/ODMOR.

46) Vozač i/ili suvozač moraju imati mogućnost ručnog odabira RADA, DOSTUPNOSTI ili STANKE/ODMORA.

47) Ako se vozilo kreće, za vozača se automatski odabire VOŽNJA, a za suvozača se automatski odabire DOSTUPNOST.

48) Kad se vozilo zaustavi, za vozača se automatski odabire RAD.

49) Prva promjena aktivnosti u aktivnost ODMOR ili DOSTUPNOST nastaje u roku od 120 sekundi od automatske promjene aktivnosti u aktivnost RAD nakon zaustavljanja vozila. Pretpostavlja se da je promjena aktivnosti nastupila u trenutku kad se vozilo zaustavilo (čime se eventualno poništava promjena aktivnosti u RAD).

50) Ova funkcija mora bilježiti podatke o promjenama aktivnosti u razlučivosti od jedne minute.

51) Ako je u minuti neposredno prije određene kalendarske minute i u minuti neposredno nakon nje registrirana aktivnost VOŽNJA, ta se minuta u cijelosti smatra minutom VOŽNJE.

52) Određena kalendarska minuta, koja se prema zahtjevu 051 ne smatra minutom VOŽNJE, u cijelosti se smatra minutom one vrste aktivnosti koja je najdulje neprekidno trajala u toj minuti (ili posljednja aktivnost od jednako dugih aktivnosti).

53) Ova funkcija mora i trajno pratiti neprekidno vrijeme vožnje i kumulativno vrijeme stanki vozača.

3.5 **Praćenje statusa vožnje**

54) Ova funkcija mora neprekidno i automatski pratiti status vožnje.

55) Status vožnje POSADA odabire se kad se dvije valjane kartice vozača umetnu u uređaj, a u svim se drugim slučajevima odabire status vožnje JEDAN VOZAČ.

3.6 **Unosi vozača**

3.6.1 *Unos mjesta početka i/ili kraja dnevnog radnog vremena*

56) Ova funkcija omogućava unos mjesta početka i/ili završetka dnevnog radnog vremena vozača i/ili suvozača.

57) Mjesta se definiraju kao država te, dodatno i prema potrebi, kao regija, a unose se i potvrđuju ručno.

58) U trenutku uklanjanja kartice vozača uređaj za bilježenje podataka mora potaknuti (su)vozača da unese „mjesto završetka dnevnog radnog vremena”.

59) Vozač zatim unosi trenutačno mjesto vozila, a taj se unos smatra privremenim.

60) S pomoću naredbi u izbornicima mora biti moguće unijeti mjesta početka i/ili završetka dnevnog radnog vremena. Ako se u jednoj kalendarskoj minuti dogodi više od jednog takvog unosa, bilježi se samo unos zadnjeg mjesta početka i unos zadnjeg mjesta završetka, izvršen u tom vremenu.

3.6.2 *Ručni unos aktivnosti vozača i suglasnost vozača u pogledu sučelja ITS-a*

61) Nakon umetanja kartice vozača (ili radionice), i samo tada, uređaj za bilježenje podataka dopušta ručne unose aktivnosti. Ručni unosi aktivnosti izvode se upotrebom vrijednosti lokalnog vremena i datuma vremenske zone (odmak UTC) koja je trenutačno namještena u jedinici u vozilu.

Pri umetanju kartice vozača ili radionice nositelja kartice podsjeća se na:

— datum i vrijeme njegova posljednjeg uklanjanja kartice;

— neobavezno: odmak lokalnog vremena koji je trenutačno namješten u jedinici u vozilu.

Pri prvom umetanju određene kartice vozača ili kartice radionice koja je trenutačno nepoznata jedinici u vozilu, nositelja kartice poziva se da dâ svoju suglasnost za prijenos osobnih podataka iz tahografa preko neobaveznog sučelja ITS-a.

U svakom se trenutku suglasnost vozača (odnosno radionice) može omogućiti ili onemogućiti s pomoću naredbi u izborniku ako je umetnuta kartica vozača (odnosno radionice).

Mora biti moguć unos aktivnosti sa sljedećim ograničenjima:

— vrste aktivnosti su RAD, DOSTUPNOST ili STANKA/ODMOR;

— vremena početka i završetka svake aktivnosti mogu biti samo u okviru razdoblja od posljednjeg uklanjanja do trenutačnog umetanja kartice;

— međusobno vremensko preklapanje aktivnosti nije dopušteno.

Prema potrebi ručni su unosi mogući pri prvom umetanju prethodno neupotrebljavane kartice vozača (ili radionice).

Postupak za ručni unos aktivnosti uključuje onoliko uzastopnih koraka koliko je potrebno za namještanje vrste, vremena početka i vremena završetka svake aktivnosti. Za bilo koji dio vremenskog razdoblja između posljednjeg uklanjanja i trenutačnog umetanja kartice nositelj kartice ima mogućnost ne prijaviti nikakvu aktivnost.

Za vrijeme ručnih unosa povezanih s umetanjem kartice, ako je primjenljivo, nositelj kartice ima mogućnost unijeti:

— mjesto gdje je završilo prethodno dnevno radno vrijeme, povezano s odgovarajućim vremenom (što se zapisuje preko unosa zapisanog pri posljednjem uklanjanju kartice),

— mjesto gdje je trenutačno dnevno radno vrijeme započelo, povezano s odgovarajućim vremenom.

Ako nositelj kartice ne unese mjesto početka ili završetka radnog vremena pri ručnim unosima povezanima s umetanjem kartice, to se smatra izjavom da se njegovo radno vrijeme nije promijenilo od posljednjeg uklanjanja kartice. Sljedeći unos mjesta gdje je završilo prethodno dnevno radno vrijeme zapisuje se preko privremenog unosa zapisanog pri posljednjem uklanjanju kartice.

Ako se unese mjesto, ono se bilježi na odgovarajuću tahografsku karticu.

Ručni se unosi prekidaju:

— ako se kartica ukloni, ili

— ako se vozilo kreće i kartica je u utoru vozača.

Dozvoljeni su dodatni prekidi, npr. zbog isteka vremena nakon određenog razdoblja korisnikove neaktivnosti. Ako se ručni unosi prekinu, uređaj za bilježenje podataka potvrđuje sva potpuno unesena mjesta i aktivnosti (koje imaju nedvojbeno mjesto i vrijeme ili vrstu aktivnosti, vrijeme početka i vrijeme završetka).

Ako se za vrijeme ručnih unosa aktivnosti za prvu umetnutu karticu umetne kartica drugog vozača ili kartica radionice, prije početka ručnih unosa za drugu umetnutu karticu mora se omogućiti završetak ručnih unosa za prvu umetnutu karticu.

Nositelj kartice ima mogućnost unijeti ručne unose prema sljedećem minimalnom postupku:

— ručni unos aktivnosti, kronološkim redom, za razdoblje od posljednjeg uklanjanja kartice do trenutačnog umetanja kartice.

— vrijeme početka prve aktivnosti namješta se na vrijeme uklanjanja kartice. Za svaki sljedeći unos, vrijeme početka unaprijed se namješta tako da odmah slijedi vrijeme završetka ranijeg unosa. Za svaku se aktivnost izabere vrsta aktivnosti i vrijeme završetka.

Postupak završava kad je vrijeme završetka ručno unesene aktivnosti jednako vremenu umetanja kartice. Uređaj za bilježenje podataka može po izboru nositelju kartice omogućiti da do potvrde unosa posebnom naredbom izmijeni bilo koju ručno unesenu aktivnost. Nakon potvrde svaka je takva izmjena zabranjena.

3.6.3 *Unos posebnih stanja*

62) Uređaj za bilježenje podataka mora vozaču dopustiti unos sljedećih dvaju posebnih stanja, u realnom vremenu:

— „IZVAN PODRUČJA PRIMJENE” (početak, završetak) i

— „VOŽNJA TRAJEKTOM/VLAKOM” (početak, završetak)

Stanje „VOŽNJA TRAJEKTOM/VLAKOM” ne može se pojaviti ako je započeto stanje „IZVAN PODRUČJA PRIMJENE”.

Započeto stanje „IZVAN PODRUČJA PRIMJENE” uređaj za bilježenje podataka mora automatski zatvoriti ako se kartica vozača umeće ili uklanja.

Započeto stanje „IZVAN PODRUČJA PRIMJENE” sprečava sljedeće događaje i upozorenja:

— vožnju bez odgovarajuće kartice i

— upozorenja povezana s neprekidnim razdobljem vožnje.

Oznaka početka VOŽNJE TRAJEKTOM/VLAKOM stavlja se prije gašenja motora na trajektu/vlaku.

Započeta VOŽNJA TRAJEKTOM/VLAKOM mora završiti ako nastupi neka od sljedećih mogućnosti:

— vozač je ručno završio VOŽNJU TRAJEKTOM/VLAKOM

— vozač je izbacio svoju karticu

Započeta VOŽNJA TRAJEKTOM/VLAKOM završava ako više nije valjana na temelju odredaba Uredbe (EZ) br. 561/2006.

3.7 **Upravljanje blokadama poduzeća**

63) Ova funkcija omogućuje upravljanje blokadama koje postavi poduzeće kako bi ograničilo pristup podatcima poduzeća za sebe.

64) Blokade poduzeća sastoje se od datuma/vremena početka (zaključavanje blokade) i datuma/vremena završetka (otključavanje blokade) pridruženih identifikaciji poduzeća naznačenoj u broju kartice poduzeća (pri zaključavanju blokade).

65) Blokade se mogu zaključati odnosno otključati samo u realnom vremenu.

66) Otključavanje blokade može izvršiti samo poduzeće čija je blokada postavljena (što je određeno s pomoću prvih 13 znamenaka broja kartice poduzeća) ili

67) otključavanje blokade automatsko je kad drugo poduzeće izvrši zaključavanje blokade.

68) U slučaju zaključavanja blokade poduzeća kad je prethodna blokada bila za isto poduzeće, pretpostavlja se da prethodna blokada nije bila otključana te da je i dalje zaključana.

3.8 **Praćenje aktivnosti nadzora**

69) Ova funkcija prati aktivnosti PRIKAZA, ISPISA, jedinice u vozilu i PREUZIMANJA podataka s kartice te provjere KALIBRACIJE NA CESTI dok je u kontrolnom načinu.

70) Ova funkcija prati i aktivnosti KONTROLE PREKORAČENJA BRZINE dok je u kontrolnom načinu. Smatra se da je kontrola prekoračenja brzine nastala ako je u kontrolnom načinu ispis „prekoračenje brzine" poslan na pisač ili na zaslon ili ako su podatci o „događajima i kvarovima" preuzeti iz podatkovne memorije jedinice u vozilu.

3.9 **Prepoznavanje događaja i/ili kvarova**

71) Ova funkcija otkriva sljedeće događaje i/ili kvarove:

3.9.1 *Događaj „umetanje nevažeće kartice"*

72) Ovaj se događaj aktivira umetanjem bilo koje nevažeće kartice, umetanjem kartice vozača koja je već zamijenjena i/ili ako istekne valjanost umetnute važeće kartice.

3.9.2 *Događaj „konflikt kartica"*

73) Ovaj se događaj aktivira ako se javi bilo koja kombinacija s valjanim karticama označena u tablici s X:

Konflikt kartica		Utor vozača				
		Bez kartice	Kartica vozača	Kontrolna kartica	Kartica radionice	Kartica poduzeća
Utor suvozača	Bez kartice					
	Kartica vozača				X	
	Kontrolna kartica			X	X	X
	Kartica radionice		X	X	X	X
	Kartica poduzeća			X	X	X

3.9.3 *Događaj „vremensko preklapanje"*

74) Ovaj se događaj aktivira kad su datum/vrijeme posljednjeg uklanjanja kartice vozača, očitani s kartice, kasniji nego tekući datum/vrijeme uređaja za bilježenje podataka u koji je umetnuta kartica.

3.9.4 *Događaj „vožnja bez odgovarajuće kartice"*

75) Ovaj se događaj aktivira za bilo koju kombinaciju s valjanim tahografskim karticama označenu znakom X u sljedećoj tablici ako se aktivnost vozača promijeni na VOŽNJU ili ako dođe do promjene načina rada kada je aktivnost vozača VOŽNJA:

Vožnja bez odgovarajuće kartice		Utor vozača				
		Bez (valjane) kartice	Kartica vozača	Kontrolna kartica	Kartica radionice	Kartica poduzeća
Utor suvozača	Bez (valjane) kartice	X		X		X
	Kartica vozača	X		X	X	X
	Kontrolna kartica	X	X	X	X	X
	Kartica radionice	X	X	X		X
	Kartica poduzeća	X	X	X	X	X

3.9.5 *Događaj „umetanje kartice tijekom vožnje"*

76) Ovaj se događaj aktivira kad se tahografska kartica umetne u bilo koji utor u vrijeme dok je aktivnost vozača VOŽNJA.

3.9.6 *Događaj „neispravno zatvaranje posljednje razmjene podataka s karticom"*

77) Ovaj se događaj aktivira kad pri umetanju kartice uređaj za bilježenje podataka utvrdi da unatoč odredbama utvrđenima u stavku 3. točki 1. prethodna razmjena podataka s karticom nije pravilno završena (kartica je uklonjena prije nego što su svi potrebni podatci spremljeni na karticu). Ovaj se događaj aktivira samo karticom vozača i karticom radionice.

3.9.7 *Događaj „prekoračenje brzine"*

78) Ovaj se događaj aktivira pri svakom prekoračenju brzine.

3.9.8 *Događaj „prekid napajanja"*

79) Ovaj se događaj aktivira izvan kalibracijskog ili kontrolnog načina pri svakom prekidu napajanja senzora kretanja i/ili jedinice u vozilu duljem od 200 milisekundi. Prag prekida utvrđuje proizvođač. Padom napajanja zbog pokretanja motora vozila ne aktivira se ovaj događaj.

3.9.9 *Događaj „greška u komunikaciji s uređajem za komunikaciju na daljinu"*

80) Ovaj se događaj aktivira izvan kalibracijskog načina kad uređaj za komunikaciju na daljinu u više od tri pokušaja ne potvrdi uspješan primitak podataka prenesenih na daljinu iz jedinice u vozilu.

3.9.10 *Događaj „izostanak podataka o položaju iz prijamnika GNSS-a"*

81) Ovaj se događaj aktivira **izvan kalibracijskog načina** u slučaju izostanka podataka o položaju iz prijamnika GNSS-a (unutarnjeg ili vanjskog) duljeg od tri sata ukupnog vremena vožnje.

3.9.11 *Događaj „greška u komunikaciji s vanjskim uređajem GNSS-a”*

82) Ovaj se događaj aktivira **izvan kalibracijskog načina** u slučaju prekida komunikacije između vanjskog uređaja GNSS-a i jedinice u vozilu duljeg od 20 uzastopnih minuta ako se vozilo kreće.

3.9.12 *Događaj „greška u podatcima o kretanju”*

83) Ovaj se događaj aktivira **izvan kalibracijskog načina** u slučaju prekida redovnog protoka podataka između senzora kretanja i jedinice u vozilu i/ili u slučaju greške u integritetu podataka ili greške u autentifikaciji podataka tijekom razmjene podataka između senzora kretanja i jedinice u vozilu.

3.9.13 *Događaj „konflikt u kretanju vozila”*

84) Ovaj se događaj aktivira **izvan kalibracijskog načina** ako su podatci o kretanju iz senzora o kretanju u suprotnosti s podatcima o kretanju izračunanima iz unutarnjeg prijamnika GNSS-a ili iz vanjskog uređaja GNSS-a, ili, prema potrebi, iz drugih neovisnih izvora, kako je utvrđeno u Dodatku 12. Ovaj se događaj ne aktivira tijekom vožnje trajektom/vlakom, u uvjetima IZVAN PODRUČJA PRIMJENE ili kad podatci o položaju iz prijamnika GNSS-a nisu raspoloživi.

3.9.14 *Događaj „pokušaj povrede sigurnosti”*

85) Ovaj se događaj aktivira za sve ostale događaje koji utječu na sigurnost senzora kretanja i/ili jedinice u vozilu i/ili vanjskog uređaja GNSS-a, kako je navedeno u Dodatku 10., dok nisu u načinu kalibracije.

3.9.15 *Događaj „vremenski konflikt”*

86) Ovaj se događaj aktivira **izvan kalibracijskog načina**, kad jedinica u vozilu otkrije razliku od više od jedne minute između vremena funkcije mjerenja vremena jedinice u vozilu i vremena iz prijamnika GNSS-a. Taj se događaj bilježi zajedno sa stanjem unutarnjeg sata jedinice u vozilu i izražava zajedno s automatskom prilagodbom vremena. Nakon što se aktivira događaj vremenskog konflikta, jedinica u vozilu neće stvarati druge događaje vremenskog preklapanja sljedećih 12 sati. Taj se događaj ne aktivira ako prijamnik GNSS-a nije mogao otkriti valjani signal GNSS-a u posljednjih 30 dana. Međutim, kad podatci o položaju iz prijamnika GNSS-a ponovno postanu dostupni, provodi se automatska prilagodba vremena.

3.9.16 *Kvar „kartica”*

87) Ovaj se kvar aktivira ako se tijekom rada javi greška na tahografskoj kartici.

3.9.17 *Kvar „uređaj za bilježenje podataka”*

88) Ovaj se kvar aktivira za neku od sljedećih grešaka, dok uređaj nije u kalibracijskom načinu:

— unutarnji kvar jedinice u vozilu,

— kvar pisača,

— kvar zaslona,

— kvar pri preuzimanju podataka,

— kvar senzora,

— kvar prijamnika GNSS-a ili vanjskog uređaja GNSS-a,

— kvar uređaja za komunikaciju na daljinu.

3.10 **Ugrađena ispitivanja i samoispitivanja**

89) Uređaj za bilježenje podataka sam otkriva kvarove samoispitivanjima i ugrađenim ispitivanjima prema sljedećoj tablici:

Podsklop za ispitivanje	Samoispitivanje	Ugrađeno ispitivanje
Softver		Integritet
Podatkovna memorija	Pristup	Pristup, integritet podataka
Uređaji s kartičnim sučeljem	Pristup	Pristup
Tipkovnica		Ručna provjera
Pisač	(ovisi o proizvođaču)	Ispis
Prikaz		Vizualna provjera
Preuzimanje podataka (provodi se samo tijekom preuzimanja podataka)	Ispravan rad	
Senzor	Ispravan rad	Ispravan rad
Uređaja za komunikaciju na daljinu	Ispravan rad	Ispravan rad
Uređaj GNSS-a	Ispravan rad	Ispravan rad

3.11 **Čitanje iz podatkovne memorije**

90) Uređaj za bilježenje podataka mora moći očitati sve podatke pohranjene u svojoj podatkovnoj memoriji.

3.12 **Bilježenje i pohrana u podatkovnoj memoriji**

Za potrebe ovog stavka:

— „365 dana” definira se kao 365 kalendarskih dana prosječne aktivnosti vozača u vozilu. Prosječna dnevna aktivnost u vozilu definira se kao najmanje šest vozača ili suvozača, šest ciklusa umetanja i uklanjanja kartice i 256 promjena aktivnosti. „365 dana” stoga uključuje najmanje 2 190 (su)vozača, 2 190 ciklusa umetanja i uklanjanja kartice i 93 440 promjena aktivnosti,

— prosječan broj položaja u danu definira se kao najmanje šest položaja gdje trenutačno dnevno radno vrijeme počinje, šest položaja gdje neprekidno vrijeme vožnje vozača dostiže višekratnik tri sata i šest položaja gdje dnevno radno vrijeme završava tako da „365 dana” uključuje najmanje 6 570 položaja,

— vremena se bilježe uz razlučivost od jedne minute, osim ako nije drukčije određeno,

— stanje brojača kilometara bilježi se uz razlučivost od jednog kilometra,

— brzine se bilježe uz razlučivost od 1 km/h,

— položaji (zemljopisne širine i dužine) bilježe se u stupnjevima i minutama, uz razlučivost od 1/10 minute te povezanu točnost GNSS-a i vrijeme dobivanja podataka.

91) Na podatke pohranjene u podatkovnoj memoriji ne smije utjecati nikakav vanjski prekid napajanja kraći od dvanaest mjeseci u uvjetima homologacije. Osim toga, na podatke pohranjene u vanjskom uređaju za komunikaciju na daljinu, kako je definiran u Dodatku 14., ne smije utjecati nikakav vanjski prekid napajanja kraći od 28 dana.

92) Uređaj za bilježenje podataka mora moći bilježiti i pohraniti izravno ili neizravno sljedeće podatke u svojoj podatkovnoj memoriji:

3.12.1 *Identifikacijski podatci o uređaju*

3.12.1.1 Identifikacijski podatci jedinice u vozilu

93) Uređaj za bilježenje podataka mora moći u svojoj podatkovnoj memoriji pohraniti sljedeće identifikacijske podatke jedinice u vozilu:

— naziv proizvođača,

— adresu proizvođača,

— kataloški broj,

— serijski broj,

— generaciju jedinice u vozilu,

— mogućnost upotrebe tahografskih kartica prve generacije

— broj verzije softvera,

— datum ugradnje verzije softvera,

— godinu proizvodnje uređaja,

— homologacijski broj.

94) Identifikacijske podatke jedinice u vozilu bilježi i pohranjuje jednom zauvijek proizvođač jedinice u vozilu, osim podataka koji se odnose na softver i homologacijski broj, koji se mogu mijenjati u slučaju ažuriranja softvera te mogućnosti upotrebe tahografskih kartica prve generacije.

3.12.1.2 Identifikacijski podatci senzora kretanja

95) Senzor kretanja mora moći pohraniti u svojoj memoriji sljedeće identifikacijske podatke:

— naziv proizvođača,

— serijski broj,

— homologacijski broj.

— identifikator ugrađene sigurnosne komponente (npr. interni kataloški broj ugrađenog čipa/procesora),

— identifikator operativnog sustava (npr. broj verzije softvera).

96) Identifikacijske podatke senzora kretanja bilježi i pohranjuje jednom zauvijek u senzoru kretanja proizvođač senzora kretanja.

97) Jedinica u vozilu mora moći bilježiti i pohraniti u svojoj podatkovnoj memoriji sljedeće podatke koji se odnose na zadnjih 20 uparivanja senzora kretanja (ako tijekom jednog kalendarskog dana dođe do više uparivanja, pohranjuju se samo prvo i posljednje uparivanje):

Za svako od spomenutih uparivanja bilježe se sljedeći podatci:

— identifikacijski podatci senzora kretanja:

— serijski broj,

— homologacijski broj;

— podatci za povezivanje sa senzorom kretanja:

— datum uparivanja.

3.12.1.3 Identifikacijski podatci globalnih satelitskih navigacijskih sustava

98) Vanjski uređaj GNSS-a mora moći pohraniti u svojoj memoriji sljedeće identifikacijske podatke:

— naziv proizvođača,

— serijski broj,

— homologacijski broj.

— identifikator ugrađene sigurnosne komponente (npr. interni kataloški broj ugrađenog čipa/procesora),

— identifikator operativnog sustava (npr. broj verzije softvera).

99) Identifikacijske podatke bilježi i pohranjuje jednom zauvijek u vanjskom uređaju GNSS-a proizvođač vanjskog uređaja GNSS-a.

100) Jedinica u vozilu mora moći bilježiti i pohraniti u svojoj podatkovnoj memoriji sljedeće podatke koji se odnose na zadnjih 20 povezivanja vanjskih uređaja GNSS-a (ako u tijeku jednog kalendarskog dana dođe do više povezivanja, pohranjuju se samo prvo i posljednje povezivanje):

Za svako od spomenutih povezivanja bilježe se sljedeći podatci:

— identifikacijski podatci vanjskog uređaja GNSS-a:

— serijski broj,

— homologacijski broj.

— podatci za povezivanje s vanjskim uređajem GNSS-a:

— datum povezivanja

3.12.2 *Ključevi i certifikati*

101) Uređaj za bilježenje podataka mora moći pohraniti niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelovima A i B.

3.12.3 *Podatci o umetanju i uklanjanju kartice vozača ili kartice radionice*

102) Za svaki ciklus umetanja i uklanjanja kartice vozača ili kartice radionice u uređaj ili iz njega, uređaj za bilježenje podataka mora zabilježiti i pohraniti u svoju podatkovnu memoriju:

— prezime(na) i ime(na) nositelja kartice pohranjena na kartici,

— broj kartice, državu članicu izdavanja i datum isteka pohranjene na kartici,

— generaciju kartice,

— datum i vrijeme umetanja,

— stanje brojača kilometara vozila pri umetanju kartice,

— utor u koji je kartica umetnuta,

— datum i vrijeme uklanjanja,

— stanje brojača kilometara vozila pri uklanjanju kartice,

— sljedeće informacije pohranjene na kartici o prethodnom vozilu kojim se vozač koristio:

— VRN i državu članicu registracije,

— generaciju jedinice u vozilu (ako je dostupna),

— datum i vrijeme uklanjanja kartice,

— oznaku koja pokazuje je li pri umetanju kartice nositelj kartice ručno unio aktivnosti.

103) Podatkovna memorija mora moći čuvati te podatke najmanje 365 dana.

104) Kad se iscrpi kapacitet za pohranu, novim se podatcima zamjenjuju najstariji podatci.

3.12.4 *Podatci o aktivnosti vozača*

105) Uređaj za bilježenje podataka bilježi i pohranjuje u svoju podatkovnu memoriju svaku promjenu aktivnosti vozača i/ili suvozača i/ili svaku promjenu statusa vožnje i/ili svako umetanje ili uklanjanje kartice vozača ili kartice radionice:

— status vožnje (POSADA, JEDAN VOZAČ),

— utor (VOZAČ, SUVOZAČ),

— status kartice u odgovarajućem utoru (UMETNUTA, NIJE UMETNUTA),

— aktivnost (VOŽNJA, DOSTUPNOST, RAD, STANKA/ODMOR),

— datum i vrijeme promjene.

UMETNUTA označuje da je važeća kartica vozača ili kartica radionice umetnuta u utor. NIJE UMETNUTA označuje suprotno, tj. da važeća kartica vozača ili kartica radionice nije umetnuta u utor (npr. da je umetnuta kartica poduzeća ili da nije umetnuta nikakva kartica).

Podatci o aktivnosti koje ručno unosi vozač ne bilježe se u podatkovnoj memoriji.

106) Podatkovna memorija mora moći čuvati podatke o aktivnosti vozača najmanje 365 dana.

107) Kad se iscrpi kapacitet za pohranu, novim se podatcima zamjenjuju najstariji podatci.

3.12.5 *Mjesta i položaji početka i završetka dnevnog radnog vremena i/ili dostizanja tri sata neprekidnog vremena vožnje*

108) Uređaj za bilježenje podataka bilježi i pohranjuje u svojoj podatkovnoj memoriji:

— mjesta i položaje na kojima vozač i/ili suvozač počinju svoje dnevno radno vrijeme;

— položaje na kojima neprekidno vrijeme vožnje vozača dostiže višekratnik tri sata;

— mjesta i položaje na kojima vozač i/ili suvozač završavaju svoje dnevno radno vrijeme.

109) Ako u tom trenutku položaj vozila nije dostupan iz prijamnika GNSS-a, uređaj za bilježenje podataka upotrebljava posljednji dostupni položaj te povezani datum i vrijeme.

110) Zajedno sa svakim mjestom ili položajem uređaj za bilježenje podataka u svojoj podatkovnoj memoriji bilježi i pohranjuje:

— broj kartice (su)vozača i državu članicu izdavatelja kartice,

— generaciju kartice,

— datum i vrijeme unosa,

— vrstu unosa (početak, završetak ili 3 sata neprekidnog vremena vožnje),

— povezanu točnost GNSS-a, datum i vrijeme ako je primjenjivo;

— stanje brojača kilometara vozila.

111) Podatkovna memorija mora moći čuvati mjesta i položaje početka i završetka dnevnog radnog vremena i/ili dostizanja tri sata neprekidnog vremena vožnje najmanje 365 dana.

112) Kad se iscrpi kapacitet za pohranu, novim se podatcima zamjenjuju najstariji podatci.

3.12.6 *Stanje brojača prijeđenih kilometara*

113) Uređaj za bilježenje podataka bilježi i pohranjuje u svoju podatkovnu memoriju stanje brojača prijeđenih kilometara i pripadajući datum u ponoć svakog kalendarskog dana.

114) Podatkovna memorija mora moći pohranjivati ponoćna stanja brojača kilometara najmanje 365 kalendarskih dana.

115) Kad se iscrpi kapacitet za pohranu, novim se podatcima zamjenjuju najstariji podatci.

3.12.7 *Detaljni podatci o brzini*

116) Uređaj za bilježenje podataka bilježi i sprema u svoju podatkovnu memoriju trenutačnu brzinu vozila te pripadajući datum i vrijeme u svakoj sekundi tijekom najmanje posljednja 24 sata kretanja vozila.

3.12.8 *Podatci o događajima*

Za potrebe ovog podstavka vrijeme se bilježi uz razlučivost od jedne sekunde.

117) Za svaki otkriveni događaj uređaj za bilježenje podataka bilježi i pohranjuje u svoju podatkovnu memoriju sljedeće podatke prema sljedećim pravilima pohrane:

Događaj	Pravila pohrane	Podatci koje je potrebno bilježiti po događaju
Umetanje nevažeće kartice	— deset najnovijih događaja.	— datum i vrijeme događaja, — vrstu, broj, državu članicu izdavatelja kartice ili kartica i generaciju kartice kojom je stvoren događaj. — broj sličnih događaja tog dana
Konflikt kartica	— deset najnovijih događaja.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu izdavatelja kartice ili kartica i generaciju dviju kartica zbog kojih je nastao konflikt.
Vožnja bez odgovarajuće kartice	— najdulji događaj za svaki od deset zadnjih dana pojave, — pet najduljih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.

Događaj	Pravila pohrane	Podatci koje je potrebno bilježiti po događaju
Umetanje kartice tijekom vožnje	— zadnji događaj za svaki od 10 zadnjih dana pojave,	— datum i vrijeme događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju kartice, — broj sličnih događaja tog dana.
Posljednja razmjena podataka s karticom koja nije ispravno zatvorena	— deset najnovijih događaja.	— datum i vrijeme umetanja kartice, — vrstu i broj kartice, državu članicu koje je izdala karticu i generaciju kartice, — posljednju razmjenu podataka očitanih s kartice: — datum i vrijeme umetanja kartice, — VRN, državu članicu registracije i generaciju jedinice u vozilu.
Prekoračenje brzine (1)	— najozbiljniji događaj za svaki od 10 zadnjih dana pojave (tj. događaj s najvećom prosječnom brzinom), — pet najozbiljnijih događaja u zadnjih 365 dana, — prvi događaj koji se dogodio nakon zadnje kalibracije.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — najveću brzinu izmjerenu tijekom događaja, — aritmetički prosjek brzine izmjerene tijekom događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju kartice vozača (ako je primjereno), — broj sličnih događaja tog dana.
Prekid napajanja (2)	— najdulji događaj za svaki od deset zadnjih dana pojave, — pet najduljih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Greška u komunikaciji s uređajem za komunikaciju na daljinu	— najdulji događaj za svaki od deset zadnjih dana pojave, — pet najduljih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Izostanak podataka o položaju iz prijamnika GNSS-a	— najdulji događaj za svaki od deset zadnjih dana pojave, — pet najduljih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.

Događaj	Pravila pohrane	Podatci koje je potrebno bilježiti po događaju
Greška u podatcima o kretanju	— najdulji događaj za svaki od deset zadnjih dana pojave, — pet najduljih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Konflikt u kretanju vozila	— najdulji događaj za svaki od deset zadnjih dana pojave, — pet najduljih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Pokušaji povrede sigurnosti	— deset najnovijih događaja po vrsti događaja.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja (ako je potrebno), — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — vrstu događaja.
Vremenski konflikt	— najdulji događaj za svaki od deset zadnjih dana pojave, — pet najduljih događaja u zadnjih 365 dana.	— datum i vrijeme iz uređaja za bilježenje podataka, — datum i vrijeme GNSS-a, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.

(1) Uređaj za bilježenje podataka bilježi i pohranjuje u svojoj podatkovnoj memoriji i:

— datum i vrijeme posljednje KONTROLE PREKORAČENJA BRZINE,

— datum i vrijeme prvog prekoračenja nakon te KONTROLE PREKORAČENJA BRZINE i

— broj događaja prekoračenja nakon posljednje KONTROLE PREKORAČENJA BRZINE.

(2) Ti se podatci mogu bilježiti samo nakon ponovnog priključenja napajanja; vremena mogu biti poznata uz točnost u minutu.

3.12.9 *Podatci o kvarovima*

Za potrebe ovog podstavka vrijeme se bilježi uz razlučivost od jedne sekunde.

118) Za svaki otkriveni kvar uređaj za bilježenje podataka mora pokušati zabilježiti i pohraniti u svoju podatkovnu memoriju sljedeće podatke prema sljedećim pravilima pohrane:

Kvar	Pravila pohrane	Podatci koje je potrebno bilježiti po kvaru
Kvar kartice	— deset najnovijih kvarova kartice vozača.	— datum i vrijeme početka kvara, — datum i vrijeme završetka kvara, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju kartice.
Kvar uređaja za bilježenje podataka	— deset najnovijih kvarova po vrsti kvara. — prvi kvar koji se dogodio nakon zadnje kalibracije.	— datum i vrijeme početka kvara, — datum i vrijeme završetka kvara, — vrsta kvara, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku kvara.

3.12.10 *Podatci o kalibraciji*

119) Uređaj za bilježenje podataka bilježi i pohranjuje u svojoj podatkovnoj memoriji podatke od važnosti za:

— poznate parametre kalibracije u trenutku aktivacije,

— njegovu prvu kalibraciju nakon aktiviranja,

— njegovu prvu kalibraciju u trenutnom vozilu (koje se identificira VIN brojem),

— 20 posljednjih kalibracija (ako je tijekom jednog kalendarskog dana izvršeno više kalibracija, pohranjuju se samo prva i posljednja izvršena tog dana).

120) Za svaku od spomenutih kalibracija bilježe se sljedeći podatci:

— svrha kalibracije (aktivacija, prva ugradnja, ugradnja, periodični pregled),

— naziv i adresa radionice,

— broj kartice radionice, država članica koja je izdala karticu i datum isteka valjanosti kartice,

— identifikacija vozila,

— parametri koji se ažuriraju ili potvrđuju: w, k, l, dimenzije guma, podešavanje uređaja za ograničavanje brzine, stanje brojača kilometara (nove i stare vrijednost), datum i vrijeme (nove i stare vrijednosti),

— tipovi i identifikatori svih postavljenih plombi.

121) Osim toga, uređaj za bilježenje podataka bilježi i pohranjuje u svoju podatkovnu memoriju mogućnost upotrebe tahografskih kartica prve generacije (bez obzira na to jesu li još uvijek aktivirane).

122) Senzor kretanja bilježi i pohranjuje u svoju memoriju sljedeće podatke o ugradnji senzora kretanja:

— prvo uparivanje s jedinicom u vozilu (datum, vrijeme, homologacijski broj jedinice u vozilu, serijski broj jedinice u vozilu),

— posljednje uparivanje s jedinicom u vozilu (datum, vrijeme, homologacijski broj jedinice u vozilu, serijski broj jedinice u vozilu).

123) Vanjski uređaj GNSS-a bilježi i pohranjuje u svoju memoriju sljedeće podatke o ugradnji vanjskog uređaja GNSS-a:

— prvo povezivanje s jedinicom u vozilu (datum, vrijeme, homologacijski broj jedinice u vozilu, serijski broj jedinice u vozilu),

— posljednje povezivanje s jedinicom u vozilu (datum, vrijeme, homologacijski broj jedinice u vozilu, serijski broj jedinice u vozilu).

3.12.11 *Podatci o prilagodbi vremena*

124) Uređaj za bilježenje podataka bilježi i pohranjuje u svojoj podatkovnoj memoriji podatke koji su važni za prilagodbu vremena izvršenu u kalibracijskom načinu rada izvan okvira redovne kalibracije (def. (f)):

— posljednju prilagodbu vremena,

— pet najvećih prilagodbi vremena.

125) Za svaku od tih prilagodbi vremena bilježe se sljedeći podatci:

— datum i vrijeme, stara vrijednost,

— datum i vrijeme, nova vrijednost,

— naziv i adresa radionice,

— broj kartice radionice, država članica koja je izdala karticu, generacija kartice i datum isteka valjanosti kartice.

3.12.12 *Podatci o aktivnostima nadzora*

126) Uređaj za bilježenje podataka bilježi i pohranjuje u svoju podatkovnu memoriju sljedeće podatke od važnosti za 20 posljednjih aktivnosti nadzora:

— datum i vrijeme nadzora,

— broj kontrolne kartice, državu članicu koja je izdala karticu i generaciju kartice,

— vrstu nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice u vozilu i/ili preuzimanje podataka s kartice i/ili provjera kalibracije na cesti).

127) U slučaju preuzimanja podataka bilježe se i datumi prvog i posljednjeg dana za koje se preuzimaju podatci.

3.12.13 *Podatci o blokadama poduzeća*

128) Uređaj za bilježenje podataka bilježi i pohranjuje u svoju podatkovnu memoriju sljedeće podatke od važnosti za 255 posljednjih blokada poduzeća:

— datum i vrijeme zaključavanja blokade,

— datum i vrijeme otključavanja blokade,

— broj kartice poduzeća, državu članicu koja je izdala karticu i generaciju kartice,

— naziv i adresa poduzeća.

Podatci koji su bili prethodno zaključani blokadom, koja je radi prethodno navedene granične vrijednosti uklonjena iz memorije, tretiraju se kao da nisu zaključani.

3.12.14 *Podatci o aktivnostima preuzimanja podataka*

129) Uređaj za bilježenje podataka bilježi i pohranjuje u svojoj podatkovnoj memoriji sljedeće podatke od važnosti za posljednje preuzimanje podataka iz podatkovne memorije na vanjske medije u načinu rada poduzeća ili kalibracije:

— datum i vrijeme preuzimanja podataka,

— broj kartice poduzeća ili radionice, državu članicu koja je izdala karticu i generaciju kartice,

— naziv poduzeća ili radionice.

3.12.15 *Podatci o posebnim stanjima*

130) Uređaj za bilježenje podataka bilježi u svoju podatkovnu memoriju sljedeće podatke od važnosti za posebna stanja:

— datum i vrijeme unosa,

— vrstu posebnog stanja.

131) Podatkovna memorija mora moći čuvati podatke o posebnim stanjima najmanje 365 dana (uz pretpostavku da se dnevno u prosjeku otvara i zatvara jedno stanje). Kad se iscrpi kapacitet za pohranu, novim se podatcima zamjenjuju najstariji podatci.

3.12.16 *Podatci o tahografskoj kartici*

132) Uređaj za bilježenje podataka mora moći pohraniti sljedeće podatke koji se odnose na različite tahografske kartice koje su upotrijebljene u jedinici u vozilu:

— broj tahografske kartice i njezin serijski broj,

— proizvođača tahografske kartice,

— vrstu tahografske kartice,

— verziju tahografske kartice.

133) Uređaj za bilježenje podataka mora moći pohraniti najmanje 88 takvih zapisa.

3.13 **Očitavanje podataka s tahografskih kartica**

134) Uređaj za bilježenje podataka mora moći očitavati s tahografskih kartica prve i druge generacije, ako je primjereno, sljedeće potrebne podatke:

— identificirati vrstu kartice, nositelja kartice, prethodno upotrijebljeno vozilo, datum i vrijeme posljednjeg uklanjanja kartice i aktivnost odabranu u to vrijeme,

— provjeriti je li posljednja razmjena podataka s karticom ispravno zatvorena,

— izračunati neprekidno vrijeme vožnje vozača, kumulativno vrijeme stanki i kumulativno vrijeme vožnje u prethodnom i tekućem tjednu,

— izraditi ispise prema podatcima zabilježenima na kartici vozača,

— preuzeti podatke s kartice vozača na vanjske medije.

Taj se uvjet primjenjuje samo na tahografske kartice prve generacije ako radionica nije onemogućila njihovu upotrebu.

135) U slučaju greške pri čitanju, uređaj za bilježenje podataka mora ponovo pokušati, najviše tri puta, istu naredbu očitavanja, a ako je očitavanje i tada neuspješno, karticu proglasiti neispravnom i nevažećom.

3.14 **Bilježenje i pohrana podataka na tahografske kartice**

3.14.1 *Bilježenje i pohrana podataka na tahografske kartice prve generacije*

136) Ako radionica nije onemogućila upotrebu tahografskih kartica prve generacije, uređaj za bilježenje podataka bilježi i pohranjuje podatke na potpuno isti način kao što bi to učinio uređaj za bilježenje podataka prve generacije.

137) Uređaj za bilježenje podataka postavlja „podatke o razmjeni podataka s karticom” u karticu vozača ili karticu radionice odmah nakon umetanja kartice.

138) Uređaj za bilježenje podataka ažurira podatke pohranjene na valjanoj kartici vozača, radionice, poduzeća i/ili kontrolnoj kartici sa svim podatcima koji su bitni za razdoblje u kojem je kartica umetnuta i koji se odnose na nositelja kartice. Podatci pohranjeni na tim karticama navedeni su u poglavlju 4.

139) Uređaj za bilježenje podataka ažurira podatke o aktivnosti vozača i mjestima (kako je navedeno u točkama 4.5.3.1.9. i 4.5.3.1.11.) pohranjene na valjanim karticama vozača i/ili karticama radionice s podatcima o aktivnostima i mjestima koje je nositelj kartice unio ručno.

140) Svi događaji koji nisu definirani za uređaje za bilježenje podataka prve generacije ne pohranjuju se na kartice vozača ili radionice.

141) Ažuriranje tahografskih kartica mora biti takvo da se, prema potrebi i uzimajući u obzir stvarni kapacitet pohrane, najnovijim podatcima zamjenjuju najstariji.

142) U slučaju greške u zapisu, uređaj za bilježenje podataka mora pokušati ponovno, najviše tri puta, izvršiti istu naredbu zapisivanja, a ako je i dalje neuspješna, proglasiti karticu neispravnom i nevažećom.

143) Prije deblokiranja kartice vozača, a nakon što su svi potrebni podatci pohranjeni na karticu, uređaj za bilježenje podataka poništava „podatke o razmjeni podataka s karticom”.

3.14.2 *Bilježenje i pohrana podataka na tahografske kartice druge generacije*

144) Tahografske kartice druge generacije moraju sadržavati dvije različite kartične aplikacije, od kojih je prva potpuno jednaka aplikaciji za tahografske kartice prve generacije TACHO, a druga je aplikacija „TACHO_G2”, kako je određeno u poglavlju 4. i Dodatku 2.

145) Uređaj za bilježenje podataka postavlja „podatke o razmjeni podataka s karticom” u karticu vozača ili karticu radionice odmah nakon umetanja kartice.

146) Uređaj za bilježenje podataka ažurira podatke pohranjene na dvije kartične aplikacije za valjane kartice vozača, radionice, poduzeća i/ili kontrolne kartice sa svim podatcima koji su bitni za razdoblje u kojem je kartica umetnuta i koji se odnose na nositelja kartice. Podatci pohranjeni na tim karticama navedeni su u poglavlju 4.

147) Uređaj za bilježenje podataka ažurira podatke o aktivnosti vozača i mjestima (kako je navedeno u točkama 4.5.3.1.9., 4.5.3.1.11., 4.5.3.2.9. i 4.5.3.2.11.) pohranjene na valjanim karticama vozača i/ili karticama radionice s podatcima o aktivnostima i mjestima koje je nositelj kartice unio ručno.

148) Ažuriranje tahografskih kartica mora biti takvo da se, prema potrebi i uzimajući u obzir stvarni kapacitet pohrane, najnovijim podatcima zamjenjuju najstariji.

149) U slučaju greške u zapisu, uređaj za bilježenje podataka mora pokušati ponovno, najviše tri puta, izvršiti istu naredbu zapisivanja, a ako je i dalje neuspješna, proglasiti karticu neispravnom i nevažećom.

150) Prije deblokiranja kartice vozača, a nakon što su svi potrebni podatci pohranjeni na dvije kartične aplikacije za karticu, uređaj za bilježenje podataka poništava podatke o razmjeni podataka s karticom.

3.15 **Prikaz**

151) Prikaz mora imati najmanje 20 znakova.

152) Najmanja veličina znaka je 5 mm u visinu i 3,5 mm u širinu.

153) Prikaz podržava znakove navedene u Dodatku 1. poglavlju 4. „Skupovi znakova". Zaslon može upotrebljavati pojednostavnjene znakove (npr. slovni znakovi s naglaskom mogu se prikazivati bez naglaska ili se mala slova mogu prikazivati kao velika slova).

154) Zaslon mora imati odgovarajuće neblješteće osvjetljenje.

155) Naznake moraju biti vidljive s vanjske strane uređaja za bilježenje podataka.

156) Uređaj za bilježenje podataka mora moći prikazati:

— standardne podatke,

— podatke povezane s upozorenjima,

— podatke povezane s pristupom izborniku,

— ostale podatke koje korisnik zatraži.

Uređaj za bilježenje podataka može prikazati dodatne informacije ako ih je moguće jasno razlikovati od prethodno navedenih podataka.

157) Zaslon uređaja za bilježenje podataka upotrebljava piktograme ili kombinacije piktograma navedene u Dodatku 3. Na zaslonu se mogu prikazati i dodatni piktogrami ili kombinacije piktograma ako ih je moguće jasno razlikovati od ranije spomenutih piktograma ili kombinacija piktograma.

158) Zaslon mora biti uključen uvijek kad se vozilo kreće.

159) Uređaj za bilježenje podataka može imati ručnu ili automatsku mogućnost isključivanja zaslona kad se vozilo ne kreće.

Oblik prikaza naveden je u Dodatku 5.

3.15.1 *Standardni prikaz*

160) Kad nije potreban prikaz nikakvih drugih podataka, uređaj za bilježenje podataka mora standardno prikazivati sljedeće informacije:

— lokalno vrijeme (kao rezultat vremena po UTC-u i odmaka koji namješta vozač),

— način rada,

— trenutačnu aktivnost vozača i trenutačnu aktivnost suvozača,

— informacije koje se odnose na vozača:

— ako je njegova trenutačna aktivnost VOŽNJA, njegovo trenutačno neprekidno vrijeme vožnje i njegovo trenutačno kumulativno vrijeme stanki,

— ako njegova trenutačna aktivnost nije VOŽNJA, trenutačno trajanje te aktivnosti (od trenutka kada je odabrana) i njegovo trenutačno kumulativno vrijeme stanki.

161) Prikaz podataka koji se odnose na svakog vozača mora biti jasan, jednostavan i nedvosmislen. U slučaju kad se informacije o vozaču i suvozaču ne mogu prikazati istodobno, uređaj za bilježenje podataka mora standardno prikazivati podatke koji se odnose na vozača, a korisniku mora omogućiti da prikaže i podatke koji se odnose na suvozača.

162) U slučaju kad širina zaslona ne omogućuje standardno prikazivanje načina rada, uređaj za bilježenje podataka mora nakratko prikazati novi način rada kad se on izmijeni.

163) Uređaj za bilježenje podataka nakratko prikazuje ime nositelja kartice pri umetanju kartice.

164) Ako je započelo stanje „IZVAN PODRUČJA PRIMJENE" ili VOŽNJA TRAJEKTOM/VLAKOM, standardni zaslon mora, upotrebljavajući odgovarajući piktogram, prikazati da je takvo stanje započelo (prihvatljivo je da se tekuća aktivnost vozača ne mora prikazati istodobno).

3.15.2 *Prikaz upozorenja*

165) Uređaj za bilježenje podataka prikazuje informacije upozorenja upotrebljavajući prvenstveno piktograme iz Dodatka 3., dopunjene prema potrebi dodatnim numerički kodiranim podatcima. Može se dodati i tekstualni opis upozorenja na jeziku po odabiru vozača.

3.15.3 *Pristup izbornicima*

166) Uređaj za bilježenje podataka mora osigurati potrebne naredbe putem odgovarajuće strukture izbornika.

3.15.4 *Ostali prikazi*

167) Na zahtjev se mora omogućiti odabir sljedećih prikaza:

— datum i vrijeme po UTC-u te odmak lokalnog vremena,

— sadržaj bilo kojeg od šest ispisa u istom obliku kao što su sami ispisi,

— neprekidno vrijeme vožnje i kumulativno vrijeme stanki vozača,

— neprekidno vrijeme vožnje i kumulativno vrijeme stanki suvozača,

— kumulativno vrijeme vožnje vozača u prethodnom i tekućem tjednu,

— kumulativno vrijeme vožnje suvozača u prethodnom i tekućem tjednu,

neobavezno:

— sadašnje trajanje aktivnosti suvozača (od trenutka kad je odabrana),

— kumulativno vrijeme vožnje vozača u tekućem tjednu,

— kumulativno vrijeme vožnje suvozača za tekuće dnevno radno vrijeme,

— kumulativno vrijeme vožnje vozača za tekuće dnevno radno vrijeme.

168) Prikaz sadržaja ispisa je u slijedu, redak po redak. Ako je širina zaslona manja od 24 slovna znaka, korisniku se pruža potpuna informacija na primjeren način (nekoliko redaka, klizni prikaz teksta, …).

Redci ispisa koji se odnose na ručno unesene informacije mogu se izostaviti iz prikaza.

3.16 **Ispis**

169) Uređaj za bilježenje podataka mora moći ispisati podatke iz svoje podatkovne memorije i/ili tahografskih kartica u obliku sljedećih sedam ispisa:

— dnevni ispis aktivnosti vozača s kartice,

— dnevni ispis aktivnosti vozača iz jedinice u vozilu,

— ispis događaja i kvarova s kartice,

— ispis događaja i kvarova iz jedinice u vozilu,

— ispis tehničkih podataka,

— ispis prekoračenja brzine,

— povijest podataka o tahografskoj kartici za određenu jedinicu u vozilu (vidjeti poglavlje 3.12.16.).

Pojedinosti o obliku i sadržaju ovih ispisa navedeni su u Dodatku 4.

Na kraju ispisa mogu se dati dodatni podatci.

Uređaj za bilježenje podataka može omogućiti i druge ispise ako se oni jasno razlikuju od sedam prethodno spomenutih ispisa.

170) „Dnevni ispis aktivnosti vozača s kartice" i „ispis događaja i kvarova s kartice" moraju biti dostupni samo kad je kartica vozača ili kartica radionice umetnuta u uređaj za bilježenje podataka. Prije početka ispisa uređaj za bilježenje podataka mora ažurirati podatke pohranjene na odgovarajućoj kartici.

171) Kako bi se izradio „dnevni ispis aktivnosti vozača s kartice" ili „ispis događaja i kvarova s kartice", uređaj za bilježenje podataka mora:

— automatski odabrati karticu vozača ili karticu radionice ako je umetnuta samo jedna od navedenih kartica,

— ili omogućiti naredbu za odabir kartice ili izabrati karticu u utoru vozača ako su obje kartice umetnute u uređaj za bilježenje podataka.

172) Pisač mora moći ispisati 24 slovna znaka po retku.

173) Najmanja veličina znaka je 2,1 mm u visinu i 1,5 mm u širinu.

174) Pisač podržava znakove navedene u Dodatku 1. poglavlju 4. „Skupovi znakova".

175) Pisači moraju biti tako izrađeni da daju ispise s takvom oštrinom da se izbjegne svaka nejasnoća pri njihovu čitanju.

176) Ispisi moraju zadržati svoje dimenzije i zapise pod uobičajenim uvjetima vlažnosti (10 – 90 %) i temperature.

177) Homologirani papir za uređaj za bilježenje podataka mora imati odgovarajuću oznaku homologacije i naznaku vrste (vrsta) uređaja za bilježenje podataka u kojima se može upotrebljavati.

178) Ispisi moraju u normalnim uvjetima pohrane, s obzirom na jakost svjetla, vlažnost i temperaturu, ostati jasno čitljivi i prepoznatljivi najmanje dvije godine.

179) Ispisi moraju biti u skladu barem sa specifikacijama ispitivanja utvrđenima u Dodatku 9.

180) Mora postojati i mogućnost da se u ove dokumente dodaju rukom pisane zabilješke, kao što je potpis vozača.

181) Događaje „nestanak papira" pri ispisu uređaj za bilježenje podataka mora riješiti tako da nakon ponovnog umetanja papira ponovno počne ispis od početka ili da se ispis nastavi uz jasno upućivanje na prethodno ispisani dio.

3.17 **Upozorenja**

182) Uređaj za bilježenje podataka upozorava vozača pri otkrivanju svakog događaja i/ili kvara.

183) Upozorenje o prekidu napajanja može se odgoditi do ponovne uspostave napajanja.

184) Uređaj za bilježenje podataka mora upozoriti vozača 15 minuta prije i u trenutku prekoračenja najvećeg dozvoljenog neprekidnog vremena vožnje.

185) Upozorenja moraju biti vizualna. Uz vizualna upozorenja može se osigurati i zvučni signal.

186) Vizualna upozorenja moraju biti korisniku jasno prepoznatljiva, moraju biti smještena u vidnom polju vozača te jasno čitljiva i danju i noću.

187) Prikaz vizualnih upozorenja može biti ugrađen u uređaj za bilježenje podataka i/ili odvojen od uređaja za bilježenje podataka.

188) U potonjem slučaju označen je simbolom „T".

189) Upozorenja moraju trajati najmanje 30 sekundi, osim ako ih korisnik ne potvrdi pritiskom na jednu specifičnu tipku uređaja za bilježenje podataka ili više njih. Prva potvrda ne smije izbrisati prikaz uzroka upozorenja iz sljedećeg stavka.

190) Uzrok upozorenja mora se prikazati na uređaju za bilježenje podataka i ostati vidljiv dok ga korisnik ne potvrdi upotrebom posebne tipke ili naredbe u uređaju za bilježenje podataka.

191) Dodatna upozorenja mogu se predvidjeti dokle god ona ne zbunjuju vozače u pogledu prethodno danih upozorenja.

3.18 **Preuzimanje podataka na vanjske medije**

192) Uređaj za bilježenje podataka mora moći na zahtjev preuzeti podatke iz svoje podatkovne memorije ili s kartice vozača na vanjske medije za pohranu preko priključka za kalibraciju / preuzimanje podataka. Prije početka preuzimanja podataka uređaj za bilježenje podataka mora ažurirati podatke pohranjene na odgovarajućoj kartici.

193) Osim toga, kao neobavezna funkcija, uređaj za bilježenje podataka može, u bilo kojem načinu rada, na bilo koji drugi način preuzimati podatke za poduzeće koje se identificiralo preko tog kanala. U tom se slučaju na takvo preuzimanje podataka primjenjuju prava pristupa podatcima u načinu rada poduzeća.

194) Preuzimanje podataka ne izmjenjuje ili briše niti jedan pohranjeni podatak.

195) Elektronsko sučelje priključka za kalibraciju / preuzimanje podataka opisano je u Dodatku 6.

196) Protokoli preuzimanja podataka opisani su u Dodatku 7.

3.19 **Komunikacija na daljinu za ciljane provjere na cesti**

197) Kad je vozilu dan kontakt, jedinica u vozilu u uređaju za komunikaciju na daljinu svakih 60 sekundi pohranjuje najnovije podatke potrebne u svrhu ciljanih provjera na cesti. Ti se podatci šifriraju i potpisuju kako je određeno u Dodatku 11. i Dodatku 14.

198) Podatci koje je potrebno provjeriti na daljinu moraju biti dostupni čitačima komunikacije na daljinu bežično, kako je određeno u Dodatku 14.

199) Podatci potrebni u svrhu ciljanih provjera na cesti odnose se na sljedeće:

— najnoviji pokušaj povrede sigurnosti,

— najdulji prekid napajanja,

— kvar senzora,

— grešku u podatcima o kretanju,

— konflikt u kretanju vozila,

— vožnju bez valjane kartice,

— umetanje kartice tijekom vožnje,

— podatke o prilagodbi vremena,

— podatke o kalibraciji, uključujući datume dvaju najnovijih pohranjenih zapisa o kalibraciji,

— registarski broj vozila,

— brzinu koju je tahograf zabilježio.

3.20 **Izlazni podatci za dodatne vanjske uređaje**

200) Uređaj za bilježenje podataka može biti opremljen i standardiziranim sučeljima putem kojih podatke koje je tahograf zabilježio ili generirao može u operativnom ili kalibracijskom načinu rada upotrebljavati vanjski uređaj.

U Dodatku 13. određeno je i standardizirano neobavezno sučelje ITS-a. Uz njega mogu postojati i druga slična sučelja ako su u potpunosti u skladu za zahtjevima Dodatka 13. u smislu minimalnog popisa podataka, sigurnosti i suglasnosti vozača.

Sljedeći se zahtjevi primjenjuju na podatke ITS-a koji su stavljeni na raspolaganje putem tog sučelja:

— ti su podatci skup odabranih postojećih podataka iz rječnika tahografskih podataka (Dodatak 1.),

— podskup tih odabranih podataka označen je kao „osobni podatci”,

— podskup „osobnih podataka” dostupan je samo ako je omogućena provjerljiva suglasnost vozača kojom prihvaća da njegovi osobni podatci mogu izaći iz mreže vozila,

— u svakom se trenutku suglasnost vozača može omogućiti ili onemogućiti s pomoću naredbi u izborniku ako je umetnuta kartica vozača,

— skup i podskup podataka šalje se bežičnim Bluetooth protokolom u radijusu kabine vozila, uz frekvenciju osvježavanja od 1 minute,

— povezivanje vanjskog uređaja sa sučeljem ITS-a zaštitit će se namjenskim nasumičnim PIN-om od najmanje četiri broja, koji će se upisati i biti dostupan na zaslonu svake jedinice u vozilu,

— ni u kojim okolnostima zbog prisutnosti sučelja ITS-a ne može se narušiti niti utjecati na ispravno funkcioniranje te sigurnost jedinice u vozilu.

Uz skup odabranih postojećih podataka, koji se smatraju minimalnim podatcima, mogu se osigurati i drugi podatci pod uvjetom da se oni ne mogu smatrati osobnim podatcima.

Uređaj za bilježenje podatka obavješćuje ostale vanjske uređaje o suglasnosti vozača.

Kad je vozilu dan kontakt, ti se podatci neprekidno šalju.

201) Tahografi mogu i dalje biti opremljeni serijskim sučeljem, kako je određeno u Prilogu I.B Uredbi Vijeća (EEZ) 3821/85, kako je zadnje izmijenjena, radi obrnute kompatibilnosti. U svakom slučaju, suglasnost vozača i dalje je potrebna ako se prenose osobni podatci.

3.21 **Kalibracija**

202) Funkcija kalibracije mora omogućavati:

— automatsko uparivanje senzora kretanja s jedinicom u vozilu,

— automatsko povezivanje vanjskog uređaja GNSS-a s jedinicom u vozilu ako je primjenjivo,

— digitalno prilagođavanje konstante uređaja za bilježenje podataka (k) karakterističnom koeficijentu vozila (w),

— prilagodbu trenutačnog vremena u okviru roka valjanosti umetnute kartice radionice,

— podešavanje trenutačne vrijednosti brojača kilometara,

— ažuriranje identifikacijskih podataka senzora kretanja pohranjenih u podatkovnoj memoriji,

— ažuriranje identifikacijskih podataka vanjskog uređaja GNSS-a pohranjenih u podatkovnoj memoriji ako je primjenjivo,

— ažuriranje tipova i identifikatora svih postavljenih plombi,

— ažuriranje ili potvrdu ostalih parametara poznatih uređaju za bilježenje podataka: identifikaciju vozila, w, l, veličinu guma i podešavanje uređaja za ograničavanje brzine ako je primjenjivo.

203) Osim toga, funkcija kalibracije mora omogućiti onemogućivanje upotrebe tahografskih kartice prve generacije u uređaju za bilježenje podataka ako su ispunjeni uvjeti određeni u Dodatku 15.

204) Uparivanje senzora kretanja s jedinicom u vozilu sastoji se barem od sljedećeg:

— ažuriranja instalacijskih podataka senzora kretanja koji se čuvaju u senzoru kretanja (prema potrebi),

— kopiranja iz senzora kretanja u podatkovnu memoriju jedinice u vozilu potrebnih identifikacijskih podataka senzora kretanja.

205) Povezivanje vanjskog uređaja GNSS-a s jedinicom u vozilu sastoji se barem od sljedećeg:

— ažuriranja podataka o ugradnji vanjskog uređaja GNSS-a koje čuva vanjski uređaj GNSS-a (prema potrebi),

— kopiranja s vanjskog uređaja GNSS-a u podatkovnu memoriju jedinice u vozilu potrebnih identifikacijskih podataka o vanjskom uređaju GNSS-a, uključujući serijski broj vanjskog uređaja GNSS-a.

Nakon povezivanja provodi se provjera podataka o položaju GNSS-a.

206) Funkcija kalibriranja mora moći unijeti potrebne podatke preko priključka za kalibraciju/preuzimanje podataka u skladu s protokolom kalibracije utvrđenim u Dodatku 8. Funkcija kalibriranja može unositi potrebne podatke i na druge načine.

3.22 **Provjera kalibracije na cesti**

207) Funkcija provjere kalibracije na cesti mora omogućiti očitavanje serijskog broja senzora kretanja (koji može biti ugrađen u adapter) i serijskog broja vanjskog uređaja GNSS-a (ako je primjenjivo) priključenog na jedinicu u vozilu u trenutku zahtjeva.

208) To očitavanje mora biti moguće barem putem zaslona jedinice u vozilu s pomoću naredbi u izbornicima.

209) Funkcija provjere kalibracije na cesti mora omogućiti i izbor U/I načina rada kalibracijske U/I signalne linije određenog u Dodatku 6., preko sučelja K-linije. To se provodi preko ECUAdjustmentSession, kako je određeno u Dodatku 8., odjeljku 7. Upravljanje ispitnim impulsima – funkcionalna jedinica za upravljanje ulazom/izlazom.

3.23 **Prilagodba vremena**

210) Funkcija prilagodbe vremena mora omogućiti automatsku prilagodbu trenutačnog vremena. Za prilagodbu vremena u uređaju za bilježenje podataka upotrebljavaju se dva izvora vremena: 1) unutarnji sat jedinice u vozilu, 2) prijamnik GNSS-a.

211) Postavljanje vremena unutarnjeg sata jedinice u vozilu automatski se ponovno prilagođava u intervalima od najviše 12 sati. Kad je ta odgoda istekla, a signal GNSS-a još uvijek nije dostupan, vrijeme se postavlja čim jedinica u vozilu dobije pristup valjanom vremenu iz prijamnika GNSS-a, u skladu s uvjetima paljenja vozila. Referentno vrijeme za automatsko postavljanje vremena unutarnjeg sata jedinice u vozilu preuzima se iz prijamnika GNSS-a. Vremenski konflikt aktivira se ako trenutačno vrijeme odstupa više od jedne (1) minute od podataka o vremenu iz prijamnika GNSS-a.

212) Funkcija prilagodbe vremena mora u kalibracijskom načinu omogućavati aktiviranje prilagodbe trenutačnog vremena.

3.24 **Karakteristike radnog učinka**

213) Jedinica u vozilu mora biti u potpunosti operativna u rasponu temperature od – 20 °C do 70 °C, vanjski uređaj GNSS-a u rasponu temperature od – 20 °C do 70 °C, a senzor kretanja u rasponu temperature od – 40 °C do 135 °C. Sadržaj podatkovne memorije mora se očuvati pri temperaturi do – 40 °C.

214) Tahograf mora biti u potpunosti spreman za rad pri rasponu vlažnosti od 10 % do 90 %.

215) Plombe upotrijebljene u pametnom tahografu moraju izdržati iste uvjete kao sastavni dijelovi tahografa na koje su stavljene.

216) Uređaj za bilježenje podataka mora biti zaštićen od prenapona, zamjene polariteta napajanja i kratkih spojeva.

217) Senzori kretanja:

— reagiraju na magnetsko polje koje ometa detekciju kretanja vozila. U takvim okolnostima jedinica u vozilu bilježi i pohranjuje kvar senzora (zahtjev 88) ili,

— imaju senzorski element zaštićen od magnetskih polja ili je na njih neosjetljiv.

218) Uređaj za bilježenje podataka i vanjski uređaj GNSS-a moraju biti u skladu s međunarodnim pravilnikom UNECE-a R10 i zaštićeni od elektrostatičkih pražnjenja i prijelaznih pojava.

3.25 **Materijali**

219) Svi sastavni dijelovi uređaja za bilježenje podataka moraju biti izrađeni od materijala dostatne stabilnosti i mehaničke čvrstoće te stabilnih električnih i magnetskih osobina.

220) U normalnim uvjetima upotrebe svi unutarnji dijelovi uređaja moraju biti zaštićeni od vlage i prašine.

221) Jedinica u vozilu i vanjski uređaj GNSS-a moraju zadovoljavati stupanj zaštite IP 40, a senzor kretanja mora zadovoljavati stupanj zaštite IP 64 prema normi IEC 60529:1989, uključujući A1:1999 i A2:2013.

222) Uređaj za bilježenje podataka mora odgovarati važećim tehničkim specifikacijama u odnosu na ergonomsku izvedbu.

223) Uređaj za bilježenje podataka mora biti zaštićen od slučajnog oštećenja.

3.26 **Oznake**

224) Ako uređaj za bilježenje podataka prikazuje stanje brojača kilometara i brzinu vozila, na zaslonu se pojavljuju sljedeće pojedinosti:

— pokraj broja koji označuje udaljenost, jedinicu mjere za udaljenost označenu kraticom „km”,

— pokraj broja koji pokazuje brzinu, oznaku „km/h”.

Uređaj za bilježenje podataka može se prebaciti i na prikaz brzine u miljama na sat, a u tom se slučaju jedinica mjere za brzinu prikazuje kraticom „mph”. Uređaj za bilježenje podataka može prebaciti i na prikaz udaljenosti u miljama, a u tom se slučaju jedinica mjere za udaljenost prikazuje kraticom „mi”.

225) Opisna pločica pričvršćuje se na svakom odvojenom sastavnom dijelu uređaja za bilježenje podataka i prikazuje sljedeće podatke:

— naziv i adresu proizvođača uređaja,

— kataloški broj proizvođača i godinu proizvodnje uređaja,

— serijski broj uređaja,

— oznaku homologacije uređaja.

226) Ako fizički prostor nije dostatan za prikaz svih prethodno navedenih podataka, identifikacijska pločica mora prikazivati barem naziv i zaštitni znak proizvođača i kataloški broj uređaja za bilježenje podataka.

4 ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNOSTI TAHOGRAFSKIH KARTICA

4.1 **Vidljivi podatci**

Prednja strana mora sadržavati:

227) riječi „kartica vozača” ili „kontrolna kartica” ili „kartica radionice” ili „kartica poduzeća” tiskane velikim slovima na službenom jeziku ili jezicima države članice koja izdaje karticu, prema vrsti kartice;

228) ime države članice koja je izdala karticu (nije obvezno);

229) razlikovnu oznaku države članice koja izdaje karticu, tiskanu u negativu u plavom pravokutniku i okruženu s 12 žutih zvijezda. Razlikovni znakovi sljedeći su:

B	Belgija	LV	Latvija
BG	Bugarska	L	Luksemburg
CZ	Češka	LT	Litva
CY	Cipar	M	Malta
DK	Danska	NL	Nizozemska

D EST	Njemačka Estonija	A PL	Austrija Poljska
GR	Grčka	P RO SK SLO	Portugal Rumunjska Slovačka Slovenija
E	Španjolska	FIN	Finska
F HR H	Francuska Hrvatska Mađarska	S	Švedska
IRL	Irska	UK	Ujedinjena Kraljevina
I	Italija		

230) podatke karakteristične za izdanu karticu, označene kako slijedi:

	Kartica vozača	Kontrolna kartica	Kartica poduzeća ili radionice
1.	prezime vozača	naziv nadzornog tijela	naziv poduzeća ili radionice
2.	ime(na) vozača	prezime nadzornika (ako je primjenjivo)	prezime nositelja kartice (ako je primjenjivo)
3.	datum rođenja vozača	ime(na) nadzornika (ako je primjenjivo)	ime(na) nositelja kartice (ako je primjenjivo)
4.a	datum početka valjanosti kartice		
4.b	datum isteka valjanosti kartice		
4.c	naziv tijela koje je izdalo karticu (može se ispisati na stražnjoj strani)		
4.d	drukčiji broj od broja pod točkom 5., zbog administrativnih razloga (nije obvezno)		
5.a	broj vozačke dozvole (na datum izdavanja kartice vozača)	—	—
5.b	broj kartice		
6.	fotografija vozača	fotografija nadzornika (nije obvezno)	fotografija instalatera (nije obvezno)

	Kartica vozača	Kontrolna kartica	Kartica poduzeća ili radionice
7.	potpis nositelja (nije obvezno)		
8.	uobičajeno boravište ili poštanska adresa nositelja (nije obvezno).	poštanska adresa nadzornog tijela	poštanska adresa poduzeća ili radionice

231) datumi se pišu u obliku „dd/mm/gggg” ili „dd.mm.gggg.” (dan, mjesec, godina).

Stražnja strana mora sadržavati:

232) objašnjenje navedenih stavki na prednjoj strani kartice;

233) uz poseban pisani pristanak nositelja mogu se dodati i informacije koje se ne odnose na vođenje kartice, pri čemu njihovo dodavanje ni na koji način neće izmijeniti upotrebu obrasca kao tahografske kartice.

234) Tahografske kartice moraju se tiskati sa sljedećim prevladavajućim bojama pozadine:

— kartica vozača: bijela,

— kontrolna kartica: plava,

— kartica radionice: crvena,

— kartica poduzeća: žuta.

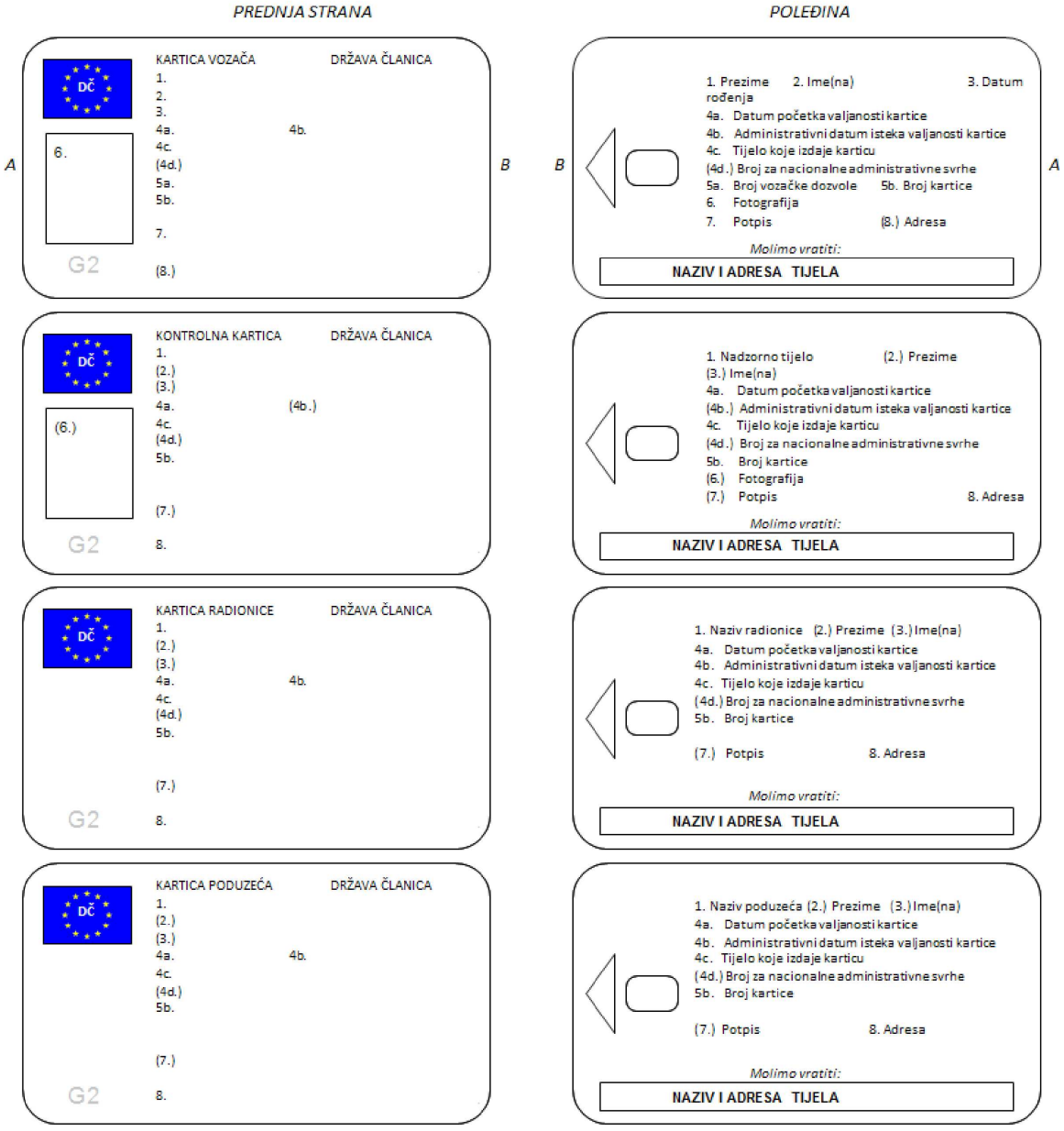
235) Tahografske kartice moraju imati barem sljedeća obilježja za zaštitu tijela kartice od krivotvorenja i neovlaštenog rukovanja:

— sigurnosnu podlogu s tankim guilloche uzorcima i tiskom s duginim efektom (irisnim tiskom),

— na prostoru za fotografiju, sigurnosno izvedena pozadina i fotografija moraju se preklapati,

— barem jednu dvobojnu liniju u mikrotisku.

OBRAZAC ZAJEDNICE ZA TAHOGRAFSKE KARTICE



236) Nakon dogovora s Komisijom države članice mogu dodavati boje i oznake kao što su nacionalni simboli i sigurnosna obilježja, ne dovodeći u pitanje druge odredbe ovog Priloga.

237) Privremene kartice iz članka 26. stavka 4. Uredbe (EU) br. 165/2014 moraju biti u skladu s odredbama ovog Priloga.

4.2 Sigurnost

Sigurnost sustava ima za cilj zaštitu integriteta i autentičnosti podataka koji se razmjenjuju između kartica i uređaja za bilježenje podataka, zaštitu integriteta i autentičnosti podataka koji se preuzimaju s kartica, omogućavanje određenih aktivnosti upisivanja na kartice samo uređaju za bilježenje podataka, dešifriranje određenih podataka, isključivanje svake mogućnosti krivotvorenja podataka pohranjenih na karticama, sprečavanje neovlaštenog rukovanja i otkrivanje svih pokušaja te vrste.

238) Kako bi se postigla sigurnost sustava, tahografske kartice moraju zadovoljavati sigurnosne zahtjeve utvrđene u dodacima 10. i 11.

239) Tahografske kartice moraju biti čitljive u drugoj opremi, kao što su osobna računala.

4.3 **Norme**

240) Tahografske kartice moraju zadovoljavati sljedeće norme:

— ISO/IEC 7810 Identification cards – Physical characteristics,

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

— Part 1: Physical characteristics,

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

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

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

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

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

— Tahografske kartice ispituju se u skladu s normom ISO/IEC 10373-3:2010 *Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices*.

4.4 **Specifikacije okruženja i elektrotehničke specifikacije**

241) Tahografske kartice moraju moći ispravno raditi u svim klimatskim uvjetima uobičajenima na teritoriju Zajednice, pri temperaturnom rasponu od najmanje – 25 °C do + 70 °C s povremenim vršnim porastom do +85 °C, pri čemu „povremeno" označuje ne dulje od 4 sata svaki puta i ne više od 100 puta tijekom vijeka trajanja kartice.

242) Tahografske kartice moraju moći ispravno raditi u rasponu vlažnosti između 10 % i 90 %.

243) Tahografske kartice moraju moći ispravno raditi tijekom razdoblja od pet godina ako se upotrebljavaju u skladu sa specifikacijama okruženja i elektrotehničkim specifikacijama.

244) Tijekom upotrebe tahografske kartice moraju biti u skladu s Pravilnikom UNECE-a R10 o elektromagnetskoj kompatibilnosti te moraju biti zaštićene od elektrostatskih pražnjenja.

4.5 **Pohrana podataka**

Za potrebe ovog stavka

— vremena se bilježe uz razlučivost od jedne minute, osim ako nije drukčije određeno,

— stanje brojača kilometara bilježi se uz razlučivost od jednog kilometra,

— brzine se bilježe uz razlučivost od 1 km/h,

— položaji (zemljopisne širine i dužine) bilježe se u stupnjevima i minutama, uz razlučivost od 1/10 minute.

Funkcije, naredbe i logičke strukture tahografskih kartica koje ispunjavaju zahtjeve u pogledu pohrane podataka navedene su u Dodatku 2.

Ako nije drukčije određeno, pohrana podataka na tahografske kartice organizira se tako da se novim podatcima zamjenjuju najstariji pohranjeni podatci ako je iscrpljena predviđena veličina memorije za određene zapise.

245) U ovom se stavku navodi minimalni kapacitet pohrane podataka za različite datoteke aplikacija. Tahografske kartice moraju moći prikazati uređaju za bilježenje podataka stvarni kapacitet pohrane tih datoteka.

246) Svi dodatni podatci koji se mogu pohraniti na tahografskim karticama, a koji se odnose na druge podatke koji su možda pohranjeni na kartici, pohranjuju se u skladu s Direktivom 95/46/EZ, s Direktivom 2002/58/EZ te u skladu s člankom 7. Uredbe (EU) br. 165/2014.

247) Svaka glavna datoteka (eng. *Master File*, MF) tahografske kartice sadržava najviše pet elementarnih datoteka (eng. *Elementary File*, EF) za upravljanje karticama te identifikaciju aplikacija i čipova kao i dvije namjenske datoteke (eng. *Dedicated File*, DF):

— DF Tachograph koji sadržava aplikaciju kojoj mogu pristupiti jedinice u vozilu prve generacije i koja je prisutna i na tahografskim karticama prve generacije,

— DF Tachograph_G2 koji sadržava aplikaciju kojoj mogu pristupiti jedinice u vozilu druge generacije i koja je prisutna i na tahografskim karticama druge generacije.

Sve pojedinosti o strukturi tahografskih kartica određene su u Dodatku 2.

4.5.1 *Elementarne datoteke za identifikaciju i upravljanje karticama*

4.5.2 *Identifikacija IC kartice*

248) Tahografske kartice moraju moći pohraniti sljedeće identifikacijske podatke pametnih kartica:

— zaustavljanje sata,

— serijski broj kartice (s proizvodnim referencama),

— homologacijski broj kartice,

— identifikaciju (ID) personalizatora kartice,

— identifikaciju ugraditelja (ID),

— identifikator IC.

4.5.2.1 Identifikacija čipa

249) Tahografske kartice moraju moći pohraniti sljedeće identifikacijske podatke o integriranom krugu (IC):

— serijski broj IC,

— proizvodne reference IC.

4.5.2.2 DIR (prisutan samo na tahografskim karticama druge generacije)

250) Tahografske kartice moraju moći pohraniti objekte programskih identifikacijskih podataka određene u Dodatku 2.

4.5.2.3 Podatci ATR-a (uvjetno, prisutno samo na tahografskim karticama druge generacije)

251) Tahografske kartice moraju moći pohraniti sljedeći objekt podataka proširene veličine:

— ako tahografska kartica podržava polja proširene veličine, objekt podataka proširene veličine određen u Dodatku 2.

4.5.2.4 Podatci proširene veličine (uvjetno, prisutno samo na tahografskim karticama druge generacije)

252) Tahografske kartice moraju moći pohraniti sljedeće objekte podataka proširene veličine:

— ako tahografska kartica podržava polja proširene veličine, objekte podataka proširene veličine određene u Dodatku 2.

4.5.3 *Kartica vozača*

4.5.3.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)

4.5.3.1.1 Identifikacija aplikacije

253) Kartica vozača mora moći pohraniti sljedeće programske identifikacijske podatke:

— identifikaciju tahografske aplikacije,

— identifikaciju vrste tahografske kartice.

4.5.3.1.2 Ključevi i certifikati

254) Kartica vozača mora moći pohraniti niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu A.

4.5.3.1.3 Identifikacija kartice

255) Kartica vozača mora moći pohraniti sljedeće identifikacijske podatke kartice:

— broj kartice,

— državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,

— datum početka i isteka valjanosti kartice.

4.5.3.1.4 Identifikacija nositelja kartice

256) Kartica vozača mora moći pohraniti sljedeće identifikacijske podatke nositelja kartice:

— prezime nositelja,

— ime(na) nositelja,

— datum rođenja,

— željeni jezik.

4.5.3.1.5 Preuzimanje podataka s kartice

257) Kartica vozača mora moći pohraniti sljedeće podatke koji se odnose na preuzimanje podataka s kartice:

— datum i vrijeme posljednjeg preuzimanja podataka s kartice (za sve potrebe osim nadzora).

258) Kartica vozača mora moći spremiti jedan takav zapis.

4.5.3.1.6 Podatci o vozačkoj dozvoli

259) Kartica vozača mora moći pohraniti sljedeće podatke o vozačkoj dozvoli:

— državu članicu izdavanja i naziv tijela koje je izdalo dozvolu,

— broj vozačke dozvole (na datum izdavanja kartice).

4.5.3.1.7 Podatci o događajima

Za potrebe ovog podstavka vrijeme se bilježi uz razlučivost od jedne sekunde.

260) Kartica vozača mora moći pohraniti podatke koji se odnose na sljedeće događaje koje je uređaj za bilježenje podataka otkrio dok je bila umetnuta kartica:

— vremensko preklapanje (ako je navedena kartica uzrokovala događaj),

— umetanje kartice tijekom vožnje (ako je navedena kartica predmet događaja),

— neispravan završetak posljednje razmjene podataka s karticom (ako je navedena kartica predmet događaja),

— prekid napajanja,

— grešku u podatcima o kretanju,

— pokušaje povrede sigurnosti.

261) Kartica vozača mora moći pohraniti sljedeće podatke za navedene događaje:

— kod događaja,

— datum i vrijeme početka događaja (ili umetanja kartice ako je događaj u to vrijeme bio u tijeku),

— datum i vrijeme završetka događaja (ili uklanjanja kartice ako je događaj u to vrijeme bio u tijeku),

— VRN i državu članicu registracije vozila u kojem je nastao događaj.

Napomena: U slučaju događaja „vremensko preklapanje”:

— datum i vrijeme početka događaja moraju odgovarati datumu i vremenu uklanjanja kartice iz prethodnog vozila,

— datum i vrijeme završetka događaja moraju odgovarati datumu i vremenu umetanja kartice u aktualno vozilo,

— podatci o vozilu moraju se odnositi na aktualno vozilo, u kojemu je događaj nastupio.

Napomena: U slučaju događaja „neispravno zatvaranje posljednje razmjene podataka s karticom”:

— datum i vrijeme početka događaja moraju odgovarati datumu i vremenu umetanja kartice pri razmjeni podataka koja nije pravilno završena,

— datum i vrijeme završetka događaja moraju odgovarati datumu i vremenu umetanja kartice pri razmjeni podataka tijekom koje je događaj otkriven (tekuća razmjena podataka),

— podatci o vozilu moraju se odnositi na vozilo u kojemu razmjena podataka nije pravilno završena.

262) Kartica vozača mora moći pohraniti podatke za šest posljednjih događaja za svaku vrstu (tj. 36 događaja).

4.5.3.1.8 Podatci o kvarovima

Za potrebe ovog podstavka vrijeme se bilježi uz razlučivost od jedne sekunde.

263) Kartica vozača mora moći pohraniti podatke koji se odnose na sljedeće kvarove koje je uređaj za bilježenje podataka otkrio dok je kartica bila umetnuta:

— kvar kartice (kad je ta kartica predmet kvara),

— kvar uređaja za bilježenje podataka.

264) Kartica vozača mora moći pohraniti sljedeće podatke za navedene kvarove:

— kod kvara,

— datum i vrijeme početka kvara (ili umetanja kartice ako je u tom trenutku kvar bio u tijeku),

— datum i vrijeme završetka kvara (ili uklanjanja kartice ako je u tom trenutku kvar bio u tijeku),

— VRN i državu članicu registracije vozila u kojemu je došlo do kvara.

265) Kartica vozača mora moći pohraniti podatke za dvanaest posljednjih kvarova za svaku vrstu (tj. 24 kvara).

4.5.3.1.9 Podatci o aktivnosti vozača

266) Kartica vozača mora moći pohraniti, za svaki kalendarski dan upotrebe kartice ili za koji je vozač ručno unio podatke, sljedeće podatke:

— datum,

— dnevni brojač prisustva (uvećan za jedan za svaki od navedenih kalendarskih dana),

— ukupnu udaljenost koju je vozač prešao u tom danu,

— status vozača u 00:00,

— kad god je vozač promijenio aktivnost i/ili status vožnje i/ili je umetnuo ili izvadio svoju karticu:

— status vožnje (POSADA, JEDAN VOZAČ),

— utor (VOZAČ, SUVOZAČ),

— status kartice (UMETNUTA, NIJE UMETNUTA),

— aktivnost (VOŽNJA, DOSTUPNOST, RAD, STANKA/ODMOR),

— vrijeme promjene.

267) Memorija kartice vozača mora moći zadržati podatke o aktivnosti vozača najmanje 28 dana (pri čemu se prosječna aktivnost vozača definira kao 93 promjene aktivnosti dnevno).

268) Podatci navedeni u zahtjevima 261, 264 i 266 pohranjuju se na način koji omogućuje učitavanje aktivnosti redoslijedom njihova pojavljivanja, čak i u slučaju vremenskog preklapanja.

4.5.3.1.10 Podatci o upotrijebljenim vozilima

269) Kartica vozača mora moći pohraniti sljedeće podatke za svaki kalendarski dan upotrebe kartice i za svako razdoblje upotrebe dotičnog vozila tog dana (razdobljem upotrebe obuhvaćeni su svi uzastopni ciklusi umetanja i uklanjanja kartice u tom vozilu s gledišta kartice):

— datum i vrijeme prve upotrebe vozila (tj. prvog umetanja kartice u navedenom razdoblju upotrebe vozila ili 00:00 ako je u to vrijeme vozilo već u upotrebi),

— stanje brojača kilometara vozila u to vrijeme,

— datum i vrijeme posljednje upotrebe vozila (tj. posljednjeg uklanjanja kartice u tom razdoblju upotrebe vozila ili 23:59 ako je u to vrijeme vozilo već u upotrebi),

— stanje brojača kilometara vozila u to vrijeme,

— VRN i državu članicu registracije vozila.

270) Kartica vozača mora moći pohraniti najmanje 84 takva zapisa.

4.5.3.1.11 Mjesta početka i/ili završetka dnevnog radnog vremena

271) Kartica vozača mora moći pohraniti sljedeće podatke koji se odnose na mjesto početka i/ili završetka dnevnog radnog vremena koje unese vozač:

— datum i vrijeme unosa (ili datum/vrijeme koje se odnosi na ručni unos),

— vrstu unosa (početak ili kraj, stanje unosa),

— državu i regiju ulaska,

— stanje brojača kilometara vozila.

272) Memorija kartice vozača mora moći pohraniti najmanje 42 para takvih zapisa.

4.5.3.1.12 Podatci o upotrebi kartice

273) Kartica vozača mora moći pohraniti podatke koji se odnose na vozilo u kojem je započela upotreba kartice:

— datum i vrijeme početka upotrebe (tj. umetanje kartice) uz razlučivost od jedne sekunde,

— VRN i državu članicu registracije.

4.5.3.1.13 Podatci o aktivnostima nadzora

274) Kartica vozača mora moći pohraniti sljedeće podatke koji se odnose na aktivnosti nadzora:

— datum i vrijeme nadzora,

— broj kontrolne kartice i državu članicu koja je karticu izdala,

— vrsta nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice vozila i/ili preuzimanje podataka s kartice (vidjeti napomenu)),

— razdoblje preuzimanja podataka (u slučaju preuzimanja podataka),

— VRN i državu članicu registracije vozila u kojoj je izvršen nadzor.

Napomena: preuzimanje podataka s kartice bilježi se samo ako je izvršeno preko uređaja za bilježenje podataka.

275) Kartica vozača mora moći spremiti jedan takav zapis.

4.5.3.1.14 Podatci o posebnim stanjima

276) Kartica vozača mora moći pohraniti sljedeće podatke koji se odnose na posebna stanja koja su unesena dok je kartica bila umetnuta (bez obzira u koji utor):

— datum i vrijeme unosa,

— vrstu posebnog stanja.

277) Kartica vozača mora moći pohraniti najmanje 56 takvih zapisa.

4.5.3.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)

4.5.3.2.1 Identifikacija aplikacije

278) Kartica vozača mora moći pohraniti sljedeće programske identifikacijske podatke:

— identifikaciju tahografske aplikacije,

— identifikaciju vrste tahografske kartice.

4.5.3.2.2 Ključevi i certifikati

279) Kartica vozača mora moći pohraniti niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu B.

4.5.3.2.3 Identifikacija kartice

280) Kartica vozača mora moći pohraniti sljedeće identifikacijske podatke kartice:

— broj kartice,

— državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,

— datum početka i isteka valjanosti kartice.

4.5.3.2.4 Identifikacija nositelja kartice

281) Kartica vozača mora moći pohraniti sljedeće identifikacijske podatke nositelja kartice:

— prezime nositelja,

— ime(na) nositelja,

— datum rođenja,

— željeni jezik.

4.5.3.2.5 Preuzimanje podataka s kartice

282) Kartica vozača mora moći pohraniti sljedeće podatke koji se odnose na preuzimanje podataka s kartice:

— datum i vrijeme posljednjeg preuzimanja podataka s kartice (za sve potrebe osim nadzora).

283) Kartica vozača mora moći spremiti jedan takav zapis.

4.5.3.2.6 Podatci o vozačkoj dozvoli

284) Kartica vozača mora moći pohraniti sljedeće podatke o vozačkoj dozvoli:

— državu članicu izdavanja i naziv tijela koje je izdalo dozvolu,

— broj vozačke dozvole (na datum izdavanja kartice).

4.5.3.2.7 Podatci o događajima

Za potrebe ovog podstavka vrijeme se bilježi uz razlučivost od jedne sekunde.

285) Kartica vozača mora moći pohraniti podatke koji se odnose na sljedeće događaje koje je uređaj za bilježenje podataka otkrio dok je bila umetnuta kartica:

— vremensko preklapanje (ako je navedena kartica uzrokovala događaj),

— umetanje kartice tijekom vožnje (ako je navedena kartica predmet događaja),

— neispravan završetak posljednje razmjene podataka s karticom (ako je navedena kartica predmet događaja),

— prekid napajanja,

— grešku u komunikaciji s uređajem za komunikaciju na daljinu,

— događaj izostanka podataka o položaju iz prijamnika GNSS-a,

— grešku u komunikaciji s vanjskim uređajem GNSS-a

— grešku u podatcima o kretanju,

— konflikt u kretanju vozila,

— pokušaje povrede sigurnosti,

— vremenski konflikt.

286) Kartica vozača mora moći pohraniti sljedeće podatke za navedene događaje:

— kod događaja,

— datum i vrijeme početka događaja (ili umetanja kartice ako je događaj u to vrijeme bio u tijeku),

— datum i vrijeme završetka događaja (ili uklanjanja kartice ako je događaj u to vrijeme bio u tijeku),

— VRN i državu članicu registracije vozila u kojem je nastao događaj.

Napomena: U slučaju događaja „vremensko preklapanje":

— datum i vrijeme početka događaja moraju odgovarati datumu i vremenu uklanjanja kartice iz prethodnog vozila,

— datum i vrijeme završetka događaja moraju odgovarati datumu i vremenu umetanja kartice u aktualnom vozilu,

— podatci o vozilu moraju se odnositi na aktualno vozilo, u kojemu je događaj nastupio.

Napomena: U slučaju događaja „neispravno zatvaranje posljednje razmjene podataka s karticom":

— datum i vrijeme početka događaja moraju odgovarati datumu i vremenu umetanja kartice pri razmjeni podataka koja nije pravilno završena,

— datum i vrijeme završetka događaja moraju odgovarati datumu i vremenu umetanja kartice pri razmjeni podataka tijekom koje je događaj otkriven (tekuća razmjena podataka),

— podatci o vozilu moraju se odnositi na vozilo u kojemu razmjena podataka nije pravilno završena.

287) Kartica vozača mora moći pohraniti podatke za šest posljednjih događaja za svaku vrstu (tj. 66 događaja).

4.5.3.2.8 Podatci o kvarovima

Za potrebe ovog podstavka vrijeme se bilježi uz razlučivost od jedne sekunde.

288) Kartica vozača mora moći pohraniti podatke koji se odnose na sljedeće kvarove koje je uređaj za bilježenje podataka otkrio dok je kartica bila umetnuta:

— kvar kartice (kad je ta kartica predmet kvara),

— kvar uređaja za bilježenje podataka.

289) Kartica vozača mora moći pohraniti sljedeće podatke za navedene kvarove:

— kod kvara,

— datum i vrijeme početka kvara (ili umetanja kartice ako je u tom trenutku kvar bio u tijeku),

— datum i vrijeme završetka kvara (ili uklanjanja kartice ako je u tom trenutku kvar bio u tijeku),

— VRN i državu članicu registracije vozila u kojemu je došlo do kvara.

290) Kartica vozača mora moći pohraniti podatke za dvanaest posljednjih kvarova za svaku vrstu (tj. 24 kvara).

4.5.3.2.9 Podatci o aktivnosti vozača

291) Kartica vozača mora moći pohraniti, za svaki kalendarski dan upotrebe kartice ili za koji je vozač ručno unio podatke, sljedeće podatke:

— datum,

— dnevni brojač prisustva (uvećan za jedan za svaki od navedenih kalendarskih dana),

— ukupnu udaljenost koju je vozač prešao u tom danu,

— status vozača u 00:00,

— kad god je vozač promijenio aktivnost i/ili status vožnje i/ili je umetnuo ili izvadio svoju karticu:

— status vožnje (POSADA, JEDAN VOZAČ),

— utor (VOZAČ, SUVOZAČ),

— status kartice (UMETNUTA, NIJE UMETNUTA),

— aktivnost (VOŽNJA, DOSTUPNOST, RAD, STANKA/ODMOR).

— vrijeme promjene,

292) Memorija kartice vozača mora moći zadržati podatke o aktivnosti vozača najmanje 28 dana (pri čemu se prosječna aktivnost vozača definira kao 93 promjene aktivnosti dnevno).

293) Podatci navedeni u zahtjevima 286, 289 i 291 pohranjuju se na način koji omogućuje učitavanje aktivnosti redoslijedom njihova pojavljivanja, čak i u slučaju vremenskog preklapanja.

4.5.3.2.10 Podatci o upotrijebljenim vozilima

294) Kartica vozača mora moći pohraniti sljedeće podatke za svaki kalendarski dan upotrebe kartice i za svako razdoblje upotrebe dotičnog vozila tog dana (razdobljem upotrebe obuhvaćeni su svi uzastopni ciklusi umetanja i uklanjanja kartice u tom vozilu s gledišta kartice):

— datum i vrijeme prve upotrebe vozila (tj. prvog umetanja kartice u navedenom razdoblju upotrebe vozila ili 00:00 ako je u to vrijeme vozilo već u upotrebi),

— stanje brojača kilometara vozila u to vrijeme prve upotrebe,

— datum i vrijeme posljednje upotrebe vozila (tj. posljednjeg uklanjanja kartice u tom razdoblju upotrebe vozila ili 23:59 ako je kartica upotrijebljena u to vrijeme),

— stanje brojača kilometara vozila u to vrijeme zadnje upotrebe,

— VRN i državu članicu registracije vozila,

— VIN vozila.

295) Kartica vozača mora moći pohraniti najmanje 84 takva zapisa.

4.5.3.2.11 Mjesta i položaji početka i/ili završetka dnevnog radnog vremena

296) Kartica vozača mora moći pohraniti sljedeće podatke koji se odnose na mjesto početka i/ili završetka dnevnog radnog vremena koje unese vozač:

— datum i vrijeme unosa (ili datum/vrijeme koje se odnosi na ručni unos),

— vrstu unosa (početak ili kraj, stanje unosa),

— državu i regiju ulaska,

— stanje brojača kilometara vozila,

— položaj vozila,

— točnost GNSS-a, datum i vrijeme kad je položaj utvrđen.

297) Memorija kartice vozača mora moći pohraniti najmanje 84 para takvih zapisa.

4.5.3.2.12 Podatci o upotrebi kartice

298) Kartica vozača mora moći pohraniti podatke koji se odnose na vozilo u kojem je započela upotreba kartice:

— datum i vrijeme početka upotrebe (tj. umetanje kartice) uz razlučivost od jedne sekunde,

— VRN i državu članicu registracije.

4.5.3.2.13 Podatci o aktivnostima nadzora

299) Kartica vozača mora moći pohraniti sljedeće podatke koji se odnose na aktivnosti nadzora:

— datum i vrijeme nadzora,

— broj kontrolne kartice i državu članicu koja je karticu izdala,

— vrsta nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice vozila i/ili preuzimanje podataka s kartice (vidjeti napomenu)),

— razdoblje preuzimanja podataka (u slučaju preuzimanja podataka),

— VRN i državu članicu registracije vozila u kojoj je izvršen nadzor.

Napomena: sigurnosnim zahtjevima podrazumijeva se da se preuzimanje podataka s kartice bilježi samo ako je izvršeno preko uređaja za bilježenje podataka.

300) Kartica vozača mora moći spremiti jedan takav zapis.

4.5.3.2.14 Podatci o posebnim stanjima

301) Kartica vozača mora moći pohraniti sljedeće podatke koji se odnose na posebna stanja koja su unesena dok je kartica bila umetnuta (bez obzira u koji utor):

— datum i vrijeme unosa,

— vrstu posebnog stanja.

302) Kartica vozača mora moći pohraniti najmanje 56 takvih zapisa.

4.5.3.2.15 Podatci o upotrijebljenoj jedinici u vozilu

303) Kartica vozača mora moći pohraniti sljedeće podatke koji se odnose na različite jedinice u vozilu u kojima je kartica upotrijebljena:

— datum i vrijeme početka razdoblja upotrebe jedinice u vozilu (tj. prvo umetanje kartice u jedinici u vozilu tijekom razdoblja),

— proizvođača jedinice u vozilu,

— vrstu jedinice u vozilu,

— broj verzije softvera u jedinici u vozilu.

304) Kartica vozača mora moći pohraniti najmanje 84 takva zapisa.

4.5.3.2.16 Podatci o mjestima na kojima se dostižu tri sata neprekidne vožnje

305) Kartica vozača mora moći pohraniti sljedeće podatke koji se odnose na položaj vozila na kojem neprekidno vrijeme vožnje vozača dostiže višekratnik tri sata:

— datum i vrijeme kad neprekidno vrijeme vožnje nositelja kartice dostiže višekratnik tri sata,

— položaj vozila,

— točnost GNSS-a, datum i vrijeme kad je položaj utvrđen.

306) Kartica vozača mora moći pohraniti najmanje 252 takva zapisa.

4.5.4 *Kartica radionice*

4.5.4.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)

4.5.4.1.1 Identifikacija aplikacije

307) Kartica radionica mora moći pohraniti sljedeće programske identifikacijske podatke:

— identifikaciju tahografske aplikacije,

— identifikaciju vrste tahografske kartice.

4.5.4.1.2 Ključevi i certifikati

308) Kartica radionice mora moći pohraniti niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu A.

309) Kartica radionice mora moći pohraniti osobni identifikacijski broj (PIN oznaku).

4.5.4.1.3 Identifikacija kartice

310) Kartica radionice mora moći pohraniti sljedeće identifikacijske podatke kartice:

— broj kartice,

— državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,

— datum početka i isteka valjanosti kartice.

4.5.4.1.4 Identifikacija nositelja kartice

311) Kartica radionice mora moći pohraniti sljedeće identifikacijske podatke nositelja kartice:

— naziv radionice,

— adresu radionice,

— prezime nositelja,

— ime(na) nositelja,

— željeni jezik.

4.5.4.1.5 Preuzimanje podataka s kartice

312) Kartica radionice mora moći pohraniti podatke o preuzimanju podataka s kartice na isti način kao i kartica vozača.

4.5.4.1.6 Podatci o kalibraciji i prilagodbi vremena

313) Kartica radionice mora moći pohraniti zapise o kalibraciji i/ili prilagodbama vremena izvršenima dok je kartica bila umetnuta u uređaj za bilježenje podataka.

314) Svaki zapis o kalibraciji mora sadržavati sljedeće podatke:

— svrhu kalibracije (aktiviranje, prva ugradnja, ugradnja, periodični pregled),

— identifikaciju vozila,

— parametre koji se ažuriraju ili potvrđuju (w, k, l, dimenzije guma, podešavanje uređaja za ograničavanje brzine, stanje brojača kilometara (novu i staru vrijednost), datum i vrijeme (novu i staru vrijednosti)),

— identifikaciju uređaja za bilježenje podataka (kataloški broj jedinice u vozilu, serijski broj jedinice u vozilu, serijski broj senzora kretanja).

315) Kartica radionice mora moći pohraniti barem 88 takvih zapisa.

316) Kartica radionice mora sadržavati brojač za označivanje ukupnog broja kalibracija izvršenih s tom karticom.

317) Kartica radionice mora sadržavati brojač za označivanje broja kalibracija izvršenih nakon posljednjeg preuzimanja podataka s kartice.

4.5.4.1.7 Podatci o događajima i kvarovima

318) Kartica radionice mora moći pohraniti podatke o događajima i kvarovima na isti način kao i kartica vozača.

319) Kartica radionice mora moći pohraniti podatke za tri posljednja događaja svake vrste (tj. 18 događaja) i šest posljednjih kvarova svake vrste (tj. 12 kvarova).

4.5.4.1.8 Podatci o aktivnosti vozača

320) Kartica radionice mora moći pohraniti podatke o aktivnostima vozača na isti način kao i kartica vozača.

321) Kartica radionice mora moći čuvati podatke o aktivnostima vozača barem tijekom jednog dana prosječne aktivnosti vozača.

4.5.4.1.9 Podatci o upotrijebljenim vozilima

322) Kartica radionice mora moći pohraniti podatke o upotrijebljenim vozilima na isti način kao i kartica vozača.

323) Kartica radionice mora moći pohraniti barem 4 takva zapisa.

4.5.4.1.10 Podatci o početku i/ili završetku dnevnog radnog vremena

324) Kartica radionice mora moći pohraniti podatke o početku i/ili završetku dnevnog radnog vremena na isti način kao i kartica vozača.

325) Kartica radionice mora moći čuvati najmanje tri para takvih zapisa.

4.5.4.1.11 Podatci o upotrebi kartice

326) Kartica radionice mora moći pohraniti podatke o upotrebi kartice na isti način kao i kartica vozača.

4.5.4.1.12 Podatci o aktivnostima nadzora

327) Kartica radionice mora moći pohraniti podatke o aktivnostima nadzora na isti način kao i kartica vozača.

4.5.4.1.13 Podatci o posebnim stanjima

328) Kartica radionice mora moći pohraniti podatke o posebnim uvjetima na isti način kao i kartica vozača.

329) Kartica radionice mora moći pohraniti barem 2 takva zapisa.

4.5.4.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)

4.5.4.2.1 Identifikacija aplikacije

330) Kartica radionica mora moći pohraniti sljedeće programske identifikacijske podatke:

— identifikaciju tahografske aplikacije,

— identifikaciju vrste tahografske kartice.

4.5.4.2.2 Ključevi i certifikati

331) Kartica radionice mora moći pohraniti niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu B.

332) Kartica radionice mora moći pohraniti osobni identifikacijski broj (PIN oznaku).

4.5.4.2.3 Identifikacija kartice

333) Kartica radionice mora moći pohraniti sljedeće identifikacijske podatke kartice:

— broj kartice,

— državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,

— datum početka i isteka valjanosti kartice.

4.5.4.2.4 Identifikacija nositelja kartice

334) Kartica radionice mora moći pohraniti sljedeće identifikacijske podatke nositelja kartice:

— naziv radionice,

— adresu radionice,

— prezime nositelja,

— ime(na) nositelja,

— željeni jezik.

4.5.4.2.5 Preuzimanje podataka s kartice

335) Kartica radionice mora moći pohraniti podatke o preuzimanju podataka s kartice na isti način kao i kartica vozača.

4.5.4.2.6 Podatci o kalibraciji i prilagodbi vremena

336) Kartica radionice mora moći pohraniti zapise o kalibraciji i/ili prilagodbama vremena izvršenima dok je kartica bila umetnuta u uređaj za bilježenje podataka.

337) Svaki zapis o kalibraciji mora sadržavati sljedeće podatke:

— svrhu kalibracije (aktiviranje, prva ugradnja, ugradnja, periodični pregled),

— identifikaciju vozila,

— parametre koji se ažuriraju ili potvrđuju (w, k, l, dimenzije guma, postavke uređaja za ograničavanje brzine, stanje brojača kilometara (nove i stare vrijednosti), datum i vrijeme (nove i stare vrijednosti)),

— identifikaciju uređaja za bilježenje podataka (kataloški broj jedinice u vozilu, serijski broj jedinice u vozilu, serijski broj senzora kretanja, serijski broj uređaja za komunikaciju na daljinu i serijski broj vanjskog uređaja GNSS-a, ako je primjenjivo),

— tip i identifikator svih postavljenih plombi,

— sposobnost jedinice u vozilu da upotrebljava tahografske kartice prve generacije (omogućeno ili ne).

338) Kartica radionice mora moći pohraniti barem 88 takvih zapisa.

339) Kartica radionice mora sadržavati brojač za označivanje ukupnog broja kalibracija izvršenih s tom karticom.

340) Kartica radionice mora sadržavati brojač za označivanje broja kalibracija izvršenih nakon posljednjeg preuzimanja podataka s kartice.

4.5.4.2.7 Podatci o događajima i kvarovima

341) Kartica radionice mora moći pohraniti podatke o događajima i kvarovima na isti način kao i kartica vozača.

342) Kartica radionice mora moći pohraniti podatke za tri posljednja događaja svake vrste (tj. 33 događaja) i šest posljednjih kvarova svake vrste (tj. 12 kvarova).

4.5.4.2.8 Podatci o aktivnosti vozača

343) Kartica radionice mora moći pohraniti podatke o aktivnostima vozača na isti način kao i kartica vozača.

344) Kartica radionice mora moći čuvati podatke o aktivnostima vozača barem tijekom jednog dana prosječne aktivnosti vozača.

4.5.4.2.9 Podatci o upotrijebljenim vozilima

345) Kartica radionice mora moći pohraniti podatke o upotrijebljenim vozilima na isti način kao i kartica vozača.

346) Kartica radionice mora moći pohraniti barem 4 takva zapisa.

4.5.4.2.10 Podatci o početku i/ili završetku dnevnog radnog vremena

347) Kartica radionice mora moći pohraniti podatke o početku i/ili završetku dnevnog radnog vremena na isti način kao i kartica vozača.

348) Kartica radionice mora moći čuvati najmanje tri para takvih zapisa.

4.5.4.2.11 Podatci o upotrebi kartice

349) Kartica radionice mora moći pohraniti podatke o upotrebi kartice na isti način kao i kartica vozača.

4.5.4.2.12 Podatci o aktivnostima nadzora

350) Kartica radionice mora moći pohraniti podatke o aktivnostima nadzora na isti način kao i kartica vozača.

4.5.4.2.13 Podatci o upotrijebljenoj jedinici u vozilu

351) Kartica radionice mora moći pohraniti sljedeće podatke koji se odnose na različite jedinice u vozilu u kojima je kartica upotrijebljena:

— datum i vrijeme početka razdoblja upotrebe jedinice u vozilu (tj. prvo umetanje kartice u jedinicu u vozilu tijekom razdoblja),

— proizvođača jedinice u vozilu,

— vrstu jedinice u vozilu,

— broj verzije softvera u jedinici u vozilu.

352) Kartica radionice mora moći pohraniti barem 4 takva zapisa.

4.5.4.2.14 Podatci o mjestima na kojima se dostižu tri sata neprekidne vožnje

353) Kartica radionice mora moći pohraniti sljedeće podatke koji se odnose na položaj vozila na kojem neprekidno vrijeme vožnje vozača dostiže višekratnik tri sata:

— datum i vrijeme kad neprekidno vrijeme vožnje nositelja kartice dostiže višekratnik tri sata,

— položaj vozila,

— točnost GNSS-a, datum i vrijeme kad je položaj utvrđen.

354) Kartica radionice mora moći pohraniti barem 18 takvih zapisa.

4.5.4.2.15 Podatci o posebnim stanjima

355) Kartica radionice mora moći pohraniti podatke o posebnim uvjetima na isti način kao i kartica vozača.

356) Kartica radionice mora moći pohraniti barem 2 takva zapisa.

4.5.5 *Kontrolna kartica*

4.5.5.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)

4.5.5.1.1 Identifikacija aplikacije

357) Kontrolna kartica mora moći pohraniti sljedeće programske identifikacijske podatke:

— identifikaciju tahografske aplikacije,

— identifikaciju vrste tahografske kartice.

4.5.5.1.2 Ključevi i certifikati

358) Kontrolna kartica mora moći pohraniti niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu A.

4.5.5.1.3 Identifikacija kartice

359) Kontrolna kartica mora moći pohraniti sljedeće identifikacijske podatke kartice:

— broj kartice,

— državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,

— datum početka i isteka valjanosti kartice (ako postoji).

4.5.5.1.4 Identifikacija nositelja kartice

360) Kontrolna kartica mora moći pohraniti sljedeće identifikacijske podatke nositelja kartice:

— naziv nadzornog tijela,

— adresu nadzornog tijela,

— prezime nositelja,

— ime(na) nositelja,

— željeni jezik.

4.5.5.1.5 Podatci o aktivnostima nadzora

361) Kontrolna kartica mora moći pohraniti sljedeće podatke o aktivnostima nadzora:

— datum i vrijeme nadzora,

— vrstu nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice u vozilu i/ili preuzimanje podataka s kartice i/ili provjera kalibracije na cesti).

— razdoblje preuzimanja podataka (ako postoji),

— VRN i tijelo države članice koje je registriralo kontrolirano vozilo.

— broj kartice i državu članicu koja je izdala kontroliranu vozačku karticu.

362) Kartica mora moći spremiti najmanje 230 takvih zapisa.

4.5.5.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)

4.5.5.2.1 Identifikacija aplikacije

363) Kontrolna kartica mora moći pohraniti sljedeće programske identifikacijske podatke:

— identifikaciju tahografske aplikacije,

— identifikaciju vrste tahografske kartice.

4.5.5.2.2 Ključevi i certifikati

364) Kontrolna kartica mora moći pohraniti niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu B.

4.5.5.2.3 Identifikacija kartice

365) Kontrolna kartica mora moći pohraniti sljedeće identifikacijske podatke kartice:

— broj kartice,

— državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,

— datum početka i isteka valjanosti kartice (ako postoji).

4.5.5.2.4 Identifikacija nositelja kartice

366) Kontrolna kartica mora moći pohraniti sljedeće identifikacijske podatke nositelja kartice:

— naziv nadzornog tijela,

— adresu nadzornog tijela,

— prezime nositelja,

— ime(na) nositelja,

— željeni jezik.

4.5.5.2.5 Podatci o aktivnostima nadzora

367) Kontrolna kartica mora moći pohraniti sljedeće podatke o aktivnostima nadzora:

— datum i vrijeme nadzora,

— vrsta nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice u vozilu i/ili preuzimanje podataka s kartice i/ili provjera kalibracije na cesti).

— razdoblje preuzimanja podataka (ako postoji),

— VRN i tijelo države članice koje je registriralo kontrolirano vozilo,

— broj kartice i državu članicu koja je izdala kontroliranu vozačku karticu.

368) Kartica mora moći spremiti najmanje 230 takvih zapisa.

4.5.6 *Kartica poduzeća*

4.5.6.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)

4.5.6.1.1 Identifikacija aplikacije

369) Kartica poduzeća mora moći pohraniti sljedeće programske identifikacijske podatke:

— identifikaciju tahografske aplikacije,

— identifikaciju vrste tahografske kartice.

4.5.6.1.2 Ključevi i certifikati

370) Kartica poduzeća mora moći pohraniti niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu A.

4.5.6.1.3 Identifikacija kartice

371) Kartica poduzeća mora moći pohraniti sljedeće identifikacijske podatke kartice:

— broj kartice,

— državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,

— datum početka i isteka valjanosti kartice (ako postoji).

4.5.6.1.4 Identifikacija nositelja kartice

372) Kartica poduzeća mora moći pohraniti sljedeće identifikacijske podatke nositelja kartice:

— naziv poduzeća,

— adresu poduzeća.

4.5.6.1.5 Podatci o aktivnostima poduzeća

373) Kartica poduzeća mora moći pohraniti sljedeće podatke o aktivnostima poduzeća:

— datum i vrijeme aktivnosti,

— vrstu aktivnosti (zaključavanje ili otključavanje blokade jedinice u vozilu, preuzimanje podataka s jedinice u vozilu i/ili s kartice),

— razdoblje preuzimanja podataka (ako postoji),

— VRN i tijelo koje je registriralo vozilo u državi članici,

— broj kartice i državu članicu izdavanja kartice (u slučaju preuzimanja podataka s kartice).

374) Kartica poduzeća mora moći pohraniti barem 230 takvih zapisa.

4.5.6.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)

4.5.6.2.1 Identifikacija aplikacije

375) Kartica poduzeća mora moći pohraniti sljedeće programske identifikacijske podatke:

— identifikaciju tahografske aplikacije,

— identifikaciju vrste tahografske kartice.

4.5.6.2.2 Ključevi i certifikati

376) Kartica poduzeća mora moći pohraniti niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu B.

4.5.6.2.3 Identifikacija kartice

377) Kartica poduzeća mora moći pohraniti sljedeće identifikacijske podatke kartice:

— broj kartice,

— državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,

— datum početka i isteka valjanosti kartice (ako postoji).

4.5.6.2.4 Identifikacija nositelja kartice

378) Kartica poduzeća mora moći pohraniti sljedeće identifikacijske podatke nositelja kartice:

— naziv poduzeća,

— adresu poduzeća.

4.5.6.2.5 Podatci o aktivnostima poduzeća

379) Kartica poduzeća mora moći pohraniti sljedeće podatke o aktivnostima poduzeća:

— datum i vrijeme aktivnosti,

— vrstu aktivnosti (zaključavanje ili otključavanje blokade jedinice u vozilu, preuzimanje podataka s jedinice u vozilu i/ili s kartice),

— razdoblje preuzimanja podataka (ako postoji),

— VRN i tijelo koje je registriralo vozilo u državi članici,

— broj kartice i državu članicu izdavanja kartice (u slučaju preuzimanja podataka s kartice).

380) Kartica poduzeća mora moći pohraniti barem 230 takvih zapisa.

5 UGRADNJA UREĐAJA ZA BILJEŽENJE PODATAKA

5.1 **Ugradnja**

381) Novi se uređaj za bilježenje podataka isporučuje neaktiviran instalaterima ili proizvođačima vozila sa svim parametrima za kalibraciju navedenima u poglavlju 3.21. podešenima na odgovarajuće i valjane osnovne vrijednosti. Ako neka određena vrijednost nije podešena, slovni parametri zamjenjuju se nizom znakova „?”, a numerički parametri postavljaju se na „0”. Dostava dijelova uređaja za bilježenje podataka koji se odnose na sigurnost može se ograničiti ako se tako zahtijeva za vrijeme sigurnosnog certificiranja.

382) Prije aktivacije uređaj za bilježenje podataka mora imati pristup funkciji kalibracije, čak i kada nije u kalibracijskom načinu rada.

383) Prije aktivacije uređaj za bilježenje podataka ne smije zapisivati niti pohraniti podatke iz točaka 3.12.3., 3.12.9. i 3.12.12. do uključujući 3.12.15.

384) Tijekom ugradnje proizvođači vozila moraju unaprijed podesiti sve poznate parametre.

385) Proizvođači vozila ili instalateri aktiviraju ugrađeni uređaj za bilježenje podataka najkasnije prije upotrebe vozila u području primjene Uredbe (EZ) br. 561/2006.

386) Aktiviranje uređaja za bilježenje podataka vrši se automatski prvim umetanjem valjane kartice radionice u bilo koji uređaj kartičnog sučelja.

387) Posebne operacije uparivanja senzora kretanja i jedinice u vozilu, ako ih ima, vrše se automatski prije ili tijekom aktiviranja.

388) Slično se posebne operacije povezivanja senzora kretanja i jedinice u vozilu, ako ih ima, vrše automatski prije ili tijekom aktiviranja.

389) Nakon aktiviranja uređaj za bilježenje podataka mora u potpunosti izvršavati funkcije i prava pristupa podatcima.

390) Nakon aktiviranja uređaj za bilježenje podataka uređaju za komunikaciju na daljinu prenosi sigurne podatke potrebne za ciljane provjere na daljinu.

391) Funkcije bilježenja i pohrane u uređaju za bilježenje podataka postižu punu radnu sposobnost nakon njegova aktiviranja.

392) Nakon ugradnje slijedi kalibracija. Prva kalibracija ne mora nužno uključivati unos registracijskog broja vozila (VRN) ako ga ovlaštena radionica koja treba obaviti tu kalibraciju ne zna. Samo u tim okolnostima vlasnik vozila samo jednom može unijeti VRN koristeći se svojom karticom poduzeća prije upotrebe vozila u području primjene Uredbe (EZ) br. 561/2006 (npr. koristeći se naredbama putem odgovarajuće strukture izbornika sučelja čovjek-stroj jedinice u vozilu) ([1]). Svako ažuriranje ili potvrda tog unosa moguća je samo karticom radionice.

393) Za ugradnju vanjskog uređaja GNSS-a potrebno je povezivanje s vanjskom jedinicom u vozilu i naknadna provjera podataka GNSS-a o položaju.

394) Uređaj za bilježenje podataka mora biti smješten u vozilu tako da omogući vozaču pristup potrebnim funkcijama iz njegova sjedala.

([1]) SL L 102, 11.4.2006., str. 1.

5.2 **Tipska pločica**

395) Nakon provjere uređaja za bilježenje podataka pri ugradnji na njega se pričvršćuje jasno vidljiva i lako dostupna tipska pločica, koja je trajno ugravirana ili tiskana. Ako to nije moguće, pločica se pričvršćuje na stup „B” vozila tako da je jasno vidljiva. Za vozila koja nemaju stup „B” tipska se pločica pričvršćuje na okvir vrata na vozačevoj strani vozila i jasno je vidljiva u svim slučajevima.

Poslije svakog pregleda kod ovlaštenog instalatera ili u ovlaštenoj radionici na mjesto prethodne postavlja se nova pločica.

396) Na pločici moraju biti navedeni najmanje sljedeći podatci:

— naziv, adresa ili trgovački naziv ovlaštenog instalatera ili radionice,

— karakteristični koeficijent vozila u obliku „w = … imp/km”,

— konstanta uređaja za bilježenje podataka u obliku „k = … imp/km”,

— djelatni opseg guma kotača u obliku „l = … mm”,

— veličina guma,

— datum mjerenja karakterističnog koeficijenta vozila i djelatnog opsega guma kotača,

— identifikacijska oznaka vozila,

— prisutnost (ili neprisutnost) vanjskog uređaja GNSS-a,

— serijski broj vanjskog uređaja GNSS-a,

— serijski broj uređaja za komunikaciju na daljinu,

— serijski broj svih postavljenih plombi,

— dio vozila na koji se ugrađuje adapter, ako postoji,

— dio vozila na koji se ugrađuje senzor kretanja, ako nije priključen na mjenjač ili ako se ne upotrebljava adapter,

— opis boje kabela između adaptera i onog dijela vozila iz kojeg prima ulazne impulse,

— serijski broj ugrađenog senzora kretanja adaptera.

397) Samo za vozila M1 i N1 koja su opremljena adapterom u skladu s Uredbom Komisije (EZ) br. 68/2009 ([1]), kako je zadnje izmijenjena, a kad nije moguće uključiti sve potrebne informacije opisane u zahtjevu 396, može se upotrijebiti druga, dodatna pločica. U takvim slučajevima dodatna pločica sadržava najmanje zadnje četiri alineje opisane u zahtjevu 396.

Ako se upotrebljava druga, dodatna pločica, pričvršćuje se pored ili uz prvu primarnu pločicu, opisanu u zahtjevu 396, i ima istu razinu zaštite. Nadalje, na dodatnoj pločici je naveden i naziv, adresa ili trgovački naziv ovlaštenog instalatera ili radionice koja je izvršila ugradnju te datum ugradnje.

([1]) Uredba Komisije (EZ) br. 68/2009 od 23. siječnja 2009. o devetoj prilagodbi tehničkom napretku Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u cestovnom prometu (SL L 21, 24.1.2009., str. 3.).

5.3 **Plombiranje**

398) Sljedeći dijelovi moraju se zaštititi plombom:

— svaki spoj čije bi razdvajanje uzrokovalo izmjene ili gubitak podataka koje ne bi bilo moguće otkriti (to se može, na primjer, primijeniti na postavljanje senzora kretanja na mjenjač, adapter za vozila M1/N1, vezu s vanjskim GNSS-om ili jedinicu u vozilu);

— tipska pločica, osim ako je pričvršćena na takav način da ju je nemoguće ukloniti bez uništavanja oznaka na njoj.

399) Prethodno navedene plombe mogu se ukloniti:

— u izvanrednom slučaju,

— pri ugradnji, podešavanju ili popravku uređaja za ograničenje brzine ili nekog drugog uređaja koji pridonosi sigurnosti na cesti, pod uvjetom da uređaj za bilježenje podataka nastavi raditi pouzdano i ispravno te da ovlašteni instalater ili radionica ponovno postavi plombe (u skladu s poglavljem 6.) odmah nakon postavljanja uređaja za ograničenje brzine ili nekog drugog uređaja koji pridonosi sigurnosti na cestama ili u roku od sedam dana u drugim slučajevima.

400) Svaki put kad se te plombe skidaju, sastavlja se pisana izjava u kojoj se navode razlozi zbog kojih je to učinjeno i koja mora biti dostupna nadležnom tijelu.

401) Plombe moraju imati identifikacijski broj koji im je odredio proizvođač. Taj broj mora biti jedinstven i mora se razlikovati od svih drugih brojeva plombi koje su odredili drugi proizvođači plombi.

Taj jedinstveni identifikacijski broj definira se na sljedeći način: MMNNNNNN oznakom koja se ne može ukloniti, pri čemu je MM jedinstvena identifikacija proizvođača (upis baze podataka vodit će EK), a NNNNNN alfanumerički broj plombe koji je jedinstven u domeni proizvođača.

402) Na plombama mora postojati slobodan prostor na kojem ovlašteni instalateri, radionice ili proizvođači vozila mogu dodati posebnu oznaku u skladu s člankom 22. stavkom 3. Uredbe (EU) br. 165/2014.

Ta oznaka ne smije prekriti identifikacijski broj plombe.

403) Proizvođači plombi moraju se upisati u posebnu bazu podataka i objaviti svoje identifikacijske brojeve plombi u okviru postupka koji će utvrditi Europska komisija.

404) U okviru Uredbe (EU) br. 165/2014 ovlaštene radionice i proizvođači vozila smiju upotrebljavati plombe samo onih proizvođača plombi koji su navedeni u prethodno navedenoj bazi podataka.

405) Proizvođači plombi i njihovi distributeri vode zapise o punoj sljedivosti prodanih plombi koje će se upotrebljavati u okviru Uredbe (EU) br. 165/2014 te ih moraju biti spremni predati nadležnim nacionalnim tijelima kad god je potrebno.

406) Jedinstveni identifikacijski brojevi plombi moraju biti vidljivi na tipskoj pločici.

6 PROVJERE, PREGLEDI I POPRAVCI

Zahtjevi u pogledu okolnosti u kojima se plombe mogu ukloniti u skladu s člankom 22. stavkom 5. Uredbe (EU) br. 165/2014 utvrđeni su u poglavlju 5.3. ovog Priloga.

6.1 **Ovlaštenje instalatera, radionica i proizvođača vozila**

Države članice ovlašćuju, redovito nadziru i potvrđuju tijela koja obavljaju:

— ugradnju,

— provjere,

— preglede,

— popravke.

Osim ako ne postoji valjano opravdanje, kartice radionice izdaju se samo instalaterima i/ili radionicama koji su ovlašteni za aktiviranje i/ili kalibraciju uređaja za bilježenje podataka u skladu s ovim Prilogom i:

— koji nemaju pravo na karticu poduzeća

— i čija druga poslovna djelatnost ne dovodi u pitanje sveukupnu sigurnost sustava kako se zahtjeva u Dodatku 10.

6.2 **Provjera novih ili popravljenih uređaja**

407) Svaki pojedini uređaj, nov ili popravljen, provjerava se kalibracijom u pogledu ispravnog rada te točnosti očitavanja i zapisa, u granicama utvrđenima u poglavljima 3.2.1., 3.2.2., 3.2.3. i 3.3., a zatim se stavljaju plombe u skladu s poglavljem 5.3.

6.3 **Pregled pri ugradnji**

408) Pri postavljanju u vozilo, čitava instalacija (uključujući i uređaj za bilježenje podataka) mora udovoljiti odredbama koje se odnose na najveća dopuštena odstupanja utvrđena u poglavljima 3.2.1., 3.2.2., 3.2.3. i 3.3.

6.4 **Periodični pregledi**

409) Periodični pregledi uređaja za bilježenje podataka u vozilu obavljaju se nakon svakog popravka uređaja ili nakon svake izmjene karakterističnog koeficijenta vozila ili djelatnog opsega guma ili nakon pogreške vremena po UTC-u u uređaju veće od 20 minuta, ili pri promjeni registracijske oznake vozila, te barem jednom svake dvije godine (24 mjeseca) nakon posljednjeg pregleda.

410) Ti pregledi obuhvaćaju sljedeće provjere:

— da uređaj za bilježenje podataka radi ispravno, uključujući funkciju pohrane podataka na tahografske kartice i komunikaciju s čitačima komunikacije na daljinu,

— da je osigurana sukladnost s odredbama poglavlja 3.2.1. i 3.2.2. o najvećem odstupanju pri ugradnji,

— da je osigurana sukladnost s odredbama poglavlja 3.2.3. i 3.3.,

— ima li uređaj za bilježenje podataka homologacijsku oznaku,

— da su ugrađene tipska pločica, kako je definirana u zahtjevu 396, i opisna pločica, kako je definirana u zahtjevu 225,

— kolika je veličina gume i stvarni opseg guma,

— da uređaju nisu dodani uređaji za manipulaciju,

— da su plombe ispravno postavljene, u dobrom stanju, da su njihovi identifikacijski brojevi valjani (ovlašteni proizvođač plombi u bazi podataka EK-a) i da njihovi identifikacijski brojevi odgovaraju oznakama tipskih pločica (vidjeti zahtjev 401).

411) Ako se ustanovi da se nakon posljednjeg pregleda dogodio jedan od događaja navedenih u poglavlju 3.9. (Otkrivanje događaja i/ili kvarova) i proizvođači tahografa i/ili nacionalna tijela smatraju da on potencijalno dovodi u opasnost sigurnost uređaja, radionica tada:

a. uspoređuje identifikacijske podatke senzora kretanja, koji je priključen na mjenjač, s podatcima povezanog senzora kretanja registriranog u jedinici u vozilu;

b. provjerava podudaraju li se informacije zabilježene na tipskoj pločici s informacijama koje sadržava zapis jedinice u vozilu;

c. provjerava podudara li se serijski broj i homologacijski broj senzora kretanja, ako je ispisan na tijelu senzora kretanja, s informacijama koje sadrži zapis jedinice u vozilu;

d. uspoređuje identifikacijske podatke označene na opisnoj pločici vanjskog uređaja GNSS-a, ako postoje, s podatcima pohranjenima u podatkovnoj memoriji jedinice u vozilu.

412) Radionice u svojim izvješćima o pregledu zapisuju sva saznanja o slomljenim plombama ili uređajima za manipulaciju. Radionice ta izvješća čuvaju najmanje dvije godine i stavljaju ih na raspolaganje na zahtjev nadležnih tijela.

413) Ti pregledi moraju uključivati kalibraciju i preventivnu zamjenu plombi za čije su postavljanje odgovorne radionice..

6.5 **Mjerenje grešaka**

414) Mjerenje grešaka kod ugradnje i tijekom upotrebe obavlja se pod sljedećim uvjetima koji se smatraju standardnim uvjetima ispitivanja:

— nenatovareno vozilo u stanju spremnom za vožnju,

— tlak u gumama prema uputama proizvođača,

— istrošenost guma u okviru zakonski dopuštenih granica,

— kretanje vozila:

— vozilo se mora kretati snagom vlastitog motora, pravocrtno na ravnoj površini brzinom od 50 ± 5 km/h. Mjerna udaljenost iznosi najmanje 1 000 m.

— Ako im je točnost usporediva, za provjeru se mogu koristiti i alternativne metode kao što je ispitivanje na odgovarajućem ispitnom stolu.

6.6 **Popravci**

415) Radionice moraju moći preuzeti podatke s uređaja za bilježenje podataka kako bi ih mogli dostaviti odgovarajućem prijevozniku.

416) Ovlaštene radionice izdaju prijevoznicima potvrdu o nemogućnosti preuzimanja podataka kada neispravnost uređaja za bilježenje podataka sprečava preuzimanje prethodno zabilježenih podataka, čak i nakon popravka u radionici. Radionice čuvaju presliku svake izdane potvrde u trajanju od najmanje dvije godine.

7 IZDAVANJE KARTICA

Postupci izdavanja kartica ustrojeni u državama članicama moraju biti u skladu sa sljedećim:

417) broj kartice prvog izdavanja tahografske kartice tražitelju mora imati redni indeks (ako je primjereno) i indeks zamjene te indeks ponovnog izdavanja postavljen na „0”.

418) Brojevi kartica svih nepersonaliziranih tahografskih kartica koje se izdaju jednom nadzornom tijelu ili jednoj radionici ili jednom prijevozniku moraju imati prvih 13 istih znamenaka, te različit redni indeks.

419) Tahografska kartica koja se izdaje kao zamjena za postojeću tahografsku karticu mora imati isti broj kartice kao i kartica koju zamjenjuje, osim indeksa zamjene koji se uvećava za „1” (redoslijedom 0, …, 9, A, …, Z).

420) Tahografska kartica koja se izdaje kao zamjena za postojeću tahografsku karticu mora imati isti datum isteka valjanosti kartice kao i kartica koju zamjenjuje.

421) Tahografska kartica koja se izdaje zbog obnavljanja postojeće tahografske kartice mora imati isti broj kartice kao i kartica koja se obnavlja, osim indeksa zamjene koji se ponovno vraća na nulu i indeksa ponovnog izdavanja koji se uvećava za „1" (redoslijedom 0, …, 9, A, …, Z).

422) Zamjena postojeće kartice tahografa radi izmjene administrativnih podataka slijedi pravila obnavljanja ako se obavlja unutar iste države članice odnosno pravila prvog izdavanja ako istu obavlja druga država članica.

423) „Prezime nositelja kartice" za nepersonalizirane kartice radionice ili kontrolne kartice popunjava se nazivom radionice ili nadzornog tijela ili imenom instalatera ili službenika za kontrolu ako države članice tako odluče.

424) Države članice elektronički razmjenjuju podatke kako bi osigurale jedinstvenost tahografske kartice vozača koju izdaju u skladu s člankom 31. Uredbe (EU) br. 165/2014.

8 HOMOLOGACIJA UREĐAJA ZA BILJEŽENJE PODATAKA I TAHOGRAFSKIH KARTICA

8.1 **Opći zahtjevi**

Za potrebe ovog poglavlja, riječi „uređaj za bilježenje podataka" znače „uređaj za bilježenje podataka ili njegovi sastavni dijelovi". Homologacija nije potrebna za kabele koji povezuju senzor kretanja s jedinom u vozilu, vanjski uređaj GNSS-a s jedinicom u vozilu ili uređaj za komunikaciju na daljinu s jedinicom u vozilu. Papir koji se upotrebljava u uređaju za bilježenje podataka smatra se sastavnim dijelom uređaja za bilježenje podataka.

Svaki proizvođač jedinice u vozilu može zahtijevati homologaciju njegova sastavnog dijela s bilo kojom vrstom senzora kretanja, vanjskim uređajem GNSS-a i obrnuto, pod uvjetom da je svaki sastavni dio usklađen sa zahtjevima iz ovog Priloga. U suprotnom, proizvođači mogu zatražiti i homologaciju uređaja za bilježenje podataka.

425) Uređaj za bilježenje podataka podnosi se za homologaciju zajedno sa svim integriranim dodatnim uređajima.

426) Homologacija uređaja za bilježenje podataka i tahografskih kartica mora uključivati sigurnosna ispitivanja, ispitivanja funkcionalnosti i interoperabilnosti. Pozitivni rezultati svih ovih ispitivanja utvrđuju se u odgovarajućoj potvrdi.

427) Tijela država članica zadužena za homologaciju neće izdati certifikat o homologaciji ako nemaju:

— certifikat o sigurnosti,

— certifikat o ispravnosti,

— i certifikat o interoperabilnosti

za uređaj za bilježenje podataka ili tahografsku karticu koja je predmet zahtjeva za homologaciju.

428) O svakoj izmjeni u softveru ili hardveru uređaja ili u naravi materijala upotrijebljenih u njegovoj proizvodnji mora se, prije nego što se primijeni, obavijestiti nadležno tijelo koje je odobrilo homologaciju za uređaj. To tijelo proizvođaču potvrđuje produljenje homologacije ili može zahtijevati ažuriranje ili potvrdu relevantnih certifikata o ispravnosti, sigurnosti i/ili o interoperabilnosti.

429) Postupke softverske nadogradnje uređaja za bilježenje podataka na licu mjesta odobrava tijelo koje je odobrilo homologaciju uređaja za bilježenje podataka. Nadogradnja softvera ne smije mijenjati ili brisati niti jedan podatak o aktivnosti vozača pohranjen u uređaju za bilježenje podataka. Softver se može nadograđivati samo pod odgovornosti proizvođača uređaja.

430) Homologacija izmjena softvera koje se odnose na nadogradnju prethodno homologiranog uređaja za bilježenje podataka ne može se odbiti ako se te izmjene primjenjuju samo na funkcije koje nisu određene u Prilogu. Nadogradnja softvera uređaja za bilježenje podataka može isključiti uvođenje novih skupova znakova ako to nije tehnički izvedivo.

8.2 **Certifikat o sigurnosti**

431) Certifikat o sigurnosti izdaje se u skladu s odredbama Dodatka 10. ovom Prilogu. Sastavni dijelovi uređaja za bilježenje podataka koje je potrebno certificirati su jedinica u vozilu, senzor kretanja, vanjski uređaj GNSS-a i tahografske kartice.

432) U iznimnim okolnostima, kad tijela za sigurnosno certificiranje odbijaju certificirati novu opremu radi zastarjelosti sigurnosnih mehanizama, homologacija se nastavlja izdavati u skladu s Uredbom samo u tim specifičnim i iznimnim okolnostima te kad ne postoji alternativno rješenje koje je u skladu s Uredbom.

433) U tim okolnostima, dotična država članica bez odgode obavješćuje Europsku komisiju, koja u roku od dvanaest kalendarskih mjeseci od dodjele homologacije pokreće postupak kojim osigurava da se ponovno uspostavi prvotna razina sigurnosti.

8.3 **Certifikat o ispravnosti**

434) Svaki kandidat za homologaciju mora dostaviti tijelu države članice odgovornom za homologaciju sve materijale i dokumente koje tijelo smatra potrebnima.

435) Proizvođači u roku od mjesec dana od datuma zahtjeva osiguravaju odgovarajuće uzorke proizvoda podnesenog za homologaciju i s tim povezanu dokumentaciju, koju zahtijevaju laboratoriji imenovani za obavljanje funkcionalnih ispitivanja. Sve troškove koji nastanu zbog tog zahtjeva snosi podnositelj zahtjeva. Laboratoriji povjerljivo postupaju sa svim poslovno osjetljivim informacijama.

436) Certifikat o ispravnosti izdaje se proizvođaču tek nakon uspješnog okončanja najmanje onih ispitivanja funkcionalnosti koja su navedena u Dodatku 9.

437) Tijelo za homologaciju izdaje certifikat o ispravnosti. Osim naziva korisnika i identifikacije modela, u toj se potvrdi detaljno opisuju izvršena ispitivanja i postignuti rezultati.

438) U certifikatu o ispravnosti bilo kojeg sastavnog dijela uređaja za bilježenje podataka navedeni su i homologacijski brojevi svih drugih homologiranih kompatibilnih sastavnih dijelova uređaja za bilježenje podataka koji su ispitani tijekom certificiranja tog dijela.

439) U certifikatu o ispravnosti svih sastavnih dijelova uređaja za bilježenje podataka navodi se i norma ISO ili CEN u odnosu na koju je funkcionalno sučelje certificirano.

8.4 **Certifikat o interoperabilnosti**

440) Ispitivanje interoperabilnosti provodi se u jednom od laboratorija pod nadležnošću i odgovornosti Europske komisije.

441) Laboratorij mora upisati zahtjeve za ispitivanje interoperabilnosti koje podnose proizvođači kronološkim redom njihova pristizanja.

442) Zahtjevi se službeno upisuju samo kad laboratorij dođe u posjed:

— cjelokupnog niza materijala i dokumenata potrebnih za takva ispitivanja interoperabilnosti,

— odgovarajućeg certifikata o sigurnosti,

— odgovarajućeg certifikata o ispravnosti,

Datum upisa zahtjeva prijavljuje se proizvođaču.

443) Laboratorij ne obavlja nikakva ispitivanja interoperabilnosti za uređaj za bilježenje podataka ili tahografske kartice koji nisu dobili sigurnosni certifikat i funkcionalni certifikat, osim u iznimnim okolnostima opisanima u zahtjevu 432.

444) Svaki proizvođač koji traži ispitivanje interoperabilnosti mora se obvezati da će laboratoriju zaduženom za takva ispitivanja ostaviti cjelokupan skup materijala i dokumenata koje je pribavio radi provedbe ispitivanja.

445) Ispitivanja interoperabilnosti moraju se izvesti u skladu s odredbama Dodatka 9. ovom Prilogu, na svim vrstama uređaja za bilježenje podataka odnosno tahografskih kartica:

— za koje homologacija još vrijedi, ili

— za koje je homologacija u tijeku i koji imaju važeći certifikat o interoperabilnosti.

446) Ispitivanja interoperabilnosti moraju uključivati sve generacije uređaja za bilježenje podataka ili tahografskih kartica koje se još uvijek upotrebljavaju.

447) Certifikat o interoperabilnosti laboratorij izdaje proizvođaču tek nakon uspješnog prolaska svih ispitivanja interoperabilnosti.

448) Ako ispitivanja interoperabilnosti na jednom uređaju za bilježenje podataka ili više njih ili jednoj tahografskoj kartici ili više njih nisu bila uspješna, certifikat o interoperabilnosti ne smije se izdati prije nego proizvođač koji je podnio zahtjev ne izvrši potrebne izmjene i prođe ispitivanje interoperabilnosti. Laboratorij uz pomoć proizvođača na koje se odnosi ta pogreška interoperabilnosti utvrđuje uzrok problema te pokušava pomoći proizvođaču podnositelju zahtjeva da pronađe tehničko rješenje. Ako je proizvođač izmijenio svoj proizvod, odgovornost je proizvođača da kod nadležnih tijela utvrdi vrijede li još uvijek certifikat o sigurnosti i certifikat o ispravnosti.

449) Certifikat o interoperabilnosti vrijedi šest mjeseci. Na kraju tog razdoblja on se opoziva ako proizvođač nije dobio odgovarajući certifikat o homologaciji. Proizvođač ga dostavlja tijelu države članice ovlaštenom za homologaciju koje je izdalo potvrdu o ispravnosti.

450) Nijedan element koji bi mogao biti ishodište neuspjeha provjere interoperabilnosti ne smije se upotrebljavati za ostvarivanje dobiti ili za preuzimanje vodećeg položaja.

8.5 **Certifikat o homologaciji**

451) Tijelo države članice ovlašteno za homologaciju može izdati certifikat o homologaciji čim zaprimi tri potrebna certifikata.

452) U certifikatu o homologaciji bilo kojeg dijela uređaja za bilježenje podataka navedeni su i homologacijski brojevi svih drugih homologiranih kompatibilnih uređaja za bilježenje podataka.

453) Tijelo ovlašteno za homologaciju certifikat o homologaciji mora istodobno dostaviti laboratoriju zaduženom za ispitivanje interoperabilnosti i proizvođaču.

454) Laboratorij nadležan za ispitivanje interoperabilnosti mora imati javne internetske stranice na kojima će se ažurirati popis modela uređaja za bilježenje podataka ili tahografskih kartica:

— za koje je upisan zahtjev za ispitivanje interoperabilnosti,

— kojima je izdan certifikat o interoperabilnosti (čak i privremeni),

— kojima je izdan certifikat o homologaciji.

8.6 **Izvanredni postupak: prvi certifikati o interoperabilnosti za uređaje za bilježenje podataka i tahografske kartice druge generacije**

455) Do isteka četiri mjeseca od izdavanja certifikata o interoperabilnosti za prvi par uređaja za bilježenje podataka druge generacije i tahografskih kartica druge generacije (kartica vozača, kartica radionice, kontrolna kartica i kartica poduzeća), svaki izdani certifikat (uključujući i prvi) u pogledu zahtjeva upisanih u tom razdoblju smatra se privremenim.

456) Ako na kraju tog razdoblja svi predmetni proizvodi budu međusobno interoperabilni, svi odgovarajući certifikati o interoperabilnosti postaju konačni.

457) Ako se tijekom tog razdoblja utvrde pogreške interoperabilnosti, laboratorij zadužen za ispitivanje interoperabilnosti mora uz pomoć svih uključenih proizvođača utvrditi uzroke problema te ih mora pozvati da izvrše potrebne izmjene.

458) Ako se po isteku tog razdoblja problemi interoperabilnosti nastave, laboratorij zadužen za ispitivanje interoperabilnosti, u suradnji sa svim zainteresiranim proizvođačima i tijelima ovlaštenima za homologaciju koja su izdala odgovarajuće certifikate o ispravnosti, mora pronaći uzrok pogrešaka interoperabilnosti i utvrditi koje izmjene svaki od dotičnih proizvođača treba izvršiti. Traženje tehničkih rješenja traje najdulje dva mjeseca, nakon čega Komisija, ako se ne pronađe nikakvo zajedničko rješenje i nakon dogovora s laboratorijem zaduženim za ispitivanje interoperabilnosti, odlučuje koji će uređaj(i) za bilježenje podataka i kartice dobiti konačni certifikat o interoperabilnosti te navesti razloge za tu odluku.

459) Svaki zahtjev za ispitivanje interoperabilnosti koji laboratorij upiše između kraja četveromjesečnog razdoblja nakon izdavanja prvog privremenog certifikata o interoperabilnosti i datuma odluke Komisije iz zahtjeva 455 mora se odgoditi dok se ne riješe prvi problemi interoperabilnosti. Takvi se zahtjevi potom obrađuju kronološkim redom njihova upisivanja.

Dodatak 1

RJEČNIK S PODATCIMA

SADRŽAJ

1. UVOD 88
1.1. Pristup definiranju vrsta podataka 88
1.2. Literatura 88
2. DEFINICIJE VRSTA PODATAKA 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. DEFINICIJE VRIJEDNOSTI I RASPONA VELIČINE 171
4. SKUPINE ZNAKOVA (CHARACTER SETS) 171
5. KODIRANJE 171
6. IDENTIFIKATORI OBJEKTA I IDENTIFIKATORI APLIKACIJE 171
6.1. Identifikatori objekta 171
6.2. Identifikatori aplikacije 172

1. UVOD

U ovom su dodatku navedeni formati podataka, podatkovni elementi i strukture podataka za upotrebu u uređajima za bilježenje podataka i tahografskim karticama.

1.1. **Pristup definiranju vrsta podataka**

U ovom se dodatku za definiranje vrsta podataka upotrebljava *Abstract Syntax Notation One* (ASN.1). Time se omogućuje definiranje jednostavnih i strukturiranih podataka bez impliciranja posebne sintakse prijenosa (pravila u pogledu kodiranja) koji će ovisiti o primjeni i okolini.

Konvencije o nazivlju tipa ASN.1 u skladu su s normom ISO/IEC 8824-1. To znači sljedeće:

— ako je to moguće, značenje vrste podataka naslućuje se iz odabranih naziva,

— ako je vrsta podataka sastavljena od drugih vrsta podataka, naziv vrste podataka svejedno se sastoji od jednog slijeda abecednih znakova koji započinje velikim početnim slovom, ali se u nazivu upotrebljavaju velika slova kako bi se naglasilo odgovarajuće značenje,

— nazivi vrsta podataka općenito su povezani s nazivom vrsta podataka iz kojih su izvedeni, uređajem u kojem su podatci pohranjeni i funkcijom u vezi s podacima.

Ako je vrsta podataka po ASN.1 već definirana kao dio neke druge norme, a važno je upotrijebiti je u uređaju za bilježenje podataka, ta ASN.1 vrsta podataka bit će definirana u ovome dodatku.

Kako bi se omogućilo više vrsta pravila u pogledu kodiranja, neke su vrste ASN.1 u ovome dodatku ograničene identifikatorima raspona vrijednosti. Identifikatori raspona vrijednosti definirani su u stavku 3. i Dodatku 2.

1.2. **Literatura**

U ovome su Dodatku upotrijebljeni sljedeći izvori:

ISO 639 Code for the representation of names of languages. Prvo izdanje: 1988.

ISO 3166 Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, 2013.

ISO 3779 Road vehicles – Vehicle identification number (VIN) – Content and structure. 2009.

ISO/IEC 7816-5 Identification cards – Integrated circuit cards – Part 5: Registration of application providers.

Drugo izdanje: 2004.

ISO/IEC 7816-6 Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange, 2004 + Technical Corrigendum 1: 2006.

ISO/IEC 8824-1 Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2008 + Technical Corrigendum 1: 2012 and Technical Corrigendum 2: 2014.

ISO/IEC 8825-2 Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). 2008.

ISO/IEC 8859-1 Information technology – 8 bit single-byte coded graphic character sets – Part 1: Latin alphabet No.1. Prvo izdanje: 1998.

ISO/IEC 8859-7 Information technology – 8 bit single-byte coded graphic character sets – Part 7: Latin/Greek alphabet. 2003.

ISO 16844-3 Road vehicles – Tachograph systems – Motion Sensor Interface. 2004 + Technical Corrigendum 1: 2006.

TR-03110-3 BSI / ANSSI Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3 Common Specifications, verzija 2.20, 3. veljače 2015.

2. DEFINICIJE VRSTA PODATAKA

Za sve vrste podataka navedene u nastavku zadana vrijednost za sadržaj „nepoznato" ili „nije primjenjivo" sastoji se od popunjavanja podatkovnog elementa bajtovima „FF".

Sve se vrste podataka upotrebljavaju za aplikacije prve i druge generacije, osim ako nije navedeno drukčije.

2.1. **ActivityChangeInfo**

Tom se vrstom podataka omogućuje kodiranje, u okviru dvobajtne riječi, statusa utora u 00:00 sati i/ili stanja vožnje u 00:00 sati i/ili promjena aktivnosti i/ili promjena stanja vožnje i/ili promjena statusa kartice vozača ili suvozača. Ta se vrsta podataka odnosi na zahtjeve 105, 266, 291, 320, 321, 343 i 344 iz Priloga 1.C.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Dodjela vrijednosti – oktetno poravnavanje: 'scpaatttttttttt'B (16 bitova)

Za zapise u podatkovnoj memoriji (ili status utora):

's'B Utor:

'0'B: VOZAČ,

'1'B: SUVOZAČ,

'c'B Stanje vožnje:

'0'B: JEDAN VOZAČ,

'1'B: POSADA,

'p'B Status kartice vozača (ili radionice) u odgovarajućem utoru:

'0'B: UMETNUTA, kartica je umetnuta,

'1'B: NIJE UMETNUTA, kartica nije umetnuta (ili je kartica uklonjena),

'aa'B Aktivnost:

'00'B: STANKA/ODMOR,

'01'B: PRIPRAVNOST,

'10'B: RAD,

'11'B: VOŽNJA,

'ttttttttttt'B Vrijeme promjene: broj minuta od 00:00 h određenog dana.

Za zapise na kartici vozača (ili radionice) (i stanje vožnje):

‘s’B	Utor (nije relevantno ako je ‘p’ = 1, osim prema napomeni navedenoj u nastavku):
	‘0’B: VOZAČ,
	‘1’B: SUVOZAČ,
‘c’B	Stanje vožnje (ako je ‘p’ = 0) ili
	Sljedeće stanje aktivnosti (ako je ‘p’ = 1):
	‘0’B: JEDAN VOZAČ,
	‘0’B: NEPOZNATO
	‘1’B: POSADA,
	‘1’B: POZNATO (= ručni unos)
‘p’B	Status kartice:
	‘0’B: UMETNUTA, kartica je umetnuta u uređaj za bilježenje podataka,
	‘1’B: NIJE UMETNUTA, kartica nije umetnuta (ili je kartica uklonjena),
‘aa’B	Aktivnost (nije relevantno ako je ‘p’ = 1 i ‘c’ = 0, osim prema napomeni navedenoj u nastavku):
	‘00’B: STANKA/ODMOR,
	‘01’B: PRIPRAVNOST,
	‘10’B: RAD,
	‘11’B: VOŽNJA,
‘ttttttttttt’B	Vrijeme promjene: broj minuta od 00:00 h određenog dana.

Napomena u slučaju „uklanjanja kartice”:

Kad je kartica uklonjena:

— bit ‘s’ je relevantan i označuje utor iz kojeg je kartica uklonjena,

— bit ‘c’ mora biti postavljen na 0,

— bit ‘p’ mora biti postavljen na 1,

— bitom ‘aa’ mora se kodirati trenutačna aktivnost odabrana u tom trenutku.

Kao rezultat ručnog unosa, kasnije se može pisati preko bitova ‘c’ i ‘aa’ riječi (pohranjenih u kartici) kako bi se odrazio unos.

2.2. **Address**

Adresa.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage označuje skup znakova definiran u poglavlju 4.,

address je adresa kodirana s pomoću posebnog skupa znakova.

2.3. **AESKey**

Druga generacija:

AES ključ duljine 128, 192 ili 256 bitova.

```
AESKey ::= CHOICE {
   aes128Key                          AES128Key,
   aes192Key                          AES192Key,
   aes256Key                          AES256Key
}
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.4. **AES128Key**

Druga generacija:

AES128 ključ.

```
AES128Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes128Key                          OCTET STRING (SIZE(16))
}
```

duljina označuje duljinu AES128 ključa u oktetima.

aes128Key je AES ključ duljine 128 bitova.

Dodjela vrijednosti:

Duljina ima vrijednost 16.

2.5. **AES192Key**

Druga generacija:

AES192 ključ.

```
AES192Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes192Key                          OCTET STRING (SIZE(24))
}
```

duljina označuje duljinu AES192 ključa u oktetima.

aes192Key je AES ključ duljine 192 bita.

Dodjela vrijednosti:

Duljina ima vrijednost 24.

2.6. **AES256Key**

Druga generacija:

AES256 ključ.

```
AES256Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes256Key                               OCTET STRING (SIZE(32))
}
```

duljina označuje duljinu AES256 ključa u oktetima.

aes256Key je AES ključ duljine 256 bitova.

Dodjela vrijednosti:

Duljina ima vrijednost 32.

2.7. **BCDString**

BCDString primjenjuje se za prikaz binarno kodiranih decimalnih brojeva (BCD). Ta se vrsta podataka upotrebljava za prikaz jednodecimalne znamenke u jednom poluoktetu (4 bita). BCDString temelji se na normi ISO/IEC 8824-1 'CharacterStringType'.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString upotrebljava zapis „hstring". Krajnja lijeva heksadecimalna znamenka najvažniji je poluoktet prvog okteta. Višekratnik okteta tvori se tako da se umetne poluoktet sa završnim nulama, prema potrebi, od mjesta krajnjeg lijevog poluokteta u prvom oktetu.

Dopuštene su znamenke sljedeće: 0, 1, … 9.

2.8. **CalibrationPurpose**

Kod kojim se pojašnjava zašto je zabilježen niz parametara kalibriranja. Ta se vrsta podataka odnosi na zahtjeve 097 i 098 iz Priloga 1.B te na zahtjev 119 iz Priloga 1.C.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti:

Prva generacija:

'00'H	rezervirana vrijednost,
'01'H	aktivacija: bilježenje poznatih parametara kalibriranja u trenutku aktivacije jedinice u vozilu,
'02'H	prva ugradnja: prvo kalibriranje jedinice u vozilu nakon njezine aktivacije,
'03'H	ugradnja: prvo kalibriranje jedinice u vozilu u sadašnjem vozilu,
'04'H	periodični pregled.

Druga generacija:

Uz vrijednosti navedene za prvu generaciju upotrebljavaju se i sljedeće:

‘05’H	poduzeće unosi registracijski broj vozila (VRN),
‘06’H	podešavanje vremena bez kalibriranja,
‘07’H do ‘7F’H	RFU,
‘80’H do ‘FF’H	specifično za proizvođača.

2.9. **CardActivityDailyRecord**

Informacije pohranjene na kartici koje se odnose na aktivnosti vozača na određeni kalendarski dan. Ta se vrsta podataka odnosi na zahtjeve 266, 291, 320 i 343 iz Priloga 1.C.

```
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 ukupna duljina u bajtovima zapisa od prethodnog dana. Najveća vrijednost iskazana je duljinom oktetnog niza (OCTET STRING) koji sadržava te zapise (vidjeti CardActivityLengthRange u Dodatku 2. stavku 4.). Kad je taj zapis najstariji dnevni zapis, vrijednost activityPreviousRecordLength mora biti postavljena na 0.

activityRecordLength je ukupna duljina u bajtovima tog zapisa. Najveća vrijednost iskazana je duljinom OCTET STRING koji sadržava te zapise.

activityRecordDate je datum zapisa.

activityDailyPresenceCounter je brojač dnevne prisutnosti za određenu karticu za taj dan.

activityDayDistance je ukupna udaljenost prijeđena tog dana.

activityChangeInfo je skup ActivityChangeInfo podataka za vozača za taj dan. Smije sadržavati najviše 1440 vrijednosti (jedna promjena aktivnosti u minuti). U taj je skup uvijek uključen activityChangeInfo kojim se kodira stanje vožnje u 00:00 h.

2.10. **CardActivityLengthRange**

Broj bajtova na kartici vozača ili kartici radionice raspoloživih za pohranjivanje zapisa o aktivnosti vozača.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.11. **CardApprovalNumber**

Homologacijski broj kartice.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Dodjela vrijednosti:

Homologacijski broj daje se u skladu s onime objavljenim na odgovarajućoj internetskoj stranici Europske komisije, odnosno, na primjer, uključujući spojnice ako postoje. Homologacijski broj mora biti lijevo poravnat.

2.12. **CardCertificate**

Prva generacija:

Certifikat javnog ključa kartice.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Informacije pohranjene na kartici koje se odnose na identifikaciju integriranog kruga (IC) kartice (zahtjev 249 iz Priloga 1.C). icSerialNumber i icManufacturingReferences zajedno čine jedinstvenu identifikaciju čipa kartice. icSerialNumber sâm za sebe ne čini jedinstvenu identifikaciju kartice.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber je serijski broj IC-a.

icManufacturingReferences je posebni identifikator proizvođača IC-a.

2.14. **CardConsecutiveIndex**

Redni indeks kartice (definicija h)).

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Dodjela vrijednosti: (vidjeti poglavlje VII. Priloga 1.C)

Redoslijed povećavanja: '0, …, 9, A, …, Z, a, …, z'

2.15. **CardControlActivityDataRecord**

Informacije pohranjene na kartici vozača ili kartici radionice koje se odnose na posljednju kontrolu kojoj je bio podvrgnut vozač (zahtjevi 274, 299, 327 i 350 iz Priloga 1.C).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                       ControlType,
   controlTime                       TimeReal,
   controlCardNumber                 FullCardNumber,
   controlVehicleRegistration        VehicleRegistrationIdentification,
   controlDownloadPeriodBegin        TimeReal,
   controlDownloadPeriodEnd          TimeReal
}
```

controlType je vrsta kontrole.

controlTime je datum i vrijeme kontrole.

controlCardNumber je FullCardNumber službenika za kontrolu koji je proveo kontrolu.

controlVehicleRegistration je VRN i država članica registracije vozila u kojem je provedena kontrola.

controlDownloadPeriodBegin i **controlDownloadPeriodEnd** su razdoblja za koja su preuzeti podatci, u slučaju preuzimanja podataka.

2.16. CardCurrentUse

Informacije o stvarnoj upotrebi kartice (zahtjevi 273, 298, 326 i 349 iz Priloga 1.C).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                  TimeReal,
   sessionOpenVehicle               VehicleRegistrationIdentification
}
```

sessionOpenTime je trenutak umetanja kartice radi trenutačne upotrebe. Taj se element pri uklanjanju kartice postavlja na nulu.

sessionOpenVehicle je identifikacija vozila koje se trenutačno upotrebljava, postavljena pri umetanju kartice. Taj se element pri uklanjanju kartice postavlja na nulu.

2.17. CardDriverActivity

Informacije pohranjene na kartici vozača ili radionice koje se odnose na aktivnosti vozača (zahtjevi 267, 268, 292, 293, 321 i 344 iz Priloga 1.C).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord      INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord         INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords                OCTET STRING
                                       (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord je određivanje početka prostora za pohranu (broj bajtova od početka niza) najstarijeg zapisa za puni dan u nizu activityDailyRecords. Najveća vrijednost iskazana je duljinom niza.

activityPointerNewestRecord je određivanje početka prostora za pohranu (broj bajtova od početka niza) najnovijeg zapisa za puni dan u nizu activityDailyRecords. Najveća vrijednost iskazana je duljinom niza.

activityDailyRecords je prostor raspoloživ za pohranu podataka o aktivnosti vozača (struktura podataka: CardActivityDailyRecord) za svaki kalendarski dan kad je upotrebljavana kartica.

Dodjela vrijednosti: ovaj se oktetni niz ciklično popunjava zapisima CardActivityDailyRecord. Pri prvoj upotrebi pohranjivanje započinje s prvim bajtom niza. Svi se novi zapisi dodaju na kraj prethodnog zapisa. Kad je niz pun, pohranjivanje se nastavlja u prvi bajt niza neovisno o prekidu u podatkovnom elementu. Prije postavljanja novih podataka o aktivnostima u niz (povećanje postojećeg activityDailyRecord ili postavljanje novog activityDailyRecord) kojima se zamjenjuju stariji podatci o aktivnostima, mora se ažurirati activityPointerOldestDayRecord kako bi se odrazilo novo mjesto najstarijeg zapisa za puni dan, a activityPreviousRecordLength tog (novog) najstarijeg zapisa za puni dan mora se ponovno postaviti na 0.

2.18. CardDrivingLicenceInformation

Informacije pohranjene na kartici vozača koje se odnose na podatke o vozačkoj dozvoli nositelja kartice (zahtjevi 259 i 284 iz Priloga 1.C).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority je tijelo nadležno za izdavanje vozačke dozvole.

drivingLicenceIssuingNation je državna pripadnost tijela koje je izdalo vozačku dozvolu.

drivingLicenceNumber je broj vozačke dozvole.

2.19. **CardEventData**

Informacije pohranjene na kartici vozača ili radionice koje se odnose na događaje povezane s nositeljem kartice (zahtjevi 260, 285, 318 i 341 iz Priloga 1.C).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData je slijed poredan prema uzlaznoj vrijednosti EventFaultType za cardEventRecords (osim u slučaju zapisa povezanih s pokušajima probijanja zaštite koji su sakupljeni u posljednjem nizu slijeda).

cardEventRecords je niz zapisa o događajima određene vrste događaja (ili kategorije, u slučaju pokušaja probijanja zaštite).

2.20. **CardEventRecord**

Informacije pohranjene na kartici vozača ili radionice koje se odnose na određeni događaj povezan s nositeljem kartice (zahtjevi 261, 286, 318 i 341 iz Priloga 1.C).

```
CardEventRecord ::= SEQUENCE {
   eventType                            EventFaultType,
   eventBeginTime                       TimeReal,
   eventEndTime                         TimeReal,
   eventVehicleRegistration             VehicleRegistrationIdentification
}
```

eventType je vrsta događaja.

eventBeginTime je datum i vrijeme početka događaja.

eventEndTime je datum i vrijeme završetka događaja.

eventVehicleRegistration je VRN i država članica registracije vozila u kojem je došlo do događaja.

2.21. **CardFaultData**

Informacije pohranjene na kartici vozača ili radionice koje se odnose na kvarove povezane s nositeljem kartice (zahtjevi 263, 288, 318 i 341 iz Priloga 1.C).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                     SET SIZE(NoOfFaultsPerType) OF
                                        CardFaultRecord
}
```

CardFaultData je niz zapisa o kvarovima uređaja za bilježenje podataka nakon kojih slijedi niz zapisa o kvarovima kartice.

cardFaultRecords je niz zapisa o kvarovima u okviru određene kategorije kvara (uređaj za bilježenje podataka ili kartica).

2.22. CardFaultRecord

Informacije pohranjene na kartici vozača ili radionice koje se odnose na određeni kvar povezan s nositeljem kartice (zahtjevi 264, 289, 318 i 341 iz Priloga 1.C).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType je vrsta kvara.

faultBeginTime je datum i vrijeme početka kvara.

faultEndTime je datum i vrijeme završetka kvara..

faultVehicleRegistration je VRN i država članica registracije vozila u kojem je došlo do kvara.

2.23. CardIccIdentification

Informacije pohranjene na kartici koje se odnose na identifikaciju integriranog kruga (IC) kartice (zahtjev 248 iz Priloga 1.C).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop je način rada „Clockstop" kako je definiran u Dodatku 2.

cardExtendedSerialNumber je jedinstveni IC serijski broj kartice kako je dodatno određeno vrstom podataka ExtendedSerialNumber.

cardApprovalNumber je homologacijski broj kartice.

cardPersonaliserID je identifikacijski broj personalizatora kartice kodiran kao ManufacturerCode.

embedderIcAssemblerId pruža informacije o ugraditelju/sastavljaču IC-a.

icIdentifier je identifikator IC-a na kartici i proizvođača IC-a kako je definirano u normi ISO/IEC 7816-6.

2.24. CardIdentification

Informacije pohranjene na kartici koje se odnose na identifikaciju kartice (zahtjevi 255, 280, 310, 333, 359, 365, 371 i 377 iz Priloga 1.C).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState              NationNumeric,
   cardNumber                          CardNumber,
   cardIssuingAuthorityName            Name,
   cardIssueDate                       TimeReal,
   cardValidityBegin                   TimeReal,
   cardExpiryDate                      TimeReal
}
```

cardIssuingMemberState je kod države članice koja izdaje karticu.

cardNumber je broj kartice.

cardIssuingAuthorityName je naziv tijela koje je izdalo karticu.

cardIssueDate je datum izdavanja kartice sadašnjem nositelju.

cardValidityBegin je datum početka valjanosti kartice.

cardExpiryDate je datum isteka valjanosti kartice.

2.25. CardMACertificate

Druga generacija:

Certifikat javnog ključa kartice za uzajamnu autentifikaciju s jedinicom u vozilu. Struktura tog certifikata utvrđena je u Dodatku 11.

```
CardMACertificate ::= Certificate
```

2.26. CardNumber

Broj kartice kako je definiran definicijom (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 jedinstvena identifikacija vozača u državi članici.

ownerIdentification je jedinstvena identifikacija poduzeća ili radionice ili nadzornog tijela u državi članici.

cardConsecutiveIndex je indeks rednog broja kartice.

cardReplacementIndex je indeks zamjene kartice.

cardRenewalIndex je indeks obnavljanja kartice.

Prvi slijed izbora prikladan je za kodiranje broja kartice vozača, drugi slijed izbora prikladan je za kodiranje brojeva kartice radionice, nadzornog tijela i poduzeća.

2.27. **CardPlaceDailyWorkPeriod**

Informacije pohranjene na kartici vozača ili radionice koje se odnose na mjesta na kojima počinju i/ili završavaju razdoblja dnevnog rada (zahtjevi 272, 297, 325 i 348 iz Priloga 1.C).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord je indeks posljednjeg ažuriranog zapisa o mjestu.

Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o mjestu, a započinje s „0” za prvu pojavu zapisâ o mjestu u strukturi.

placeRecords je niz zapisa koji sadržavaju informacije povezane s unesenim mjestima.

2.28. **CardPrivateKey**

Prva generacija:

Privatni ključ kartice.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Javni ključ kartice.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Indeks obnavljanja kartice (definicija (i)).

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Dodjela vrijednosti: (vidjeti poglavlje VII. ovog Priloga).

‘0’ Prvo izdavanje.

Redoslijed povećavanja: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

Indeks zamjene kartice (definicija (j)).

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Dodjela vrijednosti: (vidjeti poglavlje VII. ovog Priloga).

‘0’ Izvorna kartica.

Redoslijed povećavanja: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

Druga generacija:

Certifikat javnog ključa kartice za potpis. Struktura tog certifikata utvrđena je u Dodatku 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Kod namijenjen razlikovanju dvaju utora u jedinici u vozilu.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.34. **CardSlotsStatus**

Kod koji označuje vrstu kartica umetnutih u dva utora u jedinici u vozilu.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti – oktetno poravnavanje: 'ccccdddd'B

'cccc'B identifikacija vrste kartice umetnute u utor suvozača,

'dddd'B identifikacija vrste kartice umetnute u utor vozača,

sa sljedećim identifikacijskim kodovima:

'0000'B nije umetnuta kartica,

'0001'B umetnuta je kartica vozača,

'0010'B umetnuta je kartica radionice,

'0011'B umetnuta je kontrolna kartica,

'0100'B umetnuta je kartica poduzeća.

2.35. **CardSlotsStatusRecordArray**

Druga generacija:

CardSlotsStatus i meta podatci kako se upotrebljavaju u postupku preuzimanja.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType označuje vrstu zapisa (CardSlotsStatus). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka CardSlotsStatus u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa CardSlotsStatus.

2.36. **CardStructureVersion**

Kod koji označuje verziju strukture upotrijebljene u tahografskoj kartici.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Dodjela vrijednosti: 'aabb'H:

'aa'H Indeks izmjena strukture

'00'H za aplikacije prve generacije

'01'H za aplikacije druge generacije

'bb'H Indeks izmjena u pogledu upotrebe podatkovnih elemenata definiranih za strukturu prikazanu gornjim bajtom.

'00'H za ovu verziju aplikacija prve generacije

'00'H za ovu verziju aplikacija druge generacije

2.37. **CardVehicleRecord**

Informacije pohranjene na kartici vozača ili radionice koje se odnose na razdoblje upotrebe vozila tijekom kalendarskog dana (zahtjevi 269, 294, 322 i 345 iz Priloga 1.C).

Prva generacija:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin je vrijednost na brojaču kilometara vozila na početku razdoblja upotrebe vozila.

vehicleOdometerEnd je vrijednost na brojaču kilometara vozila na završetku razdoblja upotrebe vozila.

vehicleFirstUse je datum i vrijeme početka razdoblja upotrebe vozila.

vehicleLastUse je datum i vrijeme završetka razdoblja upotrebe vozila.

vehicleRegistration je VRN i država članica registracije vozila.

vuDataBlockCounter je vrijednost VuDataBlockCounter pri posljednjem preuzimanju podataka o razdoblju upotrebe vozila.

Druga generacija:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljava se i sljedeći:

VehicleIdentificationNumber je identifikacijski broj vozila koji se odnosi na vozilo kao cjelinu.

2.38. **CardVehiclesUsed**

Informacije pohranjene na kartici vozača ili radionice koje se odnose na vozila kojima se koristi nositelj kartice (zahtjevi 270, 295, 323 i 346 iz Priloga 1.C).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord je indeks posljednjeg ažuriranog zapisa o vozilu.

Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o vozilu, a započinje s „0” za prvu pojavu zapisâ o vozilu u strukturi.

cardVehicleRecords je niz zapisa koji sadržavaju informacije o upotrijebljenim vozilima.

2.39. **CardVehicleUnitRecord**

Druga generacija:

Informacije pohranjene na kartici vozača ili radionice koje se odnose na upotrijebljenu jedinicu u vozilu (zahtjevi 303 i 351 iz Priloga 1.C).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                           TimeReal,
   manufacturerCode                    ManufacturerCode,
   deviceID                            INTEGER(0..255),
   vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp je početak razdoblja upotrebe jedinice u vozilu (tj. prvo umetanje kartice u jedinicu u vozilu za to razdoblje).

manufacturerCode označuje proizvođača jedinice u vozilu.

deviceID označuje vrstu jedinice u vozilu proizvođača. Vrijednost je specifična za proizvođača.

vuSoftwareVersion je broj verzije softvera jedinice u vozilu.

2.40. **CardVehicleUnitsUsed**

Druga generacija:

Informacije pohranjene na kartici vozača ili radionice koje se odnose na jedinice u vozilu kojima se koristi nositelj kartice (zahtjevi 306 i 352 iz Priloga 1.C).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord je indeks posljednjeg ažuriranog zapisa o jedinici u vozilu.

Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o jedinici u vozilu, a započinje s „0” za prvu pojavu zapisâ o jedinici u vozilu u strukturi.

cardVehicleUnitRecords je niz zapisa koji sadržavaju informacije o upotrijebljenim jedinicama u vozilima.

2.41. **Certificate**

Certifikat javnog ključa koji je izdalo certifikacijsko tijelo.

Prva generacija:

```
Certificate ::= OCTET STRING (SIZE(194))
```

Dodjela vrijednosti: digitalni potpis s djelomičnom obnovom CertificateContent u skladu s Dodatkom 11, „Zajednički sigurnosni mehanizmi”: Potpis (128 bajtova) || preostali dio javnog ključa (58 bajtova) || oznaka certifikacijskog tijela (8 bajtova).

Druga generacija:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Dodjela vrijednosti: Vidjeti Dodatak 11.

2.42. **CertificateContent**

Prva generacija:

(Jasni) sadržaj certifikata javnog ključa u skladu s Dodatkom 11, „Zajednički sigurnosni mehanizmi”.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier         INTEGER(0..255),
   certificationAuthorityReference      KeyIdentifier,
   certificateHolderAuthorisation       CertificateHolderAuthorisation,
   certificateEndOfValidity             TimeReal,
   certificateHolderReference           KeyIdentifier,
   publicKey                            PublicKey
}
```

certificateProfileIdentifier je verzija odgovarajućeg certifikata.

Dodjela vrijednosti: ‘01h’ za ovu verziju.

certificationAuthorityReference označuje certifikacijsko tijelo koje izdaje certifikat. Označuje i javni ključ tog certifikacijskog tijela.

certificateHolderAuthorisation označuje prava vlasnika certifikata.

certificateEndOfValidity je datum administrativnog isteka valjanosti certifikata.

certificateHolderReference označuje vlasnika certifikata. Označuje i njegov javni ključ.

publicKey je javni ključ potvrđen tim certifikatom.

2.43. **CertificateHolderAuthorisation**

Označuje prava vlasnika certifikata.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

Prva generacija:

tachographApplicationID je identifikator aplikacije za tahograf.

Dodjela vrijednosti: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Taj je AID vlasnički neregistrirani identifikator aplikacije u skladu s normom ISO/IEC 7816-5.

equipmentType je identifikacija vrste opreme za koju je namijenjen certifikat.

Dodjela vrijednosti: u skladu s vrstom podataka EquipmentType. Vrijednost je **0** ako je certifikat izdala država članica.

Druga generacija:

tachographApplicationID označuje šest najvažnijih bajtova identifikatora aplikacije (AID) tahografske kartice druge generacije. AID za aplikaciju tahografske kartice naveden je u poglavlju 6.2.

Dodjela vrijednosti: 'FF 53 4D 52 44 54'

equipmentType je identifikacija vrste opreme utvrđene za drugu generaciju za koju je namijenjen certifikat.

Dodjela vrijednosti: u skladu s vrstom podataka EquipmentType.

2.44. **CertificateRequestID**

Jedinstvena identifikacija zahtjeva za certifikat. Može se upotrebljavati i kao identifikacija javnog ključa jedinice u vozilu ako serijski broj jedinice u vozilu za koju je ključ namijenjen nije poznat u trenutku generiranja certifikata.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber je serijski broj zahtjeva za certifikat, jedinstven za proizvođača i mjesec naveden u nastavku.

requestMonthYear je identifikacija mjeseca i godine zahtjeva za certifikat.

Dodjela vrijednosti: BCD kodiranje mjeseca (dvije znamenke) i godine (zadnje dvije znamenke).

crIdentifier je identifikator kojim se razlikuje zahtjev za certifikat od proširenog serijskog broja.

Dodjela vrijednosti: 'FFh'.

manufacturerCode je numerički kod proizvođača koji zahtijeva certifikat.

2.45. **CertificationAuthorityKID**

Identifikator javnog ključa certifikacijskog tijela (država članica ili europsko certifikacijsko tijelo).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric je nacionalni brojčani kod certifikacijskog tijela.

nationAlpha je nacionalni alfanumerički kod certifikacijskog tijela.

keySerialNumber je serijski broj kojim se razlikuju različiti ključevi certifikacijskog tijela u slučaju promjene ključeva.

additionalInfo je dvobajtno polje za dodatne kodove (specifično za certifikacijsko tijelo).

caIdentifier je identifikator za razlikovanje identifikatora ključa certifikacijskog tijela od drugih identifikatora ključa.

Dodjela vrijednosti: '01h'.

2.46. **CompanyActivityData**

Informacije pohranjene na kartici poduzeća koje se odnose na aktivnosti izvršene s karticom (zahtjevi 373 i 379 iz Priloga 1.C).

```
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 indeks posljednjeg ažuriranog zapisa companyActivityRecord.

Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o aktivnosti poduzeća, a započinje s „0” za prvu pojavu zapisâ o aktivnosti poduzeća u strukturi.

companyActivityRecords je niz svih zapisa o aktivnosti poduzeća.

companyActivityRecord je niz informacija povezanih s jednom aktivnošću poduzeća.

companyActivityType je vrsta aktivnosti poduzeća.

companyActivityTime je datum i vrijeme provođenja aktivnosti poduzeća.

cardNumberInformation je broj kartice i država članica koja je izdala karticu s koje se preuzimaju podatci, ako postoji.

vehicleRegistrationInformation je VRN i država članica registracije vozila u kojemu je izvršeno preuzimanje podataka odnosno postavljanje ili uklanjanje blokade.

downloadPeriodBegin i **downloadPeriodEnd** su razdoblje za koje su preuzeti podaci iz jedinice u vozilu, ako postoje.

2.47. **CompanyActivityType**

Kod koji označuje aktivnost koju provodi poduzeće upotrebom svoje kartice poduzeća.

```
CompanyActivityType ::= INTEGER {
   card downloading                    (1),
   VU downloading                      (2),
   VU lock-in                          (3),
   VU lock-out                         (4)
}
```

2.48. **CompanyCardApplicationIdentification**

Informacije pohranjene na kartici poduzeća koje se odnose na identifikaciju primjene kartice (zahtjevi 369 i 375 iz Priloga 1.C).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId označuje vrstu upotrijebljene kartice.

cardStructureVersion utvrđuje verziju strukture koja je primijenjena na kartici.

noOfCompanyActivityRecords je broj zapisa o aktivnostima poduzeća koji se najviše može pohraniti na kartici.

2.49. **CompanyCardHolderIdentification**

Informacije pohranjene na kartici poduzeća koje se odnose na identifikaciju nositelja kartice (zahtjevi 372 i 378 iz Priloga 1.C).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName je naziv poduzeća nositelja.

companyAddress je adresa poduzeća nositelja.

cardHolderPreferredLanguage je odabrani jezik nositelja kartice.

2.50. **ControlCardApplicationIdentification**

Informacije pohranjene na kontrolnoj kartici koje se odnose na identifikaciju primjene kartice (zahtjevi 357 i 363 iz Priloga 1.C).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId označuje vrstu upotrijebljene kartice.

cardStructureVersion utvrđuje verziju strukture koja je primijenjena na kartici.

noOfControlActivityRecords je broj zapisa o nadzornim aktivnostima koji se najviše može pohraniti na kartici.

2.51. **ControlCardControlActivityData**

Informacije pohranjene na kontrolnoj kartici koje se odnose na nadzorne aktivnosti izvršene s karticom (zahtjevi 361 i 367 iz Priloga 1.C).

```
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 indeks posljednjeg ažuriranog zapisa o nadzornim aktivnostima.

Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o nadzornoj aktivnosti, a započinje s „0” za prvu pojavu zapisâ o nadzornoj aktivnosti u strukturi.

controlActivityRecords je niz svih zapisa o nadzornim aktivnostima.

controlActivityRecord jeniz informacija povezanih s jednom kontrolom.

controlType je vrsta kontrole.

controlTime je datum i vrijeme kontrole.

controlledCardNumber je broj kartice i država članica koja je izdala karticu koju se kontrolira.

controlledVehicleRegistration je VRN i država članica registracije vozila u kojem je provedena kontrola.

controlDownloadPeriodBegin i **controlDownloadPeriodEnd** su razdoblje za koje su eventualno preuzeti podatci.

2.52. **ControlCardHolderIdentification**

Informacije pohranjene na kontrolnoj kartici koje se odnose na identifikaciju nositelja kartice (zahtjevi 360 i 366 iz Priloga 1.C).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                    Name,
   controlBodyAddress                 Address,
   cardHolderName                     HolderName,
   cardHolderPreferredLanguage        Language
}
```

controlBodyName je naziv nadzornog tijela nositelja kartice.

controlBodyAddress je adresa nadzornog tijela nositelja kartice.

cardHolderName je prezime i ime (imena) nositelja kontrolne kartice.

cardHolderPreferredLanguage je odabrani jezik nositelja kartice.

2.53. **ControlType**

Kod koji označuje aktivnosti provedene tijekom kontrole. Ta se vrsta podataka odnosi na zahtjeve 126, 274, 299, 327 i 350 iz Priloga 1.C.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Prva generacija:

Dodjela vrijednosti – oktetno poravnavanje: 'cvpdxxxx'B (8 bitova)

'c'B preuzimanje podataka s kartice:

'0'B: tijekom ove nadzorne aktivnosti nisu preuzeti podatci s kartice,

'1'B: tijekom ove nadzorne aktivnosti preuzeti su podatci s kartice

'v'B preuzimanje podataka s jedinice u vozilu:

'0'B: tijekom ove nadzorne aktivnosti nisu preuzeti podatci s jedinice u vozilu

'1'B: tijekom ove nadzorne aktivnosti preuzeti su podatci s jedinice u vozilu

'p'B ispis:

'0'B: tijekom ove nadzorne aktivnosti nije bilo ispisa,

'1'B: tijekom ove nadzorne aktivnosti ispisani su podatci

'd'B zaslon:

'0'B: tijekom ove nadzorne aktivnosti nije upotrijebljen zaslon,

'1'B: tijekom ove nadzorne aktivnosti upotrijebljen je zaslon

'xxxx'B ne upotrebljava se.

Druga generacija:

Dodjela vrijednosti – oktetno poravnavanje: 'cvpdexxx'B (8 bitova)

'c'B preuzimanje podataka s kartice:

'0'B: tijekom ove nadzorne aktivnosti nisu preuzeti podatci s kartice,

'1'B: tijekom ove nadzorne aktivnosti preuzeti su podatci s kartice

'v'B preuzimanje podataka s jedinice u vozilu:

'0'B: tijekom ove nadzorne aktivnosti nisu preuzeti podatci s jedinice u vozilu

'1'B: tijekom ove nadzorne aktivnosti preuzeti su podatci s jedinice u vozilu

'p'B ispis:

'0'B: tijekom ove nadzorne aktivnosti nije bilo ispisa,

'1'B: tijekom ove nadzorne aktivnosti ispisani su podatci

'd'B zaslon:

'0'B: tijekom ove nadzorne aktivnosti nije upotrijebljen zaslon,

'1'B: tijekom ove nadzorne aktivnosti upotrijebljen je zaslon

‘e’B	provjera kalibriranja uz cestu:
	‘0’B: tijekom ove nadzorne aktivnosti nisu provjereni parametri kalibriranja,
	‘1’B: tijekom ove nadzorne aktivnosti provjereni su parametri kalibriranja
‘xxx’B	RFU.

2.54. **CurrentDateTime**

Trenutačni datum i vrijeme na uređaju za bilježenje podataka.

```
CurrentDateTime ::= TimeReal
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.55. **CurrentDateTimeRecordArray**

Druga generacija:

Trenutačni datum i vrijeme te meta podatci kako se upotrebljavaju u postupku preuzimanja.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType označuje vrstu zapisa (CurrentDateTime). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka CurrentDateTime u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o trenutačnom datumu i vremenu.

2.56. **DailyPresenceCounter**

Brojač pohranjen na kartici vozača ili radionice, uvećan za jedan za svaki kalendarski dan tijekom kojeg je kartica bila umetnuta u jedinicu u vozilu. Ta se vrsta podataka odnosi na zahtjeve 266, 299, 320 i 343 iz Priloga 1.C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Dodjela vrijednosti: Redni brojevi s najvećom vrijednošću = 9 999, zatim ponovno od 0. U trenutku prvog izdavanja kartice, broj je postavljen na 0.

2.57. **Datef**

Datum iskazan u brojčanom obliku spremnom za ispis.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Dodjela vrijednosti:

gggg	godina
mm	mjesec
dd	dan
‘00000000’H	izričito označuje da nema datuma.

2.58. **DateOfDayDownloaded**

Druga generacija:

Datum i vrijeme preuzimanja.

```
DateOfDayDownloaded ::= TimeReal
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.59. **DateOfDayDownloadedRecordArray**

Druga generacija:

Datum i vrijeme preuzimanja te meta podatci kako se upotrebljavaju u postupku preuzimanja.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType označuje vrstu zapisa (DateOfDayDownloaded). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka CurrentDateTime u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o datumu i vremenu preuzimanja.

2.60. **Distance**

Prijeđena udaljenost (rezultat izračuna razlike između dviju vrijednosti na brojaču u vozilu, u kilometrima).

```
Distance ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: Nepotpisani binarni broj. Vrijednost u kilometrima u radnom rasponu od 0 do 9 999 km

2.61. **DriverCardApplicationIdentification**

Informacije pohranjene na kartici vozača koje se odnose na identifikaciju primjene kartice (zahtjevi 253 i 278 iz Priloga 1.C).

Prva generacija:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId označuje vrstu upotrijebljene kartice.

cardStructureVersion utvrđuje verziju strukture koja je primijenjena na kartici.

noOfEventsPerType je broj događaja po vrsti događaja koji se najviše može pohraniti na kartici.

noOfFaultsPerType je broj kvarova po vrsti kvara koji se najviše može pohraniti na kartici.

activityStructureLength označuje broj bajtova dostupnih za pohranjivanje zapisa o aktivnostima.

noOfCardVehicleRecords je broj zapisa o vozilu koji se najviše može pohraniti na kartici.

noOfCardPlaceRecords je broj zapisa o mjestima koji se najviše može pohraniti na kartici.

Druga generacija:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljavaju se i sljedeći:

noOfGNSSCDRecords je broj GNSS zapisa o neprekidnom razdoblju vožnje koji se najviše može pohraniti na kartici.

noOfSpecificConditionRecords je broj zapisa o posebnim uvjetima koji se najviše može pohraniti na kartici.

2.62. DriverCardHolderIdentification

Informacije pohranjene na kartici vozača koje se odnose na identifikaciju nositelja kartice (zahtjevi 256 i 281 iz Priloga 1.C).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

cardHolderName je prezime i ime (imena) nositelja kartice vozača.

cardHolderBirthDate je datum rođenja nositelja kartice vozača.

cardHolderPreferredLanguage je odabrani jezik nositelja kartice.

2.63. **DSRCSecurityData**

Druga generacija:

Informacije u običnom tekstu i MAC koji je potrebno prenijeti s pomoću DSRC-a iz tahografa u uređaj za daljinsko ispitivanje (RI), više pojedinosti u Dodatku 11. dijelu B poglavlju 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 dio koda DER-TLV, postavlja se na „81 10” (vidjeti Dodatak 11. dio B poglavlje 13.).

currentDateTime je trenutačni datum i vrijeme jedinice u vozilu.

counter označuje RTM poruke.

vuSerialNumber je serijski broj jedinice u vozilu.

dSRCMKVersionNumber je broj verzije DSRC glavnog ključa iz kojeg su dobiveni DSRC ključevi specifični za jedinicu u vozilu.

tagLengthMac je oznaka i duljina podatkovnog objekta MAC kao dio koda DER-TLV. Oznaka se postavlja na ‘8E’, a duljinom se kodira duljina MAC-a u oktetima (vidjeti Dodatak 11. dio B. poglavlje 13.).

mac je MAC izračunan s pomoću RTM poruke (vidjeti Dodatak 11. dio B poglavlje 13.).

2.64. **EGFCertificate**

Druga generacija:

Certifikat javnog ključa vanjskog uređaja GNSS-a za uzajamnu autentifikaciju s jedinicom u vozilu. Struktura tog certifikata utvrđena je u Dodatku 11.

```
EGFCertificate ::= Certificate
```

2.65. **EmbedderIcAssemblerId**

Daje informacije o ugraditelju IC-a.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode je kod zemlje ugrađivača modula, a sastoji se od dva slova u skladu s normom ISO 3166.

moduleEmbedder označuje ugrađivača modula.

manufacturerInformation za internu upotrebu proizvođača

2.66. **EntryTypeDailyWorkPeriod**

Kod za razlikovanje početka i kraja unosa mjesta dnevnog rada te uvjeta unosa.

Prva generacija

```
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)
}
```

Dodjela vrijednosti: u skladu s normom ISO/IEC8824-1.

Druga generacija

```
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)
}
```

Dodjela vrijednosti: u skladu s normom ISO/IEC8824-1.

2.67. **EquipmentType**

Kod za razlikovanje različitih vrsta opreme za aplikaciju tahografa.

```
EquipmentType ::= INTEGER(0..255)
```

Prva generacija:

```
--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)
```

Dodjela vrijednosti: U skladu s normom ISO/IEC8824-1.

Vrijednost 0 rezervirana je za označivanje države članice ili Europe u certifikacijskom polju CHA.

Druga generacija:

Upotrebljavaju se jednake vrijednosti kao i u prvoj generaciji, uz sljedeće dodane vrijednosti:

```
--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)
```

Napomena: Vrijednosti druge generacije koje se odnose na pločicu, adapter i priključak vanjskog GNSS-a, kao i vrijednosti prve generacije koje se odnose na jedinicu u vozilu i senzor kretanja mogu se upotrijebiti u SealRecord, ako je to primjenljivo.

2.68. **EuropeanPublicKey**

Prva generacija:

Europski javni ključ.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Kod kojim se objašnjava zašto je zapisan određeni događaj ili kvar.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti:

'00'H	jedan od deset najnovijih (ili posljednjih) događaja ili kvarova
'01'H	najdulji događaj za deset zadnjih dana pojave
'02'H	jedan od pet najduljih događaja u zadnjih 365 dana
'03'H	zadnji događaj za deset zadnjih dana pojave
'04'H	najozbiljniji događaj za deset zadnjih dana pojave
'05'H	jedan od pet najozbiljnijih događaja u zadnjih 365 dana
'06'H	prvi događaj ili kvar do kojeg je došlo nakon zadnjeg kalibriranja
'07'H	aktivni/tekući događaj ili kvar
'08'H to '7F'H	RFU
'80'H to 'FF'H	specifično za proizvođača

2.70. **EventFaultType**

Kod kojim se određuje događaj ili kvar.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti:

Prva generacija:

'0x'H	opći događaji,
'00'H	nema podrobnijih podataka,
'01'H	umetanje nevažeće kartice,
'02'H	konflikt kartica,
'03'H	vremensko preklapanje,
'04'H	vožnja bez odgovarajuće kartice,
'05'H	umetanje kartice tijekom vožnje,
'06'H	posljednja sesija rada s karticom nije ispravno zaključena,
'07'H	prekoračenje brzine,
'08'H	prekid napajanja,
'09'H	pogreška u podatcima o kretanju,
'0A'H	proturječnost u kretanju vozila,
'0B' to '0F'H	RFU

	događaji koji označuju pokušaje probijanja zaštite povezani s jedinicom u vozilu,
‘1x’H	nema podrobnijih podataka,
‘10’H	neuspjela autentifikacija senzora kretanja,
‘11’H	neuspjela autentifikacija tahografske kartice,
‘12’H	neovlaštena promjena senzora kretanja,
‘13’H	pogreška u integritetu podataka pohranjenih na kartici,
‘14’H	pogreška u integritetu pohranjenih korisničkih podataka,
‘15’H	pogreška pri unutarnjem prijenosu podataka,
‘16’H	neovlašteno otvaranje kućišta.
‘17’H	neovlaštene preinake hardvera,
‘18’H	RFU
‘19’H to ‘1F’H	
‘2x’H	događaji koji označuju pokušaje probijanja zaštite povezani sa senzorom
‘20’H	nema podrobnijih podataka,
‘21’H	neuspješna autentifikacija,
‘22’H	pogreška u integritetu pohranjenih podataka,
‘23’H	pogreška pri unutarnjem prijenosu podataka,
‘24’H	neovlašteno otvaranje kućišta.
‘25’H	neovlaštene preinake hardvera,
‘26’H to ‘2F’H	RFU
‘3x’H	kvarovi uređaja za bilježenje podataka,
‘30’H	nema podrobnijih podataka,
‘31’H	interni kvar jedinice u vozilu
‘32’H	kvar pisača,
‘33’H	kvar zaslona,
‘34’H	kvar pri preuzimanju,
‘35’H	kvar senzora,
‘36’H to ‘3F’H	RFU
‘4x’H	kvarovi kartice,
‘40’H	nema podrobnijih podataka,
‘41’H to ‘4F’H	RFU
‘50’H to ‘7F’H	RFU
‘80’H to ‘FF’H	specifično za proizvođača

Druga generacija:

Upotrebljavaju se jednake vrijednosti kao i u prvoj generaciji, uz sljedeće dodane vrijednosti:

‘0B’H	Proturječnost u vremenu (GNSS u odnosu na unutarnji sat jedinice u vozilu),
‘0C’ to ‘0F’H	RFU,
‘5x’H	kvarovi povezani s GNSS-om
‘50’H	nema podrobnijih podataka,
‘51’H	kvar unutarnjeg prijamnika GNSS-a,
‘52’H	kvar vanjskog prijamnika GNSS-a,
‘53’H	kvar pri vanjskoj GNSS komunikaciji,
‘54’H	nema podataka o položaju GNSS-a,
‘55’H	otkrivanje neovlaštenog zahvata na GNSS-u,
‘56’H	istekla je valjanost certifikata vanjskog uređaja GNSS-a,
‘57’H to ‘5F’H	RFU
‘6x’H	kvarovi povezani s modulom za komunikaciju na daljinu,
‘60’H	nema podrobnijih podataka,
‘61’H	kvar modula za komunikaciju na daljinu,
‘62’H	kvar u komunikaciji modula za komunikaciju na daljinu,
‘63’H to ‘6F’H	RFU
‘7x’H	kvarovi povezani s ITS sučeljem,
‘70’H	nema podrobnijih podataka,
‘71’H to ‘7F’H	RFU.

2.71. **ExtendedSealIdentifier**

Druga generacija:

Proširenim identifikatorom plombe moguće je jedinstveno identificirati plombu (zahtjev 401 iz Priloga 1.C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode je kod proizvođača plombe.

sealIdentifier je identifikator plombe jedinstven za proizvođača.

2.72. **ExtendedSerialNumber**

Jedinstvena identifikacija opreme. Može se upotrebljavati i kao identifikacija javnog ključa opreme.

Prva generacija:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber je serijski broj opreme, jedinstven za proizvođača, vrstu opreme te mjesec i godinu navedene u nastavku.

monthYear je identifikacija mjeseca i godine proizvodnje (ili dodjele serijskog broja).

Dodjela vrijednosti: BCD kodiranje mjeseca (dvije znamenke) i godine (zadnje dvije znamenke).

type je identifikator vrste opreme.

Dodjela vrijednosti: specifična za proizvođača, s rezerviranom vrijednošću „FFh”

manufacturerCode: numerički kod koji označuje proizvođača homologirane opreme.

Druga generacija:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                EquipmentType,
   manufacturerCode                    ManufacturerCode
}
```

serialNumber vidjeti prvu generaciju

monthYear vidjeti prvu generaciju

type označuje vrstu opreme

manufacturerCode: vidjeti prvu generaciju.

2.73. **FullCardNumber**

Kod kojim se u potpunosti identificira tahografska kartica.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType je vrsta tahografske kartice.

cardIssuingMemberState je kod države članice koja je izdala karticu.

cardNumber je broj kartice.

2.74. **FullCardNumberAndGeneration**

Druga generacija:

Kod kojim se u potpunosti identificiraju tahografska kartica i njezina generacija.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber označuje tahografsku karticu.

generacija označuje generaciju tahografske kartice koja se upotrebljava.

2.75. **Generation**

Druga generacija:

Označuje generaciju tahografa koji se upotrebljava.

```
Generation ::= INTEGER(0..255)
```

Dodjela vrijednosti:

'00'H	RFU
'01'H	Prva generacija
'02'H	Druga generacija
'03'H .. 'FF'H	RFU

2.76. **GeoCoordinates**

Druga generacija:

Zemljopisne koordinate kodirane su kao cijeli brojevi. Ti su cijeli brojevi višekratnici koda ±DDMM.M za zemljopisnu širinu i koda ±DDDMM.M za zemljopisnu dužinu. Ovdje ±DD odnosno ±DDD označuje stupnjeve, a MM.M minute.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude je kodiran kao višekratnik (faktor 10) prikaza ±DDMM.M.

longitude je kodiran kao višekratnik (faktor 10) prikaza ±DDDMM.M.

2.77. **GNSSAccuracy**

Druga generacija:

Točnost podataka o GNSS poziciji (definicija (eee)). Ta je točnost kodirana kao cijeli broj i višekratnik je (faktor 10) vrijednosti X.Y dobivene iz NMEA-ine rečenice GSA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Druga generacija:

Informacije pohranjene na kartici vozača ili radionice koje se odnose na GNSS poziciju vozila ako neprekidno razdoblje vožnje vozača dostigne višekratnik od tri sata (zahtjev 306 i 354 iz Priloga 1.C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord            INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords         SET SIZE(NoOfGNSSCDRecords) OF
                                        GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord je indeks posljednjeg ažuriranog zapisa GNSS-a o neprekidnom razdoblju vožnje.

Dodjela vrijednosti: Broj koji odgovara brojniku GNSS zapisa o neprekidnom razdoblju vožnje, a započinje s „0” za prvu pojavu GNSS zapisâ o neprekidnom razdoblju vožnje u strukturi.

gnssContinuousDrivingRecords je niz zapisa koji sadržavaju datum i vrijeme kada neprekidno razdoblje vožnje dostigne višekratnik od tri sata te informacije o poziciji vozila.

2.79. **GNSSContinuousDrivingRecord**

Druga generacija:

Informacije pohranjene na kartici vozača ili radionice koje se odnose na GNSS poziciju vozila ako neprekidno razdoblje vožnje vozača dostigne višekratnik od tri sata (zahtjevi 305 i 353 iz Priloga 1.C).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssPlaceRecord                      GNSSPlaceRecord
}
```

timeStamp je datum i vrijeme kada neprekidno razdoblje vožnje nositelja kartice dostigne višekratnik od tri sata.

gnssPlaceRecord sadržava informacije o poziciji vozila.

2.80. **GNSSPlaceRecord**

Druga generacija:

Informacije o GNSS poziciji vozila (zahtjevi 108, 109, 110, 296, 305, 347 i 353 iz Priloga 1.C).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssAccuracy                         GNSSAccuracy,
   geoCoordinates                       GeoCoordinates
}
```

timeStamp je datum i vrijeme utvrđivanja GNSS pozicije vozila.

gnssAccuracy je točnost podataka o GNSS poziciji.

geoCoordinates je lokacija zabilježena s pomoću GNSS-a.

2.81. **HighResOdometer**

Vrijednost na brojaču kilometara vozila: Ukupna udaljenost koju je vozilo prošlo za vrijeme rada.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Dodjela vrijednosti: Nepotpisani binarni broj. Vrijednost u 1/200 km u radnom rasponu od 0 do 21 055 406 km

2.82. **HighResTripDistance**

Udaljenost prijeđena tijekom cijelog putovanja ili nekog dijela putovanja.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Dodjela vrijednosti: Nepotpisani binarni broj. Vrijednost u 1/200 km u radnom rasponu od 0 do 21 055 406 km

2.83. **HolderName**

Prezime i ime(na) nositelja kartice.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname je prezime nositelja. U prezime se ne uključuju titule.

Dodjela vrijednosti: Ako se ne radi o osobnoj kartici, holderSurname sadržava jednake informacije sadržane u companyName ili workshopName ili controlBodyName.

holderFirstNames su ime (imena) i inicijali nositelja.

2.84. **InternalGNSSReceiver**

Druga generacija:

Informacija o tome je li GNSS prijamnik unutarnji ili vanjski u odnosu na jedinicu u vozilu. TRUE znači da je GNSS prijamnik unutarnji u odnosu na jedinicu u vozilu. FALSE znači da je GNSS prijamnik vanjski.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Konstanta uređaja za bilježenje podataka (definicija (m)).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: Broj impulsa po kilometru u radnom rasponu od 0 do 64 255 impulsa/km.

2.86. **KeyIdentifier**

Jedinstveni identifikator javnog ključa koji se upotrebljava pri navođenju i izboru ključa. Isto tako identificira i nositelja ključa.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber                ExtendedSerialNumber,
   certificateRequestID                CertificateRequestID,
   certificationAuthorityKID           CertificationAuthorityKID
}
```

Prvi izbor prikladan je za navođenje javnog ključa jedinice u vozilu ili tahografske kartice.

Drugi izbor prikladan je za navođenje javnog ključa jedinice u vozilu (ako u trenutku generiranja certifikata nije poznat serijski broj jedinice u vozilu).

Treći izbor prikladan je za navođenje javnog ključa države članice.

2.87. **KMWCKey**

Druga generacija:

AES ključ i verzija ključa povezana s njime koja se upotrebljava za uparivanje jedinice u vozilu i senzora kretanja. Više pojedinosti u Dodatku 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                             AESKey,
   keyVersion                          INTEGER (SIZE(1))
}
```

kMWCKey je duljina AES ključa ulančana s ključem koji se upotrebljava za uparivanje jedinice u vozilu i senzora kretanja.

keyVersion označuje verziju AES ključa.

2.88. **Language**

Kod koji označuje jezik.

```
Language ::= IA5String(SIZE(2))
```

Dodjela vrijednosti: Kodiranje s dva mala slova u skladu s normom ISO 639.

2.89. **LastCardDownload**

Datum i vrijeme posljednjeg preuzimanja podataka s kartice, pohranjeni na kartici vozača (u svrhe drukčije od kontrole), zahtjevi 257 i 282 iz Priloga 1.C. Taj je datum moguće ažurirati s pomoću jedinice u vozilu ili bilo kojeg čitača kartica.

```
LastCardDownload ::= TimeReal
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.90. **LinkCertificate**

Druga generacija:

Certifikat kojim se povezuju parovi ključeva glavnog europskog certifikacijskog tijela.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Djelatni opseg guma kotača (definicija (u)).

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

Dodjela vrijednosti: Nepotpisan binarni broj, vrijednost u 1/8 mm u radnom rasponu od 0 do 8 031 mm.

2.92. **MAC**

Druga generacija:

Kriptografski kontrolni zbroj duljine 8, 12 ili 16 bajtova koji odgovara slijedovima šifri utvrđenima u Dodatku 11.

```
MAC ::= CHOICE {
   mac8                                 OCTET STRING (SIZE(8)),
   mac12                                OCTET STRING (SIZE(12)),
   mac16                                OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Kod koji označuje je li nositelj kartice ručno unio aktivnosti vozača pri umetanju kartice ili nije (zahtjev 081 iz Priloga 1.B i zahtjev 102 iz Priloga 1.C).

```
ManualInputFlag ::= INTEGER {
   noEntry                              (0)
   manualEntries                        (1)
}
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.94. **ManufacturerCode**

Kod koji označuje proizvođača homologirane opreme.

```
ManufacturerCode ::= INTEGER(0..255)
```

Laboratorij nadležan za ispitivanja interoperabilnosti vodi i objavljuje popis šifri proizvođača na svojoj internetskoj stranici (zahtjev 454 iz Priloga 1.C).

ManufacturerCodes se privremeno dodjeljuju proizvođačima tahografske opreme na temelju zahtjeva upućenog laboratoriju nadležnom za ispitivanje interoperabilnosti.

2.95. **ManufacturerSpecificEventFaultData**

Druga generacija:

Kodovi pogrešaka specifični za proizvođača pojednostavnjuju analizu pogrešaka i održavanje jedinica u vozilu.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                     ManufacturerCode,
   manufacturerSpecificErrorCode        OCTET STRING(SIZE(3))
}
```

manufacturerCode označuje proizvođača jedinice u vozilu.

manufacturerSpecificErrorCode je kod pogreške specifičan za proizvođača.

2.96. **MemberStateCertificate**

Certifikat javnog ključa države članice koji izdaje europsko certifikacijsko tijelo.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Druga generacija:

Certifikat države članice i meta podatci kako se upotrebljavaju u postupku preuzimanja.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType označuje vrstu zapisa (MemberStateCertificate). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka MemberStateCertificate u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa. Vrijednost se postavlja na 1 jer certifikati mogu biti različitih duljina.

records je niz zapisa o certifikatima države članice.

2.98. **MemberStatePublicKey**

Prva generacija:

Javni ključ države članice.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Naziv.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage označuje skup znakova definiran u poglavlju 4.,

name je naziv kodiran s pomoću posebnog skupa znakova.

2.100. **NationAlpha**

Abecedna oznaka države mora biti u skladu s razlikovnim oznakama koje se upotrebljavaju na vozilima u međunarodnom prometu (Bečka konvencija Ujedinjenih naroda o cestovnom prometu, 1968.)

```
NationAlpha ::= IA5String(SIZE(3))
```

Kodovi Nation Alpha i numerički (Numeric) kodovi održavaju se na popisu na internetskoj stranici laboratorija imenovanog za ispitivanje interoperabilnosti, kako je utvrđeno u zahtjevu 440 u Prilogu 1.C.

2.101. **NationNumeric**

Brojčana oznaka države.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Dodjela vrijednosti: vidjeti vrstu podatka 2.100 (NationAlpha).

Specifikaciju Nation Alpha ili Numeric, opisanu u prethodnom stavku, može se izmijeniti ili ažurirati samo nakon što je imenovani laboratorij dobio stajališta proizvođača homologiranih digitalnih i pametnih tahografa (jedinice u vozilu).

2.102. **NoOfCalibrationRecords**

Broj zapisa o kalibriranju koji se najviše može pohraniti na kartici radionice.

Prva generacija:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

Druga generacija:

$$\texttt{NoOfCalibrationRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Dodjela vrijednosti: vidjeti Dodatak 2.

2.103. **NoOfCalibrationsSinceDownload**

Brojač koji označuje broj kalibriranja provedenih s karticom radionice od posljednjeg preuzimanja podataka s nje (zahtjevi 317 i 340 u Prilogu 1.C).

$$\texttt{NoOfCalibrationsSinceDownload ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Dodjela vrijednosti: nije dodatno utvrđena.

2.104. **NoOfCardPlaceRecords**

Broj zapisa o mjestu koji se najviše može pohraniti na kartici vozača ili radionice.

Prva generacija:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

Druga generacija:

$$\texttt{NoOfCardPlaceRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Dodjela vrijednosti: vidjeti Dodatak 2.

2.105. **NoOfCardVehicleRecords**

Broj zapisa o korištenim vozilima koji se najviše može pohraniti na kartici vozača ili radionice.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.106. **NoOfCardVehicleUnitRecords**

Druga generacija:

Broj zapisa o korištenim jedinicama u vozilu koji se najviše može pohraniti na kartici vozača ili radionice.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.107. **NoOfCompanyActivityRecords**

Broj zapisa o aktivnostima poduzeća koji se najviše može pohraniti na kartici poduzeća.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.108. **NoOfControlActivityRecords**

Broj zapisa o nadzornim aktivnostima koji se najviše može pohraniti na kontrolnoj kartici.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.109. **NoOfEventsPerType**

Broj događaja po vrsti događaja koji se najviše može pohraniti na kartici.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.110. **NoOfFaultsPerType**

Broj kvarova po vrsti kvara koji se najviše može pohraniti na kartici.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.111. **NoOfGNSSCDRecords**

Druga generacija:

Broj GNSS zapisa o neprekidnom razdoblju vožnje koji se najviše može pohraniti na kartici.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.112. **NoOfSpecificConditionRecords**

Druga generacija:

Broj zapisa o posebnim uvjetima koji se najviše može pohraniti na kartici.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.113. **OdometerShort**

Vrijednost na brojaču kilometara vozila u kratkom obliku.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Dodjela vrijednosti: Nepotpisani binarni broj. Vrijednost u kilometrima u radnom rasponu od 0 do 9 999 999 km

2.114. **OdometerValueMidnight**

Vrijednost na brojaču kilometara vozila u ponoć na određeni dan (zahtjev 090 iz Priloga 1.B i zahtjev 113 iz Priloga 1.C).

```
OdometerValueMidnight ::= OdometerShort
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.115. **OdometerValueMidnightRecordArray**

Druga generacija:

OdometerValueMidnight i meta podatci koji se upotrebljavaju u postupku preuzimanja.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType označuje vrstu zapisa (OdometerValueMidnight). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka OdometerValueMidnight u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa OdometerValueMidnight.

2.116. **OverspeedNumber**

Broj događaja prekoračenja brzine od posljednje kontrole u pogledu prekoračenja brzine.

```
OverspeedNumber ::= INTEGER(0..255)
```

Dodjela vrijednosti: Vrijednost 0 znači da od posljednje kontrole u pogledu prekoračenja brzine nije zabilježen nijedan događaj prekoračenja brzine, vrijednost 1 znači da je od posljednje kontrole u pogledu prekoračenja brzine zabilježen jedan događaj prekoračenja brzine, …, vrijednost 255 znači da je od posljednje kontrole u pogledu prekoračenja brzine zabilježeno 255 ili više događaja prekoračenja brzine.

2.117. **PlaceRecord**

Informacije povezane s mjestom na kojem počinje ili završava razdoblje dnevnog rada (zahtjevi 108, 271, 296, 324 i 347 iz Priloga 1.C).

Prva generacija:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort
}
```

entryTime je datum i vrijeme povezani s unosom.

entryTypeDailyWorkPeriod je vrsta unosa.

dailyWorkPeriodCountry je unesena zemlja.

dailyWorkPeriodRegion je unesena regija.

vehicleOdometerValue je vrijednost na brojaču kilometara u trenutku unosa mjesta.

Druga generacija:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort,
   entryGNSSPlaceRecord               GNSSPlaceRecord
}
```

Uz one navedene za prvu generaciju upotrebljava se i sljedeća komponenta:

entryGNSSPlaceRecord je zabilježena lokacija i vrijeme.

2.118. **PreviousVehicleInfo**

Informacije koje se odnose na vozilo koje je vozač prethodno upotrebljavao pri umetanju kartice u jedinicu u vozilu (zahtjev 081 iz Priloga 1.B i zahtjev 102 iz Priloga 1.C).

Prva generacija:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification je VRN i država članica registracije vozila.

cardWithdrawalTime je datum i vrijeme uklanjanja kartice.

Druga generacija:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljava se i sljedeći:

vuGeneration označuje generaciju jedinice u vozilu.

2.119. **PublicKey**

Prva generacija:

Javni RSA ključ.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                    RSAKeyModulus,
   rsaKeyPublicExponent             RSAKeyPublicExponent
}
```

rsaKeyModulus je modul para ključeva.

rsaKeyPublicExponent je javni eksponent para ključeva.

2.120. **RecordType**

Druga generacija:

Upućivanje na vrstu zapisa. Ta se vrsta podataka upotrebljava za RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

Dodjela vrijednosti:

'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	specifično za proizvođača

2.121. **RegionAlpha**

Abecedna oznaka regije u određenoj zemlji.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Prva generacija:

Dodjela vrijednosti:

```
‘   ’        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
```

Druga generacija:

Kodovi RegionAlpha održavaju se na popisu na internetskoj stranici laboratorija imenovanog za ispitivanje interoperabilnosti.

2.122. **RegionNumeric**

Brojčana oznaka regije u određenoj zemlji.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Prva generacija:

Dodjela vrijednosti:

```
‘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
```

Druga generacija:

Kodovi RegionNumeric održavaju se na popisu na internetskoj stranici laboratorija imenovanog za ispitivanje interoperabilnosti.

2.123. **RemoteCommunicationModuleSerialNumber**

Druga generacija:

Serijski broj modula za komunikaciju na daljinu.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Prva generacija:

Modul RSA para ključeva.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Dodjela vrijednosti: Neodređeno.

2.125. **RSAKeyPrivateExponent**

Prva generacija:

Privatni eksponent RSA para ključeva.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Dodjela vrijednosti: Neodređeno.

2.126. **RSAKeyPublicExponent**

Prva generacija:

Javni eksponent RSA para ključeva.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Dodjela vrijednosti: Neodređeno.

2.127. **RtmData**

Druga generacija:

Za definiciju ove vrste podataka vidjeti Dodatak 14.

2.128. **SealDataCard**

Druga generacija:

U ovoj su vrsti podataka pohranjene informacije o plombama stavljenima na različite sastavne dijelove vozila i namijenjene pohranjivanju na kartici. Ova se vrsta podataka odnosi na zahtjev 337 iz Priloga 1.C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                     INTEGER(1..5),
   sealRecords                         SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords je broj zapisâ u sealRecords.

sealRecords je niz zapisa o plombi.

2.129. **SealDataVu**

Druga generacija:

U ovoj su vrsti podataka pohranjene informacije o plombama stavljenima na različite sastavne dijelove vozila i namijenjene pohranjivanju u jedinici u vozilu.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                         SealRecord
}
```

sealRecords je niz zapisa o plombi. Ako je dostupno manje od pet plombi, vrijednost EquipmentType svih neiskorištenih sealRecords postavlja se na 16, odnosno na Unused (neiskorišteno).

2.130. **SealRecord**

Druga generacija:

U ovoj se vrsti podataka pohranjuju informacije o plombi koja se stavlja na određeni sastavni dio. Ova se vrsta podataka odnosi na zahtjev 337 iz Priloga 1.C.

```
SealRecord ::= SEQUENCE {
   equipmentType                       EquipmentType,
   extendedSealIdentifier              ExtendedSealIdentifier
}
```

equipmentType označuje vrstu opreme na koju je stavljena plomba.

extendedSealIdentifier je identifikator plombe stavljene na opremu.

2.131. **SensorApprovalNumber**

Homologacijski broj senzora.

Prva generacija:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: Neodređeno.

Druga generacija:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Dodjela vrijednosti:

Homologacijski broj daje se u skladu s onime objavljenim na odgovarajućoj internetskoj stranici Europske komisije, odnosno, na primjer, uključujući spojnice ako postoje. Homologacijski broj mora biti lijevo poravnat.

2.132. **SensorExternalGNSSApprovalNumber**

Druga generacija:

Homologacijski broj vanjskog uređaja GNSS-a.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Dodjela vrijednosti:

Homologacijski broj daje se u skladu s onime objavljenim na odgovarajućoj internetskoj stranici Europske komisije, odnosno, na primjer, uključujući spojnice ako postoje. Homologacijski broj mora biti lijevo poravnat.

2.133. **SensorExternalGNSSCoupledRecord**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na identifikaciju vanjskog uređaja GNSS-a uparenog s jedinicom u vozilu (zahtjev 100 iz Priloga 1.C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber je serijski broj vanjskog uređaja GNSS-a uparenog s jedinicom u vozilu.

sensorApprovalNumber je homologacijski broj tog vanjskog uređaja GNSS-a.

sensorCouplingDate je datum uparivanja tog vanjskog uređaja GNSS-a s jedinicom u vozilu.

2.134. **SensorExternalGNSSIdentification**

Druga generacija:

Informacije koje se odnose na identifikaciju vanjskog uređaja GNSS-a (zahtjev 98 iz Priloga 1.C).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber je proširen serijski broj vanjskog uređaja GNSS-a.

sensorApprovalNumber je homologacijski broj vanjskog uređaja GNSS-a.

sensorSCIdentifier je identifikator sigurnosne komponente vanjskog uređaja GNSS-a.

sensorOSIdentifier je identifikator operativnog sustava vanjskog uređaja GNSS-a.

2.135. **SensorExternalGNSSInstallation**

Druga generacija:

Informacije pohranjene u vanjskom uređaju GNSS-a koje se odnose na ugradnju senzora vanjskog uređaja GNSS-a (zahtjev 123 iz Priloga 1.C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst je datum prvog uparivanja vanjskog uređaja GNSS-a s jedinicom u vozilu.

firstVuApprovalNumber je homologacijski broj prve jedinice u vozilu uparene s vanjskim uređajem GNSS-a.

firstVuSerialNumber je serijski broj prve jedinice u vozilu uparene s vanjskim uređajem GNSS-a.

sensorCouplingDateCurrent je datum trenutačnog uparivanja vanjskog uređaja GNSS-a s jedinicom u vozilu.

currentVuApprovalNumber jehomologacijski broj jedinice u vozilu koja je trenutačno uparena s vanjskim uređajem GNSS-a.

currentVuSerialNumber je serijski broj jedinice u vozilu koja je trenutačno uparena s vanjskim uređajem GNSS-a.

2.136. **SensorExternalGNSSOSIdentifier**

Druga generacija:

Identifikator operativnog sustava vanjskog uređaja GNSS-a.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Dodjela vrijednosti: specifična za proizvođača.

2.137. **SensorExternalGNSSSCIdentifier**

Druga generacija:

Ova se vrsta upotrebljava, na primjer, za identifikaciju kriptografskog modula vanjskog uređaja GNSS-a.

Identifikator sigurnosne komponente vanjskog uređaja GNSS-a.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: specifična za proizvođača komponente.

2.138. **SensorGNSSCouplingDate**

Druga generacija:

Datum uparivanja vanjskog uređaja GNSS-a s jedinicom u vozilu.

```
SensorGNSSCouplingDate ::= TimeReal
```

Dodjela vrijednosti: Neodređeno.

2.139. **SensorGNSSSerialNumber**

Druga generacija:

Ova se vrsta upotrebljava za pohranjivanje serijskog broja prijamnika GNSS-a i kad je u jedinici u vozilu i kad je izvan jedinice u vozilu.

Serijski broj prijamnika GNSS-a.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Informacije pohranjene u senzoru kretanja koje se odnose na identifikaciju senzora kretanja (zahtjev 077 iz Priloga 1.B i zahtjev 95 iz Priloga 1.C).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorSCIdentifier                  SensorSCIdentifier,
   sensorOSIdentifier                  SensorOSIdentifier
}
```

sensorSerialNumber je prošireni serijski broj senzora kretanja (uključuje kataloški broj i šifru proizvođača).

sensorApprovalNumber je homologacijski broj senzora kretanja.

sensorSCIdentifier je identifikator sigurnosne komponente senzora kretanja.

sensorOSIdentifier je identifikator operativnog sustava senzora kretanja.

2.141. **SensorInstallation**

Informacije pohranjene u senzoru kretanja koje se odnose na ugradnju senzora kretanja (zahtjev 099 iz Priloga 1.B i zahtjev 122 iz Priloga 1.C).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst              SensorPairingDate,
   firstVuApprovalNumber               VuApprovalNumber,
   firstVuSerialNumber                 VuSerialNumber,
   sensorPairingDateCurrent            SensorPairingDate,
   currentVuApprovalNumber             VuApprovalNumber,
   currentVUSerialNumber               VuSerialNumber
}
```

ssensorPairingDateFirst je datum prvog uparivanja senzora kretanja s jedinicom u vozilu.

firstVuApprovalNumber je homologacijski broj prve jedinice u vozilu uparene sa senzorom kretanja.

firstVuSerialNumber je serijski broj prve jedinice u vozilu uparene sa senzorom kretanja.

sensorPairingDateCurrent je datum trenutačnog uparivanja senzora kretanja s jedinicom u vozilu.

currentVuApprovalNumber je homologacijski broj jedinice u vozilu trenutačno uparene sa senzorom kretanja.

currentVuSerialNumber je serijski broj jedinice u vozilu trenutačno uparene sa senzorom kretanja.

2.142. **SensorInstallationSecData**

Informacije pohranjene na kartici radionice koje se odnose na sigurnosne podatke potrebne za uparivanje senzora kretanja s jedinicama u vozilu (zahtjevi 308 i 331 iz Priloga 1.C).

Prva generacija:

```
SensorInstallationSecData ::= TdesSessionKey
```

Dodjela vrijednosti: u skladu s normom ISO 16844-3.

Druga generacija:

Kako je opisano u Dodatku 11., na kartici radionice pohranjuju se najviše tri ključa za uparivanje jedinice u vozilu i senzora kretanja. Ti ključevi imaju različite verzije ključa.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                           KMWCKey,
   kMWCKey2                           KMWCKey OPTIONAL,
   kMWCKey3                           KMWCKey OPTIONAL
}
```

2.143. **SensorOSIdentifier**

Identifikator operativnog sustava senzora kretanja.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Dodjela vrijednosti: specifična za proizvođača.

2.144. **SensorPaired**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na identifikaciju senzora kretanja uparenog s jedinicom u vozilu (zahtjev 079 iz Priloga 1.B).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                 SensorSerialNumber,
   sensorApprovalNumber               SensorApprovalNumber,
   sensorPairingDateFirst             SensorPairingDate
}
```

sensorSerialNumber jeserijski broj senzora kretanja trenutačno uparenog s jedinicom u vozilu.

sensorApprovalNumber je homologacijski broj senzora kretanja trenutačno uparenog s jedinicom u vozilu.

sensorPairingDateFirst je datum prvog uparivanja jedinice u vozilu i senzora kretanja koji je trenutačno uparen s jedinicom u vozilu.

2.145. **SensorPairedRecord**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na identifikaciju senzora kretanja uparenog s jedinicom u vozilu (zahtjev 97 iz Priloga 1.C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber je serijski broj senzora kretanja uparenog s jedinicom u vozilu.

sensorApprovalNumber je homologacijski broj tog senzora kretanja.

sensorPairingDate je datum uparivanja tog senzora kretanja s jedinicom u vozilu.

2.146. **SensorPairingDate**

Datum uparivanja senzora kretanja s jedinicom u vozilu.

```
SensorPairingDate ::= TimeReal
```

Dodjela vrijednosti: Neodređeno.

2.147. **SensorSCIdentifier**

Identifikator sigurnosne komponente senzora kretanja.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: specifična za proizvođača komponente.

2.148. **SensorSerialNumber**

Serijski broj senzora kretanja.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Digitalni potpis.

Prva generacija:

```
Signature ::= OCTET STRING (SIZE(128))
```

Dodjela vrijednosti: u skladu s Dodatkom 11., „Zajednički sigurnosni mehanizmi”.

Druga generacija:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Dodjela vrijednosti: u skladu s Dodatkom 11., „Zajednički sigurnosni mehanizmi”.

2.150. **SignatureRecordArray**

Druga generacija:

Niz potpisa i meta podatci koji se upotrebljavaju u postupku preuzimanja.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType označuje vrstu zapisa (Signature). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka Signature u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa. Vrijednost se postavlja na 1 jer potpisi mogu biti različitih duljina.

records je niz potpisa.

2.151. **SimilarEventsNumber**

Broj sličnih događaja u određenom danu (zahtjev 094 iz Priloga 1.B i zahtjev 117 iz Priloga 1.C).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Dodjela vrijednosti: Vrijednost 0 se ne upotrebljava, vrijednost 1 znači da je tog dana zabilježen i pohranjen samo jedan događaj te vrste, vrijednost 2 znači da su tog dana zabilježena dva takva događaja (samo je jedan pohranjen), …, 255 znači da je toga dana zabilježeno 255 ili više takvih događaja.

2.152. **SpecificConditionRecord**

Informacije pohranjene na kartici vozača ili radionice ili u jedinici u vozilu koje se odnose na posebne uvjete (zahtjevi 130, 276, 301, 328 i 355 iz Priloga 1.C).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                           TimeReal,
   specificConditionType               SpecificConditionType
}
```

entryTime je datum i vrijeme unosa.

specificConditionType je kod koji označuje poseban uvjet.

2.153. **SpecificConditions**

Informacije pohranjene na kartici vozača ili radionice ili u jedinici u vozilu koje se odnose na poseban uvjet (zahtjevi 131, 277, 302, 329 i 356 iz Priloga 1.C).

Druga generacija:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                       SpecificConditionRecord
}
```

controlPointerNewestRecord je indeks posljednjeg ažuriranog zapisa o posebnim uvjetima.

Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o posebnim uvjetima, a započinje s „0” za prvu pojavu zapisâ o posebnim uvjetima u strukturi.

specificConditionRecords je niz zapisa koji sadržavaju informacije o zabilježenim posebnim uvjetima.

2.154. **SpecificConditionType**

Kod koji označuje posebne uvjete (zahtjevi 050b, 105a, 212a i 230a iz Priloga 1.B te zahtjev 62 iz Priloga 1.C).

```
SpecificConditionType ::= INTEGER(0..255)
```

Prva generacija:

Dodjela vrijednosti:

‘00’H	RFU
‘01’H	izvan područja primjene – početak
‘02’H	izvan područja primjene – kraj
‘03’H	vožnja trajektom/vlakom
‘04’H .. ‘FF’H	RFU

Druga generacija:

Dodjela vrijednosti:

‘00’H	RFU
‘01’H	izvan područja primjene – početak
‘02’H	izvan područja primjene – kraj
‘03’H	vožnja trajektom/vlakom – početak
‘04’H	vožnja trajektom/vlakom – kraj
‘05’H .. ‘FF’H	RFU

2.155. **Speed**

Brzina vozila (km/h),

```
Speed ::= INTEGER(0..255)
```

Dodjela vrijednosti: Vrijednost u kilometrima po satu u radnom rasponu od 0 do 220 km/h.

2.156. **SpeedAuthorised**

Najviša dopuštena brzina vozila (definicija (hh)).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Prosječna brzina u prethodno određenom trajanju (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Najviša brzina izmjerena u prethodno određenom trajanju.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Druga generacija:

Za definiciju ove vrste podataka vidjeti Dodatak 14.

2.160. **TachographPayloadEncrypted**

Druga generacija:

Podaci iz tahografa šifrirani DER-TLV-om, odnosno podatci koji se šalju šifrirani u RTM poruci. Šifriranje je opisano u Dodatku 11. dijelu B. poglavlju 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 dio koda DER-TLV i postavlja se na „87” (vidjeti Dodatak 11. dio B poglavlje 13.).

length je dio koda DER-TLV i kodira duljinu vrijednosti paddingContentIndicatorByte i encryptedData navedenih u nastavku.

paddingContentIndicatorByte postavlja se na „00”.

encryptedData je šifrirani tachographPayload kako je utvrđeno u Dodatku 11. dijelu B poglavlju 13. Duljina tih podataka u oktetima uvijek je višekratnik broja 16.

2.161. **TDesSessionKey**

Prva generacija:

Ključ trostrukog DES postupka.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.162. **TimeReal**

Kod za polje s datumom i vremenom, pri čemu su datum i vrijeme izraženi kao sekunde prošle od 00h.00m.00s. na 1. siječnja 1970 GMT.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Dodjela vrijednosti – oktetno poravnavanje: Broj sekundi prošlih od ponoći 1. siječnja 1970. GMT.

Datum i vrijeme ne mogu biti dalji od 2106. godine.

2.163. **TyreSize**

Oznaka dimenzija guma.

```
TyreSize ::= IA5String(SIZE(15))
```

Dodjela vrijednosti: u skladu s Direktivom 92/23 (EEZ) od 31.3.1992., SL L 129, str. 95.

2.164. **VehicleIdentificationNumber**

Identifikacijska oznaka vozila (VIN) koja se odnosi na cijelo vozilo, a uobičajeno se radi o serijskom broju šasije ili broju okvira.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Dodjela vrijednosti: Kako je definirana u normi ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Druga generacija:

Identifikacijska oznaka vozila i meta podatci kako se upotrebljavaju u postupku preuzimanja.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType označuje vrstu zapisa (VehicleIdentificationNumber). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VehicleIdentificationNumber u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o identifikacijskim brojevima vozila.

2.166. **VehicleRegistrationIdentification**

Identifikacija vozila, jedinstvena za Europu (VRN i država članica).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation je država u kojoj je vozilo registrirano.

vehicleRegistrationNumber je registracijski broj vozila (VRN).

2.167. **VehicleRegistrationNumber**

Registracijski broj vozila (VRN). Registracijski broj dodjeljuje tijelo nadležno za registraciju.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   vehicleRegNumber                    OCTET STRING (SIZE(13))
}
```

codePage označuje skup znakova definiran u poglavlju 4.,

vehicleRegNumber je VRN kodiran s pomoću posebnog skupa znakova.

Dodjela vrijednosti: Specifično za državu.

2.168. **VehicleRegistrationNumberRecordArray**

Druga generacija:

Registracijski broj vozila i meta podatci kako se upotrebljavaju u postupku preuzimanja.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleRegistrationNumber
}
```

recordType označuje vrstu zapisa (VehicleRegistrationNumber). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VehicleRegistrationNumber u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o registracijskim brojevima vozila.

2.169. **VuAbility**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje označuju mogu li se u jedinici u vozilu upotrebljavati tahografske kartice prve generacije (zahtjev 121 iz Priloga 1.C).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti – oktetno poravnavanje: 'xxxxxxxa'B (8 bitova)

Za sposobnost podržavanja kartica prve generacije:

'a'B	sposobnost podržavanja tahografskih kartica prve generacije:
	'0' B prva generacija je podržana,
	'1' B prva generacija nije podržana,
'xxxxxxx'B	RFU

2.170. **VuActivityDailyData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na izmjene aktivnosti i/ili izmjene stanja vožnje i/ili izmjene statusa kartice na određeni kalendarski dan (zahtjev 084 iz Priloga 1.B i zahtjevi 105, 106 i 107 iz Priloga 1.C) i na statuse utora u 00:00 h tog dana.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                INTEGER SIZE(0..1440),
   activityChangeInfos                SET SIZE(noOfActivityChanges) OF
                                      ActivityChangeInfo
}
```

noOfActivityChanges je broj riječi ActivityChangeInfo u nizu activityChangeInfos.

activityChangeInfos je niz riječi ActivityChangeInfo pohranjenih u jedinici u vozilu za određeni dan. Uvijek uključuje dvije riječi ActivityChangeInfo koje označuju status dvaju utora u 00:00 h tog dana.

2.171. **VuActivityDailyRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na izmjene aktivnosti i/ili izmjene stanja vožnje i/ili izmjene statusa kartice na određeni kalendarski dan (zahtjevi 105, 106 i 107 iz Priloga 1.C) i na statuse utora u 00:00 h tog dana.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType označuje vrstu zapisa (ActivityChangeInfo). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka ActivityChangeInfo u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz riječi ActivityChangeInfo pohranjenih u jedinici u vozilu za određeni dan. Uvijek uključuje dvije riječi ActivityChangeInfo koje označuju status dvaju utora u 00:00 h tog dana.

2.172. **VuApprovalNumber**

Homologacijski broj jedinice u vozilu.

Prva generacija:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: Neodređeno.

Druga generacija:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

Dodjela vrijednosti:

Homologacijski broj daje se u skladu s onime objavljenim na odgovarajućoj internetskoj stranici Europske komisije, odnosno, na primjer, uključujući spojnice ako postoje. Homologacijski broj mora biti lijevo poravnat.

2.173. **VuCalibrationData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na kalibriranje uređaja za bilježenje podataka (zahtjev 098 iz Priloga 1.B).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords             INTEGER(0..255),
   vuCalibrationRecords                 SET SIZE(noOfVuCalibrationRecords) OF
                                        VuCalibrationRecord
}
```

noOfVuCalibrationRecords je broj zapisa koje sadržava niz vuCalibrationRecords.

vuCalibrationRecords je niz zapisa o kalibriranju.

2.174. **VuCalibrationRecord**

Informacije pohranjene u jedinici u vozilu koje se odnose na kalibriranje uređaja za bilježenje podataka (zahtjev 098 iz Priloga 1.B i zahtjevi 119 i 120 iz Priloga 1.C).

Prva generacija:

```
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 svrha kalibriranja.

workshopName, workshopAddress su naziv i adresa radionice.

workshopCardNumber označuje karticu radionice upotrijebljenu tijekom kalibriranja.

workshopCardExpiryDate je datum isteka valjanosti kartice.

vehicleIdentificationNumber je VIN.

vehicleRegistrationIdentification sadržava VRN i državu članicu registracije.

wVehicleCharacteristicConstant je karakteristični koeficijent vozila.

kConstantOfRecordingEquipment je konstanta uređaja za bilježenje podataka.

lTyreCircumference je djelatni opseg guma kotača.

tyreSize je oznaka za dimenzije guma postavljenih na vozilo.

authorisedSpeed je odobrena brzina vozila.

oldOdometerValue, newOdometerValue su stare i nove vrijednosti na brojaču kilometara.

oldTimeValue, newTimeValue su stari i novi datum i vrijeme.

nextCalibrationDate je datum sljedećeg kalibriranja vrste utvrđene u podatku CalibrationPurpose koje provodi tijelo ovlašteno za pregled.

Druga generacija:

```
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
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljava se i sljedeći:

sealDataVu pruža informacije o plombama stavljenima na različite sastavne dijelove vozila.

2.175. **VuCalibrationRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na kalibriranje uređaja za bilježenje podataka (zahtjevi 119 i 120 iz Priloga 1.C).

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCalibrationRecord
}
```

recordType označuje vrstu zapisa (VuCalibrationRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuCalibrationRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o kalibriranju.

2.176. **VuCardIWData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na cikluse umetanja kartica vozača ili radionice u jedinicu u vozilu i cikluse uklanjanja tih kartica iz jedinice u vozilu (zahtjev 081 iz Priloga 1.B i zahtjev 103 iz Priloga 1.C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

nnoOfIWRecords je broj zapisâ u nizu uCardIWRecords.

vuCardIWRecords je niz zapisa koji se odnose na cikluse umetanja kartice ili cikluse njezina uklanjanja.

2.177. **VuCardIWRecord**

Informacije pohranjene u jedinici u vozilu koje se odnose na ciklus umetanja kartice vozača ili radionice u jedinicu u vozilu i ciklus uklanjanja te kartice iz jedinice u vozilu (zahtjev 081 iz Priloga 1.B i zahtjev 102 iz Priloga 1.C).

Prva generacija:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

cardHolderName su prezime i imena nositelja kartice vozača ili radionice pohranjeni na kartici.

fullCardNumber je vrsta kartice, država članica koja ju je izdala i broj kartice kako su pohranjeni na kartici.

cardExpiryDate je datum isteka valjanosti kartice pohranjen na kartici.

cardInsertionTime je datum i vrijeme umetanja.

vehicleOdometerValueAtInsertion je stanje brojača kilometara vozila pri umetanju kartice.

cardSlotNumber je utor u koji je kartica umetnuta.

cardWithdrawalTime je datum i vrijeme uklanjanja.

vehicleOdometerValueAtWithdrawal je stanje brojača kilometara vozila pri uklanjanju kartice.

previousVehicleInfo sadržava informacije o prethodnom vozilu koje je vozač koristio, kako su pohranjene na kartici.

manualInputFlag je znak kojim se označuje je li nositelj kartice ručno unio aktivnosti vozača pri umetanju kartice.

Druga generacija:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

Umjesto fullCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element.

fullCardNumberAndGeneration je vrsta kartice, država članica koja ju je izdala te broj kartice i njezina generacija, kako su pohranjeni na kartici.

2.178. **VuCardIWRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na cikluse umetanja kartica vozača ili radionice u jedinicu u vozilu i cikluse uklanjanja tih kartica iz jedinice u vozilu (zahtjev 103 iz Priloga 1.C).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType označuje vrstu zapisa (VuCardIWRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuCardIWRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa koji se odnose na cikluse umetanja kartice ili cikluse njezina uklanjanja.

2.179. **VuCardRecord**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na korištenu karticu tahografa (zahtjev 132 iz Priloga 1.C).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber očitan iz datoteke EF_ICC u MF-u kartice.

cardPersonaliserID očitan iz datoteke EF_ICC u MF-u kartice.

typeOfTachographCardId očitan iz datoteke EF_Application_Identification u DF_Tachograph_G2.

cardStructureVersion očitan iz datoteke EF_Application_Identification u DF_Tachograph_G2..

cardNumber očitan iz datoteke EF_Identification u DF_Tachograph_G2..

2.180. **VuCardRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na kartice tahografa korištene s tom jedinicom u vozilu. Te su informacije namijenjene analizi jedinice u vozilu – problemi s karticom (zahtjev 132 iz Priloga 1.C).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType označuje vrstu zapisa (VuCardRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuCardRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa koji se odnose na tahografske kartice korištene s tom jedinicom u vozilu.

2.181. **VuCertificate**

Certifikat javnog ključa jedinice u vozilu.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Druga generacija:

Certifikat jedinice u vozilu i meta podatci kako se upotrebljavaju u postupku preuzimanja.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType označuje vrstu zapisa (VuCertificate). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuCertificate u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa. Vrijednost se postavlja na 1 jer certifikati mogu biti različitih duljina.

records je niz zapisa o certifikatima jedinice u vozilu.

2.183. **VuCompanyLocksData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na blokade od strane poduzeća (zahtjev 104 iz Priloga 1.B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                          INTEGER(0..255),
   vuCompanyLocksRecords              SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks jebroj blokada navedenih u podatku vuCompanyLocksRecords.

vuCompanyLocksRecords je niz zapisa o blokadama od strane poduzeća.

2.184. **VuCompanyLocksRecord**

Informacije pohranjene u jedinici u vozilu koje se odnose na jednu blokadu od strane poduzeća (zahtjev 104 iz Priloga 1.B i zahtjev 128 iz Priloga 1.C).

Prva generacija:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumber                  FullCardNumber
}
```

lockInTime, lockOutTime su datum i vrijeme postavljanja i uklanjanja blokade.

companyName, companyAddress su naziv i adresa poduzeća povezanog s postavljanjem blokade.

companyCardNumber označuje karticu korištenu pri postavljanju blokade.

Druga generacija:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumberAndGeneration     FullCardNumberAndGeneration
}
```

Umjesto companyCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element.

companyCardNumberAndGeneration označuje karticu, uključujući njezinu generaciju, korištenu pri postavljanju blokade.

2.185. **VuCompanyLocksRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na blokade od strane poduzeća (zahtjev 128 iz Priloga 1.C).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType označuje vrstu zapisa (VuCompanyLocksRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuCompanyLocksRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa. Vrijednost 0..255.

records je niz zapisa o blokadama od strane poduzeća.

2.186. **VuControlActivityData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na kontrole provedene s pomoću te jedinice u vozilu (zahtjev 102 iz Priloga 1.B).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfLocks je broj kontrola naveden u podatku vuControlActivityRecords.

vuControlActivityRecords je niz zapisa o nadzornim aktivnostima.

2.187. **VuControlActivityRecord**

Informacije pohranjene u jedinici u vozilu koje se odnose na kontrolu provedenu s pomoću te jedinice u vozilu (zahtjev 102 iz Priloga 1.B i zahtjev 126 iz Priloga 1.C).

Prva generacija:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType je vrsta kontrole.

controlTime je datum i vrijeme kontrole.

controlCardNumber označuje kontrolnu karticu korištenu pri kontroli.

downloadPeriodBeginTime je vrijeme koje označuje početak razdoblja za koje se preuzimaju podatci, u slučaju preuzimanja.

downloadPeriodEndTime je vrijeme koje označuje kraj razdoblja za koje se preuzimaju podatci, u slučaju preuzimanja.

Druga generacija:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Umjesto controlCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element.

controlCardNumberAndGeneration označuje kontrolnu karticu korištenu pri kontroli, uključujući njezinu generaciju.

2.188. **VuControlActivityRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na kontrole provedene s pomoću te jedinice u vozilu (zahtjev 126 iz Priloga 1.C).

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuControlActivityRecord
}
```

recordType označuje vrstu zapisa (VuControlActivityRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuControlActivityRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o nadzornim aktivnostima jedinice u vozilu.

2.189. **VuDataBlockCounter**

Brojač pohranjen na kartici koji uzastopno označuje cikluse umetanja kartice u jedinice u vozilu i njihovo uklanjanje iz jedinica u vozilu.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Dodjela vrijednosti: Redni brojevi s najvećom vrijednošću od 9 999, zatim ponovno od 0.

2.190. **VuDetailedSpeedBlock**

Informacije pohranjene u jedinici u vozilu koje se odnose na detaljnu brzinu vozila u minuti tijekom koje se vozilo kretalo (zahtjev 093 iz Priloga 1.B i zahtjev 116 iz Priloga 1.C).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate je datum i vrijeme prve vrijednosti brzine unutar bloka.

speedsPerSecond je kronološki niz izmjerenih brzina svake sekunde u minuti, počevši od speedBlockBeginDate (uključno).

2.191. **VuDetailedSpeedBlockRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na detaljnu brzinu vozila.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDetailedSpeedBlock
}
```

recordType označuje vrstu zapisa (VVuDetailedSpeedBlock). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuDetailedSpeedBlock u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o detaljnim blokovima brzina.

2.192. **VuDetailedSpeedData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na detaljnu brzinu vozila.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                     INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks               SET SIZE(noOfSpeedBlocks) OF
                                       VuDetailedSpeedBlock
}
```

noOfSpeedBlocks je broj blokova brzina u nizu vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks je niz zapisa o detaljnim blokovima brzina.

2.193. **VuDownloadablePeriod**

Najstariji i najnoviji datumi za koje su pohranjeni podatci u jedinici u vozilu koji se odnose na aktivnosti vozača (zahtjevi 081, 084 ili 087 iz Priloga 1.B i zahtjevi 102, 105, 108 iz Priloga 1.C).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                 TimeReal
   maxDownloadableTime                 TimeReal
}
```

minDownloadableTime je datum i vrijeme najstarijeg podatka o umetanju kartice ili promjeni aktivnosti ili unosu mjesta pohranjenog u jedinici u vozilu.

maxDownloadableTime je najstariji podatak o uklanjanju kartice ili promjeni aktivnosti ili unos mjesta i vremena pohranjen u jedinici u vozilu.

2.194. **VuDownloadablePeriodRecordArray**

Druga generacija:

VUDownloadablePeriod i meta podatci koji se upotrebljavaju u postupku preuzimanja.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDownloadablePeriod
}
```

recordType označuje vrstu zapisa (VuDownloadablePeriod). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuDownloadablePeriod u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o VuDownloadablePeriod.

2.195. **VuDownloadActivityData**

Informacije pohranjene u jedinici u vozilu koje se odnose na posljednje preuzimanje podataka s nje (zahtjev 105 iz Priloga 1.B i zahtjev 129 iz Priloga 1.C).

Prva generacija:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumber                      FullCardNumber,
   companyOrWorkshopName               Name
}
```

downloadingTime je datum i vrijeme preuzimanja.

fullCardNumber označuje karticu upotrijebljenu za odobrenje preuzimanja podataka.

companyOrWorkshopName je naziv poduzeća ili radionice.

Druga generacija:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   companyOrWorkshopName               Name
}
```

Umjesto fullCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element.

fullCardNumberAndGeneration označuje karticu upotrijebljenu za odobrenje preuzimanja podataka i njezinu generaciju.

2.196. **VuDownloadActivityDataRecordArray**

Druga generacija:

Informacije koje se odnose na posljednje preuzimanje podataka s jedinice u vozilu (zahtjev 129 iz Priloga 1.C).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType označuje vrstu zapisa (VuDownloadActivityData). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuDownloadActivityData u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o aktivnostima preuzimanja podataka.

2.197. **VuEventData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na događaje (zahtjev 094 iz Priloga 1.B, osim dijela u pogledu događaja prekoračenja brzine).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents je broj događaja navedenih u nizu vuEventRecords.

vuEventRecords je niz zapisa o događajima.

2.198. **VuEventRecord**

Informacije pohranjene u jedinici u vozilu koje se odnose na određeni događaj (zahtjev 094 iz Priloga 1.B i zahtjev 117 iz Priloga 1.C, osim dijela u pogledu događaja prekoračenja brzine).

Prva generacija:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType je vrsta događaja.

eventRecordPurpose je svrha za koju je zabilježen taj događaj.

eventBeginTime je datum i vrijeme početka događaja.

eventEndTime je datum i vrijeme završetka događaja.

cardNumberDriverSlotBegin označuje karticu umetnutu u utor vozača na početku događaja.

cardNumberCodriverSlotBegin označuje karticu umetnutu u utor suvozača na početku događaja.

cardNumberDriverSlotEnd označuje karticu umetnutu u utor vozača na završetku događaja.

cardNumberCodriverSlotEnd označuje karticu umetnutu u utor suvozača na završetku događaja.

similarEventsNumber je broj sličnih događaja tog dana.

Taj se niz može upotrebljavati za sve događaje osim događaje prekoračenja brzine.

Druga generacija:

```
VuEventRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventRecordPurpose                  EventFaultRecordPurpose,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin   FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd     FullCardNumberAndGeneration,
   similarEventsNumber                 SimilarEventsNumber,
   manufacturerSpecificEventFaultData  ManufacturerSpecificEventFaultData
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljavaju se i sljedeći:

manufacturerSpecificEventFaultData sadržava dodatne informacije o događaju, specifične za proizvođača.

Umjesto cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd, i cardNumber-CodriverSlotEnd, u podatkovnoj strukturi za drugu generaciju upotrebljavaju se sljedeći podatkovni elementi.

cardNumberAndGenDriverSlotBegin označuje karticu umetnutu u utor vozača na početku događaja i njezinu generaciju.

cardNumberAndGenCodriverSlotBegin označuje karticu umetnutu u utor suvozača na početku događaja i njezinu generaciju.

cardNumberAndGenDriverSlotEnd označuje karticu umetnutu u utor vozača na završetku događaja i njezinu generaciju.

cardNumberAndGenCodriverSlotEnd označuje karticu umetnutu u utor suvozača na završetku događaja i njezinu generaciju.

Ako događaj predstavlja proturječnost u vremenu, podatke eventBeginTime i eventEndTime tumači se kako slijedi:

eventBeginTime je datum i vrijeme na uređaju za bilježenje podataka.

eventEndTime je datum i vrijeme na uređaju GNSS-a.

2.199. **VuEventRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na događaje (zahtjev 117 iz Priloga 1.C, osim dijela u pogledu događaja prekoračenja brzine).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType označuje vrstu zapisa (VuEventRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuEventRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o događajima.

2.200. **VuFaultData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na kvarove (zahtjev 096 iz Priloga 1.B).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                         INTEGER(0..255),
   vuFaultRecords                       SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults je broj kvarova koje sadržava niz vuFaultRecords.

vuFaultRecords je niz zapisa o kvarovima.

2.201. **VuFaultRecord**

Informacije pohranjene u jedinici u vozilu koje se odnose na kvar (zahtjev 096 iz Priloga 1.B i zahtjev 118 iz Priloga 1.C).

Prva generacija:

```
VuFaultRecord ::= SEQUENCE {
   faultType                            EventFaultType,
   faultRecordPurpose                   EventFaultRecordPurpose,
   faultBeginTime                       TimeReal,
   faultEndTime                         TimeReal,
   cardNumberDriverSlotBegin            FullCardNumber,
   cardNumberCodriverSlotBegin          FullCardNumber,
   cardNumberDriverSlotEnd              FullCardNumber,
   cardNumberCodriverSlotEnd            FullCardNumber
}
```

faultType je vrsta kvara uređaja za bilježenje podataka.

faultRecordPurpose je svrha za koju je zabilježen taj kvar.

faultBeginTime je datum i vrijeme početka kvara.

faultEndTime je datum i vrijeme završetka kvara.

cardNumberDriverSlotBegin označuje karticu umetnutu u utor vozača na početku kvara.

cardNumberCodriverSlotBegin označuje karticu umetnutu u utor suvozača na početku kvara.

cardNumberDriverSlotEnd označuje karticu umetnutu u utor vozača na završetku kvara.

cardNumberCodriverSlotEnd označuje karticu umetnutu u utor suvozača na završetku kvara.

Druga generacija:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljava se i sljedeći:

manufacturerSpecificEventFaultData sadržava dodatne informacije o kvaru, specifične za proizvođača.

Umjesto cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd, i cardNumber-CodriverSlotEnd, u podatkovnoj strukturi za drugu generaciju upotrebljavaju se sljedeći podatkovni elementi:

cardNumberAndGenDriverSlotBegin označuje karticu umetnutu u utor vozača na početku kvara i njezinu generaciju.

cardNumberAndGenCodriverSlotBegin označuje karticu umetnutu u utor suvozača na početku kvara i njezinu generaciju.

cardNumberAndGenDriverSlotEnd označuje karticu umetnutu u utor vozača na završetku kvara i njezinu generaciju.

cardNumberAndGenCodriverSlotEnd označuje karticu umetnutu u utor suvozača na završetku kvara i njezinu generaciju.

2.202. **VuFaultRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na kvarove (zahtjev 118 iz Priloga 1.C).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType označuje vrstu zapisa (VuFaultRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuFaultRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o kvarovima.

2.203. **VuGNSSCDRecord**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na GNSS poziciju vozila ako neprekidno razdoblje vožnje vozača dostigne višekratnik od tri sata (zahtjevi 108 i 110 iz Priloga 1.C).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp je datum i vrijeme kada neprekidno razdoblje vožnje nositelja kartice dostigne višekratnik od tri sata.

cardNumberAndGenDriverSlot označuje karticu umetnutu u utor vozača i njezinu generaciju.

cardNumberAndGenCodriverSlot označuje karticu umetnutu u utor suvozača i njezinu generaciju.

gnssPlaceRecord sadržava informacije o poziciji vozila.

2.204. **VuGNSSCDRecordArray**

Druga generacija:

Informacije pohranjene u jedinici vozila koje se odnose na GNSS poziciju vozila ako neprekidno razdoblje vožnje vozača dostigne višekratnik od tri sata (zahtjevi 108 i 110 iz Priloga 1.C).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType označuje vrstu zapisa (VuGNSSCDRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuGNSSCDRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz GNSS zapisa o neprekidnom razdoblju vožnje.

2.205. **VuIdentification**

Informacije pohranjene u jedinici u vozilu koje se odnose na identifikaciju jedinice u vozilu (zahtjev 075 iz Priloga 1.B i zahtjevi 93 i 121 iz Priloga 1.C).

Prva generacija:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                     VuManufacturerName,
   vuManufacturerAddress                  VuManufacturerAddress,
   vuPartNumber                           VuPartNumber,
   vuSerialNumber                         VuSerialNumber,
   vuSoftwareIdentification               VuSoftwareIdentification,
   vuManufacturingDate                    VuManufacturingDate,
   vuApprovalNumber                       VuApprovalNumber
}
```

vuManufacturerName je naziv proizvođača jedinice u vozilu.

vuManufacturerAddress je adresa proizvođača jedinice u vozilu.

vuPartNumber je kataloški broj jedinice u vozilu.

vuSerialNumber je serijski broj jedinice u vozilu.

vuSoftwareIdentification označuje softver ugrađen u jedinicu u vozilu.

vuManufacturingDate je datum proizvodnje jedinice u vozilu.

cardApprovalNumber je homologacijski broj jedinice u vozilu.

Druga generacija:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber,
   vuGeneration                        Generation,
   vuAbility                           VuAbility
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljavaju se i sljedeći:

vuGeneration označuje generaciju jedinice u vozilu.

vuAbility pruža informacije o tome podržava li jedinica u vozilu tahografske kartice prve generacije ili ne.

2.206. **VuIdentificationRecordArray**

Druga generacija:

VuIdentification i meta podatci koji se upotrebljavaju u postupku preuzimanja.

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType označuje vrstu zapisa (VuIdentification). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuIdentification u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa VuIdentification.

2.207. **VuITSConsentRecord**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na pristanak vozača u pogledu upotrebe inteligentnih prijevoznih sustava.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen označuje karticu i njezinu generaciju. To mora biti kartica vozača ili kartica radionice.

consent je znak koji označuje je li vozač pristao na upotrebu inteligentnih prijevoznih sustava u dotičnom vozilu / jedinici u vozilu.

Dodjela vrijednosti:

TRUE označuje pristanak vozača na upotrebu inteligentnih prijevoznih sustava.

FALSE označuje da je vozač odbio upotrebu inteligentnih prijevoznih sustava.

2.208. **VuITSConsentRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na pristanak vozača u pogledu upotrebe inteligentnih prijevoznih sustava (zahtjev 200 iz Priloga 1.C).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType označuje vrstu zapisa (VuITSConsentRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuITSConsentRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o pristanku na upotrebu ITS-a.

2.209. **VuManufacturerAddress**

Adresa proizvođača jedinice u vozilu.

```
VuManufacturerAddress ::= Address
```

Dodjela vrijednosti: Neodređeno.

2.210. **VuManufacturerName**

Naziv proizvođača jedinice u vozilu.

```
VuManufacturerName ::= Name
```

Dodjela vrijednosti: Neodređeno.

2.211. **VuManufacturingDate**

Datum proizvodnje jedinice u vozilu.

```
VuManufacturingDate ::= TimeReal
```

Dodjela vrijednosti: Neodređeno.

2.212. **VuOverSpeedingControlData**

Informacije pohranjene u jedinici u vozilu koje se odnose na događaje prekoračenja brzine od posljednjee kontrole u pogledu prekoračenja brzine (zahtjev 095 iz Priloga 1.B i zahtjev 117 iz Priloga 1.C).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime            TimeReal,
   firstOverspeedSince                 TimeReal,
   numberOfOverspeedSince              OverspeedNumber
}
```

lastOverspeedControlTime je datum i vrijeme posljednje kontrole u pogledu prekoračenja brzine.

firstOverspeedSince je datum i vrijeme prvog prekoračenja brzine nakon provedbe te kontrole u pogledu prekoračenja brzine.

numberOfOverspeedSince je broj događaja prekoračenja brzine od posljednje kontrole u pogledu prekoračenja brzine.

2.213. **VuOverSpeedingControlDataRecordArray**

Druga generacija:

VuOverSpeedingControlData i meta podatci koji se upotrebljavaju u postupku preuzimanja.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuOverSpeedingControlData
}
```

recordType označuje vrstu zapisa (VuOverSpeedingControlData). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuOverSpeedingControlData u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o podacima o kontroli u pogledu prekoračenja brzine.

2.214. **VuOverSpeedingEventData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na događaje prekoračenja brzine (zahtjev 094 iz Priloga 1.B).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents            INTEGER(0..255),
   vuOverSpeedingEventRecords          SET SIZE(noOfVuOverSpeedingEvents) OF
                                       VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents je broj zapisa koje sadržava niz vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords je niz zapisa o događajima prekoračenja brzine.

2.215. **VuOverSpeedingEventRecord**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na događaje prekoračenja brzine (zahtjev 094 iz Priloga 1.B i zahtjev 117 iz Priloga 1.C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberDriverSlotBegin          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType je vrsta događaja.

eventRecordPurpose je svrha za koju je zabilježen taj događaj.

eventBeginTime je datum i vrijeme početka događaja.

eventEndTime je datum i vrijeme završetka događaja.

maxSpeedValue je najviša brzina izmjerena tijekom događaja.

averageSpeedValue je aritmetički prosjek brzine izmjerene tijekom događaja..

cardNumberDriverSlotBegin označuje karticu umetnutu u utor vozača na početku događaja.

similarEventsNumber je broj sličnih događaja tog dana.

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na događaje prekoračenja brzine (zahtjev 094 iz Priloga 1.B i zahtjev 117 iz Priloga 1.C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

Umjesto cardNumberDriverSlotBegin, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element:

cardNumberAndGenDriverSlotBegin označuje karticu umetnutu u utor vozača na početku događaja i njezinu generaciju.

2.216. **VuOverSpeedingEventRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na događaje prekoračenja brzine (zahtjev 117 iz Priloga 1.C).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuOverSpeedingEventRecord
}
```

recordType označuje vrstu zapisa (VuOverSpeedingEventRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuOverSpeedingEventRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o događajima prekoračenja brzine.

2.217. **VuPartNumber**

Kataloški broj jedinice u vozilu.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Dodjela vrijednosti: Specifična za proizvođača jedinice u vozilu.

2.218. **VuPlaceDailyWorkPeriodData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na mjesta na kojima vozači započinju ili završavaju razdoblje dnevnog rada (zahtjev 087 iz Priloga 1.B i zahtjevi 108 i 110 iz Priloga 1.C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords je broj zapisâ koje sadržava niz vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords je niz zapisa o mjestu.

2.219. **VuPlaceDailyWorkPeriodRecord**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na mjesto na kojem vozač započinje ili završava razdoblje dnevnog rada (zahtjev 087 iz Priloga 1.B i zahtjevi 108 i 110 iz Priloga 1.C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber je vrsta kartice vozača, država članica koja je izdala karticu i broj kartice.

placeRecord sadržava informacije povezane s unesenim mjestom.

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na mjesto na kojem vozač započinje ili završava razdoblje dnevnog rada (zahtjev 087 iz Priloga 1.B i zahtjevi 108 i 110 iz Priloga 1.C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Umjesto fullCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element:

fullCardNumberAndGeneration je vrsta kartice, država članica koja ju je izdala te broj kartice i njezina generacija, kako su pohranjeni na kartici.

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na mjesta na kojima vozači započinju ili završavaju razdoblje dnevnog rada (zahtjevi 108 i 110 iz Priloga 1.C).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType označuje vrstu zapisa (VuPlaceDailyWorkPeriodRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuPlaceDailyWorkPeriodRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa povezanih s mjestom.

2.221. **VuPrivateKey**

Prva generacija:

Privatni ključ jedinice u vozilu.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Prva generacija:

Javni ključ jedinice u vozilu.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Serijski broj jedinice u vozilu (zahtjev 075 iz Priloga 1.B i zahtjev 93 iz Priloga 1.C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Datum ugradnje verzije softvera u jedinicu u vozilu.

```
VuSoftInstallationDate ::= TimeReal
```

Dodjela vrijednosti: Neodređeno.

2.225. **VuSoftwareIdentification**

Informacije pohranjene u jedinici u vozilu koje se odnose na ugrađeni softver.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion je broj verzije softvera u jedinici u vozilu.

vuSoftInstallationDate je datum ugradnje verzije softvera.

2.226. **VuSoftwareVersion**

Broj verzije softvera u jedinici u vozilu.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Dodjela vrijednosti: Neodređeno.

2.227. **VuSpecificConditionData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na posebne uvjete.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords je broj zapisâ koje sadržava niz specificConditionRecords.

specificConditionRecords je niz zapisa povezanih s posebnim uvjetima.

2.228. **VuSpecificConditionRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na posebne uvjete (zahtjev 130 iz Priloga 1.C).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType označuje vrstu zapisa (SpecificConditionRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka SpecificConditionRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa povezanih s posebnim uvjetima.

2.229. **VuTimeAdjustmentData**

Prva generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na podešavanje vremena koje se izvršava izvan okvira redovnog kalibriranja (zahtjev 101 iz Priloga 1.B).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                INTEGER(0..6),
   vuTimeAdjustmentRecords             SET SIZE(noOfVuTimeAdjRecords) OF
                                       VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords je broj zapisâ u vuTimeAdjustmentRecords**.**

sealRecords je niz zapisa o podešavanju vremena.

2.230. **VuTimeAdjustmentGNSSRecord**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na podešavanje vremena na temelju podataka o vremenu iz GNSS-a (zahtjevi 124 i 125 iz Priloga 1.C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal
}
```

oldTimeValue, newTimeValue su stari i novi datum i vrijeme.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na podešavanje vremena izvršeno na temelju podataka o vremenu iz GNSS-a (zahtjevi 124 i 125 iz Priloga 1.C).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuTimeAdjustmentGNSSRecord
}
```

recordType označuje vrstu zapisa (VuTimeAdjustmentGNSSRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuTimeAdjustmentGNSSRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o podešavanju vremena na temelju GNSS-a.

2.232. **VuTimeAdjustmentRecord**

Informacije pohranjene u jedinici u vozilu koje se odnose na podešavanje vremena koje se izvršava izvan okvira redovnog kalibriranja (zahtjev 101 iz Priloga 1.B i zahtjevi 124 i 125 iz Priloga 1.C).

Prva generacija:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue su stari i novi datum i vrijeme.

workshopName, workshopAddress su naziv i adresa radionice.

workshopCardNumber označuje karticu radionice upotrijebljenu radi podešavanja vremena.

Druga generacija:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Umjesto workshopCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element.

workshopCardNumberAndGeneration označuje karticu radionice upotrijebljenu radi podešavanja vremena i njezinu generaciju.

2.233. **VuTimeAdjustmentRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na podešavanje vremena koje se izvršava izvan okvira redovnog kalibriranja (zahtjevi 124 i 125 iz Priloga 1.C).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType označuje vrstu zapisa (VuTimeAdjustmentRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuTimeAdjustmentRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o podešavanju vremena.

2.234. **WorkshopCardApplicationIdentification**

Informacije pohranjene na kartici radionice koje se odnose na identifikaciju primjene kartice (zahtjevi 307 i 330 iz Priloga 1.C).

Prva generacija:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId označuje vrstu upotrijebljene kartice.

cardStructureVersion utvrđuje verziju strukture koja je primijenjena na kartici.

noOfEventsPerType je broj događaja po vrsti događaja koji se najviše može pohraniti na kartici.

noOfFaultsPerType je broj kvarova po vrsti kvara koji se najviše može pohraniti na kartici.

activityStructureLength označuje broj bajtova dostupnih za pohranjivanje zapisa o aktivnostima.

noOfCardVehicleRecords je broj zapisa o vozilu koji se najviše može pohraniti na kartici.

noOfCardPlaceRecords je broj zapisa o mjestima koji se najviše može pohraniti na kartici.

noOfCalibrationRecords je broj zapisa o aktivnostima kalibriranja koji se najviše može pohraniti na kartici.

Druga generacija:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljavaju se i sljedeći:

noOfGNSSCDRecords je broj GNSS zapisa o neprekidnom razdoblju vožnje koji se najviše može pohraniti na kartici.

noOfSpecificConditionRecords je broj zapisa o posebnim uvjetima koji se najviše može pohraniti na kartici.

2.235. **WorkshopCardCalibrationData**

Informacije pohranjene na kartici radionice koje se odnose na aktivnosti radionice izvršene s karticom (zahtjevi 314, 316, 337 i 339 iz Priloga 1.C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber je ukupan broj kalibriranja izvršenih s karticom.

calibrationPointerNewestRecord je indeks posljednjeg ažuriranog zapisa o kalibriranju.

Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o kalibriranju, a započinje s „0” za prvu pojavu zapisâ o kalibriranju u strukturi.

calibrationRecords je niz zapisa koji sadržavaju informacije o kalibriranju i/ili podešavanju vremena.

2.236. **WorkshopCardCalibrationRecord**

Informacije pohranjene na kartici radionice koje se odnose na kalibriranje izvršeno s karticom (zahtjevi 314 i 337 iz Priloga 1.C).

Prva generacija:

```
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 svrha kalibriranja.

vehicleIdentificationNumber je VIN.

vehicleRegistration sadržava VRN i državu članicu registracije.

wVehicleCharacteristicConstant je karakteristični koeficijent vozila.

kConstantOfRecordingEquipment je konstanta uređaja za bilježenje podataka.

lTyreCircumference je djelatni opseg guma kotača.

tyreSize je oznaka za dimenzije guma postavljenih na vozilo.

authorisedSpeed je najveća odobrena brzina vozila.

oldOdometerValue, newOdometerValue su stare i nove vrijednosti na brojaču kilometara.

oldTimeValue, newTimeValue su stari i novi datum i vrijeme.

nextCalibrationDate je datum sljedećeg kalibriranja vrste utvrđene u podatku CalibrationPurpose koje provodi tijelo ovlašteno za pregled.

vuPartNumber, **vuSerialNumber** i **sensorSerialNumber** su podatkovni elementi za identifikaciju uređaja za bilježenje podataka.

Druga generacija:

```
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
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljavaju se i sljedeći:

sensorGNSSSerialNumber identificira vanjski uređaj GNSS-a.

rcmSerialNumber identificira modul za komunikaciju na daljinu.

sealDataCard pruža informacije o plombama stavljenima na različite sastavne dijelove vozila.

2.237. **WorkshopCardHolderIdentification**

Informacije pohranjene na kartici radionice koje se odnose na identifikaciju nositelja kartice (zahtjevi 311 i 334 iz Priloga 1.C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName je naziv radionice nositelja kartice.

workshopAddress je adresa radionice nositelja kartice.

cardHolderName je prezime i ime (imena) nositelja kartice (na primjer, ime mehaničara).

cardHolderPreferredLanguage je odabrani jezik nositelja kartice.

2.238. **WorkshopCardPIN**

Osobni identifikacijski broj kartice radionice (zahtjevi 309 i 332 iz Priloga 1.C).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: PIN poznat nositelju kartice, desno popunjen s bajtima 'FF' do 8 bajtova.

2.239. **W-VehicleCharacteristicConstant**

Karakteristični koeficijent vozila (definicija (k)).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Dodjela vrijednosti: Broj impulsa po kilometru u radnom rasponu od 0 do 64 255 impulsa/km.

2.240. **VuPowerSupplyInterruptionRecord**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na događaje prekida napajanja (zahtjev 117 iz Priloga 1.C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType je vrsta događaja.

eventRecordPurpose je svrha za koju je zabilježen taj događaj..

eventBeginTime je datum i vrijeme početka događaja.

eventEndTime je datum i vrijeme završetka događaja.

cardNumberAndGenDriverSlotBegin označuje karticu umetnutu u utor vozača na početku događaja i njezinu generaciju.

cardNumberAndGenDriverSlotEnd označuje karticu umetnutu u utor vozača na kraju događaja i njezinu generaciju.

cardNumberAndGenCodriverSlotBegin označuje karticu umetnutu u utor suvozača na početku događaja i njezinu generaciju.

cardNumberAndGenCodriverSlotEnd označuje karticu umetnutu u utor suvozača na kraju događaja i njezinu generaciju.

similarEventsNumber je broj sličnih događaja tog dana.

2.241. **VuPowerSupplyInterruptionRecordArray**

Druga generacija:

Informacije pohranjene u jedinici u vozilu koje se odnose na događaje prekida napajanja (zahtjev 117 iz Priloga 1.C).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType označuje vrstu zapisa (VuPowerSupplyInterruptionRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuPowerSupplyInterruptionRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o događajima prekida napajanja.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Druga generacija:

Niz zapisa SensorExternalGNSSCoupledRecord i meta podatci koji se upotrebljavaju u postupku preuzimanja.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType označuje vrstu zapisa (SensorExternalGNSSCoupledRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka SensorExternalGNSSCoupledRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o uparivanju senzora s vanjskim uređajem GNSS-a.

2.243. **VuSensorPairedRecordArray**

Druga generacija:

Niz zapisa SensorPairedRecord i meta podatci koji se upotrebljavaju u postupku preuzimanja.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType označuje vrstu zapisa (SensorPairedRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka SensorPairedRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o uparivanju senzora.

3. DEFINICIJE VRIJEDNOSTI I RASPONA VELIČINE

Definicija promjenljivih vrijednosti koje se upotrebljavaju u definicijama u stavku 2.

```
TimeRealRange ::= 2^32-1
```

4. SKUPINE ZNAKOVA (CHARACTER SETS)

Za IA5Strings upotrebljavaju se ASCII znakovi definirani u normi ISO/IEC 8824-1. Radi čitljivosti i lakšeg upućivanja, u nastavku je navedena dodjela vrijednosti. U slučaju nepodudarnosti, norma ISO/IEC 8824-1 ima prednost nad ovom informativnom bilješkom.

```
  ! " # $ % & ' ( ) * + , - . / 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 { | } ~
```

U drugim se nizovima znakova (adresa, naziv, VehicleRegistrationNumber) upotrebljavaju i znakovi iz raspona decimalnih kodova od 161 do 255 od sljedećih 8-bitnih standardnih skupina znakova, koje utvrđuje broj kodne stranice: Standardni skup znakova	Kodna stranica (Decimalno)
ISO/IEC 8859-1 Latinica-1 Zapadnoeuropski	1
ISO/IEC 8859-2 Latinica-2 Srednjeeuropski	2
ISO/IEC 8859-3 Latinica-3 Južnoeuropski	3
ISO/IEC 8859-5 Latinica/Ćirilica	5
ISO/IEC 8859-7 Latinica/Grčki	7
ISO/IEC 8859-9 Latinica-5 Turski	9
ISO/IEC 8859-13 Latinica-7 Baltički krug	13
ISO/IEC 8859-15 Latinica-9	15
ISO/IEC 8859-16 Latinica-10 Jugoistočnoeuropski	16
KOI8-R Latinica/Ćirilica	80
KOI8-U Latinica/Ćirilica	85

5. KODIRANJE

Pri kodiranju u skladu s pravilima o kodiranju ASN.1, sve definirane vrste podataka kodiraju se u skladu s normom ISO/IEC 8825-2, usklađena inačica.

6. IDENTIFIKATORI OBJEKTA I IDENTIFIKATORI APLIKACIJE

6.1. **Identifikatori objekta**

Identifikatori objekta (OID-ovi) navedeni u ovome poglavlju odnose se isključivo na drugu generaciju. Ti su OID-ovi utvrđeni u TR-03110-3, a ovdje ih se ponavlja u svrhu cjelovitosti. Ti su OID-ovi sadržani u podstablu bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Identifikatori postupka autentifikacije jedinice u vozilu

```
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}
```

Primjer: Ako se autentifikaciju jedinice u vozilu planira izvršiti s pomoću SHA-384, potrebno je upotrijebiti identifikator objekta (u ASN.1 zapisu) `bsi-de protocols(2) smartcard(2) 2 2 4`. Vrijednost je ovog identifikatora objekta u zapisu s točkama (*dot notation*) `0.4.0.127.0.7.2.2.2.2.4`.

	Zapis s točkama (*Dot notation*)	Zapis u bajtovima (*Byte notation*)
`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’

Identifikatori postupka autentifikacije čipa

```
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}
```

Primjer: Autentifikacija čipa izvršena je s pomoću ECDH algoritma i stvoren je AES ključ razmjene podataka dug 128 bitova. Taj će se ključ razmjene podataka zatim upotrijebiti u CBC načinu rada radi osiguranja tajnosti podataka i s CMAC algoritmom radi osiguranja vjerodostojnosti podataka. Stoga je potrebno upotrijebiti identifikator objekta (u ASN.1 zapisu) `bsi-de protocols(2) smartcard(2) 3 2 2`. Vrijednost je ovog identifikatora objekta u zapisu s točkama (*dot notation*) `0.4.0.127.0.7.2.2.3.2.2`.

	Zapis s točkama (*Dot notation*)	Zapis u bajtovima (*Byte notation*)
`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. Identifikatori aplikacije

Druga generacija:

Identifikator aplikacije (AID) za vanjski uređaj GNSS-a (druge generacije) određen je s ‘FF 44 54 45 47 4D’. To je vlasnički AID u skladu s normom ISO/IEC 7816-4.

Napomena: Zadnjih 5 bajtova kodira DTEGM za vanjski uređaj GNSS-a pametnog tahografa.

Identifikator aplikacije za aplikaciju tahografske kartice druge generacije određen je s ‘FF 53 4D 52 44 54’. To je vlasnički AID u skladu s normom ISO/IEC 7816-4.

Dodatak 2

SPECIFIKACIJE TAHOGRAFSKE KARTICE

SADRŽAJ

1. UVOD 175
1.1. Kratice 175
1.2. Literatura 176
2. ELEKTRIČNA I FIZIČKA OBILJEŽJA 176
2.1. Napon napajanja i potrošnja struje 177
2.2. Napon programiranja V_{pp} 177
2.3. Generiranje i frekvencija sata 177
2.4. Kontakt I/O 177
2.5. Stanja kartice 177
3. HARDVER I KOMUNIKACIJA 177
3.1. Uvod 177
3.2. Protokol prijenosa 178
3.2.1 Protokoli 178
3.2.2 ATR 179
3.2.3 PTS 179
3.3. Uvjeti pristupa 180
3.4. Pregled kodova naredbi i pogrešaka 183
3.5. Opis naredbi 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. STRUKTURA KARTICA TAHOGRAFA 216
4.1. Glavna datoteka MF 216

4.2. Aplikacija kartice vozača 217
4.2.1 Aplikacija kartice vozača prve generacije 217
4.2.2 Aplikacija kartice vozača druge generacije 221
4.3. Aplikacije kartice radionice 224
4.3.1 Aplikacija kartice radionice prve generacije 224
4.3.2 Aplikacija kartice radionice druge generacije 228
4.4. Aplikacije kontrolne kartice 233
4.4.1 Aplikacija kontrolne kartice prve generacije 233
4.4.2 Aplikacija kontrolne kartice druge generacije 235
4.5. Aplikacije kartice poduzeća 237
4.5.1 Aplikacija kartice poduzeća prve generacije 237
4.5.2 Aplikacija kartice poduzeća druge generacije 238

1. UVOD

1.1. **Kratice**

Za potrebe ovog dodatka primjenjuju se sljedeće kratice:

AC	Uvjeti pristupa (engl. *Access conditions*)
AES	Standard naprednog šifriranja (engl. *Advanced Encryption Standard*)
AID	Identifikator aplikacije (engl. *Application Identifier*)
ALW	Uvijek (engl. *Always*)
APDU	Podatkovna jedinica protokola aplikacije (struktura naredbe) (engl. *Application Protocol Data Unit*)
ATR	Odziv na povrat u početno stanje (engl. *Answer to Reset*)
AUT	Autentificiran.
C6, C7	Kontakti br. 6 i 7 kartice kako su opisani u normi ISO/IEC 7816-2
cc	Satni ciklusi (engl. *clock cycles*)
CHV	Informacije za provjeru nositelja kartice (engl. *Card holder Verification Information*)
CLA	Bajt razreda određene APDU naredbe (engl. *Class byte of an APDU command*)
DSRC	Namjenski komunikacijski sustav kratkog dometa (engl. *Dedicated Short Range Communication*)
DF	Namjenska datoteka (engl. *Dedicated File*) DF može sadržavati druge datoteke (EF ili DF)
ECC	Kriptografija na temelju eliptičke krivulje (engl. *Elliptic Curve Cryptography*)
EF	Elementarna datoteka (engl. *Elementary File*)
etu	Elementarna jedinica vremena (engl. *elementary time unit*)
G1	Prva generacija
G2	Druga generacija
IC	Integrirani krug (engl. *Integrated Circuit*)
ICC	Kartica s integriranim krugovima (engl. *Integrated Circuit Card*)
ID	Identifikator (engl. *Identifier*)
IFD	Naprava sučelja (engl. *Interface Device*)
IFS	Veličina informacijskog polja (engl. *Information Field Size*)
IFSC	Veličina informacijskog polja na kartici (engl. *Information Field Size for the card*)

IFSD	Veličina informacijskog polja naprave (za terminal) (engl. *Information Field Size Device (for the Terminal)*)
INS	Bajt instrukcije određene APDU naredbe (engl. *Instruction byte of an APDU command*)
Lc	Duljina ulaznih podataka za naredbu APDU (engl. *Length of the input data for a APDU command*)
Le	Duljina očekivanih podataka (izlazni podatci za naredbu) (engl. *Length of the expected data (output data for a command)*)
MF	Glavna datoteka (temeljni DF) (engl. *Master File (root DF)*)
NAD	Adresa čvora upotrijebljena u protokolu T = 1 (engl. *Node Address used in T=1 protocol*)
NEV	Nikad (engl. *Never*)
P1-P2	Parametarski bajtovi (engl. *Parameter bytes*)
PIN	Osobni identifikacijski broj (engl. *Personal Identification Number*)
PRO SM	Zaštićeno sigurnim prijenosom poruka (engl. *Protected with secure messaging*)
PTS	Odabir prijenosa protokola (engl. *Protocol Transmission Selection*)
RFU	Rezervirano za buduću upotrebu (engl. *Reserved for Future Use*)
RST	Povratak u početno stanje (kartice) (engl. *Reset (of the card)*)
SFID	Kratki EF identifikator (engl. *Short EF Identifier*)
SM	Sigurne poruke (engl. *Secure Messaging*)
SW1-SW2	Statusni bajtovi (engl. *Status bytes*)
TS	Početni ATR znak (engl. *Initial ATR character*)
VPP	Napon programiranja (engl. *Programming Voltage*)
VU	Jedinica u vozilu (engl. *Vehicle Unit*)
XXh	Vrijednost XX u heksadecimalnom zapisu
'XXh'	Vrijednost XX u heksadecimalnom zapisu
||	Simbol ulančavanja 03||04 = 0304

1.2. **Literatura**

U ovome su Dodatku upotrijebljeni sljedeći izvori:

ISO/IEC 7816-2 Identification cards – Integrated circuit cards – Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Identification cards – Integrated circuit cards – Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Identification cards – Integrated circuit cards – Part 8: Commands for security operations. ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function. ISO/IEC 9797-2:2011

2. ELEKTRIČNA I FIZIČKA OBILJEŽJA

TCS_01 Ako nije drukčije propisano, svi elektronički signali moraju biti u skladu s normom ISO/IEC 7816-3.

TCS_02 Položaj i dimenzije kontakata kartice moraju biti u skladu s ISO/IEC 7816-2.

2.1. **Napon napajanja i potrošnja struje**

TCS_03 Kartica radi u skladu sa specifikacijama u granicama potrošnje naznačenima u normi ISO/IEC 7816-3.

TCS_04 Kartica radi s Vcc = 3V (±0,3 V) ili s Vcc = 5V (±0,5 V).

Napon se odabire prema ISO/IEC 7816-3.

2.2. **Napon programiranja V_{pp}**

TCS_05 Kartica ne zahtijeva napon programiranja na pinu C6. Očekuje se da pin C6 nije priključen na IFD. Kontakt C6 može se priključiti na V_{cc} u kartici, ali ne smije ga se uzemljiti. Ovaj se napon ni u kojem slučaju ne bi trebao interpretirati.

2.3. **Generiranje i frekvencija sata**

TCS_06 Kartica radi u frekvencijskom rasponu od 1 do 5 MHz, a može podržavati i više frekvencije. Unutar jedne sesije rada s karticom, frekvencija sata može odstupati za ±2 %. Frekvenciju sata generira jedinica u vozilu, a ne sama kartica. Radni ciklus se može izmjenjivati između 40 i 60 %.

TCS_07 Vanjski sat može se zaustaviti u uvjetima sadržanima u datoteci kartice EF ICC. Prvi bajt sadržaja datoteke EF ICC kodira uvjete režima Clockstop:

Niska	Visoka		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop dopušten, nema povlaštene razine
0	1	1	Clockstop dopušten, povlaštena je visoka razina
1	0	1	Clockstop dopušten, povlaštena je niska razina
0	0	0	Clockstop nije dopušten
0	1	0	Clockstop je dopušten isključivo na visokoj razini
1	0	0	Clockstop je dopušten isključivo na niskoj razini

Bitovi od 4 do 8 se ne koriste.

2.4. **Kontakt I/O**

TCS_08 Kontakt I/O C7 upotrebljava se za prijam podataka iz IFD-a i odašiljanje podataka u IFD. Tijekom rada, u režimu odašiljanja treba bitiili kartica ili IFD. Ako su obje jedinice u režimu odašiljanja, to ne uzrokuje oštećenje kartice. Kad ne odašilje, kartica ulazi u režim prijama.

2.5. **Stanja kartice**

TCS_09 Dok je priključeno napajanje, kartica radi u dva stanja:

radno stanje tijekom izvršavanja naredbe ili spajanja s digitalnom jedinicom,

stanje mirovanja u svako drugo vrijeme; u tom stanju kartica zadržava sve podatke.

3. HARDVER I KOMUNIKACIJA

3.1. **Uvod**

Ovaj stavak opisuje minimalnu funkcionalnost koju moraju imati tahografske kartice i jedinice u vozilu kako bi se osigurali ispravan rad i interoperabilnost.

Tahografske kartice su što je više moguće sukladne raspoloživim primjenjivim ISO/IEC normama (posebno ISO/IEC 7816). No ipak, naredbe i protokoli su u cijelosti opisani kako bi se odredila neka ograničena uporaba ili neke razlike ako ih ima. Ako nije drukčije naznačeno, navedene naredbe u cijelosti su u skladu sa spomenutim normama.

3.2. **Protokol prijenosa**

TCS_10 Protokol prijenosa u skladu je s normom ISO/IEC 7816-3 za T = 0 i T = 1. Konkretno, jedinica vozila mora raspoznati produljenja vremena čekanja koje odašilje kartica.

3.2.1 *Protokoli*

TCS_11 Kartica mora podržavati protokol **T = 0** i protokol **T = 1**. Kartice mogu podržavati i druge protokole koji se odnose na kontakte.

TCS_12 **T = 0** zadani je protokol te je stoga potrebna naredba **PTS** za prijelaz na protokol **T = 1**.

TCS_13 Naprave podržavaju **neposrednu konvenciju** u oba protokola te je stoga za karticu obvezna neposredna konvencija.

TCS_14 Bajt **Veličina informacijskog polja na kartici** prisutan je pri ATR-u u znaku TA3. Ta vrijednost iznosi najmanje 'F0h' (= 240 bajta).

Na protokole se primjenjuju sljedeća ograničenja:

TCS_15 **T = 0**

— Naprava sučelja podržava odgovor na I/O nakon vršnog signala na RST od 400 cc.

— Naprava sučelja mora moći iščitati znakove s razmakom od 12 etu.

— Naprava sučelja mora moći iščitati pogrešan znak i njegovo ponavljanje ako su razmaknuti za 13 etu. Ako je otkriven pogrešan znak, može se pojaviti signal pogreške na I/O između 1 etu i 2 etu. Naprava podržava kašnjenje od 1 etu.

— Naprava sučelja prihvaća 33-bajtni ATR (TS + 32).

— Ako je u ATR prisutan TC1, za znakove koje šalje naprava sučelja prisutno je dodatno zaštitno vrijeme, iako znakovi koje šalje kartica i dalje mogu biti razmaknuti za 12 etu. Ovo vrijedi i za znak ACK, koji kartica šalje nakon znaka P3 koji je odaslala naprava sučelja.

— Naprava sučelja uzima u obzir znak NUL koji odašilje kartica.

— Naprava sučelja prihvaća komplementarne režime za ACK.

— Naredba kojom se potražuje odgovor (get-response) ne može se koristiti u režimu ulančavanja za dobivanje podataka čija bi duljina mogla prelaziti 255 bajtova.

TCS_16 **T = 1**

— Bajt NAD: ne upotrebljava se (NAD se postavlja na '00').

— S-block ABORT: ne upotrebljava se.

— Pogreška stanja S-block VPP: ne upotrebljava se.

— Ukupna dužina ulančavanja podatkovnog polja ne prelazi 255 bajta (što osigurava IFD).

— Veličina informacijskog polja naprave (IFSD) naznačena je s pomoću IFD-a neposredno nakon ATR-a: IFD odašilje S-Block IFS zahtjev nakon ATR-a, a kartica šalje nazad S-Block IFS. Preporučena vrijednost za IFSD je 254 bajta.

— Kartica ne traži ponovno podešavanje IFS-a.

3.2.2 *ATR*

TCS_17 Naprava provjerava bajtove ATR u skladu s normom ISO/IEC 7816-3. Ne vrši se provjera na povijesnim znakovima ATR.

Primjer osnovnog bi-protokola ATR u skladu s normom ISO/IEC 7816-3.

Znak	Vrijednost	Napomene
TS	'3Bh'.	Označuje neposrednu konvenciju.
T0	'85h'.	TD1 prisutan; prisutno je pet povijesnih bajtova.
TD1	'80h'	TD2 prisutan; upotrebljava se T = 0
TD2	'11h'.	TA3 prisutan; upotrebljava se T = 1
TA3	'XXh' (najmanje 'F0h')	Veličina informacijskog polja na kartici (IFSC)
TH1 do TH5	'XXh'	Povijesni znakovi
TCK	'XXh'	Znak za provjeravanje (isključivi OR, tj. XOR)

TCS_18 Nakon ATR-a (odziv na povrat u početno stanje) implicitno se odabire glavna datoteka (MF) i ona postaje trenutačni direktorij.

3.2.3 *PTS*

TCS_19 T = 0 je zadani protokol. Za postavljanje protokola T = 1 uređaj šalje kartici PTS (poznat i kao PPS).

TCS_20 Kako su protokoli T = 0 i T = 1 obvezni, osnovni PTS za izmjenu protokola obvezan je za karticu.

Kako je naznačeno u normi ISO/IEC 7816-3, PTS se može upotrebljavati za prijelaz na brzine prijenosa podataka više od zadane brzine prijenosa podataka koju predlaže kartica u ATR (bajt TA (1)), ako postoji.

Za karticu su više brzine prijenosa podataka neobvezne.

TCS_21 Ako nije podržana niti jedna brzina prijenosa podataka osim zadane (ili ako odabrana brzina prijenosa podataka nije podržana), kartica ispravno odgovara na PTS u skladu s normom ISO/IEC 7816-3 ispuštanjem bajta PPS1.

Primjeri osnovnih PTS za odabir protokola su sljedeći:

Znak	Vrijednost	Napomene
PPSS	'FFh'	Početni znak.
PPS0	'00h' ili '01h'	Nema PPS1 do PPS3; '00h' za odabir T0, '01h' za odabir T1.
PK	'XXh'	Znak za provjeravanje: 'XXh' = 'FFh' ako je PPS0 = '00h', 'XXh' = 'FEh' ako je PPS0 = '01h'.

3.3. **Uvjeti pristupa**

TCS_22 Pravilom za pristup utvrđuju se odgovarajući sigurnosni uvjeti za način pristupa, odnosno naredbu. Ako su ti sigurnosni zahtjevi ispunjeni, obrađuje se odgovarajuća naredba.

TCS_23 Sljedeći se sigurnosni uvjeti upotrebljavaju u tahografskim karticama:

Kratica	Značenje
ALW	Radnja je uvijek moguća i može se izvesti bez ograničenja. APDU naredbe i odgovori šalju se u običnom tekstu, odnosno bez sigurnog prijenosa poruka.
NEV	Radnja nikad nije moguća.
PLAIN-C	APDU naredbe šalju se u običnom tekstu, odnosno bez sigurnog prijenosa poruka.
PWD	Radnju je moguće provesti samo ako je PIN kartice radionice uspješno provjeren, odnosno ako je postavljen status „PIN_Verified" unutarnje sigurnosti kartice. Naredbu se mora slati bez sigurnog prijenosa poruka.
EXT-AUT-G1	Radnju je moguće provesti samo ako je naredba EXTERNAL AUTHENTICATE za autentifikaciju prve generacije (vidjeti Dodatak 11. dio A) uspješno provedena.
SM-MAC-G1	APDU (naredba i odgovor) mora se primjenjivati u sigurnom prijenosu poruka u prvoj generaciji u načinu rada namijenjenom isključivo autentifikaciji (vidjeti Dodatak 11. dio A).
SM-C-MAC-G1	Naredba APDU mora se primjenjivati u sigurnom prijenosu poruka u prvoj generaciji u načinu rada namijenjenom isključivo autentifikaciji (vidjeti Dodatak 11. dio A).
SM-R-ENC-G1	Odgovor APDU mora se primjenjivati u sigurnom prijenosu poruka u prvoj generaciji u načinu rada namijenjenom šifriranju (vidjeti Dodatak 11. dio A), odnosno ne vraća se kod za autentifikaciju poruke.
SM-R-ENC-MAC-G1	Odgovor APDU mora se primjenjivati u sigurnom prijenosu poruka u prvoj generaciji u načinu rada namijenjenom šifriranju i zatim autentifikaciji (*encrypt-then-authenticate mode*) (vidjeti Dodatak 11. dio A).
SM-MAC-G2	APDU (naredba i odgovor) mora se primjenjivati u sigurnom prijenosu poruka u drugoj generaciji u načinu rada namijenjenom isključivo autentifikaciji (vidjeti Dodatak 11. dio B).
SM-C-MAC-G2	Naredba APDU mora se primjenjivati u sigurnom prijenosu poruka u drugoj generaciji u načinu rada namijenjenom isključivo autentifikaciji (vidjeti Dodatak 11. dio B).
SM-R-ENC-MAC-G2	Odgovor APDU mora se primjenjivati u sigurnom prijenosu poruka u drugoj generaciji u načinu rada namijenjenom šifriranju i zatim autentifikaciji (*encrypt-then-authenticate mode*) (vidjeti Dodatak 11. dio B).

TCS_24 Ti sigurnosni uvjeti mogu biti povezani na sljedeće načine:

AND („i"): Svi sigurnosni uvjeti moraju biti ispunjeni

OR („ili"): Barem jedan sigurnosni uvjet mora biti ispunjen

Uvjeti pristupa datotečnom sustavu, odnosno naredbe SELECT, READ BINARY i UPDATE BINARY utvrđeni su u poglavlju 4. Uvjeti pristupa preostalim naredbama utvrđeni su u tablicama u nastavku.

TCS_25 U aplikaciji DF tahografa prve generacije upotrebljavaju se sljedeći uvjeti pristupa:

Naredba	Kartica vozača	Kartica radionice	Kontrolna kartica	Kartica poduzeća
External Authenticate				
— Za autentifikaciju prve generacije	ALW	ALW	ALW	ALW
— Za autentifikaciju druge generacije	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	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo
PSO: Compute Digital Signature	ALW ILI SM-MAC-G2	ALW ILI SM-MAC-G2	Nije primjenjivo	Nije primjenjivo
PSO: Hash	Nije primjenjivo	Nije primjenjivo	ALW	Nije primjenjivo
PSO: Hash of File	ALW ILI SM-MAC-G2	ALW ILI SM-MAC-G2	Nije primjenjivo	Nije primjenjivo
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nije primjenjivo	Nije primjenjivo	ALW	Nije primjenjivo
Verify	Nije primjenjivo	ALW	Nije primjenjivo	Nije primjenjivo

TCS_26 U aplikaciji DF tahografa druge generacije upotrebljavaju se sljedeći uvjeti pristupa:

Naredba	Kartica vozača	Kartica radionice	Kontrolna kartica	Kartica poduzeća
External Authenticate				
— Za autentifikaciju prve generacije	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo
— Za autentifikaciju druge generacije	ALW	PWD	ALW	ALW
Internal Authenticate	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo

Naredba	Kartica vozača	Kartica radionice	Kontrolna kartica	Kartica poduzeća
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	Nije primjenjivo	ALW	ALW	Nije primjenjivo
PSO: Compute Digital Signature	ALW ILI SM-MAC-G2	ALW ILI SM-MAC-G2	Nije primjenjivo	Nije primjenjivo
PSO: Hash	Nije primjenjivo	Nije primjenjivo	ALW	Nije primjenjivo
PSO: Hash of File	ALW ILI SM-MAC-G2	ALW ILI SM-MAC-G2	Nije primjenjivo	Nije primjenjivo
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nije primjenjivo	Nije primjenjivo	ALW	Nije primjenjivo
Verify	Nije primjenjivo	ALW	Nije primjenjivo	Nije primjenjivo

TCS_27 U glavnoj datoteci upotrebljavaju se sljedeći uvjeti pristupa:

Naredba	Kartica vozača	Kartica radionice	Kontrolna kartica	Kartica poduzeća
External Authenticate				
— Za autentifikaciju prve generacije	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo
— Za autentifikaciju druge generacije	ALW	PWD	ALW	ALW
Internal Authenticate	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo
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	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo

Naredba	Kartica vozača	Kartica radionice	Kontrolna kartica	Kartica poduzeća
PSO: Compute Digital Signature	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo
PSO: Hash	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo
PSO: Hash of File	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Nije primjenjivo	ALW	Nije primjenjivo	Nije primjenjivo

TCS_28 Tahografska kartica može, ali ne mora, prihvatiti naredbu više razine sigurnosti od one navedene u sigurnosnim uvjetima. Odnosno, ako je sigurnosni uvjet ALW (ili PLAIN-C), kartica može prihvatiti naredbu sa sigurnim prijenosom poruka (način rada sa šifriranjem i/ili autentifikacijom). Ako se sigurnosnim uvjetom zahtijeva siguran prijenos poruka u načinu rada s autentifikacijom, tahografska kartica može prihvatiti naredbu sa sigurnim prijenosom poruka iste generacije u načinu rada s autentifikacijom i šifriranjem.

Napomena: U opisima naredbi navedeno je više informacija o podržavanju naredbi za različite vrste tahografskih kartica i različite namjenske datoteke (DF-ove).

3.4. **Pregled kodova naredbi i pogrešaka**

Naredbe i ustroj datoteka izvedeni su i usklađeni s normom ISO/IEC 7816-4.

Ovaj odjeljak opisuje sljedeće parove naredbi i odgovora APDU: Varijante naredbi koje podržavaju aplikacije prve i druge generacije navedene su u odgovarajućim opisima naredbi.

Naredba	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	

Naredba	INS
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 Statusne riječi SW1 SW2 uključene su u svaki odgovor i označuju stanje obrade naredbe.

SW1	SW2	Značenje
90	00	Normalna obrada
61	XX	Normalna obrada XX = broj raspoloživih bajtova odgovora.
62	81	Obrada uz upozorenje. Dio vraćenih podataka može biti neispravan.
63	00	Neuspjela autentifikacija (upozorenje)
63	CX	Pogrešan CHV (PIN). ‘X’ je brojač preostalih pokušaja.
64	00	Pogreška u izvršenju – stanje postojane memorije nepromijenjeno. Pogreška u integritetu.
65	00	Pogreška u izvršenju – stanje postojane memorije promijenjeno.
65	81	Pogreška u izvršenju – stanje postojane memorije promijenjeno – pogreška memorije
66	88	Sigurnosna pogreška: pogrešan kriptografski kontrolni zbroj (tijekom sigurnog prijenosa poruka) ili pogrešan certifikat (tijekom provjere certifikata) ili pogrešan kriptogram (tijekom vanjske autentifikacije) ili pogrešan potpis (tijekom provjere potpisa)
67	00	Pogrešna dužina (pogrešan Lc ili Le)
68	82	Siguran prijenos poruke nije podržan
68	83	Zadnja očekivana naredba u lancu
69	00	Zabranjena naredba (nema odgovora u T = 0)
69	82	Sigurnosni status nije zadovoljen.
69	83	Blokiran način autentifikacije.
69	85	Uvjeti uporabe nisu zadovoljeni.
69	86	Naredba nije dopuštena (nema trenutačnog EF-a).

SW1	SW2	Značenje
69	87	Nedostaju očekivani podatkovni objekti sigurnog prijenosa poruka
69	88	Neispravni podatkovni objekti sigurnog prijenosa poruka
6A	80	Pogrešni parametri u podatkovnom polju
6A	82	Datoteka nije pronađena.
6A	86	Pogrešni parametri P1-P2.
6A	88	Podatci na koje upućuje naredba nisu pronađeni.
6B	00	Pogrešni parametri (protuvrijednost izvan EF).
6C	XX	Pogrešna dužina, SW2 označuje točnu dužinu. Nikakvo podatkovno polje nije uzvraćeno.
6D	00	Naredbeni kod nije podržan ili nije valjan.
6E	00	Razred nije podržan.
6F	00	Ostale pogreške provjere.

TCS_30 Ako je ispunjen više od jednog uvjeta za greške u jednoj APDU naredbi, kartica može uzvratiti bilo koju od odgovarajućih statusnih riječi.

3.5. **Opis naredbi**

U ovom su poglavlju opisane obvezne naredbe za tahografske kartice.

Daljnje predmetne pojedinosti, povezane s obuhvaćenim kriptografskim radnjama navedene su u Dodatku 11. „Zajednički sigurnosni mehanizmi" za tahografe prve i druge generacije.

Sve naredbe opisane su neovisno o korištenom protokolu (T = 0 ili T = 1). Uvijek su naznačeni APDU bajtovi CLA, INS, PI, P2, Lc i Le. Ako Lc ili Le nisu potrebni za opisanu naredbu, pridružena duljina, vrijednost i opis su prazni.

TCS_31 Ako se zahtijevaju oba bajta duljine (Lc i Le), opisanu naredbu potrebno je podijeliti u dva dijela ako IFD upotrebljava protokol T = 0: IFD šalje naredbu kako je opisana s P3 = Lc + podatci te zatim šalje naredbu GET RESPONSE (vidjeti točku 3.5.6) s P3 = Le.

TCS_32 Ako se zahtijevaju oba bajta duljine, a Le = 0 (sigurni prijenos poruka):

— prilikom korištenja protokola T = 1, kartica odgovara na Le = 0 slanjem svih raspoloživih izlaznih podataka

— prilikom korištenja protokola T = 0, IFD šalje prvu naredbu s P3 = Lc + podatci, kartica (na taj implicitni Le = 0) odgovara statusnim bajtovima '**61La**', pri čemu je La broj raspoloživih bajtova odgovora. IFD potom generira naredbu GET RESPONSE s P3 = La za čitanje podataka.

TCS_33 Tahografska kartica može podržavati produljena polja duljine u skladu s normom ISO/IEC 7816-4. Tahografska kartica koja podržava produljena polja duljine:

— pokazuje podržavanje produljenog polja duljine u ATR

— dostavlja podržane veličine međuspremnika s pomoću informacija o produljenju u EF ATR/INFO, vidjeti TCS_146.

— naznačuje podržava li produljena polja duljine za T = 1 i/ili T = 0 u EF Extended Length, vidjeti TCS_147.

— podržava produljena polja duljina za aplikacije tahografa prve i druge generacije.

Napomene:

Sve su naredbe namijenjene kratkim poljima duljine. Način upotrebe produljenih APDU-ova jasan je iz norme ISO/IEC 7816-4.

Naredbe su općenito navedene za nešifrirani način, odnosno bez sigurnog prijenosa poruka jer je razina sigurnog prijenosa poruka utvrđena u Dodatku 11. Iz uvjeta pristupa za naredbu jasno je podržavaju li se njome siguran prijenos poruka i siguran prijenos poruka za prvu generaciju i/ili drugu generaciju. Neke su varijante naredbi opisane sa sigurnim prijenosom poruka kako bi se prikazala upotreba sigurnog prijenosa poruka.

TCS_34 Jedinica u vozilu provodi cjelokupan protokol uzajamne autentifikacije jedinice u vozilu druge generacije i kartice unutar jedne sesije, uključujući provjeru certifikata (prema potrebi) u DF tahografu, DF tahografu druge generacije ili u MF-u.

3.5.1 *SELECT*

Ova naredba u skladu je s normom ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Naredba SELECT upotrebljava se za sljedeće:

— odabir DF-a aplikacije (obvezan odabir po imenu),

— odabir elementarne datoteke koja odgovara ID-u predane datoteke.

3.5.1.1 Odabir po nazivu (AID)

Ova naredba omogućuje odabir DF-a aplikacije na kartici.

TCS_35 Ova naredba može se izvoditi sa svakog mjesta u strukturi datoteke (poslije ATR ili u bilo kojem trenutku).

TCS_36 Odabir aplikacije vraća trenutačno sigurnosno okruženje u početno stanje. Nakon odabira aplikacije, više se ne odabire trenutačni javni ključ. Gubi se i uvjet pristupa EXT-AUT-G1. Ako je naredba izvršena bez sigurnog prijenosa poruka, ključevi prethodnog sigurnog prijenosa poruka više nisu dostupni.

TCS_37 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘04h’.	Odabir po nazivu (AID)
P2	1	‘0Ch’	Ne očekuje se odgovor.
Lc	1	‘NNh’	Broj bajtova poslanih na karticu (dužina AID-a): ‘06h’ za tahografsku aplikaciju
#6-#(5+NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ za aplikaciju prve generacije tahografa AID: ‘FF 53 4D 52 44 54’ za aplikaciju druge generacije tahografa

Za naredbu SELECT nije potreban nikakav odgovor (ako u T = 1 nema Le, ili se ne traži odgovor kod T = 0).

TCS_38 **Odgovor na poruku (ne traži se odgovor)**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije pronađena aplikacija koja odgovara AID, uzvraćeno stanje obrade je '**6A82**',

— U T = 1, ako je prisutan bajt Le, uzvraćeno stanje je '**6700**',

— U T = 0, ako se traži odgovor poslije naredbe SELECT, uzvraćeno stanje je '**6900**'

— Ako se odabrana aplikacija smatra neispravnom (u atributima datoteke otkrivena je pogreška u integritetu), uzvraćeno stanje obrade je '**6400**' ili '**6581**'.

3.5.1.2 Odabir elementarne datoteke upotrebom njezina identifikatora datoteke

TCS_39 **Poruka naredbe**

TCS_40 Tahografska kartica mora podržavati siguran prijenos poruka u drugoj generaciji kako je utvrđeno u Dodatku 11. dijelu B. za ovu varijantu naredbe.

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Odabir EF-a u okviru trenutačnog DF-a
P2	1	'0Ch'	Ne očekuje se odgovor.
Lc	1	'02h'	Broj bajtova poslanih na karticu
#6-#7	2	'XXXXh'	Identifikator datoteke

Za naredbu SELECT nije potreban nikakav odgovor (ako u T = 1 nema Le, ili se ne traži odgovor kod T = 0).

TCS_41 **Odgovor na poruku (ne traži se odgovor)**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije nađena datoteka koja odgovara identifikatoru datoteke, uzvraćeno stanje obrade je '**6A82**'.

— U T = 1, ako je prisutan bajt Le, uzvraćeno stanje je '**6700**',

— U T = 0, ako se traži odgovor poslije naredbe SELECT, uzvraćeno stanje je '**6900**'

— Ako se odabrana datoteka smatra neispravnom (u atributima datoteke je otkrivena pogreška u integritetu), uzvraćeno stanje je '**6400**' ili '**6581**'.

3.5.2 *READ BINARY*

Ova naredba u skladu je s normom ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Naredba READ BINARY upotrebljava se za čitanje podataka iz transparentne datoteke.

Odgovor kartice se sastoji od uzvraćanja pročitanih podataka koji se mogu neobvezno zatvoriti u strukturu sigurnog čitanja poruke.

3.5.2.1 Naredba s pomakom u P1-P2

Ova naredba omogućuje IFD-u čitanje podataka iz trenutačno odabranog EF-a bez sigurnog prijenosa poruka.

Napomena: Ova naredba se bez sigurnog prijenosa poruka može upotrebljavati samo za potrebe očitavanja datoteke koja podržava ALW sigurnosni uvjet pri načinu pristupa za očitavanje.

TCS_42 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'B0h'	Binarno čitanje
P1	1	'XXh'	Pomak u bajtovima od početka datoteke: najvažniji bajt
P2	1	'XXh'	Pomak u bajtovima od početka datoteke: najmanje važan bajt
Le	1	'XXh'	Očekivana duljina podatka. Broj bajtova koje se očitava.

Napomena: bit 8 u P1 mora biti postavljen na 0.

TCS_43 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
#1-#X	X	'XX..XXh'	Očitani podatci
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije odabran EF, uzvraćeno stanje obrade je '**6986**'.

— Ako za odabranu datoteku nisu ispunjeni sigurnosni uvjeti, naredba se prekida s '**6982**'.

— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.

— Ako veličina podataka koje treba pročitati ne odgovara veličini EF-a (pomak + Le > veličine EF-a), uzvraćeno stanje obrade je '**6700**' ili '**6Cxx**', pri čemu je 'xx' točna duljina.

— Ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade '**6400**' ili '**6581**'.

— Ako je otkrivena pogreška u integritetu u pohranjenim podatcima, kartica uzvraća tražene podatke, a uzvraćeno stanje obrade je '**6281**'.

3.5.2.1.1 Naredba sa sigurnim prijenosom poruke (primjeri)

Ova naredba omogućuje IFD-u čitanje podataka iz trenutačno odabranog EF-a uz siguran prijenos poruka radi povjere integriteta primljenih podataka i zaštite povjerljivosti podataka ako se primjenjuje sigurnosni uvjet SM-R-ENC-MAC-G1 (prva generacija) ili SM-R-ENC-MAC-G2 (druga generacija).

TCS_44 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'0Ch'	Traži se siguran prijenos poruka
INS	1	'B0h'	Binarno čitanje
P1	1	'XXh'	P1 (pomak u bajtovima od početka datoteke): najvažniji bajt
P2	1	'XXh'	P2 (pomak u bajtovima od početka datoteke): najmanje važan bajt
Lc	1	'XXh'	Duljina ulaznih podataka za siguran prijenos poruka
#6	1	'97h'	T_{LE}: Oznaka za očekivanu specifikaciju duljine.
#7	1	'01h'	L_{LE}: Duljina očekivane duljine
#8	1	'NNh'	Specifikacija očekivane duljine (izvorni Le): broj bajtova koje se očitava
#9	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#10	1	'XXh'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja '04h' za siguran prijenos poruka u prvoj generaciji (vidjeti Dodatak 11. dio A) '08h', '0Ch' ili '10h' ovisno o duljini AES ključa za siguran prijenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#11-#(10+L)	L	'XX..XXh'	Kriptografski kontrolni zbroj
Le	1	'00h'	Kako je utvrđeno u normi ISO/IEC 7816-4.

TCS_45 **Odgovor na poruku ako se ne zahtijeva SM-R-ENC-MAC-G1 (prva generacija) / SM-R-ENC-MAC-G2 (druga generacija) i ako je ulazni format za siguran prijenos poruka točan:**

Bajt	Duljina	Vrijednost	Opis
#1	1	'99h'	Oznaka za status obrade (SW1-SW2) – neobvezna za siguran prijenos poruka u prvoj generaciji
#2	1	'02h'	Duljina statusa obrade
#3 – #4	2	'XX XXh'	Status obrade nezaštićenog odgovora APDU
#5	1	'81h'	T_{PV}: Oznaka za vrijednost nešifriranih podataka
#6	L	'NNh' ili '81 NNh'	L_{PV}: duljina uzvraćenih podataka (= izvorni Le). L iznosi 2 bajta ako je L_{PV} > 127 bajtova.

Bajt	Duljina	Vrijednost	Opis
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Vrijednost nešifriranih podataka
#(6+L+NN)	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#(7+L+NN)	1	'XXh'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja '04h' za siguran prijenos poruka u prvoj generaciji (vidjeti Dodatak 11. dio A) '08h', '0Ch' ili '10h' ovisno o duljini AES ključa za siguran prijenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kriptografski kontrolni zbroj
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

TCS_46 **Odgovor na poruku ako se zahtijeva SM-R-ENC-MAC-G1 (prva generacija) / SM-R-ENC-MAC-G2 (druga generacija) i ako je ulazni format za siguran prijenos poruka točan:**

Bajt	Duljina	Vrijednost	Opis
#1	1	'87h'	$T_{PI\ CG}$: oznaka za šifrirane podatke (kriptogram)
#2	L	'MMh' ili '81 MMh'	$L_{PI\ CG}$: duljina uzvraćenih šifriranih podataka (razlikuje se od izvornog Le naredbe zbog popunjenja). L iznosi 2 bajta ako je $L_{PI\ CG}$ > 127 bajtova.
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Šifrirani podatci: indikator popunjenja i kriptogram
#(2+L+MM)	1	'99h'	Oznaka za status obrade (SW1-SW2) – neobvezna za siguran prijenos poruka u prvoj generaciji
#(3+L+MM)	1	'02h'	Duljina statusa obrade
#(4+L+MM) – #(5+L+MM)	2	'XX XXh'	Status obrade nezaštićenog odgovora APDU
#(6+L+MM)	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#(7+L+MM)	1	'XXh'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja '04h' za siguran prijenos poruka u prvoj generaciji (vidjeti Dodatak 11. dio A) '08h', '0Ch' ili '10h' ovisno o duljini AES ključa za siguran prijenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(8+L+MM)-#(7+N+L+MM)	N	'XX..XXh'	Kriptografski kontrolni zbroj
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

Naredba READ BINARY može uzvratiti stanja normalne obrade navedena u TCS_43 pod oznakom '99h' kako je opisano u TCS_59 upotrebom strukture sigurne razmjene poruka odgovora.

Osim toga, mogu se dogoditi i neke pogreške karakteristične za siguran prijenos poruka. U tom se slučaju stanje obrade jednostavno vraća bez uključivanja strukture sigurnog prijenosa poruka.

TCS_47 **Poruka odgovora kod netočnog ulaznog formata za siguran prijenos poruka**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako ne postoji ključ trenutačne sesije, uzvraća se stanje obrade '**6A88**'. To se može dogoditi ako još nije napravljen ključ sesije ili ako je valjanost ključa sesije istekla (u tom slučaju IFD mora ponovo pokrenuti postupak međusobne autentifikacije za postavljanje novog ključa sesije).

— Ako neki očekivani podatkovni objekti (kako su prethodno navedeni) nedostaju u formatu sigurnog prijenosa poruka, uzvraća se stanje obrade '**6987**': do ove pogreške dolazi ako nema očekivane oznake ili ako naredbodavni sadržaj nije pravilno izrađen.

— Ako neki podatkovni objekti nisu točni, uzvraćeno stanje obrade je '**6988**': ova pogreška se događa ako su prisutne sve tražene oznake, ali su neke duljine različite od očekivanih.

— Ako provjera kriptografskog kontrolnog zbroja ne uspije, uzvraćeno stanje obrade je '**6688**'.

3.5.2.2 Naredba s kratkim EF identifikatorom (identifikator elementarne datoteke)

Ovom se varijantom naredbe omogućuje IFD-u da odabere EF putem kratkog EF identifikatora i da očita podatke s tog EF-a.

TCS_48 Tahografska kartica mora podržavati tu varijantu naredbe za sve elementarne datoteke s utvrđenim kratkim EF identifikatorom. Ti su kratki EF identifikatori opisani u poglavlju 4.

TCS_49 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'B0h'	Binarno čitanje
P1	1	'XXh'	Bit 8 postavlja se na 1 Bitovi 7 i 6 postavljaju se na 00 Bit 5 – 1 kodira kratki EF identifikator odgovarajućeg EF-a
P2	1	'XXh'	Kodira pomak s 0 do 255 bajtova u EF-u na koji upućuje P1
Le	1	'XXh'	Očekivana duljina podatka. Broj bajtova koje se očitava.

Napomena: Kratki EF identifikatori koji se upotrebljavaju u aplikaciji tahografa druge generacije utvrđeni su u poglavlju 4.

Ako P1 kodira kratki EF identifikator, a naredba je uspješna, utvrđeni EF postaje trenutačno odabrani EF (trenutačni EF).

TCS_50 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
#1-#L	L	'XX..XXh'	Očitani podatci
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije nađena datoteka koja odgovara kratkom EF identifikatoru, uzvraćeno stanje obrade je '**6A82**'.

— Ako za odabranu datoteku nisu ispunjeni sigurnosni uvjeti, naredba se prekida s '**6982**'.

— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.

— Ako veličina podataka koje treba pročitati ne odgovara veličini EF-a (pomak + Le > veličine EF-a), uzvraćeno stanje obrade je '**6700**' ili '**6Cxx**', pri čemu je 'xx' točna duljina.

— Ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade '**6400**' ili '**6581**'.

— Ako je otkrivena pogreška u integritetu u pohranjenim podatcima, kartica uzvraća tražene podatke, a uzvraćeno stanje obrade je '**6281**'.

3.5.2.3 Naredba s neparnim bajtom instrukcije

Ovom se varijantom naredbe omogućuje IFD-u da očita podatke iz EF-a koji sadržavaju 32 768 ili više bajtova.

TCS_51 Tahografska kartica koja podržava EF-ove s 32 768 ili više bajtova mora podržavati tu varijantu naredbe za te EF-ove. Tahografska kartica može, ali ne mora podržavati tu varijantu naredbe za druge EF-ove, osim za EF Sensor_Installation_Data, vidjeti TCS_156 i TCS_160.

TCS_52 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'B1h'	Binarno čitanje
P1	1	'00h'	Trenutačni EF
P2	1	'00h'	
Lc	1	'NNh'	Lc Duljina pomaka podatkovnog objekta.
#6-#(5+NN)	NN	'XX..XXh'	Pomak podatkovnog objekta: Oznaka '54h' Duljina '01h' ili '02h' Vrijednost pomak
Le	1	'XXh'	Broj bajtova koje se očitava.

IFD kodira duljinu pomaka podatkovnog objekta s najmanjim mogućim brojem okteta, odnosno upotrebom bajta duljine '01h' IFD kodira pomak od 0 do 255, a upotrebom bajta duljine '02h' pomak od '256' do '65 535' bajtova.

TCS_53 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
#1-#L	L	'XX..XXh'	Očitani podatci sažeti su u diskrecijskom podatkovnom objektu s oznakom '53h'.
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije odabran EF, uzvraćeno stanje obrade je '**6986**'.

— Ako za odabranu datoteku nisu ispunjeni sigurnosni uvjeti, naredba se prekida s '**6982**'.

— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.

— Ako veličina podataka koje treba pročitati ne odgovara veličini EF-a (pomak + Le > veličine EF-a), uzvraćeno stanje obrade je '**6700**' ili '**6Cxx**', pri čemu je 'xx' točna duljina.

— Ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade '**6400**' ili '**6581**'.

— Ako je otkrivena pogreška u integritetu u pohranjenim podatcima, kartica uzvraća tražene podatke, a uzvraćeno stanje obrade je '**6281**'.

3.5.2.3.1 Naredba sa sigurnim prijenosom poruke (primjer)

U sljedećem je primjeru prikazana upotreba sigurnog prijenosa poruka ako se primjenjuje sigurnosni uvjet SM-MAC-G2.

TCS_54 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	'0Ch'	Traži se siguran prijenos poruka
INS	1	'B1h'	Binarno čitanje
P1	1	'00h'	Trenutačni EF
P2	1	'00h'	
Lc	1	'XXh'	Duljina polja zaštićenih podataka
#6	1	'B3h'	Oznaka za vrijednost nešifriranih podataka u BER-TLV
#7	1	'NNh'	L_{PV}: duljina poslanih podataka
#(8)-#(7+NN)	NN	'XX..XXh'	Nešifrirani podatci kodirani u BER-TLV, odnosno pomak podatkovnog objekta s oznakom '54'
#(8+NN)	1	'97h'	T_{LE}: Oznaka za očekivanu specifikaciju duljine.
#(9+NN)	1	'01h'	L_{LE}: Duljina očekivane duljine
#(10+NN)	1	'XXh'	Specifikacija očekivane duljine (izvorni Le): broj bajtova koje se očitava
#(11+NN)	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#(12+NN)	1	'XXh'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja '08h', '0Ch' ili '10h' ovisno o duljini AES ključa za siguran prijenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Kriptografski kontrolni zbroj
Le	1	'00h'	Kako je utvrđeno u normi ISO/IEC 7816-4.

TCS_55 Poruka odgovora ako je naredba bila uspješna

Bajt	Duljina	Vrijednost	Opis
#1	1	'B3h'	Nešifrirani podatci kodirani u BER-TLV
#2	L	'NNh' ili '81 NNh'	L_{PV}: duljina uzvraćenih podataka (= izvorni Le). L iznosi 2 bajta ako je L_{PV} > 127 bajtova.
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Vrijednost nešifriranih podataka kodiranih u BER-TLV, odnosno očitani podatci sažeti u diskrecijskom podatkovnom objektu s oznakom '53h'.
#(2+L+NN)	1	'99h'	Status obrade nezaštićenog odgovora APDU
#(3+L+NN)	1	'02h'	Duljina statusa obrade
#(4+L+NN) – #(5+L+NN)	2	'XX XXh'	Status obrade nezaštićenog odgovora APDU
#(6+L+NN)	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#(7+L+NN)	1	'XXh'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja '08h', '0Ch' ili '10h' ovisno o duljini AES ključa za siguran prijenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kriptografski kontrolni zbroj
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

3.5.3 *UPDATE BINARY*

Ova naredba u skladu je s normom ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Poruka naredbe UPDATE BINARY započinje ažuriranjem (brisanje + pisanje) bitova koji su već sadržani u binarnom EF-u, s bitovima danim u naredbi APDU.

3.5.3.1 Naredba s pomakom u P1-P2

Ova naredba omogućuje IFD-u upisivanje podataka u trenutačno odabran EF bez da kartica provjerava integritet primljenih podataka.

Napomena: Ova se naredba bez sigurnog prijenosa poruka može upotrebljavati samo za potrebe ažuriranja datoteke koja podržava ALW sigurnosni uvjet za način pristupa za ažuriranje.

TCS_56 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'D6h'	Binarno ažuriranje

Bajt	Duljina	Vrijednost	Opis
P1	1	'XXh'	Pomak u bajtovima od početka datoteke: najvažniji bajt
P2	1	'XXh'	Pomak u bajtovima od početka datoteke: najmanje važan bajt
Lc	1	'NNh'	Lc Duljina podataka koje se ažurira. broj bajtova koje se upisuje.
#6-#(5+NN)	NN	'XX..XXh'	Podatci koji se zapisuju

Napomena: bit 8 u P1 mora biti postavljen na 0.

TCS_57 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije odabran EF, uzvraćeno stanje obrade je '**6986**'.

— Ako za odabranu datoteku nisu ispunjeni sigurnosni uvjeti, naredba se prekida s '**6982**'.

— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.

— Ako veličina podataka koje treba upisati nije u skladu s veličinom EF-a (pomak + Lc > veličine EF-a), uzvraćeni status obrade je '**6700**'.

— Ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade '**6400**' ili '**6500**'.

— Ako zapisivanje nije uspješno, uzvraćeno stanje obrade je '**6581**'.

3.5.3.1.1 Naredba sa sigurnim prijenosom poruke (primjeri)

Ova naredba omogućuje IFD-u upisivanje podataka u trenutačno odabran EF, a kartica provjerava integritet primljenih podataka. Budući da nije tražena povjerljivost podataka, podatci nisu šifrirani.

TCS_58 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'0Ch'	Traži se siguran prijenos poruka
INS	1	'D6h'	Binarno ažuriranje
P1	1	'XXh'	Pomak u bajtovima od početka datoteke: najvažniji bajt
P2	1	'XXh'	Pomak u bajtovima od početka datoteke: najmanje važan bajt
Lc	1	'XXh'	Duljina polja zaštićenih podataka

Bajt	Duljina	Vrijednost	Opis
#6	1	'81h'	T_{PV}: Oznaka za vrijednost nešifriranih podataka
#7	L	'NNh' ili '81 NNh'	L_{PV}: duljina poslanih podataka. L iznosi 2 bajta ako je L_{PV} > 127 bajtova.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Vrijednost nešifriranih podataka (podatci koje se upisuje)
#(7+L+NN)	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#(8+L+NN)	1	'XXh'	L_{CC}: Duljina sljedećeg kriptografskog kontrolnog zbroja '04h' za siguran prijenos poruka u prvoj generaciji (vidjeti Dodatak 11. dio A) '08h', '0Ch' ili '10h' ovisno o duljini AES ključa za siguran prijenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Kriptografski kontrolni zbroj
Le	1	'00h'	Kako je utvrđeno u normi ISO/IEC 7816-4.

TCS_59 **Poruka odgovora kod točnog ulaznog formata za siguran prijenos poruka**

Bajt	Duljina	Vrijednost	Opis
#1	1	'99h'	T_{SW}: oznaka za statusne riječi (koje treba zaštititi sa CC)
#2	1	'02h'	L_{SV}: duljina uzvraćenih statusnih riječi
#3-#4	2	'XXXXh'	Status obrade nezaštićenog odgovora APDU
#5	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#6	1	'XXh'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja '04h' za siguran prijenos poruka u prvoj generaciji (vidjeti Dodatak 11. dio A) '08h', '0Ch' ili '10h' ovisno o duljini AES ključa za siguran prijenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#7-#(6+L)	L	'XX..XXh'	Kriptografski kontrolni zbroj
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

„Redovna" stanja obrade opisana za naredbu UPDATE BINARY bez sigurnog prijenosa poruka (vidjeti točku 3.5.3.1) mogu se uzvratiti tako da se koristi prethodno opisana struktura poruka odgovora.

Osim toga, mogu se dogoditi i neke pogreške karakteristične za siguran prijenos poruka. U tom se slučaju stanje obrade jednostavno vraća bez uključivanja strukture sigurnog prijenosa poruka:

TCS_60 **Poruka odgovora ako je u sigurnom prijenosu poruka došlo do pogreške**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako ne postoji ključ trenutačne sesije, uzvraća se stanje obrade '**6A88**'.

— Ako neki očekivani podatkovni objekti (kako su prethodno navedeni) nedostaju u formatu sigurnog prijenosa poruka, uzvraća se stanje obrade '**6987**': do ove pogreške dolazi ako nema očekivane oznake ili ako naredbodavni sadržaj nije pravilno izrađen.

— Ako neki podatkovni objekti nisu točni, uzvraćeno stanje obrade je '**6988**': ova pogreška se događa ako su prisutne sve tražene oznake, ali su neke duljine različite od očekivanih.

— Ako provjera kriptografskog kontrolnog zbroja ne uspije, uzvraćeno stanje obrade je '**6688**'.

3.5.3.2 Naredba s kratkim EF identifikatorom

Ovom se varijantom naredbe omogućuje IFD-u da odabere EF putem kratkog EF identifikatora i da upiše podatke s tog EF-a.

TCS_61 Tahografska kartica mora podržavati tu varijantu naredbe za sve elementarne datoteke s utvrđenim kratkim EF identifikatorom. Ti su kratki EF identifikatori opisani u poglavlju 4.

TCS_62 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'D6h'	Binarno ažuriranje
P1	1	'XXh'	Bit 8 postavlja se na 1 Bitovi 7 i 6 postavljaju se na 00 Bit 5 – 1 kodira kratki EF identifikator odgovarajućeg EF-a
P2	1	'XXh'	Kodira pomak s 0 do 255 bajtova u EF-u na koji upućuje P1
Lc	1	'NNh'	Lc Duljina podataka koje se ažurira. broj bajtova koje se upisuje.
#6-#(5+NN)	NN	'XX..XXh'	Podatci koji se zapisuju

TCS_63 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

Napomena: Kratki EF identifikatori koji se upotrebljavaju u aplikaciji tahografa druge generacije utvrđeni su u poglavlju 4.

Ako P1 kodira kratki EF identifikator, a naredba je uspješna, utvrđeni EF postaje trenutačno odabrani EF (trenutačni EF).

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije nađena datoteka koja odgovara kratkom EF identifikatoru, uzvraćeno stanje obrade je '**6A82**'.

— Ako za odabranu datoteku nisu ispunjeni sigurnosni uvjeti, naredba se prekida s '**6982**'.

— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.

— Ako veličina podataka koje treba upisati nije u skladu s veličinom EF-a (pomak + Lc > veličine EF-a), uzvraćeni status obrade je '**6700**'.

— Ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade '**6400**' ili '**6581**'.

— Ako zapisivanje nije uspješno, uzvraćeno stanje obrade je '**6581**'.

3.5.3.3 Naredba s neparnim bajtom instrukcije

Ovom se varijantom naredbe omogućuje IFD-u da upiše podatke u EF koji sadržavaju 32 768 ili više bajtova.

TCS_64 Tahografska kartica koja podržava EF-ove s 32 768 ili više bajtova mora podržavati tu varijantu naredbe za te EF-ove. Tahografska kartica može, ali ne mora podržavati tu varijantu naredbe za druge EF-ove.

TCS_65 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'D7h'	Binarno ažuriranje
P1	1	'00h'	Trenutačni EF
P2	1	'00h'	
Lc	1	'NNh'	Lc Duljina podataka u polju s podatcima naredbe
#6-#(5+NN)	NN	'XX..XXh'	Pomak podatkovnog objekta s oznakom '54h' || Diskrecijski podatkovni objekt s oznakom '53h' koji sažima podatke koje se upisuje

IFD kodira duljinu pomaka podatkovnog objekta i diskrecijskog podatkovnog objekta s najmanjim mogućim brojem okteta, odnosno upotrebom bajta duljine '01h' IFD kodira pomak/duljinu od 0 do 255, a upotrebom bajta duljine '02h' pomak/duljinu od '256' do '65 535' bajtova.

TCS_66 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije odabran EF, uzvraćeno stanje obrade je '**6986**'.

— Ako za odabranu datoteku nisu ispunjeni sigurnosni uvjeti, naredba se prekida s '**6982**'.

— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.

— Ako veličina podataka koje treba upisati nije u skladu s veličinom EF-a (pomak + Lc > veličine EF-a), uzvraćeni status obrade je '**6700**'.

— Ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade '**6400**' ili '**6500**'.

— Ako zapisivanje nije uspješno, uzvraćeno stanje obrade je '**6581**'.

3.5.3.3.1 Naredba sa sigurnim prijenosom poruke (primjer)

U sljedećem je primjeru prikazana upotreba sigurnog prijenosa poruka ako se primjenjuje sigurnosni uvjet SM-MAC-G2.

TCS_67 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	'0Ch'	Traži se siguran prijenos poruka
INS	1	'D7h'	Binarno ažuriranje
P1	1	'00h'	Trenutačni EF
P2	1	'00h'	
Lc	1	'XXh'	Duljina polja zaštićenih podataka
#6	1	'B3h'	Oznaka za vrijednost nešifriranih podataka u BER-TLV
#7	L	'NNh' ili '81 NNh'	L_{PV}: duljina poslanih podataka. L iznosi 2 bajta ako je L_{PV} > 127 bajtova.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Nešifrirani podatci kodirani u BER-TLV, odnosno pomak podatkovnog objekta s oznakom '54h' || Diskrecijski podatkovni objekt s oznakom '53h' koji sažima podatke koje se upisuje
#(7+L+NN)	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#(8+L+NN)	1	'XXh'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja '08h', '0Ch' ili '10h' ovisno o duljini AES ključa za siguran prijenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Kriptografski kontrolni zbroj
Le	1	'00h'	Kako je utvrđeno u normi ISO/IEC 7816-4.

TCS_68 Poruka odgovora ako je naredba bila uspješna

Bajt	Duljina	Vrijednost	Opis
#1	1	'99h'	T_{SW}: oznaka za statusne riječi (koje treba zaštititi sa CC)
#2	1	'02h'	L_{SV}: duljina uzvraćenih statusnih riječi
#3-#4	2	'XXXXh'	Status obrade nezaštićenog odgovora APDU
#5	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj

Bajt	Duljina	Vrijednost	Opis
#6	1	'XXh'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja '08h', '0Ch' ili '10h' ovisno o duljini AES ključa za siguran prijenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#7-#(6+L)	L	'XX..XXh'	Kriptografski kontrolni zbroj
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

3.5.4 *GET CHALLENGE*

Ova naredba u skladu je s normom ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Naredbom GET CHALLENGE se od kartice traži izdavanje zahtjeva za ključnu riječ (tj. *challenge*) radi korištenja u sigurnosnom postupku u kojem se kartici šalju kriptogram ili šifrirani podatci.

TCS_69 Zahtjev za ključnu riječ koji izdaje kartica vrijedi samo za sljedeću naredbu koja upotrebljava zahtjev za lozinku poslan kartici.

TCS_70 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (duljina očekivanog zahtjeva za ključnu riječ).

TCS_71 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
#1-#8	8	'XX..XXh'	Zahtjev za ključnu riječ
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako se Le razlikuje od '08h', stanje obrade je '**6700**'.

— Ako parametri P1-P2 nisu točni, stanje obrade je '**6A86**'.

3.5.5 *VERIFY*

Ova naredba u skladu je s normom ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Kako bi se podržala ta naredba, potrebna je samo kartica radionice.

Druge vrste tahografskih kartica mogu, ali ne moraju izvršavati tu naredbu, ali za njih nije personaliziran referentni CHV. Stoga te kartice ne mogu uspješno izvršiti tu naredbu. Ponašanje drugih vrsta tahografskih kartica koje nisu kartice radionice, odnosno kad se uzvrati kod pogreške, nije u području primjene ove specifikacije ako se šalje ta naredba.

Naredba VERIFY na kartici započinje usporedbu između CHV (PIN) podataka koji su poslani iz naredbe s referentnim CHV-om pohranjenim na kartici.

TCS_72 PIN koji unosi korisnik mora biti kodiran u ASCII i desno popunjen bajtima 'FFh' do duljine od 8 bajtova IFD-a, vidjeti i vrstu podataka WorkshopCardPIN u Dodatku 1.

TCS_73 Aplikacije tahografa prve i druge generacije upotrebljavaju isti referentni CHV.

TCS_74 Tahografskom karticom provjerava se je li naredba ispravno kodirana. Ako naredba nije ispravno kodirana, kartica ne uspoređuje CHV vrijednosti, ne umanjuje stanje brojača preostalih pokušaja CHV-a i ne vraća sigurnosni status „PIN_Verified" u početno stanje, nego prekida naredbu. Naredba je kodirana ispravno ako bajtovi CLA, INS, P1, P2, Lc imaju određene vrijednosti, Le nije prisutan, a polje s podatcima naredbe ispravne je duljine.

TCS_75 Ako je naredba uspješna, brojač preostalih pokušaja CHV-a pokreće se iznova. Početna je vrijednost brojača preostalih pokušaja CHV-a 5. Ako je naredba uspješna, karticom se postavlja status unutarnje sigurnosti „PIN_Verified". Kartica vraća taj sigurnosni status u početno stanje ako je kartica vraćena u početno stanje ili ako CHV kod poslan u naredbi ne odgovara pohranjenom referentnom CHV-u.

Napomena: Upotrebom istog referentnog CHV-a i globalnog sigurnosnog statusa zaposlenik radionice ne mora ponovno unositi PIN nakon što odabere drugi DF aplikacije tahografa.

TCS_76 Neuspješna usporedba bilježi se na kartici, odnosno brojač preostalih pokušaja CHV-a umanjuje se za jedan, kako bi se ograničio broj naknadnih pokušaja upotrebe referentnog CHV-a.

TCS_77 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (provjereni CHV implicitno je poznat)
Lc	1	'08h'	Duljina poslanog koda CHV
#6-#13	8	'XX..XXh'	CHV

TCS_78 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije pronađen referentni CHV, uzvraćeno stanje obrade je '**6A88**'.

— Ako je CHV blokiran (brojač preostalih pokušaja za CHV je nula), uzvraćeno stanje obrade je '**6983**'. Kada se jednom nađe u tom stanju, CHV se više nikada ne može uspješno predočiti.

— Ako je usporedba neuspješna, brojač preostalih pokušaja umanjuje se te se uzvraća status '**63CX**' (X > 0 pri čemu je X brojač preostalih pokušaja CHV-a).

— Ako se referentni CHV smatra neispravnim, uzvraćeno stanje obrade je '**6400**' ili '**6581**'.

— Ako se Lc razlikuje od '08h', stanje obrade je '**6700**'.

3.5.6 *GET RESPONSE*

Ova je naredba u skladu s normom ISO/IEC 7816-4.

Ova naredba (potrebna i dostupna samo za protokol T = 0) se koristi za prijenos pripremljenih podataka s kartice na sučelje tahografa (primjer gdje naredba uključuje i Lc i Le).

Naredba GET RESPONSE mora biti izdana neposredno nakon naredbe za pripremu podataka, inače se podatci gube. Nakon izvršenja naredbe GET RESPONSE (osim ako nastupi pogreška '**61xx**' ili '**6Cxx**', vidjeti u nastavku), ranije pripremljeni podatci više nisu dostupni.

TCS_79 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Broj bajtova koji se očekuje

TCS_80 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
#1-#X	X	'XX..XXh'	Podatci
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako kartica nije pripremila nikakve podatke, uzvraćeno stanje obrade je '**6900**' ili '**6F00**'.

— Ako Le prelazi broj raspoloživih bajtova ili ako je Le nula, uzvraćeno stanje obrade je '**6Cxx**', pri čemu 'xx' označuje točan broj raspoloživih bajtova. U tom su slučaju pripremljeni podatci još uvijek dostupni za iduću naredbu GET RESPONSE.

— Ako Le nije nula, a manji je od broja raspoloživih bajtova, kartica normalno šalje tražene podatke, a uzvraćeno stanje obrade je '**61xx**', pri čemu 'xx' označuje broj dodatnih bajtova koji su još uvijek raspoloživi za iduću naredbu GET RESPONSE.

— Ako naredba nije podržana (protokol T = 1), kartica uzvraća '**6D00**'.

3.5.7 *PSO: VERIFY CERTIFICATE*

Ova naredba u skladu je s normom ISO/IEC 7816-8, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Naredbu VERIFY CERTIFICATE kartica koristi za dobivanje izvanjskog javnog ključa i provjeru njegove valjanosti.

3.5.7.1 Naredba za prvu generaciju – par odgovora

TCS_81 Ovu varijantu naredbe podržavaju samo aplikacije tahografa prve generacije.

TCS_82 Ako je naredba VERIFY CERTIFICATE uspješna, javni ključ se pohranjuje za buduću uporabu u sigurno okruženje. Ovaj se ključ izričito postavlja za primjenu u sigurnosnim naredbama (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE ili VERIFY CERTIFICATE) upotrebom MSE naredbe (vidjeti točku 3.5.11) s pomoću identifikatora ključa.

TCS_83 U svakom slučaju, naredba VERIFY CERTIFICATE upotrebljava javni ključ koji je ranije odabran u sklopu MSE naredbe za otvaranje certifikata. Ovaj javni ključ mora biti onaj države članice ili europski.

TCS_84 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'2Ah'	Izvedba sigurnosne operacije
P1	1	'00h'	P1
P2	1	'AEh'	P2: podatci koji nisu kodirani po BER-TLV (ulančavanje podatkovnih elemenata)
Lc	1	'C2h'	Lc Duljina certifikata, 194 bajta
#6-#199	194	'XX..XXh'	Certifikat: ulančavanje podatkovnih elemenata (opisano u Dodatku 11.)

TCS_85 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako provjera certifikata ne uspije, uzvraćeno stanje obrade je '**6688**'. Postupak provjere i otvaranja certifikata opisan je u Dodatku 11. za prvu i drugu generaciju.

— Ako u sigurnosnom okruženju nije prisutan javni ključ, uzvraća se stanje obrade '**6A88**'.

— Ako se odabrani javni ključ (upotrijebljen za otvaranje certifikata) smatra oštećenim, uzvraćeno stanje obrade je '**6400**' ili '**6581**'.

— Samo za prvu generaciju: Ako je CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) odabranog javnog ključa (upotrijebljen za otvaranje certifikata) različit od '00' (odnosno ne pripada državi članici niti je europski), uzvraćeno je stanje obrade '**6985**'.

3.5.7.2 Naredba za drugu generaciju – par odgovora

Ovisno o veličini krivulje, ECC certifikati mogu biti toliko dugački da ih je nemoguće prenijeti u jednom APDU-u. U tom se slučaju mora upotrijebiti ulančavanje naredbi u skladu s normom ISO/IEC 7816-4 te prenijeti certifikat u dvama uzastopnim PSO-ima: Provjera certifikata APDU-ova.

Struktura certifikata i parametri domene definirani su u Dodatku 11.

TCS_86 Naredbu je moguće izvršiti u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_33.

TCS_87 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'X0h'	CLA bajt označuje ulančavanje naredbi: '00h' jedina ili zadnja naredba u lancu '10h' nije zadnja naredba u lancu
INS	1	'2Ah'	Izvedba sigurnosne operacije
P1	1	'00h'	
P2	1	'BEh'	Provjera samoopisnog certifikata
Lc	1	'XXh'	Duljina podatkovnog polja naredbe, vidjeti TCS_88 i TCS_89.
#6-#5+L	L	'XX..XXh'	DER-TLV kodirani podatci: Podatkovni objekt tijela ECC certifikata kao prvi podatkovni objekt ulančan s podatkovnim objektom potpisa ECC certifikata kao drugim podatkovnim objektom ili dijelom tog lanca. Oznaka '7F21' i odgovarajuća duljina ne šalju se. Redoslijed je tih objekata utvrđen.

TCS_88 Za kratke APDU-ove primjenjuju se sljedeće odredbe: IFD upotrebljava najmanji broj APDU-ova potreban za slanje naredbe i šalje najveći mogući broj bajtova u prvoj naredbi APDU-a u skladu s vrijednošću bajta veličine informacijskog polja na kartici, vidjeti TCS_14. Ako se IFD drukčije ponaša, ponašanje kartice nalazi se izvan područja primjene.

TCS_89 Za produljene APDU-ove primjenjuju se sljedeće odredbe: Ako certifikat ne stane u jedan APDU, kartica mora podržavati ulančavanje naredbi. IFD upotrebljava najmanji broj APDU-ova potreban za slanje naredbe i šalje najveći mogući broj bajtova u prvoj naredbi APDU-a. Ako se IFD drukčije ponaša, ponašanje kartice nalazi se izvan područja primjene.

Napomena: U skladu s Dodatkom 11., kartica pohranjuje certifikat ili relevantan sadržaj certifikata te ažurira currentAuthenicatedTime.

Struktura poruka odgovora i statusnih riječi odgovara definiciji iz TCS_85.

TCS_90 Uz kodove pogrešaka navedene u TCS_85, kartica može uzvratiti sljedeće kodove pogrešaka:

— Ako CHA.LSB (CertificateHolderAuthorisation.equipmentType) odabranog javnog ključa (upotrijebljenog za otvaranje certifikata) nije prikladan za provjeru certifikata u skladu s Dodatkom 11., uzvraćeno je stanje obrade '**6985**'.

— Ako je currentAuthenticatedTime kasniji od datuma isteka certifikata, uzvraćeno je stanje obrade '**6985**'.

— Ako je zadnja naredba u lancu očekivana, kartica uzvraća '**6883**'.

— Ako se u polju s podatcima naredbe šalju neispravni parametri, kartica uzvraća '**6A80**' (isto vrijedi i u slučaju da podatkovni objekti nisu poslani utvrđenim redoslijedom).

3.5.8 *INTERNAL AUTHENTICATE*

Ova je naredba u skladu s normom ISO/IEC 7816-4.

TCS_91 Sve tahografske kartice moraju podržavati tu naredbu u DF-u tahografa prve generacije. Naredba može, ali ne mora biti dostupna u MF-u i/ili DF-u tahografa druge generacije. Ako je tako, izvršavanje naredbe završava odgovarajućim kodom pogreške jer je privatni ključ kartice (Card.SK) za protokol autentifikacije za prvu generaciju dostupan samo u DF-u tahografa prve generacije.

Primjenom INTERNAL AUTHENTICATE naredbe, IFD može autentificirati karticu. Postupak autentifikacije je opisan je u Dodatku 11. Sadržava sljedeća očitovanja:

TCS_92 Naredba INTERNAL AUTHENTICATE upotrebljava privatni ključ kartice (odabran implicitno) za potpisivanje autentifikacijskih podataka, uključujući K1 (prvi element za dogovor o ključu sesije) i RND1 te upotrebljava trenutačno (putem posljednje naredbe MSE) odabrani javni ključ za šifriranje potpisa i oblikovanje autentifikacijskog tokena (podrobnije u Dodatku 11.).

TCS_93 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Duljina podataka poslanih na karticu
#6 – #13	8	'XX..XXh'	Zahtjev za ključnu riječ upotrijebljen za autentifikaciju kartice
#14 -#21	8	'XX..XXh'	VU.CHR (vidjeti Dodatak 11.)
Le	1	'80h'	Duljina podataka koji se očekuju od kartice

TCS_94 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
#1-#128	128	'XX..XXh'	Token autentifikacije kartice (vidjeti Dodatak 11.)
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako u sigurnosnom okruženju nije prisutan javni ključ, uzvraćeno je stanje obrade '**6A88**'.

— Ako u sigurnosnom okruženju nije prisutan privatan ključ, uzvraćeno je stanje obrade '**6A88**'.

— Ako VU.CHR ne odgovara identifikatoru trenutačnog javnog ključa, uzvraćeno je stanje obrade '**6A88**'.

— Ako se odabrani privatni ključ smatra neispravnim, uzvraćeno je stanje obrade '**6400**' ili '**6581**'.

TCS_95 Ako je naredba INTERNAL AUTHENTICATE uspješna, trenutačni ključ sesije, ako postoji, briše se i više nije dostupan. Da bi se dobio novi ključ sesije, naredba EXTERNAL AUTHENTICATE za autentifikaciju mehanizma prve generacije treba biti uspješno izvršena.

3.5.9 *EXTERNAL AUTHENTICATE*

Ova je naredba u skladu s normom ISO/IEC 7816-4.

Kartica naredbom EXTERNAL AUTHENTICATE može autentificirati IFD. Postupak autentifikacije opisan je u Dodatku 11. za tahografe prve i druge generacije (autentifikacija jedinice u vozilu).

TCS_96 Varijantu naredbe za mehanizam uzajamne autentifikacije prve generacije podržavaju samo aplikacije tahografa prve generacije.

TCS_97 Varijantu naredbe za uzajamnu autentifikaciju kartice i jedinice u vozilu moguće je izvesti samo u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_34.

TCS_98 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Implicitno poznati ključevi i algoritmi
P2	1	'00h'	
Lc	1	'XXh'	Lc (duljina podataka poslanih na karticu)
#6-#(5+L)	L	'XX..XXh'	Autentifikacija prve generacije: Kriptogram (vidjeti Dodatak 11. dio A) Autentifikacija druge generacije: Potpis koji je generirao IFD (vidjeti Dodatak 11. dio B)

TCS_99 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako CHA trenutačno postavljenog javnog ključa nije lanac AID-a aplikacije tahografa i vrste jedinice u vozilu, uzvraćeno je stanje obrade '**6F00**'.

— Ako neposredno prije naredbe nema naredbe GET CHALLENGE, uzvraćeno je stanje obrade '**6985**'.

Aplikacija tahografa prve generacije može uzvratiti sljedeće dodatne kodove pogrešaka:

— Ako u sigurnosnom okruženju nije prisutan javni ključ, uzvraća se stanje obrade '**6A88**'.

— Ako u sigurnosnom okruženju nije prisutan privatan ključ, uzvraćeno je stanje obrade '**6A88**'.

— Ako je provjera kriptograma pogrešna, uzvraćeno stanje obrade je '**6688**'.

— Ako se odabrani privatni ključ smatra neispravnim, uzvraćeno je stanje obrade '**6400**' ili '**6581**'.

Varijanta naredbe za autentifikaciju druge generacije može uzvratiti sljedeći dodatni kod pogreške:

— Ako je provjera potpisa neuspjela, kartica uzvraća '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Ova se naredba upotrebljava za protokol autentifikacije čipa druge generacije utvrđen u Dodatku 11. dijelu B te je u skladu s normom ISO/IEC 7816-4.

TCS_100 Naredbu je moguće izvršiti u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_34.

TCS_101 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Implicitno poznati ključevi i protokol
P2	1	'00h'	
Lc	1	'NNh'	Lc: duljina sljedećeg podatkovnog polja
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	DER-TLV kodirana vrijednost kratkotrajnog (ephemeral) javnog ključa (vidjeti Dodatak 11.) Jedinica u vozilu šalje podatkovne objekte tim redoslijedom.

TCS_102 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	DER-TLV kodirani podatci dinamičke autentifikacije: *nonce* (broj koji se koristi jednom) i token autentifikacije (vidjeti Dodatak 11.)
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Kartica uzvraća '**6A80**' kako bi se ukazalo na neispravne parametre u podatkovnom polju.

— Kartica uzvraća '**6982**' ako naredba External Authenticate nije uspješno provedena

Objekt odgovora dinamičke autentifikacije podataka '7Ch'

— mora biti prisutan ako je operacija uspješna, odnosno ako su statusne riječi '**9000**',

— ne smije biti prisutan u slučaju pogreške u izvršavanju ili pogreške provjere, odnosno ako su statusne riječi u rasponu od '**6400**' do '**6FFF**' te

— ne mora biti prisutan u slučaju upozorenja, odnosno ako su statusne riječi u rasponu od '**6200**' do '**63FF**'.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Ova se naredba koristi za postavljanje javnoga ključa za potrebe autentifikacije.

3.5.11.1 Naredba za prvu generaciju – par odgovora

Ova je naredba u skladu s normom ISO/IEC 7816-4. Primjena ove naredbe ograničena je u usporedbi s odgovarajućom normom.

TCS_103 Ovu naredbu podržavaju samo aplikacije tahografa prve generacije.

TCS_104 Ključ naveden u podatkovnom polju MSE ostaje trenutačni javni ključ do sljedeće ispravne naredbe MSE, odabire se DF ili se kartica vraća u početno stanje.

TCS_105 Ako navedeni ključ (već) nije na kartici, sigurno okruženje ostaje nepromijenjeno.

TCS_106 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: navedeni ključ vrijedi za sve kriptografske radnje
P2	1	'B6h'	P2 (navedeni podatci o digitalnom potpisu)
Lc	1	'0Ah'	Lc: duljina sljedećeg podatkovnog polja
#6	1	'83h'	Oznaka za navođenje javnog ključa u asimetričnim slučajevima
#7	1	'08h'	Duljina reference ključa (identifikatora ključa)
#8-#15	8	'XX..XXh'	Identifikator ključa kako je utvrđen u Dodatku 11.

TCS_107 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako u kartici nema navedenog ključa, uzvraćeno je stanje obrade '**6A88**'.

— Ako u formatu sigurnog prijenosa poruka nedostaju neki očekivani podatkovni objekti, uzvraćeno je stanje obrade '**6987**'. To se može dogoditi ako nema oznake '83h',

— Ako su određeni podatkovni objekti neispravni, uzvraćeno je stanje obrade '**6988**'. To se može dogoditi ako duljina identifikatora ključa nije '08h'.

— Ako se odabrani ključ smatra neispravnim, uzvraćeno je stanje obrade '**6400**' ili '**6581**'.

3.5.11.2 Naredba za drugu generaciju – parovi odgovora

Za autentifikaciju druge generacije tahografska kartica podržava sljedeći MSE: Utvrđene verzije naredbe koje su u skladu s normom ISO/IEC 7816-4. Te verzije naredbe nisu podržane u autentifikaciji prve generacije.

3.5.11.2.1 MSE:SET AT za autentifikaciju čipa

Sljedeća se MSE:SET AT naredba upotrebljava za odabir parametara za autentifikaciju čipa koja se provodi naknadnom naredbom GENERAL AUTHENTICATE (opća autentifikacija).

TCS_108 Naredbu je moguće izvršiti u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_34.

TCS_109 **MSE:SET AT Poruka naredbe za autentifikaciju čipa**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'22h'	

Bajt	Duljina	Vrijednost	Opis
P1	1	'41h'	Utvrđeno za unutarnju autentifikaciju
P2	1	'A4h'	Autentifikacija
Lc	1	'NNh'	Lc: duljina sljedećeg podatkovnog polja
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	DER-TLV kodirano upućivanje na kriptografski mehanizam: Identifikator objekta ili autentifikacija čipa (samo vrijednost, izostavlja se oznaka '06h'). Vidjeti Dodatak 1. za vrijednosti identifikatora objekta; upotrebljava se zapis u bajtovima (*byte notation*). Vidjeti Dodatak 11. za smjernice u pogledu odabira jednog od tih identifikatora objekta.

3.5.11.2.2 MSE:SET AT za autentifikaciju jedinice u vozilu

Sljedeća se MSE:SET AT naredba upotrebljava za odabir parametara i ključeva za autentifikaciju jedinice u vozilu koja se provodi naknadnom naredbom EXTERNAL AUTHENTICATE (vanjska autentifikacija).

TCS_110 Naredbu je moguće izvršiti u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_34.

TCS_111 **Poruka naredbe MSE:SET AT za autentifikaciju jedinice u vozilu**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Utvrđeno za vanjsku autentifikaciju
P2	1	'A4h'	Autentifikacija
Lc	1	'NNh'	Lc: duljina sljedećeg podatkovnog polja
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	DER-TLV kodirano upućivanje na kriptografski mehanizam: Identifikator objekta ili autentifikacija jedinice u vozilu (samo vrijednost, izostavlja se oznaka '06h'). Vidjeti Dodatak 1. za vrijednosti identifikatora objekta; upotrebljava se zapis u bajtovima (*byte notation*). Vidjeti Dodatak 11. za smjernice u pogledu odabira jednog od tih identifikatora objekta.
		'83h' + '08h' + 'XX..XXh'	DER-TLV kodirano upućivanje javnog ključa jedinice u vozilu upućivanjem na nositelja certifikata koje je spomenuto u njegovu certifikatu.
		'91h' + L_{91} + 'XX..XXh'	DER-TLV kodiran komprimirani prikaz kratkotrajnog javnog ključa jedinice u vozilu koji će se upotrebljavati tijekom autentifikacije čipa (vidjeti Dodatak 11.)

3.5.11.2.3 MSE:SET DST

Sljedeća se MSE:SET DST naredba upotrebljava za postavljanje javnog ključa bilo

— za provjeru potpisa koji je dobiven u naknadnoj naredbi PSO: Verify Digital Signature ili

— za provjeru potpisa certifikata koji je dobiven u naknadnoj naredbi PSO: Verify Certificate.

TCS_112 Naredbu je moguće izvršiti u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_33.

TCS_113 **Poruka naredbe MSE:SET:DST**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Utvrđeno za provjeru
P2	1	'B6h'	Digitalni potpis
Lc	1	'NNh'	Lc: duljina sljedećeg podatkovnog polja
#6-#(5+L)	L	'83h' + '08h' + 'XX…XXh'	DER-TLV kodirano upućivanje javnog ključa, odnosno upućivanje na nositelja certifikata u certifikatu javnog ključa (vidjeti Dodatak 11.)

Za sve verzije naredbi struktura odgovora na poruku i statusne riječi navedene su sljedećim:

TCS_114 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'. Protokol je odabran i pokrenut.

— '**6A80**' označuje neispravne parametre u podatkovnom polju naredbe.

— '**6A88**' označuje da navedeni podatci (odnosno navedeni ključ) nisu dostupni.

3.5.12 *PSO: HASH*

Ova naredba služi za prijenos rezultata izračuna raspršivanja izvršenim na nekim podacima na karticu. Ova se naredba upotrebljava za provjeru digitalnog potpisa. Vrijednost raspršivanja privremeno se pohranjuje za sljedeću naredbu PSO: Verify Digital Signature

Ova je naredba u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe ograničena je u usporedbi s odgovarajućom normom.

Da bi DF-ovi tahografa i DF-ovi tahografa druge generacije mogli podržati tu naredbu potrebna je samo kontrolna kartica.

Druge vrste tahografskih kartica mogu, ali ne moraju provoditi tu naredbu. Naredba može, ali ne mora biti dostupna u MF-u.

Aplikacija kontrolne kartice prve generacije podržava samo SHA-1.

TCS_115 Privremeno pohranjena vrijednost raspršivanja briše se ako je nova vrijednost raspršivanja izračunana naredbom PSO: HASH, ako je odabran DF i ako je tahografska kartica vraćena u početno stanje.

TCS_116 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Izvedba sigurnosne operacije
P1	1	'90h'	Vraćanje koda raspršivanja (*hash code*)
P2	1	'A0h'	Oznaka; podatkovno polje sadržava DO-ove potrebne za raspršivanje
Lc	1	'XXh'	Duljina Lc sljedećeg podatkovnog polja
#6	1	'90h'	Oznaka za kod raspršivanja
#7	1	'XXh'	Duljina L koda raspršivanja: '14h' u aplikaciji prve generacije (vidjeti Dodatak 11. dio A) '20h', '30h' ili '40h' u aplikaciji druge generacije (vidjeti Dodatak 11. dio B)
#8-#(7+L)	L	'XX..XXh'	Kod raspršivanja (*hash code*)

TCS_117 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nedostaju neki očekivani podatkovni objekti (kako su prethodno navedeni), uzvraćeno je stanje obrade '**6987**'. To se može dogoditi ako nema jedne od oznaka '90h',

— Ako su određeni podatkovni objekti neispravni, uzvraćeno je stanje obrade '**6988**'. Do te pogreške dolazi ako je potrebna oznaka prisutna, ali joj se duljina razlikuje od '14h' za SHA-1, '20h' za SHA-256, '30h' za SHA-384, '40h' za SHA-512 (aplikacije druge generacije).

3.5.13 *PERFORM HASH of FILE*

Ova naredba nije u skladu s ISO/IEC 7816-8. Stoga bajt CLA ove naredbe ukazuje na to da slijedi vlasnička uporaba funkcije PERFORM SECURITY OPERATION / HASH.

Da bi DF-ovi tahografa i DF-ovi tahografa druge generacije mogli podržati tu naredbu potrebne su samo kartica vozača i kartica radionice.

Druge vrste tahografskih kartica mogu, ali ne moraju provoditi tu naredbu. Ako ovu naredbu provodi kartica poduzeća ili kontrolna kartica, naredbu se provodi kako je navedeno u ovome poglavlju.

Naredba može, ali ne mora biti dostupna u MF-u. Ako je tako, naredba se izvršava kako je navedeno u ovome poglavlju, odnosno ne dopušta se izračun vrijednosti raspršivanja, nego se izvršavanje naredbe završava odgovarajućim kodom pogreške.

TCS_118 Naredba PERFORM HASH OF FILE upotrebljava se za raspršivanje podatkovnog područja trenutačno odabranog transparentnog EF-a.

TCS_119 Tahografska kartica mora podržavati ovu naredbu samo za EF-ove navedene u poglavlju 4. pod DF_Tachograph i DF_Tachograph_G2, uz sljedeću iznimku. Tahografska kartica ne podržava naredbu za EF Sensor_Installation_Data u DF-u tahografa druge generacije.

TCS_120 Rezultat operacije raspršivanja privremeno se pohranjuje na kartici. Zatim ga se može upotrijebiti za dobivanje digitalnog potpisa datoteke upotrebom naredbe PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Privremeno pohranjena vrijednost raspršivanja datoteke briše se ako je nova vrijednost raspršivanja datoteke izračunana naredbom PSO: Hash of File, ako je odabran DF i ako je tahografska kartica vraćena u početno stanje.

TCS_122 Aplikacija tahografa prve generacije mora podržavati SHA-1.

TCS_123 Aplikacija tahografa druge generacije mora podržavati SHA-1 i SHA-2 (256, 384 i 512 bitova).

TCS_124 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'80h'	CLA
INS	1	'2Ah'	Izvedba sigurnosne operacije
P1	1	'90h'	Oznaka: Hash
P2	1	'XXh'	P2: Ukazuje na algoritam koji je potrebno upotrebljavati za raspršivanje podataka trenutačno odabrane transparentne datoteke: '00h' za 'SHA-1' '01h' za 'SHA-256' '02h' za 'SHA-384' '03h' za 'SHA-512'

TCS_125 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako trenutačni EF ne dopušta tu naredbu (EF Sensor_Installation_Data u DF-u tahografa druge generacije), uzvraćeno je stanje obrade '**6985**'.

— Ako se odabrani EF smatra neispravnim (u atributima datoteke ili pohranjenim podatcima otkrivena je pogreška u integritetu), uzvraćeno je stanje obrade '**6400**' ili '**6581**'.

— Ako odabrana datoteka nije transparentna datoteka ili ako nema trenutačnog EF, uzvraćeno je stanje obrade '**6986**'.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Ova se naredba upotrebljava za izračun digitalnog potpisa prethodno izračunanog koda raspršivanja (vidjeti PERFORM HASH OF FILE, točka 3.5.13.).

Da bi DF-ovi tahografa i DF-ovi tahografa druge generacije mogli podržati tu naredbu potrebne su samo kartica vozača i kartica radionice.

Druge vrste tahografskih kartica mogu, ali ne moraju izvršavati tu naredbu, ali ne smiju imati ključ potpisa. Stoga te kartice ne mogu tu naredbu provesti uspješno, nego izbacuju odgovarajući kod pogreške.

Naredba može, ali ne mora biti dostupna u MF-u. Ako je tako, izvršavanje naredbe završava odgovarajućim kodom pogreške.

Ova je naredba u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe ograničena je u usporedbi s odgovarajućom normom.

TCS_126 Tom se naredbom ne izračunava digitalni potpis prethodno izračunanog koda raspršivanja putem naredbe PSO: HASH.

TCS_127 Za izračun digitalnog potpisa upotrebljava se privatni ključ kartice koji je kartici implicitno poznat.

TCS_128 Aplikacije tahografa prve generacije izvršavaju digitalni potpis upotrebom metode popunjavanja koja je u skladu s PKCS1 (za više pojedinosti vidjeti Dodatak 11.).

TCS_129 Aplikacije tahografa druge generacije izračunavaju digitalni potpis na temelju eliptičke krivulje (za više pojedinosti vidjeti Dodatak 11.).

TCS_130 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Izvedba sigurnosne operacije
P1	1	'9Eh'	Digitalni potpis koji treba uzvratiti
P2	1	'9Ah'	Oznaka: podatkovno polje sadržava podatke koje treba potpisati. Ako nije obuhvaćeno podatkovno polje, pretpostavlja se da su podatci već na kartici (raspršivanje datoteke).
Le	1	'NNh'	Duljina očekivanog potpisa

TCS_131 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
#1-#L	L	'XX..XXh'	Potpis prethodno izračunanog raspršivanja
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako se implicitno odabrani privatni ključ smatra neispravnim, uzvraćeno je stanje obrade '**6400**' ili '**6581**'.

— Ako raspršivanje izračunano prethodnom naredbom PERFORM HASH of File nije dostupno, uzvraćeno je stanje obrade '**6985**'.

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Ova se naredba upotrebljava za provjeru digitalnog potpisa koji se pruža kao ulazni podatak čije je raspršivanje poznato kartici. Kartica implicitno poznaje algoritam potpisa.

Ova je naredba u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe ograničena je u usporedbi s odgovarajućom normom.

Da bi DF-ovi tahografa i DF-ovi tahografa druge generacije mogli podržati tu naredbu potrebna je samo kontrolna kartica.

Druge vrste tahografskih kartica mogu, ali ne moraju provoditi tu naredbu. Naredba može, ali ne mora biti dostupna u MF-u.

TCS_132 Naredba VERIFY DIGITAL SIGNATURE uvijek upotrebljava javni ključ odabran prethodnom naredbom Manage Security Environment, MSE: SET DST i prethodnim kodom raspršivanja unesenim s pomoću naredbe PSO: HASH.

TCS_133 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Izvedba sigurnosne operacije
P1	1	'00h'	
P2	1	'A8h'	Oznaka: podatkovno polje sadržava DO-ove potrebne za provjeru
Lc	1	'83h'	Duljina Lc sljedećeg podatkovnog polja
6	1	'9Eh'	Oznaka za digitalni potpis
#7-#8	2	'81 XXh'	Duljina digitalnog potpisa: 128 bajtova kodiranih u skladu s Dodatkom 11. dijelom A u pogledu aplikacije tahografa prve generacije. Za aplikacije tahografa druge generacije duljina ovisi o odabranoj krivulji (vidjeti Dodatak 11. dio B)
#9-#(8+L)	L	'XX..XXh'	Sadržaj digitalnog potpisa

TCS_134 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako provjera potpisa ne uspije, uzvraćeno je stanje obrade '**6688**'. Postupak provjeravanja opisan je u Dodatku 11.

— Ako nije odabran javni ključ, uzvraćeno je stanje obrade '**6A88**'.

— Ako nedostaju neki očekivani podatkovni objekti (kako su prethodno navedeni), uzvraćeno je stanje obrade '**6987**'. To se može dogoditi ako nema jedne od traženih oznaka.

— Ako kod raspršivanja nije dostupan za obradu naredbe (zbog prethodne naredbe PSO: Hash), uzvraćeno je stanje obrade '**6985**'.

— Ako su određeni podatkovni objekti neispravni, uzvraćeno je stanje obrade '**6988**'. To se može dogoditi ako je duljina traženih podatkovnih objekata neispravna.

— Ako se odabrani javni ključ smatra neispravnim, uzvraćeno je stanje obrade '**6400**' ili '**6581**'.

3.5.16 *PROCESS DSRC MESSAGE*

Ova se naredba upotrebljava za provjeru integriteta i autentičnosti DSRC poruke i dešifriranje podataka poslanih s jedinice u vozilu nadzornom tijelu ili radionici putem DSRC poveznice. Kartica proizvodi ključ za šifriranje i MAC ključ koji se upotrebljavaju za zaštitu DSRC poruke kako je opisano u poglavlju 13. Dodatka 11. dijela B.

Da bi DF-ovi tahografa druge generacije mogli podržati tu naredbu potrebne su samo kontrolna kartica i kartica radionice.

Druge vrste tahografskih kartica mogu, ali ne moraju izvršavati tu naredbu, ali te kartice ne smiju imati DSRC glavni ključ. Stoga te kartice ne mogu tu naredbu provesti uspješno, nego izbacuju odgovarajući kod pogreške.

Naredba može, ali ne mora biti dostupna u MF-u i/ili DF-u tahografa. Ako je tako, izvršavanje naredbe završava odgovarajućim kodom pogreške.

TCS_135 DSRC glavni ključ dostupan je samo u DF-u tahografa druge generacije, tj. kontrolna kartica i kartica radionice podržavaju uspješnu provedbu naredbe samo u DF-u tahografa druge generacije.

TCS_136 Naredbom se samo dešifriraju DSRC podatci i provjerava kriptografski kontrolni zbroj, ali se ne tumače ulazni podatci.

TCS_137 Redoslijed podatkovnih objekata u podatkovnom polju naredbe utvrđen je u ovoj specifikaciji.

TCS_138 **Poruka naredbe**

Bajt	Duljina	Vrijednost	Opis
CLA	1	'80h'	Vlasnički CLA
INS	1	'2Ah'	Izvedba sigurnosne operacije
P1	1	'80h'	Podatci odziva: nešifrirana vrijednost
P2	1	'B0h'	Podatci naredbe: nešifrirana vrijednost kodirana u BER-TLV i uključujući DO-ove sigurnog prijenosa poruka
Lc	1	'NNh'	Duljina Lc sljedećeg podatkovnog polja
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	DER-TLV kodirani bajt indikatora popunjenja-sadržaja nakon kojeg slijedi kodirani prijenos podataka tahografa. Za bajt indikatora popunjenja-sadržaja upotrebljava se vrijednost '00h' ('bez dodatnih indikatora' u skladu s normom ISO/IEC 7816-4:2013, tablica 52.). Mehanizam šifriranja opisan je u Dodatku 11. dijelu B. poglavlju 13. Dopuštene su vrijednosti za duljinu L_{87} višekratnici duljine AES bloka uvećano za 1 za bajt indikatora popunjenja-sadržaja, odnosno od 17 bajtova do 193 bajta, uključivo. *Napomena:* Za SM podatkovni objekt s oznakom '87h' vidjeti normu ISO/IEC 7816-4:2013, tablicu 49.
		'81h' + '10h'	DER-TLV kodirani kontrolni referentni predložak za povjerljivost koji ugniježđuje ulančavanje sljedećih podatkovnih elemenata (vidjeti Dodatak 1. DSRCSecurityData i poglavlje 13. Dodatka 11. dijela B): — vremenski žig od 4 bajta — brojač od 3 bajta — serijski broj jedinice u vozilu od 8 bajtova — verzija DSRC glavnog ključa od 1 bajta *Napomena:* Za SM podatkovni objekt s oznakom '81h' vidjeti normu ISO/IEC 7816-4:2013, tablicu 49.
		'8Eh' + L_{8E} + 'XX..XXh'	DER-TLV kodiran MAC putem DSRC poruke. Za MAC algoritam i izračun vidjeti poglavlje 13. Dodatka 11. dijela B. *Napomena:* Za SM podatkovni objekt s oznakom '8Eh' vidjeti normu ISO/IEC 7816-4:2013, tablicu 49.

TCS_139 **Odgovor na poruku**

Bajt	Duljina	Vrijednost	Opis
#1-#L	L	'XX..XXh'	Podatci kojih nema (u slučaju pogreške) ili dešifrirani podatci (uklonjeno popunjavanje)
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— '**6A80**' označuje neispravne parametre u podatkovnom polju naredbe (isto vrijedi i u slučaju da podatkovni objekti nisu poslani utvrđenim redoslijedom).

— '**6A88**' označuje da navedeni podatci nisu dostupni, odnosno da navedeni DSRC glavni ključ nije dostupan.

— '**6900**' označuje da je provjera kriptografskog kontrolnog zbroja ili dešifriranje podataka bilo neuspješno.

4. STRUKTURA KARTICA TAHOGRAFA

Ovaj stavak propisuje strukture datoteka tahografskih kartica za pohranjivanje dostupnih podataka.

Ne propisuje unutarnje strukture koje ovise o proizvođaču kartice, npr. zaglavlja datoteke, ni pohranjivanje podatkovnih elemenata potrebnih samo za internu uporabu, primjerice `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` ili `WorkshopCardPin`. kao ni postupanje s tim elementima.

TCS_140 Na tahografskoj kartici druge generacije nalazi se glavna datoteka MF te aplikacija tahografa prve i druge generacije iste vrste (npr. aplikacije za kartice vozača).

TCS_141 Tahografska kartica mora podržavati barem najmanji broj zapisa utvrđen za odgovarajuće aplikacije, a ne podržava više zapisa od najvećeg broja zapisa utvrđenog za odgovarajuće aplikacije.

U ovome poglavlju utvrđeni su najveći i najmanji brojevi zapisa za različite aplikacije.

Sigurnosni uvjeti koji se upotrebljavaju u uvjetima pristupa u cijelom ovom poglavlju navedeni su u poglavlju 3.3. Općenito, način pristupa „read" (očitavanje) označuje naredbu READ BINARY s parnim i, ako je podržan, neparnim INS bajtom, uz iznimku EF-a Sensor_Installation_Data na kartici radionice, vidjeti TCS_156 i TCS_160. Način pristupa „update" (ažuriranje) označuje naredbu UPDATE BINARY s parnim i, ako je podržan, neparnim INS bajtom, a način pristupa „select" (odabir) naredbu SELECT.

4.1. **Glavna datoteka MF**

TCS_142 Glavna datoteka MF nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uvjete za pristup datotekama:

Napomena: SFID kratkog EF indikatora navodi se kao decimalni broj, na primjer vrijednost 30 odgovara vrijednosti 11110 u binarnom zapisu.

			Uvjeti pristupa	
Datoteka	**ID datoteke**	**SFID**	**Čitanje / Odabir**	**Ažuriranje**
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	

U ovoj se tablici upotrebljava sljedeća kratica za sigurnosni uvjet:

SC1 ALW ILI SM-MAC-G2

TCS_143 Strukture svih EF-ova moraju biti transparentne.

TCS_144 Glavna datoteka MF ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	Zadane vrijednosti
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 Osnovna datoteka EF DIR sadržava sljedeće podatkovne objekte vezane uz aplikaciju. ‘61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54’

TCS_146 Osnovna datoteka EF ATR/INFO prisutna je ako tahografska kartica u svojem ATR-u naznači da podržava produljena polja. U tom slučaju EF ATR/INFO sadržava podatkovni objekt s informacijama o produljenju (DO ‘7F66’) kako je utvrđeno u točki 12.7.1. norme ISO/IEC 7816-4:2013.

TCS_147 Osnovna datoteka EF Extended_Length prisutna je ako tahografska kartica u svojem ATR-u naznači da podržava produljena polja. U tom slučaju EF sadržava sljedeći podatkovni objekt: ‘02 01 xx’ ako vrijednost ‘xx’ označuje jesu li produljena polja podržana za protokole T = 1 i/ili T = 0.

Vrijednost ‘01’ označuje da su produljena polja podržana za protokol T = 1.

Vrijednost ‘10’ označuje da su produljena polja podržana za protokol T = 0.

Vrijednost ‘11’ označuje da su produljena polja podržana za protokole T = 1 i T = 0.

4.2. Aplikacija kartice vozača

4.2.1 *Aplikacija kartice vozača prve generacije*

TCS_148 Aplikacija kartice vozača prve generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uvjete za pristup datotekama:

		Uvjeti pristupa		
Datoteka	**ID datoteke**	**Čitanje**	**Odabir**	**Ažuriranje**
└─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

U ovoj se tablici upotrebljavaju sljedeće kratice za sigurnosne uvjete:

SC1 ALW ILI SM-MAC-G2

SC2 ALW ILI SM-MAC-G1 ILI SM-MAC-G2

SC3 SM-MAC-G1 ILI SM-MAC-G2

TCS_149 Strukture svih EF-ova moraju biti transparentne.

TCS_150 Aplikacija kartice vozača prve generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	Zadane vrijednosti
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 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice vozača mora upotrebljavati za aplikaciju prve generacije:

		Minimalno	**Maksimalno**
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 bajta (28 dana * 93 promjene aktivnosti)	13 776 bajtova (28 dana * 240 promjena aktivnosti)

4.2.2 *Aplikacija kartice vozača druge generacije*

TCS_152 Aplikacija kartice vozača druge generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uvjete za pristup datotekama:

Napomena: SFID kratkog EF indikatora navodi se kao decimalni broj, na primjer vrijednost 30 odgovara vrijednosti 11110 u binarnom zapisu.

			Uvjeti pristupa	
Datoteka	**ID datoteke**	**SFID**	**Čitanje / Odabir**	**Ažuriranje**
└─ 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

U ovoj se tablici upotrebljava sljedeća kratica za sigurnosni uvjet:

SC1 ALW ILI SM-MAC-G2

TCS_153 Strukture svih EF-ova moraju biti transparentne.

TCS_154 Aplikacija kartice vozača druge generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	Zadane vrijednosti
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 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice vozača mora upotrebljavati za aplikaciju druge generacije:

		Minimalno	**Maksimalno**
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 bajta (28 dana * 93 promjene aktivnosti)	13 776 bajtova (28 dana * 240 promjena aktivnosti)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. Aplikacije kartice radionice

4.3.1 *Aplikacija kartice radionice prve generacije*

TCS_156 Aplikacija kartice radionice prve generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uvjete za pristup datotekama:

		Uvjeti pristupa		
Datoteka	**ID datoteke**	**Čitanje**	**Odabir**	**Ažuriranje**
└─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

U ovoj se tablici upotrebljavaju sljedeće kratice za sigurnosne uvjete:

SC1 ALW ILI SM-MAC-G2

SC2 ALW ILI SM-MAC-G1 ILI SM-MAC-G2

SC3 SM-MAC-G1 ILI SM-MAC-G2

SC4 Za naredbu READ BINARY s parnim INS bajtom:

(PLAIN-C I SM-R-ENC-G1) ILI (SM-C-MAC-G1 I SM-R-ENC-MAC-G1) ILI

(SM-C-MAC-G2 I SM-R-ENC-MAC-G2)

Za naredbu READ BINARY s neparnim INS bajtom (ako je podržan): NEV

TCS_157 Strukture svih EF-ova moraju biti transparentne.

TCS_158 Aplikacija kartice radionice prve generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	Zadane vrijednosti
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 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice radionice mora upotrebljavati za aplikaciju prve generacije:

		Minimalno	**Maksimalno**
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 bajtova (1 dan * 93 promjene aktivnosti)	492 bajta (1 dan * 240 promjena aktivnosti)

4.3.2 *Aplikacija kartice radionice druge generacije*

TCS_160 Aplikacija kartice radionice druge generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uvjete za pristup datotekama:

Napomena: SFID kratkog EF indikatora navodi se kao decimalni broj, na primjer vrijednost 30 odgovara vrijednosti 11110 u binarnom zapisu.

			Uvjeti pristupa		
Datoteka	**ID datoteke**	**SFID**	**Čitanje**	**Odabir**	**Ažuriranje**
└─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

U ovoj se tablici upotrebljavaju sljedeće kratice za sigurnosne uvjete:

SC1 ALW ILI SM-MAC-G2

SC5 Za naredbu READ BINARY s parnim INS bajtom: SM-C-MAC-G2 I SM-R-ENC-MAC-G2

Za naredbu READ BINARY s neparnim INS bajtom (ako je podržan): NEV

TCS_161 Strukture svih EF-ova moraju biti transparentne.

TCS_162 Aplikacija kartice radionice druge generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	Zadane vrijednosti
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 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice radionice mora upotrebljavati za aplikaciju druge generacije:

		Minimalno	Maksimalno
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 bajtova (1 dan * 93 promjene aktivnosti)	492 bajta (1 dan * 240 promjena aktivnosti)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Aplikacije kontrolne kartice

4.4.1 *Aplikacija kontrolne kartice prve generacije*

TCS_164 Aplikacija kontrolne kartice prve generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uvjete za pristup datotekama:

		Uvjeti pristupa		
Datoteka	**ID datoteke**	**Čitanje**	**Odabir**	**Ažuriranje**
└─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

U ovoj se tablici upotrebljavaju sljedeće kratice za sigurnosne uvjete:

SC1 ALW ILI SM-MAC-G2

SC2 ALW ILI SM-MAC-G1 ILI SM-MAC-G2

SC3 SM-MAC-G1 ILI SM-MAC-G2

SC6 EXT-AUT-G1 ILI SM-MAC-G1 ILI SM-MAC-G2

TCS_165 Strukture svih EF-ova moraju biti transparentne.

TCS_166 Aplikacija kontrolne kartice prve generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	
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 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kontrolne kartice mora upotrebljavati za aplikaciju prve generacije:

		Minimalno	Maksimalno
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Aplikacija kontrolne kartice druge generacije*

TCS_168 Aplikacija kontrolne kartice druge generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uvjete za pristup datotekama:

Napomena: SFID kratkog EF indikatora navodi se kao decimalni broj, na primjer vrijednost 30 odgovara vrijednosti 11110 u binarnom zapisu.

			Uvjeti pristupa	
Datoteka	**ID datoteke**	**SFID**	**Čitanje / Odabir**	**Ažuriranje**
└─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

U ovoj se tablici upotrebljava sljedeća kratica za sigurnosni uvjet:

SC1 ALW ILI SM-MAC-G2

TCS_169 Strukture svih EF-ova moraju biti transparentne.

TCS_170 Aplikacija kontrolne kartice druge generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	
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 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kontrolne kartice mora upotrebljavati za aplikaciju druge generacije:

		Minimalno	Maksimalno
n_7	NoOfControlActivityRecords	230	520

4.5. Aplikacije kartice poduzeća

4.5.1 *Aplikacija kartice poduzeća prve generacije*

TCS_172 Aplikacija kartice poduzeća prve generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uvjete za pristup datotekama:

Datoteka	ID datoteke	Uvjeti pristupa: Čitanje	Odabir	Ažuriranje
└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

U ovoj se tablici upotrebljavaju sljedeće kratice za sigurnosne uvjete:

SC1 ALW ILI SM-MAC-G2

SC2 ALW ILI SM-MAC-G1 ILI SM-MAC-G2

SC3 SM-MAC-G1 ILI SM-MAC-G2

SC6 EXT-AUT-G1 ILI SM-MAC-G1 ILI SM-MAC-G2

TCS_173 Strukture svih EF-ova moraju biti transparentne.

TCS_174 Aplikacija kartice poduzeća prve generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	Zadane vrijednosti
└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 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice poduzeća mora upotrebljavati za aplikaciju prve generacije:

		Minimalno	Maksimalno
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Aplikacija kartice poduzeća druge generacije*

TCS_176 Aplikacija kartice poduzeća druge generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uvjete za pristup datotekama:

Napomena: SFID kratkog EF indikatora navodi se kao decimalni broj, na primjer vrijednost 30 odgovara vrijednosti 11110 u binarnom zapisu.

			Uvjeti pristupa	
Datoteka	**ID datoteke**	**SFID**	**Čitanje / Odabir**	**Ažuriranje**
└─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

U ovoj se tablici upotrebljava sljedeća kratica za sigurnosni uvjet:

SC1 ALW ILI SM-MAC-G2

TCS_177 Strukture svih EF-ova moraju biti transparentne.

TCS_178 Aplikacija kartice poduzeća druge generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	Zadane vrijednosti
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 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice poduzeća mora upotrebljavati za aplikaciju druge generacije:

		Minimalno	Maksimalno
n_8	NoOfCompanyActivityRecords	230	520

Dodatak 3.

PIKTOGRAMI

PIC_001 Tahograf može neobavezno upotrebljavati sljedeće piktograme i kombinacije piktograma (ili piktograme i kombinacije piktograma koji su dovoljno slični da ih je nedvojbeno moguće povezati s ovima):

1. OSNOVNI PIKTOGRAMI

	Osobe	**Radnje**	**Načini rada**
	Poduzeće		Način rada poduzeća
	Nadzornik	Kontrola	Kontrolni način
	Vozač	Vožnja	Operativni način
	Radionica / ispitno mjesto	Pregled/kalibracija	Kalibracijski način
	Proizvođač		
	Aktivnosti	**Trajanje**	
	Pripravnost	Razdoblje tekuće pripravnosti	
	Vožnja	Neprekidno vrijeme vožnje	
	Odmor	Razdoblje tekućeg odmora	
	Ostali rad	Razdoblje tekućeg rada	
	Stanka	Kumulativno vrijeme stanki	
	Nepoznato		
	Oprema	**Funkcije**	
	Utor vozača		
	Utor suvozača		
	Kartica		
	Sat		
	Prikaz	Prikazivanje	
	Vanjska pohrana podataka	Preuzimanje podataka	
	Napajanje		
	Pisač/ispis	Ispisivanje	
	Senzor		
	Veličina guma		
	Vozilo / jedinica u vozilu		
	GNSS uređaj		
	Uređaj za otkrivanje na daljinu		
	ITS sučelje		
	Posebna stanja		
OUT	Izvan područja primjene		
	Vožnja trajektom/vlakom		

Razno

!	Događaji	⤫	Pogreške
⏵	Početak dnevnog radnog vremena	⏹	Kraj dnevnog radnog vremena
●	Mjesto		
M	Ručni unos aktivnosti vozača		
	Sigurnost		
	Brzina		
	Vrijeme		
Σ	Ukupno/sažetak		

Oznake

24h	Dnevno
I	Tjedno
II	Dva tjedna
+	Od ili do

2. KOMBINACIJE PIKTOGRAMA

Razno

●	Mjesto kontrole		
● ⏵	Mjesto početka dnevnog radnog vremena	⏹ ●	Mjesto kraja dnevnog radnog vremena
+	Od (vrijeme)	+	Do (vrijeme)
+	Iz vozila		
OUT +	Početak aktivnosti izvan područja primjene	+ OUT	Završetak aktivnosti izvan područja primjene

Kartice

	Kartica vozača
	Kartica poduzeća
	Kontrolna kartica
	Kartica radionice
– – –	Bez kartice

Vožnja

	Vožnja u posadi
I	Vrijeme vožnje u tjedan dana
II	Vrijeme vožnje u dva tjedna

Ispisi

24h	Dnevni ispis aktivnosti vozača s kartice
24h	Dnevni ispis aktivnosti vozača iz jedinice u vozilu
! ⤫	Ispis događaja i kvarova s kartice
! ⤫	Ispis događaja i kvarova iz jedinice u vozilu
	Ispis tehničkih podataka
	Ispis prekoračenja brzine

Događaji

	Umetanje nevažeće kartice
	Konflikt kartica
	Vremensko preklapanje
	Vožnja bez odgovarajuće kartice
	Umetanje kartice tijekom vožnje
	Posljednja razmjena podataka s karticom nije ispravno zatvorena
	Prekoračenje brzine
	Prekid napajanja
	Pogreška u podatcima o kretanju
	Konflikt u kretanju vozila
	Povreda sigurnosti
	Prilagodba vremena (od strane radionice)
	Kontrola prekoračenja brzine

Kvarovi

	Kvar kartice (utor vozača)
	Kvar kartice (utor suvozača)
	Kvar zaslona
	Pogreška pri preuzimanju podataka
	Kvar pisača
	Kvar senzora
	Interni kvar jedinice u vozilu (VU)
	Kvar GNSS uređaja
	Kvar uređaja za otkrivanje na daljinu

Postupak ručnog unosa

	I dalje isto dnevno radno vrijeme?
	Kraj prethodnog radnog vremena?
	Potvrdite ili unesite mjesto kraja radnog vremena
	Unesite vrijeme početka
	Potvrdite ili unesite mjesto početka radnog vremena

Napomena: dodatne kombinacije piktograma za formiranje bloka ispisa ili identifikatora zapisa utvrđene su u Dodatku 4.

Dodatak 4

ISPISI

SADRŽAJ

1. OPĆENITO 243
2. SPECIFIKACIJA PODATKOVNOG BLOKA 243
3. SPECIFIKACIJE ISPISA 250
3.1. Dnevni ispis aktivnosti vozača s kartice 250
3.2. Dnevni ispis aktivnosti vozača iz jedinice u vozilu (VU) 251
3.3. Ispis događaja i kvarova s kartice 252
3.4. Ispis događaja i kvarova iz VU-a 252
3.5. Ispis tehničkih podataka 253
3.6. Ispis prekoračenja brzine 253
3.7. Povijesni podatci o umetnutim karticama 254

1. OPĆENITO

Svaki ispis nastaje ulančavanjem raznih podatkovnih blokova, koji se mogu identificirati s pomoću identifikatora bloka.

Jedan podatkovni blok sadržava jedan ili više zapisa, koji se mogu identificirati s pomoću identifikatora zapisa.

PRT_001 Kad identifikator bloka neposredno prethodi identifikatoru zapisa, identifikator zapisa se ne ispisuje.

PRT_002 Ako je neka podatkovna stavka nepoznata ili se ne smije ispisati zbog prava na pristup podatcima, umjesto nje ispisuju se praznine.

PRT_003 Ako je sadržaj cijelog retka nepoznat ili ga ne treba ispisivati, izostavlja se cijeli redak.

PRT_004 Numerička podatkovna polja ispisuju se u desnom poravnanju, s razmakom za tisuće i milijune i bez vodećih nula.

PRT_005 Polja s podatkovnim nizovima ispisuju se u lijevom poravnanju i popunjavaju prazninama do duljine podatkovne stavke ili se prema potrebi skraćuju na duljinu podatkovne stavke (imena i adrese).

PRT_006 U slučaju kraja retka zbog dugog teksta, kao prvi znak novog retka ispisuje se poseban znak (točka na sredini visine retka, „•”).

2. SPECIFIKACIJA PODATKOVNOG BLOKA

U ovom se poglavlju upotrebljavaju sljedeći dogovoreni formati bilježenja:

— **masno** otisnutim slovima označava se običan tekst koji treba ispisati (pri čemu se tekst ispisuje normalnim slovima),

— normalnim znakovima označavaju se varijable (piktogrami ili podatci) koje se prilikom ispisa zamjenjuju svojim vrijednostima,

— nazivi varijabli nadopunjeni su podcrtavanjem za prikaz duljine podatkovne stavke raspoložive za varijablu,

— datumi se navode u formatu „dd/mm/gggg” (dan, mjesec, godina). Može se upotrebljavati i oblik „dd.mm. gggg”,

— izraz „identifikacija kartice” je oznaka koja se sastoji od vrste kartice prikazane kombinacijom piktograma kartice, šifre države članice koja ju je izdala, kose crte te broja kartice s indeksom zamjene i indeksom obnavljanja odvojenima razmakom:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
kombinacija piktograma kartice		šifra države članice koja je izdala karticu				prvih 14 znamenaka broja kartice (po mogućnosti s indeksom rednog broja kartice)														indeks zamjene		indeks obnavljanja

PRT_007 Za ispise se upotrebljavaju sljedeći podatkovni blokovi i/ili zapisi, u skladu sa sljedećim značenjima i formatima:

Broj bloka ili zapisa Značenje	Data Format
1. ***Datum i vrijeme ispisa dokumenta***	dd/mm/yyyy hh:mm **(UTC)**
2. ***Vrsta ispisa*** Identifikator bloka Ispis kombinacije piktograma (vidjeti Dodatak 3.), postavka uređaja za ograničavanje brzine (samo za ispis prekoračenja brzine)	----------T---------- Picto xxx **km/h**
3. ***Identifikacija nositelja kartice*** Identifikator bloka P = piktogram „osoba” Prezime nositelja kartice Ime(na) nositelja kartice (ako postoji) Identifikacija kartice Datum isteka valjanosti kartice (ako postoji) i broj generacije kartice (GEN 1 ili GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

U slučaju neosobne kartice koja ne sadržava prezime nositelja kartice, umjesto toga se tiska naziv poduzeća, radionice ili nadzornog tijela.

(*) Broj generacije kartice može ispisati samo pametni tahograf.

4. ***Identifikacija vozila*** Identifikator bloka VIN Država članica registracije i registracijski broj vozila (VRN)	----------A---------- A VIN_____ Nat/VRN_____
5. ***Identifikacija jedinice u vozilu (VU)*** Identifikator bloka Naziv proizvođača jedinice u vozilu Kataloški broj jedinice u vozilu Broj generacije jedinice u vozilu (*)	----------B---------- B VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Broj generacije kartice može ispisati samo pametni tahograf.

6. ***Zadnja kalibracija tahografa*** Identifikator bloka Naziv radionice Identifikacija kartice radionice Datum kalibracije	----------T---------- T Last_Name_____ Card_Identification_____ T dd/mm/yyyy

7. ***Zadnja kontrola (od strane službenika za kontrolu)***

Identifikator bloka	----------▯----------
Identifikacija kartice nadzornika	Card_Identification_____
Datum, vrijeme i vrsta kontrole	▯ dd/mm/yyyy hh:mm ppppp

Vrsta kontrole: do pet piktograma. Vrsta kontrole može biti (kombinacija) sljedećeg:

▮: preuzimanje podataka s kartice, ↧: preuzimanje podataka s VU-a, ▼: ispis, ▯: prikaz, ⊺:provjera kalibracije na cesti

8. ***Aktivnosti vozača pohranjene na kartici prema redoslijedu nastanka***

Identifikator bloka	----------⊙----------
Datum upita (kalendarski dan ispisa) + brojač dnevne nazočnosti kartice	dd/mm/yyyy xxx
8.a *Stanje izvan područja primjene na početku ovog dana* (ostaviti prazno ako nije otvoreno stanje izvan područja primjene)	----------OUT----------
8.1. *Razdoblje u kojem kartica nije bila umetnuta*	
8.1.a Identifikator zapisa (početak razdoblja)	----------
8.1.b *Nepoznato razdoblje* Vrijeme početka, trajanje	? hh:mm hh**h**mm
8.1.c *Ručno unesena aktivnost*	A hh:mm hh**h**mm
Piktogram aktivnosti, vrijeme početka, trajanje	
8.2. *Umetanje kartice u utor S*	
Identifikator zapisa; S = piktogram utora	---------S---------
Država članica registracije vozila i registracijski broj vozila (VRN)	Nat/VRN_____
Stanje brojača kilometara vozila pri umetanju kartice	x xxx xxx **km**
8.3. *Aktivnost (dok je kartica bila umetnuta)*	
Piktogram aktivnosti, vrijeme početka, trajanje, status posade (piktogram posade za status POSADA, prazno ako je JEDAN VOZAČ)	A hh:mm hh**h**mm ⊙⊙
8.3.a *Posebno stanje* Vrijeme unosa, piktogram posebnog stanja (ili kombinacija piktograma)	hh:mm ---pppp---
8.4. *Vađenje kartice*	
Brojač kilometara vozila i prijeđena udaljenost od zadnjeg umetanja za koje je poznat brojač kilometara	x xxx xxx **km**; x xxx **km**

9. ***Aktivnosti vozača pohranjene u jedinici u vozilu, po utoru, kronološkim redom***

Identifikator bloka	----------⊙----------
Datum upita (kalendarski dan ispisa)	dd/mm/yyyy
Brojač kilometara vozila u 00:00 i 24:00	x xxx xxx - x xxx xxx **km**

10. ***Aktivnosti koje se obavljaju u utoru S***

Identifikator bloka	----------S----------
10.a *Stanje izvan područja primjene na početku ovog dana* (ostaviti prazno ako nije otvoreno stanje izvan područja primjene)	----------OUT----------
10.1. *Razdoblje kada u utoru S nema kartice*	
Identifikator zapisa	----------
Nije umetnuta kartica	⊙▮---
Brojač kilometara vozila na početku razdoblja	x xxx xxx **km**
10.2. *Umetanje kartice*	
Identifikator zapisa o umetanju kartice	----------
Prezime vozača	⊙ Last_Name_____

	Ime vozača	First_Name_____
	Identifikacija kartice vozača	Card_Identification_____
	Datum isteka valjanosti kartice (ako postoji) i broj generacije kartice (GEN 1 ili GEN 2) (*)	dd/mm/yyyy - GEN 2
	Država članica registracije i registracijski broj (VRN) prethodno korištenog vozila	+Nat/VRN_____
	Datum i vrijeme vađenja kartice iz prethodnog vozila	dd/mm/yyyy hh:mm
	Prazni redak	
	Brojač kilometara vozila pri umetanju kartice. Znak ručnog unosa aktivnosti vozača (M: da, prazno: ne).	x xxx xxx **km** M
	Ako nije bilo umetanja kartice vozača na dan kad se vrši ispis, tada se za blok 10.2. upotrebljava očitanje podataka brojača kilometara od zadnjeg dostupnog umetanja kartice prije tog dana.	
10.3.	*Aktivnost*	
	Piktogram aktivnosti, vrijeme početka, trajanje, status posade (piktogram posade za status POSADA, prazno ako je JEDAN VOZAČ)	A hh:mm hh**h**mm
10.3.a	*Posebno stanje* Vrijeme unosa, piktogram posebnog stanja (ili kombinacija piktograma)	hh:mm ---pppp---
10.4.	*Vađenje kartice ili kraj razdoblja „bez kartice”*	
	Brojač kilometara vozila pri vađenju kartice ili na kraju razdoblja „bez kartice” i prijeđena udaljenost od umetanja kartice ili od početka razdoblja „bez kartice”.	x xxx xxx **km**; x xxx **km**

(*) Broj generacije kartice može ispisati samo pametni tahograf.

11.	***Dnevni sažetak***	
	Identifikator bloka	----------Σ----------
11.1.	***Dnevni sažetak jedinice u vozilu za razdoblja bez kartice u utoru vozača***	
	Identifikator bloka	1----
11.2.	***Dnevni sažetak jedinice u vozilu za razdoblja bez kartice u utoru suvozača***	
	Identifikator bloka	2----
11.3.	***Dnevni sažetak jedinice u vozilu po vozaču***	
	Identifikator zapisa	----------
	Prezime vozača	Last_Name_____
	Ime(na) vozača	First_Name_____
	Identifikacija kartice vozača	Card_Identification_____
11.4.	*Unos mjesta početka i/ili kraja dnevnog radnog vremena*	
	pi = piktogram početka/kraja, vrijeme, država, regija	pihh:mm Cou Reg
	Brojač kilometara	x xxx xxx **km**
11.5.	*Unos mjesta početka i/ili kraja dnevnog radnog vremena*	
	i nakon 3 sata neprekidne vožnje vozača	hh:mm
	Brojač kilometara	x xxx xxx **km**

11.6.	*Aktivnosti ukupno (s kartice)*	
	Ukupno trajanje vožnje, prijeđena udaljenost	hh**h**mm x xxx **km**
	Ukupno trajanje rada i pripravnosti	hh**h**mm hh**h**mm
	Ukupno trajanje odmora i nepoznatih aktivnosti	hh**h**mm hh**h**mm
	Ukupno trajanje aktivnosti posade	hh**h**mm
11.7.	*Aktivnosti ukupno (razdoblja bez kartice u utoru vozača)*	
	Ukupno trajanje vožnje, prijeđena udaljenost	hh**h**mm x xxx **km**
	Ukupno trajanje rada i pripravnosti	hh**h**mm hh**h**mm
	Ukupno trajanje odmora	hh**h**mm

11.8. *Aktivnosti ukupno (razdoblja bez kartice u utoru suvozača)*

Ukupno trajanje rada i pripravnosti	hhhmm hhhmm
Ukupno trajanje odmora	hhhmm

11.9. *Aktivnosti ukupno (po vozaču, uključuje oba utora)*

Ukupno trajanje vožnje, prijeđena udaljenost	hhhmm x xxx km
Ukupno trajanje rada i pripravnosti	hhhmm hhhmm
Ukupno trajanje odmora	hhhmm
Ukupno trajanje aktivnosti posade	hhhmm

Ako se traži dnevni ispis za tekući dan, informacije o dnevnom sažetku računaju se iz podataka dostupnih u vrijeme ispisa.

12. ***Događaji i/ili kvarovi pohranjeni na kartici***

12.1. Identifikator bloka zadnjih pet „događaja i kvarova” s kartice

```
----------!×----------
```

12.2. Identifikator bloka svih zabilježenih „događaja” na kartici

```
----------!----------
```

12.3. Identifikator bloka svih zabilježenih „kvarova” na kartici

```
----------×----------
```

12.4. *Zapis događaja i/ili kvara*

Identifikator zapisa	
Piktogram događaja/kvara, svrha zapisa, datum i vrijeme početka	Pic (p) dd/mm/yyyy hh:mm
Dodatna šifra događaja/kvara (ako postoji), trajanje	!xx hhhmm
Država članica registracije i registracijski broj vozila (VRN) u kojem se dogodio događaj ili kvar	Nat/VRN_____

13. ***Događaji i/ili kvarovi koji su pohranjeni ili u tijeku u jedinici u vozilu (VU)***

13.1. Identifikator bloka zadnjih pet „događaja i kvarova” iz VU-a

```
----------!×----------
```

13.2. Identifikator bloka svih zabilježenih „događaja” ili „događaja” u tijeku u VU-u

```
----------!----------
```

13.3. Identifikator bloka svih zabilježenih „kvarova” ili „kvarova” u tijeku u VU-u

```
----------×----------
```

13.4. *Zapis događaja i/ili kvara*

Identifikator zapisa	
Piktogram događaja/kvara, svrha zapisa, datum i vrijeme početka	Pic (p) dd/mm/yyyy hh:mm
Dodatna šifra događaja/kvara (ako postoji), broj sličnih događaja tog dana, trajanje	!xx (xxx) hhhmm
Identifikacija kartica umetnutih na početku ili na kraju događaja ili kvara (do četiri retka bez ponavljanja istih brojeva kartica dva puta)	Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____
Slučaj kad nije bila umetnuta nijedna kartica	----
Podatci specifični za proizvođača	< Literal><ErrorCode>

Svrha zapisa (p) je numerička šifra koja objašnjava zašto je događaj ili kvar zabilježen, a šifrirana je u skladu s podatkovnim elementom `EventFaultRecordPurpose`.

`Literal` je literal specifičan za proizvođača tahografa s najviše 12 znakova.

`ErrorCode` je šifra pogreške specifična za proizvođača tahografa s najviše 12 znakova.

14. ***Identifikacija jedinice u vozilu (VU)***

Identifikator bloka	----------B----------
Naziv proizvođača VU-a	B Name_____
Adresa proizvođača VU-a	Address_____
Kataloški broj VU-a	PartNumber_____
Homologacijski broj VU-a	Apprv_____
Serijski broj VU-a	S/N_____
Godina proizvodnje VU-a	yyyy
Verzija programa u VU-u i datum instalacije	V xxxx dd/mm/yyyy

15. ***Identifikacija senzora***

Identifikator bloka	----------Л----------

15.1. *Zapis o uparivanju*

Serijski broj senzora	Л S/N_____
Homologacijski broj senzora	Apprv_____
Datum uparivanja senzora	dd/mm/yyyy hh:mm

16. *Identifikacija uređaja GNSS-a*

Identifikator bloka	----------▚----------

16.1. *Zapis o spajanju*

Serijski broj vanjskog uređaja GNSS-a	▚ S/N_____
Homologacijski broj vanjskog uređaja GNSS-a	Apprv_____
Datum spajanja vanjskog uređaja GNSS-a	dd/mm/yyyy hh:mm

17. ***Podatci o kalibraciji***

Identifikator bloka	----------T----------

17.1. *Zapis o kalibraciji*

Identifikator zapisa	----------
Radionica koja je izvršila kalibraciju	T Workshop_name_____
Adresa radionice	Workshop_address_____
Identifikacija kartice radionice	Card_Identification_____
Datum isteka valjanosti kartice radionice	dd/mm/yyyy
Prazni redak	
Datum kalibracije + svrha kalibracije	T dd/mm/yyyy (p)
VIN	A VIN_____
Država članica registracije i registracijski broj vozila (VRN)	Nat/VRN_____
Karakteristični koeficijent vozila	w xx xxx Imp/km
Konstanta uređaja za bilježenje podataka	k xx xxx Imp/km
Effective circumference of wheel tyres	l xx xxx mm
Veličina montiranih guma	● TyreSize_____
Postavka uređaja za ograničavanje brzine	> xxx km/h
Stare i nove vrijednosti na brojaču kilometara	x xxx xxx – x xxx xxx km

Svrha kalibracije (p) je numerička šifra koja objašnjava zašto su zabilježeni ti kalibracijski parametri, a šifrirana je u skladu s podatkovnim elementom `CalibrationPurpose`.

18. ***Prilagodba vremena***

	Identifikator bloka	----------◷----------
18.1.	*Zapis o prilagodbi vremena*	
	Identifikator zapisa	---
	Stari datum i vrijeme	!◷ dd/mm/yyyy hh:mm
	Novi datum i vrijeme	◷ dd/mm/yyyy hh:mm
	Radionica koja je izvršila prilagodbu vremena	T Workshop_name_____
	Adresa radionice	Workshop_address_____
	Identifikacija kartice radionice	Card_Identification_____
	Datum isteka valjanosti kartice radionice	dd/mm/yyyy

19. ***Posljednji događaj i kvar zabilježeni u jedinici u vozilu***

	Identifikator bloka	----------!×🖷----------
	Datum i vrijeme posljednjeg događaja	! dd/mm/yyyy hh:mm
	Datum i vrijeme posljednjega kvara	× dd/mm/yyyy hh:mm

20. ***Informacije o kontroli prekoračenja brzine***

	Identifikator bloka	----------»----------
	Datum i vrijeme posljednje KONTROLE PREKORAČENJA BRZINE	»▯dd/mm/yyyy hh:mm
	Datum/vrijeme prvog prekoračenja brzine i broj događaja prekoračenja brzine od tada	»dd/mm/yyyy hh:mm (nnn)

21. ***Zapis o prekoračenju brzine***

21.1.	Identifikator bloka „Prvo prekoračenje brzine nakon zadnje kalibracije”	--------»T---------
21.2.	Identifikator bloka „Pet najozbiljnijih prekoračenja u zadnjih 365 dana”	-------»(365)------
21.3.	Identifikator bloka „Najozbiljnije prekoračenje za svaki od deset zadnjih dana pojave”	-------»(10)-------
21.4.	Identifikator zapisa	---
	Datum, vrijeme i trajanje	»dd/mm/yyyy hh:mm hhhmm
	Najveća i prosječna brzina, broj sličnih događaja tog dana	xxx km/h xxx km/h(xxx)
	Prezime vozača	Last_Name_____
	Ime(na) vozača	First_Name_____
	Identifikacija kartice vozača	Card_Identification_____
21.5.	Ako u bloku nema zapisa o prekoračenju brzine	»---

22. ***Ručno unesene informacije***

	Identifikator bloka	----------
22.1.	Mjesto kontrole	▯• .....
22.2.	Potpis nadzornika	▯ .....
22.3.	Od (vrijeme)	◷+ .....
22.4.	Do (vrijeme)	+◷ .....
22.5.	Potpis vozača	◙ .....

„Ručno unesene informacije”; umetnuti dovoljno praznih redaka iznad prostora za ručni upis tako da se stvarno mogu upisati traženi podatci ili staviti potpis.

23. ***Posljednje kartice umetnute u jedinicu u vozilu***
Identifikator bloka
23.1. Umetnuta kartica
Identifikator zapisa
Vrsta kartice, generacija, verzija, proizvođač (*)
Identifikacija kartice
Serijski broj kartice
Datum i vrijeme posljednjeg umetanja kartice

```
-------- ⊟■⊙ --------

----
⍑ <gen> <version> <MC>
Card Identification
Card Serial Number
dd/mm/yyyy hh:mm
```

(*) (sve u jednom retku)
pri čemu je
type of card (vrsta kartice): piktogram, jedan znak + razmak,
gen (generacija): GEN1 ili GEN2, 4 znaka + razmak,
version (verzija): do 10 znakova,
MC: šifra proizvođača, 3 znaka.

3. SPECIFIKACIJE ISPISA

U ovom se poglavlju upotrebljavaju sljedeći dogovoreni zapisi:

N	Ispis broja bloka ili zapisa N
N	Ispis broja bloka ili zapisa N ponovljen onoliko puta koliko je potrebno
X/Y	Ispis bloka ili zapisa X i/ili Y prema potrebi, ponavljajući onoliko puta koliko je potrebno

3.1. Dnevni ispis aktivnosti vozača s kartice

PRT_008 Dnevni ispis aktivnosti vozača s kartice u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nadzornika (ako je kontrolna kartica umetnuta u VU)
3.	Identifikacija vozača (iz kartice koja je predmet ispisa + GEN)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
5.	Identifikacija VU-a (VU iz kojeg se uzima ispis + GEN)
6.	Zadnja kalibracija VU-a
7.	Zadnja kontrola kojoj je bio podvrgnut vozač
8.	Razdjelnik aktivnosti vozača
8.a	Stanje izvan područja primjene na početku ovog dana
8.1.a / 8.1.b / 8.1.c / 8.2. / 8.3. / 8.3.a / 8.4.	Aktivnosti vozača po redoslijedu nastanka
11.	Razdjelnik dnevnog sažetka

11.4.	Mjesta unijeta kronološkim redom
11.5.	Podatci GNSS-a
11.6.	Aktivnosti ukupno
12.1.	Događaji ili kvarovi s razdjelnika kartice
12.4.	Zapisi događaja/kvarova (zadnjih pet događaja ili kvarova pohranjenih na kartici)
13.1.	Događaji ili kvarovi s razdjelnika VU-a
13.4.	Zapisi događaja/kvarova (zadnjih pet događaja ili kvarova pohranjenih ili u tijeku u VU-u)
22.1.	Mjesto kontrole
22.2.	Potpis nadzornika
22.5.	Potpis vozača

3.2. **Dnevni ispis aktivnosti vozača iz jedinice u vozilu (VU)**

PRT_009 Dnevni ispis aktivnosti vozača iz VU-a u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nositelja kartice (za sve kartice umetnute u VU + GEN)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
5.	Identifikacija VU-a (VU iz kojeg se uzima ispis + GEN)
6.	Zadnja kalibracija VU-a
7.	Zadnja kontrola ovog tahografa
9.	Razdjelnik aktivnosti vozača
10.	Razdjelnik utora vozača (utor 1)
10.a	Stanje izvan područja primjene na početku ovog dana
10.1. / 10.2. / 10.3. / 10.3.a / 10.4.	Aktivnosti kronološkim redom (utor vozača)
10.	Razdjelnik utora suvozača (utor 2)
10.a	Stanje izvan područja primjene na početku ovog dana
10.1. / 10.2. / 10.3. / 10.3.a / 10.4.	Aktivnosti kronološkim redom (utor suvozača)
11.	Razdjelnik dnevnog sažetka
11.1.	Sažetak razdoblja bez kartice u utoru vozača
11.4.	Mjesta unijeta kronološkim redom
11.5.	Podatci GNSS-a
11.6.	Aktivnosti ukupno
11.2.	Sažetak razdoblja bez kartice u utoru suvozača
11.4.	Mjesta unijeta kronološkim redom
11.5.	Podatci GNSS-a

11.7.	Aktivnosti ukupno
11.3.	Sažetak aktivnosti za vozača, uključena oba utora
11.4.	Mjesta koja je taj vozač unio kronološkim redom
11.5.	Podatci GNSS-a
11.8.	Aktivnosti ukupno za tog vozača
13.1.	Razdjelnik događaja i kvarova
12.4.	Zapisi događaja/kvarova (zadnjih pet događaja ili kvarova pohranjenih ili u tijeku u VU-u)
13.1.	Mjesto kontrole
22.2.	Potpis nadzornika
22.3.	Od (vrijeme) (prostor za vozača bez kartice da navede razdoblja koja se odnose na njega)
22.4.	Do (vrijeme)
22.5.	Potpis vozača

3.3. **Ispis događaja i kvarova s kartice**

PRT_010 Ispis događaja i kvarova s kartice u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nadzornika (ako je kontrolna kartica umetnuta u VU + GEN)
3.	Identifikacija vozača (iz kartice koja je predmet ispisa)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
12.2.	Razdjelnik događaja
12.4.	Zapisi događaja (svi događaji pohranjeni na kartici)
12.3.	Razdjelnik kvarova
12.4.	Zapisi o kvarovima (svi kvarovi pohranjeni na kartici)
22.1.	Mjesto kontrole
22.2.	Potpis nadzornika
22.5.	Potpis vozača

3.4. **Ispis događaja i kvarova iz VU-a**

PRT_011 Ispis događaja i kvarova iz VU-a u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nositelja kartice (za sve kartice umetnute u VU + GEN)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)

13.2.	Razdjelnik događaja
13.4.	Zapisi događaja (svi događaji pohranjeni ili u tijeku u VU-u)
13.3.	Razdjelnik kvarova
13.4.	Zapisi o kvarovima (sve pogreške pohranjene ili u tijeku u VU-u)
22.1.	Mjesto kontrole
22.2.	Potpis nadzornika
22.5.	Potpis vozača

3.5. **Ispis tehničkih podataka**

PRT_012 Ispis tehničkih podataka u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nositelja kartice (za sve kartice umetnute u VU + GEN)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
14.	Identifikacija jedinice u vozilu (VU)
15.	Identifikacija senzora
15.1.	Podatci o uparivanju senzora (svi raspoloživi podatci kronološkim redom)
16.	Identifikacija uređaja GNSS-a
16.1.	Podatci o spajanju vanjskog uređaja GNSS-a (svi raspoloživi podatci kronološkim redom)
17.	Razdjelnik podataka o kalibraciji
17.1.	Zapisi o kalibraciji (svi raspoloživi zapisi kronološkim redom)
18.	Razdjelnik prilagodbe vremena
18.1.	Zapisi o prilagodbi vremena (svi raspoloživi zapisi od zapisa o prilagodbi vremena i od zapisa o kalibraciji)
19.	Posljednji događaj i kvar zabilježeni u VU-u

3.6. **Ispis prekoračenja brzine**

PRT_013 Ispis prekoračenja brzine u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nositelja kartice (za sve kartice umetnute u VU + GEN)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
20.	Informacije o kontroli prekoračenja brzine
21.1.	Identifikator podataka o prekoračenju brzine
21.4. / 21.5.	Prvo prekoračenje brzine nakon zadnje kalibracije

21.2.	Identifikator podataka o prekoračenju brzine
21.4. / 21.5.	Pet najozbiljnijih prekoračenja brzine u zadnjih 365 dana
21.3.	Identifikator podataka o prekoračenju brzine
21.4. / 21.5.	Najozbiljnije prekoračenje brzine za svaki od deset zadnjih dana pojave
22.1.	Mjesto kontrole
22.2.	Potpis nadzornika
22.5.	Potpis vozača

3.7. **Povijesni podatci o umetnutim karticama**

PRT_014 Ispis povijesnih podataka o umetnutim karticama u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacije nositelja kartice (za sve kartice umetnute u VU)
23.	Posljednja kartica umetnuta u VU
23.1.	Umetnute kartice (do 88 zapisa)
12.3.	Razdjelnik kvarova

Dodatak 5

PRIKAZ

U ovom se Dodatku upotrebljavaju sljedeći dogovoreni formati bilježenja:

— **masno** otisnuti znakovi označuju običan tekst koji se prikazuje (pri čemu se tekst prikazuje normalnim znakovima),

— normalni znakovi označuju varijable (piktograme ili podatke) koje se prilikom prikaza zamjenjuju svojim vrijednostima:

  — dd mm yyyy: dan, mjesec, godina,

  — hh: sati,

  — mm: minute,

  — D: piktogram trajanja,

  — EF: kombinacija piktograma događaja ili kvarova,

  — O: piktogram načina rada.

DIS_001 Tahograf prikazuje podatke primjenom sljedećeg formata:

Podatci	Format
Standardni prikaz	
Lokalno vrijeme	hh:mm
Način rada	O
Informacije koje se odnose na vozača	1 Dhh**h**mm ▮▮hh**h**mm
Informacije koje se odnose na suvozača	2 Dhh**h**mm
Otvoreno stanje izvan područja primjene	OUT
Prikaz upozorenja	
Prekoračenje neprekidnog vremena vožnje	1 ⊙ hh**h**mm ▮▮hh**h**mm
Događaj ili kvar	EF
Ostali prikazi	
datum po UTC-u	UTC ◔ dd/mm/yyyy ili UTC ◔ dd.mm.yyyy
vrijeme	hh:mm
Neprekidno vrijeme vožnje i kumulativno vrijeme stanki vozača	1 ⊙ hh**h**mm ▮▮hh**h**mm
Neprekidno vrijeme vožnje i kumulativno vrijeme stanki suvozača	2 ⊙ hh**h**mm ▮▮hh**h**mm
Ukupno vrijeme vožnje vozača u prethodnom i tekućem tjednu	1 ⊙ ▮ hhh**h**mm
Ukupno vrijeme vožnje suvozača u prethodnom i tekućem tjednu	2 ⊙ ▮ hhh**h**mm

Dodatak 6

PREDNJI PRIKLJUČAK ZA KALIBRACIJU I PREUZIMANJE PODATAKA

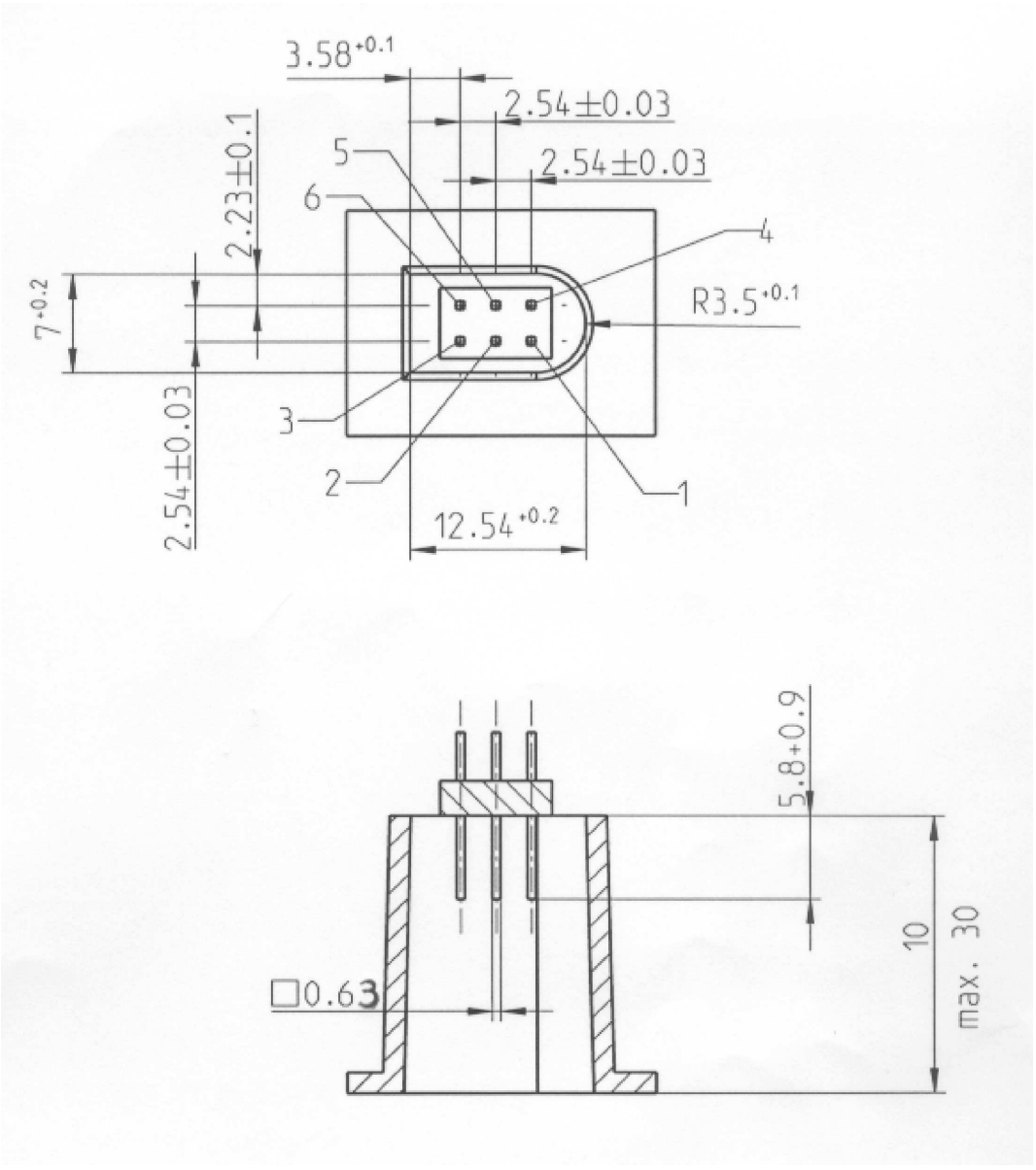
SADRŽAJ

1. HARDVER 256
1.1. Priključak 256
1.2. Raspored kontakata 257
1.3. Blok dijagram 258
2. SUČELJE ZA PREUZIMANJE PODATAKA 258
3. SUČELJE ZA KALIBRACIJU 259

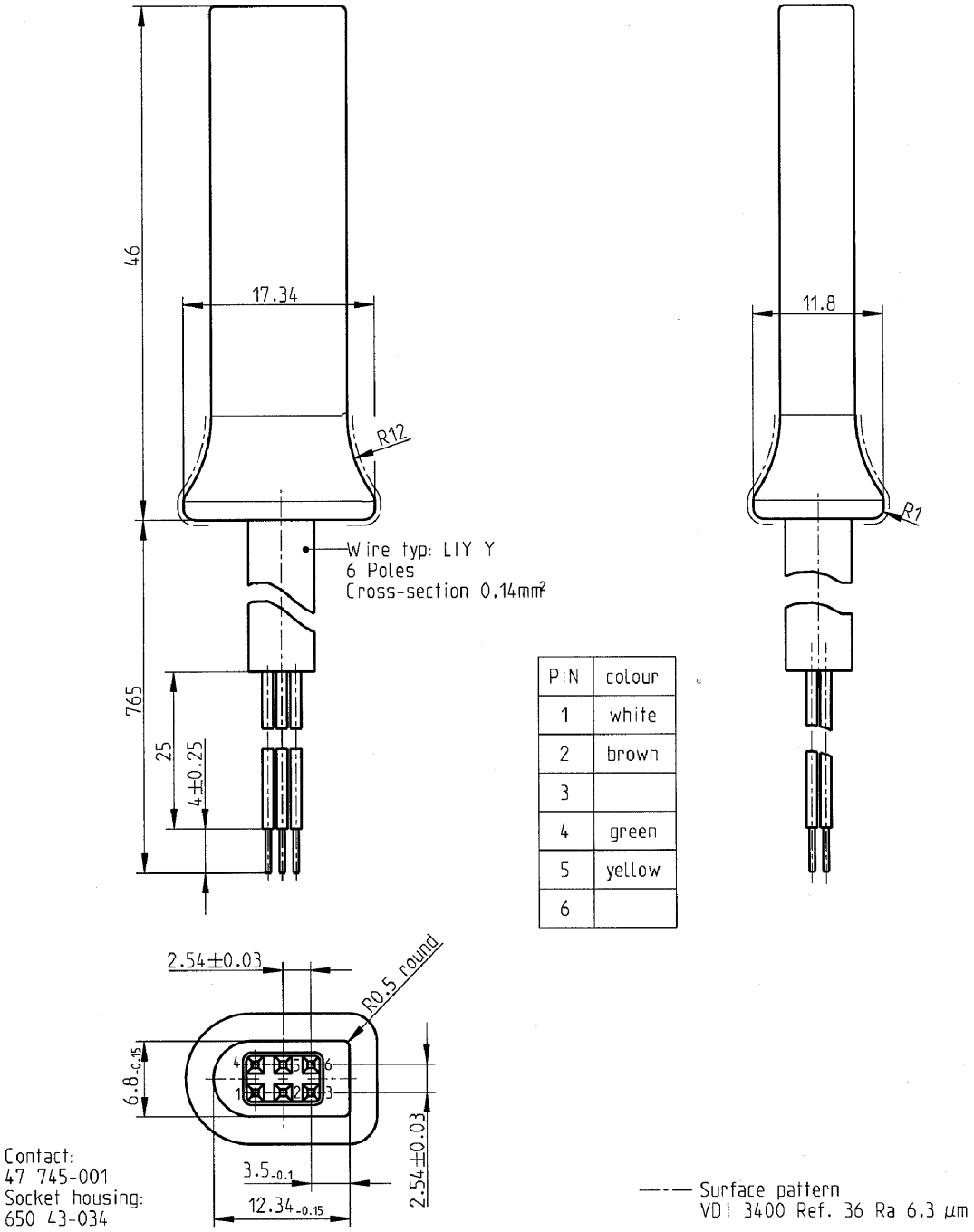
1. HARDVER

1.1. **Priključak**

INT_001 Priključak za preuzimanje podataka / kalibraciju je 6-pinski priključak, dostupan s prednje strane bez potrebe isključivanja bilo kojeg dijela tahografa, i koji udovoljava sljedećem nacrtu (sve dimenzije izražene su u milimetrima):



Sljedeći dijagram prikazuje tipični priključak za 6-pinsko uparivanje:



1.2. **Raspored kontakata**

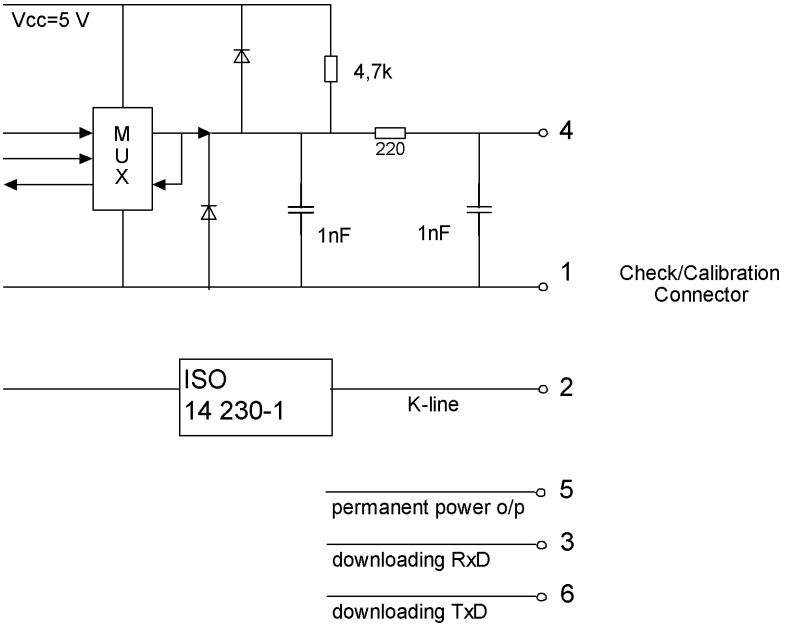
INT_002 Kontakti se raspoređuju prema sljedećoj tablici:

Pin	Opis	Napomena
1	Akumulator – minus	Priključen na negativni pol akumulatora vozila
2	Podatkovna komunikacija	K-linija (ISO 14230-1)

Pin	Opis	Napomena
3	RxD – preuzimanje podataka	Unos podataka u tahograf
4	Ulazni/izlazni signal	Kalibracija
5	Stalna izlazna snaga	Raspon napona je onaj koji je na vozilu, umanjen za 3 V kako bi se omogućio pad napona na zaštitnim strujnim krugovima. Snaga 40 mA
6	TxD – preuzimanje podataka	Izlaz podataka iz tahografa

1.3. **Blok dijagram**

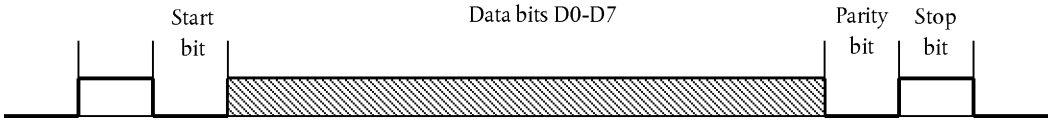
INT_003 Blok dijagram zadovoljava sljedeće:



2. SUČELJE ZA PREUZIMANJE PODATAKA

INT_004 Sučelje za preuzimanje podataka zadovoljava specifikacije RS232.

INT_005 Sučelje za preuzimanje podataka upotrebljava jedan početni bit, osam podatkovnih bitova, s LSB-om (najmanje značajnim bitom) na početku, jedan parni paritetni bit i jedan zaustavni bit.



Organizacija podatkovnog bajta

Početni bit: jedan bit na logičkoj razini 0;

Podatkovni bitovi: prenose se s LSB-om (najmanje značajnim bitom) na početku;

Paritetni bit: parni paritet

Zaustavni bit: jedan bit na logičkoj razini 1.

Kod prijenosa numeričkih podataka sastavljenih od više bajtova, najznačajniji bajt prenosi se prvi, a najmanje značajan bajt posljednji.

INT_006 Brzine prijenosa podataka moraju biti prilagodljive u rasponu od 9 600 bps do 115 200 bps. Prijenos se postiže pri najvišoj mogućoj brzini prijenosa, pri čemu je početna brzina prijenosa podataka nakon početka komunikacije postavljena na 9 600 bps.

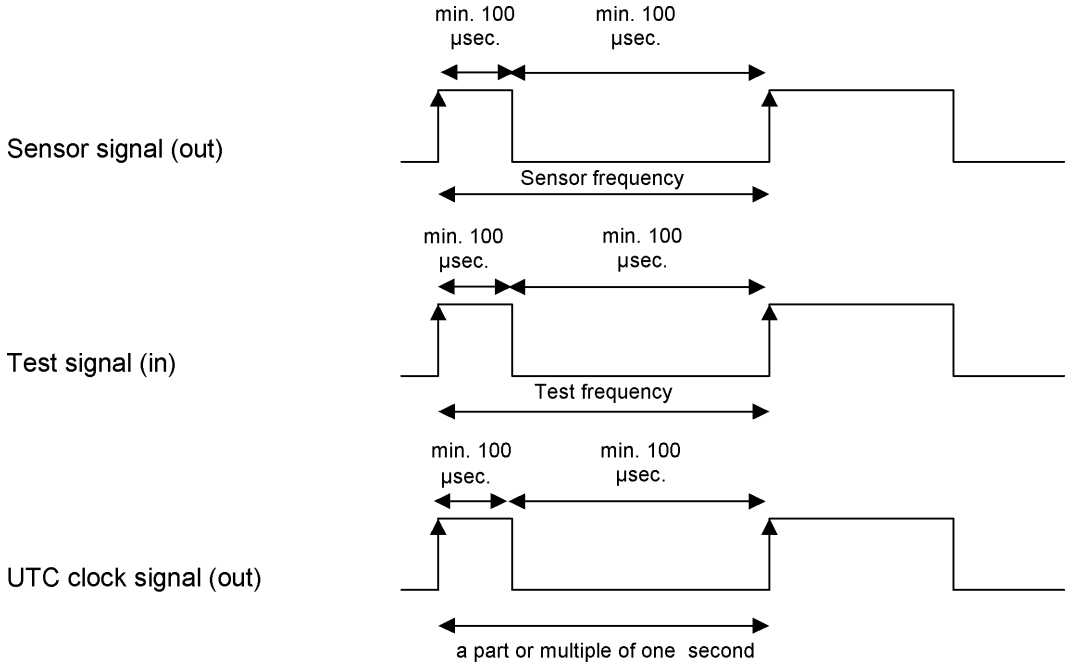
3. Sučelje za kalibraciju

INT_007 Podatkovna komunikacija mora ispunjavati zahtjeve norme ISO 14230-1 *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 1: Physical layer,* prvo izdanje: 1999.

INT_008 Ulazni/izlazni signal mora zadovoljavati sljedeće električne specifikacije:

Parametar	Najmanje	Tipično	Najviše	Napomena
U_{low} (ulazni)			1,0 V	I = 750 µA
U_{high} (ulazni)	4 V			I = 200 µA
Frekvencija			4 kHz	
U_{low} (izlazni)			1,0 V	I = 1 mA
U_{high} (izlazni)	4 V			I = 1 mA

INT_009 Ulazni/izlazni signal mora biti u skladu sa sljedećim vremenskim dijagramima:



Dodatak 7.

PROTOKOLI PREUZIMANJA PODATAKA

SADRŽAJ

1.	UVOD	261
1.1.	Područje primjene	261
1.2.	Skraćenice i zabilješke	261
2.	PREUZIMANJE PODATAKA S JEDINICE U VOZILU (VU)	262
2.1.	Postupak preuzimanja podataka	262
2.2.	Protokol preuzimanja podataka	262
2.2.1	Struktura poruke	262
2.2.2	Vrste poruka	264
2.2.2.1	Zahtjev za početak komunikacije (SID 81)	266
2.2.2.2	Pozitivan odgovor za početak komunikacije (SID C1)	266
2.2.2.3	Zahtjev za početak dijagnostičke razmjene podataka (SID 10)	266
2.2.2.4	Pozitivan odgovor za početak dijagnostike (SID 50)	266
2.2.2.5	Usluga upravljanja vezom (SID 87)	266
2.2.2.6	Pozitivan odgovor na zahtjev za upravljanje vezom (SID C7)	266
2.2.2.7	Zahtjev za prihvat podataka (SID 35)	266
2.2.2.8	Pozitivan odgovor na zahtjev za prihvat podataka (SID 75)	266
2.2.2.9	Zahtjev za prijenos podataka (SID 36)	266
2.2.2.10	Pozitivan odgovor za prijenos podataka (SID 76)	267
2.2.2.11	Zahtjev za prekid prijenosa (SID 37)	267
2.2.2.12	Pozitivan odgovor na zahtjev za prekid prijenosa (SID 77)	267
2.2.2.13	Zahtjev za prekid komunikacije (SID 82)	267
2.2.2.14	Pozitivan odgovor na zahtjev za prekid komunikacije (SID C2)	267
2.2.2.15	Potvrda dijela poruke (SID 83)	267
2.2.2.16	Negativan odgovor (SID 7F)	268
2.2.3	Tok poruke	268
2.2.4	Vremenski raspored	269
2.2.5	Obrada pogrešaka	270
2.2.5.1	Stadij početka komunikacije	270
2.2.5.2	Stadij komunikacije	270
2.2.6	Sadržaj poruke odgovora	272
2.2.6.1	Pozitivan odgovor za prijenos pregleda podataka	273
2.2.6.2	Pozitivan odgovor za prijenos podataka o aktivnostima	274
2.2.6.3	Pozitivan odgovor za prijenos podataka o događajima i pogreškama	275
2.2.6.4	Pozitivan odgovor za prijenos detaljnih podataka o brzini	276
2.2.6.5	Pozitivan odgovor za prijenos tehničkih podataka	276
2.3.	Spremanje datoteke ESM	277

3. PROTOKOL PREUZIMANJA PODATAKA S TAHOGRAFSKE KARTICE 277
3.1. Područje primjene 277
3.2. Definicije 277
3.3. Preuzimanje podataka s kartice 277
3.3.1 Slijed inicijalizacije 278
3.3.2 Slijed za nepotpisane podatkovne datoteke 278
3.3.3 Slijed za potpisane podatkovne datoteke 279
3.3.4 Slijed povrata brojača kalibracija u početno stanje 279
3.4. Format za pohranu podataka 280
3.4.1 Uvod 280
3.4.2 Format datoteke 280
4. PREUZIMANJE PODATAKA S TAHOGRAFSKE KARTICE PREKO JEDINICE U VOZILU 281

1. UVOD

U ovom se Dodatku navode postupci za obavljanje različitih vrsta preuzimanja podataka na vanjski medij za pohranu podataka (ESM) zajedno s protokolima koje treba provesti kako bi se osigurao ispravan prijenos podataka i potpuna sukladnost formata preuzetih podataka, čime se svakom nadzorniku omogućava da pregleda te podatke te da može kontrolirati njihovu autentičnost i cjelovitost prije analize.

1.1. **Područje primjene**

Podatci se mogu preuzeti na ESM:

— iz jedinice u vozilu posebnom namjenskom opremom (IDE) priključenom na jedinicu u vozilu (VU),

— s tahografske kartice putem opreme IDE opremljene napravom kartičnog sučelja (IFD),

— s tahografske kartice preko jedinice u vozilu putem IDE opreme priključene na VU.

Da bi se omogućila provjera autentičnosti i integriteta preuzetih podataka pohranjenih na ESM, podatci se preuzimaju potpisom stavljenim sukladno Dodatku 11. „Zajednički sigurnosni mehanizmi". Preuzimaju se i identifikacija uređaja izvora (jedinica u vozilu ili kartica) i njegovi sigurnosni certifikati (države članice i opreme). Onaj tko provjerava podatke mora posjedovati vlastiti pouzdan europski javni ključ.

DDP_001 Podatci preuzeti tijekom jednog procesa preuzimanja podataka moraju se pohraniti u ESM unutar jedne jedinstvene datoteke.

1.2. **Skraćenice i zabilješke**

U ovom se Dodatku upotrebljavaju sljedeće skraćenice:

AID identifikator aplikacije (eng. *Application Identifier*)

ATR odziv na povrat u početno stanje (eng. *Answer To Reset*)

CS bajt kontrolnog zbroja (eng. *Checksum Byte*)

DF namjenska datoteka (eng. *Dedicated File*)

DS_ dijagnostički proces (eng. *Diagnostic Session*)

EF elementarna datoteka (eng. *Elementary File*)

ESM vanjski medij za pohranu podataka (eng. *External Storage Medium*)

FID identifikator datoteke (eng. *File Identifier*) (ID datoteke (*File ID*))

FMT formatni bajt (eng. *Format Byte*) (prvi bajt zaglavlja poruke)

ICC kartica s integriranim krugovima (eng. *Integrated Circuit Card*)

IDE posebna namjenska oprema (eng. *Intelligent Dedicated Equipment*): oprema koja se upotrebljava za preuzimanje podataka na ESM (npr. osobno računalo)

IFD naprava sučelja (eng. *Interface Device*)

KWP protokol Keyword 2000 (eng. *Keyword Protocol 2000*)

LEN bajt duljine (eng. *Length Byte*) (posljednji bajt zaglavlja poruke)

PPS protokol odabira parametra (eng. *Protocol Parameter Selection*)

PSO izvođenje sigurnosne radnje (eng. *Perform Security Operation*)

SID identifikator usluge (eng. *Service Identifier*)

SRC izvorni bajt (eng. *Source Byte*)

TGT ciljni bajt (eng. *Target Byte*)

TLV vrijednost duljine oznake (eng. *Tag Length Value*)

TREP parametar odgovora za prijenos (eng. *Transfer Response Parameter*)

TRTP parametar zahtjeva za prijenos (eng. *Transfer Request Parameter*)

VU jedinica u vozilu (eng. *Vehicle Unit*)

2. PREUZIMANJE PODATAKA S JEDINICE U VOZILU (VU)

2.1. **Postupak preuzimanja podataka**

Za preuzimanje podataka s jedinice u vozilu korisnik mora obaviti sljedeće radnje:

— umetnuti svoju tahografsku karticu u utor jedinice u vozilu (*),

— priključiti IDE na priključak za preuzimanje podataka iz jedinice u vozilu,

— uspostaviti vezu između IDE-a i jedinice u vozilu,

— odabrati na IDE-u podatke za preuzimanje i poslati zahtjev jedinici u vozilu,

— zaključiti proces preuzimanja podataka.

2.2. **Protokol preuzimanja podataka**

Protokol je strukturiran na načelu nadređen-podređen, pri čemu IDE ima nadređenu, a jedinica u vozilu podređenu ulogu.

Struktura, vrste i tok poruka načelno su utemeljeni na protokolu Keyword 2000 (KWP) (ISO 14230-2 *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 2*: *Data link layer*).

Aplikacijska razina u načelu se temelji na sadašnjem nacrtu ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1*: *Diagnostic services*, verzija 6. od 22. veljače 2001.).

2.2.1 *Struktura poruke*

DDP_002 Sve poruke koje se razmjenjuju između IDE-a i jedinice u vozilu formatirane su u strukturi koja se sastoji od tri dijela:

— zaglavlja koje čine formatni bajt (FMT), ciljni bajt (TGT), izvorni bajt (SRC) i eventualno bajt za duljinu (LEN),

— podatkovnog polja koje čine bajt identifikatora usluge (SID) i promjenjivi broj podatkovnih bajtova koji može obuhvaćati neobavezni bajt dijagnostičke razmjene podataka (DS_) ili neobavezni bajt parametara prijenosa (TRTP ili TREP),

— kontrolnog zbroja koji čini bajt kontrolnog zbroja (CS).

Zaglavlje				Podatkovno polje					Kontrolni zbroj
FMT	TGT	SRC	LEN	SID	POD-ATCI	…	…	…	CS
4 bajta				najviše 255 bajtova					1 bajt

(*) Umetnuta će kartica aktivirati odgovarajuća prava pristupa funkciji preuzimanja podataka i samim podatcima. Međutim, mora biti moguće preuzeti podatke s kartice vozača umetnute u jedan od utora jedinice u vozilu ako nijedna druga kartica nije umetnuta u drugi utor.

Bajtovi TGT i SRC predstavljaju fizičku adresu primatelja i tvorca poruke. Vrijednosti su F0 Hex za IDE i EE Hex za jedinicu u vozilu.

Bajt LEN je duljina dijela podatkovnog polja.

Bajt kontrolnog zbroja je 8-bitni zbroj serije modula 256 svih bajtova poruke s izuzetkom samog kontrolnog zbroja.

Bajtovi FMT, SID, DS_, TRTP i TREP definirani su u nastavku ovog dokumenta.

DDP_003 Kada su podatci koje prenosi poruka dulji od raspoloživog prostora u dijelu podatkovnog polja, poruka se u stvarnosti šalje u nekoliko dijelova poruke. Svaki dio poruke nosi zaglavlje, isti SID, TREP i 2-bajtni brojač dijelova poruke koji označuje broj dijelova poruke u cjelokupnoj poruci. Kako bi se omogućilo provjeravanje pogrešaka i prekid, IDE potvrđuje svaki dio poruke. IDE može primiti dio poruke, tražiti da se ona ponovo prenese, zahtijevati od jedinice u vozilu da ponovo počne ili prekine prijenos.

DDP_004 Ako posljednji dio poruke sadržava točno 255 bajtova u podatkovnom polju, mora se staviti zadnji dio poruke s praznim podatkovnim poljem (osim SID TREP i brojača dijelova poruke) kako bi se označio kraj poruke.

Primjer:

Zaglavlje	SID	TREP	Poruka	CS
4 bajta	dulja od 255 bajtova			

Prenosi se kao:

Zaglavlje	SID	TREP	00	01	Dio poruke 1	CS
4 bajta	255 bajtova					

Zaglavlje	SID	TREP	00	02	Dio poruke 2	CS
4 bajta	255 bajtova					

…

Zaglavlje	SID	TREP	xx	yy	Dio poruke n	CS
4 bajta	kraća od 255 bajtova					

ili kao:

Zaglavlje	SID	TREP	00	01	Dio poruke 1	CS
4 bajta	255 bajtova					

Zaglavlje	SID	TREP	00	02	Dio poruke 2	CS
4 bajta	255 bajtova					

…

Zaglavlje	SID	TREP	xx	yy	Dio poruke n	CS
4 bajta	255 bajtova					

Zaglavlje	SID	TREP	xx	yy + 1	CS
4 bajta	4 bajta				

2.2.2 *Vrste poruka*

Komunikacijski protokol za preuzimanje podataka između jedinice u vozilu i IDE-a zahtijeva razmjenu osam različitih vrsta poruka.

U sljedećoj se tablici nalazi sažeti prikaz tih poruka.

Struktura poruke	Najviše 4 bajta Zaglavlje				Najviše 255 bajtova Podatci			1 bajt Kontrolni zbroj
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	PODATCI	CS
Zahtjev za početak komunikacije	81	EE	F0		81			E0
Pozitivan odgovor za početak komunikacije	80	F0	EE	03	C1		EA, 8F	9B
Zahtjev za početak dijagnostičke razmjene podataka	80	EE	F0	02	10	81		F1
Pozitivan odgovor za početak dijagnostičke razmjene podataka	80	F0	EE	02	50	81		31
Usluga upravljanja vezom Provjera brzine prijenosa podataka (stadij 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
Pozitivan odgovor na provjeru brzine prijenosa podataka	80	F0	EE	02	C7		01	28
Prijelazna brzina prijenosa podataka (stadij 2)	80	EE	F0	03	87		02,03	ED
Zahtjev za prihvat podataka	80	EE	F0	0A	35		00,00, 00,00, 00,FF,FF, FF,FF	99
Pozitivan odgovor na zahtjev za prihvat podataka	80	F0	EE	03	75		00,FF	D5

Struktura poruke	Najviše 4 bajta Zaglavlje				Najviše 255 bajtova Podatci			1 bajt Kontrolni zbroj
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	PODATCI	CS
Zahtjev za prijenos podataka								
Pregled	80	EE	F0	02	36	01		97
Aktivnosti	80	EE	F0	06	36	02	Datum	CS
Događaji i kvarovi	80	EE	F0	02	36	03		99
Detaljni podatci o brzini	80	EE	F0	02	36	04		9A
Tehnički podatci	80	EE	F0	02	36	05		9B
Preuzimanje podataka s kartice	80	EE	F0	02	36	06	Utor	CS
Pozitivan odgovor na zahtjev za prijenos podataka	80	F0	EE	Len	76	TREP	Podatci	CS
Zahtjev za prekid prijenosa podataka	80	EE	F0	01	37			96
Pozitivan odgovor na zahtjev za prekid prijenosa	80	F0	EE	01	77			D6
Zahtjev za prekid komunikacije	80	EE	F0	01	82			E1
Pozitivan odgovor za prekid komunikacije	80	F0	EE	01	C2			21
Potvrda dijela poruke	80	EE	F0	Len	83		Podatci	CS
Negativni odgovori								
Opće odbacivanje	80	F0	EE	03	7F	Sid Req	10	CS
Usluga nije podržana	80	F0	EE	03	7F	Sid Req	11	CS
Podfunkcija nije podržana	80	F0	EE	03	7F	Sid Req	12	CS
Neispravna duljina poruke	80	F0	EE	03	7F	Sid Req	13	CS
Uvjeti nisu ispravni ili pogreška u slijedu zahtjeva	80	F0	EE	03	7F	Sid Req	22	CS
Zahtjev izvan raspona	80	F0	EE	03	7F	Sid Req	31	CS
Prihvat podataka nije prihvaćen	80	F0	EE	03	7F	Sid Req	50	CS
Čekanje na odgovor	80	F0	EE	03	7F	Sid Req	78	CS
Podatci nisu dostupni	80	F0	EE	03	7F	Sid Req	FA	CS

Napomene:

— Sid Req = Sid odgovarajućeg zahtjeva.

— TREP = TRTP odgovarajućeg zahtjeva.

— Osjenčana polja označuju da se ne prenosi ništa.

— Izraz prihvat (s gledišta IDE-a) upotrebljava se zbog usklađenosti s normom ISO 14229. Znači isto što i preuzimanje podataka (s gledišta jedinice u vozilu).

— Potencijalni 2-bajtni brojači dijelova poruke nisu prikazani u ovoj tablici.

— Utor je broj utora, ili „1” (kartica u utoru vozača) ili „2” (kartica u utoru suvozača).

— U slučaju da utor nije naveden, jedinica u vozilu (VU) odabire utor 1 ako je kartica umetnuta u taj utor, dok utor 2 odabire samo kada je to izričito odabrao korisnik.

2.2.2.1 Zahtjev za početak komunikacije (SID 81)

DDP_005 Ovu poruku šalje IDE za uspostavljanje komunikacijske veze s jedinicom u vozilu. Početne komunikacije uvijek se obavljaju pri brzini od 9 600 bauda (dok se brzina prijenosa podataka eventualno ne promijeni upotrebom odgovarajućih usluga upravljanja vezom).

2.2.2.2 Pozitivan odgovor za početak komunikacije (SID C1)

DDP_006 Ovu poruku šalje jedinica u vozilu (VU) kao pozitivan odgovor na zahtjev za početak komunikacije. Ona sadržava 2 bajta ključa 'EA' '8F', koji označuju da jedinica podržava protokol sa zaglavljem koje sadržava podatke o ciljanom izvoru i duljini.

2.2.2.3 Zahtjev za početak dijagnostičke razmjene podataka (SID 10)

DDP_007 Poruku sa zahtjevom za početak dijagnostičke razmjene podataka šalje IDE radi davanja zahtjeva za novu dijagnostičku razmjenu podataka s jedinicom u vozilu. Podfunkcija „standardni proces" (81 Hex) označuje da je potrebno otvoriti standardnu dijagnostičku razmjenu podataka.

2.2.2.4 Pozitivan odgovor za početak dijagnostike (SID 50)

DDP_008 Poruku s pozitivnim odgovorom za početak dijagnostičke razmjene podataka šalje jedinica u vozilu (VU) kao pozitivan odgovor na zahtjev za početak dijagnostičke razmjene podataka.

2.2.2.5 Usluga upravljanja vezom (SID 87)

DDP_052 IDE upotrebljava uslugu upravljanja vezom za pokretanje postupka promjene brzine prijenosa podataka. Taj se postupak odvija u dva koraka. U prvom koraku IDE predlaže promjenu brzine prijenosa podataka navodeći novu brzinu. Po primitku pozitivne poruke iz jedinice u vozilu, IDE odašilje potvrdu promjene brzine prijenosa podataka u jedinicu u vozilu (drugi korak). IDE potom prelazi na novu brzinu prijenosa podataka. Po primitku potvrde jedinica u vozilu prelazi na novu brzinu prijenosa podataka.

2.2.2.6 Pozitivan odgovor na zahtjev za upravljanje vezom (SID C7)

DDP_053 Pozitivan odgovor na zahtjev za upravljanje vezom šalje jedinica u vozilu kao pozitivan odgovor na zahtjev za uslugu upravljanja vezom (prvi korak). Napominje se da nema odgovora na zahtjev za potvrdom (drugi korak).

2.2.2.7 Zahtjev za prihvat podataka (SID 35)

DDP_009 Poruku sa zahtjevom za prihvat podataka IDE šalje jedinici u vozilu kao obavijest da je zatražena radnja prihvata podataka. Za ispunjavanje zahtjeva norme ISO 14229 obuhvaćeni su podatci koji sadržavaju pojedinosti o adresi, veličini i formatu zatraženih podataka. S obzirom na to da su oni za IDE nepoznati prije preuzimanja podataka, adresa memorije postavlja se na 0, format je nešifriran i nekomprimiran i veličina memorije je postavljena na maksimum.

2.2.2.8 Pozitivan odgovor na zahtjev za prihvat podataka (SID 75)

DDP_010 Poruku s pozitivnim odgovorom na zahtjev za prihvat podataka jedinica u vozilu šalje IDE-u kao obavijest da je jedinica u vozilu spremna za preuzimanje podataka. Za ispunjenje zahtjeva norme ISO 14229, u toj se poruci s pozitivnim odgovorom navode podatci koji obavještavaju IDE da će daljnje poruke s pozitivnim odgovorom na zahtjev za prijenos podataka sadržavati najviše 00FFh bajtova.

2.2.2.9 Zahtjev za prijenos podataka (SID 36)

DDP_011 Zahtjev za prijenos podataka IDE šalje jedinici u vozilu kao obavijest o vrsti podataka koje treba preuzeti. Jednobajtni parametar zahtjeva za prijenos podataka (TRTP) označuje vrstu prijenosa.

Postoji šest vrsta prijenosa podataka:

— pregled (TRTP 01),

— aktivnosti navedenog dana (TRTP 02),

— događaji i pogreške (TRTP 03),

— detaljni podatci o brzini (TRTP 04),

— tehnički podatci (TRTP 05),

— preuzimanje podataka s kartice (TRTP 06).

DDP_054 IDE mora obavezno zahtijevati prijenos pregleda podataka (TRTP 01) tijekom procesa preuzimanja podataka s obzirom na to da se samo time osigurava da se certifikati jedinice u vozilu zabilježe unutar preuzete datoteke (i omogućava provjera digitalnog potpisa).

U drugom slučaju (TRTP 02), poruka sa zahtjevom za prijenos podataka obuhvaća oznaku kalendarskog dana (u formatu `TimeReal`) za koji treba preuzeti podatke.

2.2.2.10 Pozitivan odgovor za prijenos podataka (SID 76)

DDP_012 Pozitivan odgovor za prijenos podataka šalje jedinica u vozilu kao odgovor na zahtjev za prijenos podataka. Poruka sadržava zahtijevane podatke s parametrom odgovora za prijenos (TREP) koji odgovara TRTP-u zahtjeva.

DDP055 U prvom slučaju (TREP 01), jedinica u vozilu poslat će podatke koji pomažu operatoru IDE-a da izabere podatke koje želi dalje preuzeti. Ta poruka sadržava sljedeće informacije:

— sigurnosni certifikati,

— identifikacija vozila,

— trenutačni datum i vrijeme jedinice u vozilu,

— najkasniji i najraniji datum na koji je moguće preuzeti podatke (podatci iz jedinice u vozilu),

— oznaka prisustva kartice u jedinici u vozilu,

— prethodno preuzimanje podataka od strane poduzeća,

— blokade poduzeća,

— prethodne kontrole.

2.2.2.11 Zahtjev za prekid prijenosa (SID 37)

DDP_013 Zahtjev za prekid prijenosa IDE šalje jedinici u vozilu kao obavijest da je proces preuzimanja podataka završen.

2.2.2.12 Pozitivan odgovor na zahtjev za prekid prijenosa (SID 77)

DDP_014 Poruku s pozitivnim odgovorom na zahtjev za prekid prijenosa jedinica u vozilu šalje kao potvrdu zahtjeva za prekid prijenosa.

2.2.2.13 Zahtjev za prekid komunikacije (SID 82)

DDP_015 Poruku sa zahtjevom za prekid komunikacije IDE šalje za prekid komunikacijske veze s jedinicom u vozilu.

2.2.2.14 Pozitivan odgovor na zahtjev za prekid komunikacije (SID C2)

DDP_016 Poruku s pozitivnim odgovorom za prekid komunikacije jedinica u vozilu šalje kao potvrdu zahtjeva za prekid komunikacije.

2.2.2.15 Potvrda dijela poruke (SID 83)

DDP_017 Potvrdu dijela poruke IDE šalje za potvrdu primitka svakog dijela poruke koja se prenosi u više dijelova. Podatkovno polje sadrži SID koji se prima od jedinice u vozilu i 2-bajtni kod kako slijedi:

— MsgC + 1 potvrđuje ispravan primitak broja dijela poruke MsgC.

IDE šalje zahtjev jedinici u vozilu da pošalje sljedeći dio poruke.

— MsgC ukazuje na problem s primitkom broja dijela poruke MsgC.

IDE ponovno šalje zahtjev jedinici u vozilu da pošalje taj dio poruke.

— FFFF zahtijeva kraj poruke.

Tim se postupkom IDE može služiti za okončanje prijenosa poruke iz jedinice u vozilu iz bilo kojeg razloga.

Posljednji dio neke poruke (bajt LEN < 255) može se potvrditi bilo kojim od navedenih kodova ili se ne mora potvrditi.

Odgovori jedinice u vozilu koji se sastoje od više dijelova poruke sljedeći su:

— Pozitivan odgovor za prijenos podataka (SID 76).

2.2.2.16 Negativan odgovor (SID 7F)

DDP_018 Poruku s negativnim odgovorom jedinica u vozilu šalje kao odgovor na prethodno navedene poruke zahtjeva ako jedinica u vozilu ne može udovoljiti zahtjevu. Podatkovna polja poruke sadržavaju SID odgovora (7F), SID zahtjeva i kod koji označuje razlog za negativan odgovor. Na raspolaganju su sljedeći kodovi:

— 10 opće odbacivanje

Radnja se ne može obaviti zbog razloga koji nije naveden u nastavku.

— 11 usluga nije podržana

SID zahtjeva nije razumljiv.

— 12 podfunkcija nije podržana

DS_ ili TRTP zahtjeva nije razumljiv ili nema daljnjih dijelova poruke koje treba prenijeti.

— 13 neispravna duljina poruke

Duljina primljene poruke pogrešna je.

— 22 uvjeti nisu ispravni ili pogreška u slijedu zahtjeva

Zahtijevana usluga nije aktivna ili slijed poruka zahtjeva nije ispravan.

— 31 zahtjev izvan raspona

Zapis parametra zahtjeva (podatkovno polje) nije valjan.

— 50 prihvat podataka nije prihvaćen

Zahtjev se ne može izvršiti (jedinica u vozilu u neprimjerenom načinu rada ili unutarnja pogreška jedinice u vozilu).

— 78 čekanje na odgovor

Zahtijevana radnja ne može se pravovremeno dovršiti i jedinica u vozilu nije spremna za prihvaćanje drugog zahtjeva.

— FA podatci nisu dostupni

Podatkovni objekt zahtjeva za prijenos podataka nije dostupan u jedinici u vozilu (npr. nije umetnuta kartica…).

2.2.3 *Tok poruke*

Tipičan tok poruke tijekom redovnog postupka preuzimanja podataka sljedeći je:

IDE		VU
Zahtjev za početak komunikacije	⇨ ⇦	Pozitivan odgovor
Zahtjev za početak dijagnostičke usluge	⇨ ⇦	Pozitivan odgovor
Zahtjev za prihvat podataka	⇨ ⇦	Pozitivan odgovor

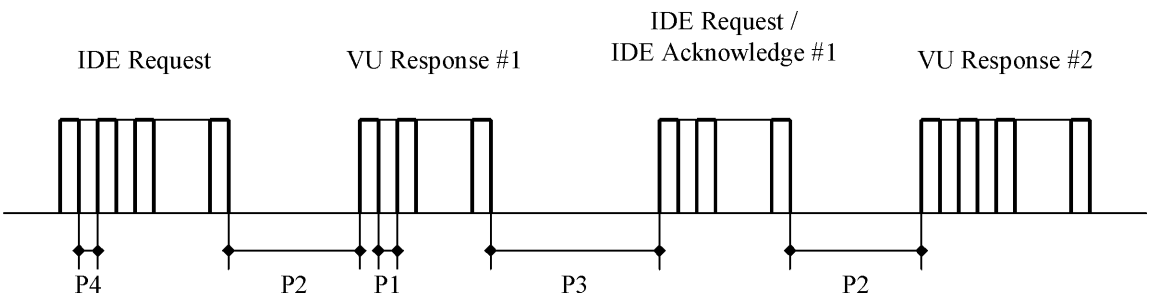
IDE		VU
Zahtjev za prijenos pregleda podataka	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prijenos podataka #2	⇨	
	⇦	Pozitivan odgovor #1
Potvrda dijela poruke #1	⇨	
	⇦	Pozitivan odgovor #2
Potvrda dijela poruke #2	⇨	
	⇦	Pozitivan odgovor #m
Potvrda dijela poruke #m	⇨	
	⇦	Pozitivan odgovor (podatkovno polje < 255 bajtova)
Potvrda dijela poruke (neobvezno)	⇨	
...		
Zahtjev za prijenos podataka #n	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prekid prijenosa podataka	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prekid komunikacije	⇨	
	⇦	Pozitivan odgovor

2.2.4 *Vremenski raspored*

DDP_019 Tijekom redovnog rada mjerodavni su vremenski parametri prikazani na sljedećoj slici:

Slika 1.

Tok poruke, vremenski raspored



Gdje je:

P1 = međubajtno vrijeme za odgovor jedinice u vozilu (VU),

P2 = vrijeme između kraja zahtjeva IDE-a i početka odgovora jedinice u vozilu, ili između kraja potvrde IDE-a i početka sljedećeg odgovora jedinice u vozilu,

P3 = vrijeme između kraja odgovora jedinice u vozilu i početka novog zahtjeva IDE-a ili između kraja odgovora jedinice u vozilu i početka potvrde IDE-a, ili između kraja zahtjeva IDE-a i početka novog zahtjeva IDE-a ako jedinica u vozilu ne odgovori,

P4 = međubajtno vrijeme za zahtjev IDE-a,

P5 = produljena vrijednost P3 za preuzimanje podataka s kartice.

Dopuštene vrijednosti vremenskih parametara prikazane su u sljedećoj tablici (prošireni niz vremenskih parametara KWP, upotrebljava se u slučaju fizičkog adresiranja za bržu komunikaciju).

Vremenski parametar	Donja granična vrijednost (ms)	Gornja granična vrijednost (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minuta

(*) Ako jedinica u vozilu pošalje negativan odgovor s kodom koji znači „zahtjev uredno primljen, čekanje na odgovor", ta se vrijednost proteže na istu gornju graničnu vrijednost P3.

2.2.5 *Obrada pogrešaka*

Ako tijekom razmjene poruka dođe do pogreške, shema toka poruke mijenja se ovisno o tome koja je oprema utvrdila pogrešku i o poruci koja uzrokuje pogrešku.

Na slikama 2. i 3. prikazani su postupci obrade pogrešaka za jedinicu u vozilu odnosno IDE.

2.2.5.1 Stadij početka komunikacije

DDP_020 Ako IDE utvrdi pogrešku u stadiju početka komunikacije u vezi s vremenom ili protokom bitova, čekat će u trajanju od najmanje P3 prije ponovnog izdavanja zahtjeva.

DDP_021 Ako jedinica u vozilu utvrdi pogrešku u slijedu koji dolazi iz IDE-a, ona neće poslati odgovor i čekat će u trajanju od najviše P3 drugu poruku sa zahtjevom za početak komunikacije.

2.2.5.2 Stadij komunikacije

Mogu se odrediti dva različita područja obrade pogrešaka:

1. **Jedinica u vozilu utvrđuje pogrešku prijenosa iz IDE-a.**

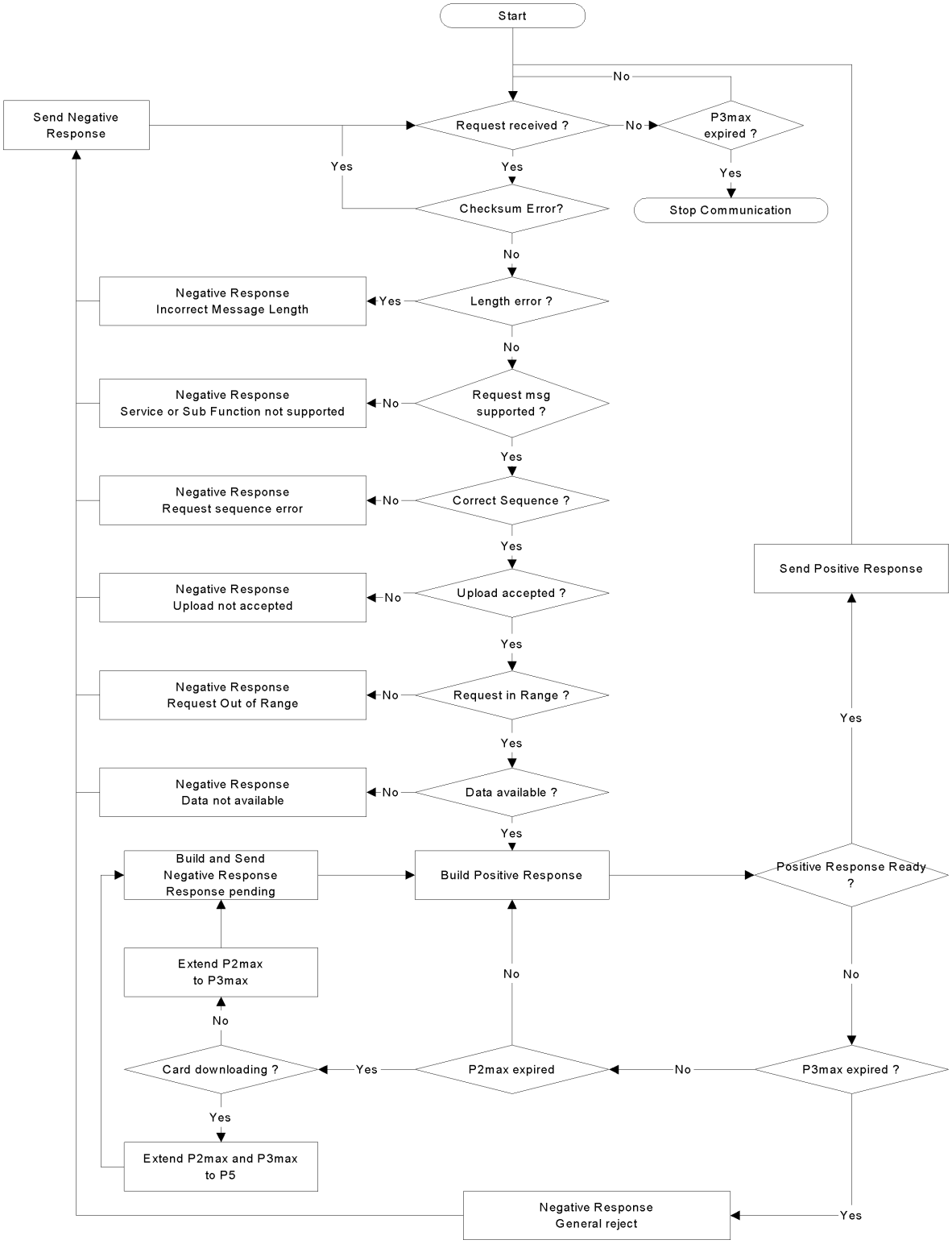
DDP_022 Za svaku primljenu poruku jedinica u vozilu utvrđuje pogreške u vezi s vremenom, pogreške formata bajta (npr. kršenje početnog i zaustavnog bita) i greške pri upisu (pogrešan broj primljenih bajtova, pogrešan bajt kontrolnog zbroja).

DDP_023 Ako jedinica u vozilu utvrdi jednu od prethodno navedenih pogrešaka, ona ne šalje nikakav odgovor i zanemaruje primljenu poruku.

DDP_024 Jedinica u vozilu može utvrditi ostale pogreške u formatu ili sadržaju primljene poruke (npr. poruka nije podržana) čak i ako poruka udovoljava zahtjevima duljine i kontrolnog zbroja; u tom slučaju jedinica u vozilu odgovara IDE-u porukom s negativnim odgovorom u kojoj se navodi narav pogreške.

Slika 2.

Obrada pogrešaka u jedinici u vozilu



2. **IDE utvrđuje pogrešku prijenosa iz jedinice u vozilu.**

DDP_025 Za svaku primljenu poruku IDE utvrđuje pogreške povezane s vremenom, pogreške formata bajta (npr. kršenje početnog i zaustavnog bita) i greške pri upisu (pogrešan broj primljenih bajtova, pogrešan bajt kontrolnog zbroja).

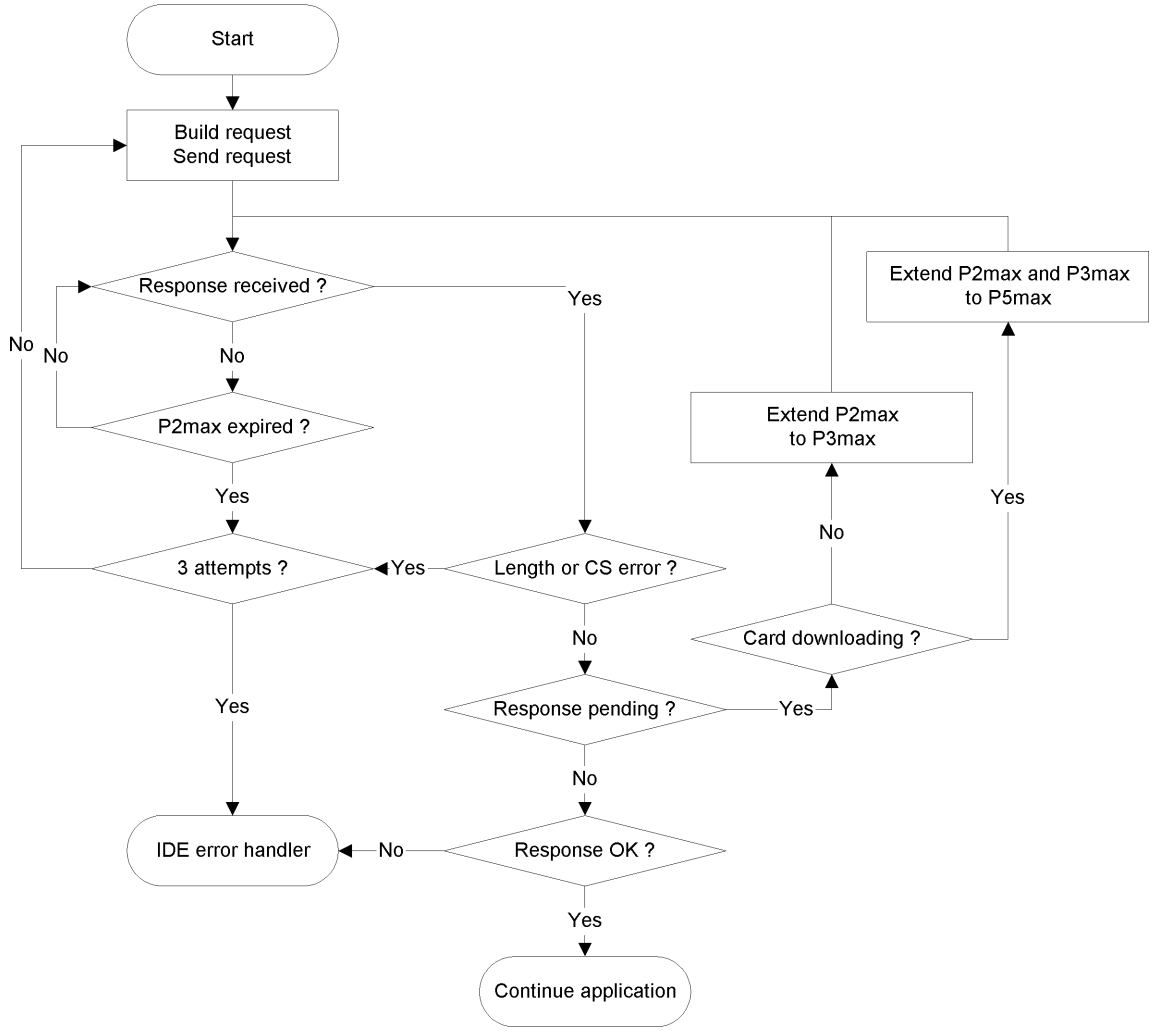
DDP_026 IDE utvrđuje pogreške u slijedu, npr. neispravan korak povećanja brojača dijelova poruke za sljedeće primljene poruke.

DDP_027 Ako IDE utvrdi pogrešku ili nema odgovora iz jedinice u vozilu u trajanju od najviše P2, ponovo će poslati poruku sa zahtjevom za najviše tri prijenosa ukupno. Za potrebe utvrđivanja te pogreške, potvrda dijela poruke smatrat će se zahtjevom upućenim jedinici u vozilu.

DDP_028 IDE mora čekati u trajanju od najmanje P3 prije početka svakog prijenosa; razdoblje čekanja mjeri se od posljednjeg izračunanog javljanja zaustavnog bita nakon otkrivanja pogreške.

Slika 3.

Obrada pogrešaka u IDE-u



2.2.6 *Sadržaj poruke odgovora*

U ovom se stavku navodi sadržaj podatkovnih polja različitih poruka s pozitivnim odgovorom.

Podatkovni elementi definirani su u rječniku podataka u Dodatku 1.

Napomena: Za preuzimanja podataka druge generacije, svaki podatkovni element gornje razine predstavlja se nizom zapisa (eng. *record array*), čak i ako sadržava samo jedan zapis. Niz zapisa počinje zaglavljem; to zaglavlje sadržava vrstu, veličinu i broj zapisa. Nizovi zapisa navode se kao „…niz zapisa" (sa zaglavljem) u tablicama u nastavku.

2.2.6.1 Pozitivan odgovor za prijenos pregleda podataka

DDP_029 Podatkovno polje poruke „pozitivnog odgovora za prijenos pregleda podataka" pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 01h te odgovarajućoj podjeli na dijelove i brojanju dijelova poruke:

Struktura podataka prve generacije

Podatkovni element	Komentar
MemberStateCertificate VUCertificate	Sigurnosni certifikati jedinice u vozilu
VehicleIdentificationNumber VehicleRegistrationIdentification	Identifikacija vozila
CurrentDateTime	Trenutačni datum i vrijeme jedinice u vozilu
VuDownloadablePeriod	Razdoblje u kojem je moguće preuzimati podatke
CardSlotsStatus	Vrsta kartica umetnutih u jedinicu u vozilu
VuDownloadActivityData	Prethodno preuzimanje podataka iz jedinice u vozilu
VuCompanyLocksData	Sve blokade poduzeća koje su pohranjene. Ako je odjeljak prazan, šalje se samo noOfLocks = 0.
VuControlActivityData	Svi kontrolni zapisi koji su pohranjeni u jedinici u vozilu. Ako je odjeljak prazan, šalje se samo noOfControls = 0.
Signature	RSA potpis svih podataka (osim certifikata) od VehicleIdentificationNumber do posljednjeg bajta zadnjeg VuControlActivityData.

Struktura podataka druge generacije

Podatkovni element	Komentar
MemberStateCertificateRecordArray	Certifikat države članice
VUCertificateRecordArray	Certifikat jedinice u vozilu
VehicleIdentificationNumberRecordArray	Identifikacija vozila
VehicleRegistrationNumberRecordArray	Registracijski broj vozila
CurrentDateTimeRecordArray	Trenutačni datum i vrijeme jedinice u vozilu
VuDownloadablePeriodRecordArray	Razdoblje u kojem je moguće preuzimati podatke
CardSlotsStatusRecordArray	Vrsta kartica umetnutih u jedinicu u vozilu
VuDownloadActivityDataRecordArray	Prethodno preuzimanje podataka iz jedinice u vozilu
VuCompanyLocksRecordArray	Sve blokade poduzeća koje su pohranjene. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuControlActivityRecordArray	Svi kontrolni zapisi koji su pohranjeni u jedinici u vozilu. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
SignatureRecordArray	ECC potpis svih prethodnih podataka osim certifikata.

2.2.6.2 Pozitivan odgovor za prijenos podataka o aktivnostima

DDP_030 Podatkovno polje poruke „pozitivnog odgovora za prijenos podataka o aktivnostima" pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 02h te odgovarajućoj podjeli na dijelove i brojanju dijelova poruke:

Struktura podataka prve generacije

Podatkovni element	Komentar
TimeReal	Datum dana preuzimanja podataka.
OdometerValueMidnight	Stanje brojača kilometara na kraju dana preuzimanja podataka.
VuCardIWData	Podatci o broju ciklusa umetanja i izvlačenja kartice. — Ako je odjeljak prazan, šalje se samo noOfVuCardIWRecords = 0. — Kada se zapis VuCardIWRecord proteže preko 00:00 (umetanje kartice prethodnog dana) ili preko 24:00 (izvlačenje kartice sljedećeg dana), pojavljuje se u cijelosti u oba navedena dana.
VuActivityDailyData	Stanje utora u 00:00 i promjene aktivnosti zabilježene na dan preuzimanja podataka.
VuPlaceDailyWorkPeriodData	Podatci koji se odnose na mjesta zabilježeni na dan preuzimanja podataka. Ako je odjeljak prazan, šalje se samo noOfPlaceRecords = 0.
VuSpecificConditionData	Podatci o posebnim stanjima zabilježeni na dan preuzimanja podataka. Ako je odjeljak prazan, šalje se samo noOfSpecificConditionRecords = 0.
Signature	RSA potpis svih podataka od TimeReal do posljednjeg bajta zadnjeg zapisa o posebnom stanju.

Struktura podataka druge generacije

Podatkovni element	Komentar
DateOfDayDownloadedRecordArray	Datum dana preuzimanja podataka.
OdometerValueMidnightRecordArray	Stanje brojača kilometara na kraju dana preuzimanja podataka.
VuCardIWRecordArray	Podatci o broju ciklusa umetanja i izvlačenja kartice. — Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0. — Kada se zapis VuCardIWRecord proteže preko 00:00 (umetanje kartice prethodnog dana) ili preko 24:00 (izvlačenje kartice sljedećeg dana), pojavljuje se u cijelosti u oba navedena dana.
VuActivityDailyRecordArray	Stanje utora u 00:00 i promjene aktivnosti zabilježene na dan preuzimanja podataka.
VuPlaceDailyWorkPeriodRecordArray	Podatci koji se odnose na mjesta zabilježeni na dan preuzimanja podataka. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuGNSSCDRecordArray	GNSS položaji vozila ako neprekidno vrijeme vožnje vozača premaši višekratnik tri sata. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuSpecificConditionRecordArray	Podatci o posebnim stanjima zabilježeni na dan preuzimanja podataka. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
SignatureRecordArray	ECC potpis svih prethodnih podataka.

2.2.6.3 Pozitivan odgovor za prijenos podataka o događajima i pogreškama

DDP_031 Podatkovno polje poruke „pozitivnog odgovora za prijenos podataka o događajima i pogreškama" pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 03h te odgovarajućoj podjeli na dijelove i brojanju dijelova poruke:

Struktura podataka prve generacije

Podatkovni element	Komentar
VuFaultData	Sve pogreške koje su pohranjene ili još uvijek traju u jedinici u vozilu. Ako je odjeljak prazan, šalje se samo noOfVuFaults = 0.
VuEventData	Svi događaji (osim prekoračenja brzine) koji su pohranjeni ili još uvijek traju u jedinici u vozilu. Ako je odjeljak prazan, šalje se samo noOfVuEvents = 0.
VuOverSpeedingControlData	Podatci koji se odnose na posljednju kontrolu prekoračenja brzine (standardna vrijednost ako nema podataka).
VuOverSpeedingEventData	Svi događaji u pogledu prekoračenja brzine koji su pohranjeni u jedinici u vozilu. Ako je odjeljak prazan, šalje se samo noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Svi događaji o prilagodbi vremena koji su pohranjeni u jedinici u vozilu (izvan okvira pune kalibracije). Ako je odjeljak prazan, šalje se samo noOfVuTimeAdjRecords = 0.
Signature	RSA potpis svih podataka od noOfVuFaults do posljednjeg bajta zadnjeg zapisa o prilagodbi vremena.

Struktura podataka druge generacije

Podatkovni element	Komentar
VuFaultRecordArray	Sve pogreške koje su pohranjene ili još uvijek traju u jedinici u vozilu. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuEventRecordArray	Svi događaji (osim prekoračenja brzine) koji su pohranjeni ili još uvijek traju u jedinici u vozilu. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Podatci koji se odnose na posljednju kontrolu prekoračenja brzine (standardna vrijednost ako nema podataka).
VuOverSpeedingEventRecordArray	Svi događaji u pogledu prekoračenja brzine koji su pohranjeni u jedinici u vozilu. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuTimeAdjustmentRecordArray	Svi događaji o prilagodbi vremena koji su pohranjeni u jedinici u vozilu (izvan okvira pune kalibracije). Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	ECC potpis svih prethodnih podataka.

2.2.6.4 Pozitivan odgovor za prijenos detaljnih podataka o brzini

DDP_032 Podatkovno polje poruke „pozitivan odgovor za prijenos detaljnih podataka o brzini" pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 04 Hex te odgovarajućoj podjeli na dijelove i brojanju dijelova poruke:

Struktura podataka prve generacije

Podatkovni element	Komentar
VuDetailedSpeedData	Svi detaljni podatci o brzini koji su pohranjeni u jedinici u vozilu (jedan blok brzine u minuti tijekom koje se vozilo kretalo). 60 vrijednosti brzine u minuti (jedna u sekundi).
Signature	RSA potpis svih podataka od noOfSpeedBlocks do posljednjeg bajta zadnjeg bloka brzine.

Struktura podataka druge generacije

Podatkovni element	Komentar
VuDetailedSpeedBlockRecordArray	Svi detaljni podatci o brzini koji su pohranjeni u jedinici u vozilu (jedan blok brzine u minuti tijekom koje se vozilo kretalo). 60 vrijednosti brzine u minuti (jedna u sekundi).
SignatureRecordArray	ECC potpis svih prethodnih podataka.

2.2.6.5 Pozitivan odgovor za prijenos tehničkih podataka

DDP_033 Podatkovno polje „pozitivnog odgovora za prijenos tehničkih podataka" pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 05h te odgovarajućoj podjeli na dijelove i brojanju dijelova poruke:

Struktura podataka prve generacije

Podatkovni element	Komentar
VuIdentification	
SensorPaired	
VuCalibrationData	Svi zapisi o kalibraciji koji su pohranjeni u jedinici u vozilu.
Signature	RSA potpis svih podataka od vuManufacturerName do posljednjeg bajta zadnjeg VuCalibrationRecord.

Struktura podataka druge generacije

Podatkovni element	Komentar
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Sva uparivanja država članica pohranjena u jedinici u vozilu.
VuSensorExternalGNSSCoupledRecordArray	Sva spajanja vanjskih uređaja GNSS-a pohranjena u jedinici u vozilu.
VuCalibrationRecordArray	Svi zapisi o kalibraciji koji su pohranjeni u jedinici u vozilu.
VuCardRecordArray	Svi podatci o umetanju kartice koji su pohranjeni u jedinici u vozilu.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	ECC potpis svih prethodnih podataka.

2.3. **Spremanje datoteke ESM**

DDP_034 Ako je proces preuzimanja podataka obuhvatio i prijenos podataka iz jedinice u vozilu, IDE unutar jedne fizičke datoteke pohranjuje sve podatke primljene iz jedinice u vozilu tijekom procesa preuzimanja podataka u okviru poruka s pozitivnim odgovorom na zahtjev za prijenos podataka. Pohranjeni podatci ne sadržavaju zaglavlja poruka, brojače dijelova poruke, prazne dijelove poruka i kontrolne zbrojeve, ali obuhvaćaju SID i TREP (prvog dijela poruke samo ako ima više dijelova poruka).

3. PROTOKOL PREUZIMANJA PODATAKA S TAHOGRAFSKE KARTICE

3.1. **Područje primjene**

U ovom se stavku opisuje izravno preuzimanje podataka s tahografske kartice na IDE. IDE nije dio sigurnog okruženja; stoga se ne provodi nikakva autentifikacija između kartice i IDE-a.

3.2. **Definicije**

Proces preuzimanja podataka: svaki put kad se obavlja preuzimanje podataka s ICC-a. Proces obuhvaća cjelokupan postupak od povrata u početno stanje ICC-a od strane IFD-a do deaktivacije ICC-a (izvlačenje kartice ili sljedeći povrat u početno stanje).

Potpisana podatkovna datoteka: datoteka iz ICC-a. Datoteka se prenosi na IFD u običnom tekstu. Na ICC-u datoteka se raspršuje (*hash*) i potpisuje, a potpis se prenosi na IFD.

3.3. **Preuzimanje podataka s kartice**

DDP_035 Preuzimanje podataka s tahografske kartice obuhvaća sljedeće korake:

— Preuzimanje zajedničkih podataka kartice u EF-ovima `ICC` i `IC`. Ovi su podatci neobvezni i nisu zaštićeni digitalnim potpisom,

— Preuzimanje EF-ova `Card_Certificate` (ili `CardSignCertificate`) i `CA_Certificate`. Ovaj podatak nije zaštićen digitalnim potpisom.

Obvezno je preuzeti ove datoteke u svakom procesu preuzimanja podataka.

— Preuzimanje EF-ova podataka drugih aplikacija (unutar `Tachograph DF` i `Tachograph_G2 DF` prema potrebi) osim EF-a `Card_Download`. Ovi su podatci zaštićeni digitalnim potpisom.

— U svakom je procesu preuzimanja podataka obvezno preuzeti EF-ove `Application_Identification` i `ID`.

— Prilikom preuzimanja podataka s kartice vozača isto je tako obvezno preuzeti sljedeće EF-ove:

- Events_Data;
- Faults_Data;
- Driver_Activity_Data;
- Vehicles_Used;
- Places;
- GNSS_Places (if relevant);
- Control_Activity_Data;
- Specific_Conditions.

— Prilikom preuzimanja podataka s kartice vozača, ažuriranje datuma LastCardDownload EF-u Card_Download,

— Prilikom preuzimanja podataka s kartice radionice, povrat u početno stanje brojača kalibracija u EF-u Card_Download.

— Prilikom preuzimanja podataka s kartice radionice ne preuzima se EF Sensor_Installation_Data.

3.3.1 *Slijed inicijalizacije*

DDP_036 IDE započinje sljedeći slijed:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	Povrat hardvera u početno stanje	
ATR	⇨		

Za prijelaz na višu brzinu prijenosa podataka može se upotrijebiti PPS ako ICC to podržava.

3.3.2 *Slijed za nepotpisane podatkovne datoteke*

DDP_037 Slijed za preuzimanje EF-ova ICC, IC, Card_Certificate (ili CardSignCertificate) i CA_Certificate je sljedeći:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	**Odabir datoteke (*Select File*)**	Odabir s pomoću identifikatora datoteke
OK	⇨		
	⇦	**Čitanje datoteke (*Read Binary*)**	Ako datoteka sadržava više podataka nego što je veličina međumemorije čitača ili kartice, naredba se ponavlja dok se ne pročita cijela datoteka.
File Data **OK**	⇨	Pohrana podataka na ESM	prema **3.4.** Format za pohranu podataka

Napomena 1.: prije odabira EF-a Card_Certificate (ili CardSignCertificate), mora se odabrati tahografska aplikacija (odabir putem AID-a).

Napomena 2.: odabir i čitanje datoteke isto se tako može obaviti u jednom koraku naredbom READ BINARY (čitanje datoteke) s kratkim identifikatorom EF-a.

3.3.3 *Slijed za potpisane podatkovne datoteke*

DDP_038 Za svaku od sljedećih datoteka koje treba preuzeti s njihovim potpisom upotrebljava se sljedeći slijed:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	**Odabir datoteke (*Select File*)**	
OK	⇨		
	⇦	**Raspršivanje datoteke (*Perform Hash of File*)**	Izračunava vrijednost raspršivanja sadržaja podataka odabrane datoteke upotrebom propisanog algoritma raspršivanja u skladu s Dodatkom 11. Ova naredba nije ISO-naredba.
Izračun vrijednosti raspršivanja datoteke i privremeno pohranjivanje vrijednosti raspršivanja			
OK	⇨		
	⇦	**Čitanje datoteke (*Read Binary*)**	Ako datoteka sadržava više podataka nego što međumemorija čitača ili kartice može primiti, naredba se ponavlja dok se ne pročita cijela datoteka.
Podatci o datoteci (*File Data*) **OK**	⇨	Pohrana primljenih podataka na ESM	prema **3.4.** Format za pohranu podataka
	⇦	**PSO: Izračun digitalnog potpisa (*Compute Digital Signature*)**	
Zaštitna radnja „izračuna digitalnog potpisa" upotrebom privremeno pohranjene vrijednosti raspršivanja (*hash*)			
Potpis (*Signature*) **OK**	⇨	Podatci se pridodaju podatcima koji su prethodno pohranjeni na ESM.	prema **3.4.** Format za pohranu podataka

Napomena: odabir i čitanje datoteke isto se tako može obaviti u jednom koraku naredbom READ BINARY (čitanje datoteke) s kratkim identifikatorom EF-a. U tom se slučaju EF može odabrati i pročitati prije primjene naredbe PERFORM HASH OF FILE (raspršivanje datoteke).

3.3.4 *Slijed povrata brojača kalibracija u početno stanje*

DDP_039 Slijed povrata u početno stanje brojača `NoOfCalibrationsSinceDownload` u EF-u `Card_Download` na kartici radionice je sljedeći:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	**Odabir datoteke (*Select File*)** EF Card_Download	Odabir s pomoću identifikatora datoteke
OK	⇨		

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	**Ažuriranje datoteke (*Update Binary*)** NoOfCalibrationsSinceDownload = '00 00'	
Povrat u početno stanje broja preuzimanja podataka s kartice			
OK	⇨		

Napomena: odabir i ažuriranje datoteke isto se tako može obaviti u jednom koraku naredbom READ BINARY (čitanje datoteke) s kratkim identifikatorom EF-a.

3.4. **Format za pohranu podataka**

3.4.1 *Uvod*

DDP_040 Preuzeti podatci pohranjuju se u skladu sa sljedećim uvjetima:

— podatci se pohranjuju transparentno. To znači da se poredak bajtova kao i poredak bitova unutar bajtova koji se prenose s kartice mora očuvati tijekom pohranjivanja,

— sve datoteke s kartice koje su preuzete tijekom procesa preuzimanja podataka pohranjuju se u jednoj datoteci na ESM.

3.4.2 *Format datoteke*

DDP_041 Format datoteke lanac je više TLV objekata.

DDP_042 Oznaka za EF je FID plus dodatak „00”.

DDP_043 Oznaka za potpis EF-a je FID datoteke plus dodatak „01”.

DDP_044 Duljina je dvobajtna vrijednost. Vrijednost određuje broj bajtova u polju vrijednosti. Vrijednost „FF FF” u polju duljine rezervirana je za buduću upotrebu.

DDP_045 Ako datoteka nije preuzeta, ništa što se odnosi na datoteku ne smije se pohraniti (nikakva oznaka i nikakva nulta duljina).

DDP_046 Potpis se pohranjuje kao sljedeći TLV objekt izravno nakon TLV objekta koji sadržava podatke datoteke.

Definicija	Značenje	Duljina
FID (2 bajta) || „00”	Oznaka za EF (FID)	3 bajta
FID (2 bajta) || „01”	Oznaka za potpis EF-a (FID)	3 bajta
xx xx	Duljina polja vrijednosti	2 bajta

Primjer podataka u datoteci preuzetoj na ESM

Oznaka	Duljina	Vrijednost
00 02 00	00 11	Podatci EF-a ICC
C1 00 00	00 C2	Podatci EF-a Card_Certificate
		…
05 05 00	0A 2E	Podatci EF-a Vehicles_Used
05 05 01	00 80	Potpis EF-a Vehicles_Used

4. PREUZIMANJE PODATAKA S TAHOGRAFSKE KARTICE PREKO JEDINICE U VOZILU

DDP_047 Jedinica u vozilu mora omogućiti preuzimanje sadržaja s kartice vozača umetnute u priključeni IDE.

DDP_048 IDE jedinici u vozilu šalje poruku „zahtjev za prijenos podataka s kartice" za pokretanje tog načina rada (vidjeti 2.2.2.9).

DDP_049 Jedinica u vozilu potom preuzima sve podatke s kartice, datoteku po datoteku, u skladu s protokolom preuzimanja s kartice definiranim u stavku 3 i dostavlja sve podatke primljene s kartice na IDE u odgovarajućem formatu datoteke TLV (vidjeti 3.4.2) i sažete unutar poruke „pozitivan odgovor za prijenos podataka".

DDP_050 IDE uzima podatke s kartice iz poruke „pozitivan odgovor za prijenos podataka" (bez svih zaglavlja, SID-ova, TREP-ova, brojača dijelova poruke i kontrolnih zbrojeva) i pohranjuje ih u jednu fizičku datoteku kako je opisano u stavku 2.3.

DDP_051 Jedinica u vozilu nakon toga, prema potrebi, ažurira datoteku `Control_Activity_Data` ili `Card_Download` s kartice vozača.

Dodatak 8

PROTOKOL KALIBRACIJE

SADRŽAJ

1. UVOD 283
2. IZRAZI, DEFINICIJE I REFERENTNI DOKUMENTI 283
3. PREGLED USLUGA 284
3.1. Raspoložive usluge 284
3.2. Kodovi odgovora 285
4. KOMUNIKACIJSKE USLUGE 285
4.1. Usluga StartCommunication 285
4.2. Usluga StopCommunication 287
4.2.1 Opis poruka 287
4.2.2 Format poruka 288
4.2.3 Opis parametara 289
4.3. Usluga TesterPresent 289
4.3.1 Opis poruka 289
4.3.2 Format poruka 289
5. USLUGE UPRAVLJANJA 291
5.1. Usluga StartDiagnosticSession 291
5.1.1 Opis poruka 291
5.1.2 Format poruka 292
5.1.3 Opis parametara 293
5.2. Usluga SecurityAccess 294
5.2.1 Opis poruka 294
5.2.2 Format poruka – SecurityAccess – requestSeed 295
5.2.3 Format poruka – SecurityAccess – sendKey 296
6. USLUGE PRIJENOSA PODATAKA 297
6.1. Usluga ReadDataByIdentifier 298
6.1.1 Opis poruka 298
6.1.2 Format poruka 298
6.1.3 Opis parametara 299
6.2. Usluga WriteDataByIdentifier 300
6.2.1 Opis poruka 300
6.2.2 Format poruka 300
6.2.3 Opis parametara 302

7. UPRAVLJANJE ISPITNIM IMPULSIMA – FUNKCIONALNA JEDINICA ZA UPRAVLJANJE ULAZOM/IZLAZOM 302

7.1. Usluga InputOutputControlByIdentifier 302

7.1.1 Opis poruka 302

7.1.2 Format poruka 303

7.1.3 Opis parametara 304

8. FORMATI DATARECORDS 305

8.1. Rasponi prenesenih parametara 305

8.2. Formati dataRecords 306

1. UVOD

U ovom se Dodatku opisuje način razmjene podataka između jedinice u vozilu i ispitnog uređaja putem K-linije koja čini sastavni dio sučelja za kalibraciju opisanog u Dodatku 6. Isto se tako opisuje upravljanje linijom ulaznih/izlaznih signala na priključku za kalibraciju.

Uspostavljanje komunikacije putem K-linije opisano je u odjeljku 4. „Komunikacijske usluge".

U ovom se Dodatku upotrebljava pojam dijagnostičkih „razmjena podataka" (eng. *session*) za određivanje opsega upravljanja putem K-linije u različitim uvjetima. Standardna je razmjena podataka „StandardDiagnosticSession" u kojoj se svi podatci mogu čitati s jedinice u vozilu, ali niti jedan podatak nije moguće upisati u jedinicu u vozilu.

Odabir dijagnostičke razmjene podataka opisan je u odjeljku 5. „Usluge upravljanja".

Ovaj Dodatak smatra se relevantnim za obje generacije jedinica u vozilu i kartica radionica u skladu sa zahtjevima za interoperabilnost utvrđenima u ovoj Uredbi.

CPR_001 „ECUProgrammingSession" omogućuje unos podataka u jedinicu u vozilu. Osim toga, u slučaju unosa podataka za kalibraciju, jedinica u vozilu mora biti u načinu rada KALIBRACIJA.

Prijenos podataka putem K-linije opisan je u odjeljku 6. „Usluge prijenosa podataka". Formati prenesenih podataka detaljno su izloženi u odjeljku 8. „Formati dataRecords".

CPR_002 „ECUAdjustmentSession" omogućuje odabir U/I (ulazno/izlaznog) načina rada linije kalibracije U/I signala putem sučelja K-linije. Upravljanje linijom kalibracije U/I signala opisano je u odjeljku 7. „Upravljanje ispitnim impulsima – funkcionalna jedinica za upravljanje ulazom/izlazom".

CPR_003 U ovom se dokumentu adresa ispitnog uređaja navodi kao 'tt'. Iako mogu postojati preferirane adrese ispitnih uređaja, jedinica u vozilu ispravno odgovara na svaku adresu ispitnog uređaja. Fizička je adresa jedinice u vozilu 0xEE.

2. IZRAZI, DEFINICIJE I REFERENTNI DOKUMENTI

Protokoli, poruke i kodovi pogrešaka u načelu se temelje na nacrtu norme ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1: Diagnostic services*, verzija 6. od 22. veljače 2001.).

Za identifikatore usluge, zahtjeve za usluge i odgovore te za standardne parametre upotrebljavaju se bajtno kodiranje i heksadecimalne vrijednosti.

Izraz „ispitni uređaj" odnosi se na uređaj koji se upotrebljava za unos podataka za programiranje/kalibraciju u jedinicu u vozilu (VU).

Izrazi „korisnik" i „poslužitelj" odnose se na ispitni uređaj odnosno jedinicu u vozilu.

Izraz ECU označuje „elektroničku upravljačku jedinicu" i odnosi se na jedinicu u vozilu.

Referentni dokumenti:

ISO 14230-2: *Road Vehicles – Diagnostic Systems – Keyword Protocol 2000 – Part 2: Data Link Layer.*

Prvo izdanje, 1999.

3. PREGLED USLUGA

3.1. **Raspoložive usluge**

U sljedećoj je tablici naveden pregled usluga koje će biti raspoložive u tahografu i koje su definirane u ovom dokumentu.

CPR_004 U tablici su prikazane usluge koje su raspoložive u aktiviranoj dijagnostičkoj razmjeni podataka.

— **U prvom stupcu** navode se usluge koje su raspoložive,

— **u drugom stupcu** navodi se broj odjeljka u ovom Dodatku u kojem je usluga detaljnije definirana,

— u **trećem stupcu** pridružene su vrijednosti identifikatora usluge (SId) za poruke zahtjeva,

— **u četvrtom stupcu** navode se usluge **„StandardDiagnosticSession" (SD)** koje se moraju primjenjivati u svakoj jedinici u vozilu,

— u **petom stupcu** navode se usluge **„ECUAdjustmentSession" (ECUAS)** koje se moraju primjenjivati za omogućivanje upravljanja linijom U/I signala u priključku za kalibraciju na prednjoj stranici jedinice u vozilu,

— u **šestom stupcu** navode se usluge **„ECUProgrammingSession" (ECUPS)** koje se moraju primjenjivati za omogućivanje programiranja parametara u jedinici u vozilu.

Tablica 1.

Sažetak vrijednosti identifikatora usluge

			Dijagnostička razmjena podataka		
Naziv dijagnostičke usluge	Broj odjeljka	Zaht. vrijednost SId	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		■	

■ Ovaj simbol označuje da je usluga obvezna u ovoj dijagnostičkoj razmjeni podataka.

Izostanak simbola označuje da ta usluga nije dopuštena u ovoj dijagnostičkoj razmjeni podataka.

3.2. **Kodovi odgovora**

Za svaku su uslugu definirani kodovi odgovora.

4. KOMUNIKACIJSKE USLUGE

Neke su usluge potrebne za uspostavljanje i održavanje komunikacije. One se ne javljaju na aplikacijskoj razini. Raspoložive usluge opisane su u sljedećoj tablici:

Tablica 2.

Komunikacijske usluge

Naziv usluge	Opis
StartCommunication	Korisnik zahtijeva početak komunikacijske razmjene podataka s poslužiteljem (poslužiteljima).
StopCommunication	Korisnik zahtijeva prekid komunikacijske razmjene podataka koja je u tijeku.
TesterPresent	Korisnik ukazuje poslužitelju da je još uvijek prisutan.

CPR_005 Usluga StartCommunication upotrebljava se za početak komunikacije. Da bi se obavila neka usluga, komunikacija se mora pokrenuti, a komunikacijski parametri moraju biti primjereni željenom načinu rada.

4.1. **Usluga StartCommunication**

CPR_006 Po prijemu primitiva indikacije StartCommunication, jedinica u vozilu provjerava može li se zahtijevana komunikacijska veza pokrenuti u trenutačnim uvjetima. Valjani uvjeti za početak komunikacijske veze opisani su u normi ISO 14230-2.

CPR_007 Potom jedinica u vozilu obavlja sve potrebne radnje za pokretanje (inicijalizaciju) komunikacijske veze i šalje primitiv odgovora StartCommunication s odabranim parametrima pozitivnog odgovora.

CPR_008 Ako jedinica u vozilu koja je već pokrenuta (i započela je dijagnostičku razmjenu podataka) primi novi zahtjev StartCommunication (npr. zbog ispravljanja pogreške u ispitnom uređaju), zahtjev se prihvaća i jedinica u vozilu se ponovno pokreće.

CPR_009 Ako se iz nekog razloga komunikacijska veza ne može pokrenuti, jedinica u vozilu nastavlja raditi kao i neposredno prije pokušaja pokretanja komunikacijske veze.

CPR_010 Poruka sa zahtjevom StartCommunication mora biti fizički naslovljena.

CPR_011 Pokretanje jedinice u vozilu za usluge obavlja se metodom „brzog pokretanja”:

— prije svake aktivnosti postoji razdoblje neaktivnosti sabirnice,

— ispitni uređaj potom šalje obrazac za pokretanje,

— svi podatci koji su potrebni za uspostavljanje komunikacije sadržani su u odgovoru jedinice u vozilu.

CPR_012 Po završetku pokretanja:

— svi komunikacijski parametri postavljaju se na vrijednosti utvrđene u tablici 4. prema bajtovima ključa,

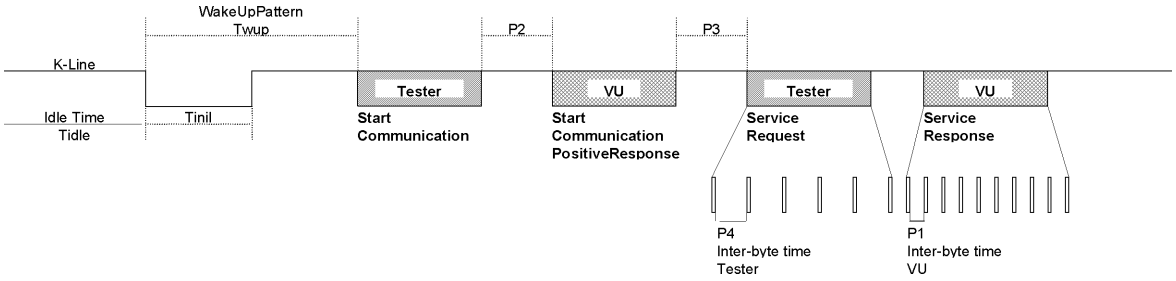
— jedinica u vozilu čeka na prvi zahtjev ispitnog uređaja,

— jedinica u vozilu u standardnom je dijagnostičkom načinu rada, tj. StandardDiagnosticSession,

— linija kalibracije U/I signala je u standardnom odnosno isključenom stanju.

CPR_014 Brzina prijenosa podataka na K-liniji iznosi 10 400 bauda.

CPR_016 Brzo pokretanje započinje kada ispitni uređaj prenese obrazac pobude (Wup) na K-liniji. Obrazac započinje nakon vremena mirovanja na K-liniji u vremenu smanjene aktivnosti Tinil. Ispitni uređaj prenosi prvi bit usluge StartCommunication nakon razdoblja Twup i prvog prekida.



CPR_017 Vremenski raspored za brzo pokretanje i komunikaciju općenito naveden je u tablicama u nastavku. Postoje različite mogućnosti za razdoblje mirovanja:

— prvi prijenos nakon uključivanja, Tidle = 300 ms,

— nakon okončanja usluge StopCommunication, Tidle = P3 min.,

— nakon prekida komunikacije zbog isteka vremena P3 maks., Tidle = 0.

Tablica 3.

Vremenski raspored za brzo pokretanje

Parametar		najmanja vrijednost	najveća vrijednost
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tablica 4.

Vremenski raspored komunikacije

Vremenski parametar	Opis parametra	Donje granične vrijednosti [ms]	Gornje granične vrijednosti [ms]
		min.	maks.
P1	Međubajtno vrijeme za odgovor jedinice u vozilu	0	20
P2	Vrijeme između zahtjeva ispitnog uređaja i odgovora jedinice u vozilu ili dvaju odgovora jedinice u vozilu	25	250
P3	Vrijeme između kraja odgovora jedinice u vozilu i početka novog zahtjeva ispitnog uređaja	55	5 000
P4	Međubajtno vrijeme za zahtjev ispitnog uređaja	5	20

CPR_018 Format poruka za brzo pokretanje prikazan je u sljedećim tablicama:

Tablica 5.

Poruka zahtjeva StartCommunication

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	81	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	**Identifikator usluge zahtjeva StartCommunication**	**81**	**SCR**
#5	Kontrolni zbroj	00-FF	CS

Tablica 6.

Poruka StartCommunication s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	**Identifikator usluge StartCommunication s pozitivnim odgovorom**	**C1**	**SCRPR**
#6	Bajt ključa 1	EA	KB1
#7	Bajt ključa 2	8F	KB2
#8	Kontrolni zbroj	00-FF	CS

CPR_019 Nema negativnog odgovora na poruku zahtjeva StartCommunication; ako nema poruke s pozitivnim odgovorom za prijenos, tada se jedinica u vozilu ne pokreće, ništa se ne prenosi i ona nastavlja s redovnim radom.

4.2. **Usluga StopCommunication**

4.2.1 *Opis poruka*

Svrha je ove usluge komunikacijske razine prekid komunikacijske razmjene podataka.

CPR_020 Po prijemu primitiva indikacije StopCommunication, jedinica u vozilu provjerava omogućuju li prevladavajući uvjeti prekid ove komunikacije. U tom slučaju jedinica u vozilu obavlja sve radnje potrebne za okončanje ove komunikacije.

CPR_021 Ako je moguće prekinuti komunikaciju, jedinica u vozilu izdaje primitiv odgovora StopCommunication s odabranim parametrima pozitivnog odgovora prije prekida komunikacije.

CPR_022 Ako se komunikacija iz nekog razloga ne može prekinuti, jedinica u vozilu izdaje primitiv odgovora StopCommunication s odabranim parametrom negativnog odgovora.

CPR_023 Ako jedinica u vozilu utvrdi istek vremena P3 maks., komunikacija se prekida bez izdavanja primitiva bilo kakvog odgovora.

4.2.2 *Format poruka*

CPR_024 Formati poruke za primitive StopCommunication prikazani su u sljedećim tablicama:

Tablica 7.

Poruka zahtjeva StopCommunication

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu duljinu	01	LEN
#5	**StopCommunication Request Service Id**	**82**	**SPR**
#6	Kontrolni zbroj	00-FF	CS

Tablica 8.

Poruka StopCommunication s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Kontrolni zbroj	00-FF	CS

Tablica 9.

Poruka StopCommunication s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	Identifikator usluge zahtjeva StopCommunication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Kontrolni zbroj	00-FF	CS

4.2.3 *Opis parametara*

Ova usluga ne zahtijeva opis parametara.

4.3. **Usluga TesterPresent**

4.3.1 *Opis poruka*

Ispitni uređaj upotrebljava uslugu TesterPresent kako bi poslužitelju ukazao da je još uvijek prisutan, kako bi se spriječilo automatsko vraćanje poslužitelja u redovan rad i mogući prekid komunikacije. Ova usluga, koja se povremeno šalje, održava dijagnostičku razmjenu podataka / komunikaciju aktivnom ponovnim postavljanjem sata P3 prilikom svakog primitka zahtjeva za ovu uslugu.

4.3.2 *Format poruka*

CPR_079 Format poruka za primitive TesterPresent prikazan je u sljedećim tablicama:

Tablica 10.

Poruka zahtjeva TesterPresent

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu duljinu	02	LEN
#5	**TesterPresent Request Service Id**	**3E**	**TP**

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#6	Podfunkcija = responseRequired = [da	01	RESPREQ_Y
	ne]	02	RESPREQ_NO
#7	Kontrolni zbroj	00-FF	CS

CPR_080 Ako je parametar responseRequired postavljen na „da”, poslužitelj odgovara porukom sa sljedećim pozitivnim odgovorom. Ako je postavljen na „ne”, poslužitelj ne šalje nikakav odgovor.

Tablica 11.

Poruka TesterPresent s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Kontrolni zbroj	00-FF	CS

CPR_081 Usluga podržava sljedeće kodove negativnih odgovora:

Tablica 12.

Poruka TesterPresent s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	TesterPresent Request Service Identification	3E	TP

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#7	responseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Kontrolni zbroj		00-FF	CS

5. USLUGE UPRAVLJANJA

Raspoložive usluge opisane su u sljedećoj tablici:

Tablica 13.

Usluge upravljanja

Naziv usluge	Opis
StartDiagnosticSession	Korisnik zahtijeva početak dijagnostičke razmjene podataka s jedinicom u vozilu.
SecurityAccess	Korisnik zahtijeva pristup funkcijama koje su ograničene na ovlaštene korisnike.

5.1. **Usluga StartDiagnosticSession**

5.1.1 *Opis poruka*

CPR_025 Usluga StartDiagnosticSession upotrebljava se kako bi omogućila različite dijagnostičke razmjene podataka u poslužitelju. Dijagnostička razmjena podataka omogućuje poseban skup usluga prema tablici 17. Razmjena podataka može proizvođačima vozila omogućiti posebne usluge koje nisu dio ovog dokumenta. Provedbena pravila ispunjavaju sljedeće zahtjeve:

— uvijek je samo jedna dijagnostička razmjena podataka aktivna u jedinici u vozilu,

— prilikom uključenja jedinica u vozilu uvijek pokreće StandardDiagnosticSession. Ako nije pokrenuta niti jedna druga dijagnostička razmjena podataka, StandardDiagnosticSession je aktivan sve dok je uključena jedinica u vozilu,

— ako je ispitni uređaj zatražio dijagnostičku razmjenu podataka koja je već aktivna, tada jedinica u vozilu šalje poruku s pozitivnim odgovorom,

— svaki put kada ispitni uređaj zatraži novu dijagnostičku razmjenu podataka, jedinica u vozilu najprije šalje poruku StartDiagnosticSession s pozitivnim odgovorom prije nego što novi proces postane aktivan u jedinici u vozilu. Ako nije u stanju započeti zatraženu novu dijagnostičku razmjenu podataka, jedinica u vozilu odgovara porukom StartDiagnosticSession s negativnim odgovorom te nastavlja tekuću razmjenu podataka.

CPR_026 Dijagnostička razmjena podataka započinje samo ako je uspostavljena komunikacija između korisnika i jedinice u vozilu.

CPR_027 Vremenski parametri utvrđeni u tablici 4. moraju biti aktivni nakon uspješne usluge StartDiagnosticSession s parametrom diagnosticSession postavljenim na „StandardDiagnosticSession” u poruci zahtjeva ako je prethodno bila aktivna druga dijagnostička razmjena podataka.

5.1.2 *Format poruka*

CPR_028 Formati poruka za primitive StartDiagnosticSession prikazani su u sljedećim tablicama:

Tablica 14.

Poruka zahtjeva StartDiagnosticSession

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu duljinu	02	LEN
#5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
#6	diagnosticSession = [jedna vrijednost iz tablice 17.]	xx	DS_…
#7	Kontrolni zbroj	00-FF	CS

Tablica 15.

Poruka StartDiagnosticSession s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	diagnosticSession = [ista vrijednost kao u bajtu #6 iz tablice 14.]	xx	DS_…
#7	Kontrolni zbroj	00-FF	CS

Tablica 16.

Poruka StartDiagnosticSession s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#3	Bajt izvorne adrese		EE	SRC
#4	Bajt za dodatnu duljinu		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	Kontrolni zbroj		00-FF	CS

([a]) Vrijednost unesena u bajt #6 poruke zahtjeva ne podržava se, tj. nije u tablici 17.
([b]) Duljina poruke pogrešna je.
([c]) Kriteriji za zahtjev StartDiagnosticSession nisu ispunjeni.

5.1.3 *Opis parametara*

CPR_029 Usluga StartDiagnosticSession upotrebljava parametar diagnosticSession (DS_) za odabir posebnog postupka jednog ili više poslužitelja. U ovom su dokumentu opisane sljedeće dijagnostičke razmjene podataka:

Tablica 17.

Određivanje vrijednosti diagnosticSession

Heksadecimalna vrijednost	Opis	Mnemonik
81	**StandardDiagnosticSession** Ova dijagnostička razmjena podataka omogućuje sve usluge navedene u **tablici 1. stupcu 4. „SD”**. Te usluge omogućuju čitanje svih podataka s poslužitelja (jedinice u vozilu). Ova je dijagnostička razmjena podataka aktivna nakon što je uspješno obavljeno pokretanje između korisnika (ispitnog uređaja) i poslužitelja (jedinice u vozilu). Preko ove dijagnostičke razmjene podataka mogu se memorirati druge dijagnostičke razmjene podataka navedene u ovom odjeljku.	**SD**
85	**ECUProgrammingSession** Ova dijagnostička razmjena podataka omogućuje sve usluge navedene u **tablici 1. stupcu 6. „ECUPS”**. Te usluge podržavaju programiranje memorije poslužitelja (jedinice u vozilu). Preko ove dijagnostičke razmjene podataka mogu se memorirati druge dijagnostičke razmjene podataka navedene u ovom odjeljku.	**ECUPS**
87	**ECUAdjustmentSession** Ova dijagnostička razmjena podataka omogućuje sve usluge navedene u **tablici 1. stupcu 5. „ECUAS”.** Te usluge podržavaju upravljanje ulazom/izlazom poslužitelja (jedinice u vozilu). Preko ove dijagnostičke razmjene podataka mogu se memorirati druge dijagnostičke razmjene podataka navedene u ovom odjeljku.	**ECUAS**

5.2. **Usluga SecurityAccess**

Upisivanje podataka kalibracije nije moguće osim ako je jedinica u vozilu u načinu rada KALIBRACIJA. Osim unošenja valjane kartice radionice u jedinicu u vozilu, u jedinicu u vozilu potrebno je upisati odgovarajući PIN prije dobivanja dopuštenja za pristup načinu rada KALIBRACIJA.

Kad je jedinica u vozilu u načinu rada KALIBRACIJA ili UPRAVLJANJE, moguć je pristup liniji kalibracije ulaznih/izlaznih signala.

Usluga SecurityAccess osigurava način unosa PIN-a i ukazivanje ispitnom uređaju je li jedinica u vozilu u načinu rada KALIBRACIJA.

Dopušten je unos PIN-a na neki drugi način.

5.2.1 *Opis poruka*

Uslugu SecurityAccess čine SecurityAccess poruke „requestSeed”, nakon čega može slijediti SecurityAccess poruka „sendKey”. Usluga SecurityAccess mora se provesti nakon usluge StartDiagnosticSession.

CPR_033 Ispitni uređaj može upotrebljavati SecurityAccess poruku „requestSeed” za provjeru je li jedinica u vozilu spremna za prihvaćanje PIN-a.

CPR_034 Ako je jedinica u vozilu već u načinu rada KALIBRACIJA, na zahtjev odgovara upućivanjem signala („seed”) od 0x0000 upotrebom usluge SecurityAccess s pozitivnim odgovorom.

CPR_035 Ako je jedinica u vozilu spremna prihvatiti PIN za provjeru putem kartice radionice, na zahtjev odgovara slanjem signala („seed”) većeg od 0x0000 upotrebom usluge SecurityAccess s pozitivnim odgovorom.

CPR_036 Ako jedinica u vozilu nije spremna prihvatiti PIN iz ispitnog uređaja, bilo zato što umetnuta kartica radionice nije valjana ili zato što kartica radionice nije umetnuta ili stoga što jedinica u vozilu očekuje PIN na neki drugi način, na zahtjev odgovara negativnim odgovorom s kodom odgovora koji je postavljen na conditionsNotCorrectOrRequestSequenceError.

CPR_037 Ispitni uređaj može potom upotrijebiti SecurityAccess poruku „sendKey” za slanje PIN-a jedinici u vozilu. Kako bi se dalo vremena za provođenje postupka autentifikacije kartice, jedinica u vozilu upotrebljava kod negativnog odgovora requestCorrectlyReceived-ResponsePending kako bi se produljilo vrijeme za davanje odgovora. Međutim, dopušteno vrijeme za davanje odgovora ne smije biti dulje od pet minuta. Čim se zahtijevana usluga završi, jedinica u vozilu šalje poruku s pozitivnim odgovorom ili poruku s negativnim odgovorom s kodom odgovora koji je različit od navedenog. Jedinica u vozilu može ponavljati kod negativnog odgovora requestCorrectlyReceived-ResponsePending do završetka zahtijevane usluge i do upućivanja poruke s konačnim odgovorom.

CPR_038 Jedinica u vozilu odgovara na ovaj zahtjev upotrebom usluge SecurityAccess s pozitivnim odgovorom samo kada je u načinu rada KALIBRACIJA.

CPR_039 U sljedećim slučajevima, jedinica u vozilu odgovara na ovaj zahtjev negativnim odgovorom s kodom odgovora postavljenim na:

— subFunctionNotSupported: nepravilan format parametra podfunkcije (accessType),

— conditionsNotCorrectOrRequestSequenceError: jedinica u vozilu nije spremna za prihvaćanje unosa PIN-a,

— invalidKey: PIN nije valjan i broj pokušaja provjere PIN-a nije premašen,

— exceededNumberOfAttempts: PIN nije valjan i broj pokušaja provjere PIN-a je premašen,

— generalReject: ispravan PIN, ali uzajamna autentifikacija s karticom radionice nije uspjela.

5.2.2 *Format poruka – SecurityAccess – requestSeed*

CPR_040 Formati poruka za SecurityAccess primitive „requestSeed” prikazani su u sljedećim tablicama:

Tablica 18.

Zahtjev SecurityAccess – poruka requestSeed

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu duljinu	02	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Kontrolni zbroj	00-FF	CS

Tablica 19.

SecurityAccess – poruka requestSeed s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	04	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	SeedHigh	00-FF	SEEDH
#8	SeedLow	00-FF	SEEDL
#9	Kontrolni zbroj	00-FF	CS

Tablica 20.

Poruka SecurityAccess s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#4	Bajt za dodatnu duljinu	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	Identifikator usluge zahtjeva SecurityAccess	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Kontrolni zbroj	00-FF	CS

5.2.3 *Format poruka – SecurityAccess – sendKey*

CPR_041 Formati poruka za SecurityAccess primitive „sendKey" prikazani su u sljedećim tablicama:

Tablica 21.

Zahtjev SecurityAccess – poruka sendKey

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu duljinu	m+2	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7 do #m +6	Ključ #1 (viši)	xx	KEY
	…	…	
	Ključ #m (niži, m mora biti najmanje 4, a najviše 8)	xx	
#m+7	Kontrolni zbroj	00-FF	CS

Tablica 22.

SecurityAccess – poruka sendKey s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#4	Bajt za dodatnu duljinu	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Kontrolni zbroj	00-FF	CS

Tablica 23.

Poruka SecurityAccess s negativnim odgovorom

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje		80	FMT
#2	Bajt ciljne adrese		tt	TGT
#3	Bajt izvorne adrese		EE	SRC
#4	Bajt za dodatnu duljinu		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	Kontrolni zbroj		00-FF	CS

6. USLUGE PRIJENOSA PODATAKA

Raspoložive usluge opisane su u sljedećoj tablici:

Tablica 24.

Usluge prijenosa podataka

Naziv usluge	Opis
ReadDataByIdentifier	Korisnik zahtijeva prijenos trenutačne vrijednosti zapisa kojem recordDataIdentifier ima pristup.
WriteDataByIdentifier	Korisnik zahtijeva upisivanje zapisa kojem je recordDataIdentifier pristupio.

6.1. **Usluga ReadDataByIdentifier**

6.1.1 *Opis poruka*

CPR_050 Uslugu ReadDataByIdentifier korisnik upotrebljava za traženje vrijednosti podatkovnih zapisa iz poslužitelja. Podatke identificira recordDataIdentifier. Proizvođač jedinice u vozilu odgovoran je za ispunjavanje uvjeta poslužitelja prilikom obavljanja ove usluge.

6.1.2 *Format poruka*

CPR_051 Formati poruka za primitive ReadDataByIdentifier prikazani su u sljedećim tablicama:

Tablica 25.

Poruka zahtjeva ReadDataByIdentifier

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
#6 do #7	recordDataIdentifier = [jedna vrijednost iz tablice 28.]	xxxx	RDI_…
#8	Kontrolni zbroj	00-FF	CS

Tablica 26.

Poruka ReadDataByIdentifier s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	m+3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 i #7	recordDataIdentifier = [ista vrijednost kao bajtovi #6 i #7 iz tablice 25.]	xxxx	RDI_…
#8 do #m +7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrolni zbroj	00-FF	CS

Tablica 27.

Poruka ReadDataByIdentifier s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	Identifikator usluge zahtjeva ReadDataByIdentifier	22	RDBI
#7	ResponseCode = [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Kontrolni zbroj	00-FF	CS

6.1.3 *Opis parametara*

CPR_052 Parametar ***recordDataIdentifier (RDI_)*** u poruci zahtjeva ReadDataByIdentifier identificira podatkovni zapis.

CPR_053 Vrijednosti recordDataIdentifier utvrđene u ovom dokumentu prikazane su u tablici u nastavku.

Tablicu recordDataIdentifier čine četiri stupca i više redaka.

— **U prvom stupcu (Heks.)** navodi se „heksadecimalna vrijednost" dodijeljena parametru recordDataIdentifier opisanom u trećem stupcu.

— **U drugom stupcu (Podatkovni element)** prikazan je podatkovni element iz Dodatka 1. na kojem se temelji recordDataIdentifier (ponekad je potrebno prekodiranje).

— **U trećem stupcu (Opis)** navodi se odgovarajući naziv parametra recordDataIdentifier.

— **U četvrtom stupcu (Mnemonik)** navodi se mnemonik tog parametra recordDataIdentifier.

Tablica 28.

Određivanje vrijednosti recordDataIdentifier

Heks.	Podatkovni element	Naziv parametra recordDataIdentifier (vidjeti format u odjeljku 8.2.)	Mnemonik
F90B	`CurrentDateTime`	TimeDate	RDI_TD
F912	`HighResOdometer`	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	`K-ConstantOfRecordingEquipment`	Kfactor	RDI_KF

Heks.	Podatkovni element	Naziv parametra recordDataIdentifier (vidjeti format u odjeljku 8.2.)	Mnemonik
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 Parametar ***dataRecord (DREC_)*** upotrebljava poruka ReadDataByIdentifier s pozitivnim odgovorom za pružanje korisniku (ispitnom uređaju) vrijednosti podatkovnog zapisa koji je identificirao recordDataIdentifier. Formati podataka navedeni su u odjeljku 8. Mogu se primijeniti dodatni korisnički neobvezni dataRecords, uključujući posebne ulazne, unutarnje i izlazne podatke jedinice u vozilu, no oni nisu definirani u ovom dokumentu.

6.2. **Usluga WriteDataByIdentifier**

6.2.1 *Opis poruka*

CPR_056 Uslugu WriteDataByIdentifier korisnik upotrebljava za upisivanje vrijednosti podatkovnih zapisa na poslužitelj. Podatke identificira parametar recordDataldentifier. Proizvođač jedinice u vozilu odgovoran je za ispunjavanje uvjeta poslužitelja prilikom obavljanja ove usluge. Za ažuriranje parametara navedenih u tablici 28. jedinica u vozilu mora biti u načinu rada KALIBRACIJA.

6.2.2 *Format poruka*

CPR_057 Formati poruka za primitive WriteDataByIdentifier prikazani su u sljedećim tablicama:

Tablica 29.

Poruka zahtjeva WriteDataByIdentifier

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu duljinu	m+3	LEN
#5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
#6 do #7	recordDataIdentifier = [jedna vrijednost iz tablice 28.]	xxxx	RDI_…

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#8 do m +7	dataRecord[] = [data#1	xx	DREC_DATA1
	:	:	:
	data#m]	xx	DREC_DATAm
#m+8	Kontrolni zbroj	00-FF	CS

Tablica 30.

Poruka WriteDataByIdentifier s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 do #7	recordDataIdentifier = [ista vrijednost kao bajtovi #6 i #7 iz tablice 25.]	xxxx	RDI_…
#8	Kontrolni zbroj	00-FF	CS

Tablica 31.

Poruka WriteDataByIdentifier s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	WriteDataByIdentifier Request Service Id	2E	WDBI

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#7	ResponseCode =	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrolni zbroj		00-FF	CS

6.2.3 *Opis parametara*

Parametar ***recordDataIdentifier (RDI_)*** određen je u tablici 28.

Parametar ***dataRecord (DREC_)*** upotrebljava poruka zahtjeva WriteDataByIdentifier za davanje poslužitelju (jedinici u vozilu) vrijednosti podatkovnih zapisa koje je identificirao recordDataIdentifier. Formati podataka navedeni su u odjeljku 8.

7. UPRAVLJANJE ISPITNIM IMPULSIMA – FUNKCIONALNA JEDINICA ZA UPRAVLJANJE ULAZOM/IZLAZOM

Raspoložive usluge opisane su u sljedećoj tablici:

Tablica 32.

Funkcionalna jedinica za upravljanje ulazom/izlazom

Naziv usluge	Opis
InputOutputControlByIdentifier	Korisnik zahtijeva upravljanje ulazom/izlazom specifično za poslužitelj

7.1. **Usluga InputOutputControlByIdentifier**

7.1.1 *Opis poruka*

Postoji veza putem priključka na prednjoj strani tahografa koja omogućuje upravljanje ispitnim impulsima ili njihovo praćenje upotrebom odgovarajućeg ispitnog uređaja.

CPR_058 Ova linija kalibracije U/I signala može se konfigurirati naredbom iz K-linije putem usluge InputOutput-ControlByIdentifier za odabir zahtijevane funkcije ulaza ili izlaza za liniju. Raspoloživa su stanja linije:

— isključeno,

— speedSignalInput, pri čemu se linija kalibracije U/I signala upotrebljava za ulaz signala brzine (ispitni signal) koji nadomješta signal brzine senzora kretanja; ova funkcija nije moguća u kontrolnom načinu rada,

— realTimeSpeedSignalOutputSensor, pri čemu se linija kalibracije signala U/I upotrebljava za izlaz signala brzine senzora kretanja,

— RTCOutput, pri čemu se linija kalibracije U/I signala upotrebljava za izlaz signala UTC sata; ova funkcija nije moguća u kontrolnom načinu rada.

CPR_059 Jedinica u vozilu morala je pristupiti procesu podešavanja i mora biti u kalibracijskom ili kontrolnom načinu rada za konfiguraciju stanja linije. Kad je jedinica u vozilu u kalibracijskom načinu rada, dostupne su četiri linije stanja (isključeno, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Kad je jedinica u vozilu u kontrolnom načinu rada, dostupne su samo dvije linije stanja (isključeno, realTimeSpeedSignalOutputSensor). Prilikom izlaza iz procesa podešavanja ili kalibracijskog ili kontrolnog načina rada, jedinica u vozilu mora osigurati da se linija kalibracije U/I signala vrati u „isključeno” (standardno) stanje.

CPR_060 Ako se impulsi brzine u realnom vremenu primaju na liniju ulaza signala brzine jedinice u vozilu dok je linija kalibracije U/I signala postavljena na ulaz, tada se linija kalibracije U/I signala postavlja na izlaz ili vraća u isključeno stanje.

CPR_061 Redoslijed je sljedeći:

— uspostava komunikacije putem usluge StartCommunication,

— ulazak u proces podešavanja putem usluge StartDiagnosticSession i kalibracijski ili kontrolni način rada (redoslijed ovih dviju operacija nije bitan),

— promjena stanja izlaza putem usluge InputOutputControlByIdentifier.

7.1.2 *Format poruka*

CPR_062 Formati poruka za primitive InputOutputControlByIdentifier prikazani su u sljedećim tablicama:

Tablica 33.

Poruka zahtjeva InputOutputControlByIdentifier

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu duljinu	xx	LEN
#5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
#6 i #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ili #8 do #9	ControlOptionRecord = [inputOutputControlParameter – jedna vrijednost iz tablice 36. controlState – jedna vrijednost iz tablice 37. (vidjeti napomenu u nastavku)]	 xx xx	COR_… IOCP_… CS_…
#9 ili #10	Kontrolni zbroj	00-FF	CS

Napomena: Parametar controlState prisutan je samo u nekim slučajevima (vidjeti točku 7.1.3.).

Tablica 34.

Poruka InputOutputControlByIdentifier s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	xx	LEN
#5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 i #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ili #8 do #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter = [ista vrijednost kao bajt #8 iz tablice 33.]	xx	IOCP_…
	controlState (ista vrijednost kao bajt #9 iz tablice 33.)(ako je primjenjivo)	xx	CS_…
#9 ili #10	Kontrolni zbroj	00-FF	CS

Tablica 35.

Poruka InputOutputControlByIdentifier s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	Identifikator usluge zahtjeva inputOutputControlByIdentifier	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Kontrolni zbroj	00-FF	CS

7.1.3 *Opis parametara*

CPR_064 Parametar ***inputOutputControlParameter (IOCP_)*** određen je u sljedećoj tablici:

Tablica 36.

Određivanje vrijednosti inputOutputControlParameter

Heksadecimalna vrijednost	Opis	Mnemonik
00	**ReturnControlToECU** Ova vrijednost upozorava poslužitelja (jedinicu u vozilu) da ispitni uređaj više ne upravlja linijom kalibracije U/I signala.	RCTECU
01	**ResetToDefault** Ova vrijednost upozorava poslužitelja (jedinicu u vozilu) da se od njega zahtijeva povrat linije kalibracije U/I signala u standardno stanje.	RTD
03	**ShortTermAdjustment** Ova vrijednost upozorava poslužitelja (jedinicu u vozilu) da se od njega zahtijeva podešavanje linije kalibracije U/I signala s vrijednošću obuhvaćenom parametrom controlState.	STA

CPR_065 Parametar ***controlState*** prisutan je samo kada je inputOutputControlParameter postavljen na ShortTermAdjustment i definiran je u sljedećoj tablici:

Tablica 37.

Određivanje vrijednosti controlState

Način rada	Heksadecimalna vrijednost	Opis
Isključi	00	U/I linija je isključena (standardno stanje)
Uključi	01	Uključuje U/I liniju kalibracije kao speedSignalInput
Uključi	02	Uključuje U/I liniju kalibracije kao realTimeSpeedSignalOutputSensor
Uključi	03	Uključuje U/I liniju kalibracije kao RTCOutput

8. FORMATI DATARECORDS

U ovom se odjeljku opisuju:

— opća pravila koja se primjenjuju na raspon parametara koje jedinica u vozilu prenosi ispitnom uređaju,

— formati koji se upotrebljavaju za podatke koji se prenose putem usluga prijenosa podataka opisanih u odjeljku 6.

CPR_067 Jedinica u vozilu podržava sve utvrđene parametre.

CPR_068 Podatci koje jedinica u vozilu prenosi ispitnom uređaju kao odgovor na poruku zahtjeva moraju biti izmjereni podatci (tj. trenutačna vrijednost zahtijevanog parametra koji je jedinica u vozilu izmjerila ili uočila).

8.1. **Rasponi prenesenih parametara**

CPR_069 U tablici 38. određeni su rasponi koji se upotrebljavaju za utvrđivanje valjanosti prenesenog parametra.

CPR_070 Vrijednosti u rasponu „indikator pogreške” omogućuju jedinici u vozilu da odmah upozori da valjani parametarski podatak trenutačno nije dostupan zbog neke pogreške u tahografu.

CPR_071 Vrijednosti u rasponu „nije dostupno” omogućuju jedinici u vozilu da prenese poruku koja sadržava parametar koji nije dostupan ili ga taj modul ne podržava. Vrijednosti u području „nije traženo” omogućuju uređaju da prenese poruku naredbe i odredi one parametre kod kojih se ne očekuje odgovor prijamnog uređaja.

CPR_072 Ako pogreška sastavnog dijela spriječi prijenos valjanog podatka za parametar, umjesto podatka za takav parametar treba upotrijebiti indikator pogreške opisan u tablici 38. Međutim, ako izmjereni ili izračunani podatak daje valjanu vrijednost, ali premašuje utvrđeni raspon parametra, ne smije se upotrebljavati indikator pogreške. Podatke treba prenositi upotrebljavajući odgovarajuću najmanju ili najveću vrijednost parametra.

Tablica 38.

Rasponi dataRecords

Naziv raspona	1 bajt (heksadecimalna vrijednost)	2 bajta (heksadecimalna vrijednost)	4 bajta (heksadecimalna vrijednost)	ASCII
Valjan signal	00 do FA	0000 do FAFF	00000000 do FAFFFFFF	1 do 254
Indikator specifičnog parametra	FB	FB00 do FBFF	FB000000 do FBFFFFFF	nema
Rezervirani raspon za bitove budućih indikatora	FC do FD	FC00 do FDFF	FC000000 do FDFFFFFF	nema
Indikator pogreške	FE	FE00 do FEFF	FE000000 do FEFFFFFF	0
Nije dostupno ili nije traženo	FF	FF00 do FFFF	FF000000 do FFFFFFFF	FF

CPR_073 Za parametre kodirane u ASCII, ASCII znak „*” rezerviran je kao razdjelnik.

8.2. **Formati dataRecords**

U tablicama 39. do 42. navedenima u nastavku detaljno su prikazani formati koji se upotrebljavaju putem usluga ReadDataByIdentifier i WriteDataByIdentifier.

CPR_074 U tablici 39. navedeni su duljina, razlučivost i radno područje za svaki parametar koji je identificirao njegov recordDataIdentifier:

Tablica 39.

Format dataRecords

Naziv parametra	Duljina podatka (u bajtovima)	Razlučivost	Radno područje
TimeDate	8	Vidjeti pojedinosti u tablici 40.	
HighResolutionTotalVehicleDistance	4	uvećanje 5 m/bit, pomak 0 m	0 do + 21 055 406 km
Kfactor	2	uvećanje 0,001 impulsa/m/bit, pomak 0	0 do 64,255 impulsa/m
LfactorTyreCircumference	2	uvećanje 0,125 10^{-3} m /bit, pomak 0	0 do 8,031 m
WvehicleCharacteristicFactor	2	uvećanje 0,001 impulsa/m/bit, pomak 0	0 do 64,255 impulsa/m
TyreSize	15	ASCII	ASCII

Naziv parametra	Duljina podatka (u bajtovima)	Razlučivost	Radno područje
NextCalibrationDate	3	Vidjeti pojedinosti u tablici 41.	
SpeedAuthorised	2	uvećanje 1/256 km/h/bit, pomak 0	0 do 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Vidjeti pojedinosti u tablici 42.	
VIN	17	ASCII	ASCII

CPR_075 U tablici 40. detaljno su opisani formati različitih bajtova parametra TimeDate:

Tablica 40.

Detaljni format TimeDate (vrijednost recordDataIdentifier # F90B)

Bajt	Opis parametara	Razlučivost	Radno područje
1	Sekunde	uvećanje 0,25 s/bit, pomak 0 s	0 do 59,75 s
2	Minute	uvećanje 1 min/bit, pomak 0 min	0 do 59 min
3	Sati	uvećanje 1 h/bit, pomak 0 h	0 do 23 h
4	Mjesec	uvećanje 1 mjesec/bit, pomak 0 mjeseci	1 do 12 mjeseci
5	Dan	uvećanje 0,25 dana/bit, pomak 0 dana (vidjeti napomenu ispod tablice 41.)	0,25 do 31,75 dana
6	Godina	uvećanje 1 godina/bit, pomak + 1985 godina (vidjeti napomenu ispod tablice 41.)	godina 1985. do 2235.
7	Pomak po minutama u lokalnom vremenu	uvećanje 1 min/bit, pomak – 125 min	– 59 do + 59 min
8	Pomak po satima u lokalnom vremenu	uvećanje 1 h/bit, pomak – 125 h	– 23 do + 23 h

CPR_076 U tablici 41. detaljno su opisani formati različitih bajtova parametra NextCalibrationDate:

Tablica 41.

Detaljni format NextCalibrationDate (vrijednost recordDataIdentifier # F922)

Bajt	Opis parametara	Razlučivost	Radno područje
1	Mjesec	uvećanje 1 mjesec/bit, pomak 0 mjeseci	1 do 12 mjeseci
2	Dan	uvećanje 0,25 dana/bit, pomak 0 dana (vidjeti napomenu u nastavku)	0,25 do 31,75 dana
3	Godina	uvećanje 1 godina/bit, pomak + 1985 godina (vidjeti napomenu u nastavku)	godina 1985. do 2235.

NAPOMENA povezana s upotrebom parametra „Dan”:

1) Vrijednost 0 u datumu je prazna vrijednost. Vrijednosti 1, 2, 3 i 4 upotrebljavaju se za označivanje prvog dana u mjesecu; 5, 6, 7 i 8 određuju drugi dan u mjesecu itd.

2) Ovaj parametar ne utječe niti mijenja prethodno navedeni parametar sati.

NAPOMENA povezana s upotrebom parametra „Godina”:

Vrijednost 0 za godinu označuje 1985. godinu; vrijednost 1 označuje 1986. itd.

CPR_078 U tablici 42. detaljno su opisani formati različitih bajtova parametra VehicleRegistrationNumber:

Tablica 42.

Detaljni format VehicleRegistrationNumber (vrijednost recordDataIdentifier # F97E)

Bajt	Opis parametara	Razlučivost	Radno područje
1	Kodna stranica (kako je utvrđena u Dodatku 1.)	ASCII	01 do 0A
2 – 14	Registracijski broj vozila (kako je utvrđen u Dodatku 1.)	ASCII	ASCII

Dodatak 9.

HOMOLOGACIJA POPIS OBVEZNIH ISPITIVANJA

SADRŽAJ

1. UVOD 309

2. FUNKCIONALNA ISPITIVANJA JEDINICE U VOZILU 311

3. FUNKCIONALNA ISPITIVANJA SENZORA KRETANJA 315

4. FUNKCIONALNA ISPITIVANJA TAHOGRAFSKIH KARTICA 318

5. ISPITIVANJA VANJSKOG UREĐAJA GNSS-A 328

6. ISPITIVANJA UREĐAJA ZA KOMUNIKACIJU NA DALJINU 331

7. FUNKCIONALNA ISPITIVANJA PAPIRA 333

8. ISPITIVANJA INTEROPERABILNOSTI 335

1. UVOD

1.1. **Homologacija**

EZ homologacija uređaja za bilježenje podataka (ili njegova sastavnog dijela) ili tahografske kartice temelji se na:

— **sigurnosnoj certifikaciji** koja se temelji na specifikacijama zajedničkih mjerila u odnosu na sigurnosni cilj koji je potpuno usklađen s Dodatkom 10. ovom Prilogu,

— **funkcionalnoj certifikaciji** koju provodi tijelo države članice koje potvrđuje da ispitivani predmet zadovoljava zahtjeve ovog Priloga u smislu izvršenih funkcija, točnosti mjerenja i obilježja okruženja,

— **certifikaciji interoperabilnosti** koju obavlja nadležno tijelo koje potvrđuje da je uređaj za bilježenje podataka (ili tahografska kartica) u cijelosti interoperabilan sa zahtijevanim modelima tahografske kartice (ili uređaja za bilježenje podataka) (vidjeti poglavlje 8. ovog Priloga).

U ovom se Dodatku navode obvezna ispitivanja koja tijelo države članice mora obaviti tijekom funkcionalnih ispitivanja te obvezna ispitivanja koja nadležno tijelo mora obaviti tijekom ispitivanja interoperabilnosti. Postupci koji se provode za obavljanje ispitivanja ili vrsta ispitivanja nisu podrobnije opisani.

Ovim Dodatkom nisu obuhvaćeni aspekti sigurnosne certifikacije. Ako se neka ispitivanja zahtijevana za homologaciju obavljaju tijekom sigurnosne procjene i postupka certifikacije, tada ta ispitivanja ne treba ponavljati. U tom se slučaju mogu samo pregledati rezultati tih ispitivanja sigurnosti. U informativne svrhe, zahtjevi za koje se očekuje da će biti ispitani (ili koji su blisko povezani s ispitivanjima za koja se očekuje da će biti obavljena) tijekom sigurnosne certifikacije u ovom su Dodatku označeni znakom „*”.

Numerirani zahtjevi odnose se na tekstove Priloga, dok se ostali zahtjevi odnose na ostale dodatke (npr. PIC_001 odnosi se na zahtjev PIC_001 piktograma iz Dodatka 3.).

U ovom se Dodatku razmatraju odvojeno homologacija senzora kretanja, jedinice u vozilu i vanjskog uređaja GNSS-a kao sastavnih dijelova uređaja za bilježenje podataka. Svaki sastavni dio dobiva vlastiti certifikat o homologaciji u kojem su naznačeni ostali kompatibilni sastavni dijelovi. Funkcionalno ispitivanje senzora kretanja (ili vanjskog uređaja GNSS-a) provodi se zajedno s jedinicom u vozilu i obrnuto.

Ne zahtijeva se interoperabilnost između svakog modela senzora kretanja (odnosno vanjskog uređaja GNSS-a) i svakog modela jedinice u vozilu. U tom slučaju homologacija senzora kretanja (odnosno vanjskog uređaja GNSS-a) može se dodijeliti samo u kombinaciji s homologacijom relevantne jedinice u vozilu i obrnuto.

1.2. **Referentni dokumenti**

U ovom su Dodatku upotrijebljeni sljedeći izvori:

IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold;

IEC 60068-2-2: Basic environmental testing procedures; Part 2: Tests; Tests B: Dry heat (sinusoidal);

IEC 60068-2-6: Environmental testing – Part 2: Tests – Test Fc: Vibration;

IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature;

IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock;

IEC 60068-2-30: Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle);

IEC 60068-2-64: Environmental testing – Part 2-64: Tests– Test Fh: Vibration, broadband random and guidance;

IEC 60068-2-78 Environmental testing – Part 2-78: Tests – Test Cab: Damp heat, steady state;

ISO 16750-3 – Mechanical loads (2012-12);

ISO 16750-4 – Climatic loads (2010-04);

ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access;

ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014 Road vehicles – Test methods for electrical disturbances from electrostatic discharge;

ISO 7637-1:2002 + AMD1: 2008 Road vehicles – Electrical disturbances from conduction and coupling – Part 1: Definitions and general considerations;

ISO 7637-2 Road vehicles – Electrical disturbances from conduction and coupling – Part 2: Electrical transient conduction along supply lines only;

ISO 7637-3 Road vehicles – Electrical disturbances from conduction and coupling – Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines;

ISO/IEC 7816-1 Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics;

ISO/IEC 7816-2 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts;

ISO/IEC 7816-3 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol;

ISO/IEC 10373-1:2006 + AMD1:2012 Identification cards – Test methods – Part 1: General characteristics;

ISO/IEC 10373-3:2010 + Technical Corrigendum:2013 Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices;

ISO 16844-3:2004, Cor 1:2006 Road vehicles – Tachograph systems – Part 3: Motion sensor interface (with vehicle units);

ISO 16844-4 Road vehicles – Tachograph systems – Part 4: CAN interface;

ISO 16844-6 Road vehicles – Tachograph systems – Part 6: Diagnostics;

ISO 16844-7 Road vehicles – Tachograph systems – Part 7: Parameters;

ISO 534 Paper and board – Determination of thickness, density and specific volume;

UN ECE R10 Jedinstvene odredbe o homologaciji vozila s obzirom na elektromagnetsku kompatibilnost (Gospodarska komisija Ujedinjenih naroda za Europu).

2. FUNKCIONALNA ISPITIVANJA JEDINICE U VOZILU

Br.	Ispitivanje	Opis	Povezani zahtjevi
1	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
1.2	Rezultati ispitivanja proizvođača	Rezultati ispitivanja proizvođača provedenog tijekom ugradnje. Osiguravanje dokumentacije.	88, 89, 91
2	**Vizualni pregled**		
2.1	Sukladnost s dokumentacijom		
2.2	Identifikacija/oznake		224 do 226
2.3	Materijali		219 do 223
2.4	Plombiranje		398, 401 do 405
2.5	Vanjska sučelja		
3	**Funkcionalna ispitivanja**		
3.1	Predviđene funkcije		03, 04, 05, 07, 382
3.2	Načini rada		09 do 11*, 132, 133
3.3	Funkcije i prava na pristup podatcima		12* 13*, 382, 383, 386 do 389
3.4	Praćenje umetanja i uklanjanja kartica		15, 16, 17, 18, 19*, 20*, 132
3.5	Mjerenje brzine i udaljenosti		21 do 31
3.6	Mjerenje vremena (ispitivanje se obavlja na 20 °C)		38 do 43
3.7	Praćenje aktivnosti vozača		44 do 53, 132
3.8	Praćenje statusa vožnje		54, 55, 132

Br.	Ispitivanje	Opis	Povezani zahtjevi
3.9	Ručni unosi		56 do 62
3.10	Upravljanje blokadama poduzeća		63 do 68
3.11	Praćenje aktivnosti nadzora		69, 70
3.12	Otkrivanje događaja i/ili pogrešaka		71 do 88, 132
3.13	Identifikacijski podatci o uređaju		93*, 94*, 97, 100
3.14	Podatci o umetanju i uklanjanju kartice vozača		102* do 104*
3.15	Podatci o aktivnosti vozača		105* do 107*
3.16	Podatci o mjestima i pozicijama		108* do 112*
3.17	Stanje brojača prijeđenih kilometara		113* do 115*
3.18	Detaljni podatci o brzini		116*
3.19	Podatci o događajima		117*
3.20	Podatci o pogreškama		118*
3.21	Podatci o kalibraciji		119* do 121*
3.22	Podatci o prilagodbi vremena		124*, 125*
3.23	Podatci o aktivnostima nadzora		126*, 127*
3.24	Podatci o blokadama poduzeća		128*
3.25	Podatci o aktivnostima preuzimanja podataka		129*
3.26	Podatci o posebnim stanjima		130*, 131*
3.27	Bilježenje i pohrana podataka na tahografske kartice		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Prikaz		90, 132, 149 do 166 PIC_001, DIS_001
3.29	Ispis		90, 132, 167 do 179, PIC_001, PRT_001 do PRT_014
3.30	Upozorenje		132, 180 do 189 PIC_001

Br.	Ispitivanje	Opis	Povezani zahtjevi
3.31	Preuzimanje podataka na vanjske medije		90, 132, 190 do 194
3.32	Komunikacija na daljinu za ciljane provjere na cesti		195 do 197
3.33	Izlaz podataka na dodatne vanjske uređaje		198, 199
3.34	Kalibracija		202 do 206*, 383, 384, 386 do 391
3.35	Provjera kalibracije na cesti		207 do 209
3.36	Prilagodba vremena		210 do 212*
3.37	Neometanje dodatnih funkcija		06, 425
3.38	Sučelje senzora kretanja		02, 122
3.39	Vanjski uređaj GNSS-a		03, 123
3.40	Provjeriti otkriva li, bilježi i pohranjuje jedinica u vozilu događaj(e) i/ili pogrešku (pogreške) koje je definirao proizvođač jedinica u vozilu kad upareni senzor kretanja reagira na magnetska polja koja ometaju detekciju kretanja vozila.		217
3.41	Slijed šifri (*cypher suite*) i normirani parametri domene		CSM_48, CSM_50
4	**Ispitivanja utjecaja okoliša**		
4.1	Temperatura	Provjera funkcionalnosti putem: ispitivanja u skladu s ISO 16750-4, poglavlje 5.1.1.2.: ispitivanje rada pri niskoj temperaturi (72 h na – 20 °C) Ovo se ispitivanje odnosi na IEC 60068-2-1: *Environmental testing – Part 2-1: Tests – Test A: Cold*. Ispitivanje u skladu s ISO 16750-4, poglavlje 5.1.2.2.: ispitivanje rada pri visokoj temperaturi (72 h na 70 °C). Ovo se ispitivanje odnosi na IEC 60068-2-2: *Basic environmental testing procedures; Part 2: Tests; Tests B: Dry heat*. Ispitivanje u skladu s ISO 16750-4, poglavlje 5.3.2.: brze promjene temperature s određenim trajanjem prelaska (– 20 °C/70 °C, 20 ciklusa, 2 sata držanja pri svakoj temperaturi). Skraćeni niz ispitivanja (između onih utvrđenih u odjeljku 3. ove tablice) može se obaviti pri nižoj temperaturi, višoj temperaturi i tijekom temperaturnih ciklusa.	213

Br.	Ispitivanje	Opis	Povezani zahtjevi
4.2	Vlažnost	Provjeriti može li jedinica u vozilu izdržati cikličnu vlažnost (ispitivanje toplinom) putem IEC 60068-2-30, ispitivanje Db, šest ciklusa u trajanju od 24 h, pri svakom promjena temperature od + 25 °C do + 55 °C i relativna vlažnost od 97 % pri + 25 °C te od 93 % pri + 55 °C.	214
4.3	Mehanički	1. Sinusne vibracije: provjeriti može li jedinica u vozilu izdržati sinusne vibracije sa sljedećim značajkama: konstantan pomak između 5 i 11 Hz: vršna amplituda 10 mm; konstantno ubrzanje između 11 i 300 Hz: 5 g. Ovaj se zahtjev provjerava putem IEC 60068-2-6, ispitivanje Fc, uz minimalno trajanje ispitivanja od 3 × 12 sati (12 sati po osi). Norma ISO 16750-3 ne zahtijeva ispitivanje na sinusne vibracije za uređaje smještene u odspojenoj kabini vozila. 2. Nasumične vibracije: Ispitivanje u skladu s ISO 16750-3, poglavlje 4.1.2.8., Test VIII: Commercial vehicle, decoupled vehicle cab. Ispitivanje na nasumične vibracije, 10…2 000 Hz, RMS okomito 21,3 m/s^2, RMS uzdužno 11,8 m/s^2, RMS bočno 13,1 m/s^2, 3 osi, 32 h po osi, uključujući temperaturni ciklus – 20…70 °C. Ovo se ispitivanje odnosi na IEC 60068-2-64: Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance. 3. Udarci: mehanički udarac s 3 g, polu-sinus, u skladu s ISO 16750. Prethodno opisana ispitivanja provode se na različitim uzorcima vrste opreme koja se ispituje.	219
4.4	Zaštita od vode i stranih tijela	Ispitivanje u skladu s ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (bez promjene parametara); minimalna vrijednost IP 40.	220, 221
4.5	Prenaponska zaštita	Provjeriti može li jedinica u vozilu izdržati snagu napajanja od: izvedbe od 24 V: 34 V pri + 40 °C 1 sat, izvedbe od 12 V: 17 V pri + 40 °C 1 sat, (ISO 16750-2)	216
4.6	Zaštita od zamjene polariteta	Provjeriti može li jedinica u vozilu izdržati inverziju svojeg napajanja (ISO 16750-2)	216

Br.	Ispitivanje	Opis	Povezani zahtjevi
4.7	Zaštita od kratkog spoja	Provjeriti jesu li ulazno/izlazni signali zaštićeni od kratkog spoja u odnosu na napajanje i uzemljenje (ISO 16750-2)	216
5	**Ispitivanja elektromagnetske kompatibilnosti (EMC)**		
5.1	Emisije zračenja i osjetljivost	Sukladnost s Pravilnikom ECE R10	218
5.2	Elektrostatičko pražnjenje	Sukladnost s normom ISO 10605:2008 + Tehnički ispravak:2010 + AMD1:2014: +/– 4 kV za kontakt i +/– 8 kV za ispuštanje zraka	218
5.3	Osjetljivost napajanja na električne prijelazne pojave	Za izvedbe od 24 V: sukladnost s normom ISO 7637-2 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1a: Vs = – 450V, Ri = 50 oma, impuls 2a: Vs = + 37V, Ri = 2 oma, impuls 2b: Vs = + 20V, Ri = 0,05 oma, impuls 3a: Vs = – 150V, Ri = 50 oma, impuls 3b: Vs = + 150V, Ri = 50 oma, impuls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms, impuls 5: Vs = + 120 V, Ri = 2,2 oma, td = 250 ms. Za izvedbe od 12V: sukladnost s ISO 7637-1 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1: Vs = – 75V, Ri = 10 oma, impuls 2a: Vs = + 37V, Ri = 2 oma, impuls 2b: Vs = + 10V, Ri = 0,05 oma, impuls 3a: Vs = – 112V, Ri = 50 oma, impuls 3b: Vs = + 75V, Ri = 50 oma, impuls 4: Vs = – 6 V, Va = –5 V, t6 = 15 ms, impuls 5: Vs = + 65 V, Ri = 3 oma, td = 100 ms. Impuls 5 ispituje se samo za jedinice u vozilu namijenjene ugradnji u vozila na kojima se ne provodi jedinstvena vanjska zaštita od rasterećenja. Za prijedlog rasterećenja, vidjeti ISO 16750-2, 4. izdanje, poglavlje 4.6.4.	218

3. FUNKCIONALNA ISPITIVANJA SENZORA KRETANJA

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	

Br.	Ispitivanje	Opis	Povezani zahtjevi
2.	**Vizualni pregled**		
2.1.	Sukladnost s dokumentacijom		
2.2.	Identifikacija/oznake		225, 226,
2.3	Materijali		219 do 223
2.4	Plombiranje		398, 401 do 405
3.	**Funkcionalna ispitivanja**		
3.1	Identifikacijski podatci senzora		95* do 97*
3.2	Uparivanje senzora kretanja i jedinice u vozilu		122*, 204
3.3	Detekcija kretanja Točnost mjerenja kretanja		30 do 35
3.4	Sučelje jedinice u vozilu		02
3.5	Provjeriti je li senzor kretanja neosjetljiv na magnetsko polje. Alternativno, provjeriti reagira li senzor kretanja na konstantna magnetska polja koja ometaju detekciju kretanja vozila tako da spojena jedinica u vozilu može detektirati, zabilježiti i pohraniti pogreške senzora.		217
4.	**Ispitivanja utjecaja okoliša**		
4.1	Radna temperatura	Provjera funkcionalnosti (kako je određeno u ispitivanju br. 3.3) u temperaturnom rasponu [– 40 °C; + 135 °C] putem: IEC 60068-2-1, ispitivanje Ad, trajanje ispitivanja 96 sati pri najnižoj temperaturi To_{min}, IEC 60068-2-2, ispitivanje Bd, trajanje ispitivanja 96 sati pri najvišoj temperaturi To_{max}. Ispitivanje u skladu s ISO 16750-4, poglavlje 5.1.1.2.: ispitivanje rada pri niskoj temperaturi (24 h na – 40 °C). Ovo se ispitivanje odnosi na IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold; IEC 68-2-2, ispitivanje Bd, trajanje ispitivanja 96 sati pri najnižoj temperaturi od – 40 °C. Ispitivanje u skladu s ISO 16750-4, poglavlje 5.1.2.2.: ispitivanje rada pri visokoj temperaturi (96 h na 135 °C). Ovo se ispitivanje odnosi na IEC 60068-2-2: Basic environmental testing procedures; Part 2: Tests; Tests B: Dry heat	213

Br.	Ispitivanje	Opis	Povezani zahtjevi
4.2	Temperaturni ciklusi	Ispitivanje u skladu s ISO 16750-4, poglavlje 5.3.2.: brze promjene temperature s određenim trajanjem prelaska (– 40 °C/135 °C, 20 ciklusa, 30 min držanja pri svakoj temperaturi). IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature.	213
4.3	Ciklusi vlažnosti	Provjera funkcionalnosti (kako je određeno u ispitivanju br. 3.3) putem IEC 60068-2-30, ispitivanje Db, šest ciklusa u trajanju od 24 h, pri svakom primjena temperature od + 25°C do + 55°C i relativna vlažnost od 97 % pri + 25°C te od 93 % pri + 55°C.	214
4.4	Vibracije	ISO 16750-3, poglavlje 4.1.2.6., Test VI: Commercial vehicle, engine, gearbox. Ispitivanje na vibracije u mješovitom načinu, uključujući a) ispitivanje na sinusne vibracije, 20…520 Hz, 11,4 … 120 m/s², <= 0,5 okt/min; b) ispitivanje na nasumične vibracije, 10…2 000 Hz, RMS 177 m/s², 94 h po osi, uključujući temperaturni ciklus – 20…70 °C). Ovo se ispitivanje odnosi na IEC 60068-2-80: Environmental testing – Part 2-80: Tests – Test Fi: Vibration – Mixed mode.	219
4.5	Mehanički udarac	ISO 16750-3, poglavlje 4.2.3., Test VI: Test for devices in or on the gearbox. Polu-sinusni udarac, ubrzanje treba dogovoriti u rasponu 3 000…15 000 m/s², trajanje impulsa treba dogovoriti, međutim < 1 ms, broj udaraca: treba dogovoriti. Ovo se ispitivanje odnosi na IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock.	219
4.6	Zaštita od vode i stranih tijela	Ispitivanje u skladu s ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (ciljana vrijednost IP 64)	220, 221
4.7	Zaštita od zamjene polariteta	Provjeriti može li senzor kretanja izdržati inverziju svojeg napajanja.	216
4.8	Zaštita od kratkog spoja	Provjeriti jesu li ulazno/izlazni signali zaštićeni od kratkog spoja u odnosu na napajanje i uzemljenje.	216

Br.	Ispitivanje	Opis	Povezani zahtjevi
5.	**Elektromagnetska kompatibilnost (EMC)**		
5.1	Emisije zračenja i osjetljivost	Provjera sukladnosti s Pravilnikom ECE R10	218
5.2	Elektrostatičko pražnjenje	Sukladnost s ISO 10605:2008 + Tehnički ispravak:2010 + AMD1:2014: +/– 4 kV za kontakt i +/– 8 kV za ispuštanje zraka	218
5.3	Osjetljivost podatkovnih vodova na električne prijelazne pojave	Za izvedbe od 24 V: sukladnost s ISO 7637-2 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1a: Vs = – 450V, Ri = 50 oma, impuls 2a: Vs = + 37V, Ri = 2 oma, impuls 2b: Vs = + 20V, Ri = 0,05 oma, impuls 3a: Vs = – 150V, Ri = 50 oma, impuls 3b: Vs = +150V, Ri = 50 oma, impuls 4: Vs = –16 V, Va = –12 V, t6 = 100 ms, impuls 5: Vs = + 120 V, Ri = 2,2 oma, td = 250 ms. Za izvedbe od 12V: sukladnost s ISO 7637-1 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1: Vs = – 75V, Ri = 10 oma, impuls 2a: Vs = + 37V, Ri = 2 oma, impuls 2b: Vs = + 10V, Ri = 0,05 oma, impuls 3a: Vs = – 112V, Ri = 50 oma, impuls 3b: Vs = +75V, Ri = 50 oma, impuls 4: Vs = – 6 V, Va = –5 V, t6 = 15 ms, impuls 5: Vs = + 65 V, Ri = 3 oma, td = 100 ms. Impuls 5 ispituje se samo za jedinice u vozilu namijenjene ugradnji u vozila na kojima se ne provodi jedinstvena vanjska zaštita od rasterećenja. Za prijedlog rasterećenja, vidjeti ISO 16750-2, 4. izdanje, poglavlje 4.6.4.	218

4. FUNKCIONALNA ISPITIVANJA TAHOGRAFSKIH KARTICA

Ispitivanja u skladu s ovim odjeljkom 4.,

br. 5 „Ispitivanja protokola”,

br. 6 „Struktura kartice” i

br. 7 „Funkcionalna ispitivanja”

može provesti osoba zadužena za evaluaciju ili certifikaciju tijekom postupka sigurnosne certifikacije prema zajedničkim mjerilima (CC) za modul čipa.

Ispitivanja br. 2.3 i 4.2 jednaka su. To su mehanička ispitivanja kombinacije tijela kartice i modula čipa. Ako se jedan od tih sastavnih dijelova (tijelo kartice, modul čipa) promijeni, tada su potrebna ova ispitivanja.

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
2	**Tijelo kartice**		
2.1	Tiskani dizajn	Osigurati da su sva obilježja zaštite i vidljivi podatci ispravno ispisani na kartici i sukladni. [Označitelj] Prilog 1.C, poglavlje 4.1. „Vidljivi podatci”, 227) Prednja stranica mora sadržavati: riječi „kartica vozača” ili „kontrolna kartica” ili „kartica radionice” ili „kartica poduzeća” tiskane velikim slovima na službenom jeziku ili jezicima države članice koja izdaje karticu, prema vrsti kartice; [Ime države članice] Prilog 1.C, poglavlje 4.1. „Vidljivi podatci”, 228) Prednja stranica mora sadržavati: ime države članice koja je izdala karticu (nije obvezno); [Razlikovna oznaka] Prilog 1.C, poglavlje 4.1. „Vidljivi podatci”, 229) Prednja stranica mora sadržavati: razlikovnu oznaku države članice koja izdaje karticu, tiskanu u negativu u plavom pravokutniku i okruženu s 12 žutih zvijezda. [Numeriranje] Prilog 1.C, poglavlje 4.1. „Vidljivi podatci”, 232) Stražnja stranica mora sadržavati: objašnjenje numeriranih stavki na prednjoj stranici kartice. [Boja] Prilog 1.C, poglavlje 4.1. „Vidljivi podatci”, 234) Tahografske kartice moraju se tiskati sa sljedećim prevladavajućim bojama pozadine: — kartica vozača: bijela, — kartica radionice: crvena, — kontrolna kartica: plava — kartica poduzeća: žuta.	227 do 229, 232, 234 do 236

Br.	Ispitivanje	Opis	Povezani zahtjevi
		[Sigurnost] Prilog 1.C, poglavlje 4.1. „Vidljivi podatci”, 235) Tahografske kartice moraju imati barem sljedeća obilježja za zaštitu tijela kartice od krivotvorenja i neovlaštenog rukovanja: — sigurnosnu podlogu s tankim guilloche uzorcima i tiskom s duginim efektom, — barem jednu dvobojnu liniju u mikrotisku.	
		[Oznake] Prilog 1.C, poglavlje 4.1. „Vidljivi podatci”, 236) Države članice mogu dodavati boje i oznake kao što su nacionalni simboli i sigurnosna obilježja.	
		[Homologacijska oznaka] Kartice tahografa moraju sadržavati homologacijsku oznaku. Homologacijsku oznaku čine: — pravokutnik, unutar kojeg se upisuje slovo „e”, nakon kojeg slijedi razlikovni broj ili slovo države koja je izdala homologaciju, — broj homologacije koji odgovara broju certifikata o homologaciji za tahografsku karticu, zapisan u neposrednoj blizini pravokutnika.	
2.2	Mehanička ispitivanja	[Veličina kartice] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [5.] Dimenzije kartice, [5.1.] Veličina kartice, [5.1.1.] Dimenzije kartice i dopuštena odstupanja, vrsta kartice ID-1 Neupotrijebljena kartica	240, 243 ISO/IEC 7810
		[Rubovi kartice] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [5.] Dimenzije kartice, [5.1.] Veličina kartice, [5.1.2.] Rubovi kartice	

Br.	Ispitivanje	Opis	Povezani zahtjevi
		[Izrada kartice] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [6.] Izrada kartice	
		[Materijali kartice] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [7.] Materijali kartice	
		[Krutost pri savijanju] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.1.] Krutost pri savijanju	
		[Toksičnost] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.3.] Toksičnost	
		[Otpornost na kemikalije] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.4.] Otpornost na kemikalije	
		[Stabilnost kartice] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.5.] Dimenzijska stabilnost kartice i izobličenje zbog temperature i vlage	

Br.	Ispitivanje	Opis	Povezani zahtjevi
		[Svjetlost] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.6.] Svjetlost	
		[Trajnost] Prilog 1C, poglavlje 4.4. „Specifikacije okruženja i elektrotehničke specifikacije”, 241) Tahografske kartice moraju moći ispravno raditi tijekom razdoblja od pet godina ako se upotrebljavaju u skladu sa specifikacijama okruženja i elektrotehničkim specifikacijama.	
		[Čvrstoća ljuštenja] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.8.] Čvrstoća ljuštenja	
		[Prianjanje ili blokiranje] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.9.] Prianjanje ili blokiranje	
		[Izobličenje] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.11.] Ukupno izobličenje kartice	
		[Otpornost na toplinu] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.12.] Otpornost na toplinu	

Br.	Ispitivanje	Opis	Povezani zahtjevi
		[Izobličenja površine] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.13.] Izobličenja površine	
		[Onečišćenje] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics,* [8.] Značajke kartice, [8.14.] Onečišćenje i međudjelovanje sastavnih dijelova kartice	
2.3	Mehanička ispitivanja s ugrađenim modulom čipa	[Savijanje] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits*. [9.2.] Dinamičko opterećenje savijanjem Ukupni broj ciklusa savijanja: 4 000.	ISO/IEC 7810
		[Uvijanje (torzija)] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.3.] Dinamičko opterećenje uvijanjem Ukupni broj ciklusa uvijanja: 4 000.	
3	**Modul**		
3.1	Modul	Modul je kućište čipa i kontaktna pločica. [Profil površine] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7816-1:2011, *Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics* [4.2.] Profil površine kontakata	ISO/IEC 7816

Br.	Ispitivanje	Opis	Povezani zahtjevi
		[Mehanička čvrstoća] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7816-1:2011, *Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics* [4.3.] Mehanička čvrstoća (kartice i kontakata)	
		[Električni otpor] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7816-1:2011, *Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics* [4.4.] Električni otpor (kontakata)	
		[Dimenzije] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7816-2:2007, *Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts* [3.] Dimenzije kontakata	
		[Položaj] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7816-2:2007, *Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts* [4.] Broj i položaj kontakata U slučaju modula sa šest kontakata, kontakti „C4” i „C8” nisu dio zahtjeva ovog ispitivanja.	
4	**Čip**		
4.1	Čip	[Radna temperatura] Čip tahografske kartice mora djelovati u rasponu temperature okoline između – 25 °C i + 85 °C.	241 do 244 ECE R10 ISO/IEC 7810 ISO/IEC 10373

Br.	Ispitivanje	Opis	Povezani zahtjevi
		[Temperatura i vlažnost] Prilog 1C, poglavlje 4.4. „Specifikacije okruženja i elektrotehničke specifikacije”, 241) Tahografske kartice moraju moći ispravno raditi u svim klimatskim uvjetima uobičajenima na teritoriju Zajednice, pri temperaturnom rasponu od najmanje – 25 °C do + 70 °C s povremenim vršnim porastom do + 85 °C, pri čemu „povremeno” označuje ne dulje od 4 sata svaki puta i ne više od 100 puta tijekom vijeka trajanja kartice. Tahografske kartice u uzastopnim se koracima izlažu sljedećim temperaturama i vlažnosti tijekom određenog vremena. Nakon svakog koraka ispituje se električna funkcionalnost tahografskih kartica. 1. Temperatura od – 20 °C na 2 sata. 2. Temperatura od +/– 0 °C na 2 sata. 3. Temperatura od + 20 °C, relativna vlažnost 50 %, na 2 sata. 4. Temperatura od 50 °C, relativna vlažnost 50 %, na 2 sata. 5. Temperatura od + 70 °C, relativna vlažnost 50 %, na 2 sata. Temperatura se povremeno povećava na + 85 °C, relativna vlažnost 50 %, na 60 min. 6. Temperatura od + 70 °C, relativna vlažnost 85 %, na 2 sata. Temperatura se povremeno povećava na + 85 °C, relativna vlažnost 85 %, na 30 min.	
		[Vlažnost] Prilog 1C, poglavlje 4.4. „Specifikacije okruženja i elektrotehničke specifikacije”, 242) Tahografske kartice moraju moći ispravno raditi u rasponu vlažnosti između 10 % i 90 %.	
		[Elektromagnetska kompatibilnost – EMC] Prilog 1C, poglavlje 4.4. „Specifikacije okruženja i elektrotehničke specifikacije”, 244) Tijekom rada, tahografske kartice moraju biti u skladu s Pravilnikom ECE R10 o elektromagnetskoj kompatibilnosti.	

Br.	Ispitivanje	Opis	Povezani zahtjevi
		[Statički elektricitet] Prilog 1C, poglavlje 4.4. „Specifikacije okruženja i elektrotehničke specifikacije”, 244) Tijekom rada, tahografske kartice moraju biti zaštićene od elektrostatičkih pražnjenja. Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.4.] Statički elektricitet [9.4.1.] Elektroničke kartice s kontaktima Ispitni napon: 4 000 V.	
		[Rendgenske zrake] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.1.] Rendgenske zrake	
		[Ultraljubičasto svjetlo] ISO/IEC 10373-1:2006, *Identification cards – Test methods – Part 1: General characteristics* [5.11.] Ultraljubičasto svjetlo	
		[Uređaj za ispitivanje mehaničkog opterećenja kartice (*3-wheel*)] Tahografske kartice moraju biti u skladu s normom ISO/IEC 10373-1:2006/Amd. 1:2012, *Identification cards – Test methods – Part 1: General characteristics, Amendment 1*. [5.22.] ICC – Mehanička čvrstoća: *3-wheel* ispitivanje ICC-a s kontaktima	
		[Savitljivost] Tahografske kartice moraju biti u skladu s normom MasterCard CQM V2.03:2013 [11.1.3.] R-L3-14-8: Ispitivanje izdržljivosti pri savijanju [13.2.1.32.] TM-422: Mehanička pouzdanost: Ispitivanje savitljivosti	

Br.	Ispitivanje	Opis	Povezani zahtjevi
4.2	Mehanička ispitivanja modula čipa ugrađenog u tijelo kartice -> isto kao 2.3.	[Savijanje] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits*. [9.2.] Dinamičko opterećenje savijanjem Ukupni broj ciklusa savijanja: 4 000. [Uvijanje (torzija)] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits*. [9.3] Dinamičko opterećenje uvijanjem Ukupni broj ciklusa uvijanja: 4 000.	ISO/IEC 7810
5	**Ispitivanja protokola**		
5.1	ATR	Provjeriti sukladnost ATR-a	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T = 0	Provjeriti sukladnost protokola T = 0	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Provjeriti sukladnost naredbe PTS postavljanjem s T = 0 na T = 1.	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T = 1	Provjeriti sukladnost protokola T = 1	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Struktura kartice**		
6.1		Ispitati sukladnost strukture datoteke provjerom prisutnosti obveznih datoteka na kartici i uvjeta pristupa tim datotekama.	TCS_22 do TCS_28 TCS_140 do TCS_179
7	**Funkcionalna ispitivanja**		
7.1	Normalna obrada	Najmanje jednom ispitati svaku dopuštenu upotrebu svake naredbe (npr.: ispitivanje naredbe UPDATE BINARY (ažuriranje datoteke) s CLA = '00', CLA = '0C' s različitim parametrima P1, P2 i Lc). Provjeriti jesu li postupci doista provedeni na kartici (npr.: čitanjem datoteke za koju je izvršena naredba).	TCS_29 do TCS_139

Br.	Ispitivanje	Opis	Povezani zahtjevi
7.2	Poruke o pogrešci	Najmanje jednom ispitati svaku poruku o pogrešci (kako je određeno u Dodatku 2.) za svaku naredbu. Najmanje jednom ispitati svaku generičku pogrešku (osim „**6400**" pogrešaka integriteta provjerenih tijekom sigurnosne certifikacije).	
7.3	Slijed šifri (*cypher suite*) i normirani parametri domene		CSM_48, CSM_50
8	**Personalizacija**		
8.1	Optička personalizacija	Prilog 1C, poglavlje 4.1. „Vidljivi podatci", 230) Prednja stranica mora sadržavati: podatke karakteristične za izdanu karticu. Prilog 1C, poglavlje 4.1. „Vidljivi podatci", 231) Prednja stranica mora sadržavati: datume koji se pišu u obliku „dd/mm/gggg" ili „dd.mm. gggg." (dan, mjesec, godina). Prilog 1.C, poglavlje 4.1. „Vidljivi podatci", 235) Tahografske kartice moraju imati barem sljedeća obilježja za zaštitu tijela kartice od krivotvorenja i neovlaštenog rukovanja: — na prostoru za fotografiju, pozadina sa sigurnosnim uzorkom i fotografija moraju se preklapati.	230, 231, 235

5. ISPITIVANJA VANJSKOG UREĐAJA GNSS-A

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
2.	**Vizualna provjera vanjskog uređaja GNSS-a**		
2.1.	Sukladnost s dokumentacijom		
2.2.	Identifikacija/oznake		224 do 226
2.3	Materijali		219 do 223
3.	**Funkcionalna ispitivanja**		
3.1	Identifikacijski podatci senzora		98.99
3.2	Povezivanje vanjskog uređaja GNSS-a i jedinice u vozilu		123, 205

Br.	Ispitivanje	Opis	Povezani zahtjevi
3.3	Položaj GNSS-a		36, 37
3.4	Sučelje jedinice u vozilu kada je GNSS prijamnik vanjski u odnosu na jedinicu u vozilu		03
3.5	Slijed šifri (*cypher suite*) i normirani parametri domene		CSM_48, CSM_50
4.	**Ispitivanja utjecaja okoliša**		
4.1	Temperatura	Provjera funkcionalnost putem: ispitivanja u skladu s ISO 16750-4, poglavlje 5.1.1.2. Ispitivanje rada pri niskoj temperaturi (72 h na – 20 °C). Ovo se ispitivanje odnosi na IEC 60068-2-1: *Environmental testing – Part 2-1: Tests – Test A: Cold*. Ispitivanje u skladu s ISO 16750-4: poglavlje 5.1.2.2.: ispitivanje rada pri visokoj temperaturi (72 h na 70 °C). Ovo se ispitivanje odnosi na IEC 60068-2-2: *Basic environmental testing procedures; Part 2: Tests; Tests B: Dry heat*. Ispitivanje u skladu s ISO 16750-4, poglavlje 5.3.2.: brze promjene temperature s određenim trajanjem prelaska (– 20 °C/70 °C, 20 ciklusa, 1 h zadržavanja pri svakoj temperaturi). Skraćeni niz ispitivanja (između onih utvrđenih u odjeljku 3. ove tablice) može se obaviti pri nižoj temperaturi, višoj temperaturi i tijekom temperaturnih ciklusa.	213
4.2	Vlažnost	Provjeriti može li jedinica u vozilu izdržati cikličnu vlažnost (ispitivanje toplinom) putem IEC 60068-2-30, ispitivanje Db, šest ciklusa u trajanju od 24 h, pri svakom promjena temperature od + 25°C do + 55°C i relativna vlažnost od 97 % pri + 25°C te od 93 % pri + 55°C.	214
4.3	Mehanički	1. Sinusne vibracije: provjeriti može li jedinica u vozilu izdržati sinusne vibracije sa sljedećim značajkama: konstantan pomak između 5 i 11 Hz: vršna amplituda 10 mm; konstantno ubrzanje između 11 i 300 Hz: 5 g. Ovaj se zahtjev provjerava putem IEC 60068-2-6, ispitivanje Fc, uz minimalno trajanje ispitivanja od 3 × 12 sati (12 sati po osi). Norma ISO 16750-3 ne zahtijeva ispitivanje na sinusne vibracije za uređaje smještene u odspojenoj kabini vozila.	219

Br.	Ispitivanje	Opis	Povezani zahtjevi
		2. Nasumične vibracije: Ispitivanje u skladu s ISO 16750-3, poglavlje 4.1.2.8., *Test VIII: Commercial vehicle, decoupled vehicle cab*. Ispitivanje na nasumične vibracije, 10…2 000 Hz, RMS vertikalno 21,3 m/s^2, RMS uzdužno 11,8 m/s^2, RMS bočno 13,1 m/s^2, 3 osi, 32 h po osi, uključujući temperaturni ciklus – 20…70 °C. Ovo se ispitivanje odnosi na IEC 60068-2-64: *Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance*. 3. Udarci: mehanički udarac s 3 g, polu-sinus, u skladu s ISO 16750. Prethodno opisana ispitivanja provode se na različitim uzorcima vrste opreme koja se ispituje.	
4.4	Zaštita od vode i stranih tijela	Ispitivanje u skladu s ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (bez promjene parametara).	220, 221
4.5	Prenaponska zaštita	Provjeriti može li jedinica u vozilu izdržati snagu napajanja od: izvedbe od 24 V: 34 V pri + 40 °C 1 sat, izvedbe od 12 V: 17 V pri + 40 °C 1 sat. (ISO 16750-2, poglavlje 4.3.)	216
4.6	Zaštita od zamjene polariteta	Provjeriti može li jedinica u vozilu izdržati inverziju svojeg napajanja. (ISO 16750-2, poglavlje 4.7.)	216
4.7	Zaštita od kratkog spoja	Provjeriti jesu li ulazno/izlazni signali zaštićeni od kratkog spoja u odnosu na napajanje i uzemljenje. (ISO 16750-2, poglavlje 4.10.)	216
5	**Ispitivanja elektromagnetske kompatibilnosti (EMC)**		
5.1	Emisije zračenja i osjetljivosti	Sukladnost s Pravilnikom ECE R10	218

Br.	Ispitivanje	Opis	Povezani zahtjevi
5.2	Elektrostatičko pražnjenje	Sukladnost s ISO 10605:2008 + Tehnički ispravak:2010 + AMD1:2014: +/– 4 kV za kontakt i +/– 8 kV za ispuštanje zraka	218
5.3	Osjetljivost napajanja na električne prijelazne pojave	Za izvedbe od 24 V: sukladnost s ISO 7637-2 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1a: Vs = – 450V, Ri = 50 oma, impuls 2a: Vs = + 37V, Ri = 2 oma, impuls 2b: Vs = + 20V, Ri = 0,05 oma, impuls 3a: Vs = – 150V, Ri = 50 oma, impuls 3b: Vs = + 150V, Ri = 50 oma, impuls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms, impuls 5: Vs = + 120 V, Ri = 2,2 oma, td = 250 ms. Za izvedbe od 12 V: sukladnost s ISO 7637-1 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1: Vs = – 75 V, Ri = 10 oma, impuls 2a: Vs = + 37 V, Ri = 2 oma, impuls 2b: Vs = + 10 V, Ri = 0,05 oma, impuls 3a: Vs = –112 V, Ri = 50 oma, impuls 3b: Vs = + 75 V, Ri = 50 oma, impuls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms, impuls 5: Vs = + 65 V, Ri = 3 oma, td = 100 ms. Impuls 5 ispituje se samo za jedinice u vozilu namijenjene ugradnji u vozila na kojima se ne provodi jedinstvena vanjska zaštita od rasterećenja. Za prijedlog rasterećenja, vidjeti ISO 16750-2, 4. izdanje, poglavlje 4.6.4.	218

6. ISPITIVANJA UREĐAJA ZA KOMUNIKACIJU NA DALJINU

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
2.	**Vizualni pregled**		
2.1.	Sukladnost s dokumentacijom		
2.2.	Identifikacija/oznake		225, 226
2.3	Materijali		219 do 223

Br.	Ispitivanje	Opis	Povezani zahtjevi
4.	**Ispitivanja utjecaja okoliša**		
4.1	Temperatura	Provjera funkcionalnost putem: ispitivanja u skladu s ISO 16750-4, poglavlje 5.1.1.2.: ispitivanje rada pri niskoj temperaturi (72 h na – 20 °C). Ovo se ispitivanje odnosi na IEC 60068-2-1: *Environmental testing – Part 2-1: Tests – Test A: Cold*. Ispitivanje u skladu s ISO 16750-4, poglavlje 5.1.2.2.: ispitivanje rada pri visokoj temperaturi (72 h na 70 °C). Ovo se ispitivanje odnosi na IEC 60068-2-2: *Basic environmental testing procedures; Part 2: Tests; Tests B: Dry heat*. Ispitivanje u skladu s ISO 16750-4, poglavlje 5.3.2.: brze promjene temperature s određenim trajanjem prelaska (– 20 °C/70 °C, 20 ciklusa, 1 h zadržavanja pri svakoj temperaturi). Skraćeni niz ispitivanja (između onih utvrđenih u odjeljku 3. ove tablice) može se obaviti pri nižoj temperaturi, višoj temperaturi i tijekom temperaturnih ciklusa.	213
4.4	Zaštita od vode i stranih tijela	Ispitivanje u skladu s ISO 20653: *Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (targeted value IP40)*.	220, 221
5	**Ispitivanja elektromagnetske kompatibilnosti (EMC)**		
5.1	Emisije zračenja i osjetljivost	Sukladnost s Pravilnikom ECE R10	218
5.2	Elektrostatičko pražnjenje	Sukladnost s ISO 10605:2008 + Tehnički ispravak: 2010 + AMD1:2014: +/– 4 kV za kontakt i +/– 8 kV za ispuštanje zraka	218
5.3	Osjetljivost napajanja na električne prijelazne pojave	Za izvedbe od 24 V: sukladnost s ISO 7637-2 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1a: Vs = – 450V, Ri = 50 oma, impuls 2a: Vs = + 37V, Ri = 2 oma, impuls 2b: Vs = + 20V, Ri = 0,05 oma, impuls 3a: Vs = – 150V, Ri = 50 oma, impuls 3b: Vs = + 150V, Ri = 50 oma, impuls 4: Vs = – 16 V, Va = –12 V, t6 = 100 ms, impuls 5: Vs = + 120 V, Ri = 2,2 oma, td = 250 ms.	218

Br.	Ispitivanje	Opis	Povezani zahtjevi
		Za izvedbe od 12 V: sukladnost s ISO 7637-1 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1: Vs = – 75 V, Ri = 10 oma, impuls 2a: Vs = + 37 V, Ri = 2 oma, impuls 2b: Vs = + 10 V, Ri = 0,05 oma, impuls 3a: Vs = – 112 V, Ri = 50 oma, impuls 3b: Vs = + 75 V, Ri = 50 oma, impuls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms, impuls 5: Vs = + 65 V, Ri = 3 oma, td = 100 ms. Impuls 5 ispituje se samo za jedinice u vozilu namijenjene ugradnji u vozila na kojima se ne provodi jedinstvena vanjska zaštita od rasterećenja. Za prijedlog rasterećenja, vidjeti ISO 16750-2, 4. izdanje, poglavlje 4.6.4.	

7. FUNKCIONALNA ISPITIVANJA PAPIRA

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
2	**Opća ispitivanja**		
2.1	Broj slovnih znakova po retku	Vizualni pregled ispisa.	172
2.2	Najmanja veličina znaka	Vizualni pregled ispisa i pregled znakova.	173
2.3	Podržani skupovi znakova	Pisač mora podržavati znakove navedene u Dodatku 1. poglavlju 4. „Skupovi znakova”.	174
2.4	Određivanje ispisa	Provjera homologacije tahografa i vizualni pregled ispisa	174
2.5	Čitljivost i identifikacija ispisa	Pregled ispisa: dokazuje se izvješćima o ispitivanju i protokolima ispitivanja proizvođača. Svi homologacijski brojevi tahografa s kojima se može upotrebljavati papir pisača otisnuti su na papiru.	175, 177, 178
2.6	Dodavanje rukom pisanih napomena	Vizualni pregled: dostupno je polje za potpis vozača. Dostupna su polja za ostale dodatne rukom pisane unose.	180

Br.	Ispitivanje	Opis	Povezani zahtjevi
2.7	Dodatne pojedinosti o stranicama papira	Prednja i stražnja stranica papira mogu uključivati dodatne pojedinosti i informacije. Ove dodatne pojedinosti i informacije ne smiju utjecati na čitljivost ispisa. Vizualni pregled.	177, 178
3	**Ispitivanja skladištenja**		
3.1	Suha toplina	Pretkondicioniranje: 16 sati pri temperaturi + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 72 sata pri + 70 °C ± 2 °C. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176, 178 IEC 60068-2-2-Bb
2.2	Toplina s vlagom	Pretkondicioniranje: 16 sati pri temperaturi + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 144 sata pri + 55 °C ± 2 °C i relativnoj vlažnosti 93 % ± 3 %. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176, 178 IEC 60068-2-78-Cab
4	**Ispitivanja papira u upotrebi**		
4.1	Otpornost podloge na vlagu (neispisani papir)	Pretkondicioniranje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 144 sata pri + 55 °C ± 2 °C i relativnoj vlažnosti 93 % ± 3 %. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176 do 178 IEC 60068-2-78-Cab
4.2	Kvaliteta ispisa	Pretkondicioniranje: 24 sata pri + 40 °C ± 2 °C i relativnoj vlažnosti 93 % ± 3 %. Ispitno okruženje: ispis izrađen pri + 23 °C ± 2 °C. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176, 178
4.3	Otpornost na toplinu	Pretkondicioniranje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 2 sata pri + 70 °C ± 2 °C, suha toplina. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176, 178 IEC 60068-2-2-Bb
4.4	Otpornost na niske temperature	Pretkondicioniranje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 24 sata – 20°C ± 3 °C, suha hladnoća. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176 do 178 ISO 60068-2-1-Ab

Br.	Ispitivanje	Opis	Povezani zahtjevi
4.5	Otpornost na svjetlo	Pretkondicioniranje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 100 sati s osvijetljenošću od 5 000 luksa, pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176, 178

Mjerila čitljivosti za ispitivanja 3.x i 4.x:

Čitljivost ispisa osigurana je ako optičke gustoće ispunjavaju sljedeće granične vrijednosti:

ispisani znakovi: min. 1,0;

pozadina (neispisani papir): maks. 0,2.

Optičke gustoće dobivenih ispisa mjere se u skladu s DIN EN ISO 534.

Ispisi ne smiju pokazivati promjene dimenzija i moraju ostati jasno čitljivi.

8. ISPITIVANJA INTEROPERABILNOSTI

Br.	Ispitivanje	Opis
9.1. Ispitivanja interoperabilnosti između jedinica u vozilu i tahografskih kartica		
1	Uzajamna autentifikacija	Provjeriti provodi li se normalno uzajamna autentifikacija između jedinice u vozilu i kartice tahografa.
2	Ispitivanja pisanja/čitanja	Na jedinici u vozilu izvršiti tipičan scenarij aktivnosti. Scenarij se prilagođava vrsti kartice koja se ispituje i uključuje upise u što je više moguće elementarnih datoteka (EF) na kartici. Na jedinici u vozilu koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Na kartici koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Putem dnevnih ispisa provjeriti mogu li se svi odgovarajući zapisi ispravno pročitati.
9.2. Ispitivanja interoperabilnosti između jedinica u vozilu i senzora kretanja		
1	Uparivanje	Provjeriti provodi li se normalno uparivanje između jedinice u vozilu i senzora kretanja.
2	Ispitivanja aktivnosti	Na senzoru kretanja izvršiti tipičan scenarij aktivnosti. Scenarij uključuje uobičajenu aktivnost i stvaranje što je više moguće događaja ili kvarova. Na jedinici u vozilu koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Na kartici koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Putem dnevnog ispisa provjeriti mogu li se svi odgovarajući zapisi ispravno pročitati.

Br.	Ispitivanje	Opis
9.3. Ispitivanja interoperabilnosti između jedinica u vozilu i vanjskih uređaja GNSS-a (ako je primjenjivo)		
1	Uzajamna autentifikacija	Provjeriti provodi li se normalno uzajamna autentifikacija (povezivanje) između jedinice u vozilu i vanjskog uređaja GNSS-a.
2	Ispitivanja aktivnosti	Na vanjskom uređaju GNSS-a izvršiti tipičan scenarij aktivnosti. Scenarij uključuje uobičajenu aktivnost i stvaranje što je više moguće događaja ili kvarova. Na jedinici u vozilu koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Na kartici koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Putem dnevnog ispisa provjeriti mogu li se svi odgovarajući zapisi ispravno pročitati.

Dodatak 10

SIGURNOSNI ZAHTJEVI

U ovom se Dodatku navode zahtjevi u pogledu informatičke sigurnosti za sastavne dijelove uređaja za bilježenje podataka.

SEC_001 Sljedeći sastavni dijelovi uređaja za bilježenje podataka podliježu sigurnosnoj certifikaciji u skladu sa shemom zajedničkih mjerila:

— jedinica u vozilu,

— tahografska kartica,

— senzor kretanja,

— vanjski uređaj GNSS-a.

SEC_002 Minimalni zahtjevi u pogledu informatičke sigurnosti koje treba ispuniti svaki sastavni dio koji podliježe sigurnosnoj certifikaciji utvrđuju se u profilu zaštite sastavnog dijela u skladu sa shemom zajedničkih mjerila.

SEC_003 Europska komisija osigurava da su četiri profila zaštite usklađena s ovim Prilogom sponzorirana, razvijena i odobrena od strane državnih tijela nadležnih za certifikaciju informatičke sigurnosti organiziranih unutar Radne skupine za zajedničko tumačenje (eng. *Joint Interpretation Working Group*, JIWG) koja podržava uzajamno priznavanje certifikata u okviru europskog Sporazuma o uzajamnom priznavanju certifikata o evaluaciji sigurnosti informacijske tehnologije, i da su ti profili registrirani:

— profil zaštite za jedinicu u vozilu,

— profil zaštite za tahografsku karticu,

— profil zaštite za senzor kretanja,

— profil zaštite za vanjski uređaj GNSS-a.

Profil zaštite za jedinicu u vozilu odnosi se na slučajeve kada je jedinica u vozilu (VU) namijenjena za upotrebu s vanjskim uređajem GNSS-a i kada nije. U prvom su slučaju sigurnosni zahtjevi za vanjski uređaj GNSS-a navedeni u posebnom profilu zaštite.

SEC_004 Proizvođači sastavnih dijelova prema potrebi dorađuju i dovršavaju profil zaštite za odgovarajući sastavni dio, bez izmjena ili brisanja postojećih opasnosti, ciljeva, načina postupanja i propisanih funkcija za provedbu sigurnosti kako bi utvrdili sigurnosni cilj u odnosu na koji mogu zatražiti sigurnosnu certifikaciju sastavnog dijela.

SEC_005 Tijekom postupka evaluacije mora se dati izjava o strogoj sukladnosti takvog posebnog sigurnosnog cilja s odgovarajućim profilom zaštite.

SEC_006 Razina osiguranja za svaki profil zaštite je razina EAL4 pojačana s komponentama osiguranja ATE_DPT.2 i AVA_VAN.5.

Dodatak 11.

ZAJEDNIČKI SIGURNOSNI MEHANIZMI

SADRŽAJ

PREAMBULA		340
DIO A	SUSTAV TAHOGRAFA PRVE GENERACIJE	341
1.	UVOD	341
1.1.	Referentni dokumenti:	341
1.2.	Označivanje i pokrate	341
2.	KRIPTOGRAFSKI SUSTAVI I ALGORITMI	343
2.1.	Kriptografski sustavi	343
2.2.	Kriptografski algoritmi	343
2.2.1	Algoritam RSA	343
2.2.2	Algoritam raspršivanja	343
2.2.3	Algoritam šifriranja podataka	343
3.	KLJUČEVI I CERTIFIKATI	343
3.1.	Generiranje i raspodjela ključeva	343
3.1.1	Generiranje i raspodjela ključeva RSA	343
3.1.2	Ispitni ključevi RSA	345
3.1.3	Ključevi senzora kretanja	345
3.1.4	Generiranje i raspodjela T-DES ključeva razmjene podataka	345
3.2.	Ključevi	345
3.3.	Certifikati	345
3.3.1	Sadržaj certifikata	346
3.3.2	Izdani certifikati	348
3.3.3	Provjera i otvaranje certifikata	349
4.	MEHANIZAM UZAJAMNE AUTENTIFIKACIJE	349
5.	MEHANIZMI POVJERLJIVOSTI, INTEGRITETA I AUTENTIFIKACIJE PRIJENOSA PODATAKA IZMEĐU KARTICE I JEDINICE U VOZILU	352
5.1.	Siguran prijenos poruka	352
5.2.	Postupanje s pogreškama u sigurnom prijenosu poruka	354
5.3.	Algoritam izračuna kriptografskih kontrolnih zbrojeva	354
5.4.	Algoritam izračuna kriptograma za pouzdanost DO-ova	355
6.	MEHANIZMI DIGITALNOG POTPISA KOD PREUZIMANJA PODATAKA	355
6.1.	Generiranje potpisa	355
6.2.	Provjera potpisa	356

DIO B SUSTAV TAHOGRAFA DRUGE GENERACIJE 357
7. UVOD 357
7.1. Referentni dokumenti 357
7.2. Označivanje i skraćenice 357
7.3. Definicije 359
8. KRIPTOGRAFSKI SUSTAVI I ALGORITMI 359
8.1. Kriptografski sustavi 359
8.2. Kriptografski algoritmi 360
8.2.1 Simetrični algoritmi 360
8.2.2 Asimetrični algoritmi i normirani parametri domene 360
8.2.3 Algoritmi raspršivanja (*hashing*) 361
8.2.4 Slijedovi šifri (eng. *Cipher Suites*) 361
9. KLJUČEVI I CERTIFIKATI 361
9.1. Asimetrični parovi ključeva i certifikati javnih ključeva 361
9.1.1 Općenito 361
9.1.2 Europska razina 362
9.1.3 Razina države članice 362
9.1.4 Razina opreme: Jedinice u vozilu 363
9.1.5 Razina opreme: Tahografske kartice 365
9.1.6 Razina opreme: Vanjski uređaji GNSS-a 366
9.1.7 Pregled: Zamjena certifikata 367
9.2. Simetrični ključevi 368
9.2.1 Ključevi za sigurnu komunikaciju između jedinice u vozilu i senzora kretanja 368
9.2.2 Ključevi za sigurnu komunikaciju preko DSRC-a 372
9.3. Certifikati 375
9.3.1 Općenito 375
9.3.2 Sadržaj certifikata 375
9.3.3 Podnošenje zahtjeva za certifikate 377
10. UZAJAMNA AUTENTIFIKACIJA I SIGURAN PRIJENOS PORUKA IZMEĐU JEDINICA U VOZILU I KARTICA 378
10.1. Općenito 378
10.2. Uzajamna provjera lanca certifikata 379
10.2.1 Provjera lanca certifikata kartice koju provodi jedinica u vozilu 379
10.2.2 Provjera lanca certifikata jedinice u vozilu koju provodi kartica 381
10.3. Autentifikacija jedinice u vozilu 384
10.4. Autentifikacija čipa i dogovaranje ključa razmjene podataka 385

10.5. Siguran prijenos poruka 387
10.5.1 Općenito 387
10.5.2 Struktura sigurne poruke 388
10.5.3 Prekid procesa sigurnog prijenosa poruka 391
11. POVEZIVANJE, UZAJAMNA AUTENTIFIKACIJA I SIGURAN PRIJENOS PORUKA IZMEĐU JEDINICE U VOZILU I VANJSKOG UREĐAJA GNSS-A 392
11.1. Općenito 392
11.2. Povezivanje jedinice u vozilu i vanjskog uređaja GNSS-a (EGF-a) 393
11.3. Uzajamna provjera lanca certifikata 393
11.3.1 Općenito 393
11.3.2 Tijekom povezivanja jedinica u vozilu (VU) – EGF 393
11.3.3 Tijekom redovnog rada 394
11.4. Autentifikacija jedinice u vozilu, autentifikacija čipa i dogovaranje ključa razmjene podataka 395
11.5. Siguran prijenos poruka 395
12. UPARIVANJE I KOMUNIKACIJA IZMEĐU JEDINICE U VOZILU I SENZORA KRETANJA 396
12.1. Općenito 396
12.2. Uparivanje jedinice u vozilu i senzora kretanja upotrebom različitih generacija ključeva 396
12.3. Uparivanje i komunikacija između jedinice u vozilu i senzora kretanja upotrebom AES 397
12.4. Uparivanje jedinice u vozilu i senzora kretanja za različite generacije opreme 399
13. SIGURNOST KOMUNIKACIJE NA DALJINU PUTEM DSRC-A 399
13.1. Općenito 399
13.2. Šifriranje prijenosa podataka tahografa i generiranje MAC-a 400
13.3. Provjera i dešifriranje prijenosa podataka tahografa 401
14. POTPISIVANJE PREUZIMANJA PODATAKA I PROVJERA POTPISA 401
14.1. Općenito 401
14.2. Generiranje potpisa 402
14.3. Provjera potpisa 402

PREAMBULA

U ovom se Dodatku propisuju sigurnosni mehanizmi kojima se osiguravaju:

— uzajamna autentifikacija između različitih sastavnih dijelova opreme u sustavu tahografa;

— povjerljivost, integritet, autentičnost i/ili nepobitnost podataka koji se prenose između različitih sastavnih dijelova sustava tahografa ili koji se preuzimaju na vanjske medije za pohranu podataka.

Ovaj se Dodatak sastoji od dva dijela. U dijelu A utvrđeni su sigurnosni mehanizmi za sustav tahografa prve generacije (digitalni tahograf). U dijelu B utvrđeni su sigurnosni mehanizmi za sustav tahografa druge generacije (pametni tahograf).

Mehanizmi iz dijela A ovog Dodatka primjenjuju se ako najmanje jedan sastavni dio sustava tahografa uključenog u postupak uzajamne autentifikacije i/ili prijenosa podataka pripada opremi prve generacije.

Mehanizmi iz dijela B ovog Dodatka primjenjuju se ako oba sastavna dijela sustava tahografa uključenog u postupak uzajamne autentifikacije i/ili prijenosa podataka pripadaju opremi druge generacije.

U Dodatku 15. navedeno je više informacija o upotrebi sastavnih dijelova prve generacije u kombinaciji sa sastavnim dijelovima druge generacije.

DIO A

SUSTAV TAHOGRAFA PRVE GENERACIJE

1. UVOD

1.1. **Referentni dokumenti:**

U ovom su Dodatku upotrijebljeni sljedeći izvori:

SHA-1	Nacionalni institut za norme i tehnologiju SAD-a (NIST), *FIPS Publication 180-1 (Publikacija FIPS 180-1): Secure Hash Standard*, travanj 1995.
PKCS1	Laboratoriji RSA. PKCS # 1: *RSA Encryption Standard*, verzija 2.0, listopad 1998.
TDES	Nacionalni institut za norme i tehnologiju SAD-a (NIST), *FIPS Publication 46-3 Data Encryption Standard*, nacrt, 1999.
TDES-OP	ANSI X9.52, *Triple Data Encryption Algorithm Modes of Operation*, 1998.
ISO/IEC 7816-4	*Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interexchange*. Prvo izdanje, 1995. + Izmjena 1.: 1997.
ISO/IEC 7816-6	*Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements*. Prvo izdanje, 1996. + ispravak 1., 1998.
ISO/IEC 7816-8	*Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands*. Prvo izdanje, 1999.
ISO/IEC 9796-2	*Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function*. Prvo izdanje, 1997.
ISO/IEC 9798-3	*Information Technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm*. Drugo izdanje, 1998.
ISO 16844-3	Road vehicles – Tachograph systems – Part 3: Motion sensor interface.

1.2. **Označivanje i pokrate**

U ovom se Dodatku upotrebljavaju sljedeće oznake i pokrate:

(K_a, K_b, K_c)	snop ključeva koji upotrebljava algoritam za trostruko šifriranje podataka,
CA	certifikacijsko tijelo (eng. *Certification Authority*),
CAR	upućivanje na certifikacijsko tijelo (eng. *Certification Authority Reference*),
CC	kriptografski kontrolni zbroj (eng. *Cryptographic Checksum*),
CG	kriptogram (eng. *Cryptogram*),
CH	zaglavlje naredbe (eng. *Command Header*),
CHA	ovlaštenje nositelja certifikata (eng. *Certificate Holder Authorisation*),
CHR	upućivanje na nositelja certifikata (eng. *Certificate Holder Reference*),
D()	dešifriranje s pomoću DES-a,

DE	podatkovni element (eng. *Data Element*),
DO	podatkovni objekt (eng. *Data Object*),
d	privatni ključ RSA, privatni eksponent,
e	javni ključ RSA, javni eksponent,
E()	šifriranje s pomoću DES-a,
EQT	oprema (eng. *Equipment*),
Hash()	vrijednost raspršene poruke, izlazni podatak Hash,
Hash	funkcija raspršivanja (eng. *hash*),
KID	identifikator ključa (eng. *Key Identifier*),
Km	ključ TDES. Glavni ključ definiran u normi ISO 16844-3,
Km_{VU}	ključ TDES unesen u jedinice u vozilu,
Km_{WC}	ključ TDES unesen na kartice radionica,
m	predstavnik poruke, cijeli broj između 0 i n–1,
n	ključevi RSA, modul,
PB	bajtovi za popunjenje (eng. *Padding Bytes*),
PI	bajt indikatora popunjenja (za kriptograme povjerljivih podatkovnih objekata) (eng. *Padding Indicator byte*),
PV	nešifrirana vrijednost (eng. *Plain Value*),
s	predstavnik potpisa, cijeli broj između 0 i *n*–1,
SSC	brojač redoslijeda slanja (eng. *Send Sequence Counter*),
SM	siguran prijenos poruka (eng. *Secure Messaging*),
TCBC	način rada „ulančavanje šifriranih blokova TDEA" (eng. *TDEA Cipher Block Chaining Mode of Operation*),
TDEA	algoritam trostrukog šifriranja podataka (eng. *Triple Data Encryption Algorithm*),
TLV	vrijednost duljine oznake (eng. *Tag Length Value*),
VU	jedinica u vozilu (eng. *Vehicle Unit*),
X.C	certifikat korisnika X koji izdaje certifikacijsko tijelo,
X.CA	certifikacijsko tijelo korisnika X,
X.CA.PK $_{o}$ X.C	radnja otvaranja certifikata za izdvajanje javnog ključa. To je infiksni operator čiji je lijevi operand javni ključ certifikacijskog tijela, a desni operand je certifikat koji izdaje navedeno certifikacijsko tijelo. Ishod je javni ključ korisnika X čiji je certifikat desni operand,
X.PK	privatni ključ RSA korisnika X,
X.PK[I]	šifra RSA nekog podatka I, upotrebom javnog ključa korisnika X,
X.SK	privatni ključ RSA korisnika X,
X.SK[I]	šifra RSA nekog podatka I, upotrebom privatnog ključa korisnika X,
„xx"	heksadecimalna vrijednost,
||	operator ulančavanja.

2. KRIPTOGRAFSKI SUSTAVI I ALGORITMI

2.1. **Kriptografski sustavi**

CSM_001 U jedinicama u vozilu i tahografskim karticama upotrebljava se klasičan kriptografski sustav javnog ključa RSA kojim se osiguravaju sljedeći sigurnosni mehanizmi:

— autentifikacija između jedinica u vozilu i kartica,

— prijenos ključeva trostrukog procesa DES između jedinica u vozilu i tahografskih kartica,

— digitalni potpis podataka preuzetih s jedinica u vozilu ili tahografskih kartica na vanjske medije.

CSM_002 U jedinicama u vozilu i tahografskim karticama upotrebljava se trostruki simetričan kriptografski sustav DES za osiguranje mehanizma integriteta podataka tijekom razmjene korisničkih podataka između jedinica u vozilu i tahografskih kartica te za osiguranje, ako je primjereno, povjerljivosti razmjene podataka između jedinica u vozilu i tahografskih kartica.

2.2. **Kriptografski algoritmi**

2.2.1 *Algoritam RSA*

CSM_003 Algoritam RSA u potpunosti je definiran sljedećim odnosima:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Potpuniji opis funkcije RSA može se naći u izvoru [PKCS1]. Javni eksponent e za izračun RSA cijeli je broj između 3 i n–1 koji zadovoljava gcd(e, lcm(p–1, q–1)) = 1.

2.2.2 *Algoritam raspršivanja*

CSM_004 Mehanizmi digitalnog potpisa upotrebljavaju algoritam raspršivanja (*hash*) SHA-1 definiran u izvoru [SHA-1].

2.2.3 *Algoritam šifriranja podataka*

CSM_005 Algoritmi utemeljeni na DES-u upotrebljavaju se u načinu rada „ulančavanje šifriranih blokova”.

3. KLJUČEVI I CERTIFIKATI

3.1. **Generiranje i raspodjela ključeva**

3.1.1 *Generiranje i raspodjela ključeva RSA*

CSM_006 Ključevi RSA generiraju se preko tri funkcionalne hijerarhijske razine:

— europska razina,

— razina države članice,

— razina opreme.

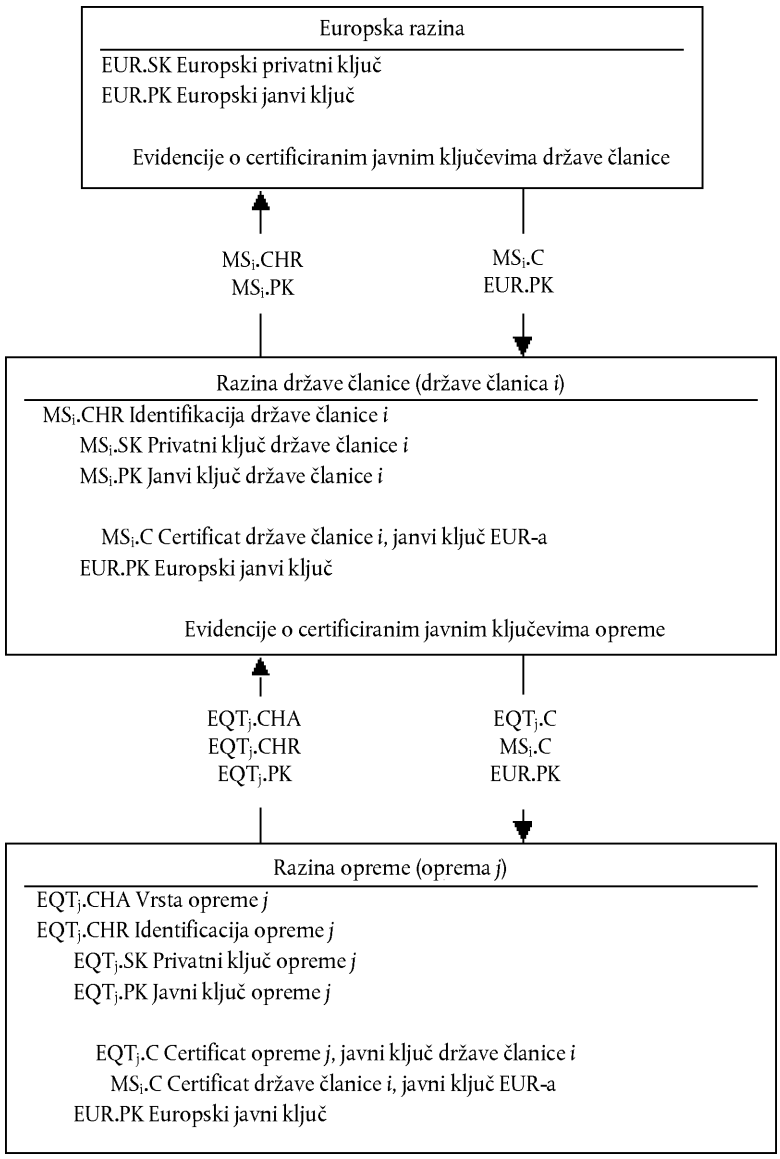
CSM_007 Na europskoj se razini generira jedinstveni europski par ključeva (EUR.SK i EUR.PK). Europski privatni ključ upotrebljava se za certifikaciju javnih ključeva država članica. Potrebno je voditi evidenciju svih certificiranih ključeva. Te zadatke obavlja europsko certifikacijsko tijelo, pod nadležnošću i odgovornosti Europske komisije.

CSM_008 Na razini države članice generira se par ključeva države članice (MS.SK i MS.PK). Javne ključeve država članica certificira europsko certifikacijsko tijelo. Privatni ključ države članice upotrebljava se za certificiranje javnih ključeva koji se unose u opremu (jedinica u vozilu ili tahografska kartica). Evidencija svih certificiranih javnih ključeva vodi se zajedno s identifikacijom opreme za koju su namijenjeni. Te zadatke obavlja certifikacijsko tijelo države članice. Država članica može redovito mijenjati svoj par ključeva.

CSM_009 Na razini opreme generira se jedan pojedinačni par ključeva (EQT.SK i EQT.PK) i unosi u svaki dio opreme. Javne ključeve opreme certificira certifikacijsko tijelo države članice. Te zadatke mogu obavljati proizvođači opreme, izvođači personalizacije opreme ili nadležna tijela države članice. Taj se par ključeva upotrebljava za usluge autentifikacije, digitalnog potpisa i šifriranja.

CSM_010 Povjerljivost privatnih ključeva održava se tijekom generiranja, prijenosa (ako postoji) i čuvanja.

Na sljedećoj je slici sažeti prikaz protoka podataka u ovom postupku:



3.1.2 *Ispitni ključevi RSA*

CSM_011 U svrhu ispitivanja opreme (uključujući ispitivanje interoperabilnosti) europsko certifikacijsko tijelo generira različit jedinstveni europski par ispitnih ključeva i najmanje dva para ispitnih ključeva države članice, čiji se javni ključevi certificiraju europskim privatnim ispitnim ključem. U opremu koja podliježe homologaciji proizvođači unose ispitne ključeve certificirane jednim od tih ispitnih ključeva države članice.

3.1.3 *Ključevi senzora kretanja*

Povjerljivost triju ključeva trostrukog DES-a koji su opisani u nastavku održava se na odgovarajući način tijekom generiranja, prijenosa (ako postoji) i čuvanja.

Za podršku sastavnim dijelovima tahografa koji zadovoljavaju normu ISO 16844, europsko certifikacijsko tijelo i certifikacijska tijela država članica dodatno osiguravaju sljedeće:

CSM_036 Europsko certifikacijsko tijelo generira KmVU i KmWC, dva neovisna i jedinstvena ključa trostrukog DES-a, te generira Km kao: $Km = Km_{VU}$ XOR Km_{WC} . Europsko certifikacijsko tijelo dostavlja navedene ključeve certifikacijskim tijelima država članica u odgovarajuće zaštićenim postupcima, na njihov zahtjev.

CSM_037 Certifikacijska tijela država članica:

— upotrebljavaju Km za šifriranje podataka senzora kretanja koje traže proizvođači senzora kretanja (podatci koji se šifriraju s Km definirani su u normi ISO 16844-3),

— u odgovarajuće zaštićenim postupcima proizvođačima jedinica u vozilu dostavljaju Km_{VU} za unošenje u jedinice u vozilu,

— osiguravaju unos ključa Km_{WC} u sve kartice radionica (`SensorInstallationSecData` u elementarnoj datoteci `Sensor_Installation_Data`) tijekom personalizacije kartice.

3.1.4 *Generiranje i raspodjela T-DES ključeva razmjene podataka*

CSM_012 Jedinice u vozilu i tahografske kartice, kao dio postupka uzajamne autentifikacije, generiraju i razmjenjuju podatke potrebne za izradu zajedničkog ključa trostrukog procesa DES-a. Povjerljivost te razmjene podataka zaštićena je mehanizmom šifriranja RSA.

CSM_013 Ovaj se ključ upotrebljava za sve naredne kriptografske radnje koje upotrebljavaju siguran prijenos poruka. Njegova valjanost ističe na kraju razmjene podataka (povlačenje kartice ili povrat kartice u početno stanje) i/ili nakon 240 upotreba (jedna upotreba ključa = jedna naredba koja upotrebljava sigurni prijenos poruka upućena kartici i odgovarajući odgovor).

3.2. **Ključevi**

CSM_014 Ključevi RSA imaju (bez obzira na razinu) sljedeće duljine: modul *n* 1 024 bita, javni eksponent *e* najviše 64 bita, privatni eksponent *d* 1 024 bita.

CSM_015 Ključevi trostrukog DES-a imaju oblik (K_a, K_b, K_a) pri čemu su K_a i K_b neovisni ključevi duljine 64 bita. Ne smiju biti namješteni bitovi koji utvrđuju paritetnu grešku.

3.3. **Certifikati**

CSM_016 Certifikati javnih ključeva su „nesamoopisni”, „karticom provjerljivi” certifikati (izvor: ISO/IEC 7816-8).

3.3.1 *Sadržaj certifikata*

CSM_017 Certifikati javnih ključeva RSA ugrađeni su u sljedeće podatke sljedećim redom:

Podatci	Format	Bajtova	Opis
CPI	CIJELI BROJ	1	Identifikator profila certifikata (u ovoj verziji „01”)
CAR	OKTETNI NIZ	8	Upućivanje na certifikacijsko tijelo
CHA	OKTETNI NIZ	7	Ovlaštenje nositelja certifikata
EOV	TimeReal	4	Istek valjanosti certifikata. Nije obvezno, popunjava se s „FF” ako se ne upotrebljava.
CHR	OKTETNI NIZ	8	Upućivanje na nositelja certifikata
n	OKTETNI NIZ	128	Javni ključ (modul)
e	OKTETNI NIZ	8	Javni ključ (javni eksponent)
		164	

Napomene:

1. „Identifikator profila certifikata” (CPI) označuje točnu strukturu autentifikacijskog certifikata. Može se upotrebljavati kao unutarnji identifikator opreme iz zaglavlja odgovarajućeg popisa koji opisuje ulančavanje podatkovnih elemenata unutar certifikata.

   Zaglavlje popisa pridruženo sadržaju tog certifikata sljedeće je:

‘4D’	‘16’	‘5F 29’	‘01’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	‘81 80’	‘82’	‘08’
Oznaka proširenog zaglavlja popisa	Duljina zaglavlja popisa	Oznaka CPI	Duljina CPI	Oznaka CAR	Duljina CAR	Oznaka CHA	Duljina CHA	Oznaka EOV	Duljina EOV	Oznaka CHR	Duljina CHR	Oznaka javnog ključa (konstruirana)	Duljina narednih DO-ova	Oznaka modula	Duljina modula	Oznaka javnog eksponenta	Duljina javnog eksponenta

2. „Upućivanje na certifikacijsko tijelo” (CAR) služi za identifikaciju certifikacijskog tijela (CA) koje je izdalo certifikat tako da se podatkovni element može istodobno upotrebljavati kao identifikator ključa tijela za upućivanje na javni ključ certifikacijskog tijela (za kodiranje vidjeti identifikator ključa u nastavku).

3. „Ovlaštenje nositelja certifikata” (CHA) upotrebljava se za identifikaciju prava nositelja certifikata. Ono se sastoji od identifikatora (ID) tahografske aplikacije i vrste opreme za koju je certifikat namijenjen (prema podatkovnom elementu `EquipmentType`, ‘00’ za državu članicu).

4. „Upućivanje na nositelja certifikata” (CHR) služi za jedinstvenu identifikaciju nositelja certifikata tako da se podatkovni element može istodobno upotrebljavati kao identifikator ključa nositelja za upućivanje na javni ključ nositelja certifikata.

5. Identifikatori ključa na jedinstven način identificiraju nositelja certifikata ili certifikacijsko tijelo. Oni su kodirani kako slijedi:

5.1. Oprema (VU ili kartica):

Podatci	Serijski broj opreme	Datum	Tip	Proizvođač
Duljina	4 bajta	2 bajta	1 bajt	1 bajt
Vrijednost	cijeli broj	BCD kodiranje mm gg	specifičan za proizvođača	kôd proizvođača

U slučaju jedinice u vozilu proizvođač, prilikom traženja certifikata, može ili ne mora znati identifikaciju opreme u koju se unose ključevi.

U prvom slučaju proizvođač će tijelu svoje države članice na certifikaciju poslati identifikaciju opreme s javnim ključem. Certifikat će nakon toga sadržavati identifikaciju opreme, a proizvođač mora osigurati da se ključevi i certifikat unesu u opremu za koju su namijenjeni. Identifikator ključa ima prethodno prikazani oblik.

U potonjem slučaju proizvođač mora na jedinstven način identificirati svaki zahtjev za certifikat i poslati takvu identifikaciju s javnim ključem tijelu svoje države članice na certifikaciju. Certifikat će sadržavati identifikaciju zahtjeva. Proizvođač mora povratno obavijestiti tijelo svoje države članice o dodjeli ključa opremi (tj. identifikaciji zahtjeva za certifikat, identifikaciji opreme) nakon ugradnje ključa u opremu. Identifikator ključa ima sljedeći oblik:

Podatci	Serijski broj zahtjeva za certifikat	Datum	Tip	Proizvođač
Duljina	4 bajta	2 bajta	1 bajt	1 bajt
Vrijednost	cijeli broj	BCD kodiranje mm gg	‘FF’	kôd proizvođača

5.2. Certifikacijsko tijelo:

Podatci	Identifikacija tijela	Serijski broj ključa	Dodatne informacije	Identifikator
Duljina	4 bajta	1 bajt	2 bajta	1 bajt

Vrijednost	1-bajtni numerički kod države 3-bajtni alfanumerički kod države	cijeli broj	dodatno kodiranje (specifično za CA); 'FF FF' ako nije upotrijebljeno	'01'

Serijski broj ključa upotrebljava se za raspoznavanje različitih ključeva države članice u slučaju da se ključ promijeni.

6. Osobe koje vrše provjeru certifikata implicitno znaju da je certificirani javni ključ RSA ključ koji se odnosi na autentifikaciju, provjeru digitalnog potpisa i šifriranje za usluge povjerljivosti (certifikat ne sadržava identifikator objekta koji bi to navodio).

3.3.2 *Izdani certifikati*

CSM_018 Izdani certifikat je digitalni potpis s djelomičnim obnavljanjem sadržaja certifikata u skladu s normom ISO/IEC 9796-2 (osim njezina priloga A4) s priloženim „upućivanjem na certifikacijsko tijelo".

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, Hash(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Sa sadržajem certifikata = Cc = C_r || C_n

106 bajtova 58 bajtova

Napomene:

1. Duljina ovog certifikata je 194 bajta.

2. CAR, koji je skriven potpisom, isto je tako priložen potpisu tako da javni ključ certifikacijskog tijela može biti odabran za provjeru certifikata.

3. Osoba koja provjerava certifikat implicitno je upoznata s algoritmom koji je certifikacijsko tijelo upotrijebilo za potpisivanje certifikata.

4. Zaglavlje popisa pridruženo navedenom izdanom certifikatu sljedeće je:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Oznaka certifikata CV (konstruirana)	Duljina narednih DO-ova	Oznaka potpisa	Duljina potpisa	Oznaka ostatka	Duljina ostatka	Oznaka CAR	Duljina CAR

3.3.3 *Provjera i otvaranje certifikata*

Provjera i otvaranje certifikata sastoji se od provjere potpisa prema normi ISO/IEC 9796 2, preuzimanja sadržaja certifikata i sadržanog javnog ključa: X.PK = X.CA.PK $_o$ X.C, te provjere valjanosti certifikata.

CSM_019 Obuhvaća sljedeće korake:

Provjeriti potpis i preuzeti sadržaj:

— iz X.C preuzeti Sign, C_n' i CAR': X.C = Sign || C_n' || CAR'

128 bajtova | 58 bajtova | 8 bajtova,

— odabrati iz CAR' odgovarajući javni ključ certifikacijskog tijela (ako to nije učinjeno ranije na neki drugi način),

— otvoriti Sign s javnim ključem CA: Sr'= X.CA.PK [Sign],

— provjeriti da Sr' započinje sa '6A' i završava s 'BC',

— izračunati C_r' i H' iz: Sr' = '6A' || C_r' || H' || 'BC'

106 bajtova | 20 bajtova,

— ponovno učitati sadržaj certifikata C' = C_r' || C_n',

— provjeriti *Hash*(C') = H'.

Ako su provjere u redu, certifikat je autentičan, njegov sadržaj je C'.

Provjeriti valjanost. Iz C':

— prema potrebi, provjeriti datum isteka valjanosti.

Preuzeti i pohraniti javni ključ, identifikator ključa, ovlaštenje nositelja certifikata i istek valjanosti certifikata iz C':

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MEHANIZAM UZAJAMNE AUTENTIFIKACIJE

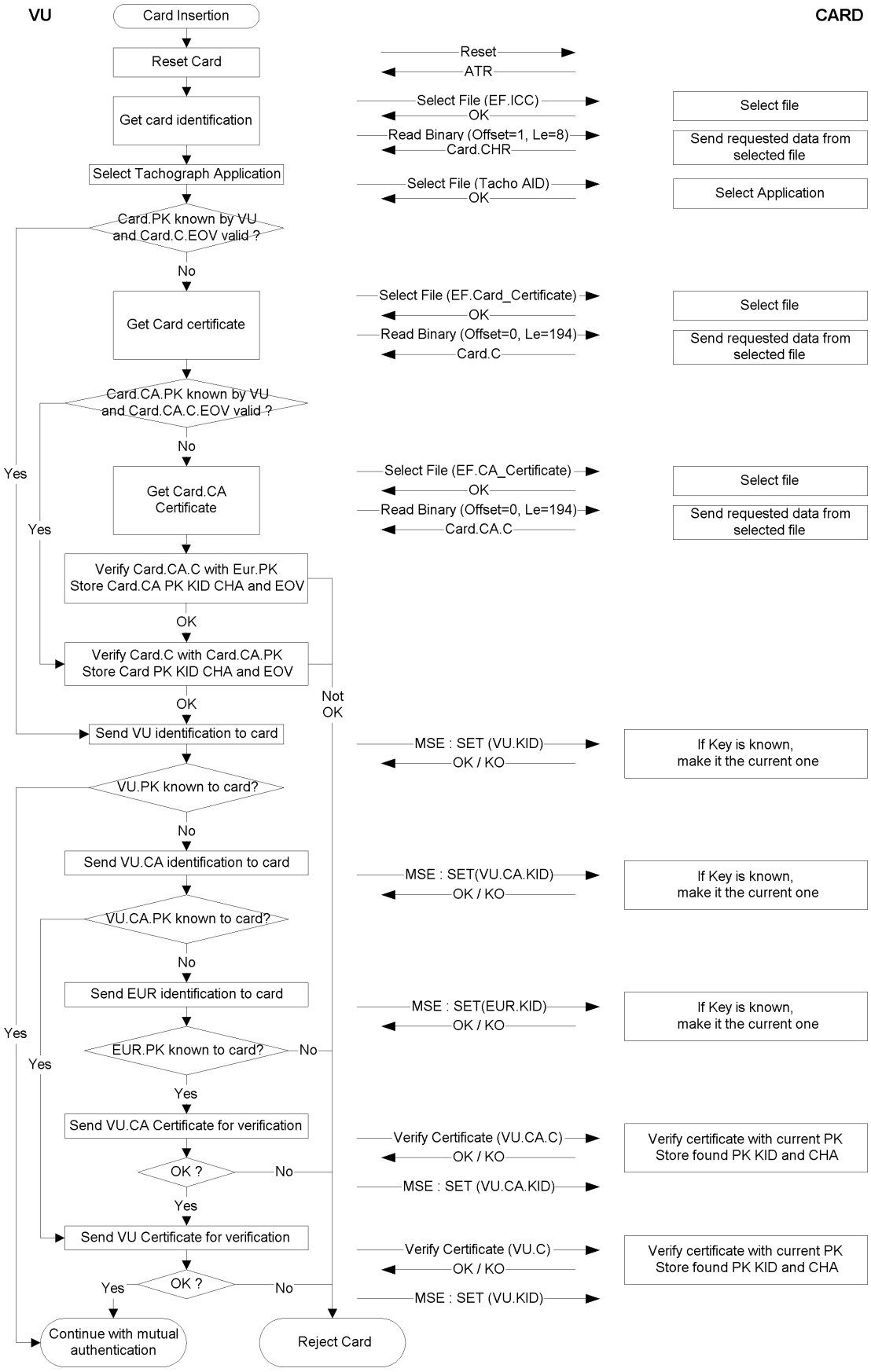
Uzajamna autentifikacija između kartica i jedinica u vozilu (VU) temelji se na sljedećem načelu:

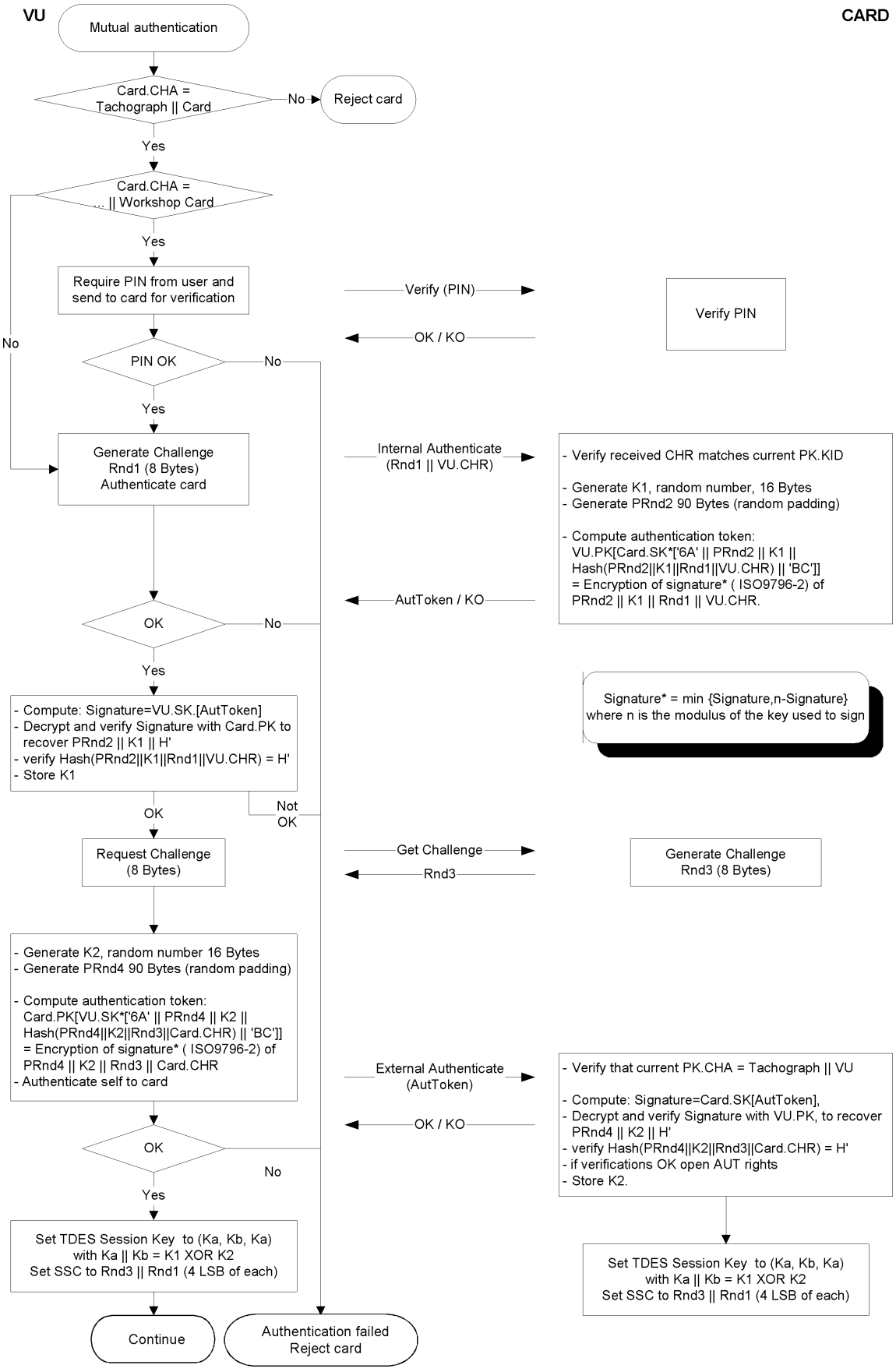
Svaka strana dokazuje drugoj strani da posjeduje valjan par ključeva čiji je javni ključ certificiralo certifikacijsko tijelo države članice koje je certificiralo europsko certifikacijsko tijelo.

Dokazivanje se obavlja potpisivanjem privatnim ključem slučajnog broja koji je poslala druga strana koja mora obnoviti slučajni broj poslan prilikom provjere potpisa.

Mehanizam aktivira jedinica u vozilu pri umetanju kartice. On započinje razmjenom certifikata i otvaranjem javnih ključeva te završava postavljanjem ključa razmjene podataka.

CSM_020 Upotrebljava se sljedeći protokol (strelice ukazuju na naredbe i razmijenjene podatke (vidjeti Dodatak 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. MEHANIZMI POVJERLJIVOSTI, INTEGRITETA I AUTENTIFIKACIJE PRIJENOSA PODATAKA IZMEĐU KARTICE I JEDINICE U VOZILU

5.1. **Siguran prijenos poruka**

CSM_021 Integritet prijenosa podataka između jedinice u vozilu i kartice zaštićen je sigurnim prijenosom poruka u skladu s izvorima [ISO/IEC 7816-4] i [ISO/IEC 7816-8].

CSM_022 Kada podatci trebaju biti zaštićeni tijekom prijenosa, podatkovni objekt kriptografskog kontrolnog zbroja dodaje se podatkovnim objektima koji se šalju u okviru naredbe ili odgovora. Kriptografski kontrolni zbroj provjerava primatelj.

CSM_023 Kriptografski kontrolni zbroj podataka koji se šalju u okviru naredbe objedinjuje zaglavlje naredbe i sve poslane podatkovne objekte (= > CLA = '0C', a svi podatkovni objekti moraju biti sažeti s oznakama u kojima je b1 = 1).

CSM_024 Bajtovi informacija o stanju odgovora zaštićeni su kriptografskim kontrolnim zbrojem ako odgovor ne sadržava podatkovno polje.

CSM_025 Kriptografski kontrolni zbroj ima duljinu od četiri bajta.

Struktura naredbi i odgovora pri sigurnom prijenosu poruka stoga je sljedeća:

Upotrijebljeni DO-vi su parcijalni skup DO-ova za siguran prijenos poruka opisan u normi ISO/IEC 7816-4:

Oznaka	Mnemonik	Značenje
'81'	T_{PV}	Nešifrirana vrijednost, podatci koji nisu kodirani u BER-TLV (zaštićena CC-om)
'97'	$\mathbf{T_{LE}}$	Vrijednost Le u nezaštićenoj naredbi (zaštićena CC-om)
'99'	T_{SW}	Statusne informacije (zaštićene CC-om)
'8E'	T_{CC}	Kriptografski kontrolni zbroj
'87'	$T_{PI\ CG}$	Bajt indikatora popunjenja || kriptogram (vrijednost koja nije kodirana u BER-TLV)

Pod pretpostavkom nezaštićenog para odgovora naredbe:

Zaglavlje naredbe				Sadržaj naredbe		
CLA	INS	P1	P2	[Polje L_c]	[Podatkovno polje]	[Polje L_e]
četiri bajta				Bajtovi L, označeni kao B_1 do B_L		

Sadržaj odgovora	Nastavak odgovora	
[Podatkovno polje]	SW1	SW2
L_r bajtova podataka	dva bajta	

Odgovarajući par zaštićenog odgovora naredbe je:

Zaštićena naredba:

Zaglavlje naredbe (CH)				Sadržaj naredbe										
CLA	INS	P1	P2	[Novo polje L_c]	[Novo podatkovno polje]									[Novo polje L_e]
'OC'				Duljina novog podatkovnog polja	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
					'81'	L_c	Podatkovno polje	'97'	'01'	L_e	'8E'	'04'	CC	

Podatci koje treba integrirati u kontrolni zbroj = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = bajtovi za popunjenje (80 .. 00) u skladu s normom ISO-IEC 7816-4 i metodom 2. iz norme ISO 9797.

DO PV i LE prisutni su samo kada postoje neki odgovarajući podatci u nezaštićenoj naredbi.

Zaštićeni odgovor:

1. Slučaj kada podatkovno polje odgovora nije prazno i ne treba ga zaštititi u pogledu povjerljivosti:

Sadržaj odgovora						Nastavak odgovora
[Novo podatkovno polje]						novi SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	podatkovno polje	'8E'	'04'	CC	

Podatci koje treba integrirati u kontrolni zbroj = T_{PV} || L_{PV} || PV || PB

2. Slučaj kada podatkovno polje odgovora nije prazno i treba ga zaštititi u pogledu povjerljivosti:

Sadržaj odgovora						Nastavak odgovora
[Novo podatkovno polje]						novi SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Podatci koje prenosi CG: podatci koji nisu kodirani u BER-TLV i bajtovi za popunjenje.

Podatci koje treba integrirati u kontrolni zbroj = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Slučaj kada je podatkovno polje odgovora prazno:

Sadržaj odgovora						Nastavak odgovora
[Novo podatkovno polje]						novi SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Novi SW1 SW2	'8E'	'04'	CC	

Podatci koje treba integrirati u kontrolni zbroj = T_{SW} || L_{SW} || SW || PB

5.2. **Postupanje s pogreškama u sigurnom prijenosu poruka**

CSM_026 Kada tahografska kartica pri tumačenju naredbe prepozna pogrešku u sigurnom prijenosu poruka (SM), tada se statusni bajtovi moraju vratiti bez SM-a. U skladu s normom ISO/IEC 7816-4, za označivanje pogrešaka u sigurnom prijenosu poruka (SM) utvrđeni su sljedeći statusni bajtovi:

'66 88': neuspješna provjera kriptografskog kontrolnog zbroja,

'69 87': nedostaju očekivani podatkovni objekti sigurnog prijenosa poruka,

'69 88': neispravni podatkovni objekti sigurnog prijenosa poruka.

CSM_027 Kada tahografska kartica vrati statusne bajtove bez SM DO ili s pogrešnim SM DO, jedinica u vozilu (VU) mora prekinuti razmjenu podataka.

5.3. **Algoritam izračuna kriptografskih kontrolnih zbrojeva**

CSM_028 Kriptografski kontrolni zbrojevi sastavljeni su upotrebom *retail* MAC-ova u skladu s ANSI X9.19 s DES-om:

— početni stadij: početni kontrolni blok y0 je E(Ka, SSC),

— naredni stadij: kontrolni blokovi y1, .., yn računaju se s pomoću Ka,

— konačni stadij: kriptografski kontrolni zbroj izračunava se od posljednjeg kontrolnog bloka yn kako slijedi: E(Ka, D(Kb, yn)).

pri čemu E() označuje šifriranje s pomoću DES-a, a D() označuje dešifriranje s pomoću DES-a.

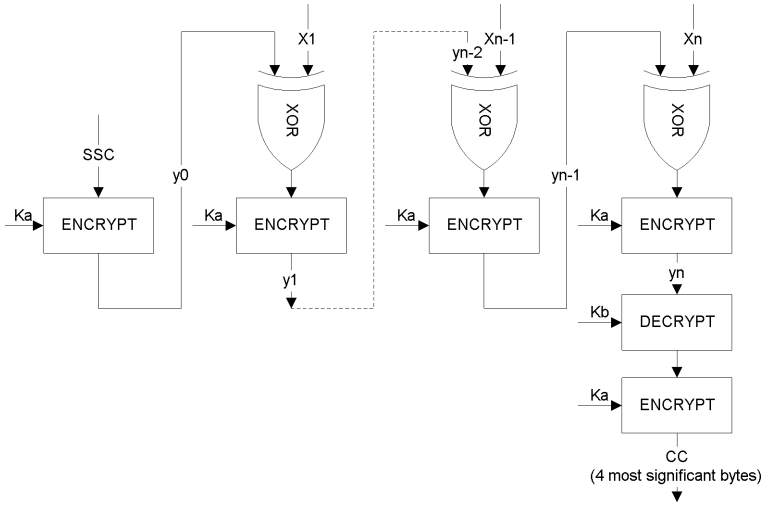
Četiri se najznačajnija bajta kriptografskog kontrolnog zbroja prenose.

CSM_029 Brojač redoslijeda slanja (SSC) aktivira se u postupku dogovaranja ključa na:

početni SCC: Rnd3 (4 najmanje značajna bajta) || Rnd1 (4 najmanje značajna bajta).

CSM_030 Brojač redoslijeda slanja povećava se za 1 svaki put prije izračuna MAC-a (tj. SSC za prvu naredbu je početni SCC + 1, SCC za prvi odgovor je početni SCC + 2).

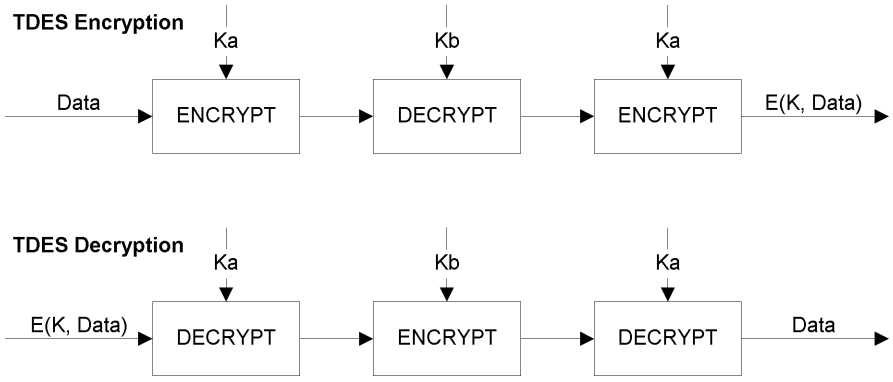
Na sljedećoj je slici prikazan izračun *retail* MAC-a:



5.4. **Algoritam izračuna kriptograma za pouzdanost DO-ova**

CSM_031 Kriptogrami se izračunavaju s pomoću TDEA u načinu rada TCBC u skladu s izvorima [TDES] i [TDES-OP] i s nultim vektorom kao blokom početne vrijednosti.

Na sljedećoj je slici prikazana primjena ključeva u TDES-u:



6. MEHANIZMI DIGITALNOG POTPISA KOD PREUZIMANJA PODATAKA

CSM_032 Posebna namjenska oprema (IDE) pohranjuje podatke primljene s opreme (jedinica u vozilu ili kartica) tijekom jednog procesa preuzimanja podataka u jednoj fizičkoj podatkovnoj datoteci. Ta datoteka mora sadržavati certifikate MS_i.C i EQT.C. Datoteka sadržava digitalne potpise podatkovnih blokova navedenih u Dodatku 7. „Protokoli preuzimanja podataka”.

CSM_033 Digitalni potpisi preuzetih podataka upotrebljavaju shemu digitalnog potpisa s takvim dodatkom da se preuzeti podatci mogu čitati bez dešifriranja, ako se to želi.

6.1. **Generiranje potpisa**

CSM_034 Generiranje podatkovnog potpisa koje se provodi s pomoću opreme slijedi shemu potpisa s dodatkom koji je definiran u izvoru [PKCS1] s funkcijom raspršivanja (*hash*) SHA-1:

Potpis = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Podatci))]

PS = oktetni niz (eng. *octet string*) za popunjenje s takvom vrijednošću ‘FF’ da je duljina 128.

DER(SHA-1(*M*)) je kodiranje identifikatora (ID) algoritma za funkciju raspršivanja (*hash*) i vrijednost raspršivanja u vrijednosti ASN.1 tipa DigestInfo (posebna pravila kodiranja):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’||vrijednost raspršivanja (*hash*).

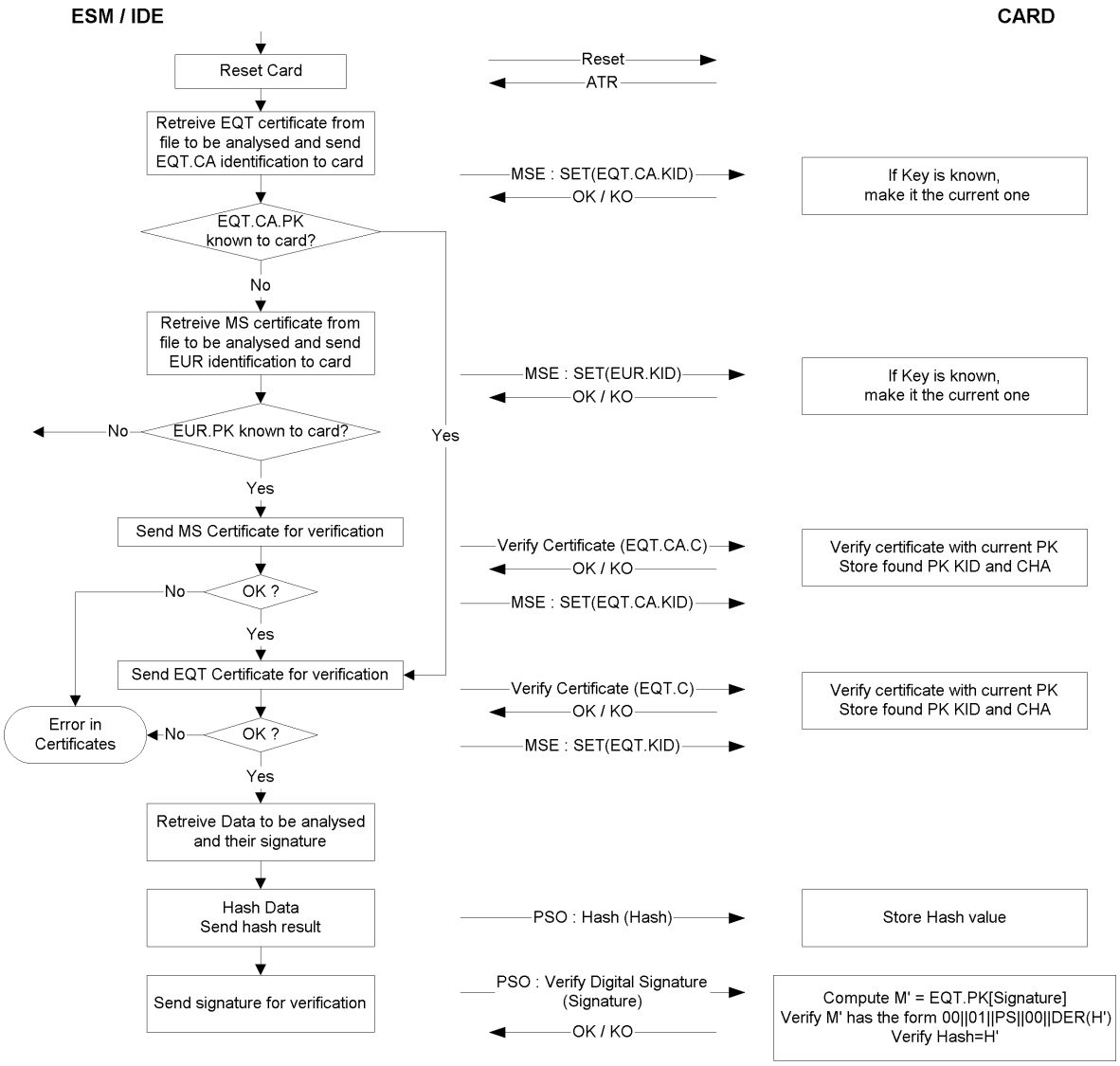
6.2. Provjera potpisa

CSM_035 Provjera potpisa na preuzetim podatcima slijedi shemu potpisa s dodatkom koji je opisan u izvoru [PKCS1] s funkcijom raspršivanja (*hash*) SHA-1.

Verifikator mora neovisno poznavati europski javni ključ EUR.PK (i u njega imati povjerenja).

U sljedećoj je tablici prikazan protokol koji IDE s kontrolnom karticom može slijediti za provjeru integriteta podataka preuzetih i pohranjenih na ESM (vanjski medij za pohranu podataka). Kontrolna kartica upotrebljava se za dešifriranje digitalnih potpisa. U tom slučaju takva funkcija ne mora biti ugrađena u IDE.

Oprema koja je preuzela i potpisala podatke koji se analiziraju označena je s EQT.



DIO B

SUSTAV TAHOGRAFA DRUGE GENERACIJE

7. UVOD

7.1. Referentni dokumenti

U ovom su dijelu ovog Dodatka upotrijebljeni sljedeći izvori:

AES	Nacionalni institut za norme i tehnologiju SAD-a (NIST), FIPS PUB 197: *Advanced Encryption Standard (AES)*, 26. studenoga 2001.
DSS	Nacionalni institut za norme i tehnologiju (NIST), FIPS PUB 186-4: *Digital Signature Standard (DSS)*, srpanj 2013.
ISO 7816-4	ISO/IEC 7816-4, *Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*, treće izdanje, 15.4.2013.
ISO 7816-8	ISO/IEC 7816-8, *Identification cards – Integrated circuit cards – Part 8: Commands for security operations*, drugo izdanje, 1.6.2004.
ISO 8825-1	ISO/IEC 8825-1, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*, četvrto izdanje, 15.12.2008.
ISO 9797-1	ISO/IEC 9797-1, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*, drugo izdanje, 1.3.2011.
ISO 10116	ISO/IEC 10116, *Information technology – Security techniques – Modes of operation of an n-bit block cipher*, treće izdanje, 1.2.2006.
ISO 16844-3	ISO/IEC 16844-3, *Road vehicles – Tachograph systems – Part 3: Motion sensor interface*, prvo izdanje, 2004., uključujući tehnički ispravak 1 2006.
RFC 5480	*Elliptic Curve Cryptography Subject Public Key Information*, ožujak 2009.
RFC 5639	*Elliptic Curve Cryptography (ECC) – Brainpool Standard Curves and Curve Generation*, 2010.
RFC 5869	*HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*, svibanj 2010.
SHS	Nacionalni institut za norme i tehnologiju SAD-a (NIST), FIPS PUB 180-4: *Secure Hash Standard*, ožujak 2012.
SP 800-38B	Nacionalni institut za norme i tehnologiju SAD-a (NIST), Posebno izdanje 800-38B: *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, 2005.
TR-03111	*BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00*, 28.6.2012.

7.2. Označivanje i skraćenice

U ovom se Dodatku upotrebljavaju sljedeće oznake i skraćenice:

AES	norma naprednog šifriranja (eng. *Advanced Encryption Standard*)
CA	certifikacijsko tijelo (eng. *Certificate Authority*)
CAR	upućivanje na certifikacijsko tijelo (eng. *Certificate Authority Reference*)
CBC	ulančavanje šifriranih blokova (eng. *Cipher Block Chaining*) (način rada)

CH	zaglavlje naredbe (eng. *Command Header*)
CHA	ovlaštenje nositelja certifikata (eng. *Certificate Holder Authorisation*)
CHR	upućivanje na nositelja certifikata (eng. *Certificate Holder Reference*)
CV	konstantni vektor (eng. *Constant Vector*)
DER	posebna pravila kodiranja (eng. *Distinguished Encoding Rules*)
DO	podatkovni objekt (eng. *Data Object*)
DSRC	komunikacijski sustav kratkog dometa (eng. *Dedicated Short Range Communication*)
ECC	kriptografija eliptičkih krivulja (eng. *Elliptic Curve Cryptography*)
ECDSA	algoritam digitalnog potpisa na temelju eliptičkih krivulja (eng. *Elliptic Curve Digital Signature Algorithm*)
ECDH	eliptička krivulja Diffie-Hellman (algoritam dogovaranja ključa)
EGF	vanjski uređaj GNSS-a (eng. *External GNSS Facility*)
EQT	oprema (eng. *Equipment*)
IDE	posebna namjenska oprema (eng. *Intelligent Dedicated Equipment*)
K_M	glavni ključ senzora kretanja koji omogućuje uparivanje jedinice u vozilu sa senzorom kretanja
K_{M-VU}	ključ unesen u jedinice u vozilu koji omogućuje jedinici u vozilu (VU) da dobije glavni ključ senzora kretanja ako je kartica radionice umetnuta u VU
K_{M-WC}	ključ unesen u kartice radionice koji omogućuje jedinici u vozilu (VU) da dobije glavni ključ senzora kretanja ako je kartica radionice umetnuta u VU
MAC	kod za autentifikaciju poruke (eng. *Message Authentication Code*)
MoS	senzor kretanja (eng. *Motion Sensor*)
MSB	najznačajniji bit (eng. *Most Significant Bit*)
PKI	infrastruktura javnih ključeva (eng. *Public Key Infrastructure*)
RCF	uređaj za komunikaciju na daljinu (eng. *Remote Communication Facility*)
SSC	brojač redoslijeda slanja (eng. *Send Sequence Counter*)
SM	siguran prijenos poruka (eng. *Secure Messaging*)
TDES	norma trostrukog šifriranja podataka (eng. *Triple Data Encryption Standard*)
TLV	vrijednost duljine oznake (eng. *Tag Length Value*)
VU	jedinica u vozilu (eng. *Vehicle Unit*)
X.C	certifikat javnog ključa korisnika X
X.CA	certifikacijsko tijelo koje je izdalo certifikat korisniku X
X.CAR	upućivanje na certifikacijsko tijelo koje je izdalo certifikat korisniku X
X.CHR	upućivanje na nositelja certifikata navedenog u certifikatu korisnika X
X.PK	javni ključ korisnika X
X.SK	privatni ključ korisnika X
$X.PK_{eph}$	kratkotrajni javni ključ korisnika X
$X.SK_{eph}$	kratkotrajni privatni ključ korisnika X
‘xx’	heksadecimalna vrijednost
||	operator ulančavanja

7.3. **Definicije**

Definicije pojmova koji se upotrebljavaju u ovom Dodatku navedene su u odjeljku I. Priloga I.C.

8. KRIPTOGRAFSKI SUSTAVI I ALGORITMI

8.1. **Kriptografski sustavi**

CSM_38 Jedinice u vozilu i tahografske kartice upotrebljavaju kriptografski sustav eliptičkih krivulja javnog ključa za pružanje sljedećih sigurnosnih usluga:

— uzajamna autentifikacija između jedinice u vozilu i kartice,

— dogovor AES ključeva razmjene podataka između jedinice u vozilu i kartice,

— osiguravanje autentičnosti, integriteta i nepobitnosti podataka preuzetih s jedinica u vozilu ili tahografskih kartica na vanjske medije.

CSM_39 Jedinice u vozilu i vanjski uređaji GNSS-a upotrebljavaju kriptografski sustav eliptičkih krivulja javnog ključa za pružanje sljedećih sigurnosnih usluga:

— povezivanje jedinice u vozilu i vanjskog uređaja GNSS-a,

— uzajamna autentifikacija između jedinice u vozilu i vanjskog uređaja GNSS-a,

— dogovor AES ključa razmjene podataka između jedinice u vozilu i vanjskog uređaja GNSS-a.

CSM_40 Jedinice u vozilu i tahografske kartice upotrebljavaju simetrični kriptografski sustav na temelju AES-a za pružanje sljedećih sigurnosnih usluga:

— osiguravanje autentičnosti i integriteta podataka razmijenjenih između jedinice u vozilu i tahografske kartice,

— ako je primjenjivo, osiguravanje povjerljivosti podataka razmijenjenih između jedinice u vozilu i tahografske kartice.

CSM_41 Jedinice u vozilu i vanjski uređaji GNSS-a upotrebljavaju simetrični kriptografski sustav na temelju AES-a za pružanje sljedećih sigurnosnih usluga:

— osiguravanje autentičnosti i integriteta podataka razmijenjenih između jedinice u vozilu i vanjskog uređaja GNSS-a.

CSM_42 Jedinice u vozilu i senzori kretanja upotrebljavaju simetrični kriptografski sustav na temelju AES-a za pružanje sljedećih sigurnosnih usluga:

— uparivanje jedinice u vozilu i senzora kretanja,

— uzajamna autentifikacija između jedinice u vozilu i senzora kretanja,

— osiguranje povjerljivosti podataka razmijenjenih između jedinice u vozilu i senzora kretanja.

CSM_43 Jedinice u vozilu i kontrolne kartice upotrebljavaju simetrični kriptografski sustav na temelju AES-a za pružanje sljedećih sigurnosnih usluga na sučelju za komunikaciju na daljinu:

— osiguranje povjerljivosti, autentičnosti i integriteta podataka koje jedinica u vozilu šalje kontrolnoj kartici.

Napomene:

— Konkretnije, podatci se iz jedinice u vozilu šalju uređaju za daljinsko ispitivanje (eng. *remote interrogator*) koji je pod kontrolom službenika za kontrolu s pomoću uređaja za komunikaciju na daljinu koji može biti vanjski ili unutarnji u odnosu na jedinicu u vozilu; vidjeti Dodatak 14. Međutim, uređaj za daljinsko ispitivanje šalje primljene podatke kontrolnoj kartici radi dešifriranja i potvrde autentičnosti. Što se tiče sigurnosti, uređaj za komunikaciju na daljinu i uređaj za daljinsko ispitivanje potpuno su transparentni.

— Kartica radionice pruža iste sigurnosne usluge za sučelje DSRC-a kao i kontrolna kartica. Time se radionici omogućuje potvrda ispravnog funkcioniranja sučelja jedinice u vozilu za komunikaciju na daljinu, uključujući sigurnost. Za više informacija vidjeti odjeljak 9.2.2.

8.2. **Kriptografski algoritmi**

8.2.1 *Simetrični algoritmi*

CSM_44 Jedinice u vozilu, tahografske kartice, senzori kretanja i vanjski uređaji GNSS-a podržavaju AES algoritam kako je definirano u [AES], s duljinama ključa od 128, 192 i 256 bitova.

8.2.2 *Asimetrični algoritmi i normirani parametri domene*

CSM_45 Jedinice u vozilu, tahografske kartice i vanjski uređaji GNSS-a podržavaju kriptografiju eliptičkih krivulja s veličinom ključa od 256, 384 i 512/521 bitova.

CSM_46 Jedinice u vozilu, tahografske kartice i vanjski uređaji GNSS-a podržavaju algoritam potpisa ECDSA kako je navedeno u [DSS].

CSM_47 Jedinice u vozilu, tahografske kartice i vanjski uređaji GNSS-a podržavaju algoritam dogovaranja ključa ECKA-EG kako je navedeno u [TR 03111].

CSM_48 Jedinice u vozilu, tahografske kartice i vanjski uređaji GNSS-a podržavaju sve normirane parametre domene iz tablice 1. u nastavku za kriptografiju eliptičkih krivulja:

Tablica 1.

Normirani parametri domene

Naziv	Veličina (bitova)	Upućivanje	Identifikator objekta
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`

Napomena: identifikatori objekta u zadnjem stupcu tablice 1. navedeni su u [RFC 5639] za krivulje Brainpool i u [RFC 5480] za krivulje NIST.

Primjer 1.: identifikator objekta krivulje BrainpoolP256r1 je

```
{iso(1)
        identified-organization(3) teletrust(36) algorithm(3)
  signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8)
                              ellipticCurve(1) versionOne(1) 7}.
```

Ili u *dot* zapisu (eng. *dot notation*): `1.3.36.3.3.2.8.1.1.7.`

Primjer 2.: identifikator objekta krivulje NIST P-384 je

```
{iso(1) identified-organization(3) certicom(132) curve(0) 34}.
```

Ili u *dot* zapisu: `1.3.132.0.34.`

8.2.3 *Algoritmi raspršivanja (hashing)*

CSM_49 Jedinice u vozilu i tahografske kartice podržavaju algoritme SHA-256, SHA-384 i SHA-512 navedene u [SHS].

8.2.4 *Sljedovi šifri (eng. Cipher Suites)*

CSM_50 U slučaju simetričnog algoritma, asimetrični algoritam i algoritam raspršivanja upotrebljavaju se zajedno kako bi oblikovali sigurnosni protokol; njihove su duljine ključeva i veličine raspršivanja (približno) jednake jakosti. U tablici 2. prikazani su dopušteni slijedovi šifri:

Tablica 2.

Dopušteni sljedovi šifri

ID slijeda šifri	Veličina ECC ključa (bitovi)	Duljina AES ključa (bitovi)	Algoritam kompresije	Duljina MAC (u bajtovima)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Napomena: veličine ECC ključeva od 512 bitova odnosno 521 bita smatraju se jednakima po jakosti za sve namjene obuhvaćene ovim Dodatkom.

9. KLJUČEVI I CERTIFIKATI

9.1. **Asimetrični parovi ključeva i certifikati javnih ključeva**

9.1.1 *Općenito*

Napomena: ključevi opisani u ovom odjeljku upotrebljavaju se za uzajamnu autentifikaciju i siguran prijenos poruka između jedinica u vozilu i tahografskih kartica te između jedinica u vozilu i vanjskih uređaja GNSS-a. Ti su postupci detaljno opisani u poglavljima 10. i 11. ovog Dodatka.

CSM_51 U okviru Europskog sustava pametnog tahografa, parovi ECC ključeva i odgovarajući certifikati generiraju se i njima se upravlja preko tri funkcionalne hijerarhijske razine:

— europska razina,

— razina države članice,

— razina opreme.

CSM_52 U okviru cijelog Europskog sustava pametnog tahografa, javni i privatni ključevi i certifikati generiraju se, njima se upravlja te komuniciraju s pomoću normiranih i sigurnih metoda.

9.1.2 *Europska razina*

CSM_53 Na europskoj se razini generira jedan jedinstveni par ECC ključeva označen kao EUR. Sastoji se od privatnog ključa (EUR.SK) i javnog ključa (EUR.PK). Taj par ključeva čini glavni (eng. *root*) par ključeva cijelog Europskog pametnog tahografa PKI. Taj zadatak obavlja europsko tijelo za izdavanje glavnog certifikata (eng. *European Root Certificate Authority*, ERCA), pod nadležnošću i odgovornošću Europske komisije.

CSM_54 ERCA upotrebljava europski privatni ključ za potpisivanje (samopotpisanog) glavnog certifikata europskog javnog ključa te taj europski glavni certifikat dostavlja svim državama članicama.

CSM_55 ERCA upotrebljava europski privatni ključ za potpisivanje certifikata javnog ključa država članica na zahtjev. ERCA vodi evidenciju svih potpisanih certifikata javnih ključeva država članica.

CSM_56 Kako je prikazano na slici 1. u odjeljku 9.1.7., ERCA generira novi europski glavni par ključeva svakih 17 godina. Kada generira novi europski glavni par ključeva, ERCA stvara i novi samopotpisani glavni certifikat za novi europski javni ključ. Rok valjanosti europskog glavnog certifikata je 34 godine uvećano za tri mjeseca.

Napomena: uvođenje novog glavnog para ključeva isto tako znači da će ERCA generirati novi glavni ključ senzora kretanja i novi glavni ključ DSRC-a, vidjeti odjeljke 9.2.1.2. i 9.2.2.2.

CSM_57 Prije generiranja novog europskog glavnog para ključeva, ERCA provodi analizu kriptografske jakosti koja je potrebna za novi par ključeva s obzirom na to da treba ostati zaštićen sljedeće 34 godine. Ako to smatra potrebnim, ERCA može prijeći na slijed šifri koji je jači od postojećeg, kako je navedeno u CSM_50.

CSM_58 Kada generira novi europski glavni par ključeva, ERCA stvara i certifikat o povezanosti za novi europski javni ključ i potpisuje ga s prethodnim europskim privatnim ključem. Rok valjanosti certifikata o povezanosti je 17 godina. To je prikazano i na slici 1. u odjeljku 9.1.7.

Napomena: Budući da certifikat o povezanosti sadržava javni ključ ERCA generacije *X* koji je potpisan privatnim ključem ERCA generacije *X-1*, certifikat o povezanosti opremi izdanoj na temelju generacije *X-1* pruža metodu za uspostavu povjerenja u opremu izdanu na temelju generacije *X*.

CSM_59 ERCA ne upotrebljava privatni ključ glavnog para ključeva ni u koju svrhu od trenutka u kojem novi glavni certifikat ključa postane valjan.

CSM_60 ERCA u svakom trenutku ima na raspolaganju sljedeće kriptografske ključeve i certifikate:

— trenutačni par EUR ključeva i odgovarajući certifikat,

— sve prethodne certifikate EUR koji se upotrebljavaju za provjeru certifikata MSCA koji su još uvijek valjani,

— certifikate o povezanosti za sve generacije certifikata EUR osim prve.

9.1.3 *Razina države članice*

CSM_61 Na razini države članice, sve države članice koje trebaju potpisivati certifikate tahografskih kartica generiraju jedan ili više jedinstvenih parova ECC ključeva označenih kao MSCA_Card. Sve države članice koje trebaju potpisivati certifikate za jedinice u vozilu ili vanjske GNSS uređaje dodatno generiraju jedan ili više jedinstvenih parova ECC ključeva označenih kao MSCA_VU-EGF.

CSM_62 Zadatak generiranja parova ključeva država članica obavlja certifikacijsko tijelo države članice (MSCA). Kada generira par ključeva države članice, MSCA šalje javni ključ ERCA-i kako bi dobila odgovarajući certifikat države članice koji je potpisala ERCA.

CSM_63 MSCA odabire jakost para ključeva države članice jednaku jakosti europskog glavnog para ključeva koji se upotrebljava za potpisivanje odgovarajućeg certifikata države članice.

CSM_64 Ako postoji, par ključeva MSCA_VU-EGF sastoji se od privatnog ključa MSCA_VU-EGF.SK i javnog ključa MSCA_VU-EGF.PK. MSCA upotrebljava privatni ključ MSCA_VU-EGF.SK isključivo za potpisivanje certifikata javnih ključeva jedinica u vozilu i vanjskih uređaja GNSS-a.

CSM_65 Par ključeva MSCA_Card sastoji se od privatnog ključa MSCA_Card.SK i javnog ključa MSCA_Card. PK. MSCA upotrebljava privatni ključ MSCA_Card.SK isključivo za potpisivanje certifikata javnih ključeva tahografskih kartica.

CSM_66 MSCA vodi evidenciju svih potpisanih certifikata jedinica u vozilu, certifikata vanjskih uređaja GNSS-a i certifikata kartica zajedno s identifikacijom opreme za koju je certifikat namijenjen.

CSM_67 Rok valjanosti certifikata MSCA_VU-EGF je 17 godina uvećano za tri mjeseca. Rok valjanosti certifikata MSCA_Card je sedam godina uvećano za jedan mjesec.

CSM_68 Kako je prikazano na slici 1. u odjeljku 9.1.7, razdoblje upotrebe privatnog ključa para ključeva MSCA_VU-EGF i privatnog ključa para ključeva MSCA_Card iznosi dvije godine.

CSM_69 MSCA ne upotrebljava privatni ključ para ključeva MSCA_VU-EGF ni u koju svrhu nakon što je isteklo njegovo razdoblje upotrebe. Nadalje, MSCA ne upotrebljava privatni ključ para ključeva MSCA_Card ni u koju svrhu nakon što je isteklo njegovo razdoblje upotrebe.

CSM_70 MSCA u svakom trenutku ima na raspolaganju sljedeće kriptografske ključeve i certifikate:

— trenutačni par ključeva MSCA_Card i odgovarajući certifikat,

— sve prethodne certifikate MSCA_Card koji se upotrebljavaju za provjeru certifikata tahografskih kartica koji su još uvijek valjani,

— trenutačni certifikat EUR potreban za provjeru trenutačnog certifikata MSCA,

— sve prethodne certifikate EUR potrebne za provjeru certifikata MSCA koji su još uvijek valjani.

CSM_71 Ako treba potpisivati certifikate za jedinice u vozilu ili vanjske uređaje GNSS-a, MSCA dodatno ima na raspolaganju sljedeće ključeve i certifikate:

— trenutačni par ključeva MSCA_VU-EGF i odgovarajući certifikat,

— sve prethodne javne ključeve MSCA_VU-EGF koji se upotrebljavaju za provjeru certifikata jedinica u vozilu ili vanjskih uređaja GNSS-a koji su još uvijek valjani.

9.1.4 *Razina opreme: Jedinice u vozilu*

CSM_72 Za svaku se jedinicu u vozilu generiraju dva jedinstvena para ECC ključeva označena kao VU_MA i VU_Sign. Taj zadatak obavljaju proizvođači jedinica u vozilu. Kada generira par ključeva za jedinicu u vozilu, strana koja generira ključ šalje javni ključ MSCA-u države u kojoj ima prebivalište kako bi dobila odgovarajući certifikat jedinice u vozilu koji je potpisao MSCA. Privatni ključ upotrebljava isključivo jedinica u vozilu (VU).

CSM_73 Certifikati VU_MA i VU_Sign određene jedinice u vozilu imaju isti datum početka valjanosti certifikata.

CSM_74 Proizvođač jedinica u vozilu odabire jakost para ključeva jedinice u vozilu jednaku jakosti para MSCA ključeva koji se upotrebljava za potpisivanje odgovarajućeg certifikata jedinice u vozilu.

CSM_75 Jedinica u vozilu upotrebljava svoj par VU_MA ključeva, koji se sastoji od privatnog ključa VU_MA. SK i javnog ključa VU_MA.PK, isključivo kako bi izvršila autentifikaciju jedinice u vozilu s obzirom na tahografske kartice i vanjske uređaje GNSS-a, kako je navedeno u odjeljcima 10.3. i 11.4. ovog Dodatka.

CSM_76 Jedinica u vozilu može generirati kratkotrajne parove ECC ključeva, pri čemu kratkotrajni par ključeva upotrebljava isključivo za dogovaranje ključa razmjene podataka s tahografskom karticom ili vanjskim uređajem GNSS-a, kako je navedeno u odjeljcima 10.4. i 11.4. ovog Dodatka.

CSM_77 Jedinica u vozilu upotrebljava privatni ključ VU_Sign.SK iz svojeg para VU_Sign ključeva isključivo za potpisivanje preuzetih podatkovnih datoteka, kako je navedeno u poglavlju 14. ovog Dodatka. Odgovarajući javni ključ VU_Sign.PK upotrebljava se isključivo za provjeru potpisa koje stvara jedinica u vozilu.

CSM_78 Kako je prikazano na slici 1. u odjeljku 9.1.7., rok valjanosti certifikata VU_MA je 15 godina i tri mjeseca. Rok valjanosti certifikata VU_Sign je 15 godina i tri mjeseca.

Napomene:

— produljenim se rokom valjanosti certifikata VU_Sign jedinici u vozilu omogućuje stvaranje valjanih potpisa za preuzete podatke tijekom prva tri mjeseca nakon isteka valjanosti certifikata u skladu s Uredbom (EU) br. 581/2010.

— Produljeni je rok valjanosti certifikata VU_MA potreban kako bi se jedinici u vozilu omogućila autentifikacija kontrolne kartice ili kartice poduzeća tijekom prva tri mjeseca nakon isteka valjanosti certifikata tako da može izvršiti preuzimanje podataka.

CSM_79 Jedinica u vozilu ne upotrebljava privatni ključ para ključeva jedinice u vozilu ni u koju svrhu od trenutka isteka odgovarajućeg certifikata.

CSM_80 Parovi ključeva jedinice u vozilu (osim kratkotrajnih parova ključeva) i odgovarajući certifikati određene jedinice u vozilu ne smiju se zamjenjivati ili obnavljati na terenu nakon što je jedinica u vozilu stavljena u upotrebu.

Napomene:

— kratkotrajni parovi ključeva nisu obuhvaćeni ovim zahtjevom jer jedinica u vozilu generira kratkotrajni par ključeva svaki put kad se izvršava autentifikacija čipa ili dogovaranje ključa razmjene podataka,; vidjeti odjeljak 10.4. Potrebno je napomenuti da kratkotrajni parovi ključeva nemaju odgovarajuće certifikate.

— Ovim se zahtjevom ne zabranjuje mogućnost zamjene statičkih parova ključeva jedinice u vozilu tijekom obnove ili popravka u sigurnom okruženju koje kontrolira proizvođač jedinice u vozilu.

CSM_81 Kada su stavljene u upotrebu, jedinice u vozilu sadržavaju sljedeće kriptografske ključeve i certifikate:

— privatni ključ VU_MA i odgovarajući certifikat,

— privatni ključ VU_Sign i odgovarajući certifikat,

— certifikat MSCA_VU-EGF s javnim ključem MSCA_VU-EGF.PK koji se upotrebljava za provjeru VU_MA certifikata i VU_Sign certifikata,

— certifikat EUR s javnim ključem EUR.PK koji se upotrebljava za provjeru certifikata MSCA_VU-EGF,

— certifikat EUR čiji rok valjanosti izravno prethodi roku valjanosti certifikata EUR koji se upotrebljava za provjeru certifikata MSCA_VU-EGF, ako postoji,

— certifikat o povezanosti koji povezuje ta dva certifikata EUR, ako postoji.

CSM_82 Osim kriptografskih ključeva i certifikata navedenih u CSM_81, jedinice u vozilu isto tako sadržavaju ključeve i certifikate iz dijela A ovog Dodatka kojima se jedinici u vozilu omogućuje interakcija s tahografskim karticama prve generacije.

9.1.5 *Razina opreme: Tahografske kartice*

CSM_83 Za svaku tahografsku karticu generira se jedan jedinstveni par ECC ključeva označen kao Card_MA. Za svaku se karticu vozača i svaku karticu radionice dodatno generira drugi jedinstveni par ECC ključeva označen kao Card_Sign. Taj zadatak mogu obavljati proizvođači kartice ili izvođači personalizacije kartice. Kada generira par ključeva kartica, strana koja generira ključ šalje javni ključ MSCA-u države u kojoj ima prebivalište kako bi dobila odgovarajući certifikat kartice koji je potpisao MSCA. Privatni ključ upotrebljava isključivo tahografska kartica.

CSM_84 Certifikati Card_MA i Card_Sign određene kartice vozača ili kartice radionice imaju isti datum početka valjanosti certifikata.

CSM_85 Proizvođač kartice ili izvođač personalizacije kartice odabire jakost para ključeva kartice jednaku jakosti para MSCA ključeva koji se upotrebljava za potpisivanje odgovarajućeg certifikata kartice.

CSM_86 Tahografska kartica upotrebljava svoj par VU_Card ključeva, koji se sastoji od privatnog ključa Card_MA.SK i javnog ključa Card_MA.PK, isključivo kako bi izvršila uzajamnu autentifikaciju i dogovaranje ključa razmjene podataka s obzirom na jedinice u vozilu, kako je navedeno u odjeljcima 10.3. i 10.4. ovog Dodatka.

CSM_87 Kartica vozača ili kartica radionice upotrebljava privatni ključ Card_Sign.SK iz svojeg para Card_Sign ključeva isključivo za potpisivanje preuzetih podatkovnih datoteka, kako je navedeno u poglavlju 14. ovog Dodatka. Odgovarajući javni ključ Card_Sign.PK upotrebljava se isključivo za provjeru potpisa koje stvara kartica.

CSM_88 Rok valjanosti certifikata Card_MA sljedeći je:

— za kartice vozača: pet godina,

— za kartice poduzeća: dvije godine,

— za kontrolne kartice: dvije godine,

— za kartice radionica: jedna godina.

CSM_89 Rok valjanosti certifikata Card_Sign sljedeći je:

— za kartice vozača: pet godina i jedan mjesec,

— za kartice radionica: jedna godina i jedan mjesec.

Napomena: produljenim se rokom valjanosti certifikata Card_Sign kartici vozača omogućuje stvaranje valjanih potpisa za preuzete podatke tijekom prvog mjeseca nakon isteka valjanosti certifikata. To je potrebno s obzirom na Uredbu (EU) br. 581/2010 kojom se zahtijeva da preuzimanje podataka s kartice vozača mora biti moguće do 28 dana nakon posljednjeg zapisa podataka.

CSM_90 Parovi ključeva i odgovarajući certifikati određene tahografske kartice ne smiju se zamjenjivati ili obnavljati nakon izdavanja kartice.

CSM_91 Kada su izdane, tahografske kartice sadržavaju sljedeće kriptografske ključeve i certifikate:

— privatni ključ Card_MA i odgovarajući certifikat,

— dodatno za kartice vozača i kartice radionica: privatni ključ Card_Sign i odgovarajući certifikat,

— certifikat MSCA_Card s javnim ključem MSCA_Card.PK koji se upotrebljava za provjeru certifikata Card_MA i certifikata Card_Sign,

— certifikat EUR s javnim ključem EUR.PK koji se upotrebljava za provjeru certifikata MSCA_Card,

— certifikat EUR čiji rok valjanosti izravno prethodi roku valjanosti certifikata EUR koji se upotrebljava za provjeru certifikata MSCA_Card, ako postoji,

— certifikat o povezanosti koji povezuje ta dva certifikata EUR, ako postoji.

CSM_92 Osim kriptografskih ključeva i certifikata navedenih u CSM_91, tahografske kartice sadržavaju i ključeve i certifikate navedene u dijelu A ovog Dodatka koji tim karticama omogućuju interakciju s jedinicama u vozilu prve generacije.

9.1.6 *Razina opreme: Vanjski uređaji GNSS-a*

CSM_93 Za svaki vanjski uređaj GNSS-a generira se jedan jedinstveni par ECC ključeva označen kao EGF_MA. Taj zadatak obavljaju proizvođači vanjskih uređaja GNSS-a. Kada generira par EGF_MA ključeva, strana koja generira ključ šalje javni ključ MSCA-u države u kojoj ima prebivalište kako bi dobila odgovarajući certifikat EGF_MA koji je potpisao MSCA. Privatni ključ upotrebljava isključivo vanjski uređaj GNSS-a.

CSM_94 Proizvođač vanjskog uređaja GNSS-a (EGF) odabire jakost para EGF_MA ključeva jednaku jakosti para MSCA ključeva koji se upotrebljava za potpisivanje odgovarajućeg certifikata EGF_MA.

CSM_95 Vanjski uređaj GNSS-a upotrebljava svoj par EGF_MA ključeva, koji se sastoji od privatnog ključa EGF_MA.SK i javnog ključa EGF_MA.PK, isključivo kako bi izvršio uzajamnu autentifikaciju i dogovaranje ključa razmjene podataka s obzirom na jedinice u vozilu, kako je navedeno u odjeljku 11.4. ovog Dodatka.

CSM_96 Rok valjanosti certifikata EGF_MA je 15 godina.

CSM_97 Vanjski uređaj GNSS-a ne upotrebljava privatni ključ iz svojeg para EGF-MA ključeva za povezivanje s jedinicom u vozilu nakon isteka odgovarajućeg certifikata.

Napomena: kako je objašnjeno u odjeljku 11.3.3., EGF potencijalno može upotrijebiti svoj privatni ključ za uzajamnu autentifikaciju s obzirom na jedinicu u vozilu s kojom je već povezan čak i nakon isteka odgovarajućeg certifikata.

CSM_98 Par EGF_MA ključeva i odgovarajući certifikat određenog vanjskog uređaja GNSS-a ne smiju se zamjenjivati ili obnavljati na terenu nakon što je EGF stavljen u upotrebu.

Napomena: ovim se zahtjevom ne zabranjuje mogućnost zamjene parova EGF ključeva tijekom obnove ili popravka u sigurnom okruženju koje kontrolira proizvođač EGF-a.

CSM_99 Kada je stavljen u upotrebu, vanjski uređaj GNSS-a sadržava sljedeće kriptografske ključeve i certifikate:

— privatni ključ EGF_MA i odgovarajući certifikat,

— certifikat MSCA_VU-EGF s javnim ključem MSCA_VU-EGF.PK koji se upotrebljava za provjeru certifikata EGF_MA,

— certifikat EUR s javnim ključem EUR.PK koji se upotrebljava za provjeru certifikata MSCA_VU-EGF,

— certifikat EUR čiji rok valjanosti izravno prethodi roku valjanosti certifikata EUR koji se upotrebljava za provjeru certifikata MSCA_VU-EGF, ako postoji,

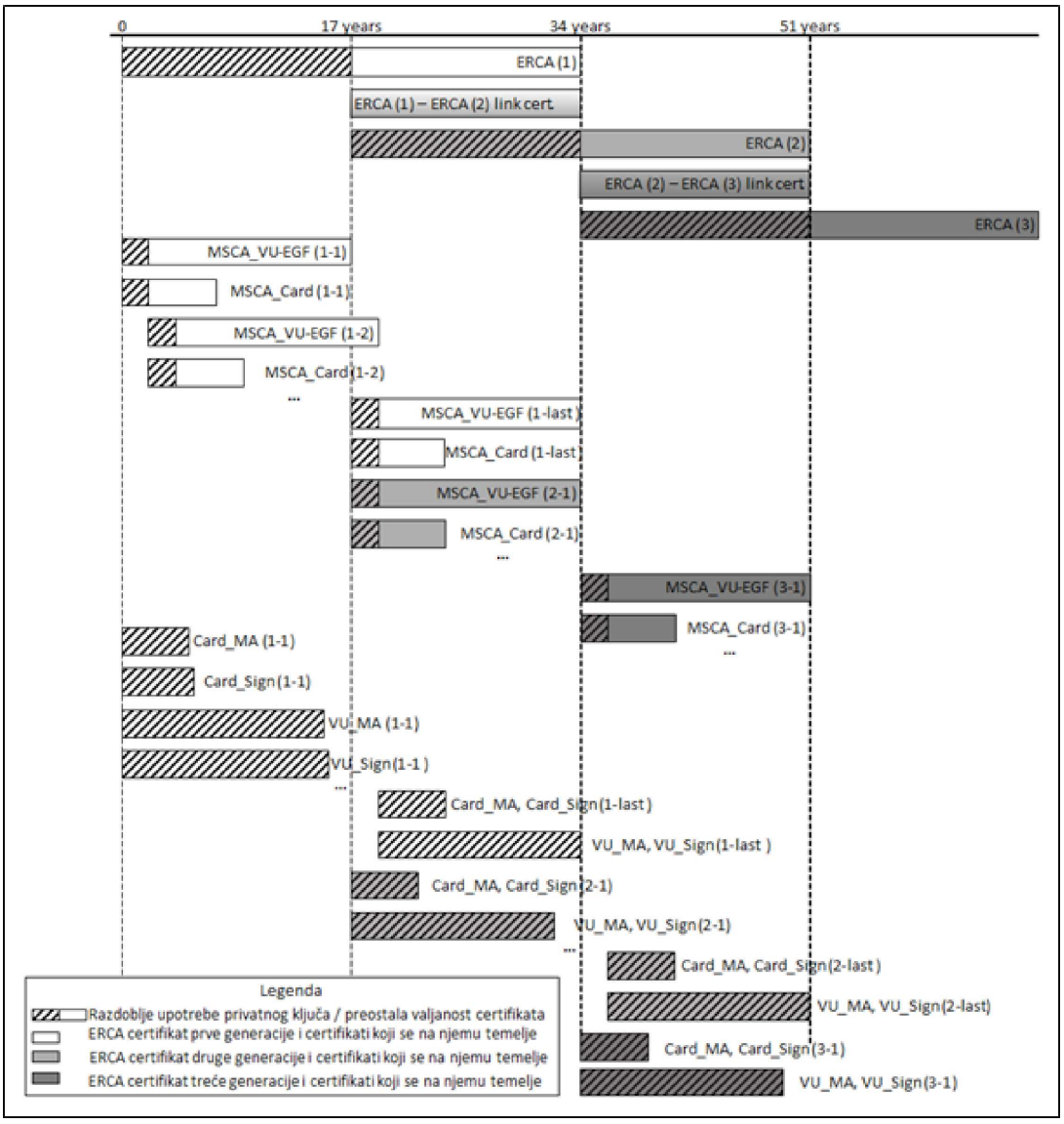
— certifikat o povezanosti koji povezuje ta dva certifikata EUR, ako postoji.

9.1.7 *Pregled: Zamjena certifikata*

Na slici 1. u nastavku prikazan je način izdavanja i upotrebe različitih generacija glavnih certifikata ERCA, certifikata o povezanosti ERCA, certifikata MSCA i certifikata opreme (jedinica u vozilu i kartica) tijekom vremena:

Slika 1.

Izdavanje i upotreba različitih generacija glavnih certifikata ERCA, certifikata o povezanosti ERCA, certifikata MSCA i certifikata opreme



Napomene za sliku 1.:

1. različite generacije glavnog certifikata označene su brojem u zagradi. Npr. ERCA (1) znači prva generacija glavnog certifikata ERCA; ERCA (2) znači druga generacija itd.

2. Ostali su certifikati označeni s dva broja u zagradi, pri čemu prvi označuje generaciju glavnog certifikata na temelju kojeg su izdani, a drugi generaciju samog certifikata. Npr. MSCA_Card (1-1) znači prvi certifikat MSCA_Card izdan na temelju ERCA (1); MSCA_Card (2-1) znači prvi certifikat MSCA_Card izdan na temelju ERCA (2); MSCA_Card (2-zadnji) znači zadnji certifikat MSCA_Card izdan na temelju ERCA (2); Card_MA(2-1) znači prvi certifikat kartice za uzajamnu autentifikaciju koji je izdan na temelju ERCA (2) itd.

3. Certifikati MSCA_Card (2-1) i MSCA_Card (1-zadnji) izdaju se na gotovo (ali ne potpuno) isti datum. Certifikat MSCA_Card (2-1) je prvi certifikat MSCA_Card izdan na temelju ERCA (2) i izdat će se malo kasnije od certifikata MSCA_Card (1-zadnji), zadnjeg certifikata MSCA_Card na temelju ERCA (1).

4. Kako je prikazano na slici, prvi certifikati jedinice u vozilu i kartica izdani na temelju ERCA (2) pojavit će se gotovo dvije godine prije pojave zadnjih certifikata jedinice u vozilu i kartica izdanih na temelju ERCA (1). To je zbog činjenice da se certifikati jedinice u vozilu i kartica izdaju na temelju certifikata MSCA, a ne izravno na temelju certifikata ERCA. Certifikat MSCA (2-1) izdaje se neposredno nakon što ERCA (2) postane valjan, ali certifikat MSCA (1-zadnji) izdaje se samo malo prije tog vremena, u posljednjem trenutku u kojem je certifikat ERCA (1) još uvijek valjan. Stoga će ta dva certifikata MSCA imati gotovo jednak rok valjanosti unatoč činjenici da pripadaju različitim generacijama.

5. Rok valjanosti prikazan za kartice odnosi se na kartice vozača (pet godina).

6. Zbog uštede prostora razlika u roku valjanosti između certifikata Card_MA i Card_Sign te između certifikata VU_MA i VU_Sign prikazana je samo za prvu generaciju.

9.2. **Simetrični ključevi**

9.2.1 *Ključevi za sigurnu komunikaciju između jedinice u vozilu i senzora kretanja*

9.2.1.1 *Općenito*

Napomena: čitatelji ovog odjeljka trebaju biti upoznati sa sadržajem norme [ISO 16844-3] u kojoj se opisuje sučelje između jedinice u vozilu i senzora kretanja. Postupak uparivanja između jedinice u vozilu i senzora kretanja detaljno je opisan u poglavlju 12. ovog Dodatka.

CSM_100 Za uparivanje jedinica u vozilu i senzora kretanja, uzajamnu autentifikaciju između jedinica u vozilu i senzora kretanja te šifriranje komunikacije između jedinica u vozilu i senzora kretanja potreban je niz simetričnih ključeva, kako je prikazano u tablici 3. Svi su ti ključevi AES ključevi, pri čemu je duljina ključa jednaka duljini glavnog ključa senzora kretanja, koji su povezani s duljinom (predviđenog) europskog glavnog para ključeva kako je opisano u CSM_50.

Tablica 3.

Ključevi za sigurnu komunikaciju između jedinice u vozilu (VU) i senzora kretanja

Ključ	Simbol	Generira	Metoda generiranja	Pohranjuje
Glavni ključ senzora kretanja – dio VU-a	$K_{M\text{-}VU}$	ERCA	Nasumično	ERCA, MSCA uključeni u izdavanje certifikata VU-ova, proizvođači VU-ova, jedinice u vozilu

Ključ	Simbol	Generira	Metoda generiranja	Pohranjuje
Glavni ključ senzora kretanja – dio radionice	K_{M-WC}	ERCA	Nasumično	ERCA, MSCA, proizvođači kartica, kartice radionica
Glavni ključ senzora kretanja	K_M	Ne generira se neovisno	Izračunava se kao $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, MSCA uključeni u izdavanje ključeva senzora kretanja (neobavezno) (*)
Identifikacijski ključ	K_{ID}	Ne generira se neovisno	Izračunava se kao $K_{ID} = K_M$ XOR CV, pri čemu je CV navedeno u CSM_106	ERCA, MSCA uključeni u izdavanje ključeva senzora kretanja (neobavezno) (*)
Ključ uparivanja	K_P	Proizvođač senzora kretanja	Nasumično	Jedan senzor kretanja
Ključ razmjene podataka	K_S	VU (tijekom uparivanja VU-a i senzora kretanja)	Nasumično	Jedan VU i jedan senzor kretanja

(*) Pohranjivanje K_M i K_{ID} nije obvezno jer se te ključeve može izvesti iz K_{M-VU}, K_{M-WC} i CV.

CSM_101 Europsko tijelo za izdavanje glavnog certifikata (ERCA) generira K_{M-VU} i K_{M-WC}, dva nasumična i jedinstvena AES ključa, iz kojih se glavni ključ senzora kretanja K_M može izračunati kao K_{M-VU} XOR K_{M-WC}. ERCA dostavlja K_M, K_{M-VU} i K_{M-WC} certifikacijskim tijelima država članica na njihov zahtjev.

CSM_102 ERCA svakom glavnom ključu senzora kretanja K_M dodjeljuje jedinstveni broj verzije koji isto tako vrijedi za stvaranje ključeva K_{M-VU} i K_{M-WC} i povezanog identifikacijskog ključa K_{ID}. ERCA obavješćuje MSCA-ove o broju verzije kada im šalje K_{M-VU} i K_{M-WC}.

Napomena: Broj verzije upotrebljava se za razlikovanje različitih generacija tih ključeva, kako je detaljno objašnjeno u odjeljku 9.2.1.2.

CSM_103 Certifikacijsko tijelo države članice dostavlja K_{M-VU}, zajedno s brojem verzije proizvođačima jedinica u vozilu na njihov zahtjev. Proizvođači jedinica u vozilu unose K_{M-VU} i njegov broj verzije u sve proizvedene jedinice u vozilu.

CSM_104 Certifikacijsko tijelo države članice (MSCA) osigurava da je K_{M-WC}, zajedno s njegovim brojem verzije, unesen na svaku karticu radionice pod njegovom odgovornošću.

Napomene:

— vidjeti opis vrste podataka `SensorInstallationSecData` u Dodatku 2.

— Kako je objašnjeno u odjeljku 9.2.1.2., zapravo može biti potrebno unijeti više generacija K_{M-WC} na jednu karticu radionice.

CSM_105 Osim AES ključa navedenog u CSM_104, MSCA osigurava da je TDES ključ Km_{WC}, naveden u zahtjevu CSM_037 u dijelu A ovog Dodatka, unesen na svaku karticu radionice pod njezinom odgovornošću.

Napomene:

— Time se omogućuje upotreba kartice radionice druge generacije za povezivanje s jedinicom u vozilu prve generacije.

— Kartica radionice druge generacije imat će dvije različite primjene, jednu koja je sukladna dijelu B ovog Dodatka i jednu koja je sukladna dijelu A. Potonja će sadržavati TDES ključ Km_{WC}.

CSM_106 MSCA uključena u izdavanje ključeva senzora kretanja izvodi identifikacijski ključ iz glavnog ključa senzora kretanja primjenom funkcije XOR na konstantni vektor CV. Vrijednost CV-a je sljedeća:

— za glavne ključeve senzora kretanja od 128 bitova: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83',

— za glavne ključeve senzora kretanja od 192 bita: 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',

— za glavne ključeve senzora kretanja od 256 bitova: 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'.

Napomena: konstantni vektori generiraju se kako slijedi:

Pi_10 = prvih 10 bajtova decimalnog dijela matematičke konstante π = '24 3F 6A 88 85 A3 08 D3 13 19'

CV_128-bits = prvih 16 bajtova SHA-256(Pi_10)

CV_192-bits = prva 24 bajta SHA-384(Pi_10)

CV_256-bits = prva 32 bajta SHA-512(Pi_10)

CSM_107 Proizvođači senzora kretanja generiraju nasumični i jedinstveni ključ uparivanja K_P za svaki senzor kretanja te svaki ključ uparivanja šalju certifikacijskom tijelu države članice. MSCA šifrira svaki ključ uparivanja s glavnim ključem senzora kretanja K_M te šifrirani ključ vraća proizvođaču senzora kretanja. Za svaki šifrirani ključ MSCA obavješćuje proizvođača senzora kretanja o broju verzije povezanog K_M.

Napomena: kako je objašnjeno u odjeljku 9.2.1.2., proizvođač senzora kretanja zapravo može trebati generirati više jedinstvenih ključeva uparivanja za jedan senzor kretanja.

CSM_108 Proizvođači senzora kretanja generiraju jedinstveni serijski broj za svaki senzor kretanja te sve serijske brojeve šalju certifikacijskom tijelu države članice. MSCA šifrira svaki serijski broj s identifikacijskim ključem K_{ID} te šifrirani serijski broj vraća proizvođaču senzora kretanja. Za svaki šifrirani serijski broj MSCA obavješćuje proizvođača senzora kretanja o broju verzije povezanog K_{ID}.

CSM_109 Za zahtjeve CSM_107 i CSM_108, MSCA upotrebljava AES algoritam u načinu rada „ulančavanje šifriranih blokova", kako je utvrđeno u normi [ISO 10116], s parametrom preraspodjele (eng. *interleave parameter*) *m* = 1 i inicijalizacijskim vektorom (eng. *initialization vector*) SV = '00' {16}, tj. 16 bajtova s binarnom vrijednošću 0. Prema potrebi, MSCA upotrebljava metodu popunjenja br. 2 iz norme [ISO 9797-1].

CSM_110 Proizvođač senzora kretanja pohranjuje šifrirani ključ uparivanja i šifrirani serijski broj u predviđeni senzor kretanja zajedno s odgovarajućim vrijednostima nešifriranog teksta i brojem verzije K_M i K_{ID} koji je upotrijebljen za šifriranje.

Napomena: kako je objašnjeno u odjeljku 9.2.1.2., proizvođač senzora kretanja zapravo može trebati unijeti više šifriranih ključeva uparivanja i šifriranih serijskih brojeva u jedan senzor kretanja.

CSM_111 Osim kriptografskog sadržaja na temelju AES-a utvrđenog u CSM_110, proizvođač senzora kretanja isto tako može u svaki senzor kretanja pohraniti kriptografski sadržaj na temelju TDES-a naveden u zahtjevu CSM_037 u dijelu A ovog Dodatka.

Napomena: time se omogućuje povezivanje senzora kretanja druge generacije s jedinicom u vozilu prve generacije.

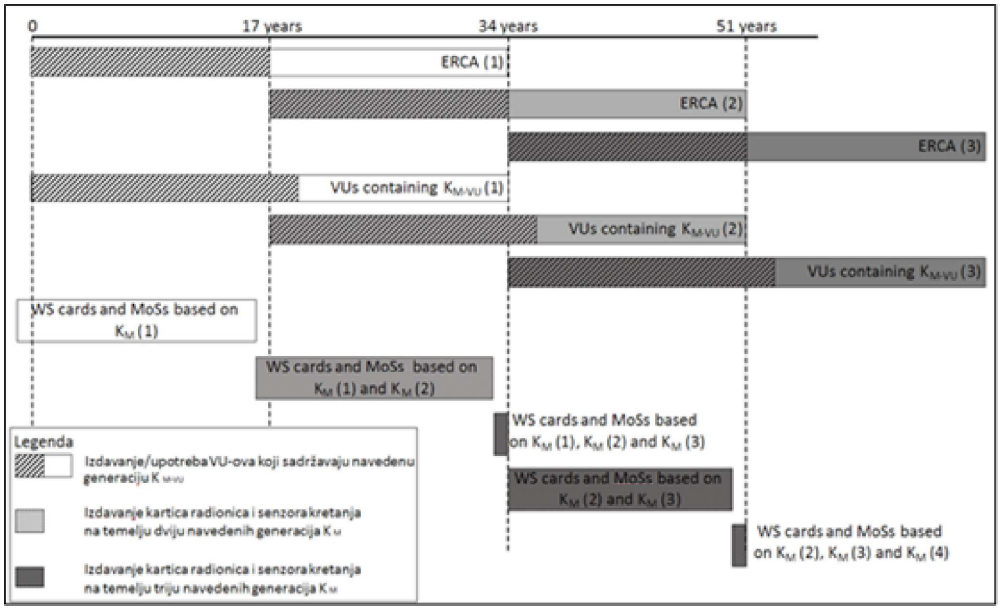
CSM_112 Duljina ključa razmjene podataka K_S koji generira jedinica u vozilu (VU) tijekom uparivanja sa senzorom kretanja povezana je s duljinom njezinog $K_{M\text{-}VU,}$ kako je opisano u CSM_50.

9.2.1.2 *Zamjena glavnog ključa senzora kretanja kod opreme druge generacije*

CSM_113 Svaki glavni ključ senzora kretanja i svi povezani ključevi (vidjeti tablicu 3.) povezani su s određenom generacijom glavnog para ključeva ERCA. Stoga se ti ključevi zamjenjuju svakih 17 godina. Rok valjanosti svake generacije glavnog ključa senzora kretanja počinje godinu dana prije nego što povezani glavni par ključeva ERCA postane važeći te završava kad istekne povezani glavni par ključeva ERCA. To je prikazano na slici 2.

Slika 2.

Izdavanje i upotreba različitih generacija glavnog ključa senzora kretanja u jedinicama u vozilu, senzorima kretanja i karticama radionica



CSM_114 Najmanje godinu dana prije generiranja novog europskog glavnog para ključeva, kako je opisano u CSM_56, ERCA generira novi glavni ključ senzora kretanja K_M generiranjem novih $K_{M\text{-}VU}$ i $K_{M\text{-}WC}$. Duljina glavnog ključa senzora kretanja povezana je s predviđenom jakošću novog europskog glavnog para ključeva u skladu s CSM_50. ERCA dostavlja nove K_M, $K_{M\text{-}VU}$ i $K_{M\text{-}WC}$ MSCA-ovima na njihov zahtjev, zajedno s njihovim brojem verzije.

CSM_115 MSCA osigurava da su sve važeće generacije $K_{M\text{-}WC}$ pohranjene u svakoj kartici radionice izdanoj pod njezinom nadležnošću zajedno s njihovim brojevima verzije, kako je prikazano na slici 2.

Napomena: to znači da će u posljednjoj godini roka valjanosti certifikata ERCA kartice radionica biti izdane s tri različite generacije K_{M-WC}, kako je prikazano na slici 2.

CSM_116 U odnosu na postupak opisan u prethodnim CSM_107 i CSM_108: MSCA šifrira svaki ključ uparivanja K_P koji primi od proizvođača senzora kretanja posebno za svaku važeću generaciju glavnog ključa senzora kretanja K_M. Osim toga, MSCA šifrira svaki serijski broj koji primi od proizvođača senzora kretanja posebno za svaku važeću generaciju identifikacijskog ključa K_{ID}. Proizvođač senzora kretanja pohranjuje sva šifriranja ključa uparivanja i sva šifriranja serijskog broja u predviđeni senzor kretanja zajedno s odgovarajućim vrijednostima nešifriranog teksta i brojem (brojevima) verzije K_M i K_{ID} koji je upotrijebljen za šifriranje.

Napomena: to znači da će u posljednjoj godini roka valjanosti certifikata ERCA senzori kretanja biti izdani sa šifriranim podatcima na temelju tri različite generacije K_M, kako je prikazano na slici 2.

CSM_117 U odnosu na postupak opisan u prethodnom CSM_107: budući da je duljina ključa uparivanja K_P povezana s duljinom K_M (vidjeti CSM_100), proizvođač senzora kretanja može trebati generirati do tri različita ključa uparivanja (različitih duljina) za jedan senzor kretanja u slučaju da naredne generacije K_M imaju različite duljine. U takvom slučaju proizvođač svaki ključ uparivanja šalje MSCA-u. MSCA osigurava da je svaki ključ uparivanja šifriran s ispravnom generacijom glavnog ključa senzora kretanja tj. onom jednake duljine.

Napomena: ako proizvođač senzora kretanja izabere generiranje ključa uparivanja na temelju TDES-a za senzor kretanja druge generacije (vidjeti CSM_111), proizvođač MSCA-u navodi da se za šifriranje tog ključa uparivanja mora upotrijebiti glavni ključ senzora kretanja na temelju TDES-a. To je stoga što duljina TDES ključa može biti jednaka duljini AES ključa, a MSCA ne može zaključiti o kojem se ključu radi samo na osnovi duljine ključa.

CSM_118 Proizvođači jedinica u vozilu unose samo jednu generaciju K_{M-VU} u svaku jedinicu u vozilu zajedno s njegovim brojem verzije. Generacija K_{M-VU} povezana je s certifikatom ERCA na kojem se temelje certifikati jedinice u vozilu.

Napomene:

— Jedinica u vozilu na temelju generacije *X* certifikata ERCA sadržava samo generaciju *X* $K_{M-VU,}$ čak i ako je izdana nakon početka roka valjanosti generacije *X+1* certifikata ERCA. To je prikazano na slici 2.

— Jedinica u vozilu generacije *X* ne može se upariti sa senzorom kretanja generacije *X-1*.

— Budući da kartice radionica imaju rok valjanosti od jedne godine, rezultat CSM_113 – CSM_118 je taj da će sve kartice radionica sadržavati novi K_{M-WC} u trenutku izdavanja prve jedinice u vozilu s novim K_{M-VU}. Stoga će takva jedinica u vozilu uvijek moći izračunati novi K_M. Nadalje, do tog će trenutka većina novih senzora kretanja isto tako sadržavati šifrirane podatke na temelju $K_{M.}$

9.2.2 *Ključevi za sigurnu komunikaciju preko DSRC-a*

9.2.2.1 *Općenito*

CSM_119 Autentičnost i povjerljivost podataka poslanih s jedinice u vozilu nadzornom tijelu putem kanala za komunikaciju na daljinu DSRC-a osigurava se skupom AES ključeva specifičnih za jedinicu u vozilu (VU), koji se izvode iz jedinstvenog DSRC glavnog ključa, KM_{DSRC}.

CSM_120 Glavni ključ DSRC-a KM_{DSRC} je AES ključ koji ERCA generira, pohranjuje i distribuira na siguran način. Duljina ključa može biti 128, 192 ili 256 bitova i povezana je s duljinom europskog glavnog para ključeva, kako je opisano u CSM_50.

CSM_121 ERCA na siguran način dostavlja glavni ključ DSRC-a certifikacijskim tijelima država članica na njihov zahtjev, kako bi im omogućila izvođenje ključeva DSRC-a specifičnih za jedinicu u vozilu i kako bi osigurala da je glavni ključ DSRC-a unesen u sve kontrolne kartice i kartice radionica izdane pod njihovom odgovornošću.

CSM_122 ERCA svakom glavnom ključu DSRC-a dodjeljuje jedinstveni broj verzije. ERCA obavješćuje MSCA-ove o broju verzije kada im šalje glavni ključ DSRC-a.

Napomena: broj verzije upotrebljava se za razlikovanje različitih generacija glavnog ključa DSRC-a, kako je detaljno objašnjeno u odjeljku 9.2.2.2.

CSM_123 Proizvođač jedinica u vozilu za svaku jedinicu u vozilu stvara jedinstveni serijski broj jedinice u vozilu te taj broj šalje svojem certifikacijskom tijelu države članice u zahtjevu za dobivanje skupa od dvaju ključeva DSRC-a specifičnih za jedinicu u vozilu. Serijski broj jedinice u vozilu sadržava vrstu podataka `VuSerialNumber`, a za kodiranje se upotrebljavaju posebna pravila kodiranja (DER) u skladu s normom [ISO 8825-1].

CSM_124 Po primitku zahtjeva za ključeve DSRC-a specifične za VU, MSCA izvodi dva AES ključa za jedinicu u vozilu, koji se nazivaju K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC. Ti ključevi specifični za jedinicu u vozilu imaju jednaku duljinu kao glavni ključ DSRC-a. MSCA upotrebljava funkciju izvođenja ključeva utvrđenu u [RFC 5869]. Funkcija raspršivanja (eng. *hash*) koja je potrebna za funkciju HMAC-Hash povezana je s duljinom glavnog ključa DSRC-a, kako je opisano u CSM_50. Funkcija izvođenja ključeva [RFC 5869] upotrebljava se kako slijedi:

Korak 1. (Extract):

— *PRK* = HMAC-Hash (*salt, IKM*), pri čemu je *salt* prazni niz (eng. *empty string*), a *IKM* je KM_{DSRC}.

Korak 2. (Expand):

— *OKM* = *T(1)*, pri čemu je

T(1) = HMAC-Hash (*PRK, T(0)* || *info* || '01'), gdje je

— *T(0)* = prazni niz (' '),

— *info* = serijski broj VU kako je navedeno u CSM_123,

— K_VU_{DSRC}_ENC = prvi *L* okteti *OKM*-a i

K_VU_{DSRC}_MAC = posljednji *L* okteti *OKM*-a

gdje je *L* zahtijevana duljina K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC u oktetima.

CSM_125 MSCA dostavlja K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC proizvođaču jedinice u vozilu na siguran način za unos u predviđenu jedinicu u vozilu.

CSM_126 Kad je izdana, jedinica u vozilu u svojoj sigurnoj memoriji ima pohranjene K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC radi osiguravanja integriteta, autentičnosti i povjerljivosti podataka koji se šalju kanalom za komunikaciju na daljinu. Jedinica u vozilu isto tako pohranjuje broj verzije glavnog ključa DSRC-a koji je upotrijebljen za izvođenje tih ključeva specifičnih za jedinicu u vozilu.

CSM_127 Kad su izdane, kontrolne kartice i kartice radionica u svojoj sigurnoj memoriji imaju pohranjen KM_{DSRC} kako bi mogle provjeriti integritet i autentičnost podataka koje je jedinica u vozilu poslala kanalom za komunikaciju na daljinu te za dešifriranje tih podataka. Kontrolne kartice i kartice radionica pohranjuju i broj verzije glavnog ključa DSRC-a.

Napomena: kako je objašnjeno u odjeljku 9.2.2.2., zapravo može biti potrebno unijeti više generacija K_{DSRC} na jednu karticu radionice ili kontrolnu karticu.

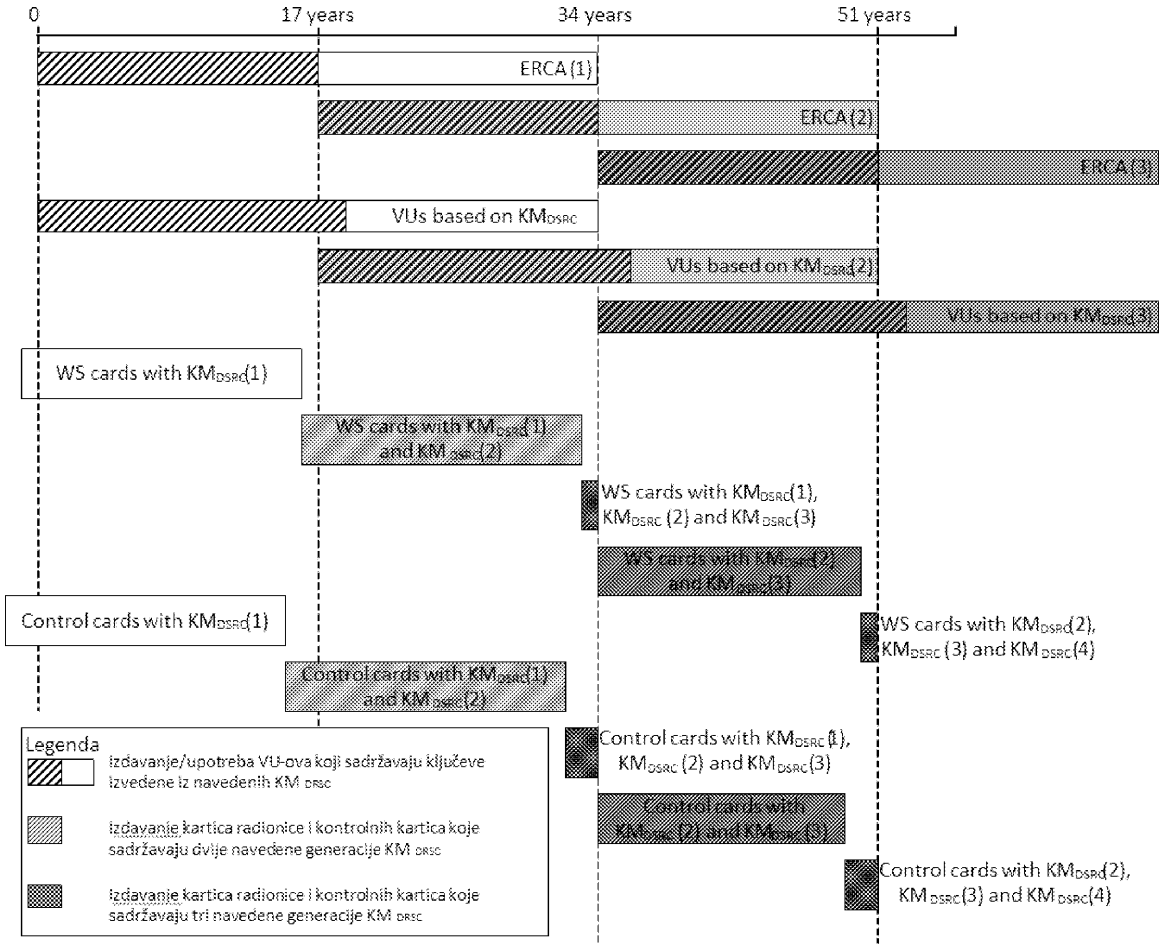
CSM_128 MSCA vodi evidenciju svih ključeva DSRC-a specifičnih za jedinicu u vozilu koje je generirala, njihova broja verzije te identifikacije jedinice u vozilu kojoj je svaki skup ključeva namijenjen.

9.2.2.2 *Zamjena glavnog ključa DSRC-a*

CSM_129 Svaki glavni ključ DSRC-a povezan je s određenom generacijom glavnog para ključeva ERCA. Stoga ERCA zamjenjuje glavni ključ DSRC-a svakih 17 godina. Rok valjanosti svake generacije glavnog ključa DSRC-a počinje dvije godine prije nego što povezani glavni par ključeva ERCA postane važeći te završava kada istekne povezani glavni par ključeva ERCA. To je prikazano na slici 3.

Slika 3.

Izdavanje i upotreba različitih generacija glavnog ključa DSRC-a u jedinicama u vozilu, karticama radionica i kontrolnim karticama



CSM_130 Najmanje dvije godine prije generiranja novog europskog glavnog para ključeva, kako je opisano u CSM_56, ERCA generira novi glavni ključ DSRC-a. Duljina glavnog ključa DSRC-a povezana je s predviđenom jakošću novog europskog glavnog para ključeva u skladu s CSM_50. ERCA dostavlja novi glavni ključ DSRC-a MSCA-ovima na njihov zahtjev, zajedno s njegovim brojem verzije.

CSM_131 MSCA osigurava da su sve važeće generacije K_{DSRC} pohranjene u svakoj kontrolnoj kartici izdanoj pod njezinom nadležnošću zajedno s njihovim brojevima verzije, kako je prikazano na slici 3.

Napomena: to znači da će u posljednje dvije godine roka valjanosti certifikata ERCA kontrolne kartice biti izdane s tri različite generacije K_{DSRC}, kako je prikazano na slici 3.

CSM_132 MSCA osigurava da su sve generacije K_{DSRC}, koje su bile važeće najmanje godinu dana i još su uvijek važeće, pohranjene u svakoj kartici radionice izdanoj pod njezinom nadležnošću zajedno s njihovim brojevima verzije, kako je prikazano na slici 3.

Napomena: to znači da će u posljednjoj godini roka valjanosti certifikata ERCA kartice radionica biti izdane s tri različite generacije K_{DSRC}, kako je prikazano na slici 3.

CSM_133 Proizvođači jedinica u vozilu unose samo jedan skup ključeva DSRC-a specifičnih za jedinicu u vozilu u svaku jedinicu u vozilu zajedno s njegovim brojem verzije. Taj se skup ključeva izvodi iz generacije KM_{DSRC} povezane s certifikatom ERCA na kojem se temelje certifikati jedinica u vozilu.

Napomene:

— To znači da jedinica u vozilu na temelju generacije *X* certifikata ERCA sadržava samo generaciju *X* K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC, čak i ako je VU izdan nakon početka roka valjanosti generacije *X+1* certifikata ERCA. To je prikazano na slici 3.

— Budući da kartice radionica imaju rok valjanosti od jedne godine, a kontrolne kartice od dvije godine, rezultat CSM_131 – CSM_133 je taj da će sve kartice radionica i kontrolne kartice sadržavati novi glavni ključ DSRC-a u trenutku izdavanja prve jedinice u vozilu s novim ključevima specifičnima za jedinicu u vozilu na temelju tog glavnog ključa.

9.3. **Certifikati**

9.3.1 *Općenito*

CSM_134 Svi su certifikati u Europskom sustavu pametnog tahografa samoopisni, karticom provjerljivi (eng. *card-verifiable*, CV) certifikati u skladu s normama [ISO 7816-4] i [ISO 7816-8].

CSM_135 Za kodiranje strukture podataka ASN.1 i podatkovnih objekata (za određenu primjenu) u certifikatima upotrebljavaju se posebna pravila kodiranja (DER) u skladu s normom [ISO 8825-1].

Napomena: takvo kodiranje daje sljedeću strukturu vrijednosti duljine oznake (eng. *Tag-Length-Value*, TLV):

oznaka: Oznaka je kodirana u jednom ili dva okteta i označuje sadržaj.

duljina: Duljina je kodirana kao nepotpisani cijeli broj u jednom, dva ili tri okteta, što dovodi do najveće duljine od 65 535 okteta. Upotrebljava se najmanji broj okteta.

vrijednost: Vrijednost je kodirana u nula ili više okteta.

9.3.2 *Sadržaj certifikata*

CSM_136 Svi certifikati imaju strukturu prikazanu u profilu certifikata u tablici 4.

Tablica 4.

Profil certifikata – verzija 1

Polje	ID polja	Oznaka	Duljina (bajtova)	Vrsta podataka ASN.1 (vidjeti Dodatak 1.)
ECC certifikat	C	'7F 21'	var	
Tijelo ECC certifikata	B	'7F 4E'	var	

Polje	ID polja	Oznaka	Duljina (bajtova)	Vrsta podataka ASN.1 (vidjeti Dodatak 1.)
Identifikator profila certifikata	CPI	‘5F 29’	‘01’	`INTEGER(0..255)`
Upućivanje na certifikacijsko tijelo	CAR	‘42’	‘08’	`KeyIdentifier`
Ovlaštenje nositelja certifikata	CHA	‘5F 4C’	‘07’	`CertificateHolder Authorisation`
Javni ključ	PK	‘7F 49’	var	
Parametri domene	DP	‘06’	var	`OBJECT IDENTIFIER`
Javna točka	PP	‘86’	var	`OCTET STRING`
Upućivanje na nositelja certifikata	CHR	‘5F 20’	‘08’	`KeyIdentifier`
Datum početka valjanosti certifikata	CEfD	‘5F 25’	‘04’	`TimeReal`
Datum isteka valjanosti certifikata	CExD	‘5F 24’	‘04’	`TimeReal`
Potpis ECC certifikata	S	‘5F 37’	var	`OCTET STRING`

Napomena: ID polja upotrebljavat će se u kasnijim odjeljcima ovog Dodatka za označivanje pojedinačnih polja certifikata, npr. X.CAR je upućivanje na certifikacijsko tijelo navedeno u certifikatu korisnika X.

9.3.2.1 Identifikator profila certifikata

CSM_137 Certifikati upotrebljavaju identifikator profila certifikata za označivanje upotrijebljenog profila certifikata. Verzija 1, kako je navedena u tablici 4., identificira se vrijednošću ‘00’.

9.3.2.2 Upućivanje na certifikacijsko tijelo

CSM_138 Upućivanje na certifikacijsko tijelo upotrebljava se za identifikaciju javnog ključa koji treba upotrijebiti za provjeru potpisa certifikata. Upućivanje na certifikacijsko tijelo stoga je jednako upućivanju na nositelja certifikata u certifikatu odgovarajućeg certifikacijskog tijela.

CSM_139 Glavni certifikat ERCA samopotpisan je, tj. upućivanje na certifikacijsko tijelo i upućivanje na nositelja certifikata u certifikatu jednaki su.

CSM_140 Za certifikat o povezanosti ERCA, upućivanje na nositelja certifikata jednako je CHR-u novog glavnog certifikata ERCA. Upućivanje na certifikacijsko tijelo za certifikat o povezanosti jednako je CHR-u prethodnog glavnog certifikata ERCA.

9.3.2.3 Ovlaštenje nositelja certifikata

CSM_141 Ovlaštenje nositelja certifikata upotrebljava se za identifikaciju vrste certifikata. Sastoji se od šest najznačajnijih bajtova identifikatora (ID) tahografske aplikacije ulančanih s vrstom opreme za koju je certifikat namijenjen.

9.3.2.4 Javni ključ

Javni ključ sadržava dva podatkovna elementa: normirane parametre domene koji se upotrebljavaju s javnim ključem u certifikatu i vrijednosti javne točke (eng. *public point*).

CSM_142 Podatkovni element parametara domene sadržava jedan od identifikatora objekta navedenih u tablici 1. za upućivanje na skup normiranih parametara domene.

CSM_143 Podatkovni element javne točke sadržava javnu točku. Javne točke eliptičke krivulje pretvaraju se u oktetne nizove kako je navedeno u [TR-03111]. Upotrebljava se nekomprimirani format kodiranja. Pri obnavljanju točke eliptičke krivulje iz njezina kodiranog formata uvijek se provode potvrde opisane u [TR-03111].

9.3.2.5 Upućivanje na nositelja certifikata

CSM_144 Upućivanje na nositelja certifikata je identifikator za javni ključ osiguran u certifikatu. Upotrebljava se za upućivanje na taj javni ključ u drugim certifikatima.

CSM_145 Za certifikate kartica i certifikate vanjskih uređaja GNSS-a, upućivanje na nositelja certifikata sadržava vrstu podataka `ExtendedSerialNumber` navedenu u Dodatku 1.

CSM_146 Za jedinice u vozilu proizvođač pri podnošenju zahtjeva za certifikat može, ali ne mora, znati serijski broj jedinice u vozilu, specifičan za proizvođača, za koju su taj certifikat i povezani privatni ključ namijenjeni. U prvom slučaju, upućivanje na nositelja certifikata sadržava vrstu podataka `ExtendedSerialNumber` navedenu u Dodatku 1. U drugom slučaju, upućivanje na nositelja certifikata sadržava vrstu podataka `CertificateRequestID` navedenu u Dodatku 1.

CSM_147 Za certifikate ERCA i MSCA, upućivanje na nositelja certifikata sadržava vrstu podataka `CertificationAuthorityKID` navedenu u Dodatku 1.

9.3.2.6 Datum početka valjanosti certifikata

CSM_148 Datum početka valjanosti certifikata označuje datum i vrijeme početka roka valjanosti certifikata. Datum početka valjanosti certifikata je datum generiranja certifikata.

9.3.2.7 Datum isteka valjanosti certifikata

CSM_149 Datum isteka valjanosti certifikata označuje datum i vrijeme isteka roka valjanosti certifikata.

9.3.2.8 Potpis certifikata

CSM_150 Potpis certifikata stvara se za kodirano tijelo certifikata, uključujući oznaku i duljinu tijela certifikata. Algoritam potpisa je ECDSA, kako je utvrđeno u [DSS], upotrebom algoritma raspršivanja (*hash*) povezanog s veličinom ključa nadležnog tijela potpisnika, kako je navedeno u CSM_50. Format potpisa je nešifriran, kako je navedeno u [TR-03111].

9.3.3 *Podnošenje zahtjeva za certifikate*

CSM_151 Prilikom podnošenja zahtjeva za certifikat, podnositelj zahtjeva svojem certifikacijskom tijelu šalje sljedeće podatke:

— identifikator profila certifikata zahtijevanog certifikata,

— upućivanje na certifikacijsko tijelo za koje se očekuje da će se upotrebljavati za potpisivanje certifikata,

— javni ključ koji treba potpisati.

CSM_152 Osim podataka iz CSM_151, MSCA šalje sljedeće podatke u zahtjevu za certifikat ERCA-i, čime ERCA-i omogućuje stvaranje upućivanja na nositelja certifikata novog certifikata MSCA:

— numerički kod države certifikacijskog tijela (vrsta podataka `NationNumeric` utvrđena u Dodatku 1.),

— alfanumerički kod države certifikacijskog tijela (vrsta podataka `NationAlpha` utvrđena u Dodatku 1.),

— Jednobajtni serijski broj za razlikovanje različitih ključeva certifikacijskog tijela u slučaju promjene ključeva,

— Dvobajtno polje koje sadržava posebne dodatne informacije o certifikacijskom tijelu.

CSM_153 Osim podataka iz CSM_151, proizvođač opreme šalje sljedeće podatke u zahtjevu za certifikat MSCA-i, čime MSCA-i omogućuje stvaranje upućivanja na nositelja certifikata novog certifikata opreme:

— identifikator vrste opreme specifičan za proizvođača,

— ako je poznat (vidjeti CSM_154), serijski broj opreme, jedinstven za proizvođača, vrstu opreme te mjesec proizvodnje. U protivnom, jedinstveni identifikator zahtjeva za certifikat,

— mjesec i godinu proizvodnje opreme ili zahtjeva za certifikat.

Proizvođač osigurava da su ti podatci točni i da je certifikat koji je MSCA vratio unesen u predviđenu opremu.

CSM_154 U slučaju jedinice u vozilu, proizvođač pri podnošenju zahtjeva za certifikat može, ali ne mora, znati serijski broj jedinice u vozilu, specifičan za proizvođača, za koju su taj certifikat i povezani privatni ključ namijenjeni. Ako je poznat, proizvođač jedinice u vozilu šalje serijski broj MSCA-i. Ako nije poznat, proizvođač na jedinstveni način identificira svaki zahtjev za certifikat te taj serijski broj zahtjeva za certifikat šalje MSCA-i. Dobiveni certifikat nakon toga sadržava serijski broj zahtjeva za certifikat. Nakon unošenja certifikata u specifičnu jedinicu u vozilu, proizvođač MSCA-i šalje vezu između serijskog broja zahtjeva za certifikat i identifikacije jedinice u vozilu.

10. UZAJAMNA AUTENTIFIKACIJA I SIGURAN PRIJENOS PORUKA IZMEĐU JEDINICA U VOZILU I KARTICA

10.1. **Općenito**

CSM_155 Na visokoj se razini sigurna komunikacija između jedinice u vozilu i tahografske kartice temelji na sljedećim koracima:

— Prvo, svaka strana drugoj strani dokazuje da je vlasnik valjanog certifikata javnog ključa koji je potpisalo certifikacijsko tijelo države članice. Zauzvrat, certifikat javnog ključa MSCA mora potpisati europsko tijelo za izdavanje glavnog certifikata. Taj se korak naziva provjera lanca certifikata te su njegove pojedinosti navedene u odjeljku 10.2.

— Drugo, jedinica u vozilu dokazuje kartici da posjeduje privatni ključ koji odgovara javnom ključu u predočenom certifikatu. To radi tako da potpiše slučajni broj koji je poslala kartica. Kartica provjerava potpis tog slučajnog broja. Ako je ta provjera uspješna, jedinica u vozilu je autentificirana. Taj se korak naziva autentifikacija jedinice u vozilu te su njegove pojedinosti navedene u odjeljku 10.3.

— Treće, obje strane samostalno izračunavaju dva AES ključa razmjene podataka s pomoću asimetričnog algoritma dogovaranja ključa. Upotrebom jednog od tih ključeva razmjene podataka, kartica stvara kod za autentifikaciju poruke (MAC) za određene podatke koje je poslala jedinica u vozilu. Jedinica u vozilu provjerava MAC. Ako je ta provjera uspješna, kartica je autentificirana. Taj se korak naziva autentifikacija kartice te su njegove pojedinosti navedene u odjeljku 10.4.

— Četvrto, jedinica u vozilu i kartica upotrebljavaju dogovorene ključeve razmjene podataka kako bi osigurale povjerljivost, integritet i autentičnost svih razmijenjenih poruka. Taj se korak naziva siguran prijenos poruka te su njegove pojedinosti navedene u odjeljku 10.5.

CSM_156 Mehanizam opisan u CSM_155 aktivira jedinica u vozilu svaki put kad je kartica umetnuta u jedan od njezinih utora za kartice.

10.2. **Uzajamna provjera lanca certifikata**

10.2.1 *Provjera lanca certifikata kartice koju provodi jedinica u vozilu*

CSM_157 Za provjeru lanca certifikata tahografske kartice, jedinice u vozilu upotrebljavaju protokol prikazan na slici 4.

Napomene za sliku 4.:

— Certifikati Card i javni ključevi prikazani na slici oni su za uzajamnu autentifikaciju. U odjeljku 9.1.5. označeni su kao Card_MA,

— Certifikati Card.CA i javni ključevi prikazani na slici oni su za potpisivanje certifikata kartica navedeni u CAR-u certifikata Card. U odjeljku 9.1.3. označeni su kao MSCA_Card,

— Certifikat Card.CA.EUR prikazan na slici je europski glavni certifikat koji je naveden u CAR certifikata Card.CA,

— Certifikat Card.Link prikazan na slici je certifikat o povezanosti kartice, ako postoji. Kako je navedeno u odjeljku 9.1.2., to je certifikat o povezanosti za novi europski glavni par ključeva koji je ERCA stvorila i potpisala prethodnim europskim privatnim ključem,

— Certifikat Card.Link.EUR je europski glavni certifikat koji je naveden u CAR certifikata Card. Link,

CSM_158 Kako je prikazano na slici 4., provjera lanca certifikata kartice počinje nakon umetanja kartice. Jedinica u vozilu čita upućivanje na nositelja kartice (`cardExtendedSerialNumber`) iz elementarne datoteke (EF) ICC. Jedinica u vozilu provjerava poznaje li karticu, tj. je li u prošlosti uspješno provjerila certifikat kartice i pohranila ga za buduću upotrebu. Ako poznaje karticu te je certifikat kartice još uvijek valjan, postupak se nastavlja provjerom lanca certifikata jedinice u vozilu. U protivnom, jedinica u vozilu uzastopno s kartice čita certifikat MSCA_Card koji se upotrebljava za provjeru certifikata kartice, certifikat Card.CA.EUR koji se upotrebljava za provjeru certifikata MSCA_Card te eventualno certifikat o povezanosti koji se upotrebljava za provjeru certifikata EUR dok ne nađe certifikat koji poznaje ili može provjeriti. Ako nađe takav certifikat, jedinica u vozilu upotrebljava taj certifikat za provjeru temeljnih certifikata kartice koje je pročitala s kartice. Ako je provjera uspješna, postupak se nastavlja provjerom lanca certifikata jedinice u vozilu. Ako provjera nije uspješna, jedinica u vozilu zanemaruje karticu.

Napomena: Postoje tri načina na koje jedinica u vozilu može prepoznati certifikat Card.CA.EUR:

— certifikat Card.CA.EUR isti je certifikat kao i vlastiti certifikat EUR jedinice u vozilu;

— certifikat Card.CA.EUR prethodi vlastitom certifikatu EUR jedinice u vozilu te je jedinica u vozilu već sadržavala taj certifikat pri izdavanju (vidjeti CSM_81);

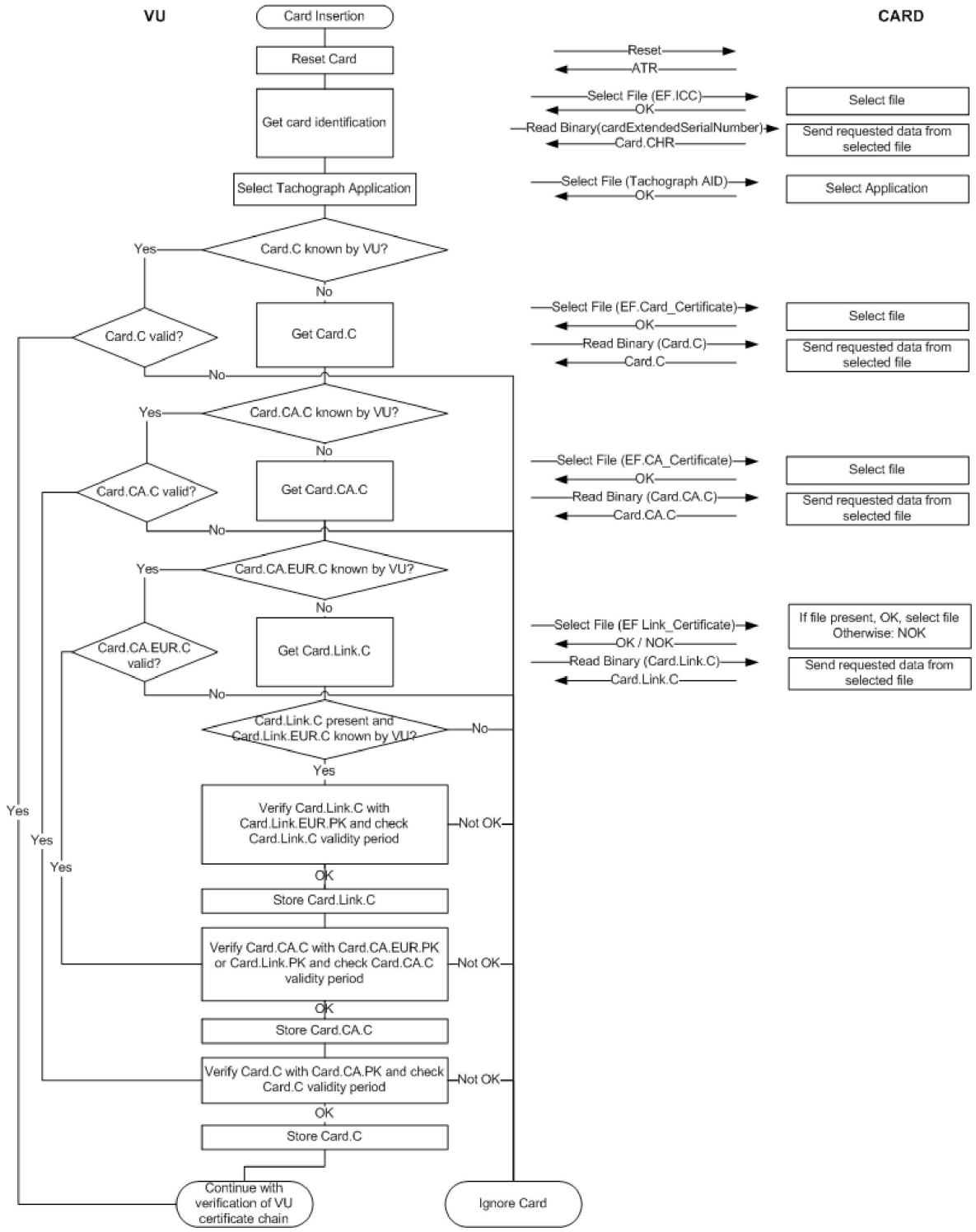
— certifikat Card.CA.EUR nasljeđuje vlastiti certifikat EUR jedinice u vozilu te je jedinica u vozilu u prošlosti primila certifikat o povezanosti od druge tahografske kartice, provjerila ga i pohranila za buduću upotrebu.

CSM_159 Kako je prikazano na slici 4., kad je jedinica u vozilu provjerila autentičnost i valjanost prethodno nepoznatog certifikata, taj certifikat može pohraniti za buduću upotrebu tako da ne mora ponovno provjeravati autentičnost tog certifikata ako je ponovno predočen jedinici u vozilu. Osim pohranjivanja cijelog certifikata, jedinica u vozilu može odabrati pohraniti samo sadržaj tijela certifikata, kako je navedeno u odjeljku 9.3.2.

CSM_160 Jedinica u vozilu provjerava vremensku valjanost svakog certifikata pročitanog s kartice ili pohranjenog u memoriji jedinice u vozilu te odbija certifikate koji su istekli. Jedinica u vozilu za provjeru vremenske valjanosti certifikata koji je predočila kartica upotrebljava svoj unutarnji sat.

Slika 4.

Protokol za provjeru lanca certifikata kartice koju provodi jedinica u vozilu (VU)

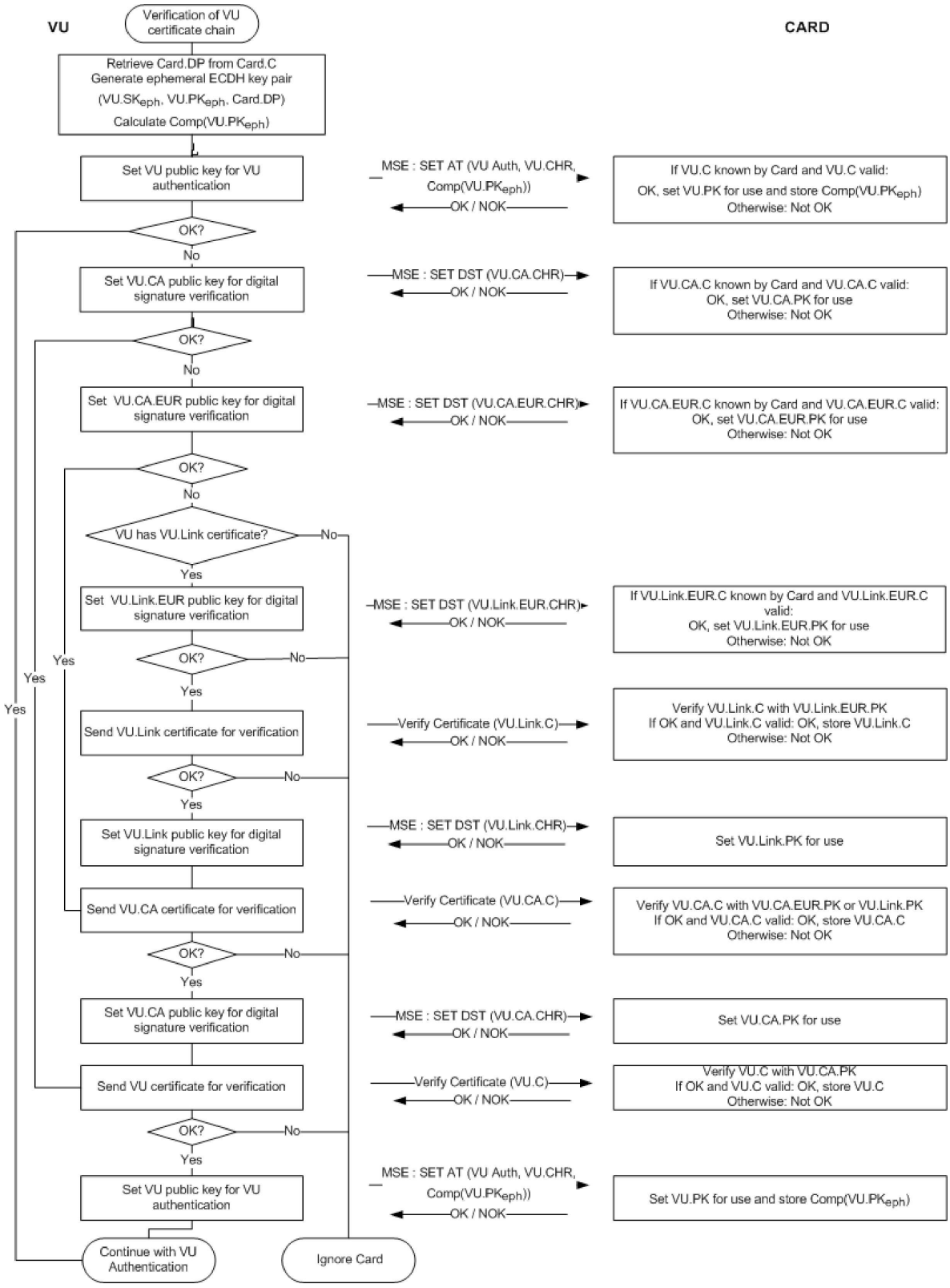


10.2.2 *Provjera lanca certifikata jedinice u vozilu koju provodi kartica*

CSM_161 Za provjeru lanca certifikata jedinice u vozilu tahografske kartice upotrebljavaju protokol prikazan na slici 5.

Slika 5.

Protokol za provjeru lanca certifikata jedinice u vozilu (VU) koju provodi kartica



Napomene za sliku 5.:

— Certifikati jedinice u vozilu i javni ključevi prikazani na slici oni su za uzajamnu autentifikaciju. U odjeljku 9.1.4. označeni su kao VU_MA,

— Certifikati VU.CA i javni ključevi prikazani na slici oni su za potpisivanje certifikata jedinica u vozilu i vanjskih uređaja GNSS-a. U odjeljku 9.1.3. označeni su kao MSCA_VU-EGF.

— Certifikat VU.CA.EUR prikazan na slici je europski glavni certifikat koji je naveden u CAR certifikata VU. CA,

— Certifikat VU.Link prikazan na slici je certifikat o povezanosti jedinice u vozilu, ako postoji. Kako je navedeno u odjeljku 9.1.2., to je certifikat o povezanosti za novi europski glavni par ključeva koji je ERCA stvorila i potpisala prethodnim europskim privatnim ključem.

— Certifikat VU.Link.EUR je europski glavni certifikat koji je naveden u CAR certifikata VU.Link.

CSM_162 Kako je prikazano na slici 5., provjera lanca certifikata jedinice u vozilu počinje tako da jedinica u vozilu pokuša postaviti svoj vlastiti javni ključ za upotrebu u tahografskoj kartici. Ako u tome uspije, znači da je kartica u prošlosti uspješno provjerila lanac certifikata jedinice u vozilu i pohranila certifikat jedinice u vozilu za buduću upotrebu. U tom se slučaju certifikat jedinice u vozilu postavlja za upotrebu i postupak se nastavlja autentifikacijom jedinice u vozilu. Ako kartica ne prepoznaje jedinicu u vozilu, jedinica u vozilu uzastopno predočuje certifikat MSCA_VU koji se upotrebljava za provjeru njezina certifikata jedinice u vozilu, certifikat VU.CA.EUR koji se upotrebljava za provjeru certifikata MSCA_VU te potencijalno certifikat o povezanosti, kako bi se pronašao certifikat koji kartica prepoznaje ili može provjeriti. Ako je takav certifikat pronađen, kartica upotrebljava taj certifikat za provjeru temeljnih certifikata jedinice u vozilu koji su joj predočeni. Ako je uspješna, jedinica u vozilu konačno postavlja svoj javni ključ za upotrebu u tahografskoj kartici. Ako provjera nije uspješna, jedinica u vozilu zanemaruje karticu.

Napomena: Postoje tri načina na koje kartica može prepoznati certifikat VU.CA.EUR:

— certifikat VU.CA.EUR isti je certifikat kao i vlastiti certifikat EUR kartice;

— certifikat VU.CA.EUR prethodi vlastitom certifikatu EUR kartice te je kartica već sadržavala taj certifikat pri izdavanju (vidjeti CSM_91);

— certifikat VU.CA.EUR nasljeđuje vlastiti certifikat EUR kartice te je kartica u prošlosti primila certifikat o povezanosti od druge jedinice u vozilu, provjerila ga i pohranila za buduću upotrebu.

CSM_163 VU upotrebljava naredbu MSE: SET AT za postavljanje svojeg javnog ključa za upotrebu u tahografskoj kartici. Kako je navedeno u Dodatku 2., ta naredba sadržava oznaku kriptografskog mehanizma koji će se upotrebljavati s postavljenim ključem. Taj je mehanizam „autentifikacija jedinice u vozilu upotrebom algoritma ECDSA u kombinaciji s algoritmom raspršivanja (*hash*) povezanim s veličinom ključa para VU_MA ključeva jedinice u vozilu, kako je navedeno u CSM_50”.

CSM_164 Naredba MSE: SET AT isto tako sadržava oznaku kratkotrajnog para ključeva koje jedinica u vozilu upotrebljava tijekom dogovaranja ključa razmjene podataka (vidjeti odjeljak 10.4.). Stoga prije slanja naredbe MSE: SET AT jedinica u vozilu generira kratkotrajni par ECC ključeva. Za generiranje kratkotrajnog para ključeva VU upotrebljava normirane parametre domene navedene u certifikatu kartice. Kratkotrajni par ključeva označuje se kao ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). Jedinica u vozilu uzima x-koordinatu ECDH kratkotrajne javne točke kao identifikaciju ključa; to se naziva komprimirano predstavljanje javnog ključa i označuje se kao Comp($VU.PK_{eph}$).

CSM_165 Ako je naredba MSE: SET AT uspješna, kartica postavlja navedeni VU.PK za kasniju upotrebu tijekom autentifikacije VU te privremeno pohranjuje Comp($VU.PK_{eph}$). U slučaju slanja jedne ili više uspješnih naredbi MSE: SET AT prije provedbe dogovaranja ključa razmjene podataka, kartica pohranjuje samo zadnji primljeni Comp($VU.PK_{eph}$).

CSM_166 Kartica provjerava vremensku valjanost svakog certifikata koji jedinica u vozilu predočava ili na njega upućuje dok je pohranjen u memoriji kartice te odbija certifikate koji su istekli.

CSM_167 Za provjeru vremenske valjanosti certifikata koji je predočila jedinica u vozilu, svaka tahografska kartica interno pohranjuje određene podatke koji predstavljaju trenutačno vrijeme. Jedinica u vozilu te podatke ne smije moći izravno ažurirati. Pri izdavanju trenutačno se vrijeme kartice postavlja tako da je jednako datumu početka valjanosti certifikata kartice Card_MA. Kartica ažurira svoje trenutačno vrijeme ako je datum početka valjanosti autentičnog certifikata „valjanog izvora vremena" koji je predočila jedinica u vozilu noviji od trenutačnog vremena kartice. U tom slučaju kartica postavlja svoje trenutačno vrijeme na datum početka valjanosti tog certifikata. Kartica kao valjani izvor vremena prihvaća samo sljedeće certifikate:

— certifikate o povezanosti ERCA druge generacije,

— certifikate MSCA druge generacije,

— certifikate jedinice u vozilu druge generacije koje je izdala ista država kao i vlastiti certifikat (certifikate) kartice.

Napomena: posljednji zahtjev znači da kartica može prepoznati CAR certifikata jedinice u vozilu, tj. certifikat MSCA_VU-EGF. On nije jednak CAR-u njezina vlastitog certifikata, odnosno certifikata MSCA_Card.

CSM_168 Kako je prikazano na slici 5., kada je kartica provjerila autentičnost i valjanost prethodno nepoznatog certifikata, taj certifikat može pohraniti za buduću upotrebu tako da ne mora ponovno provjeravati autentičnost tog certifikata ako je ponovno predočen kartici. Osim pohranjivanja cijelog certifikata, kartica može odabrati pohraniti samo sadržaj tijela certifikata, kako je navedeno u odjeljku 9.3.2.

10.3. **Autentifikacija jedinice u vozilu**

CSM_169 Jedinice u vozilu i kartice upotrebljavaju protokol autentifikacije jedinice u vozilu prikazan na slici 6. za autentifikaciju jedinice u vozilu s obzirom na karticu. Autentifikacija jedinice u vozilu omogućuje tahografskoj kartici da izričito provjeri autentičnost jedinice u vozilu. Kako bi to učinila, jedinica u vozilu upotrebljava svoj privatni ključ za potpisivanje zahtjeva za ključnu riječ koji generira kartica.

CSM_170 Uz zahtjev kartice za ključnu riječ, jedinica u vozilu u potpis uključuje upućivanje na nositelja kartice preuzeto iz certifikata kartice.

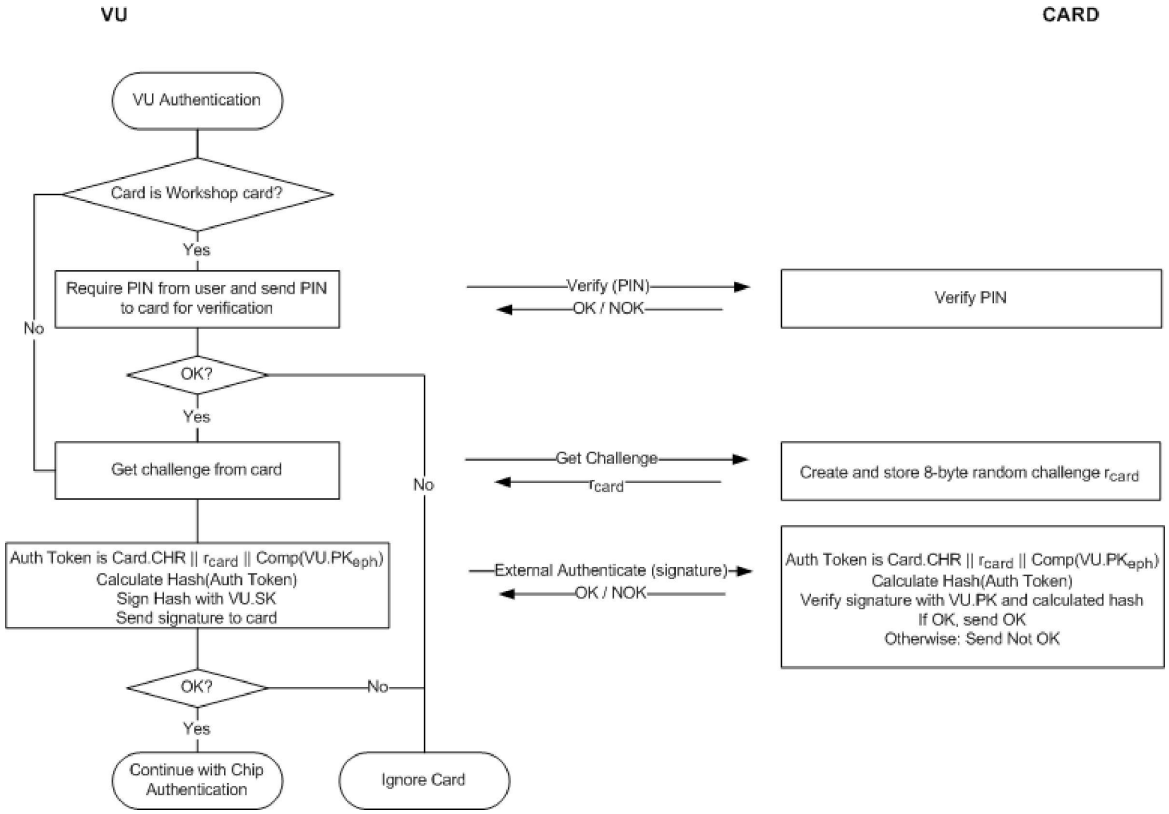
Napomena: time se osigurava da je kartica koju jedinica u vozilu sama autentificira ista kartica čiji je lanac certifikata jedinica u vozilu prethodno provjerila.

CSM_171 Osim toga, jedinica u vozilu u potpis uključuje identifikator kratkotrajnog javnog ključa Comp(VU.PK_{eph}) koji jedinica u vozilu upotrebljava za uspostavu sigurnog prijenosa poruka tijekom postupka autentifikacije čipa navedenog u odjeljku 10.4.

Napomena: time se osigurava da je jedinica u vozilu s kojom kartica komunicira tijekom procesa sigurnog prijenosa poruka ista jedinica u vozilu koju je autentificirala kartica.

Slika 6.

Protokol za autentifikaciju jedinice u vozilu (VU)



CSM_172 Ako jedinica u vozilu tijekom autentifikacije jedinice u vozilu pošalje više naredbi GET CHALLENGE, kartica svaki put vraća novi 8-bajtni nasumični zahtjev za ključnu riječ, ali pohranjuje samo posljednji zahtjev za ključnu riječ.

CSM_173 Algoritam potpisivanja koji jedinica u vozilu upotrebljava za autentifikaciju jedinice u vozilu je ECDSA, kako je navedeno u [DSS], upotrebom algoritma raspršivanja (*hashing*) povezanog s veličinom ključa para VU_MA ključeva jedinice u vozilu, kako je navedeno u CSM_50. Format potpisa je nešifriran, kako je navedeno u [TR-03111]. Dobiveni potpis jedinica u vozilu šalje kartici.

CSM_174 Nakon što primi potpis jedinice u vozilu u naredbi EXTERNAL AUTHENTICATE, kartica:

— izračunava token autentifikacije ulančavanjem Card.CHR, zahtjeva kartice za ključnu riječ r_{card} i identifikatora kratkotrajnog javnog ključa jedinice u vozilu Comp($VU.PK_{eph}$),

— izračunava raspršivanje (*hash*) za token autentifikacije s pomoću algoritma raspršivanja (*hashing*) povezanog s veličinom ključa para VU_MA ključeva jedinice u vozilu, kako je navedeno u CSM_50,

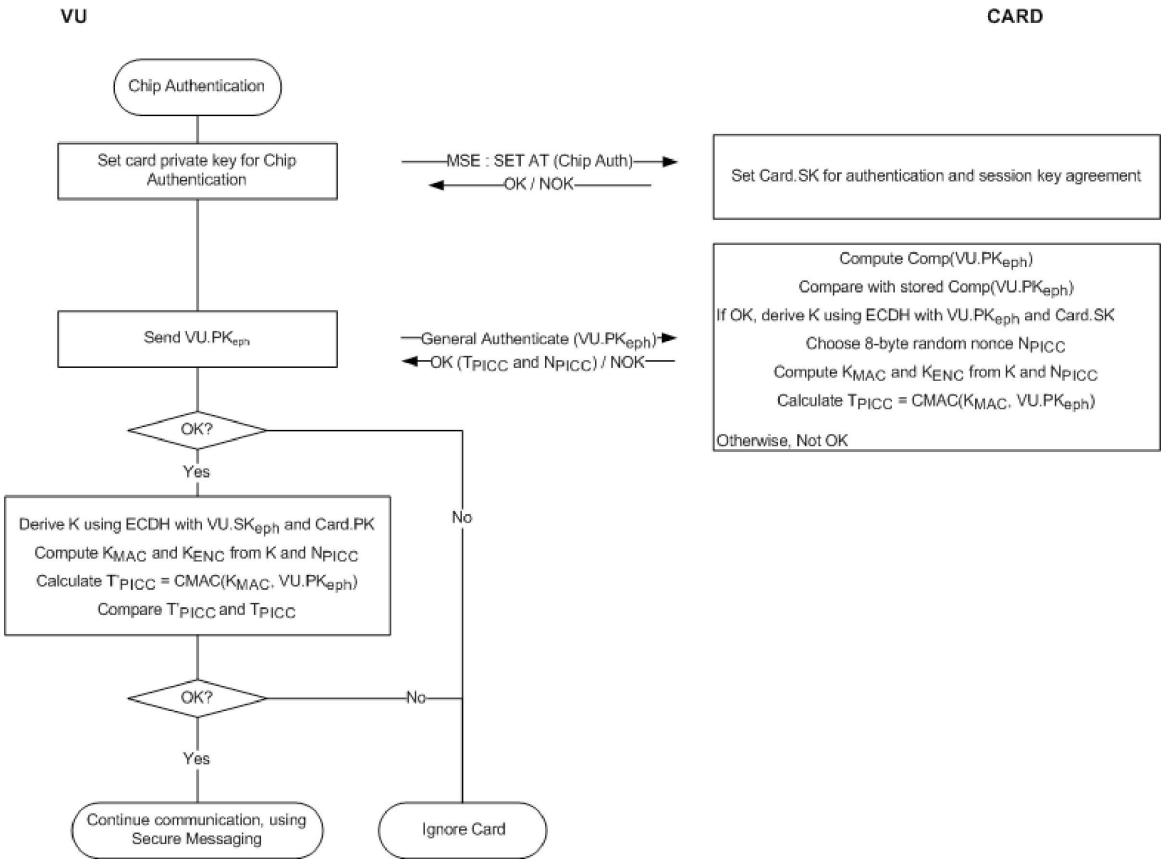
— provjerava potpis jedinice u vozilu upotrebom algoritma ECDSA u kombinaciji s VU.PK i izračunanim raspršivanjem (*hash*).

10.4. Autentifikacija čipa i dogovaranje ključa razmjene podataka

CSM_175 Jedinice u vozilu i kartice upotrebljavaju protokol autentifikacije čipa prikazan na **slici 7.** za autentifikaciju kartice u odnosu na jedinicu u vozilu. Autentifikacija čipa omogućuje jedinici u vozilu da izričito provjeri autentičnost kartice.

Slika 7.

Autentifikacija čipa i dogovaranje ključa razmjene podataka



CSM_176 Jedinica u vozilu i kartica poduzimaju sljedeće korake:

1. Jedinica u vozilu započinje postupak autentifikacije čipa slanjem naredbe MSE: SET AT u kojoj se navodi „autentifikacija čipa s pomoću algoritma ECDSA kojim se dobiva duljina AES ključa razmjene podataka povezana s veličinom ključa para Card_MA ključeva kartice, kako je navedeno u CSM_50”. Jedinica u vozilu utvrđuje veličinu ključa para ključeva kartice iz certifikata kartice.

2. Jedinica u vozilu šalje kartici javnu točku $VU.PK_{eph}$ svojeg kratkotrajnog para ključeva. Kako je objašnjeno u CSM_164, jedinica u vozilu taj kratkotrajni par ključeva generira prije provjere lanca certifikata jedinice u vozilu. Jedinica u vozilu šalje kartici identifikator kratkotrajnog javnog ključa $Comp(VU.PK_{eph})$ te ga kartica pohranjuje.

3. Kartica izračunava $Comp(VU.PK_{eph})$ iz $VU.PK_{eph}$ i uspoređuje ga s pohranjenom vrijednošću Comp(VU.PKeph).

4. Primjenom algoritma ECDH u kombinaciji sa statičkim privatnim ključem i kratkotrajnim javnim ključem jedinice u vozilu, kartica izračunava tajni K.

5. Kartica odabire nasumični 8-bajtni broj za jednokratnu upotrebu (eng. *number used only once, nonce*) N_{PICC} i upotrebljava ga za izvođenje dvaju AES ključeva razmjene podataka K_{MAC} i K_{ENC} iz K. Vidjeti CSM_179.

6. S pomoću K_{MAC} kartica izračunava token autentifikacije za identifikator kratkotrajnog javnog ključa VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Kartica šalje N_{PICC} i T_{PICC} jedinici u vozilu.

7. Primjenom algoritma ECDH u kombinaciji sa statičkim javnim ključem i kratkotrajnim javnim ključem jedinice u vozilu, jedinica u vozilu izračunava isti tajni K kao kartica u koraku 4.

8. Jedinica u vozilu izvodi ključeve razmjene podataka K_{MAC} i K_{ENC} iz K i N_{PICC}. Vidjeti CSM_179.

9. Jedinica u vozilu provjerava token autentifikacije T_{PICC}.

CSM_177 U prethodnom koraku 3. kartica izračunava Comp(VU.PK_{eph}) kao x-koordinatu javne točke u VU.PK_{eph}.

CSM_178 U prethodnim koracima 4. i 7. kartica i jedinica u vozilu upotrebljavaju algoritam ECKA-EG kako je utvrđeno u [TR-03111].

CSM_179 U prethodnim koracima 5. i 8. kartica i jedinica u vozilu upotrebljavaju funkciju izvođenja ključeva za AES ključeve razmjene podataka utvrđene u [TR-03111] sa sljedećim preciznostima i promjenama:

— vrijednost brojača iznosi '00 00 00 01' za K_{ENC} i '00 00 00 02'za K_{MAC},.

— upotrebljava se neobavezni broj za jednokratnu upotrebu (*nonce*) r koji je jednak N_{PICC}.

— Za izvođenje AES ključeva od 128 bitova upotrebljava se algoritam raspršivanja (*hashing*) SHA-256,

— Za izvođenje AES ključeva od 192 bita upotrebljava se algoritam raspršivanja (*hashing*) SHA-384,

— Za izvođenje AES ključeva od 256 bitova upotrebljava se algoritam raspršivanja (*hashing*) SHA-512.

Duljina ključeva razmjene podataka (tj. duljina na koju je *hash* skraćen) povezana je s veličinom para Card_MA ključeva, kako je navedeno u CSM_50.

CSM_180 U prethodnim koracima 6. i 9. kartica i jedinica u vozilu upotrebljavaju AES algoritam u načinu rada CMAC, kako je navedeno u [SP 800-38B]. Duljina T_{PICC} povezana je s duljinom AES ključeva razmjene podataka, kako je navedeno u CSM_50.

10.5. **Siguran prijenos poruka**

10.5.1 *Općenito*

CSM_181 Sve naredbe i odgovori razmijenjeni između jedinice u vozilu i tahografske kartice nakon uspješne autentifikacije čipa i do završetka razmjene podataka zaštićeni su sigurnim prijenosom poruka.

CSM_182 Osim pri čitanju iz datoteke s uvjetom pristupa SM-R-ENC-MAC-G2 (vidjeti Dodatak 2., odjeljak 4.), siguran prijenos poruka upotrebljava se u načinu rada namijenjenom isključivo autentifikaciji. U tom se načinu rada kriptografski kontrolni zbroj (odnosno MAC) dodaje svim naredbama i odgovorima u svrhu osiguranja autentičnosti i integriteta poruke.

CSM_183 Pri čitanju podataka iz datoteke s uvjetom pristupa SM-R-ENC-MAC-G2, siguran prijenos poruka upotrebljava se u načinu rada namijenjenom šifriranju i zatim autentifikaciji, tj. podatci odgovora prvo se šifriraju u svrhu osiguranja povjerljivosti poruke, a zatim se izračunava MAC za formatirane šifrirane podatke u svrhu osiguranja autentičnosti i integriteta.

CSM_184 Siguran prijenos poruka upotrebljava AES kako je utvrđen u [AES] s ključevima razmjene podataka K_{MAC} i K_{ENC} koji su dogovoreni tijekom autentifikacije čipa.

CSM_185 Kao brojač redoslijeda slanja (SSC) upotrebljava se nepotpisani cijeli broj u svrhu sprječavanja napada reprodukcijom. Veličina SSC-a jednaka je veličini AES bloka, tj. 128 bitova. SSC je u formatu MSB-first. Brojač redoslijeda slanja (SSC) postavlja se na nulu (tj. '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00') prilikom početka sigurnog prijenosa poruka. SSC se povećava svaki put prije generiranja naredbe ili odgovora APDU, tj. budući da je početna vrijednost SSC-a u procesu sigurnog prijenosa poruke (SM) 0, u prvoj će naredbi vrijednost SSC-a biti 1. Vrijednost SSC-a za prvi odgovor bit će 2.

CSM_186 Za šifriranje poruka upotrebljava se K_{ENC} s AES-om u načinu rada „ulančavanje šifriranih blokova" (CBC), kako je utvrđeno u [ISO 10116], s parametrom preraspodjele (eng. *interleave parameter*) *m* = 1 i inicijalizacijskim vektorom (eng. *initialization vector*) SV = E(K_{ENC}, SSC), tj. trenutačnom vrijednošću brojača redoslijeda slanja šifriranom s K_{ENC}.

CSM_187 Za autentifikaciju poruka upotrebljava se K_{MAC} s AES-om u načinu rada CMAC kako je navedeno u [SP 800-38B]. Duljina MAC povezana je s duljinom AES ključeva razmjene podataka, kako je navedeno u CSM_50. Brojač redoslijeda slanja (SSC) uključuje se u MAC njegovim dodavanjem na početak prije bloka podataka (eng. *datagram*) koji se autentificira.

10.5.2 *Struktura sigurne poruke*

CSM_188 Siguran prijenos poruka upotrebljava samo podatkovne objekte sigurnog prijenosa poruka (vidjeti normu [ISO 7816-4]) navedene u tablici 5. U svakoj se poruci ti podatkovni objekti upotrebljavaju redoslijedom navedenim u sljedećoj tablici:

Tablica 5.

Podatkovni objekti sigurnog prijenosa poruka

Naziv podatkovnog objekta	Oznaka	Prisutnost obvezna (O), uvjetna (U) ili zabranjena (Z) u	
		naredbama	odgovorima
Vrijednost koja nije kodirana u BER-TLV	'81'	U	U
Vrijednost koja je kodirana u BER-TLV, ali ne uključujući SM DO-ove	'B3'	U	U
Indikator popunjenja sadržaja nakon kojeg slijedi kriptogram, vrijednost koja nije kodirana u BER-TLV	'87'	U	U
Zaštićena Le	'97'	U	Z
Status obrade	'99'	Z	O
Kriptografski kontrolni zbroj	'8E'	O	O

Napomena: kako je navedeno u Dodatku 2., tahografske kartice mogu podržavati naredbe READ BINARY (čitanje datoteke) i UPDATE BINARY (ažuriranje datoteke) s neparnim INS bajtom ('B1' odnosno 'D7'). Te varijante naredbi trebaju čitati i ažurirati datoteke s više od 32 768 bajtova. U slučaju upotrebe takve varijante, podatkovni objekt s oznakom 'B3' upotrebljava se umjesto objekta s oznakom '81'. Za više informacija vidjeti Dodatak 2.

CSM_189 Svi podatkovni objekti sigurnog prijenosa poruka (SM) kodirani su u DER TLV kako je navedeno u normi [ISO 8825-1]. To kodiranje daje sljedeću strukturu vrijednosti duljine oznake (TLV):

Oznaka: Oznaka je kodirana u jednom ili dva okteta i označuje sadržaj.

Duljina: Duljina je kodirana kao nepotpisani cijeli broj u jednom, dva ili tri okteta, što dovodi do najveće duljine od 65 535 okteta. Upotrebljava se najmanji broj okteta.

Vrijednost: Vrijednost je kodirana u nula ili više okteta.

CSM_190 APDU-ovi zaštićeni sigurnim prijenosom poruka stvaraju se kako slijedi:

— Zaglavlje naredbe uključeno je u izračun MAC-a, stoga se upotrebljava vrijednost '0C' za bajt razreda CLA.

— Kako je navedeno u Dodatku 2., svi INS bajtovi su parni, s mogućim izuzetkom neparnih INS bajtova za naredbe READ BINARY i UPDATE BINARY.

— Stvarna vrijednost Lc preinačuje se u Lc' nakon primjene sigurnog prijenosa poruka.

— Podatkovno polje sastoji se od podatkovnih objekata sigurnog prijenosa poruka (SM).

— U zaštićenoj APDU naredbi novi bajt Le postavlja se na '00'. Ako je potrebno, podatkovni objekt '97' uključuje se u podatkovno polje kako bi proslijedio izvornu vrijednost Le.

CSM_191 Bilo koji podatkovni objekt koji se šifrira popunjuje se u skladu s normom [ISO 7816-4] upotrebom indikatora popunjenja sadržaja '01'. Za izračun MAC-a, svaki podatkovni objekt APDU isto se tako zasebno popunjuje u skladu s normom [ISO 7816-4].

Napomena: popunjenje za siguran prijenos poruka uvijek se provodi na razini sigurnog prijenosa poruka, a ne s pomoću algoritama CMAC ili CBC.

Sažetak i primjeri

Naredba APDU s primjenom sigurnog prijenosa poruka ima sljedeću strukturu, ovisno o slučaju odgovarajuće nezaštićene naredbe (DO je podatkovni objekt):

Slučaj 1.:	CLA INS P1 P2 || Lc' || DO '8E' || Le
Slučaj 2.:	CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le
Slučaj 3. (parni INS bajt):	CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le
Slučaj 3. (neparni INS bajt):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le
Slučaj 4. (parni INS bajt):	CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le
Slučaj 4. (neparni INS bajt):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

gdje je Le = '00' ili '00 00', ovisno o tome upotrebljavaju li se kratka polja (eng. *short length fields*) ili produljena polja (eng. *extended length fields*); vidjeti normu [ISO 7816-4].

Odgovor APDU s primjenom sigurnog prijenosa poruka ima sljedeću strukturu, ovisno o slučaju odgovarajućeg nezaštićenog odgovora:

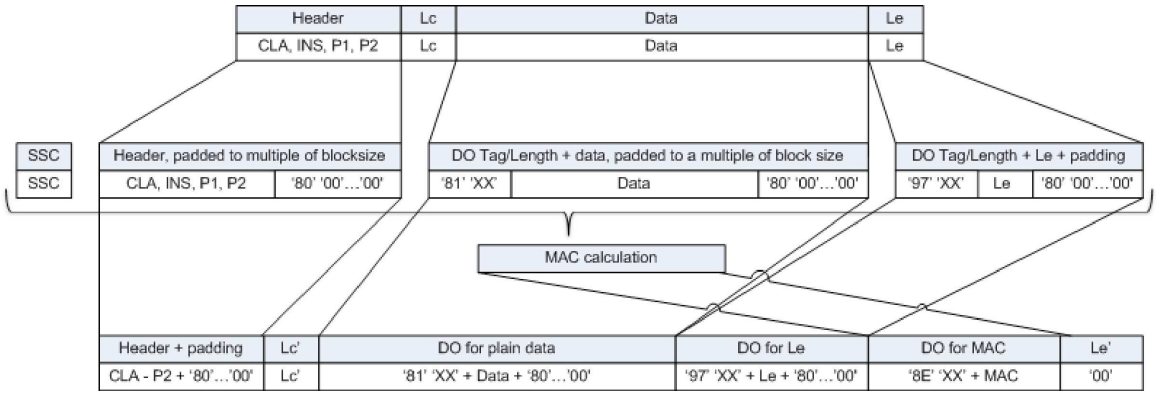
Slučaj 1. ili 3.:	DO '99' || DO '8E' || SW1SW2
Slučaj 2. ili 4. (parni INS bajt) sa šifriranjem:	DO '81' || DO '99' || DO '8E' || SW1SW2
Slučaj 2. ili 4. (parni INS bajt) bez šifriranja:	DO '87' || DO '99' || DO '8E' || SW1SW2
Slučaj 2. ili 4. (neparni INS bajt) bez šifriranja:	DO 'B3' || DO '99' || DO '8E' || SW1SW2

Napomena: slučaj 2. ili 4. (neparni INS bajt) sa šifriranjem nikad se ne upotrebljava za komunikaciju između jedinice u vozilu i kartice.

U nastavku su navedena tri primjera transformacije APDU za naredbe s parnim INS kodom. Slika 8. prikazuje autentificiranu naredbu APDU u slučaju 4., slika 9. prikazuje autentificirani odgovor APDU u slučaju 2. / slučaju 4., a slika 10. prikazuje šifrirani i autentificirani odgovor APDU u slučaju 2. / slučaju 4.

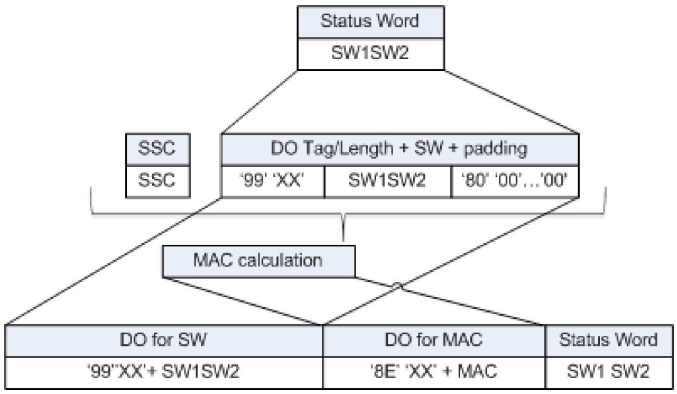
Slika 8.

Transformacija autentificirane naredbe APDU u slučaju 4.



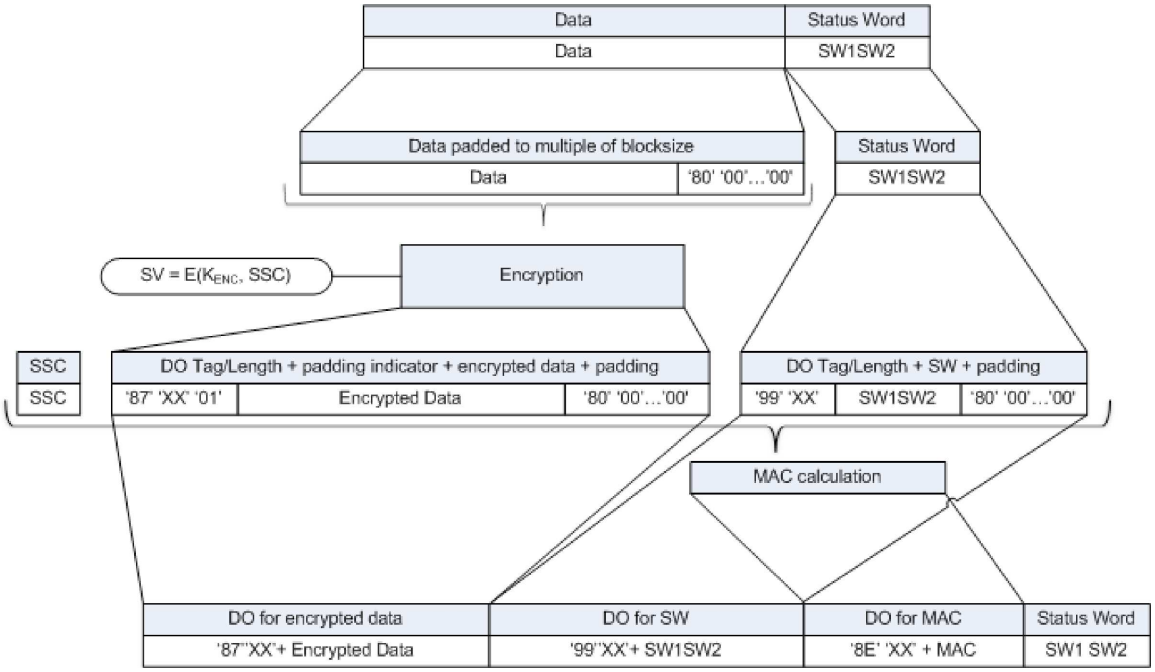
Slika 9.

Transformacija autentificiranog odgovora APDU u slučaju 1. / slučaju 3.



Slika 10.

Transformacija šifriranog i autentificiranog odgovora APDU u slučaju 2. / slučaju 4.



10.5.3 *Prekid procesa sigurnog prijenosa poruka*

CSM_192 Jedinica u vozilu prekida proces sigurnog prijenosa poruka koji je u tijeku ako i samo ako nastupi jedno od sljedećih stanja:

— ako primi nešifrirani odgovor APDU,

— ako u odgovoru APDU otkrije pogrešku u sigurnom prijenosu poruka:

— nedostaje očekivani podatkovni objekt sigurnog prijenosa poruka, redoslijed podatkovnih objekata netočan je ili je uključen nepoznati podatkovni objekt,

— podatkovni objekt sigurnog prijenosa poruka netočan je, npr. netočna je vrijednost MAC, netočna je struktura TLV ili indikator popunjenja u oznaci '87' nije jednak '01',

— ako je kartica poslala statusni bajt kojim javlja da je otkrila pogrešku u sigurnom prijenosu poruka (SM) (vidjeti CSM_194),

— ako je dosegnuta granica za broj naredbi i povezanih odgovora u razmjeni podataka koja je u tijeku. Tu granicu za određenu jedinicu u vozilu utvrđuje njezin proizvođač, uzimajući u obzir sigurnosne zahtjeve korištenog hardvera s najvećom vrijednošću od 240 SM naredbi i povezanih odgovora u jednoj razmjeni podataka.

CSM_193 Tahografska kartica prekida proces sigurnog prijenosa poruka koji je u tijeku ako i samo ako nastupi jedno od sljedećih stanja:

— ako primi nešifriranu naredbu APDU,

— ako u naredbi APDU otkrije pogrešku u sigurnom prijenosu poruka:

— nedostaje očekivani podatkovni objekt sigurnog prijenosa poruka, redoslijed podatkovnih objekata netočan je ili je uključen nepoznati podatkovni objekt,

— podatkovni objekt sigurnog prijenosa poruka netočan je, npr. netočna vrijednost MAC, netočna struktura TLV,

— ako je kartica isključena ili vraćena u početno stanje,

— ako jedinica u vozilu odabere aplikaciju na kartici,

— ako jedinica u vozilu započne postupak autentifikacije VU,

— ako je dosegnuta granica za broj naredbi i povezanih odgovora u razmjeni podataka koja je u tijeku. Tu granicu za određenu karticu utvrđuje njezin proizvođač uzimajući u obzir sigurnosne zahtjeve korištenog hardvera s najvećom vrijednošću od 240 SM naredbi i povezanih odgovora u jednom procesu.

CSM_194 U vezi s obradom SM pogrešaka koju provodi tahografska kartica:

— ako u naredbi APDU nedostaju neki očekivani podatkovni objekti sigurnog prijenosa poruka, redoslijed podatkovnih objekata netočan je ili je uključen nepoznati podatkovni objekt, tahografska kartica odgovara statusnim bajtovima ‘69 87’,

— ako je podatkovni objekt sigurnog prijenosa poruka u naredbi APDU netočan, tahografska kartica odgovara statusnim bajtovima ‘69 88’.

U takvom se slučaju statusni bajtovi vraćaju bez upotrebe sigurnog prijenosa poruka.

CSM_195 U slučaju prekida procesa sigurnog prijenosa poruka između jedinice u vozilu i tahografske kartice, jedinica u vozilu i tahografska kartica:

— na siguran način uništavaju pohranjene ključeve razmjene podataka,

— odmah uspostavljaju novi proces sigurne razmjene poruka, kako je opisano u odjeljcima od 10.2. do 10.5.

CSM_196 Ako zbog nekog razloga jedinica u vozilu odluči ponovno pokrenuti uzajamnu autentifikaciju s obzirom na umetnutu karticu, postupak počinje ponovno s provjerom lanca certifikata kartice, kako je opisano u odjeljku 10.2., i nastavlja se kako je opisano u odjeljcima od 10.2. do 10.5.

11. POVEZIVANJE, UZAJAMNA AUTENTIFIKACIJA I SIGURAN PRIJENOS PORUKA IZMEĐU JEDINICE U VOZILU I VANJSKOG UREĐAJA GNSS-a

11.1. **Općenito**

CSM_197 Uređaj GNSS-a koji jedinica u vozilu upotrebljava za utvrđivanje svojeg položaja može biti unutarnji (tj. ugrađen u jedinicu i neodvojiv) ili to može biti vanjski modul. U prvom slučaju nema potrebe za standardizacijom unutarnje komunikacije između uređaja GNSS-a i jedinice u vozilu te se zahtjevi ovog poglavlja ne primjenjuju. U potonjem slučaju, komunikacija između jedinice u vozilu i vanjskog uređaja GNSS-a standardizirana je i zaštićena kako je opisano u ovom poglavlju.

CSM_198 Sigurna komunikacija između jedinice u vozilu i vanjskog uređaja GNSS-a odvija se na isti način kao i sigurna komunikacija između jedinice u vozilu i tahografske kartice, pri čemu vanjski uređaj GNSS-a (EGF) ima ulogu kartice. Za EGF moraju biti ispunjeni svi zahtjevi navedeni u poglavlju 10. za tahografske kartice, uzimajući u obzir odstupanja, pojašnjenja i dodatke navedene u ovom poglavlju. Posebno se uzajamna provjera lanca certifikata, autentifikacija jedinice u vozilu i autentifikacija čipa provode na način opisan u odjeljcima 11.3. i 11.4.

CSM_199 Komunikacija između jedinice u vozilu i EGF-a razlikuje se od komunikacije između jedinice u vozilu i kartice u činjenici da se jedinica u vozilu i EGF moraju povezati kada su u radionici, prije nego što jedinica u vozilu može s EGF-om razmijeniti podatke na temelju GNSS-a tijekom redovnog rada. Postupak povezivanja opisan je u odjeljku 11.2.

CSM_200 Za komunikaciju između jedinice u vozilu i EGF-a upotrebljavaju se naredbe i odgovori APDU u skladu s normama [ISO 7816-4] i [ISO 7816-8]. Točna je struktura tih APDU-ova definirana u Dodatku 2. ovom Prilogu.

11.2. **Povezivanje jedinice u vozilu i vanjskog uređaja GNSS-a (EGF-a)**

CSM_201 Povezivanje jedinice u vozilu i EGF-a u vozilu provodi radionica. Jedinica u vozilu i EGF mogu komunicirati tijekom redovnog rada samo ako su povezani.

CSM_202 Povezivanje jedinice u vozilu i EGF-a moguće je ako je jedinica u vozilu u kalibracijskom načinu rada. Povezivanje pokreće jedinica u vozilu.

CSM_203 Radionica može u bilo kojem trenutku ponovno povezati jedinicu u vozilu s drugim EGF-om ili s istim EGF-om. Tijekom ponovnog uparivanja jedinica u vozilu na siguran način uništava postojeći certifikat EGF_MA u svojoj memoriji te pohranjuje certifikat EGF_MA na EGF s kojim se povezuje.

CSM_204 Radionica može u bilo kojem trenutku ponovno povezati vanjski uređaj GNSS-a s drugom jedinicom u vozilu ili s istom jedinicom u vozilu. Tijekom ponovnog povezivanja EGF na siguran način uništava postojeći certifikat VU_MA u svojoj memoriji te pohranjuje certifikat VU_MA na jedinicu u vozilu s kojom se povezuje.

11.3. **Uzajamna provjera lanca certifikata**

11.3.1 *Općenito*

CSM_205 Uzajamna provjera lanca certifikata između jedinice u vozilu i EGF-a odvija se samo tijekom povezivanja jedinice u vozilu i EGF-a koje provodi radionica. Tijekom redovnog rada povezanih jedinice u vozilu i EGF-a ne provjeravaju se certifikati. Umjesto toga, jedinica u vozilu i EGF imaju povjerenja u certifikate koje su pohranili tijekom povezivanja, nakon provjere vremenske valjanosti tih certifikata. Jedinica u vozilu i EGF nemaju povjerenja u druge certifikate za zaštitu komunikacije jedinica u vozilu – EGF tijekom redovnog rada.

11.3.2 *Tijekom povezivanja jedinica u vozilu (VU) – EGF*

CSM_206 Tijekom povezivanja na EGF, jedinica u vozilu upotrebljava protokol prikazan na slici 4. (odjeljak 10.2.1.) za provjeru lanca certifikata vanjskog uređaja GNSS-a.

Napomene za sliku 4. u tom kontekstu:

— Upravljanje komunikacijom nije u području primjene ovog Dodatka. Međutim, EGF nije pametna kartica te stoga jedinica u vozilu vjerojatno neće poslati naredbu vraćanja u početno stanje (eng. *reset*) za pokretanje komunikacije te neće primiti ATR.

— Certifikati Card i javni ključevi prikazani na slici tumače se kao certifikati EGF i javni ključevi za uzajamnu autentifikaciju. U odjeljku 9.1.6. označeni su kao EGF_MA.

— Certifikati Card:CA i javni ključevi prikazani na slici tumače se kao certifikati MSCA i javni ključevi za potpisivanje certifikata EGF. U odjeljku 9.1.3. označeni su kao MSCA_VU-EGF.

— Certifikat Card.CA.EUR prikazan na slici tumači se kao europski glavni certifikat koji je naveden u CAR certifikata MSCA_VU-EGF.

— Certifikat Card.Link prikazan na slici tumači se kao certifikat o povezanosti EGF-a, ako postoji. Kako je navedeno u odjeljku 9.1.2., to je certifikat o povezanosti za novi europski glavni par ključeva koji je ERCA stvorila i potpisala prethodnim europskim privatnim ključem.

— Certifikat Card.Link.EUR je europski glavni certifikat koji je naveden u CAR certifikata Card. Link.

— Umjesto `cardExtendedSerialNumber`, jedinica u vozilu čita `sensorGNSSserialNumber` iz elementarne datoteke (EF) ICC.

— Umjesto odabira AID tahografa, jedinica u vozilu odabire AID EGF-a.

— „Ignore Card" tumači se kao „Ignore EGF".

CSM_207 Jednom kad je provjerila certifikat EGF_MA, jedinica u vozilu pohranjuje taj certifikat za upotrebu tijekom redovnog rada; vidjeti odjeljak 11.3.3.

CSM_208 Tijekom povezivanja na jedinicu u vozilu, vanjski uređaj GNSS-a upotrebljava protokol prikazan na slici 5. (odjeljak 10.2.2.) za provjeru lanca certifikata jedinice u vozilu.

Napomene za sliku 5. u tom kontekstu:

— Jedinica u vozilu generira novi kratkotrajni par ključeva s pomoću parametara domene u certifikatu EGF.

— Certifikati jedinice u vozilu i javni ključevi prikazani na slici oni su za uzajamnu autentifikaciju. U odjeljku 9.1.4. označeni su kao VU_MA,

— Certifikati VU.CA i javni ključevi prikazani na slici oni su za potpisivanje certifikata jedinica u vozilu i vanjskih uređaja GNSS-a. U odjeljku 9.1.3. označeni su kao MSCA_VU-EGF.

— Certifikat VU.CA.EUR prikazan na slici je europski glavni certifikat koji je naveden u CAR certifikata VU.CA.

— Certifikat VU.Link prikazan na slici je certifikat o povezanosti jedinice u vozilu, ako postoji. Kako je navedeno u odjeljku 9.1.2., to je certifikat o povezanosti za novi europski glavni par ključeva koji je ERCA stvorila i potpisala prethodnim europskim privatnim ključem.

— Certifikat VU.Link.EUR je europski glavni certifikat koji je naveden u CAR certifikata VU.Link.

CSM_209 Odstupajući od zahtjeva CSM_167, EGF upotrebljava vrijeme GNSS-a za provjeru vremenske valjanosti svakog predočenog certifikata.

CSM_210 Jednom kada je provjerio certifikat VU_MA, vanjski uređaj GNSS-a pohranjuje taj certifikat za upotrebu tijekom redovnog rada; vidjeti odjeljak 11.3.3.

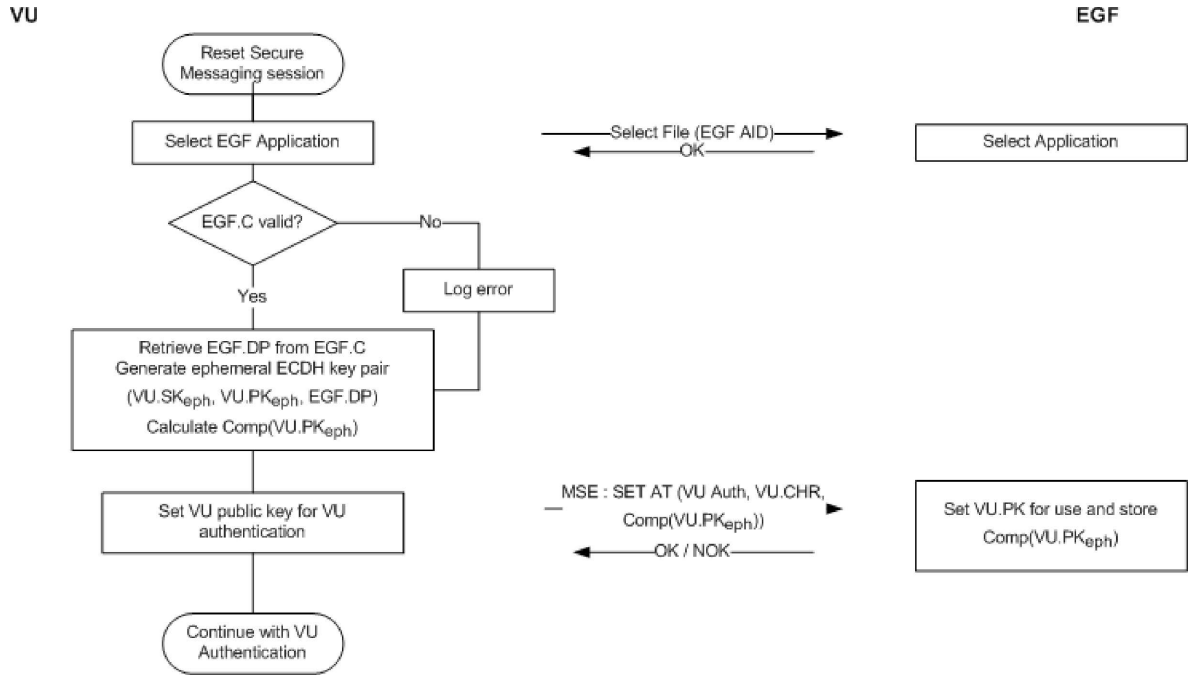
11.3.3 *Tijekom redovnog rada*

CSM_211 Tijekom redovnog rada, jedinica u vozilu i EGF upotrebljavaju protokol prikazan na slici 11. za provjeru vremenske valjanosti pohranjenih certifikata EGF_MA i VU_MA te za postavljanje javnog ključa VU_MA za kasniju autentifikaciju jedinice u vozilu. Tijekom redovnog rada ne odvija se nikakva daljnja uzajamna provjera lanca certifikata.

Treba napomenuti da se slika 11. zapravo sastoji od prvih koraka prikazanih na slikama 4. i 5. Nadalje, treba uzeti u obzir da EGF nije pametna kartica te da jedinica u vozilu vjerojatno neće poslati naredbu vraćanja u početno stanje (eng. *reset*) za pokretanje komunikacije te neće primiti ATR. U svakom je slučaju to izvan područja primjene ovog Dodatka.

Slika 11.

Uzajamna provjera vremenske valjanosti certifikata tijekom redovnog rada VU – EGF



CSM_212 Kako je prikazano na slici 11., jedinica u vozilu (VU) bilježi pogrešku ako certifikat EGF_MA više nije valjan. Međutim, uzajamna autentifikacija, dogovaranje ključa i kasnija komunikacija sigurnim prijenosom poruka normalno se nastavljaju.

11.4. Autentifikacija jedinice u vozilu, autentifikacija čipa i dogovaranje ključa razmjene podataka

CSM_213 Autentifikacija jedinice u vozilu, autentifikacija čipa i dogovaranje ključa razmjene podataka između jedinice u vozilu i EGF-a odvijaju se tijekom povezivanja i svaki put kad je proces sigurnog prijenosa poruka ponovno uspostavljen tijekom redovnog rada. Jedinica u vozilu i EGF provode postupke opisane u odjeljcima 10.3. i 10.4. Primjenjuju se svi zahtjevi iz tih odjeljaka.

11.5. Siguran prijenos poruka

CSM_214 Sve naredbe i odgovori razmijenjeni između jedinice u vozilu i vanjskog uređaja GNSS-a nakon uspješne autentifikacije čipa i do završetka razmjene podataka zaštićeni su sigurnim prijenosom poruka u načinu rada namijenjenom isključivo autentifikaciji. Primjenjuju se svi zahtjevi iz odjeljka 10.5.

CSM_215 U slučaju prekida procesa sigurnog prijenosa poruka između jedinice u vozilu i EGF-a, jedinica u vozilu odmah uspostavlja novi proces sigurnog prijenosa poruka, kako je opisano u odjeljcima 11.3.3. i 11.4.

12. UPARIVANJE I KOMUNIKACIJA IZMEĐU JEDINICE U VOZILU I SENZORA KRETANJA

12.1. **Općenito**

CSM_216 Jedinica u vozilu i senzor kretanja komuniciraju upotrebom protokola sučelja navedenog u normi [ISO 16844-3] tijekom uparivanja i redovnog rada, uz promjene navedene u ovom poglavlju i odjeljku 9.2.1.

Napomena: čitatelji ovog poglavlja trebaju biti upoznati sa sadržajem norme [ISO 16844-3].

12.2. **Uparivanje jedinice u vozilu i senzora kretanja upotrebom različitih generacija ključeva**

Kako je objašnjeno u odjeljku 9.2.1., glavni ključ senzora kretanja i svi povezani ključevi redovito se zamjenjuju. To dovodi do prisutnosti najviše triju AES ključeva K_{M-WC} (uzastopnih generacija ključeva) povezanih sa senzorom kretanja na karticama radionica. Jednako tako, u senzorima kretanja mogu biti prisutna do tri različita šifriranja podataka na temelju AES (na temelju uzastopnih generacija glavnog ključa senzora kretanja K_M). Jedinica u vozilu sadržava samo jedan ključ $K_{M-VU,}$ povezan sa senzorom kretanja.

CSM_217 Jedinica u vozilu druge generacije i senzor kretanja druge generacije uparuju se kako slijedi (usporediti s tablicom 6. u normi [ISO 16844-3]):

1. u jedinicu u vozilu umeće se kartica radionice druge generacije te se jedinica u vozilu povezuje sa senzorom kretanja;

2. Jedinica u vozilu čita sve dostupne ključeve K_{M-WC} s kartice radionice, pregledava njihove brojeve verzija ključa i odabire onaj koji odgovara broju verzije ključa K_{M-VU} jedinice u vozilu. Ako na kartici radionice nije prisutan odgovarajući ključ K_{M-WC}, jedinica u vozilu prekida postupak uparivanja te nositelju kartice radionice prikazuje odgovarajuću poruku o pogrešci.

3. Jedinica u vozilu izračunava glavni ključ senzora kretanja K_M iz K_{M-VU} i $K_{M-WC,}$ te identifikacijski ključ K_{ID} iz K_M, kako je navedeno u odjeljku 9.2.1.

4. Jedinica u vozilu šalje uputu za pokretanje postupka uparivanja s obzirom na senzor kretanja, kako je opisano u normi [ISO 16844-3], te šifrira serijski broj koji je primila od senzora kretanja s identifikacijskim ključem $K_{ID.}$ Jedinica u vozilu šalje šifrirani serijski broj senzoru kretanja.

5. Senzor kretanja uzastopno uspoređuje šifrirani serijski broj sa svakim šifriranjem serijskog broja koje je interno pohranio. Ako nađe odgovarajući broj, jedinica u vozilu je autentificirana. Senzor kretanja bilježi generaciju K_{ID} koju upotrebljava jedinica u vozilu i vraća odgovarajuću šifriranu vrijednost svojeg ključa uparivanja; tj. šifriranje je stvoreno upotrebom iste generacije K_M.

6. Jedinica u vozilu dešifrira ključ uparivanja s pomoću K_M, generira ključ razmjene podataka $K_{S,}$ šifrira ga s ključem uparivanja i rezultat šalje senzoru kretanja. Senzor kretanja dešifrira K_S.

7. Jedinica u vozilu prikuplja informacije za uparivanje, kako je utvrđeno u normi [ISO 16844-3], šifrira informacije s ključem uparivanja i rezultat šalje senzoru kretanja. Senzor kretanja dešifrira informacije za uparivanje.

8. Senzor kretanja šifrira primljene informacije za uparivanje s primljenim K_S i to vraća jedinici u vozilu. Jedinica u vozilu provjerava da su informacije za uparivanje iste informacije koje je jedinica u vozilu poslala senzoru kretanja u prethodnom koraku. Ako jest, to dokazuje da je senzor kretanja upotrijebio isti K_S kao jedinica u vozilu te je stoga u koraku 5. poslao svoj ključ uparivanja šifriran s ispravnom generacijom K_M. Slijedom toga, senzor kretanja je autentificiran.

Treba napomenuti da se koraci 2. i 5. razlikuju od standardnog postupka u normi [ISO 16844-3]; ostali su koraci standardni.

Primjer: pretpostavimo da se uparivanje odvija u prvoj godini valjanosti certifikata ERCA (3); vidjeti sliku 2. u odjeljku 9.2.1.2. Nadalje,

— pretpostavimo da je senzor kretanja izdan u posljednjoj godini valjanosti certifikata ERCA (1). Stoga će sadržavati sljedeće ključeve i podatke:

  — $N_s[1]$: vlastiti serijski broj šifriran s prvom generacijom K_{ID},

  — $N_s[2]$: vlastiti serijski broj šifriran s drugom generacijom K_{ID},

  — $N_s[3]$: vlastiti serijski broj šifriran s trećom generacijom K_{ID},

  — $K_P[1]$: vlastiti ključ uparivanja prve generacije ([1]), šifriran s prvom generacijom K_M,

  — $K_P[2]$: vlastiti ključ uparivanja druge generacije, šifriran s drugom generacijom K_M,

  — $K_P[3]$: vlastiti ključ uparivanja treće generacije, šifriran s trećom generacijom K_M;

— pretpostavimo da je kartica radionice izdana u prvoj godini valjanosti certifikata ERCA (3). Zato će sadržavati drugu generaciju i treću generaciju ključa $K_{M\text{-}WC}$;

— pretpostavimo da je VU jedinica u vozilu druge generacije i sadržava drugu generaciju $K_{M\text{-}VU.}$

U tom se slučaju u koracima od 2. do 5. događa sljedeće:

— 2. korak: VU čita drugu generaciju i treću generaciju $K_{M\text{-}WC}$ s kartice radionice i pregledava njihove brojeve verzija.

— 3. korak: VU kombinira drugu generaciju $K_{M\text{-}WC}$ sa svojim $K_{M\text{-}VU}$ za izračun K_M i $K_{ID.}$

— 4. korak: VU šifrira serijski broj koji je primila od senzora kretanja s $K_{ID.}$

— 5. korak: senzor kretanja uspoređuje primljene podatke s $N_s[1]$ i ne nalazi odgovarajući broj. Nakon toga, uspoređuje primljene podatke s $N_s[2]$ i nalazi odgovarajući broj. Zaključuje da je ta VU jedinica u vozilu druge generacije i stoga nazad šalje $K_P[2]$.

12.3. **Uparivanje i komunikacija između jedinice u vozilu i senzora kretanja upotrebom AES**

CSM_218 Kako je navedeno u tablici 3. odjeljka 9.2.1., svi su ključevi uključeni u uparivanje jedinice u vozilu (druge generacije) i senzora kretanja te u kasniju komunikaciju AES ključevi, a ne TDES ključevi dvostruke duljine kako je navedeno u normi [ISO 16844-3]. Ti AES ključevi mogu biti duljine 128, 192 ili 256 bitova. Budući da je veličina AES bloka 16 bajtova, duljina šifrirane poruke mora biti višekratnik 16 bajtova u usporedbi s 8 bajtova za TDES. Nadalje, neke će se od tih poruka upotrebljavati za prijenos AES ključeva, čija duljina može biti 128, 192 ili 256 bitova. Stoga se broj bajtova podataka po uputi u tablici 5. iz norme [ISO 16844-3] mijenja kako je prikazano u tablici 6.:

Tablica 6.

Broj bajtova nešifriranih i šifriranih podataka prema uputi utvrđenoj u normi [ISO 16844-3]

Uputa	Zahtjev / odgovor	Opis podataka	# bajtova nešifriranih podataka u skladu s normom [ISO 16844-3]	# bajtova nešifriranih podataka upotrebom AES ključeva	# bajtova šifriranih podataka upotrebom AES ključeva duljine bitova od		
					128	192	256
10	zahtjev	podatci za autentifikaciju + broj datoteke	8	8	16	16	16

([1]) Treba napomenuti da ključevi uparivanja prve, druge i treće generacije mogu zapravo biti isti ključ ili mogu biti tri različita ključa različite duljine, kako je objašnjeno u CSM_117.

Uputa	Zahtjev / odgovor	Opis podataka	# bajtova nešifriranih podataka u skladu s normom [ISO 16844-3]	# bajtova nešifriranih podataka upotrebom AES ključeva	# bajtova šifriranih podataka upotrebom AES ključeva duljine bitova od		
					128	192	256
11	odgovor	podatci za autentifikaciju + sadržaj datoteke	16 ili 32, ovisno o datoteci	16 ili 32, ovisno o datoteci	16 / 32	16 / 32	16 / 32
41	zahtjev	serijski broj senzora kretanja (MoS)	8	8	16	16	16
41	odgovor	ključ uparivanja	16	16 / 24 / 32	16	32	32
42	zahtjev	ključ razmjene podataka	16	16 / 24 / 32	16	32	32
43	zahtjev	informacije za uparivanje	24	24	32	32	32
50	odgovor	informacije za uparivanje	24	24	32	32	32
70	zahtjev	podatci za autentifikaciju	8	8	16	16	16
80	odgovor	vrijednost brojača MoS + podatci za autentifikaciju	8	8	16	16	16

CSM_219 Informacije za uparivanje koje se šalju u uputama 43. (zahtjev VU) i 50. (odgovor MoS) prikupljaju se kako je navedeno u odjeljku 7.6.10. norme [ISO 16844-3], osim što se u shemi šifriranja podataka za uparivanje upotrebljava AES algoritam umjesto TDES algoritma, čime nastaju dva AES šifriranja te se popunjenje navedeno u CSM_220 primjenjuje za usklađivanje s veličinom AES bloka. Ključ K'_P koji se upotrebljava za to šifriranje generira se kako slijedi:

— u slučaju da je ključ uparivanja K_P duljine 16 bajtova: $K'_P = K_P \text{ XOR } (N_s||N_s)$,

— u slučaju da je ključ uparivanja K_P duljine 24 bajta: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s)$,

— u slučaju da je ključ uparivanja K_P duljine 32 bajta: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s||N_s)$,

pri čemu je N_s 8-bajtni serijski broj senzora kretanja.

CSM_220 U slučaju da duljina nešifriranih podataka (upotrebom AES ključeva) nije višekratnik 16 bajtova, upotrebljava se metoda popunjenja br. 2 iz norme [ISO 9797-1].

Napomena: u normi [ISO 16844-3] broj bajtova nešifriranih podataka uvijek je višekratnik broja 8 tako da popunjenje nije potrebno pri upotrebi TDES. Definicija podataka i poruka iz norme [ISO 16844-3] ne mijenja se ovim dijelom ovog Dodatka te je stoga potrebna primjena popunjenja.

CSM_221 Za uputu 11. i u slučaju da se mora šifrirati više od jednog bloka podataka, upotrebljava se način rada „ulančavanje šifriranih blokova" (CBC), kako je utvrđeno u normi [ISO 10116], s parametrom preraspodjele *m* = 1. Inicijalizacijski vektor upotrebljava se:

— za uputu 11.: 8-bajtni blok autentifikacije naveden u odjeljku 7.6.3.3. norme [ISO 16844-3], popunjen upotrebom metode popunjenja br. 2 iz norme [ISO 9797-1]; vidjeti i odjeljke 7.6.5. i 7.6.6. u normi [ISO 16844-3],

— za sve ostale upute u kojima se prenosi više od 16 bajtova, kako je navedeno u tablici 6.: '00' {16}, tj. šesnaest bajtova s binarnom vrijednošću 0.

Napomena: kako je prikazano u odjeljcima 7.6.5. i 7.6.6. norme [ISO 16844-3], kada MoS šifrira podatkovne datoteke za uključivanje u uputu 11. blok autentifikacije se:

— upotrebljava kao inicijalizacijski vektor za šifriranje podatkovnih datoteka u načinu rada CBC,

— šifrira i uključuje u prvi blok u podatcima koji se šalju u jedinicu u vozilu.

12.4. **Uparivanje jedinice u vozilu i senzora kretanja za različite generacije opreme**

CSM_222 Kako je objašnjeno u odjeljku 9.2.1., senzor kretanja druge generacije može sadržavati šifriranje podataka za uparivanje na temelju TDES (kako je utvrđeno u dijelu A ovog Dodatka), koje omogućuje da senzor kretanja bude uparen s jedinicom u vozilu prve generacije. U tom se slučaju jedinica u vozilu prve generacije i senzor kretanja druge generacije uparuju kako je opisano u dijelu A ovog Dodatka i u normi [ISO 16844-3]. Za postupak uparivanja može se upotrijebiti kartica radionice prve ili druge generacije.

Napomene:

— Nije moguće upariti jedinicu u vozilu druge generacije sa senzorom kretanja prve generacije.

— Nije moguće upotrijebiti karticu radionice prve generacije za povezivanje VU druge generacije sa senzorom kretanja.

13. SIGURNOST KOMUNIKACIJE NA DALJINU PUTEM DSRC-a

13.1. **Općenito**

Kako je navedeno u Dodatku 14., jedinica u vozilu redovito generira podatke za praćenje tahografa na daljinu (eng. *Remote Tachograph Monitoring*, RTM) i te podatke šalje (unutarnjem ili vanjskom) uređaju za komunikaciju na daljinu (eng. *Remote Communication Facility*, RCF). Uređaj za komunikaciju na daljinu odgovoran je za slanje tih podataka uređaju za ispitivanje na daljinu putem sučelja DSRC-a opisanog u Dodatku 14. U Dodatku 1. utvrđeno je da podatci RTM-a čine ulančavanje:

šifriranog prijenosa podataka iz tahografa (eng. *encrypted tachograph payload*) – šifriranje nešifriranog prijenosa podataka iz tahografa,

sigurnosnih podataka DSRC-a (eng. *DSRC security data*) – opisani u nastavku.

Format nešifriranog prijenosa podataka iz tahografa naveden je u Dodatku 1. te detaljnije opisan u Dodatku 14. U ovom se odjeljku opisuje struktura sigurnosnih podataka DSRC-a; službena je specifikacija navedena u Dodatku 1.

CSM_223 Nešifrirani podatci `tachographPayload` koje jedinica u vozilu (VU) dostavlja uređaju za komunikaciju na daljinu (ako je RCF vanjski u odnosu na VU) ili ih VU putem sučelja DSRC-a dostavlja uređaju za ispitivanje na daljinu (ako je RCF unutarnji u odnosu na VU) zaštićuju se u načinu rada namijenjenom šifriranju i zatim autentifikaciji, tj. podatci iz tahografa prvo se šifriraju u svrhu osiguranja povjerljivosti poruke te se nakon toga izračunava MAC u svrhu osiguranja autentičnosti i integriteta.

CSM_224 Sigurnosni podatci DSRC-a sastoje se od ulančavanja sljedećih podatkovnih elemenata sljedećim redoslijedom; vidjeti i sliku 12.:

trenutačni datum i vrijeme – trenutačni datum i vrijeme jedinice u vozilu (vrsta podataka `TimeReal`),

brojač – 3-bajtni brojač, vidjeti CSM_225,

serijski broj jedinice u vozilu – serijski broj jedinice u vozilu (vrsta podataka `VuSerialNumber`),

broj verzije glavnog ključa DSRC-a – 1-bajtni broj verzije glavnog ključa DSRC-a iz kojeg su izvedeni ključevi DSRC-a specifični za jedinicu u vozilu; vidjeti odjeljak 9.2.2.,

MAC – MAC izračunan za sve prethodne bajtove u podatcima RTM-a.

CSM_225 Trobajtni brojač u sigurnosnim podatcima DSRC-a je u formatu MSB-first. Kad jedinica u vozilu prvi put otkad je stavljena u upotrebu izračunava niz podataka RTM-a, postavlja vrijednost brojača na 0. Jedinica u vozilu povećava vrijednost podataka brojača za 1 svaki put prije nego što izračuna sljedeći niz podataka RTM-a.

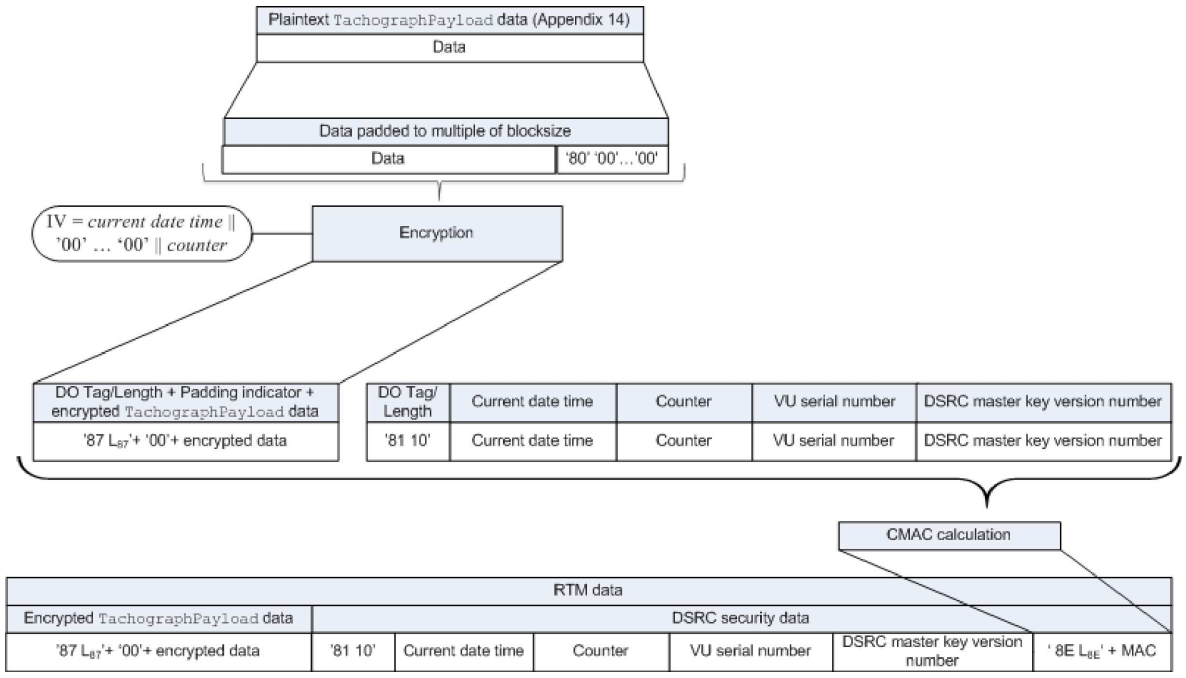
13.2. Šifriranje prijenosa podataka tahografa i generiranje MAC-a

CSM_226 S obzirom na nešifrirani podatkovni element s vrstom podataka `TachographPayload` , kako je opisan u Dodatku 14., jedinica u vozilu šifrira te podatke kako je prikazano na slici 12.: ključ DSRC-a jedinice u vozilu za šifriranje $K_VU_{DSRC}_ENC$ (vidjeti odjeljak 9.2.2.) upotrebljava se s AES-om u načinu rada „ulančavanje šifriranih blokova" (CBS), kako je utvrđeno u normi [ISO 10116], s parametrom preraspodjele $m = 1$. Inicijalizacijski vektor jednak je *IV = trenutačni datum i vrijeme*|| *'00 00 00 00 00 00 00 00'* || *brojač*, pri čemu su *trenutačni datum i vrijeme* i *brojač* navedeni u CSM_224. Podatci za šifriranje popunjavaju se metodom br. 2 iz norme [ISO 9797-1].

CSM_227 Jedinica u vozilu izračunava MAC u sigurnosnim podatcima DSRC-a kako je prikazano na slici 12.: MAC se izračunava za sve prethodne bajtove u RTM podatcima, do broja verzije glavnog ključa DSRC-a i uključujući taj broj te uključujući oznake i duljine podatkovnih objekata. Jedinica u vozilu upotrebljava svoj ključ DSRC-a za autentičnost $K_VU_{DSRC}_MAC$ (vidjeti odjeljak 9.2.2.) s AES algoritmom u načinu rada CMAC, kako je navedeno u [SP 800-38B]. Duljina MAC-a povezana je s duljinom ključeva DSRC-a specifičnih za jedinicu u vozilu, kako je navedeno u CSM_50.

Slika 12.

Šifriranje prijenosa podataka tahografa i generiranje MAC-a



13.3. **Provjera i dešifriranje prijenosa podataka tahografa**

CSM_228 Kada primi RTM podatke iz jedinice u vozilu, uređaj za daljinsko ispitivanje šalje sve RTM podatke na kontrolnu karticu u podatkovnom polju naredbe PROCESS DSRC MESSAGE, kako je opisano u Dodatku 2. Zatim:

1. kontrolna kartica pregledava broj verzije glavnog ključa DSRC-a u sigurnosnim podatcima DSRC-a. Ako ne prepoznaje navedeni glavni ključ DSRC-a, kontrolna kartica javlja pogrešku navedenu u Dodatku 2. i prekida postupak;

2. kontrolna kartica upotrebljava navedeni glavni ključ DSRC-a u kombinaciji sa serijskim brojem jedinice u vozilu u sigurnosnim podatcima DSRC-a za izvođenje ključeva DSRC-a specifičnih za jedinicu u vozilu K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC, kako je navedeno u CSM_124;

3. kontrolna kartica upotrebljava K_VU_{DSRC}_MAC za provjeru MAC-a u sigurnosnim podatcima DSRC-a, kako je navedeno u CSM_227. Ako je MAC netočan, kontrolna kartica javlja pogrešku navedenu u Dodatku 2. i prekida postupak;

4. kontrolna kartica upotrebljava K_VU_{DSRC}_ENC za dešifriranje šifriranog prijenosa podataka tahografa, kako je navedeno u CSM_226. Kontrolna kartica uklanja popunjenje i uređaju za daljinsko ispitivanje vraća dešifrirani prijenos podataka tahografa.

CSM_229 U svrhu sprječavanja napada reprodukcijom, uređaj za daljinsko ispitivanje provjerava aktualnost (eng. *freshness*) RTM podataka provjerom da *trenutačni datum i vrijeme* u sigurnosnim podatcima DSRC-a ne odstupa previše od trenutačnog vremena uređaja za daljinsko ispitivanje.

Napomene:

— To zahtijeva da uređaj za daljinsko ispitivanje ima točan i pouzdan izvor vremena.

— Budući da se u Dodatku 14. od jedinice u vozilu zahtijeva novi niz RTM podataka svakih 60 sekundi te je dopušteno da sat jedinice u vozilu odstupa jednu minutu od realnog vremena, donja granica za aktualnost RTM podataka je dvije minute. Stvarna aktualnost podataka koja se zahtijeva ovisi i o točnosti sata uređaja za daljinsko ispitivanje.

CSM_230 Nakon što provjeri pravilan rad funkcije DSRC-a jedinice u vozilu, radionica šalje sve RTM podatke primljene iz jedinice u vozilu na karticu radionice u podatkovnom polju naredbe PROCESS DSRC MESSAGE, kako je opisano u Dodatku 2. Kartica radionice obavlja sve provjere i radnje navedene u CSM_228.

14. POTPISIVANJE PREUZIMANJA PODATAKA I PROVJERA POTPISA

14.1. **Općenito**

CSM_231 Posebna namjenska oprema (IDE) pohranjuje podatke primljene s jedinice u vozilu ili kartice tijekom jednog procesa preuzimanja podataka u jednoj fizičkoj podatkovnoj datoteci. Podatci se mogu pohraniti na ESM (vanjski medij za pohranu podataka). Ta datoteka sadržava digitalne potpise podatkovnih blokova navedenih u Dodatku 7. Ta datoteka sadržava i sljedeće certifikate (vidjeti odjeljak 9.1.):

— u slučaju preuzimanja podataka iz jedinice u vozilu:

  — certifikat VU_Sign,

  — certifikat MSCA_VU-EGF s javnim ključem koji se upotrebljava za provjeru certifikata VU_Sign;

— u slučaju preuzimanja podataka s kartice:

— certifikat Card_Sign,

— certifikat MSCA_Card s javnim ključem koji se upotrebljava za provjeru certifikata Card_Sign.

CSM_232 IDE na raspolaganju ima i sljedeće:

— u slučaju da za provjeru potpisa upotrebljava kontrolnu karticu, kako je prikazano na slici 13.: certifikat o povezanosti koji povezuje najnoviji certifikat EUR s certifikatom EUR čiji mu rok valjanosti izravno prethodi, ako postoji,

— u slučaju da sam provjerava potpis: sve valjane europske glavne certifikate.

Napomena: metoda koju IDE upotrebljava za preuzimanje tih certifikata nije utvrđena u ovom Dodatku.

14.2. **Generiranje potpisa**

CSM_233 Algoritam potpisivanja za stvaranje digitalnih potpisa preuzetih podataka je ECDSA, kako je utvrđeno u [DSS], upotrebom algoritma raspršivanja (*hashing*) povezanog s veličinom ključa jedinice u vozilu ili kartice, kako je navedeno u CSM_50. Format potpisa je nešifriran, kako je navedeno u [TR-03111].

14.3. **Provjera potpisa**

CSM_234 IDE provjeru potpisa preuzetih podataka može provesti sam ili za to može upotrijebiti kontrolnu karticu. U slučaju da za provjeru potpisa upotrebljava kontrolnu karticu, provjera potpisa odvija se na način prikazan na slici 13. U slučaju da provjeru potpisa provodi sam, IDE provjerava autentičnost i valjanost svih certifikata u lancu certifikata u podatkovnoj datoteci te provjerava potpis podataka u skladu sa shemom potpisa utvrđenom u [DSS].

Napomene za sliku 13.:

— Oprema koja je potpisala podatke koji se analiziraju označena je s EQT.

— Certifikati EQT i javni ključevi prikazani na slici su oni za potpisivanje, tj. VU_Sign ili Card_Sign.

— Certifikati EQT.CA i javni ključevi prikazani na slici oni su za potpisivanje certifikata jedinice u vozilu ili kartice, kako je primjenjivo.

— Certifikat EQT.CA.EUR prikazan na slici je europski glavni certifikat koji je naveden u CAR certifikata EQT.CA.

— Certifikat EQT.Link prikazan na slici je certifikat o povezanosti EQT, ako postoji. Kako je navedeno u odjeljku 9.1.2., to je certifikat o povezanosti za novi europski glavni par ključeva koji je ERCA stvorila i potpisala prethodnim europskim privatnim ključem,

— Certifikat EQT.Link.EUR je europski glavni certifikat koji je naveden u CAR certifikata EQT. Link.

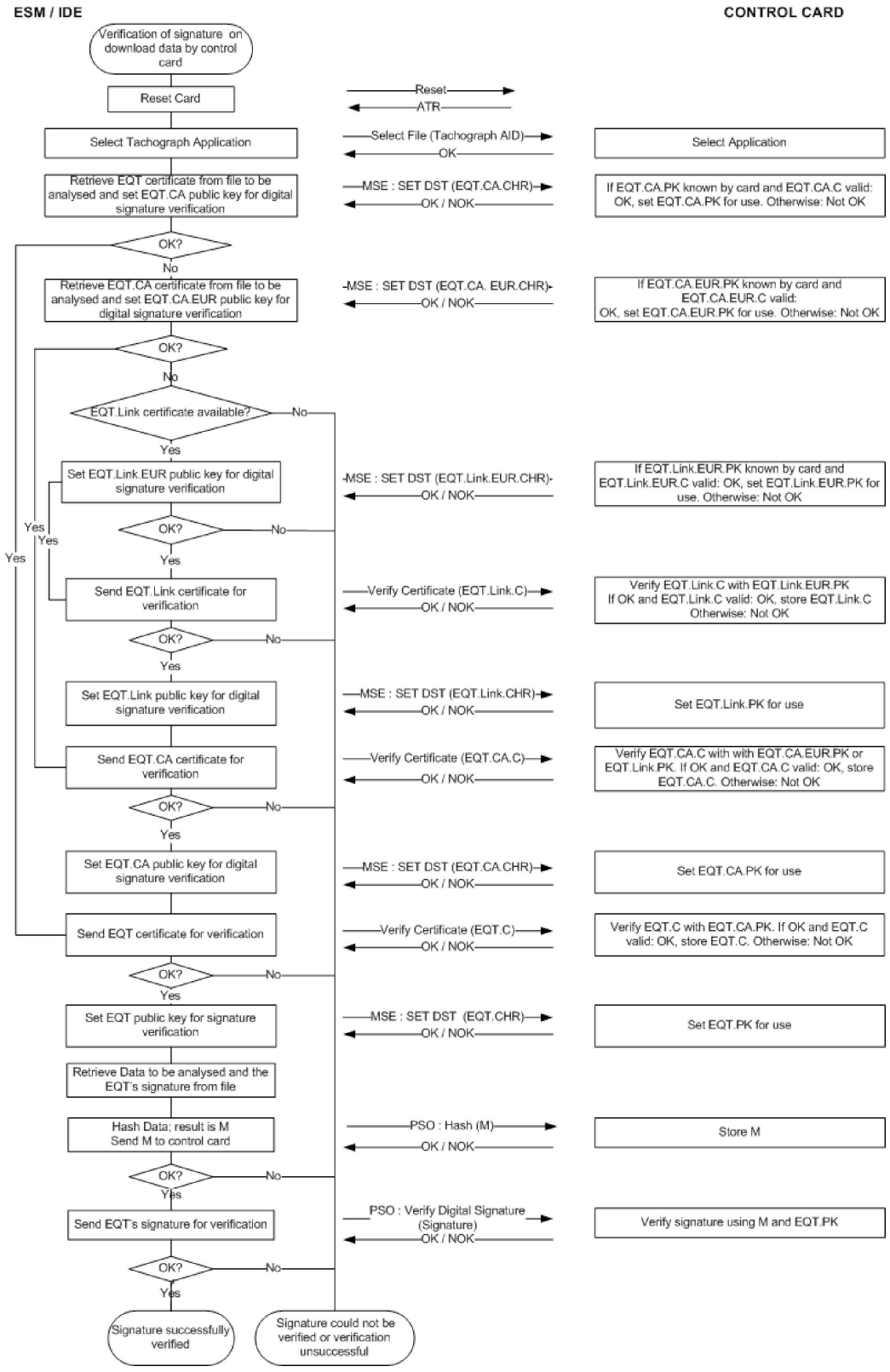
CSM_235 Za izračun raspršivanja (*hash*) M poslanog kontrolnoj kartici u naredbi PSO:Hash, IDE upotrebljava algoritam raspršivanja (*hashing*) povezan s veličinom ključa jedinice u vozilu ili kartice s koje se preuzimaju podatci, kako je navedeno u CSM_50.

CSM_236 Za provjeru potpisa EQT kontrolna kartica slijedi shemu potpisa utvrđenu u [DSS].

Napomena: ovim se dokumentom ne određuju bilo kakve mjere koje treba poduzeti ako se potpis preuzete podatkovne datoteke ne može provjeriti ili je provjera neuspješna.

Slika 13.

Protokol za provjeru potpisa preuzete podatkovne datoteke



Dodatak 12.

UTVRĐIVANJE POLOŽAJA NA TEMELJU GLOBALNOG SATELITSKOG NAVIGACIJSKOG SUSTAVA (GNSS)

SADRŽAJ

1. UVOD 405

1.1. Područje primjene 405

1.2. Pokrate i bilješke 405

2. SPECIFIKACIJE PRIJAMNIKA GNSS-A 406

3. NMEA REČENICE 406

4. JEDINICA U VOZILU S VANJSKIM UREĐAJEM GNSS-A 408

4.1. Konfiguracija 408

4.1.1 Glavni sastavni dijelovi i sučelja 408

4.1.2 Stanje vanjskog uređaja GNSS-a na kraju proizvodnog procesa 408

4.2. Komunikacija između vanjskog uređaja GNSS-a i jedinice u vozilu 409

4.2.1 Komunikacijski protokol 409

4.2.2 Zaštićeni prijenos podataka GNSS-a 411

4.2.3 Struktura naredbe Read Record 412

4.3. Spajanje, međusobna autentifikacija i dogovor o ključu za razmjenu podataka između vanjskog uređaja GNSS-a i jedinice u vozilu 413

4.4. Upravljanje greškama 413

4.4.1 Greška u komunikaciji s vanjskim uređajem GNSS-a 413

4.4.2 Proboj fizičkog integriteta vanjskog uređaja GNSS-a 413

4.4.3 Izostanak podataka o položaju iz prijamnika GNSS-a 413

4.4.4 Istekla je valjanost certifikata vanjskog uređaja GNSS-a 414

5. JEDINICA U VOZILU BEZ VANJSKOG UREĐAJA GNSS-A 414

5.1. Konfiguracija 414

5.2. Upravljanje greškama 414

5.2.1 Izostanak podataka o položaju iz prijamnika GNSS-a 414

6. VREMENSKI KONFLIKT GNSS-A 414

7. KONFLIKT U KRETANJU VOZILA 415

1. UVOD

U ovom su Dodatku navedeni tehnički zahtjevi za podatke GNSS-a koje upotrebljava jedinica u vozilu, uključujući protokole koji se moraju provoditi kako bi se osigurao zaštićen i točan podatkovni prijenos informacija za utvrđivanje položaja.

Glavni članci Uredbe (EZ) br. 165/2014 na kojima se temelje ti zahtjevi su: članak 8., Bilježenje položaja vozila na određenim mjestima tijekom dnevnog radnog vremena, članak 10., Povezanost s inteligentnim prijevoznim sustavima i članak 11., Detaljne odredbe za pametni tahograf.

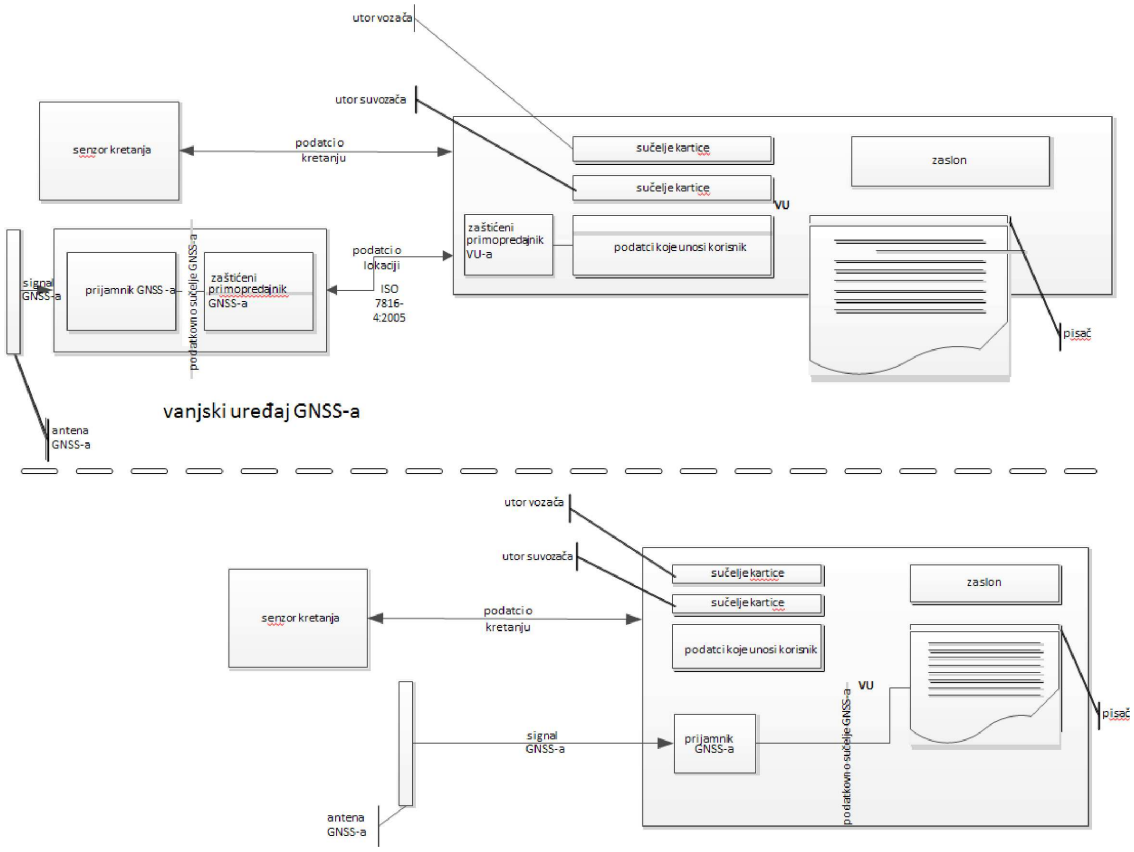
1.1. **Područje primjene**

GNS_1 Jedinica u vozilu prikuplja podatke o lokaciji iz barem jednog GNSS-a kako bi se pružila potpora provedbi članka 8.

Jedinica u vozilu može, ali ne mora, imati vanjski uređaj GNSS-a kako je prikazano na slici 1.:

Slika 1.

Različite konfiguracije prijamnika GNSS-a



1.2. **Pokrate i bilješke**

U ovom se Dodatku upotrebljavaju sljedeće pokrate:

DOP slabljenje preciznosti (eng. *Dilution of Precision*)

EGF elementarna datoteka uređaja GNSS-a (eng. *Elementary file GNSS Facility*)

EGNOS Europski geostacionarni navigacijski sustav (eng. *European Geostationary Navigation Overlay Service*)

GNSS globalni satelitski navigacijski sustav (eng. *Global Navigation Satellite System*)

GSA GPS DOP (slabljenje preciznosti GPS-a) i aktivni sateliti (eng. *GPS DOP and active satellites*)

HDOP horizontalno slabljenje preciznosti (eng. *Horizontal Dilution of Precision*)

ICD dokument upravljanja sučeljem (eng. *Interface Control Document*)

NMEA Nacionalno udruženje za pomorsku elektroniku (eng. *National Marine Electronics Association*)

PDOP slabljenje preciznosti položaja (eng. *Position Dilution of Precision*)

RMC preporučena minimalna određenost (eng. *Recommended Minimum Specific*)

SIS signal u svemiru (eng. *Signal in Space*)

VDOP vertikalno slabljenje preciznosti (eng. *Vertical Dilution of Precision*)

VU jedinica u vozilu (eng. *Vehicle Unit*)

2. SPECIFIKACIJE PRIJAMNIKA GNSS-A

Bez obzira na konfiguraciju pametnog tahografa s vanjskim uređajem GNSS-a ili bez njega, pružanje točnih i pouzdanih informacija za utvrđivanje položaja ključan je element učinkovitog rada pametnog tahografa. Stoga je primjereno zahtijevati njegovu kompatibilnost s uslugama koje pružaju programi Galileo i Europski geostacionarni navigacijski sustav (EGNOS), kako je navedeno u Uredbi (EU) br. 1285/2013 Europskog parlamenta i Vijeća ([1]). Sustav uveden u okviru programa Galileo nezavisni je globalni satelitski navigacijski sustav, dok je sustav uveden u okviru programa EGNOS regionalni satelitski navigacijski sustav kojim se poboljšava kvaliteta signala globalnog sustava za utvrđivanje položaja.

GNS_2 Proizvođači osiguravaju da su prijamnici GNSS-a u pametnim tahografima kompatibilni s uslugama utvrđivanja položaja koje pružaju sustavi Galileo i EGNOS. Proizvođači se također mogu odlučiti i na kompatibilnost s drugim satelitskim navigacijskim sustavima.

GNS_3 Prijamnik GNSS-a mora imati mogućnost autentifikacije za otvorenu uslugu programa Galileo ako takvu uslugu pruža sustav Galileo i ako je podržavaju proizvođači prijamnika GNSS-a. Međutim, za pametne tahografe koji su stavljeni na tržište prije ispunjenja gore navedenih zahtjeva i koji nemaju mogućnosti autentifikacije za otvorenu uslugu programa Galileo neće se zahtijevati nikakva prilagodba.

3. NMEA REČENICE

U ovom su odjeljku opisane NMEA rečenice koje se upotrebljavaju u radu pametnog tahografa. Ovaj se odjeljak primjenjuje na konfiguraciju pametnih tahografa s vanjskim uređajem GNSS-a ili bez njega.

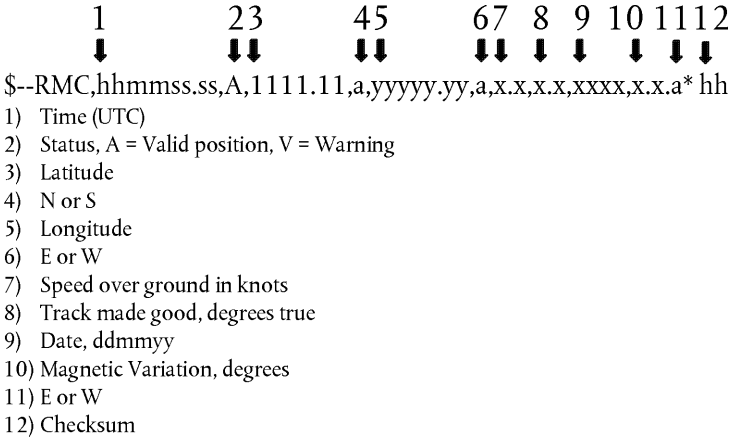
GNS_4 Podatci o lokaciji temelje se na NMEA rečenici *Recommended Minimum Specific* (RMC) *GNSS Data*, koja sadržava informacije o položaju (zemljopisna širina, zemljopisna dužina), vrijeme u UTC formatu (hhmmss.ss) te brzinu preko dna u čvorovima uz dodatne vrijednosti.

Format RMC rečenice glasi kako slijedi (prema normi NMEA V4.1):

([1]) Uredba (EU) br. 1285/2013 Europskog parlamenta i Vijeća od 11. prosinca 2013. o provedbi i uporabi europskih sustava za satelitsku navigaciju i stavljanju izvan snage Uredbe Vijeća (EZ) br. 876/2002 i Uredbe (EZ) br. 683/2008 Europskog parlamenta i Vijeća (SL L 347, 20.12.2013., str. 1.).

Slika 2.

Struktura RMC rečenice



Status označava je li signal GNSS-a dostupan. Sve dok se vrijednost statusa ne postavi na A, primljeni podatci (npr. o vremenu ili zemljopisnoj dužini/širini) ne mogu se upotrijebiti za bilježenje položaja vozila u jedinici u vozilu.

Razlučivost položaja temelji se na formatu prethodno opisane RMC rečenice. Prvi dijelovi polja 3) i 5) (prva dva broja) upotrebljavaju se za prikaz stupnjeva. Ostatak se upotrebljava za prikaz minuta s tri decimale. Stoga razlučivost iznosi 1/1 000 minute ili 1/60 000 stupnja (jer jedna minuta iznosi 1/60 stupnja).

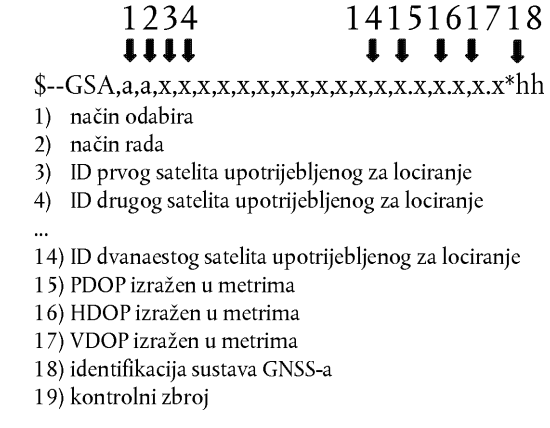
GNS_5 Jedinica u vozilu sprema u svojoj bazi podataka informacije o položaju za zemljopisnu dužinu i zemljopisnu širinu pri razlučivosti od 1/10 minute ili 1/600 stupnja, kako je opisano u Dodatku 1. za vrstu *GeoCoordinates*.

Jedinica u vozilu može upotrebljavati naredbu *GPS DOP and active satellites* (GSA) za određivanje i bilježenje dostupnosti i preciznosti signala. HDOP se posebno upotrebljava za ukazivanje na razinu preciznosti zabilježenih podataka o lokaciji (vidjeti točku 4.2.2.). Jedinica u vozilu spremit će vrijednost horizontalnog slabljenja preciznosti (HDOP) izračunanu kao minimum HDOP vrijednosti prikupljenih na raspoloživim sustavima GNSS-a.

Identifikacija sustava GNSS-a (*GNSS System Id*) označava sustave GPS, Glonass, Galileo, Beidou ili satelitski sustav proširivanja (*Satellite-Based Augmentation System*, SBAS).

Slika 3

Struktura GSA rečenice



Pri čemu način rada (*Mode*) (2) ukazuje da lociranje nije dostupno (Mode=1) ili da je lociranje dostupno za 2D (Mode=2) ili 3D (Mode=3).

GNS_6 *GSA* rečenica sprema se pod brojem zapisa '06'.

GNS_7 Maksimalna veličina NMEA rečenice (npr. RMC, GSA ili druge) koja se može upotrijebiti za određivanje veličine naredbe za čitanje zapisa iznosi 85 bajtova (vidjeti tablicu 1).

4. JEDINICA U VOZILU S VANJSKIM UREĐAJEM GNSS-A

4.1. **Konfiguracija**

4.1.1 *Glavni sastavni dijelovi i sučelja*

U ovoj je konfiguraciji prijamnik GNSS-a sastavni dio vanjskog uređaja GNSS-a.

GNS_8 Vanjski uređaj GNSS-a mora se napajati putem specifičnog sučelja vozila.

GNS_9 Vanjski uređaj GNSS-a sastoji se od sljedećih sastavnih dijelova (vidjeti sliku 4.):

a) komercijalnog prijamnika GNSS-a koji pruža podatke o položaju putem podatkovnog sučelja GNSS-a. Primjerice, podatkovno sučelje GNSS-a može upotrebljavati normu NMEA V4.10 pri čemu prijamnik GNSS-a služi kao odašiljač i prenosi NMEA rečenice zaštićenom primopredajniku GNSS-a pri frekvenciji od 1 Hz za predefinirani niz NMEA rečenica, koji mora sadržavati barem RMC i GSA rečenice. Proizvođači vanjskog uređaja GNSS-a odabiru način provedbe podatkovnog sučelja GNSS-a;

b) primopredajne jedinice (zaštićenog primopredajnika GNSS-a) koja može podržati standard ISO/IEC 7816-4:2013 (vidjeti 4.2.1) za komunikaciju s jedinicom u vozilu te podržati podatkovno sučelje GNSS-a do prijamnika GNSS-a. Jedinica je opremljena memorijom za spremanje identifikacijskih podataka prijamnika GNSS-a i vanjskog uređaja GNSS-a;

c) kućišta s funkcijom otkrivanja neovlaštenog rukovanja u kojem se nalaze prijamnik GNSS-a i zaštićeni primopredajnik GNSS-a. Funkcijom otkrivanja neovlaštenog rukovanja provode se sigurnosne mjere zaštite navedene u profilu zaštite pametnih tahografa;

d) antene GNSS-a ugrađene na vozilo i spojene na prijamnik GNSS-a kroz kućište.

GNS_10 Vanjski uređaj GNSS-a sadržava barem sljedeća vanjska sučelja:

a) sučelje prema anteni GNSS-a ugrađenoj na vozilo, ako se upotrebljava vanjska antena;

b) sučelje prema jedinici u vozilu.

GNS_11 U jedinici u vozilu zaštićeni primopredajnik jedinice u vozilu predstavlja drugi kraj zaštićene komunikacije sa zaštićenim primopredajnikom GNSS-a te mora podržavati normu ISO/IEC 7816-4:2013 za spajanje s vanjskim uređajem GNSS-a.

GNS_12 Za fizički dio komunikacije s vanjskim uređajem GNSS-a jedinica u vozilu podržava normu ISO/IEC 7816-12:2005 ili neku drugu normu koja može podržavati normu ISO/IEC 7816-4:2013. (vidjeti odjeljak 4.2.1).

4.1.2 *Stanje vanjskog uređaja GNSS-a na kraju proizvodnog procesa*

GNS_13 Vanjski uređaj GNSS-a pri izlasku iz tvornice sprema sljedeće vrijednosti u neizbrisivu memoriju zaštićenog primopredajnika GNSS-a:

— par ključeva EGF_MA i odgovarajući certifikat;

— certifikat MSCA_VU-EGF koji sadržava javni ključ MSCA_VU-EGF.PK koji se upotrebljava za provjeravanje certifikata EGF_MA;

— EUR certifikat koji sadržava javni ključ EUR.PK koji se upotrebljava za provjeravanje certifikata MSCA_VU-EGF;

— EUR certifikat čije razdoblje valjanosti izravno prethodi razdoblju valjanosti EUR certifikata koji se upotrebljava za provjeravanje certifikata MSCA_VU-EGF, ako postoji;

— certifikat o povezanosti koji povezuje ta dva EUR certifikata, ako postoji;

— prošireni serijski broj vanjskog uređaja GNSS-a;

— identifikator operativnog sustava uređaja GNSS-a;

— homologacijski broj vanjskog uređaja GNSS-a;

— identifikator sigurnosne komponente vanjskog uređaja GNSS-a.

4.2. **Komunikacija između vanjskog uređaja GNSS-a i jedinice u vozilu**

4.2.1 *Komunikacijski protokol*

GNS_14 Komunikacijski protokol između vanjskog uređaja GNSS-a i jedinice u vozilu podržava tri funkcije:

1. prikupljanje i distribuciju podataka GNSS-a (npr. položaj, vrijeme, brzinu);
2. prikupljanje konfiguracijskih podataka vanjskog uređaja GNSS-a;
3. upravljački protokol za podršku spajanju, međusobnoj autentifikaciji i dogovoru o ključu za razmjenu podataka između vanjskog uređaja GNSS-a i jedinice u vozilu.

GNS_15 Komunikacijski protokol temelji se na normi ISO/IEC 7816 4:2013, pri čemu zaštićeni primopredajnik jedinice u vozilu ima nadređenu, a zaštićeni primopredajnik GNSS-a podređenu ulogu. Fizička veza između vanjskog uređaja GNSS-a i jedinice u vozilu temelji se na normi ISO/IEC 7816-12:2005 ili nekoj drugoj normi koja može podržavati zahtjeve norme ISO/IEC 7816-4:2013.

GNS_16 Polja proširene dužine ne moraju biti podržana u komunikacijskom protokolu.

GNS_17 Komunikacijski protokol norme ISO 7816 (*-4:2013 i *-12:2005) između vanjskog uređaja GNSS-a i jedinice u vozilu ima vrijednost T=1.

GNS_18 S obzirom na funkcije 1) prikupljanja i distribucije podataka GNSS-a, 2) prikupljanja konfiguracijskih podataka vanjskog uređaja GNSS-a i 3) upravljačkog protokola, zaštićeni primopredajnik GNSS-a simulira pametnu karticu čija se arhitektura sustava datoteka sastoji od glavne datoteke (eng. *Master File*, MF), datoteke popisa (eng. *Directory File*, DF) s identifikatorom aplikacije određenim u poglavlju 6.2. Dodatka 1. ('FF 44 54 45 47 4D'), tri elementarne datoteke (eng. *Elementary File*, EF) koje sadržavaju certifikate i jedne elementarne datoteke (EF.EGF) s identifikatorom datoteke koji odgovara vrijednosti '2F2F' kako je opisano u tablici 1.

GNS_19 Zaštićeni primopredajnik GNSS-a sprema podatke iz prijamnika GNSS-a i konfiguraciju u datoteku EF. EGF. To je linearna datoteka zapisa promjenjive dužine čiji identifikator odgovara vrijednosti '2F2F' u heksadecimalnom formatu.

GNS_20 Zaštićeni primopredajnik GNSS-a upotrebljava memoriju za spremanje podataka i može izvršiti najmanje 20 milijuna ciklusa čitanja/pisanja. Osim ovoga, interno projektiranje i implementacija zaštićenog primopredajnika GNSS-a prepušta se proizvođačima na izbor.

Mapiranje brojeva i podataka zapisa prikazano je u tablici 1. Napominjemo da postoje četiri GSA rečenice za četiri satelitska sustava i satelitski sustav proširivanja (SBAS).

GNS_21 Struktura datoteka navedena je u tablici 1. Za uvjete pristupa (ALW, NEV, SM-MAC) vidjeti poglavlje 3.5. Dodatka 2.

Tablica 1.

Struktura datoteke

		Uvjeti pristupa		
Datoteka	Identifikacija datoteke	Čitanje	Ažuriranje	Šifrirano
MF	3F00			
EF.ICC	0002	ALW	NEV (provodi ga jedinica u vozilu)	Ne
DF uređaja GNSS-a	0501	ALW	NEV	Ne
EF EGF_MACertificate	C100	ALW	NEV	Ne
EF CA_Certificate	C108	ALW	NEV	Ne
EF Link_Certificate	C109	ALW	NEV	Ne
EF.EGF	2F2F	SM-MAC	NEV (provodi ga jedinica u vozilu)	Ne

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima)		Zadane vrijednosti
		min.	maks.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF uređaja GNSS-a		*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				
RMC NMEA rečenica	‘01’	85	85	
prva GSA NMEA rečenica	‘02’	85	85	
druga GSA NMEA rečenica	‘03’	85	85	

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima)		Zadane vrijednosti
		min.	maks.	
treća GSA NMEA rečenica	'04'	85	85	
četvrta GSA NMEA rečenica	'05'	85	85	
peta GSA NMEA rečenica	'06'	85	85	
proširenisi serijski broj vanjskog uređaja GNSS-a definiran u Dodatku 1. kao SensorGNSSSerialNumber.	'07'	8	8	
identifikator operativnog sustava GNSS-a zaštićeni primopredajnik definiran u Dodatku 1. kao SensorOSIdentifier.	'08'	2	2	
homologacijski broj vanjskog uređaja GNSS-a definiran u Dodatku 1. kao SensorExternalGNSSApprovalNumber.	'09'	16	16	
identifikator sigurnosne komponente vanjskog uređaja GNSS-a definiran u Dodatku 1. kao SensorExternalGNSSSCIdentifier	'10'	8	8	
RFU – rezervirano za buduću upotrebu	Od '11' do 'FD'			

4.2.2 *Zaštićeni prijenos podataka GNSS-a*

GNS_22 Zaštićeni prijenos podataka o položaju GNSS-a dopušta se samo u sljedećim okolnostima:

1. proces spajanja izvršen je kako je opisano u Dodatku 11., Zajednički sigurnosni mehanizmi;

2. povremena međusobna autentifikacija i dogovor o ključu za razmjenu podataka između jedinice u vozilu i vanjskog uređaja GNSS-a, isto tako opisani u Dodatku 11., Zajednički sigurnosni mehanizmi, izvršeni su prema naznačenoj učestalosti.

GNS_23 Svakih T sekundi, pri čemu je T vrijednost niža od 10 ili jednaka 10, osim ako dođe do spajanja ili međusobne autentifikacije i dogovora o ključu za razmjenu podataka, jedinica u vozilu traži od vanjskog uređaja GNSS-a informacije o položaju na temelju sljedećeg toka:

1. Jedinica u vozilu traži podatke o lokaciji od vanjskog uređaja GNSS-a zajedno s podatcima o slabljenju preciznosti (iz GSA NMEA rečenice). Zaštićeni primopredajnik jedinice u vozilu upotrebljava normu ISO/IEC 7816-4:2013, naredbu *SELECT and READ RECORD(S)* u sigurnom prijenosu poruka u načinu rada namijenjenom isključivo autentifikaciji, kako je opisano u odjeljku 11.5. Dodatka 11., s identifikatorom datoteke '2F2F' te RECORD brojem koji ima vrijednost '01' za RMC NMEA rečenice te vrijednosti '02', '03', '04', '05', '06' za GSA NMEA rečenice.

2. Zadnji zaprimljeni podatci o lokaciji spremaju se u EF-u s identifikatorom '2F2F' i zapisima opisanima u tablici 1. u zaštićeni primopredajnik GNSS-a kada zaštićeni primopredajnik GNSS-a zaprimi NMEA podatke pri frekvenciji od najmanje 1 Hz od prijamnika GNSS-a putem podatkovnog sučelja GNSS-a.

3. Zaštićeni primopredajnik GNSS-a šalje odgovor zaštićenom primopredajniku jedinice u vozilu koristeći se APDU odgovorom u sigurnom prijenosu poruka u načinu rada namijenjenom isključivo autentifikaciji, kako je opisano u odjeljku 11.5. Dodatka 11.

4. Zaštićeni primopredajnik jedinice u vozilu provjerava autentičnost i integritet primljenog odgovora. U slučaju pozitivnog rezultata podatci o lokaciji šalju se u procesor jedinice u vozilu putem podatkovnog sučelja GNSS-a.

5. Procesor jedinice u vozilu provjerava primljene podatke, dobivajući podatke (npr. zemljopisna širina, zemljopisna dužina, vrijeme) iz RMC NMEA rečenice. RMC NMEA rečenica uključuje informacije o valjanosti položaja. Ako položaj nije valjan, podatci o lokaciji još nisu dostupni i ne mogu se upotrijebiti za bilježenje položaja vozila. Ako je položaj valjan, procesor jedinice u vozilu isto tako dobiva HDOP vrijednosti iz GSA NMEA rečenica i računa prosječnu vrijednost na dostupnom satelitskom sustavu (to jest, kada je lociranje dostupno).

6. Procesor jedinice u vozilu sprema primljene i obrađene informacije, poput zemljopisne širine, zemljopisne dužine, vremena i brzine, u jedinici u vozilu u formatu definiranom u Dodatku 1., Rječnik s podatcima, kao *GeoCoordinates* zajedno s HDOP vrijednošću izračunanom kao minimum HDOP vrijednosti prikupljenih na dostupnim sustavima GNSS-a.

4.2.3 *Struktura naredbe Read Record*

U ovom odjeljku detaljno je opisana struktura naredbe *Read Record* (čitanje zapisa). Sigurni prijenos poruka (u načinu rada namijenjenom isključivo autentifikaciji) dodaje se kako je opisano u Dodatku 11., Zajednički sigurnosni mehanizmi.

GNS_24 Naredba podržava sigurni prijenos poruka u načinu rada namijenjenom isključivo autentifikaciji; vidjeti Dodatak 11.

GNS_25 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	'0Ch'	Zahtjev za sigurni prijenos poruka.
INS	1	'B2h'	Čitanje zapisa
P1	1	'XXh'	Broj zapisa ('00' označava da se radi o trenutnom zapisu)
P2	1	'04h'	Čitanje zapisa čiji je broj zapisa naveden u P1
Le	1	'XXh'	Očekivana duljina podataka. Broj bajtova koji se očitava.

GNS_26 Zapis naveden u P1 postaje trenutačni zapis.

Bajt	Duljina	Vrijednost	Opis
#1-#X	X	'XX..XXh'	Očitani podatci
SW	2	'XXXXh'	Statusne riječi (SW1,SW2)

— Ako je naredba uspješna, zaštićeni primopredajnik GNSS-a uzvraća '**9000**'.

— Ako trenutačna datoteka nije postavljena za zapis, zaštićeni primopredajnik GNSS-a uzvraća '**6981**'.

— Ako se naredba koristi s P1 = '00', no ne postoji trenutni EF, zaštićeni primopredajnik GNSS-a uzvraća '**6986**' (naredba nije dozvoljena).

— Ako zapis nije pronađen, zaštićeni primopredajnik GNSS-a uzvraća '**6A 83**'.

— Ako je vanjski uređaj GNSS-a otkrio neovlašteno rukovanje, uzvraća statusne riječi '**66 90**'.

GNS_27 Zaštićeni primopredajnik GNSS-a podržava sljedeće naredbe druge generacije tahografa, navedene u Dodatku 2.:

Naredba	Upućivanje
Select	poglavlje 3.5.1. Dodatka 2.
Read Binary	poglavlje 3.5.2. Dodatka 2.
Get Challenge	poglavlje 3.5.4. Dodatka 2.
PSO: Verify Certificate	poglavlje 3.5.7. Dodatka 2.
External Authenticate	poglavlje 3.5.9. Dodatka 2.
General Authenticate	poglavlje 3.5.10. Dodatka 2.
MSE:SET	poglavlje 3.5.11. Dodatka 2.

4.3. **Spajanje, međusobna autentifikacija i dogovor o ključu za razmjenu podataka između vanjskog uređaja GNSS-a i jedinice u vozilu**

Spajanje, međusobna autentifikacija i dogovor o ključu za razmjenu podataka između vanjskog uređaja GNSS-a i jedinice u vozilu opisani su u poglavlju 11. Dodatka 11., Zajednički sigurnosni mehanizmi.

4.4. **Upravljanje greškama**

U ovom odjeljku opisano je kako se moguća stanja greške vanjskog uređaja GNSS-a obrađuju i zapisuju u jedinici u vozilu.

4.4.1 *Greška u komunikaciji s vanjskim uređajem GNSS-a*

GNS_28 Ako jedinica u vozilu ne može uspostaviti komunikaciju sa spojenim vanjskim uređajem GNSS-a dulje od 20 uzastopnih minuta, jedinica u vozilu generira i bilježi u jedinici u vozilu događaj vrste EventFaultType koji ima vrijednost enumerirane vrste '53'H *External GNSS communication fault* te oznaku vremena koja navodi vrijeme u tom trenutku. Događaj će se generiratisamo ako su ispunjena sljedeća dva uvjeta: a) pametni tahograf nije u načinu rada za kalibraciju i b) vozilo se kreće. U ovom kontekstu, greška u komunikaciji nastaje kada zaštićeni primopredajnik jedinice u vozilu ne primi odgovor nakon zahtjeva, kako je opisano u 4.2.

4.4.2 *Proboj fizičkog integriteta vanjskog uređaja GNSS-a*

GNS_29 Ako je došlo do proboja vanjskog uređaja GNSS-a, zaštićeni primopredajnik GNSS-a briše cijelu svoju memoriju, uključujući kriptografski materijal. Kako je opisano u GNS_25 i GNS_26, jedinica u vozilu otkriva neovlašteno rukovanje ako odgovor ima status '6690'. Jedinica u vozilu tada generira događaj vrste EventFaultType, enumerirane vrste *'55'H Tamper detection of GNSS* (otkriveno neovlašteno rukovanje GNSS-om).

4.4.3 *Izostanak podataka o položaju iz prijamnika GNSS-a*

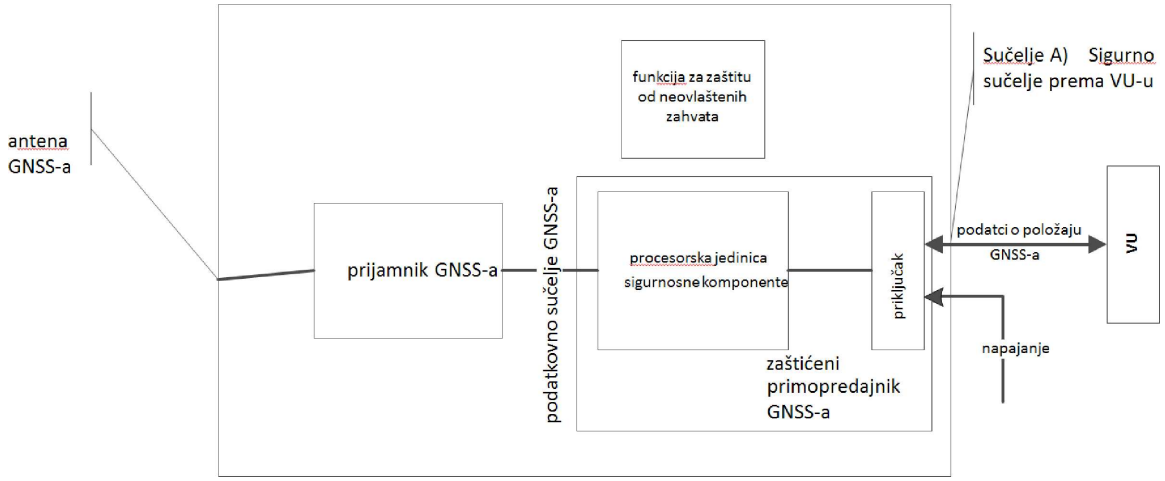
GNS_30 Ako zaštićeni primopredajnik GNSS-a ne zaprimi podatke od prijamnika GNSS-a dulje od tri uzastopna sata, zaštićeni primopredajnik GNSS-a generira odgovor na naredbu READ RECORD s RECORD brojem koji ima vrijednost '01', s podatkovnim poljem (eng. *Data Field*) od 12 bajtova od kojih svi imaju vrijednost '0xFF'. Po zaprimanju odgovora čije podatkovno polje ima tu vrijednost, jedinica u vozilu generira i bilježi događaj vrste EventFaultType, enumerirane vrste '52'H *external GNSS receiver fault* (kvar prijamnika vanjskog uređaja GNSS-a) s oznakom vremena koja navodi vrijeme u tom trenutku, pod uvjetom da su ispunjena sljedeća dva uvjeta: a) pametni tahograf nije u načinu rada za kalibraciju i b) vozilo se kreće.

4.4.4 *Istekla je valjanost certifikata vanjskog uređaja GNSS-a*

GNS_31 Ako jedinica u vozilu otkrije da EGF certifikat koji se upotrebljava za međusobnu autentifikaciju više nije valjan, jedinica u vozilu generira i bilježi grešku uređaja za bilježenje podataka vrste EventFaultType, enumerirane vrste *'56'H External GNSS facility certificate expired* (istekla je valjanost certifikata vanjskog uređaja GNSS-a) s oznakom vremena koja navodi vrijeme u tom trenutku. Jedinica u vozilu i dalje upotrebljava zaprimljene podatke o položaju GNSS-a.

Slika 4

Nacrt vanjskog uređaja GNSS-a



5. JEDINICA U VOZILU BEZ VANJSKOG UREĐAJA GNSS-A

5.1. **Konfiguracija**

U ovoj se konfiguraciji prijamnik GNSS-a nalazi unutar jedinice u vozilu kako je opisano na slici 1.

GNS_32 Prijamnik GNSS-a ima ulogu odašiljača i prenosi NMEA rečenice procesoru jedinice u vozilu, koji ima ulogu prijamnika s frekvencijom od 1/10 Hz ili bržom za predefinirani niz NMEA rečenica, koje uključuju barem RMC i GSA rečenice.

GNS_33 Na jedinicu u vozilu spaja se vanjska antena GNSS-a ugrađena na vozilo ili interna antena GNSS-a.

5.2. **Upravljanje greškama**

5.2.1 *Izostanak podataka o položaju iz prijamnika GNSS-a*

GNS_34 Ako jedinica u vozilu ne primi podatke iz prijamnika GNSS-a dulje od 3 uzastopna sata, jedinica u vozilu generira i bilježi događaj vrste EventFaultType, enumerirane vrste '51'H *Internal GNSS receiver fault* (kvar unutarnjeg prijamnika GNSS-a) s oznakom vremena koja navodi vrijeme u tom trenutku, pod uvjetom da su ispunjena sljedeća dva kriterija: a) pametni tahograf nije u načinu rada za kalibraciju i b) vozilo se kreće.

6. VREMENSKI KONFLIKT GNSS-A

Ako jedinica u vozilu otkrije nepodudarnost dulju od 1 minute između vremena koje je izmjerila funkcija mjerenja vremena jedinice u vozilu i vremena koje je izmjerio prijamnik GNSS-a, jedinica u vozilu zabilježit će događaj vrste EventFaultType, enumerirane vrste *'0B'H Time conflict (GNSS versus VU internal clock)* (vremenski konflikt između GNSS-a i unutarnjeg sata jedinice u vozilu). Taj se događaj bilježi zajedno sa stanjem unutarnjeg sata jedinice u vozilu i izražava zajedno s automatskom prilagodbom vremena. Nakon što se aktivira vremenski konflikt, jedinica u vozilu neće provjeravati nepodudarnost vremena sljedećih 12 sati. Taj se događaj neće aktivirati ako prijamnik GNSS-a nije mogao otkriti valjani signal GNSS-a u posljednjih 30 dana. Međutim, kad podatci o položaju iz prijamnika GNSS-a ponovno postanu dostupni, provodi se automatska prilagodba vremena.

7. KONFLIKT U KRETANJU VOZILA

GNS_35 Jedinica u vozilu pokreće i bilježi događaj konflikta u kretanju vozila (vidjeti zahtjev 84 u Prilogu I.C) s oznakom vremena koja odgovara trenutačnom vremenu, u slučaju da su informacije o kretanju izračunane s pomoću senzora kretanja proturječne informacijama o kretanju dobivenima iz unutarnjeg prijamnika GNSS-a ili iz vanjskog uređaja GNSS-a. U svrhu otkrivanja takvih proturječnosti upotrebljava se srednja vrijednost razlika u brzini između tih izvora, kako je navedeno u nastavku:

— najviše svakih deset sekundi izračunava se apsolutna vrijednost razlike između brzine vozila koju je procijenio GNSS i one koju je procijenio senzor kretanja,

— sve se vrijednosti izračunane u razdoblju koje se odnosi na posljednjih pet minuta kretanja upotrebljavaju za izračunavanje srednje vrijednosti,

— srednja se vrijednost izračunava kao prosjek od 80 % preostalih vrijednosti, nakon eliminiranja onih najviših u apsolutnim vrijednostima.

Događaj konflikta u kretanju vozila nastaje ako je srednja vrijednost viša od 10 km/h tijekom pet neprekidnih minuta kretanja vozila. Mogu se upotrebljavati i drugi neovisni izvori otkrivanja kretanja vozila kako bi se omogućilo pouzdanije otkrivanje manipuliranja tahografom. (Napomena: upotreba srednje vrijednosti posljednjih pet minuta primjenjuje se radi ublažavanja rizika od netipičnih vrijednosti mjerenja i prijelaznih vrijednosti). Ovaj se događaj neće aktivirati u sljedećim uvjetima: a) tijekom vožnje trajektom/vlakom, b) kada podatci o položaju iz prijamnika GNSS-a nisu raspoloživi i c) kada je u načinu rada za kalibraciju.

Dodatak 13

ITS SUČELJE

SADRŽAJ

1. UVOD 416

2. PODRUČJE PRIMJENE 416

2.1. Pokrate, definicije i zapisi 417

3. UPUĆIVANJA NA UREDBE I NORME 418

4. NAČELA RADA SUČELJA 418

4.1. Preduvjeti za prijenos podataka ITS sučeljem 418

4.1.1 Podatci dostupni preko ITS sučelja 418

4.1.2 Sadržaj podataka 418

4.1.3 ITS aplikacije 418

4.2. Komunikacijska tehnologija 419

4.3. Autorizacija PIN-om 419

4.4. Format poruke 421

4.5. Suglasnost vozača 425

4.6. Učitavanje standardnih podataka 426

4.7. Učitavanje osobnih podataka 426

4.8. Učitavanje podataka o događajima i kvarovima 426

1. UVOD

U ovom se Dodatku utvrđuju izvedba i postupci koje treba slijediti za provedbu sučelja s inteligentnim prijevoznim sustavima (ITS) u skladu sa zahtjevima iz članka 10. Uredbe (EU) br. 165/2014 (u daljnjem tekstu: Uredba).

Uredbom se utvrđuje da tahografi vozila mogu biti opremljeni standardiziranim sučeljima putem kojih podatke koje je tahograf zabilježio ili generirao može upotrebljavati vanjski uređaj u operativnom načinu rada ako su ispunjeni sljedeći uvjeti:

(a) sučelje ne utječe na ispravnost i integritet podataka koje je zabilježio tahograf;

(b) sučelje je usklađeno s detaljnim odredbama iz članka 11. Uredbe;

(c) vanjski uređaj povezan sa sučeljem ima pristup osobnim podatcima, uključujući podatke o zemljopisnom položaju, samo nakon prethodnog odobrenja vozača na kojeg se podatci odnose.

2. PODRUČJE PRIMJENE

U okviru područja primjene ovog Dodatka utvrđuje se kako aplikacije na vanjskim uređajima preko Bluetooth® veze dobivaju podatke (u daljnjem tekstu: podatci) iz tahografa.

Podatci dostupni preko tog sučelja opisani su u Prilogu 1. ovom dokumentu. Sučelje ne zabranjuje provedbu drugih sučelja (npr. preko CAN sabirnice) za prijenos podataka iz jedinice u vozilu u druge procesorske jedinice u vozilu.

U ovom se Dodatku utvrđuju:

— podatci dostupni preko ITS sučelja,

— Bluetooth® profil koji se upotrebljava za prijenos podataka,

— postupci povezani s upitima i preuzimanjem podataka te slijed operacija,

— mehanizam uparivanja tahografa i vanjskog uređaja,

— mehanizam za davanje suglasnosti koji je dostupan vozaču.

Radi pojašnjenja, u ovom se Prilogu ne utvrđuju:

— prikupljanje podataka i upravljanje prikupljanjem podataka unutar jedinice u vozilu (oni se utvrđuju drugdje u Uredbi ili su funkcija izvedbe proizvoda),

— oblik prikaza prikupljenih podataka u aplikaciji na vanjskom uređaju,

— odredbe o sigurnosti podataka izvan onoga što osigurava Bluetooth® (kao što je šifriranje) u vezi sa sadržajem podataka (one će biti utvrđene drugdje u Uredbi [Dodatak 10. „Zajednički sigurnosni mehanizmi"]),

— Bluetooth® protokoli koje primjenjuje ITS sučelje.

2.1. **Pokrate, definicije i zapisi**

U ovom se Dodatku upotrebljavaju sljedeće pokrate i definicije specifične za ovaj Dodatak:

komunikacija razmjena informacija/podataka između glavne jedinice (tj. tahografa) i vanjske jedinice preko ITS sučelja primjenom Bluetootha®.

podatci skupovi podataka kako je utvrđeno u Prilogu 1.

Uredba Uredba (EU) br. 165/2014 Europskog parlamenta i Vijeća od 4. veljače 2014. o tahografima u cestovnom prometu, stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u cestovnom prometu i izmjeni Uredbe (EZ) br. 561/2006 Europskog parlamenta i Vijeća o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na cestovni promet.

BR osnovna brzina (eng. *Basic Rate*)

EDR povećana brzina prijenosa podataka (eng. *Enhanced Data Rate*)

GNSS globalni satelitski navigacijski sustav (eng. *Global Navigation Satellite System*)

IRK ključ za utvrđivanje identiteta (eng. *Identity Resolution Key*)

ITS inteligentni prijevozni sustav (eng. *Intelligent Transport System*)

LE niska energija (eng. *Low Energy*)

PIN osobni identifikacijski broj (eng. *Personal Identification Number*)

PUC osobna šifra za deblokadu (eng. *Personal Unblocking Code*)

SID identifikator usluge (eng. *Service Identifier*)

SPP profil serijskog ulaza (eng. *Serial Port Profile*)

SSP sigurno jednostavno uparivanje (eng. *Secure Simple Pairing*)

TRTP parametar zahtjeva za prijenos (eng. *Transfer Request Parameter*)

TREP parametar odgovora na prijenos (eng. *Transfer Response Parameter*)

VU jedinica u vozilu (eng. *Vehicle Unit*)

3. UPUĆIVANJA NA UREDBE I NORME

Specifikacija utvrđena u ovom Dodatku odnosi se na sve sljedeće uredbe i norme ili njihove dijelove te o njima ovisi. U klauzulama ovog Dodatka navedene su relevantne norme ili njihove relevantne klauzule. U slučaju bilo kakve proturječnosti, prednost imaju klauzule ovog Dodatka.

U ovom se Dodatku upućuje na sljedeće uredbe i norme:

— Uredbu (EU) br. 165/2014 Europskog parlamenta i Vijeća od 4. veljače 2014. o tahografima u cestovnom prometu, stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u cestovnom prometu i izmjeni Uredbe (EZ) br. 561/2006 Europskog parlamenta i Vijeća o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na cestovni promet,

— Uredbu (EZ) br. 561/2006 Europskog parlamenta i Vijeća od 15. ožujka 2006. o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na cestovni promet i o izmjeni uredbi Vijeća (EEZ) br. 3821/85 i (EZ) br. 2135/98 te o stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3820/85,

— ISO 16844 – 4: *Road vehicles – Tachograph systems – Part 4: Can interface*,

— ISO 16844 – 7: *Road vehicles – Tachograph systems – Part 7: Parameters*,

— Bluetooth® – Serial Port Profile – V1.2,

— *Bluetooth® – Core Version 4.2*,

— protokol NMEA 0183 V4.1.

4. NAČELA RADA SUČELJA

4.1. **Preduvjeti za prijenos podataka ITS sučeljem**

Jedinica u vozilu odgovorna je za ažuriranje i održavanje podataka koji se pohranjuju na jedinici u vozilu bez uključivanja ITS sučelja. To se postiže na način svojstven jedinici u vozilu koji nije utvrđen u ovom Dodatku, već drugdje u Uredbi.

4.1.1 *Podatci dostupni preko ITS sučelja*

Jedinica u vozilu odgovorna je za ažuriranje podataka koji će biti dostupni putem ITS sučelja učestalošću koja se utvrđuje u okviru postupaka jedinice u vozilu, bez uključivanja ITS sučelja. Podatci iz jedinice u vozilu upotrebljavaju se kao osnova za dopunjavanje i ažuriranje podataka; način na koji se to ostvaruje utvrđen je drugdje u Uredbi, a ako takva specifikacija ne postoji, taj je način funkcija izvedbe proizvoda i nije utvrđen u ovom Dodatku.

4.1.2 *Sadržaj podataka*

Sadržaj podataka utvrđen je u Prilogu 1. ovom Dodatku.

4.1.3 *ITS aplikacije*

ITS aplikacije upotrebljavat će podatke koji su stavljeni na raspolaganje preko ITS sučelja za, na primjer, optimizaciju upravljanja aktivnostima vozača u skladu s Uredbom, otkrivanje mogućih kvarova tahografa ili upotrebu podataka GNSS-a. Specifikacija aplikacija nije obuhvaćena područjem primjene ovog Dodatka.

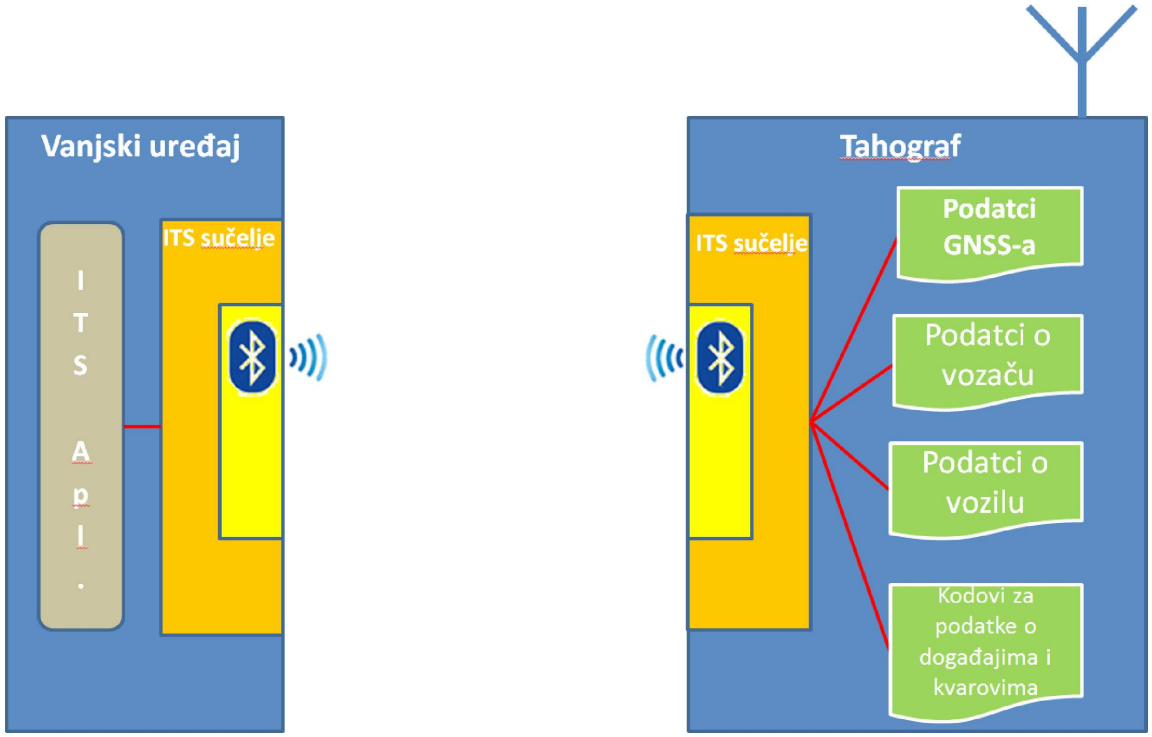
4.2. **Komunikacijska tehnologija**

Podatci se razmjenjuju primjenom ITS sučelja preko Bluetooth® sučelja koje je kompatibilno s verzijom 4.2 ili kasnijom verzijom. Bluetooth® radi u nelicenciranom pojasu od 2,4 do 2,485 GHz za industrijsku, znanstvenu i medicinsku primjenu (ISM). Bluetooth® 4.2 nudi unaprijeđene mehanizme za zaštitu privatnosti i sigurnosne mehanizme te veću brzinu i pouzdanost prijenosa podataka. U smislu ove specifikacije, primjenjuje se Bluetooth® radio drugog razreda s dometom od najviše 10 metara. Više informacija o Bluetoothu® 4.2 dostupno je na stranici www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Komunikacija se uspostavlja komunikacijskom opremom nakon što odobreni uređaj završi proces uparivanja. Budući da Bluetooth® upotrebljava model nadređenog/podređenog uređaja kojim nadzire kada i kako uređaji mogu slati podatke, tahograf će imati nadređenu ulogu, dok će vanjski uređaji imati podređenu ulogu.

Proces uparivanja putem Bluetootha® može započeti kada vanjski uređaj prvi put dođe u domet jedinice u vozilu (vidjeti i Prilog 2.). Uređaji dijele adrese, nazive i profile te zajednički tajni ključ kojim im se omogućuje povezivanje pri svakom budućem susretu. Tim je korakom uspostavljeno povjerenje u odnosu na vanjski uređaj te je on u stanju pokrenuti zahtjeve za preuzimanje podataka iz tahografa. Nije predviđeno dodavanje mehanizama za šifriranje povrh onih koje pruža Bluetooth®. Međutim, ako su potrebni dodatni sigurnosni mehanizmi, oni se osiguravaju u skladu s Dodatkom 10. „Zajednički sigurnosni mehanizmi”.

Opće komunikacijsko načelo opisano je sljedećom slikom.



SPP (profil serijskog ulaza) profil Bluetootha® upotrebljava se za prijenos podataka iz jedinice u vozilu na vanjski uređaj.

4.3. **Autorizacija PIN-om**

Iz sigurnosnih razloga jedinica u vozilu uspostavlja sustav za autorizaciju PIN lozinkom odvojen od uparivanja Bluetoothom. Svaka jedinica u vozilu mora moći generirati PIN lozinke za autentifikaciju koje se sastoje od najmanje četiri znamenke. Pri svakom uparivanju vanjskog uređaja s jedinicom u vozilu vanjski uređaj mora osigurati točnu PIN lozinku prije zaprimanja podataka.

Nakon uspješnog unosa PIN-a uređaj se stavlja na popis dopuštenih uređaja. Na popisu dopuštenih uređaja nalazi se najmanje 64 uređaja uparenih s određenom jedinicom u vozilu.

U slučaju unosa netočne PIN lozinke tri puta zaredom, uređaj se privremeno stavlja na popis zabranjenih uređaja. Svaki pokušaj uređaja odbija se sve dok se uređaj nalazi na popisu zabranjenih uređaja. Ponovni unos netočne PIN lozinke tri puta zaredom za posljedicu ima dulje trajanje zabrane (vidjeti tablicu 1.). Unosom točne PIN lozinke poništava se trajanje zabrane i broj pokušaja. Na slici 1. u Prilogu 2. prikazan je dijagram slijeda za pokušaj potvrde PIN-a.

Tablica 1

Trajanje zabrane ovisno o broju uzastopnih neuspješnih pokušaja unosa točne PIN lozinke

Broj uzastopnih neuspješnih pokušaja	Trajanje zabrane
3	30 sekundi
6	5 minuta
9	1 sat
12	24 sata
15	trajno

U slučaju unosa netočne PIN lozinke petnaest puta (5 x 3) zaredom ITS jedinica trajno se uvrštava na popis zabranjenih uređaja. Trajna se zabrana ukida samo unosom točne PUC lozinke.

PUC lozinku, koja se sastoji od osam znamenki, dostavlja proizvođač zajedno s jedinicom u vozilu. U slučaju unosa netočne PUC lozinke deset puta zaredom ITS jedinica neopozivo se stavlja na popis zabranjenih uređaja.

Proizvođač može ponuditi mogućnost promjene PIN lozinke izravno putem jedinice u vozilu, no PUC lozinka nepromjenjiva je. Za eventualnu promjenu PIN lozinke potrebno je unijeti trenutačnu PIN lozinku izravno u jedinicu u vozilu.

Nadalje, svi uređaji navedeni na popisu dopuštenih uređaja čuvaju se dok ih ručno ne ukloni korisnik (npr. preko sučelja čovjek – stroj jedinice u vozilu ili drugim sredstvima). Time se izgubljene ili ukradene ITS jedinice mogu ukloniti s popisa dopuštenih uređaja. Nadalje, svaka ITS jedinica koja izađe izvan dometa Bluetooth veze u trajanju duljem od 24 sata automatski se uklanja s popisa dopuštenih uređaja za jedinicu u vozilu i mora ponovno osigurati točnu PIN lozinku pri ponovnom uspostavljanju veze.

Format poruka između sučelja jedinice u vozilu i jedinice u vozilu nije predviđen, već ga po vlastitom nahođenju određuje proizvođač. Međutim, predmetni proizvođač osigurava da se poštuje format poruka između ITS jedinice i sučelja jedinice u vozilu (vidjeti specifikacije za ASN.1).

Stoga se na svaki zahtjev za podatke odgovara prikladnom provjerom ovlaštenja pošiljatelja prije bilo kakvog oblika obrade. Na slici 2. u Prilogu 2. prikazan je dijagram slijeda za taj postupak. Svaki uređaj uvršten na popis zabranjenih uređaja automatski se odbija, dok svaki uređaj koji nije uvršten na popis zabranjenih uređaja ni na popis dopuštenih uređaja dobiva zahtjev za PIN koji treba ispuniti prije ponovnog slanja zahtjeva za podatke.

4.4. **Format poruke**

Sve poruke koje razmjenjuju ITS jedinica i sučelje jedinice u vozilu po svojem formatu imaju strukturu koja se sastoji od triju dijelova: zaglavlja koje se sastoji od ciljanog bajta (TGT), izvornog bajta (SRC) i bajta duljine (LEN);

podatkovnog polja koje se sastoji od bajta identifikatora usluge (SID) i promjenjivog iznosa podatkovnih bajtova (najviše 255) te

bajta kontrolnog zbroja koji je jedna serija zbroja bajtova modulo 256 svih bajtova poruke osim samog kontrolnog zbroja (CS).

Poruka prati redoslijed zapisa big endian.

Tablica 2

Opći format poruke

Zaglavlje			Podatkovno polje					Kontrolni zbroj
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 bajta			Najviše 255 bajtova					1 bajt

Zaglavlje

TGT i SRC: identifikator ciljnih (TGT) i izvornih (SRC) uređaja poruke. Sučelje jedinice u vozilu ima standardni identifikator „EE”. Taj identifikator nije moguće promijeniti. ITS jedinica upotrebljava standardni identifikator „A0” za svoju prvu poruku u komunikacijskoj razmjeni podataka. Sučelje jedinice u vozilu zatim ITS jedinici dodjeljuje jedinstveni identifikator i obavješćuje ju o tom identifikatoru za buduće poruke tijekom razmjene podataka.

LEN bajt uzima u obzir samo dio „DATA” podatkovnog polja (vidjeti tablicu 2.); implicitna su prva četiri bajta.

Sučelje jedinice u vozilu potvrđuje autentičnost pošiljatelja poruke usporedbom svojeg popisa identifikatora s Bluetooth podatcima tako što provjerava je li ITS jedinica navedena uz dostavljeni identifikator trenutačno u dometu Bluetooth veze.

Podatkovno polje

Osim SID-a, podatkovno polje sadržava i druge parametre: parametar zahtjeva za prijenos (TRTP) i bajtove brojača.

Ako su podatci koji se prenose dulji od raspoloživog prostora u jednoj poruci, oni se dijele u nekoliko potporuka. Svaka potporuka ima jednako zaglavlje i SID, ali sadržava brojač od dva bajta, trenutačni brojač (CC) i maksimalni brojač (CM) za označavanje broja potporuke. Kako bi se omogućili provjera grešaka i prekid, uređaj koji prima podatke potvrđuje svaku potporuku. Uređaj koji prima podatke može prihvatiti potporuku, zatražiti njezino ponovno slanje i zatražiti od uređaja koji šalje podatke da ponovno započne ili prekine prijenos.

Ako se ne upotrebljavaju, za CC i CM određuje se vrijednost 0 x FF.

Na primjer, sljedeća poruka

ZAGLAVLJE (eng. *HEADER*)	SID	TRTP	CC	CM	DATA	CS
3 bajta	više od 255 bajtova					1 bajt

prenosi se kao:

ZAGLAVLJE	SID	TRTP	01	n	DATA	CS
3 bajta	255 bajtova					1 bajt

ZAGLAVLJE	SID	TRTP	02	n	DATA	CS
3 bajta	255 bajtova					1 bajt

…

ZAGLAVLJE (eng. *HEADER*)	SID	TRTP	N	N	DATA	CS
3 bajta	najviše 255 bajtova					1 bajt

Tablica 3. sadržava poruke koje mogu razmjenjivati jedinica u vozilu i ITS jedinica. Sadržaj svakog parametra naveden je u heksadecimalnom zapisu. U tablici radi jasnoće nisu navedeni CC i CM; za potpuni format vidjeti prethodno.

Tablica 3

Detaljan sadržaj poruke

Poruka	Zaglavlje			DATA			Kontrolni zbroj
	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	vrijeme (*Time*)	
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		

Poruka	Zaglavlje			DATA			Kontrolni zbroj
	TGT	SRC	LEN	SID	TRTP	DATA	
ResquestAccepted	*ITSID*	EE	Len	09	TREP	podatci (*Data*)	
DataUnavailable							
Podatci nisu dostupni	*ITSID*	EE	02	0A	TREP	10	
Osobni se podatci ne dijele	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Opće odbijanje	*ITSID*	EE	02	0B	SID Req	10	
Usluga nije podržana	*ITSID*	EE	02	0B	SID Req	11	
Podfunkcija nije podržana	*ITSID*	EE	02	0B	SID Req	12	
Nepravilna duljina poruke	*ITSID*	EE	02	0B	SID Req	13	
Nepravilni uvjeti ili greška u slijedu zahtjeva	*ITSID*	EE	02	0B	SID Req	22	
Zahtjev izvan dometa	*ITSID*	EE	02	0B	SID Req	31	
Čeka se odgovor	*ITSID*	EE	02	0B	SID Req	78	
Neusklađenost ITSID-a	*ITSID*	EE	02	0B	SID Req	FC	
Nije pronađen ITSID	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Poruku šalje sučelje jedinice u vozilu ako ITS jedinica koja nije na popisu zabranjenih uređaja, ali ni na popisu dopuštenih uređaja, pošalje bilo kakav zahtjev za podatke.

SendITSID (SID 02)

Poruku šalje sučelje jedinice u vozilu svaki put kada novi uređaj pošalje zahtjev. Taj uređaj upotrebljava standardni identifikator „A0” prije no što mu se dodijeli jedinstveni identifikator za buduću komunikacijsku razmjenu podataka.

SendPIN (SID 03)

Poruku šalje ITS jedinica koju sučelje jedinice u vozilu treba uvrstiti na popis dopuštenih uređaja. Sadržaj je poruke kod od četiri cijela broja (4 INTEGER) između nula i devet.

PairingResult (SID 04)

Poruku šalje sučelje jedinice u vozilu kako bi obavijestilo ITS jedinicu da je PIN lozinka koju je poslala točna. Sadržaj je poruke Booleov izraz s vrijednošću „točno” („True”) ako je PIN lozinka bila točna ili „netočno” („False”) ako je PIN lozinka bila netočna.

SendPUC (SID 05)

Poruku šalje ITS jedinica kako bi se sučelje jedinice u vozilu uklonilo s popisa zabranjenih uređaja. Sadržaj je poruke kod od četiri cijela broja (8 INTEGER) između nula i devet.

BanLiftingResult (SID 06)

Poruku šalje sučelje jedinice u vozilu kako bi obavijestilo ITS jedinicu da je PUC lozinka koju je poslala točna. Sadržaj je poruke Booleov izraz s vrijednošću „točno” („True”) ako je PUC lozinka bila točna ili „netočno” („False”) ako je PUC lozinka bila netočna.

RequestRejected (SID 07)

Poruku šalje sučelje jedinice u vozilu kao odgovor na bilo koju poruku koju je poslala ITS jedinica uvrštena na popis zabranjenih uređaja osim poruke „SendPUC”. Poruka sadržava preostalo vrijeme tijekom kojeg je ITS jedinica uvrštena na popis zabranjenih uređaja u skladu s formatom slijeda „Time” kako je utvrđeno u Prilogu 3.

RequestData (SID 08)

Poruku za pristup podatcima šalje ITS jedinica. Parametrom zahtjeva za prijenos od jednog bajta (TRTP) označena je vrsta traženih podataka. Nekoliko je vrsta podataka:

— standardTachData (TRTP 01): podatci dostupni iz tahografa koji su klasificirani kao neosobni,

— personalTachData (TRTP 02): podatci dostupni iz tahografa koji su klasificirani kao osobni,

— gnssData (TRTP 03): podatci GNSS-a, koji su uvijek osobni,

— standardEventData (TRTP 04): zabilježeni podatci o događaju koji su klasificirani kao neosobni,

— personalEventData (TRTP 05): zabilježeni podatci o događaju koji su klasificirani kao osobni,

— standardFaultData (TRTP 06): zabilježeni kvarovi koji su klasificirani kao neosobni,

— manufacturerData (TRTP 07): podatci koje je na raspolaganje stavio proizvođač.

Vidjeti Prilog 3. ovom Dodatku za više informacija o sadržaju svake vrste podataka.

Vidjeti Dodatak 12. za više informacija o formatu i sadržaju podataka GNSS-a.

Vidjeti priloge I.B i I.C za više informacija o kodu podataka o događaju i o kvarovima.

ResquestAccepted (SID 09)

Poruku šalje sučelje jedinice u vozilu ako je prihvatilo poruku „RequestData” ITS jedinice. Poruka sadržava TREP od jednog bajta, koji je TRTP bajt povezane poruke „RequestData”, i sve podatke zatražene vrste.

DataUnavailable (SID 0A)

Poruku šalje sučelje jedinice u vozilu ako iz nekog razloga zatraženi podatci nisu dostupni za slanje ITS jedinici s popisa dopuštenih uređaja. Poruka sadržava TREP od jednog bajta, koji je TRTP zatraženih podataka, i kod greške od jednog bajta kako je navedeno u tablici 3. Dostupni su sljedeći kodovi:

— Podatci nisu dostupni (10): Sučelje jedinice u vozilu ne može pristupiti podatcima jedinice u vozilu iz neutvrđenih razloga.

— Osobni se podatci ne dijele (11): ITS jedinica pokušava učitati osobne podatke ako se oni ne dijele.

NegativeAnswer (SID 0B)

Poruke šalje sučelje jedinice u vozilu ako zahtjev ne može biti ispunjen iz bilo kojeg drugog razloga osim nedostupnosti podataka. Poruke su obično posljedica nepravilnog formata zahtjeva (duljina, SID, ITSID…), ali razlozi nisu ograničeni na to. TRTP u podatkovnom polju sadržava SID zahtjeva. Podatkovno polje sadržava kod na temelju kojeg se utvrđuje razlog negativnog odgovora. Dostupni su sljedeći kodovi:

— Opće odbijanje (kôd 10)

— Radnja se ne može provesti zbog razloga koji nije naveden u nastavku ili u odjeljku (unos broja odjeljka *DataUnavailable*).

— Usluga nije podržana (kôd 11)

— Nerazumljiv SID zahtjeva.

— Podfunkcija nije podržana (kôd 12)

— Nerazumljiv TRTP zahtjeva. To, na primjer, može biti vrijednost koja nedostaje ili neprihvatljiva vrijednost.

— Nepravilna duljina poruke (kôd 13)

— Duljina primljene poruke pogrešna je (neusklađenost LEN bajta i stvarne duljine poruke).

— Nepravilni uvjeti ili greška u slijedu zahtjeva (kôd 22)

— Zatražena usluga nije aktivna ili slijed poruka zahtjeva nije točan.

— Zahtjev izvan dometa (kôd 33)

— Zapis parametra zahtjeva (podatkovno polje) nije valjan.

— Čeka se odgovor (kôd 78)

— Zatražena se radnja ne može provesti na vrijeme i jedinica u vozilu nije spremna prihvatiti drugi zahtjev.

— Neusklađenost ITSID-a (kôd FB)

— SRC *ITSID* nije usklađen s povezanim uređajem nakon usporedbe s Bluetooth informacijama.

— Nije pronađen *ITSID* (kôd FC)

— SRC *ITSID* nije povezan ni s jednim uređajem.

U redcima od 1. do 72. (**FormatMessageModule**) ASN.1 koda u Prilogu 3. utvrđen je format poruka kako je opisano u tablici 3. Više pojedinosti o sadržaju poruka navedeno je u nastavku.

4.5. **Suglasnost vozača**

Svi dostupni podatci klasificirani su kao standardni ili kao osobni. Osobni su podatci dostupni samo ako je vozač dao suglasnost i prihvatio da se njegovi osobni podatci iz tahografa mogu prenositi izvan mreže vozila aplikacijama trećih strana.

Vozač suglasnost daje pri prvom umetanju određene kartice vozača ili kartice radionice koja je trenutačno nepoznata jedinici u vozilu; nositelja kartice poziva se da dâ svoju suglasnost za prijenos osobnih podataka iz tahografa preko neobveznog ITS sučelja. (Vidjeti i Prilog I.C stavak 3.6.2.).

Stanje suglasnosti (omogućeno/onemogućeno) bilježi se u memoriji tahografa.

U slučaju više vozača, s ITS sučeljem dijele se samo osobni podatci vozača koji su dali svoju suglasnost. Na primjer, ako su u vozilu dva vozača i ako je samo prvi vozač pristao dijeliti svoje osobne podatke, podatci koji se odnose na drugog vozača ne dijele se.

4.6. **Učitavanje standardnih podataka**

Na slici 3. u Prilogu 2. prikazani su dijagrami slijeda za valjani zahtjev za pristup standardnim podatcima koji je poslala ITS jedinica. Ako je ITS jedinica pravilno uvrštena na popis dopuštenih uređaja i ne traži osobne podatke, dodatna provjera nije potrebna. U dijagramima se smatra da se poštovao pravilan postupak prikazan na slici 2. u Prilogu 2. Dijagrami mogu biti izjednačeni sa sivim poljem *REQUEST TREATMENT* na slici 2.

Od dostupnih se podataka standardnima smatraju sljedeći:

— standardTachData (TRTP 01),

— StandardEventData (TRTP 04),

— standardFaultData (TRTP 06).

4.7. **Učitavanje osobnih podataka**

Na slici 4. u Prilogu 2. prikazan je dijagram slijeda za obradu zahtjeva za osobne podatke. Kako je ranije navedeno, sučelje jedinice u vozilu šalje osobne podatke samo ako je vozač dao izričitu suglasnost (vidjeti i 4.5.). U suprotnom zahtjev se mora automatski odbiti.

Od dostupnih se podataka osobnima smatraju sljedeći:

— personalTachData (TRTP 02),

— gnssData (TRTP 03),

— personalEventData (TRTP 05),

— manufacturerData (TRTP 07).

4.8. **Učitavanje podataka o događajima i kvarovima**

ITS jedinice moraju moći zatražiti podatke o događajima koji sadržavaju popis svih neočekivanih događaja. Ti se podatci smatraju standardnima ili osobnima; vidjeti Prilog 3. Sadržaj svakog događaja u skladu je s dokumentacijom iz Priloga 1. ovom Dodatku.

PRILOG 1.

POPIS PODATAKA DOSTUPNIH PREKO ITS SUČELJA

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) KONTINUIRANI PODATCI GNSS-A DOSTUPNI NAKON SUGLASNOSTI VOZAČA

Vidjeti Dodatak 12. – GNSS.

3) KODOVI DOGAĐAJA DOSTUPNI BEZ SUGLASNOSTI VOZAČA

Događaj	Pravila pohrane	Podatci koje je potrebno bilježiti po događaju
Umetanje nevažeće kartice	— deset najnovijih događaja.	— datum i vrijeme događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju kartice kojom je stvoren događaj, — broj sličnih događaja tog dana.
Konflikt kartica	— deset najnovijih događaja.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju dviju kartica zbog kojih je nastao sukob.
Posljednja razmjena podataka s karticom koja nije ispravno zatvorena	— deset najnovijih događaja.	— datum i vrijeme umetanja kartice, — vrstu i broj kartice, državu članicu koje je izdala karticu i generaciju kartice, — posljednju razmjenu podataka očitanih s kartice: — datum i vrijeme umetanja kartice, — VRN, državu članicu registracije i generaciju jedinice u vozilu.
Prekid napajanja (2)	— najdulji događaj za svaki od deset posljednjih dana pojave, — pet najduljih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Greška u komunikaciji s uređajem za komunikaciju na daljinu	— najdulji događaj za svaki od deset posljednjih dana pojave, — pet najduljih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Izostanak podataka o položaju iz prijamnika GNSS-a	— najdulji događaj za svaki od deset posljednjih dana pojave, — pet najduljih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Greška u podatcima o kretanju	— najdulji događaj za svaki od deset posljednjih dana pojave, — pet najduljih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.

Događaj	Pravila pohrane	Podatci koje je potrebno bilježiti po događaju
Konflikt u kretanju vozila	— najdulji događaj za svaki od deset posljednjih dana pojave, — pet najduljih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Pokušaji povrede sigurnosti	deset najnovijih događaja po vrsti događaja.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja (ako je relevantno), — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — vrstu događaja.
Vremenski konflikt	— najdulji događaj za svaki od deset posljednjih dana pojave, — pet najduljih događaja u posljednjih 365 dana.	— datum i vrijeme iz uređaja za bilježenje podataka, — datum i vrijeme GNSS-a, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.

4) KODOVI DOGAĐAJA DOSTUPNI UZ SUGLASNOST VOZAČA

Događaj	Pravila pohrane	Podatci koje je potrebno bilježiti po događaju
Vožnja bez odgovarajuće kartice	— najdulji događaj za svaki od deset posljednjih dana pojave, — pet najduljih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Umetanje kartice tijekom vožnje	— posljednji događaj za svaki od deset posljednjih dana pojave,	— datum i vrijeme događaja, — vrstu i broj kartice, državu članicu koje je izdala karticu i generaciju kartice, — broj sličnih događaja tog dana.
Prekoračenje brzine (1)	— najozbiljniji događaj za svaki od deset posljednjih dana pojave (tj. događaj s najvećom prosječnom brzinom), — pet najozbiljnijih događaja u posljednjih 365 dana. — prvi događaj koji se dogodio nakon posljednje kalibracije.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — najveću brzinu izmjerenu tijekom događaja, — aritmetički prosjek brzine izmjerene tijekom događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju kartice vozača (ako je primjereno), — broj sličnih događaja tog dana.

5) KODOVI ZA PODATKE O KVARU DOSTUPNI BEZ SUGLASNOSTI VOZAČA

Kvar	Pravila pohrane	Podatci koje je potrebno bilježiti po kvaru
Kvar kartice	— deset najnovijih kvarova kartice vozača.	— datum i vrijeme početka kvara, — datum i vrijeme završetka kvara, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju kartice.
Kvar uređaja za bilježenje podataka	— deset najnovijih kvarova po vrsti kvara, — prvi kvar koji se dogodio nakon posljednje kalibracije.	— datum i vrijeme početka kvara, — datum i vrijeme završetka kvara, — vrstu kvara, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku kvara.

Taj se kvar aktivira za neku od sljedećih grešaka dok nije u kalibracijskom načinu:

— unutarnji kvar jedinice u vozilu,

— kvar pisača,

— kvar zaslona,

— kvar pri preuzimanju podataka,

— kvar senzora,

— kvar prijamnika GNSS-a ili vanjskog uređaja GNSS-a,

— kvar uređaja za komunikaciju na daljinu.

6) DOGAĐAJI I KVAROVI SPECIFIČNI ZA PROIZVOĐAČA BEZ SUGLASNOSTI VOZAČA

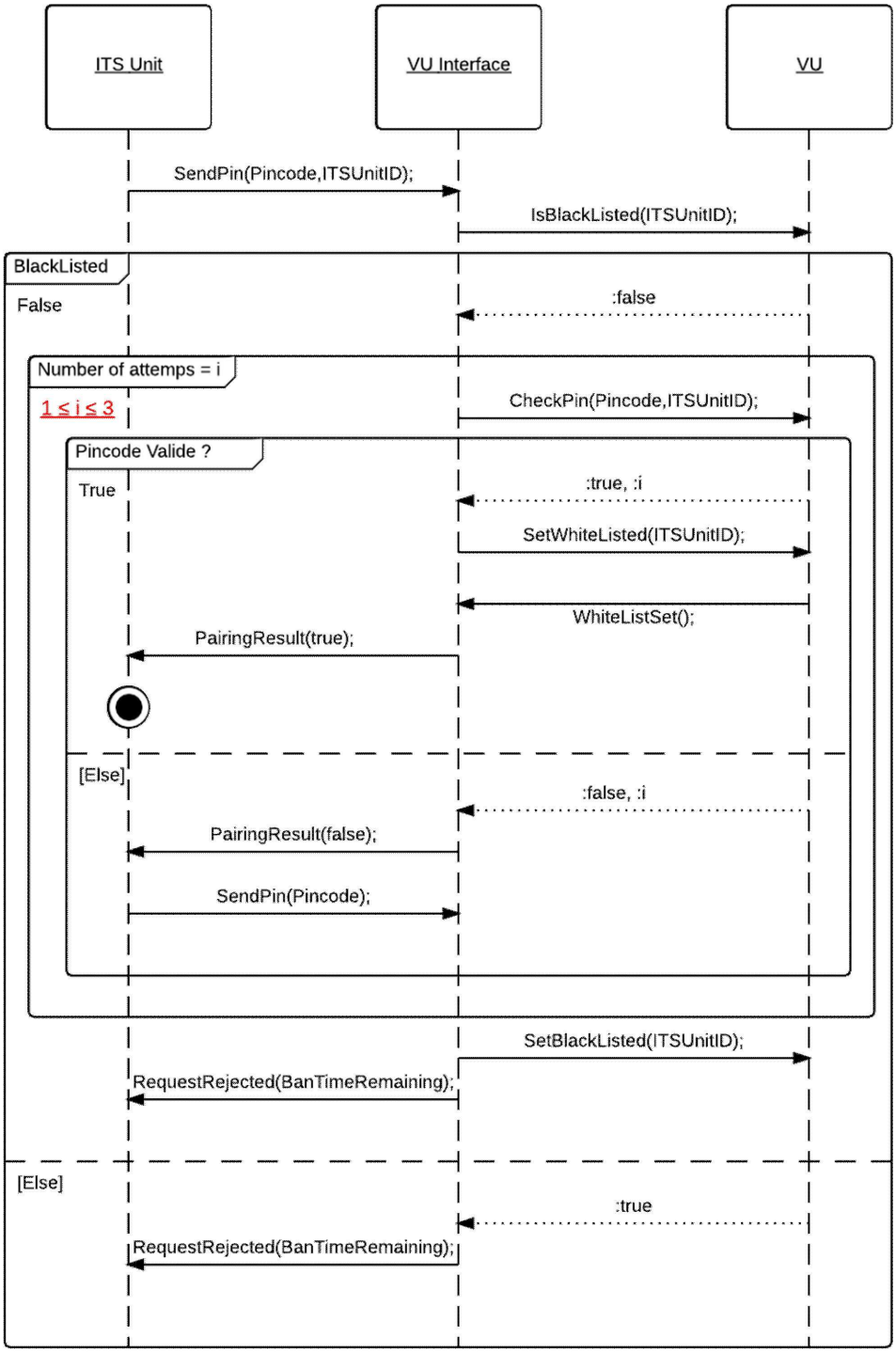
Događaj ili kvar	Pravila pohrane	Podatci koje je potrebno bilježiti po događaju
Utvrđuje proizvođač.	Utvrđuje proizvođač.	Utvrđuje proizvođač.

PRILOG 2.

DIJAGRAMI SLIJEDA RAZMJENA PORUKA S ITS JEDINICOM

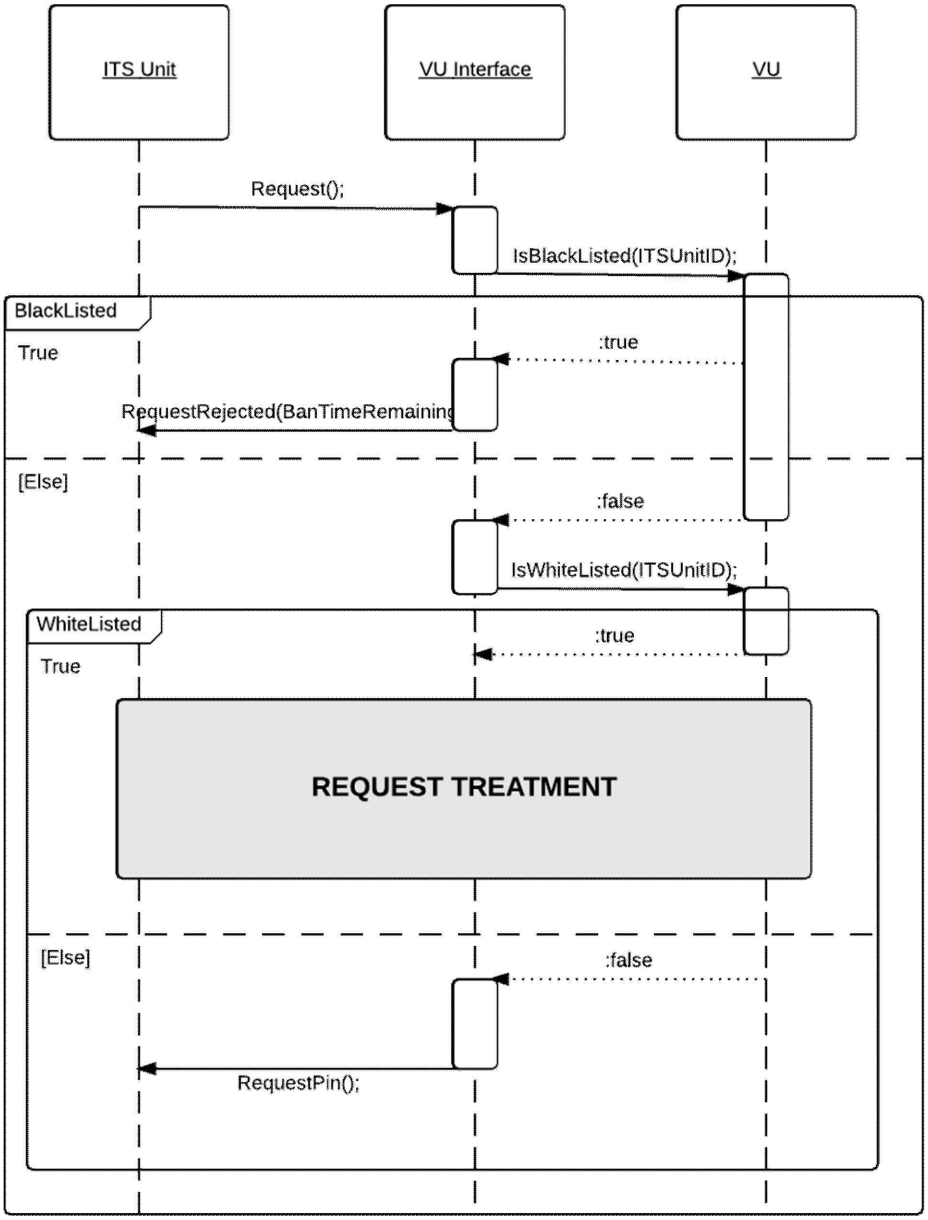
Slika 1

Dijagram slijeda za pokušaj potvrde PIN-a



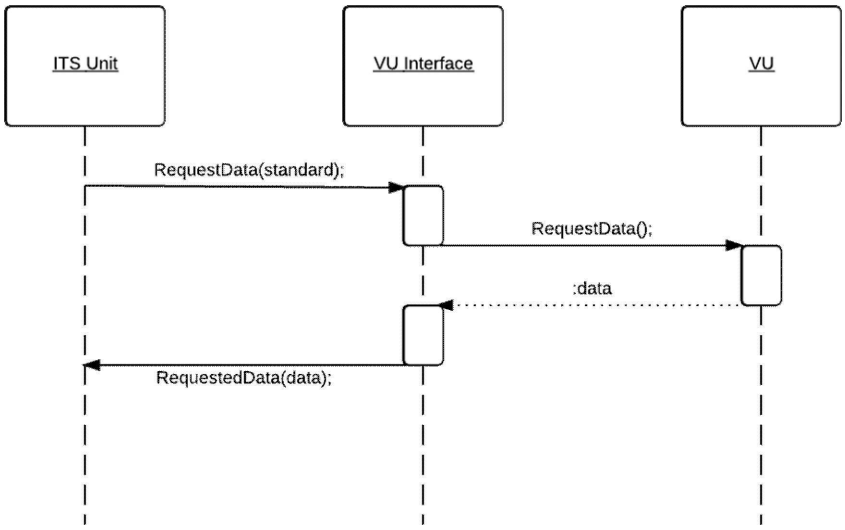
Slika 2

Dijagram slijeda za provjeru autorizacije ITS jedinice



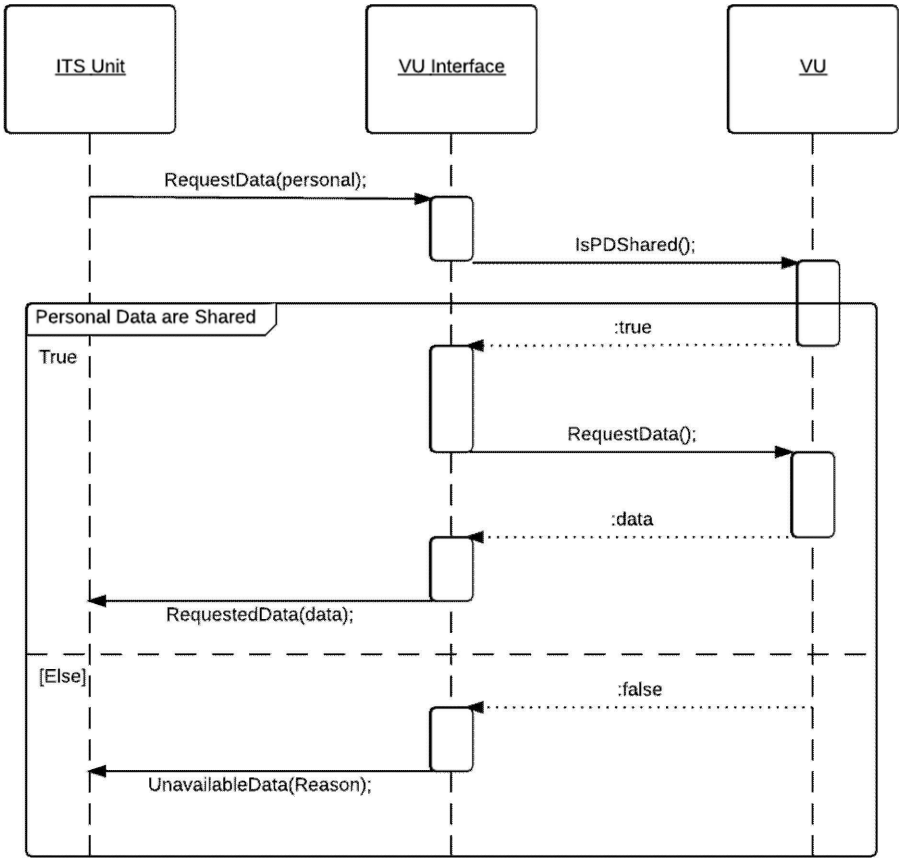
Slika 3

Dijagram slijeda za obradu zahtjeva za podatke koji su klasificirani kao neosobni (pristup nakon unosa točnog PIN-a)



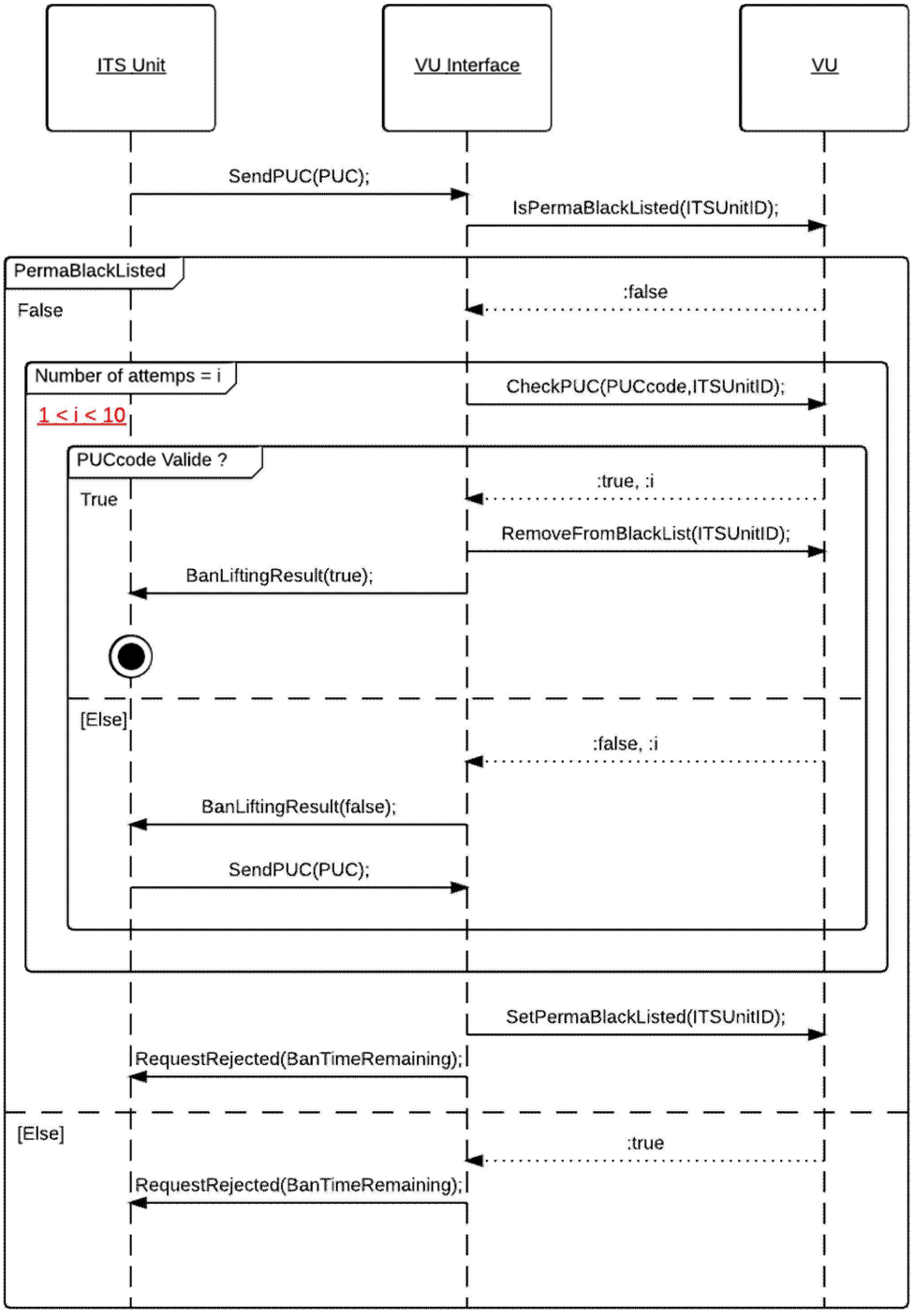
Slika 4

Dijagram slijeda za obradu zahtjeva za podatke koji su klasificirani kao osobni (pristup nakon unosa točnog PIN-a)



Slika 5

Dijagram slijeda za pokušaj potvrde PUC-a



PRILOG 3.

ASN.1 – SPECIFIKACIJE

```
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
```

Dodatak 14.

FUNKCIJA KOMUNIKACIJE NA DALJINU

SADRŽAJ

1 UVOD ... 450

2 PODRUČJE PRIMJENE ... 451

3 KRATICE, DEFINICIJE I BILJEŠKE ... 452

4 OPERATIVNI SCENARIJI ... 454

4.1 Pregled ... 454

4.1.1 Preduvjeti za prijenos podataka putem sučelja DSRC-a na frekvenciji od 5,8 GHz ... 454

4.1.2 Profil 1.a: putem ručnog usmjerenog ili privremeno postavljenog uz cestu i usmjerenog čitača komunikacije ranog otkrivanja na daljinu ... 455

4.1.3 Profil 1.b: putem ugrađenog u vozilu i usmjerenog čitača komunikacije ranog otkrivanja na daljinu (REDCR) ... 456

4.2 Sigurnost/integritet ... 456

5 IZVEDBA I PROTOKOLI KOMUNIKACIJE NA DALJINU ... 456

5.1 Izvedba ... 456

5.2 Tijek rada ... 459

5.2.1 Radnje ... 459

5.2.2 Tumačenje podataka primljenih putem komunikacije DSRC-a ... 461

5.3 Parametri fizičkog sučelja DSRC-a za komunikaciju na daljinu ... 461

5.3.1 Ograničenja u pogledu lokacije ... 461

5.3.2 Parametri silazne i uzlazne veze ... 461

5.3.3 Izvedba antene ... 466

5.4 Zahtjevi u pogledu protokola DSRC-a za RTM ... 466

5.4.1 Pregled ... 466

5.4.2 Naredbe ... 469

5.4.3 Slijed naredbi za ispitivanje ... 469

5.4.4 Strukture podataka ... 470

5.4.5 Elementi RtmData, provedene radnje i definicije ... 472

5.4.6 Mehanizam prijenosa podataka ... 476

5.4.7 Detaljni opis transakcija u okviru DSRC-a ... 476

5.4.8 Opis ispitivanja transakcija u okviru DSRC-a ... 486

5.5 Potpora Direktivi (EU) 2015/719 ... 490

5.5.1 Pregled ... 490

5.5.2 Naredbe 490

5.5.3 Slijed naredbi za ispitivanje 490

5.5.4 Strukture podataka 490

5.5.5 Modul ASN.1 za transakcije OWS-a u okviru DSRC-a 491

5.5.6 Elementi OwsData, provedene radnje i definicije 492

5.5.7 Mehanizmi prijenosa podataka 492

5.6 Prijenos podataka između DSRC-VU-a i VU-a 492

5.6.1 Fizička veza i sučelja 492

5.6.2 Protokol aplikacije 493

5.7 Rješavanje pogrešaka 494

5.7.1 Bilježenje i prijenos podataka u okviru DSRC-VU-a 494

5.7.2 Pogreške bežične komunikacije 494

6 PUŠTANJE U POGON I PERIODIČKA ISPITIVANJA PREGLEDA ZA FUNKCIJU KOMUNIKACIJE NA DALJINU 496

6.1 Opće značajke 496

6.2 ECHO 496

6.3 Ispitivanja za potvrđivanje sigurnog sadržaja podataka 496

1 UVOD

U ovom se Dodatku utvrđuju izvedba i postupci koje treba slijediti kako bi se provela funkcija komunikacije na daljinu (komunikacije) kako se zahtijeva u članku 9. Uredbe (EU) br. 165/2014 (Uredba).

DSC_1 U Uredbi (EU) br. 165/2014 utvrđuje se da tahograf mora biti opremljen funkcijom za komunikaciju na daljinu kojom se djelatnicima nadležnih nadzornih tijela omogućuje da očitaju tahografske informacije iz vozila u prolazu upotrebom opreme za ispitivanje na daljinu (čitača komunikacije ranog otkrivanja na daljinu (eng. *Remote early detection communication reader*, REDCR), konkretno, opreme za ispitivanje koja se bežično spaja putem sučelja namjenskog komunikacijskog sustava kratkog dometa (eng. *Dedicated Short Range Communication*, DSRC) na frekvenciji od 5,8 GHz u skladu s normom CEN.

Važno je znati da je ta funkcija namijenjena isključivo kao predfiltar kako bi se odabrala vozila za detaljniji pregled te ne zamjenjuje službeni postupak pregleda kako je utvrđeno u odredbama Uredbe (EU) br. 165/2014. Vidjeti uvodnu izjavu 9. u preambuli te Uredbe u kojoj se navodi da komunikacija na daljinu između tahografa i nadzornih tijela u svrhu nadzora na cesti olakšava provedbu ciljanih provjera na cesti.

DSC_2 Podatci se razmjenjuju komunikacijom koja se odvija bežično upotrebom bežične namjenske komunikacije kratkog dometa na frekvenciji od 5,8 GHz koja je u skladu s ovim Dodatkom i ispitana u odnosu na odgovarajuće parametre norme 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 Komunikacija se uspostavlja s pomoću komunikacijske opreme samo kada to zahtijeva oprema nadležnog nadzornog tijela upotrebom sukladnih radiokomunikacijskih sredstava (REDCR-a).

DSC_4 Podatci su zaštićeni kako bi se osigurao integritet.

DSC_5 Pristup prenesenim podatcima ograničen je na nadležna nadzorna tijela koja imaju ovlasti za provjeru kršenja Uredbe (EZ) br. 561/2006 i Uredbe (EU) br. 165/2014 te na radionice ako treba provjeriti radi li tahograf ispravno.

DSC_6 Podatci razmijenjeni tijekom komunikacije ograničuju se na podatke potrebne u svrhu ciljanih provjera vozila na cesti čijim se tahografom možda neovlašteno rukovalo ili koji se pogrešno upotrebljavao.

DSC_7 Integritet i sigurnost podataka postižu se zaštitom podataka jedinice u vozilu (VU) i prijenosom isključivo zaštićenih podataka te sigurnosnih podataka (vidjeti odjeljak 5.4.4) putem bežičnog komunikacijskog sredstva DSRC na frekvenciji od 5,8 GHz, što znači da samo ovlaštene osobe nadležnih nadzornih tijela mogu razumjeti podatke prenesene komunikacijom i provjeriti njihovu vjerodostojnost. Vidjeti Dodatak 11., Zajednički sigurnosni mehanizmi.

DSC_8 Podatci sadržavaju vremensku oznaku koja označava vrijeme njihova posljednjeg ažuriranja.

DSC_9 Sadržaj sigurnosnih podataka poznat je isključivo nadležnim nadzornim tijelima i stranama s kojima ona dijele te informacije u skladu s odredbama komunikacije koja je predmet ovog Dodatka, osim što se komunikacijom omogućuje prijenos sigurnosnih podataka sa svakim paketom prenesenih podataka.

DSC_10 Ista struktura i oprema prikladne su za upotrebu kako bi se dobili ostali koncepti podataka (kao što je vaganje u vozilu) upotrebom strukture navedene u nastavku.

DSC_11 Radi objašnjenja, u skladu s odredbama Uredbe (EU) br. 165/2014 (članka 7.), podatci o identitetu vozača ne smiju se prenositi komunikacijom.

2 PODRUČJE PRIMJENE

Područje primjene ovog Dodatka utvrđivanje je načina na koji djelatnici nadležnih nadzornih tijela upotrebljavaju navedenu bežičnu komunikaciju DSRC-a na frekvenciji od 5,8 GHz kako bi na daljinu od ciljanog vozila dobili podatke s pomoću kojih se utvrđuje krši li ciljano vozilo Uredbu (EU) br. 165/2014 i treba li ga se ciljano zaustavljati radi daljnje istrage.

U Uredbi (EU) br. 165/2014 zahtijeva se da se prikupljeni podatci ograniče na podatke ili pripadaju podatcima kojima se utvrđuje moguće kršenje kako je navedeno u članku 9. Uredbe (EU) br. 165/2014.

U takvom je slučaju raspoloživo vrijeme za komunikaciju ograničeno jer je komunikacija ciljana i kratkog dometa. Nadalje, ista komunikacijska sredstva za praćenje tahografa na daljinu (*remote tachograph monitoring*, RTM) nadležna nadzorna tijela mogu upotrebljavati i u druge svrhe (kao što su praćenje najveće mase i dimenzija za teška teretna vozila kako je utvrđeno u Direktivi (EU) 2015/719), a takve radnje mogu biti zasebne ili uzastopne, o čemu odluku donose nadležna nadzorna tijela.

U ovom se Dodatku navodi sljedeće:

— komunikacijska oprema, postupci i protokoli koji će se upotrebljavati za komunikaciju;

— norme i uredbe s kojima je usklađena radijska oprema;

— iznošenje podataka komunikacijskoj opremi;

— postupci za ispitivanje i preuzimanje te slijed radnji;

— podatci koje je potrebno prenijeti;

— moguće tumačenje podataka prenesenih komunikacijom;

— odredbe za sigurnosne podatke koje se odnose na komunikaciju;

— dostupnost podataka nadležnim nadzornim tijelima;

— način na koji čitač komunikacije ranog otkrivanja na daljinu može zatražiti različite koncepte podataka o teretu i voznom parku (eng. *Freight&Fleet*).

Radi objašnjenja, u ovom se Dodatku ne navodi sljedeće:

— prikupljanje podataka i upravljanje podatcima u jedinici u vozilu (što je funkcija izvedbe proizvoda osim ako nije drugačije navedeno u Uredbi (EU) br. 165/2014);

— način iznošenja prikupljenih podataka djelatniku nadležnog nadzornog tijela, kao ni kriteriji koje nadležna nadzorna tijela upotrebljavaju za donošenje odluke o tome koja će vozila zaustaviti (što je funkcija izvedbe proizvoda osim ako nije drugačije navedeno u Uredbi (EU) br. 165/2014 ili odluci u okviru politike nadležnih nadzornih tijela). Radi objašnjenja: komunikacijom se podatci stavljaju na raspolaganje nadležnim nadzornim tijelima isključivo kako bi ona mogla donositi informirane odluke;

— odredbe o sigurnosti podataka (kao što je šifriranje) koje se odnose na sadržaj podataka (koje se navode u Dodatku 11., Zajednički sigurnosni mehanizmi);

— pojedinosti o svim konceptima podataka osim RTM-a koji se mogu dobiti upotrebom iste strukture i opreme;

— pojedinosti o ponašanju i upravljanju između VU-a i DSRC-VU-a, kao ni ponašanje u DSRC-VU-u (osim u svrhu slanja podataka kada to zatraži REDCR).

3 KRATICE, DEFINICIJE I BILJEŠKE

U ovom Dodatku upotrebljavaju se sljedeće pokrate i definicije specifične za ovaj Dodatak:

antena	električni uređaj koji pretvara električnu energiju u radiovalove i obratno, a upotrebljava se u kombinaciji s radio-odašiljačem ili radio-prijamnikom. Pri radu, radio-odašiljač dovodi električnu struju koja oscilira na radijskoj frekvenciji na priključku antene, a antena zrači energiju iz struje u obliku elektromagnetskih valova (radiovalova). Pri prijamu, antena presreće dio energije elektromagnetskog vala kako bi proizvela minimalni napon na svojim priključcima koji se primjenjuje na prijamnik kako bi se pojačao;
komunikacija	razmjena informacija/podataka između DSRC-REDCR-a i DSRC-VU-a u skladu s odjeljkom 5. prema načelu odnosa „nadređen–podređen” kako bi se dobili podatci.
podatci	zaštićeni podatci utvrđena formata (vidjeti odjeljak 5.4.4.) koje zahtijeva DSRC-REDCR, a DSRC-REDCR-u ih šalje DSRC-VU putem veze DSRC-a na frekvenciji od 5,8 GHz kako je utvrđeno u odjeljku 5. u nastavku;
Uredba (EU) br. 165/2014	Europskog parlamenta i Vijeća od 4. veljače 2014. o tahografima u cestovnom prometu, stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u cestovnom prometu i izmjeni Uredbe (EZ) br. 561/2006 Europskog parlamenta i Vijeća o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na cestovni promet;
AID	identifikator aplikacije (eng. *Application Identifier*)
BLE	sustav Bluetooth niske razine energije (eng. *Bluetooth Low Energy*)
BST	tablica usluga radiofara (eng. *Beacon Service Table*)

CIWD	umetanje kartice tijekom vožnje (eng. *Card insertion while driving*)
CRC	kružna provjera zalihosti u prijenosu podataka (eng. *cyclic redundancy check*)
DSC (n)	identifikator zahtjeva za određeni dodatak DSRC-u (eng. *identifier of a requirement for a specific DSRC appendix*)
DSRC	namjenski komunikacijski sustav kratkog dometa (eng. *Dedicated Short Range Communication*)
DSRC-REDCR	DSRC – čitač komunikacije ranog otkrivanja na daljinu (eng. *DSRC – Remote Early Detection Communication Reader*)
DSRC-VU	DSRC – jedinica u vozilu. (eng. *DSRC – Vehicle Unit*) Riječ je o „uređaju za rano otkrivanje na daljinu" koji je definiran u Prilogu I.C.
DWVC	vožnja bez valjane kartice (eng. *Driving without valid card*)
EID	identifikator elemenata (eng. *Element Identifier*)
LLC	kontrola logičke veze (eng. *Logical Link Control*)
LPDU	podatkovna jedinica protokola LLC (eng. *LLC Protocol Data Unit*)
OWS	sustav za vaganje u vozilu (eng. *Onboard Weighing System*)
PDU	podatkovna jedinica protokola (eng. *Protocol Data Unit*)
REDCR	čitač komunikacije ranog otkrivanja na daljinu (eng. *Remote early detection communication reader*). Riječ je o „opremi čitača komunikacije ranog otkrivanja na daljinu" koja je definirana u Prilogu I.C.
RTM	praćenje tahografa na daljinu (eng. *Remote Tachograph Monitoring*)
SM-REDCR	sigurnosni modul čitača komunikacije ranog otkrivanja na daljinu (eng. *Security Module-Remote early detection communication reader*)
TARV	telematske aplikacije za regulirana vozila (serija normi ISO 15638) (eng. *Telematics Applications for Regulated Vehicles*)
VU	jedinica u vozilu (eng. *Vehicle Unit*)
VUPM	prijenosna memorija jedinice u vozilu (eng. *Vehicle Unit Payload Memory*)
VUSM	sigurnosni modul jedinice u vozilu (eng. *Vehicle Unit Security Module*)
VST	tablica usluga vozila (eng. *Vehicle Service Table*)
WIM	vaganje u pokretu (eng. *Weigh in motion*)
WOB	vaganje u vozilu (eng. *Weigh on board*)

Specifikacija utvrđena u ovom Dodatku odnosi se na i ovisi o svim sljedećim uredbama i normama ili o njihovim dijelovima. U okviru odredbi ovog Dodatka utvrđuju se mjerodavne norme ili mjerodavne odredbe normi. U slučaju proturječnosti, odredbe ovog Dodatka imaju prednost. U slučaju bilo kakve proturječnosti, pri čemu se u ovom Dodatku jasno ne utvrđuje nikakva specifikacija, postupanje u skladu s preporukom ERC 70-03 (i ispitano u odnosu na odgovarajuće parametre norme EN 300 674-1) ima prednost, a slijede ih, počevši s najpoželjnijom, norme EN 12795, EN 12253, EN 12834 i EN 13372, točke 6.2., 6.3., 6.4. i 7.1.

Uredbe i norme na koje se upućuje u ovom Dodatku su:

[1] Uredba (EU) br. 165/2014 Europskog parlamenta i Vijeća od 4. veljače 2014. o tahografima u cestovnom prometu, stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u cestovnom prometu i izmjeni Uredbe (EZ) br. 561/2006 Europskog parlamenta i Vijeća o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na cestovni promet;

[2] Uredba (EZ) br. 561/2006 Europskog parlamenta i Vijeća od 15. ožujka 2006. o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na cestovni promet i o izmjeni uredbi Vijeća (EEZ) br. 3821/85 i (EZ) br. 2135/98 te o stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3820/85 (Tekst značajan za EGP);

[3] ERC 70-03 CEPT: *ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)*;

[4] norma ISO 15638, *Intelligent transport systems – Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV)*;

[5] norma EN 300 674-1, *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU)*;

[6] norma EN 12253, *Road transport and traffic telematics – Dedicated short-range communication – Physical layer using microwave at 5.8 GHz*;

[7] norma EN 12795, R*oad transport and traffic telematics – Dedicated short-range communication – Data link layer: medium access and logical link control*;

[8] norma EN 12834, *Road transport and traffic telematics – Dedicated short-range communication – Application layer*;

[9] norma EN 13372, *Road transport and traffic telematics – Dedicated short-range communication – Profiles for RTTT applications*;

[10] norma ISO 14906, *Electronic fee collection – Application interface definition for dedicated short- range communication*.

4 OPERATIVNI SCENARIJI

4.1 **Pregled**

U Uredbi (EU) br. 165/2014 navode se specifični i kontrolirani scenariji u kojima se komunikacija treba upotrebljavati.

Podržani su scenariji sljedeći:

„Komunikacijski profil 1.: Provjera na cesti upotrebom čitača komunikacije ranog otkrivanja na daljinu u okviru bežičnog komunikacijskog sustava kratkog dometa čime se pokreće fizički pregled na cesti (načelo ‚nadređen-podređen').

Profil čitača 1.a: putem ručnog usmjerenog ili privremeno postavljenog uz cestu i usmjerenog čitača komunikacije ranog otkrivanja na daljinu

Profil čitača 1.b: putem ugrađenog u vozilu i usmjerenog čitača komunikacije ranog otkrivanja na daljinu".

4.1.1 *Preduvjeti za prijenos podataka putem sučelja DSRC-a na frekvenciji od 5,8 GHz*

NAPOMENA: Za razumijevanje konteksta ovih preduvjeta čitatelja se upućuje na sliku 14.3. u nastavku.

4.1.1.1 Podatci sadržani u jedinici u vozilu (VU)

DSC_12 VU je zadužen za ažuriranje svakih 60 sekundi i za održavanje podataka koji se pohranjuju u VU-u, bez uključivanja funkcije komunikacije DSRC-a. Način na koji se to postiže unutarnji je u odnosu na VU i naveden je u Uredbi (EU) br. 165/2014 Prilogu I.C odjeljku 3.19., „Komunikacija na daljinu za ciljane provjere na cesti", no nije naveden u ovom Dodatku.

4.1.1.2 Podatci koji se šalju uređaju DSRC-VU

DSC_13 VU je zadužen za ažuriranje tahografskih podataka DSRC-a (podataka) svaki put kad se podatci pohranjeni u VU-u ažuriraju u intervalu određenom u odjeljku 4.1.1.1. (DSC_12), bez uključivanja funkcije komunikacije DSRC-a.

DSC_14 Podatci VU-a upotrebljavaju se kao osnova za popunjavanje i ažuriranje podataka, a način na koji se to postiže naveden je u Prilogu I.C odjeljku 3.19., „Komunikacija na daljinu za ciljane provjere na cesti" ili, ako takva specifikacija ne postoji, čini funkciju izvedbe proizvoda i nije navedena u ovom Dodatku. Izvedba priključka između uređaja DSRC-VU i VU-a opisana je u odjeljku 5.6.

4.1.1.3 Sadržaj podataka

DSC_15 Sadržaj i format podataka takvi su da se nakon dešifriranja strukturiraju i čine dostupnima u obliku i formatu navedenima u odjeljku 5.4.4. ovog Dodatka (Strukture podataka).

4.1.1.4 Iznošenje podataka

DSC_16 Podatci, koji se redovito ažuriraju u skladu s postupcima utvrđenima u odjeljku 4.1.1.1., zaštićuju se prije iznošenja u DSRC-VU te se iznose kao zaštićena vrijednost koncepata podataka za privremenu pohranu u DSRC-VU-u kao trenutačna verzija podataka. Ti se podatci prenose iz VUSM-a u funkciju DSRC-a VUPM. VUSM i VUPM su funkcije i nisu nužno fizički subjekti. Oblik fizičke instance za izvršenje tih funkcija pitanje je izvedbe proizvoda osim ako nije drugačije navedeno u Uredbi (EU) br. 165/2014.

4.1.1.5 Sigurnosni podatci

DSC_17 Sigurnosni podatci (*securityData*), koji obuhvaćaju podatke koje zahtijeva REDCR kako bi dovršio svoju mogućnost dešifriranja podataka, dostavljaju se kako je navedeno u Dodatku 11., Zajednički sigurnosni mehanizmi, te iznose kao vrijednost koncepata podataka za privremenu pohranu u DSRC-VU-u kao trenutačna verzija sigurnosnih podataka *securityData*, u obliku utvrđenom u odjeljku 5.4.4. ovog Dodatka.

4.1.1.6 Podatci VUPM-a dostupni za prijenos sučeljem DSRC-a

DSC_18 Koncept podataka koji mora uvijek biti dostupan u okviru funkcije VUPM-a za DSRC za neposredan prijenos na zahtjev putem REDCR-a utvrđuje se u odjeljku 5.4.4. za potpune specifikacije modula ASN.1.

Opći pregled komunikacijskog profila 1.

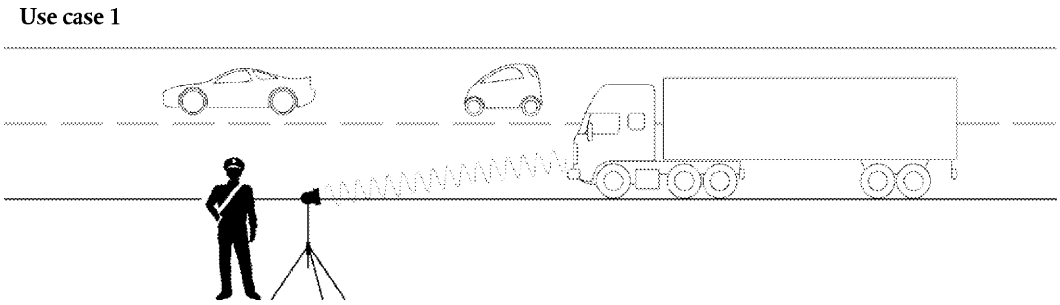
Ovaj profil obuhvaća slučajeve upotrebe u kojima djelatnik nadležnog nadzornog tijela upotrebljava čitač komunikacije ranog otkrivanja na daljinu komunikacijskog sustava kratkog dometa (uz sučelja DSRC-a na frekvenciji od 5,8 GHz koja rade u skladu s preporukom ERC 70-03, a ispitana su u odnosu na odgovarajuće parametre norme EN 300 674-1 kako je opisano u odjeljku 5.) (REDCR) za daljinsko utvrđivanje vozila koje bi moglo kršiti odredbe Uredbe (EU) br. 165/2014. Nakon njegova utvrđivanja, djelatnik nadležnog nadzornog tijela koji nadzire ispitivanje donosi odluku o tome treba li vozilo zaustaviti.

4.1.2 *Profil 1.a: putem ručnog usmjerenog ili privremeno postavljenog uz cestu i usmjerenog čitača komunikacije ranog otkrivanja na daljinu*

U ovom slučaju upotrebe djelatnik nadležnog nadzornog tijela nalazi se uz cestu i usmjeruje ručni uređaj, uređaj na postolju ili sličan prijenosni REDCR prema središtu vjetrobranskog stakla ciljanog vozila. Ispitivanja se vrše upotrebom sučelja DSRC-a na frekvenciji od 5,8 GHz koja rade u skladu s preporukom ERC 70-03, a ispitana su u odnosu na odgovarajuće parametre norme EN 300 674-1, kako je opisano u odjeljku 5. Vidjeti sliku 14.1. (slučaj upotrebe 1.).

Slika 14.1.

Ispitivanje uz cestu upotrebom DSRC-a na frekvenciji od 5,8 GHz



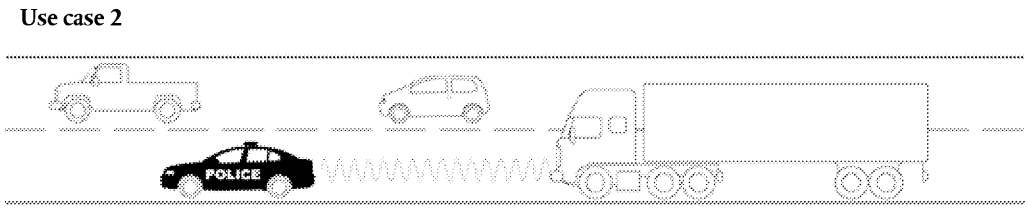
REDCR uz cestu

4.1.3 *Profil 1.b: putem ugrađenog u vozilu i usmjerenog čitača komunikacije ranog otkrivanja na daljinu (REDCR)*

U ovom slučaju upotrebe djelatnik nadležnog nadzornog tijela nalazi se u vozilu koje se kreće te usmjeruje ručni prijenosni REDCR iz vozila prema središtu vjetrobranskog stakla ciljanog vozila, ili je REDCR ugrađen u ili na vozilo kako bi bio usmjeren prema središtu vjetrobranskog stakla ciljanog vozila kada se vozilo s čitačem komunikacije ranog otkrivanja na daljinu nalazi u određenom položaju bitnom za ciljano vozilo (primjerice, izravno ispred kolone vozila u prometu). Ispitivanja se vrše upotrebom sučelja DSRC-a na frekvenciji od 5,8 GHz koja rade u skladu s preporukom ERC 70-03, a ispitana su u odnosu na odgovarajuće parametre norme EN 300 674-1, kako je opisano u odjeljku 5. Vidjeti sliku 14.2. (slučaj upotrebe 2.).

Slika 14.2.

Ispitivanje s pomoću vozila upotrebom DSRC-a na frekvenciji od 5,8 GHz



mobilni REDCR

4.2 **Sigurnost/integritet**

Kako bi se omogućila provjera vjerodostojnosti i integriteta preuzetih podataka putem komunikacije na daljinu, zaštićeni podatci provjeravaju se i dešifriraju u skladu s Dodatkom 11., Zajednički sigurnosni mehanizmi.

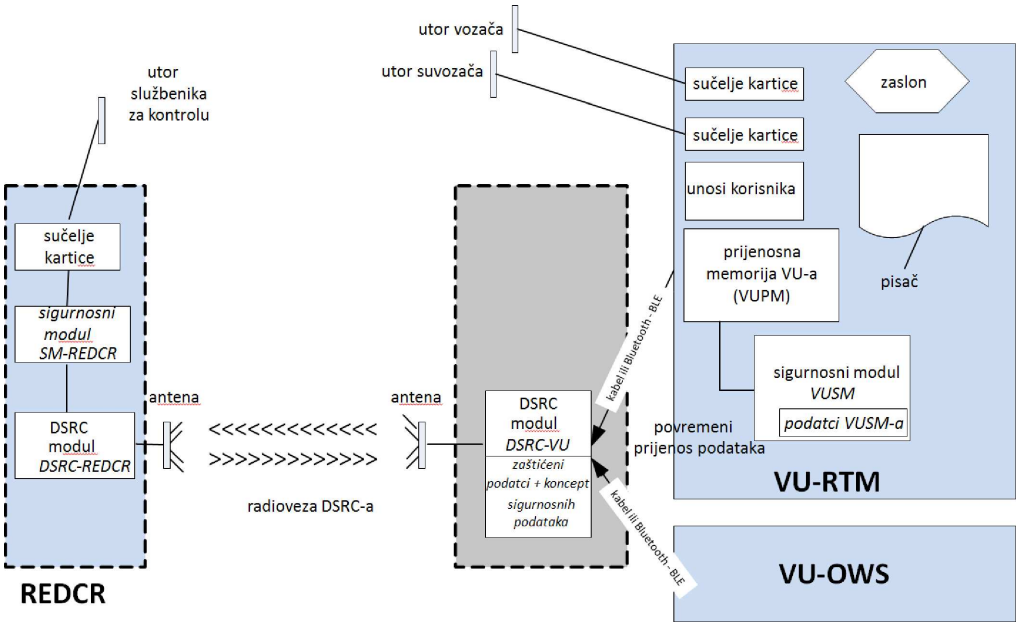
5 IZVEDBA I PROTOKOLI KOMUNIKACIJE NA DALJINU

5.1 **Izvedba**

Izvedba funkcije komunikacije na daljinu u pametnom tahografu prikazana je kako je opisano na slici 14.3.

Slika 14.3.

Izvedba funkcije komunikacije na daljinu



DSC_19 Sljedeće funkcije nalaze se u VU-u:

— Sigurnosni modul (*VUSM*). Ova je funkcija prisutna u VU-u zadužena za zaštitu podataka koji će se prenijeti iz DSRC-VU-a djelatniku nadležnog nadzornog tijela putem komunikacije na daljinu.

— Zaštićeni podatci pohranjuju se u memoriju VUSM-a. U intervalima utvrđenima u odjeljku 4.1.1.1. (DSC_12) VU šifrira i nadopunjuje koncept RTMdata (koji obuhvaća vrijednosti koncepata prenesenih podataka i sigurnosnih podataka utvrđenih u ovom Dodatku) sadržan u memoriji DSRC-VU-a. Rad sigurnosnih modula utvrđen je u Dodatku 11., Zajednički sigurnosni mehanizmi, i nalazi se izvan područja primjene ovog Dodatka, osim ako je to potrebno kako bi se osigurala ažuriranja komunikacijskog uređaja VU-a svaki put kada se podatci iz VUSM-a promijene.

— Komunikacija između VU-a i DSRC-VU-a može biti žična komunikacija ili komunikacija putem sustava Bluetooth niske razine energije (BLE), a DSRC-VU fizički može biti spojen s antenom na vjetrobranskom staklu vozila, u unutrašnjosti VU-a ili negdje između.

— DSRC-VU mora u svakom trenutku imati pouzdan izvor napajanja. Način na koji se DSRC-VU napaja ovisi o njegovoj izvedbi.

— Memorija DSRC-VU-a neizbrisiva je kako bi se podatci zadržali u DSRC-VU-u čak i kada je kontakt vozila isključen.

— Ako se komunikacija između VU-a i DSRC-VU-a ostvaruje putem BLE-a, a izvor napajanja je baterija koja se ne puni ponovno, izvor napajanja DSRC-VU-a zamjenjuje se pri svakom periodičnom pregledu, a odgovornost je proizvođača opreme za DSRC-VU da osigura prikladno napajanje kako bi trajalo od jednog periodičnog pregleda do sljedećeg periodičnog pregleda te da se pritom održava uobičajen pristup podatcima putem REDCR-a tijekom čitava razdoblja bez pogrešaka ili prekida u radu.

— Uređaj VU RTM za „prijenosnu memoriju” (*VUPM*). Ova je funkcija prisutna u VU-u zadužena za slanje i ažuriranje podataka. Sadržaj podataka („TachographPayload”) utvrđuje se u odjeljcima 5.4.4. i 5.4.5. u nastavku i ažurira u intervalu određenom u odjeljku 4.1.1.1. (DSC_12).

— DSRC-VU. Riječ je o funkciji antene ili s antenom povezanoj funkciji koja je u komunikaciji s VU-om putem žičnog ili bežičnog (BLE) priključka i koja zadržava trenutačne podatke (VUPM-podatke) i upravlja odgovorom na ispitivanje putem medija DSRC-a na frekvenciji od 5,8 GHz. Isključenje uređaja DSRC ili ometanje rada uređaja DSRC tijekom uobičajenog rada vozila smatra se kršenjem Uredbe (EU) br. 165/2014.

— Sigurnosni modul (REDCR) (SM-REDCR) funkcija je koja se upotrebljava za dešifriranje i provjeru integriteta podataka koji potječu iz VU-a. Način na koji se to postiže utvrđen je u Dodatku 11., Zajednički sigurnosni mehanizmi, te nije definiran u ovom Dodatku.

— Funkcija uređaja DSRC-a (REDCR) (*DSRC-REDCR*) obuhvaća primopredajnik koji radi na frekvenciji od 5,8 GHz i povezani ugrađeni program te softver koji upravlja komunikacijom s DSRC-VU-om u skladu s ovim Dodatkom.

— DSRC-REDCR ispituje DSRC-VU ciljanog vozila i dobiva podatke (trenutačne VUPM-podatke o ciljanom vozilu) putem veze i postupaka u okviru DSRC-a te pohranjuje primljene podatke u svoj SM-REDCR.

— Antena DSRC-VU-a postavlja se na mjesto koje omogućuje optimalnu komunikaciju DSRC-a između vozila i antene uz cestu (obično u središte ili blizu središta vjetrobranskog stakla vozila). U slučaju lakih vozila prikladna je ugradnja na gornji dio vjetrobranskog stakla.

— Ispred ili u blizini antene ne smije biti nikakvih metalnih predmeta (npr. tablica s imenima, naljepnica, antireflektirajućih zaštitnih folija (za zatamnjivanje), štitnika od sunca, brisača za vjetrobransko staklo) koji mogu ometati komunikaciju.

— Antena se postavlja tako da je njezin smjer maksimalnog zračenja otprilike paralelan s površinom ceste.

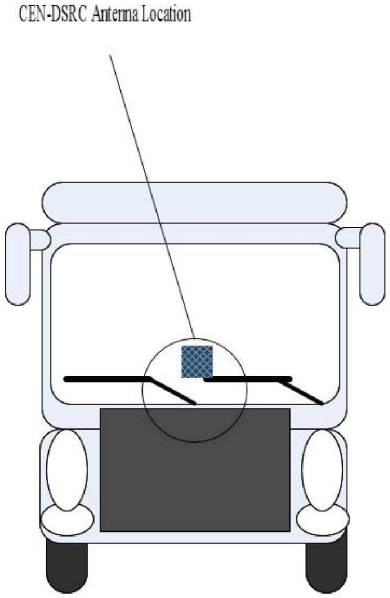
DSC_20 Antena i komunikacija rade u skladu s preporukom ERC 70-03, a ispitane su u odnosu na odgovarajuće parametre norme EN 300 674-1 kako je opisano u odjeljku 5. Antena i komunikacija mogu primijeniti tehnike ublažavanja rizika od interferencija u bežičnoj vezi kako je opisano u izvješću ECC-a 228, npr. primjenom filtara u komunikaciji CEN DSRC na frekvenciji od 5,8 Ghz.

DSC_21 Antena DSRC-a spaja se s uređajem DSRC-VU izravno unutar modula postavljenog na ili blizu vjetrobranskog stakla, ili putem namjenskog kabela izrađenog tako da otežava nezakonito isključenje. Isključenje ili ometanje rada antene smatraju se kršenjem Uredbe (EU) br. 165/2014. Namjerno prekrivanje ili drugačije štetno utjecanje na radnu učinkovitost antene smatra se kršenjem Uredbe (EU) br. 165/2014.

DSC_22 Faktor oblika antene nije utvrđen i ovisi o komercijalnoj odluci pod uvjetom da ugrađeni DSRC-VU ispunjava zahtjeve u pogledu sukladnosti utvrđene u odjeljku 5. u nastavku. Antena se postavlja kako je utvrđeno u DSC_19 i prikazano na slici 14.4. (ovalna linija) te učinkovito podržava slučajeve upotrebe opisane u odjeljcima 4.1.2. i 4.1.3.

Slika 14.4.

Primjer postavljanja antene DSRC-a s frekvencijom od 5,8 GHz na vjetrobransko staklo reguliranih vozila



Faktor oblika REDCR-a i njegove antene može se razlikovati u skladu s okolnostima čitača (na postolju, ručni, ugrađen u vozilo itd.) i načinom rada koji primjenjuje djelatnik nadležnog nadzornog tijela.

Funkcija prikaza i/ili obavijesti upotrebljava se za iznošenje rezultata funkcije komunikacije na daljinu djelatniku nadležnog nadzornog tijela. Prikaz se može osigurati na zaslonu, u obliku ispisa na papiru, zvučnog signala ili kombinacije takvih obavijesti. Oblik takvog prikaza i/ili obavijesti pitanje je zahtjeva djelatnika nadležnog nadzornog tijela i izvedbe opreme te nije naveden u ovom Dodatku.

DSC_23 Izvedba i faktor oblika REDCR-a ovise o komercijalnoj izvedbi, koja je u skladu s preporukom ERC 70-03, te specifikacijama za izvedbu i učinkovitost utvrđenima u ovom Dodatku (odjeljku 5.3.2.) čime se tržištu omogućuje maksimalna razina fleksibilnosti za izradu i osiguravanje opreme kako bi se ispunile određene potrebe u pogledu specifičnih scenarija ispitivanja svakog pojedinog nadležnog nadzornog tijela.

DSC_24 Izvedba i faktor oblika DSRC-VU-a te njegovo postavljanje unutar ili izvan VU-a ovise o komercijalnoj izvedbi koja je u skladu s preporukom ERC 70-03 i specifikacijama u pogledu izvedbe i učinkovitosti utvrđenima u ovom Dodatku (odjeljku 5.3.2.) te u ovoj točki (5.1.).

DSC_25 Međutim, DSRC-VU mora biti sposoban u razumnoj mjeri prihvaćati vrijednosti koncepata podataka iz ostale pametne opreme vozila s pomoću veza i protokola u skladu s otvorenim industrijskim normama. To treba biti moguće, primjerice, iz opreme za vaganje u vozilu, pod uvjetom da se takvi koncepti podataka utvrde s pomoću jedinstvenih i prepoznatljivih identifikatora aplikacija ili naziva datoteka, a upute za rukovanje tim protokolima stavljaju se na raspolaganje Europskoj komisiji i proizvođačima odgovarajuće opreme bez naknade.

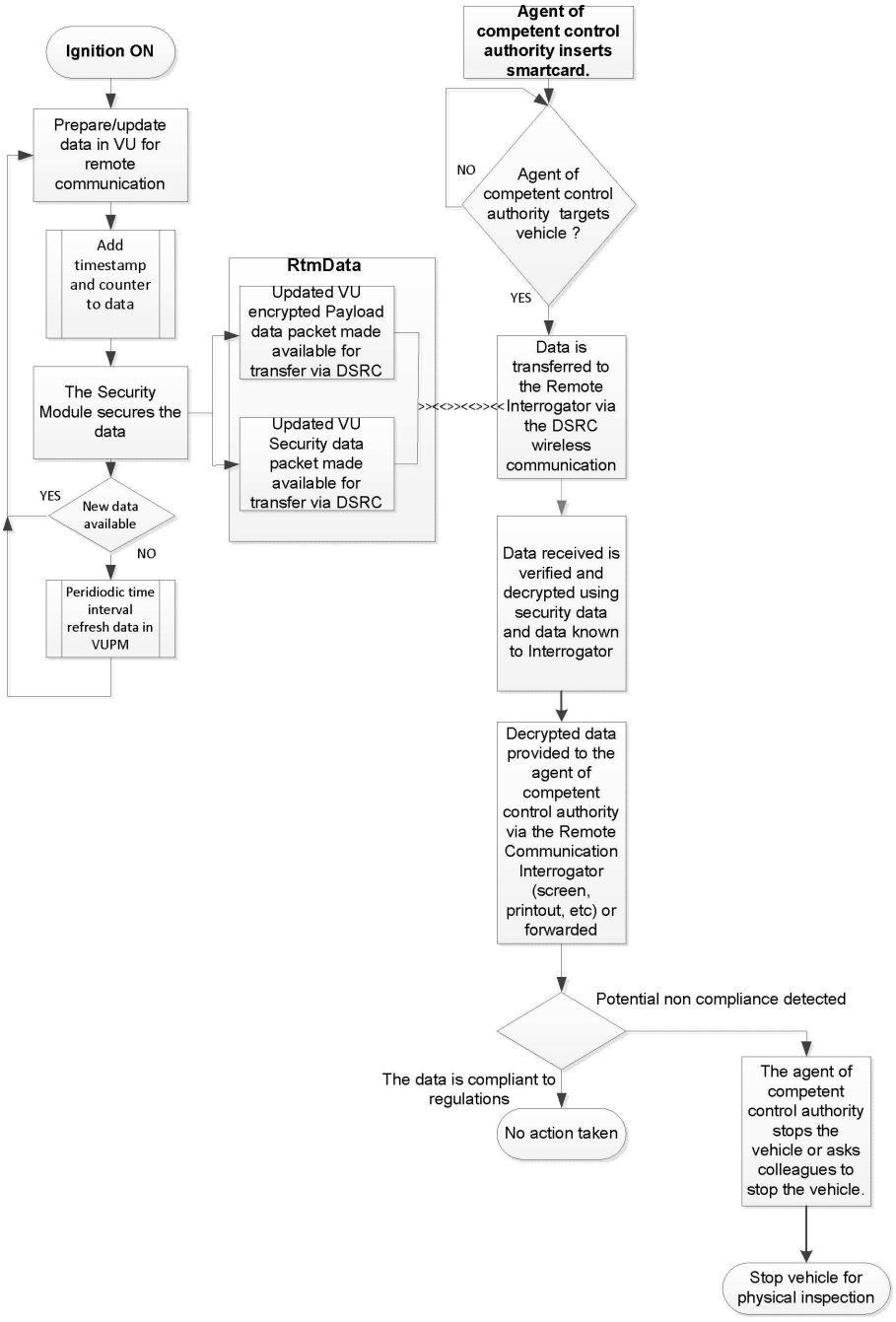
5.2 Tijek rada

5.2.1 *Radnje*

Tijek rada za radnje prikazan je na slici 14.5.

Slika 14.5.

Tijek rada funkcije komunikacije na daljinu



Koraci su opisani u nastavku:

a. Kad god vozilo radi (kontakt UKLJUČEN), tahograf šalje podatke funkciji VU-a. Funkcija VU-a priprema podatke za funkciju komunikacije na daljinu (šifrirane) i ažurira VUPM sadržan u memoriji DSRC-VU-a (kako je utvrđeno u odjeljcima 4.1.1.1. i 4.1.1.2.). Prikupljeni podatci formatiraju se kako je utvrđeno u odjeljcima 5.4.4. i 5.4.5. u nastavku.

b. Svaki put kada se podatci ažuriraju, ažurira se i vremenska oznaka utvrđena u konceptu sigurnosnih podataka.

c. Funkcija VUSM-a zaštićuje podatke u skladu s postupcima utvrđenima u Dodatku 11.

d. Svaki put kada se podatci ažuriraju (vidjeti odjeljke 4.1.1.1. i 4.1.1.2.), prenose se u DSRC-VU gdje zamjenjuju sve prethodne podatke kako bi ažurirani trenutačni podatci uvijek bili dostupni za slanje u slučaju ispitivanja s pomoću *REDCR-a*. Kada ih VU dostavi DSRC-VU-u, podatci se prepoznaju prema nazivu datoteke RTMData ili prema identifikatorima ApplicationID i Attribute.

e. Ako djelatnik nadležnog nadzornog tijela želi ciljati vozilo i prikupiti podatke iz ciljanog vozila, djelatnik nadležnog nadzornog tijela prvo umeće svoju pametnu karticu u REDCR kako bi se omogućila komunikacija i kako bi SM-REDCR mogao provjeriti njezinu vjerodostojnost i dešifrirati podatke.

f. Djelatnik nadležnog nadzornog tijela zatim cilja vozilo i zahtijeva podatke putem komunikacije na daljinu. REDCR otvara razmjenu podataka između sučelja DSRC-a na frekvenciji od 5,8 GHz i DSRC-VU-a ciljanog vozila te zahtijeva podatke. Podatci se prenose REDCR-u putem bežičnog komunikacijskog sustava kao atribut DSRC-a primjenom usluge aplikacije GET kako je utvrđeno u odjeljku 5.4. Atribut sadržava šifrirane vrijednosti prenesenih podataka i sigurnosne podatke DSRC-a.

g. Podatke analizira oprema REDCR-a te se šalju djelatniku nadležnog nadzornog tijela.

h. Djelatnik nadležnog nadzornog tijela upotrebljava podatke kao pomoć u donošenju odluke o tome hoće li zaustaviti vozilo radi detaljnog pregleda ili zatražiti od drugog djelatnika nadležnog nadzornog tijela da zaustavi vozilo.

5.2.2 *Tumačenje podataka primljenih putem komunikacije DSRC-a*

DSC_26 Podatci primljeni putem sučelja na frekvenciji od 5,8 GHz nose samo i isključivo značenje i format utvrđene u odjeljcima 5.4.4. i 5.4.5. u nastavku i tumače se u okviru ondje utvrđenih ciljeva. U skladu s odredbama Uredbe (EU) br. 165/2014, podatci se upotrebljavaju isključivo za pružanje bitnih informacija nadležnom nadzornom tijelu i služe im kao pomoć u donošenju odluke o tome koje vozilo treba zaustaviti radi fizičkog pregleda, a potom se uništavaju u skladu s člankom 9. Uredbe (EU) br. 165/2014.

5.3 **Parametri fizičkog sučelja DSRC-a za komunikaciju na daljinu**

5.3.1 *Ograničenja u pogledu lokacije*

DSC_27 Ispitivanje vozila na daljinu primjenom sučelja DSRC-a na frekvenciji od 5,8 GHz ne bi se trebalo provoditi unutar 200 metara od operativnog pokretnog postolja DSRC-a na frekvenciji od 5,8 GHz.

5.3.2 *Parametri silazne i uzlazne veze*

DSC_28 Oprema koja se upotrebljava za praćenje tahografa na daljinu mora biti usklađena i raditi u skladu s preporukom ERC 70-03 i parametrima utvrđenima u tablicama 14.1. i 14.2. u nastavku.

DSC_29 Nadalje, kako bi se osigurala sukladnost s operativnim parametrima ostalih normiranih sustava DSRC-a na frekvenciji od 5,8 GHz, oprema koja se upotrebljava za praćenje tahografa na daljinu mora biti usklađena s parametrima normi EN 12253 i EN 13372.

To su:

Tablica 14.1.

Parametri silazne veze

Točka br.	Parametar	Vrijednost(i)	Napomena
D1	Frekvencije nosača silazne veze	Postoje četiri mogućnosti koje može upotrebljavati REDCR: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	U skladu s preporukom ERC 70-03. Frekvencije nosača može odabrati provoditelj sustava uz cestu i ne moraju biti poznate u DSRC-VU-u. (U skladu s normama EN 12253, EN 13372)
D1a (*)	Dopušteno odstupanje nosača Frekvencije	unutar ± 5 ppm	(U skladu s normom EN 12253)
D2 (*)	Spektralna maska prijenosnika RSU-a (REDCR-a)	U skladu s preporukom ERC 70-03. REDCR je u skladu s razredima B i C, kako je utvrđeno u normi EN 12253. Nema drugih specifičnih zahtjeva u okviru ovog Priloga.	Parametar koji se upotrebljava za nadzor interferencije između REDCR-ova u blizini (kako je utvrđeno u normama EN 12253 i EN 13372).
D3	Najmanji raspon frekvencije OBU-a (DSRC-VU-a)	5,795 – 5,815 GHz	(U skladu s normom EN 12253)
D4 (*)	Najveći EIRP	U skladu s preporukom ERC 70-03 (nelicenciran) i u skladu s nacionalnim propisima Najviše +33 dBm	(U skladu s normom EN 12253)
D4a	Kutna maska za EIRP	U skladu s objavljenom specifikacijom proizvođača REDCR-a	(U skladu s normom EN 12253)
D5	Polarizacija	Lijeva kružna	(U skladu s normom EN 12253)
D5a	Križna polarizacija	XPD: U smjeru maksimalnog zračenja: (REDCR) RSU t ≥ 15 dB (DSRC-VU) OBU r ≥ 10 dB Na području od −3 dB: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(U skladu s normom EN 12253)
D6 (*)	Modulacija	Dvorazinska amplitudna modulacija	(U skladu s normom EN 12253)
D6a (*)	Indeks modulacije	0,5 ... 0,9	(U skladu s normom EN 12253)

Točka br.	Parametar	Vrijednost(i)	Napomena
D6b	Otvor oka	≥ 90 % (vrijeme) / ≥ 85 % (amplituda)	
D7 (*)	Kodiranje podataka	FM0 Bit „1” ima prijelaze samo na početku i kraju intervala bita. Bit „0” ima dodatne prijelaze u sredini intervala bita u usporedbi s bitom „1”.	(U skladu s normom EN 12253)
D8 (*)	Brzina bita	500 kBit/s	(U skladu s normom EN 12253)
D8a	Dopušteno odstupanje brojača bitova	više od ± 100 ppm	(U skladu s normom EN 12253)
D9	Brzina pogreške bita (BER) za komunikaciju	≤ 10^{-6} kada je ulazno napajanje u OBU-u (DSRC-VU-u) u rasponu navedenom [od D11a do D11b].	(U skladu s normom EN 12253)
D10	Okidač za ponovno pokretanje OBU-a (DSRC-VU-a)	OBU (DSRC-VU) ponovno se pokreće nakon primanja okvira s 11 ili više okteta (uključujući preambulu).	Nije potreban nikakav poseban uzorak ponovnog pokretanja. DSRC-VU se može ponovno pokrenuti nakon primanja okvira s manje od 11 okteta. (U skladu s normom EN 12253)
D10a	Najveće vrijeme početka	≤ 5 ms	(U skladu s normom EN 12253)
D11	Komunikacijska zona	Područje unutar kojeg se postiže BER u skladu s D9.	(U skladu s normom EN 12253)
D11a (*)	Ograničenje napajanja za komunikaciju (gornje)	– 24 dBm	(U skladu s normom EN 12253)
D11b (*)	Ograničenje napajanja za komunikaciju (donje)	Ulazno napajanje: – 43 dBm (smjer maksimalnog zračenja) – 41 dBm (unutar – 45° do + 45°, što odgovara ravnini paralelnoj s površinom ceste kada se DSRC-VU naknadno ugrađuje u vozilo (azimut))	(U skladu s normom EN 12253) Prošireni zahtjev za vodoravne kutove do ± 45° zbog slučajeva upotrebe utvrđenih u ovom Prilogu.
D12 (*)	Razina prekida napajanja DSRC-VU-a	– 60 dBm	(U skladu s normom EN 12253)
D13	Preambula	Preambula je obvezna.	(U skladu s normom EN 12253)
D13a	Duljina i uzorak preambule	16 bitova ± 1 bit bitova „1” kodiranih putem FM0	(U skladu s normom EN 12253)

Točka br.	Parametar	Vrijednost(i)	Napomena
D13b	Valni oblik preambule	Naizmjenični slijed niske razine i visoke razine uz trajanje impulsa od 2 μs. Dopušteno odstupanje navedeno je u D8a.	(U skladu s normom EN 12253)
D13c	Prateći bitovi	RSU (REDCR) smije prenijeti najviše 8 bitova nakon oznake završetka. OBU (DSRC-VU) ne treba uzeti u obzir takve dodatne bitove.	(U skladu s normom EN 12253)

(*) Parametri silazne veze podložni su ispitivanju sukladnosti u skladu s mjerodavnim ispitivanjem parametara iz norme EN 300 674-1.

Tablica 14.2.

Parametri uzlazne veze

Točka br.	Parametar	Vrijednost(i)	Napomena
U1 (*)	Frekvencije podnosača	OBU (DSRC-VU) podržava 1,5 MHz i 2,0 MHz. RSU (REDCR) podržava 1,5 MHz ili 2,0 MHz ili oboje. U1-0: 1,5 MHz U1-1: 2,0 MHz	Odabir frekvencije podnosača (1,5 MHz ili 2,0 MHz) ovisi o odabranom profilu iz norme EN 13372.
U1a (*)	Dopušteno odstupanje frekvencija podnosača	unutar ± 0,1 %	(U skladu s normom EN 12253)
U1b	Upotreba bočnih pojaseva	Isti podatci na obje strane	(U skladu s normom EN 12253)
U2 (*)	Spektralna maska prijenosnika OBU-a (DSRC-VU-a)	U skladu s normom EN12253 1. ulazno napajanje: vidjeti normu ETSI EN 300674-1; 2. izlazno napajanje: [U4a] dBm u 500 kHz; 3. emisija u bilo koji drugi uzlazni kanal: U2(3)-1 = – 35 dBm u 500 kHz	(U skladu s normom EN 12253)
U4a (*)	Najveći jedinstveni bočni pojas EIRP-a (smjer maksimalnog zračenja)	Dvije mogućnosti: U4a-0: – 14 dBm U4a-1: – 21 dBm	U skladu s objavljenom specifikacijom proizvođača opreme
U4b (*)	Najveći jedinstveni bočni pojas EIRP-a (35°)	Dvije mogućnosti: — nije primjenjivo — – 17 dBm	U skladu s objavljenom specifikacijom proizvođača opreme
U5	Polarizacija	Lijeva kružna	(U skladu s normom EN 12253)

Točka br.	Parametar	Vrijednost(i)	Napomena
U5a	Križna polarizacija	XPD: U smjeru maksimalnog zračenja: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB Na − 3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(U skladu s normom EN 12253)
U6	Modulacija podnosača	2-PSK Kodirani podatci sinkronizirani s podnosačem: prijelazi kodiranih podataka podudaraju se s prijelazima podnosača.	(U skladu s normom EN 12253)
U6b	Radni ciklus	Radni ciklus: 50 % ± α, α ≤ 5 %	(U skladu s normom EN 12253)
U6c	Modulacija na nosaču	Multiplikacija moduliranog podnosača s nosačem	(U skladu s normom EN 12253)
U7 (*)	Kodiranje podataka	NRZI (nema prijelaza na početku bita „1”, prijelazi na početku bita „0”, nema prijelaza unutar bita)	(U skladu s normom EN 12253)
U8 (*)	Brzina bita	250 kbit/s	(U skladu s normom EN 12253)
U8a	Dopušteno odstupanje brojača bitova	Unutar ± 1 000 ppm	(U skladu s normom EN 12253)
U9	Brzina pogreške bita (eng. *Bit Error Rate*, BER) za komunikaciju	≤ 10^{-6}	(U skladu s normom EN 12253)
U11	Komunikacijska zona	Područje unutar kojeg se nalazi DSRC-VU tako da njegove prijenose prima REDCR s BER-om manjim od navedenog u U9a.	(U skladu s normom EN 12253)
U12a (*)	Dobitak pretvorbe (donja granica)	1 dB za svaki bočni pojas Raspon kuta: kružno simetričan između smjera maksimalnog zračenja i ± 35°	
		i unutar − 45° do + 45°, što odgovara ravnini paralelnoj s površinom ceste kada se DSRC-VU naknadno ugrađuje u vozilo (azimut).	Veći od navedene vrijednosti raspona za vodoravne kutove do ± 45° zbog slučajeva upotrebe utvrđenih u ovom Prilogu.
U12b (*)	Dobitak pretvorbe (gornja granica)	10 dB za svaki bočni pojas	Manji od određenog raspona vrijednosti za svaki bočni pojas unutar kružnog stošca oko smjera maksimalnog zračenja kuta otvaranja od ± 45°.
U13	Preambula	Preambula je obvezna.	(U skladu s normom EN 12253)

Točka br.	Parametar	Vrijednost(i)	Napomena
U13a	Preambula Duljina i uzorak	32 do 36 µs isključivo uz modulaciju podnosača, zatim 8 bitova „0” kodiranih putem NRZI-a	(U skladu s normom EN 12253)
U13b	Prateći bitovi	DSRC-VU smije prenijeti najviše 8 bitova nakon oznake završetka. RSU (REDCR) ne treba uzeti u obzir takve dodatne bitove.	(U skladu s normom EN 12253)

(*) Parametri uzlazne veze podložni ispitivanju sukladnosti u skladu s mjerodavnim ispitivanjem parametara iz norme EN 300 674-1.

5.3.3 *Izvedba antene*

5.3.3.1 Antena REDCR-a

DSC_30 Izvedba antene REDCR-a ovisi o komercijalnoj izvedbi koja je u skladu s ograničenjima utvrđenima u odjeljku 5.3.2., prilagođenoj radi optimizacije učinkovitosti očitavanja DSRC-REDCR-a za određenu svrhu i okolnosti očitavanja za koje je REDCR izrađen i u kojima mora raditi.

5.3.3.2 Antena VU-a

DSC_31 Izvedba antene DSRC-VU-a ovisi o komercijalnoj izvedbi koja je u skladu s ograničenjima utvrđenima u odjeljku 5.3.2., prilagođenoj radi optimizacije učinkovitosti očitavanja DSRC-REDCR-a za određenu svrhu i okolnosti očitavanja za koje je *REDCR* izrađen i u kojima mora raditi.

DSC_32 Antena VU-a pričvršćuje se ili postavlja na prednje vjetrobransko staklo vozila ili blizu njega, kako je navedeno u odjeljku 5.1.

DSC_33 U ispitnom okruženju radionice (vidjeti odjeljak 6.3.) antena DSRC-VU-a, pričvršćena u skladu s odjeljkom 5.1., učinkovito se povezuje s normiranom ispitnom komunikacijom te učinkovito osigurava transakcije RTM-a kako je utvrđeno u ovom Dodatku, na udaljenosti između 2 i 10 metara, tijekom najmanje 99 % vremena, izračunano kao prosjek na temelju 1 000 ispitivanja s pomoću čitača.

5.4 **Zahtjevi u pogledu protokola DSRC-a za RTM**

5.4.1 *Pregled*

DSC_34 Protokol transakcije za preuzimanje podataka putem veze sučelja DSRC-a na frekvenciji od 5,8 GHz mora biti u skladu sa sljedećim koracima. U ovom je odjeljku opisan tijek transakcije u idealnim uvjetima bez ponovnih prijenosa ili prekida komunikacije.

NAPOMENA Svrha faze inicijalizacije (1. korak) uspostavljanje je komunikacije između REDCR-a i DSRC-VU-ova koji su ušli u transakcijsko područje DSRC-a na frekvenciji od 5,8 GHz (u skladu s načelom odnosa „nadređen – podređen”), ali još nisu uspostavili komunikaciju s REDCR-om, te slanje obavijesti o procesima uređaja.

— **1. korak** Inicijalizacija. REDCR šalje okvir koji sadržava „tablicu s uslugama radiofara” (BST) koja uključuje identifikatore aplikacije (AID-ove) na popisu usluga koji podržava. U aplikaciji RTM-a to će jednostavno biti usluga s vrijednošću AID = 2 (Freight&Fleet). DSRC-VU ocjenjuje primljeni BST i odgovara (vidjeti u nastavku) popisom podržanih aplikacija unutar domene Freight&Fleet, ili ne odgovara ako nijedna aplikacija nije podržana. Ako *REDCR* ne ponudi vrijednost AID = 2, DSRC-VU ne odgovara REDCR-u.

— **2. korak** DSRC-VU šalje okvir koji sadržava zahtjev za dodjelu privatnog prozora.

— **3. korak** REDCR šalje okvir koji sadržava dodjelu privatnog prozora.

— **4. korak** DSRC-VU upotrebljava dodijeljeni privatni prozor za slanje okvira koji sadržava tablicu usluga vozila (VST). VST uključuje popis različitih instanci aplikacija koje DSRC-VU podržava u okviru vrijednosti AID = 2. Različite instance utvrđuju se s pomoću EID-ova generiranih na jedinstven način, a svaka je povezana s vrijednošću parametra kontekstualne oznake aplikacije koja označava podržanu aplikaciju i normu.

— **5. korak** Zatim REDCR analizira ponuđeni VST i prekida vezu (RELEASE) jer mu nije potrebno ništa od onoga što nudi VST (odnosno prima VST iz DSRC-VU-a koji ne podržava transakciju RTM-a) ili, u slučaju da prima odgovarajući VST, pokreće instancu uređaja.

— **6. korak** Kako bi se to provelo, REDCR šalje okvir koji sadržava naredbu za dohvat podataka RTM-a i koji utvrđuje instancu aplikacije RTM-a određivanjem identifikatora koji odgovara instanci aplikacije RTM-a (kako je navedeno u okviru DSRC-VU-a u VST-u) te dodjeljuje privatni prozor.

— **7. korak** DSRC-VU upotrebljava novi dodijeljeni privatni prozor za slanje okvira koji sadržava navedeni identifikator koji odgovara instanci aplikacije RTM-a kako je navedeno u VST-u, a slijedi ga atribut RtmData (prijenosni element + sigurnosni element).

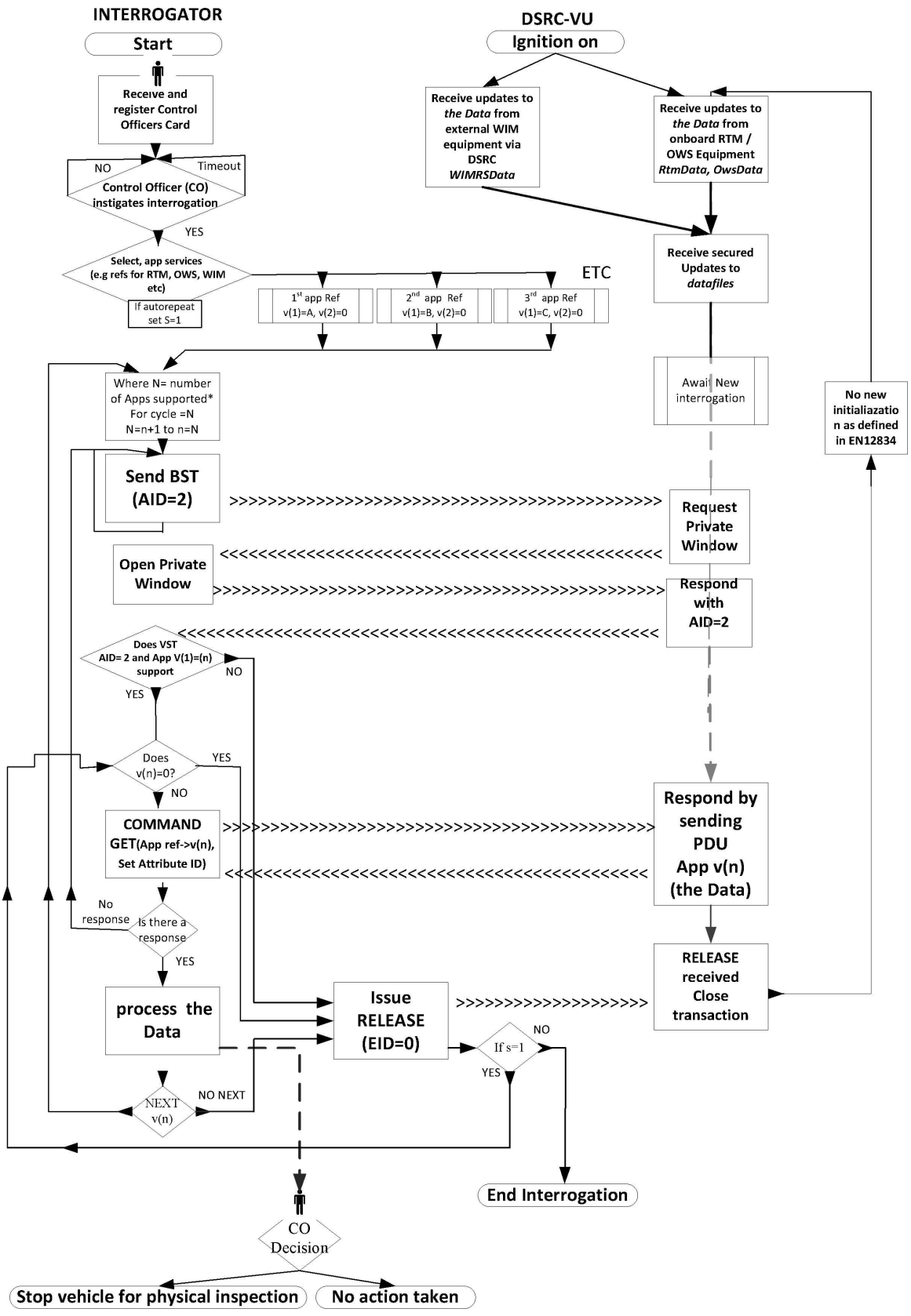
— **8. korak** Ako se zatraži veći broj usluga, vrijednost „n” mijenja se na sljedeći referentni broj usluge, a postupak se ponavlja.

— **9. korak** REDCR potvrđuje primitak podataka slanjem okvira koji sadržava naredbu RELEASE DSRC-VU-u za prekid razmjene podataka ili se, u slučaju da potvrđivanje uspješnog primitka LDPU-a nije uspjelo, vraća na 6. korak.

Slikovni opis protokola transakcije prikazan je na slici 14.6.

Slika 14.6.

Tijek postupka RTM-a putem DSRC-a na frekvenciji od 5,8 GHz



5.4.2 *Naredbe*

DSC_35 Sljedeće naredbe jedine su funkcije koje se upotrebljavaju u transakcijskoj fazi RTM-a.

— **INITIALISATION.request**: Naredba koju izdaje REDCR u obliku slanja s definicijom aplikacija koje podržava REDCR.

— **INITIALISATION.response**: Odgovor iz DSRC-VU-a kojim se potvrđuje veza i koji sadržava popis podržanih instanci aplikacija sa značajkama i informacijama o tome kako ih riješiti (EID).

— **GET.request**: Naredba, koju REDCR izdaje DSRC-VU-u, u kojoj se navode instance aplikacija koje treba riješiti putem utvrđenog EID-a, kako je primljeno u VST-u, i kojom se DSRC-VU-u nalaže da pošalje jedan ili više odabranih atributa s podatcima. Cilj je naredbe GET da REDCR dobije podatke iz DSRC-VU-a.

— **GET.response**: Odgovor iz DSRC-VU-a koji sadržava zatražene podatke.

— **ACTION.request ECHO**: Naredba kojom se DSRC-VU-u nalaže da vrati podatke iz DSRC-VU-a REDCR-u. Cilj je naredbe ECHO omogućiti radionicama ili uređajima za homologacijska ispitivanja da ispitaju radi li DSRC veza bez potrebe za pristupom sigurnosnim podatcima.

— **ACTION**.response ECHO: Odgovor iz DSRC-VU-a na naredbu ECHO.

— **EVENT_REPORT.request** RELEASE: Naredba kojom se DSRC-VU-u nalaže prekid transakcije. Cilj naredbe RELEASE prekid je razmjene podataka s DSRC-VU-om. Nakon primitka naredbe RELEASE, DSRC-VU ne smije odgovoriti na daljnja ispitivanja u sklopu trenutačne veze. Imajte na umu da se, u skladu s normom EN 12834, DSRC-VU neće dvaput povezati s istim REDCR-om osim u slučaju da se nalazio izvan komunikacijskog područja tijekom razdoblja od 255 sekundi ili u slučaju da je identifikator radiofara REDCR-a promijenjen.

5.4.3 *Slijed naredbi za ispitivanje*

DSC_36 S gledišta slijeda naredbi i odgovora, transakcija je opisana kako slijedi:

Slijed	Pošiljatelj		Primatelj	Opis	Radnja
1	REDCR	>	DSRC-VU	Inicijalizacija komunikacijske veze – zahtjev	REDCR šalje BST
2	*DSRC-VU*	>	*REDCR*	*Inicijalizacija komunikacijske veze – odgovor*	*Ako BST podržava vrijednost AID = 2, DSRC-VU šalje zahtjev za privatni prozor.*
3	REDCR	>	DSRC-VU	Dodjeljuje privatni prozor.	Šalje okvir koji sadržava dodjelu privatnog prozora.
4	*DSRC-VU*	>	*REDCR*	*Šalje VST.*	*Šalje okvir koji sadržava VST.*
5	REDCR	>	DSRC-VU	Šalje GET.request za podatke u atributu za određeni EID.	
6	*DSRC-VU*	>	*REDCR*	*Šalje GET.response sa zatraženim atributom za određeni EID.*	*Šalje atribut (RTMData, OWS-Data...) s podatcima za određeni EID.*

Slijed	Pošiljatelj		Primatelj	Opis	Radnja
7	REDCR	>	DSRC-VU	Šalje GET.request za podatke osim atributa (prema potrebi).	
8	*DSRC-VU*	>	*REDCR*	*Šalje GET.response sa zatraženim atributom.*	*Šalje atribut s podatcima za određeni EID.*
9	REDCR	>	DSRC-VU	Potvrđuje uspješan primitak podataka.	Šalje naredbu RELEASE koja zatvara transakciju.
10	*DSRC-VU*			*Zatvara transakciju.*	

Primjer slijeda transakcije i sadržaja razmijenjenih okvira utvrđen je u odjeljcima 5.4.7. i 5.4.8.

5.4.4 *Strukture podataka*

DSC_37 Semantička struktura podataka pri prolazu sučeljem DSRC-a na frekvenciji od 5,8 GHz u skladu je s opisom u ovom Dodatku. Način na koji su ti podatci strukturirani naveden je u ovoj točki.

DSC_38 Prijenos (podatci RTM-a) sastoji se od ulančavanja

1. podataka EncryptedTachographPayload, što čini šifru TachographPayload kako je utvrđeno u modulu ASN.1 u odjeljku 5.4.5. Način šifriranja opisan je u Dodatku 11.

2. DSRCSecurityData naveden je u Dodatku 11.

DSC_39 Podatci RTM-a rješavaju se kao atribut RTM-a = 1 i prenose se u spremnik RTM-a = 10.

DSC_40 Kontekstualna oznaka RTM-a utvrđuje podržani dio norme u seriji normi TARV (RTM odgovara Dijelu 9.).

Definicija modula ASN.1 za podatke DSRC-a u okviru aplikacije RTM-a utvrđuje se kako slijedi:

```
   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 *Elementi RtmData, provedene radnje i definicije*

DSC_41 Vrijednosti podataka koje treba izračunati VU i koje se upotrebljavaju za ažuriranje zaštićenih podataka u DSRC-VU-u izračunavaju se u skladu s pravilima utvrđenima u tablici 14.3.:

Tablica 14.3.

Elementi RtmData, provedene radnje i definicije

(1) Element podataka RTM-a	(2) Radnja koju provodi VU		(3) Definicija podataka u skladu s modulom ASN.1
RTM1 **Registarska pločica vozila**	VU postavlja vrijednost *tp15638VehicleRegistrationPlate* podatkovnog elementa RTM1 iz zabilježene vrijednosti vrste podataka VehicleRegistrationIdentification kako je utvrđeno u Dodatku 1. *VehicleRegistrationIdentification*	Registarska pločica vozila u obliku skupine znakova	`tp15638VehicleRegstrationPlate LPN, --Registarska pločica vozila uvezena iz ISO 14906 s ograničenjem iz EN 15509, koja je SLIJED koji sadržava oznaku države nakon koje slijede abecedna oznaka i broj registarske pločice, koji je uvijek u obliku 14 okteta (nadopunjenih nulama) tako da je duljina tipa EN 15509 LPN uvijek 17 okteta, od kojih 14 predstavlja "pravi" broj registarske pločice.`

(1) Element podataka RTM-a	(2) Radnja koju provodi VU		(3) Definicija podataka u skladu s modulom ASN.1
RTM2 **Događaj prekoračenja brzine**	VU generira Booleovu vrijednost za varijablu podatkovnog elementa RTM2 tp15638SpeedingEvent. Vrijednost tp15638SpeedingEvent izračunava se s pomoću VU-a iz broja varijabli speedingEvents zabilježenih u VU-u u zadnjih 10 dana pojave kako je utvrđeno u Prilogu I.C. Ako postoji najmanje jedna varijabla tp15638SpeedingEvent zadnjih 10 dana pojave, vrijednost varijable tp15638SpeedingEvent postavlja se na TOČNO (TRUE). ILI ako nije bilo nikakvih događaja u zadnjih 10 dana pojave, vrijednost varijable tp15638SpeedingEvent postavlja se na NETOČNO (FALSE).	1 (TOČNO) – označava nepravilnosti u brzini u zadnjih 10 dana pojave	`tp15638speedingEvent BOOLEAN,`
RTM3 **Vožnja bez valjane kartice**	VU generira Booleovu vrijednost za varijablu podatkovnog elementa RTM3 tp15638DrivingWithoutValidCard. VU dodjeljuje vrijednost TOČNO varijabli tp15638DrivingWithoutValidCard ako je u podatcima VU-a zabilježen najmanje jedan događaj u zadnjih 10 dana pojave vrste događaja „vožnja bez odgovarajuće kartice" kako je utvrđeno u Prilogu I.C. ILI ako nije bilo nikakvih događaja u zadnjih 10 dana pojave, vrijednost varijable tp15638DrivingWithoutValidCard postavlja se na NETOČNO.	1 (TOČNO) = označava nevaljanu upotrebu kartice	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Valjana kartica vozača**	VU generira Booleovu vrijednost za varijablu podatkovnog elementa RTM4 tp15638DriverCard na temelju podataka pohranjenih u VU-u i utvrđenih u Dodatku 1. Ako nije prisutna valjana kartica vozača, VU postavlja varijablu na TOČNO. ILI ako je valjana kartica vozača prisutna, VU postavlja varijablu na NETOČNO.	0 (NETOČNO) = označava valjanu karticu vozača	`tp15638DriverCard BOOLEAN,`
RTM5 **Umetanje kartice tijekom vožnje**	VU generira Booleovu vrijednost za podatkovni element RTM5. VU dodjeljuje vrijednost TOČNO varijabli tp15638CardInsertion ako je u podatcima VU-a u zadnjih 10 dana pojave zabilježena najmanje jedna vrsta događaja „umetanje kartice tijekom vožnje" kako je utvrđeno u Prilogu I.C. ILI ako nije bilo nikakvih događaja u posljednjih 10 dana pojave, vrijednost varijable tp15638CardInsertion postavlja se na NETOČNO.	1 (TOČNO) = označava umetanje kartice tijekom vožnje u zadnjih 10 dana pojave	`tp15638CardInsertion BOOLEAN,`
RTM6 **Pogreška u podatcima o kretanju**	VU generira Booleovu vrijednost za podatkovni element RTM6. VU dodjeljuje vrijednost TOČNO varijabli tp15638MotionDataError ako je u podatcima VU-a u zadnjih 10 dana pojave zabilježena najmanje jedna vrsta događaja „pogreška u podatcima o kretanju" kako je utvrđeno u Prilogu I.C. ILI ako nije bilo nikakvih događaja u posljednjih 10 dana pojave, vrijednost varijable tp15638MotionDataError postavlja se na NETOČNO.	1 (TOČNO) = označava pogrešku u podatcima o kretanju u zadnjih 10 dana pojave.	`tp15638motionDataError BOOLEAN,`

(1) Element podataka RTM-a	(2) Radnja koju provodi VU		(3) Definicija podataka u skladu s modulom ASN.1
RTM7 **Konflikt u kretanju vozila**	VU generira Booleovu vrijednost za podatkovni element RTM7. VU dodjeljuje vrijednost TOČNO varijabli tp15638vehicleMotionConflict ako je u podatcima VU-a zabilježen najmanje jedan događaj u zadnjih 10 dana pojave vrste događaja „konflikt u kretanju vozila" (vrijednost '0A'H). ILI ako nije bilo nikakvih događaja u posljednjih 10 dana pojave, vrijednost varijable tp15638vehicleMotionConflict postavlja se na NETOČNO.	1 (TOČNO) = označava konflikt u kretanju u zadnjih 10 dana pojave.	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Druga kartica vozača**	VU generira Booleovu vrijednost za podatkovni element RTM8 na temelju Priloga I.C („podatci o aktivnosti vozača", POSADA i SUVOZAČ). Ako je druga valjana kartica vozača prisutna, VU postavlja varijablu na TOČNO. ILI ako druga valjana kartica vozača nije prisutna, VU postavlja varijablu na NETOČNO.	1 (TOČNO) = označava umetnutu drugu karticu vozača	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Trenutačna aktivnost**	VU generira Booleovu vrijednost za podatkovni element RTM9. Ako je trenutačna aktivnost zabilježena u VU-u kao bilo koja aktivnost osim „VOŽNJE", kako je utvrđeno u Prilogu I.C, VU postavlja varijablu na TOČNO. ILI ako je trenutačna aktivnost zabilježena u VU-u kao „VOŽNJA", VU postavlja varijablu na NETOČNO.	1 (TOČNO) = odabrana druga aktivnost; 0 (NETOČNO) = odabrana vožnja	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Posljednja razmjena podataka zatvorena**	VU generira Booleovu vrijednost za podatkovni element RTM10. Ako posljednja razmjena podataka kartice nije ispravno zatvorena, kako je utvrđeno u Prilogu I.C, VU postavlja varijablu na TOČNO. ILI ako je posljednja razmjena podataka kartice ispravno zatvorena, VU postavlja varijablu na NETOČNO.	1 (TOČNO) = neispravno zatvorena 0 (NETOČNO) = ispravno zatvorena	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Prekid napajanja**	VU generira vrijednost u obliku cijelog broja za podatkovni element RTM11. VU dodjeljuje vrijednost za varijablu tp15638PowerSupplyInterruption jednaku najduljem razdoblju prekida napajanja u skladu s člankom 9. Uredbe (EU) br. 165/2014 vrste događaja „prekid napajanja" kako je utvrđeno u Prilogu 1.C. ILI ako u posljednjih 10 dana pojave nije bilo nikakvih događaja prekida napajanja, vrijednost u obliku cijelog broja postavlja se na 0.	— broj prekida napajanja u zadnjih 10 dana pojave	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

(1) Element podataka RTM-a	(2) Radnja koju provodi VU		(3) Definicija podataka u skladu s modulom ASN.1
RTM12 **Kvar senzora**	VU generira vrijednost u obliku cijelog broja za podatkovni element RTM10. VU dodjeljuje varijabli sensorFault vrijednost: — 1 ako je događaj vrste „pogreška senzora s rednim brojem ‘35’H” zabilježen u zadnjih10 dana; — 2 ako je događaj vrste „kvar prijamnika GNSS-a” (unutarnjeg ili vanjskog s rednim brojem ‘51’H ili ‘52’H) zabilježen u zadnjih 10 dana; — 3 ako je događaj vrste „kvar vanjskog prijamnika GNSS-a s rednim brojem ‘53’H” zabilježen u zadnjih 10 dana pojave; — 4 ako su „kvar senzora” i „kvar prijemnika GNSS-a” zabilježeni u zadnjih 10 dana pojave; — 5 ako su „kvar senzora” i „kvar vanjskog prijamnika GNSS-a” zabilježeni u zadnjih 10 dana pojave; — 6 ako su „kvar prijamnika GNSS-a” i „kvar vanjskog prijamnika GNSS-a” zabilježeni u zadnjih 10 dana pojave; — 7 ako su sva tri kvara senzora zabilježena u zadnjih 10 dana pojave. ILI će VU dodijeliti vrijednost 0 ako nijedan od tih događaja nije zabilježen u zadnjih 10 dana pojave.	— kvar senzora od jednog okteta u skladu s rječnikom s podatcima	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Prilagodba vremena**	VU generira vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.) za podatkovni element RTM13 na temelju prisutnosti podataka o prilagodbi vremena kako je utvrđeno u Prilogu I.C. VU dodjeljuje vrijednost vremena u kojem se odvio posljednji događaj prilagodbe vremena podataka. ILI ako u podatcima VU-a nije prisutan nijedan događaj „prilagodbe vremena” kako je utvrđeno u Prilogu I.C, VU postavlja vrijednost 0.	Vrijeme posljednje prilagodbe	`tp15638TimeAdjustment` `INTEGER(0..4294967295),`
RTM14 **Pokušaj povrede sigurnosti**	VU generira vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.) za podatkovni element RTM14 na temelju prisutnosti događaja „pokušaj povrede sigurnosti” kako je utvrđeno u Prilogu I.C. VU postavlja vrijednost vremena posljednjeg događaja pokušaja povrede sigurnosti zabilježenog u VU-u. ILI ako u podatcima VU-a nije prisutan nijedan događaj „pokušaj povrede sigurnosti” kako je utvrđeno u Prilogu I.C, VU postavlja vrijednost 0x00FF.	Vrijeme posljednjeg pokušaja povrede — Zadana vrijednost = 0x00FF	`tp15638LatestBreachAttempt` `INTEGER(0..4294967295),`
RTM15 **Posljednja kalibracija**	VU generira vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.) za podatkovni element RTM15 na temelju prisutnosti podataka o posljednjoj kalibraciji kako je utvrđeno u Prilogu I. C. VU postavlja vrijednost vremena posljednjih dviju kalibracija (RTM15 i RTM16) koje su postavljene u podatcima VuCalibrationData utvrđenima u Dodatku 1. VU postavlja vrijednost za RTM15 na timeReal posljednjeg zapisa kalibracije.	Vrijeme podataka posljednje kalibracije	`tp15638LastCalibrationData` `INTEGER(0..4294967295),`

(1) Element podataka RTM-a	(2) Radnja koju provodi VU		(3) Definicija podataka u skladu s modulom ASN.1
RTM16 **Prethodna kalibracija**	VU generira vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.) za podatkovni element RTM16 za zapis kalibracije koja je prethodila zapisu posljednje kalibracije. ILI ako nije bilo prethodne kalibracije, VU postavlja vrijednost RTM16 na 0.	Vrijeme podataka prethodne kalibracije	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Datum povezivanja tahografa**	Za podatkovni element RTM17 VU generira vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.). VU postavlja vrijednost vremena prve ugradnje VU-a. VU izdvaja ove podatke iz VuCalibrationData (Dodatak 1.) iz vuCalibrationRecords uz CalibrationPurpose koja je jednaka: '03'H	Vrijeme povezivanja tahografa	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Trenutačna brzina**	VU generira vrijednost u obliku cijelog broja za podatkovni element RTM18. VU postavlja vrijednost za RTM16 na posljednju trenutačnu zabilježenu brzinu u trenutku posljednjeg ažuriranja RtmData.	Posljednja trenutačna zabilježena brzina	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Vremenska oznaka**	Za podatkovni element RTM19 VU generira vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.). VU postavlja vrijednost za RTM19 na vrijeme posljednjeg ažuriranja RtmData.	Vremenska oznaka trenutačnog zapisa TachographPayload	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Mehanizam prijenosa podataka*

DSC_42 REDCR zahtijeva prethodno utvrđene prenesene podatke nakon faze inicijalizacije, a zatim ih prenosi putem DSRC-VU-a u dodijeljeni prozor. REDCR upotrebljava naredbu GET za dohvaćanje podataka.

DSC_43 Za sve razmjene u DSRC-u podatci se kodiraju primjenom PER-a (pravila paketnog šifriranja, eng. *Packed Encoding Rules*).

5.4.7 *Detaljni opis transakcija u okviru DSRC-a*

DSC_44 Inicijalizacija se provodi prema DSC_44 do DSC_48 i tablicama 14.4. do 14.9. U fazi inicijalizacije REDCR počinje slati okvir koji sadržava BST (tablicu usluga radiofara, eng. *Beacon Service Table*) u skladu s normama EN 12834 i EN 13372, točkama 6.2., 6.3., 6.4. i 7.1., uz postavke kako su navedene u tablici 14.4.

Tablica 14.4

Inicijalizacija – postavke okvira BST-a

Polje	Postavke
Link Identifier	Adresa slanja
BeaconId	U skladu s normom EN 12834
Time	U skladu s normom EN 12834
Profile	Nema proširenja, upotrebljavati 0 ili 1
MandApplications	Nema proširenja, EID nije prisutan, parametar nije prisutan, AID = 2 Freight&Fleet
NonMandApplications	Nije prisutno
ProfileList	Nema proširenja, broj profila na popisu = 0
Fragmentation header	Nema fragmentiranja
Layer 2 settings	Naredba PDU-a, naredba UI-a

Praktični primjer postavki utvrđenih u tablici 14.4. uz oznaku kodiranja bitova naveden je u tablici 14.5. u nastavku.

Tablica 14.5.

Inicijalizacija – primjer sadržaja okvira BST-a

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG	0111 1110	Oznaka početka
2	Broadcast ID	1111 1111	Adresa slanja
3	MAC Control Field	1010 0000	Naredba PDU-a
4	LLC Control field	0000 0011	Naredba UI-a
5	Fragmentation header	1xxx x001	Nema fragmentiranja

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
6	BST	1000	Zahtjev za inicijalizaciju
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	aplikacije NonMand nisu prisutne
		xxx	Identifikator proizvođača
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27-bitni identifikator dostupan za proizvođača
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	Realno vrijeme 32-bitnog sustava UNIX
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,…)	0000 0000	Nema proširenja, primjer profila 0
17	MandApplications SEQUENCE (SIZE(0..127, …)) OF {	0000 0001	Nema proširenja, broj mandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	EID nije prisutan
	OPTION indicator	0	Parametar nije prisutan
	AID DSRCApplicationEntityID } }	00 0010	Nema proširenja, AID = 2 Freight&Fleet

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
19	ProfileList SEQUENCE (0..127,…) OF Profile }	0000 0000	Nema proširenja, broj profila na popisu = 0
20	FCS	xxxx xxxx	Slijed provjere okvira
21		xxxx xxxx	
22	Flag	0111 1110	Oznaka završetka

DSC_45 DSRC-VU, nakon primanja BST-a, šalje zahtjev za dodjelu privatnog prozora kako je navedeno u normama EN 12795 i EN 13372 točki 7.1.1., bez posebnih postavki RTM-a. U tablici 14.6. nalazi se primjer kodiranja bitova.

Tablica 14.6.

Inicijalizacija – sadržaj okvira zahtjeva za dodjelu privatnog prozora

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG	0111 1110	Oznaka početka
2	Private LID	xxxx xxxx	Adresa veze određenog DSRC-VU-a
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Zahtjev za privatni prozor
7	FCS	xxxx xxxx	Slijed provjere okvira
8		xxxx xxxx	
9	Flag	0111 1110	Oznaka završetka

DSC_46 REDCR zatim odgovara dodjeljivanjem privatnog prozora, kako je navedeno u normama EN 12795 i EN 13372, točki 7.1.1., bez posebnih postavki RTM-a.

U tablici 14.7. nalazi se primjer kodiranja bitova.

Tablica 14.7.

Inicijalizacija – sadržaj okvira dodjele privatnog prozora

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG	0111 1110	Oznaka početka
2	Private LID	xxxx xxxx	Adresa veze određenog DSRC-VU-a
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Dodjela privatnog prozora
7	FCS	xxxx xxxx	Slijed provjere okvira
8		xxxx xxxx	
9	Flag	0111 1110	Oznaka završetka

DSC_47 DSRC-VU, nakon primanja dodjele privatnog prozora, šalje svoj VST (tablicu usluga vozila) kako je utvrđeno u normama EN 12834 i EN 13372, točkama 6.2., 6.3., 6.4. i 7.1., uz postavke kako su navedene u tablici 14.8., upotrebom dodijeljenog prozora za prijenos.

Tablica 14.8.

Inicijalizacija – postavke okvira VST-a

Polje	Postavke
Private LID	U skladu s normom EN 12834
VST parameters	Fill = 0, zatim za svaku podržanu aplikaciju: EID prisutan, parametar prisutan, AID = 2, EID kako ga je generirao OBU
Parameter	Nema proširenja, sadržava kontekstualnu oznaku RTM-a
ObeConfiguration	Opcionalno polje ObeStatus može biti prisutno, ali ga REDCR ne smije upotrebljavati.
Fragmentation header	Nema fragmentiranja
Layer 2 settings	Naredba PDU-a, naredba UI-a

DSC_48 DSRC-VU podržava aplikaciju za „Freight and Fleet" kako je utvrđena u okviru identifikatora aplikacije „2". Ostali identifikatori aplikacije mogu biti podržani, no ne smiju biti prisutni u ovom VST-u jer BST zahtijeva isključivo AID = 2. Polje „Aplikacije" sadržava popis podržanih instanci aplikacija u DSRC-VU-u. Za svaku podržanu instancu aplikacije navedeno je upućivanje na odgovarajuću normu, a čini je kontekstualna oznaka RTM-a koja se sastoji od IDENTIFIKATORA OBJEKATA (OBJECT IDENTIFIER) koji predstavlja povezanu normu, njezina dijela (Dijela 9. za RTM) i po mogućnosti njezine verzije te EID-a koji generira DSRC-VU, a povezan je s tom instancom aplikacije.

Praktični primjer postavki utvrđenih u tablici 14.8. uz oznaku kodiranja bitova naveden je u tablici 14.9.

Tablica 14.9.

Inicijalizacija – primjer sadržaja okvira VST-a

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG	0111 1110	Oznaka početka
2	Private LID	xxxx xxxx	Adresa veze određenog DSRC-VU-a
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	Naredba PDU-a
7	LLC Control field	0000 0011	Naredba UI-a
8	Fragmentation header	1xxx x001	Nema fragmentiranja
9	VST SEQUENCE {	1001	Odgovor inicijalizacije
	Fill BIT STRING (SIZE(4))	0000	Neupotrijebljeno i postavljeno na 0
10	Profile INTEGER (0..127,...) Applications SEQUENCE OF {	0000 0000	Nema proširenja, primjer profila 0
11		0000 0001	Nema proširenja, 1 aplikacija
12	SEQUENCE {		
	OPTION indicator	1	EID prisutan
	OPTION indicator	1	Parametar prisutan
	AID DSRCApplicationEntityID	00 0010	Nema proširenja, AID = 2 Freight&-Fleet
13	EID Dsrc-EID	xxxx xxxx	Utvrđen u okviru OBU-a i utvrđuje instancu aplikacije.

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
14	Parameter Container {	0000 0010	Nema proširenja, odabir spremnika = 02, niz okteta
15		0000 1000	Nema proširenja, duljina kontekstualne oznake RTM-a = 8
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	Identifikator objekata podržane norme, dio i verzija. Primjer: ISO (1) norma (0) TARV (15638) Dio 9. (9) verzija 1. (1). Prvi je oktet 06H koji čini identifikator objekata. Drugi je oktet 06H koji čini njegovu duljinu. Sljedećih 6 okteta kodira primjer identifikatora objekta. Imajte na umu da je prisutan samo jedan element slijeda (opcionalni je element RtmCommProfile izostavljen).
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 nije prisutan
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Identifikator proizvođača za DSRC-VU kako je opisano u registru normi ISO 14816
27		xxxx xxxx	
28	FCS	xxxx xxxx	Slijed provjere okvira
29		xxxx xxxx	
30	Flag	0111 1110	Oznaka završetka

DCS_49 REDCR zatim očitava podatke izdavanjem naredbe GET, u skladu s naredbom GET utvrđenom u normi EN 13372, točkama 6.2., 6.3., 6.4., i u normi EN 12834, uz postavke kako su navedene u tablici 14.10.

Tablica 14.10.

Iznošenje –postavke okvira za GET.request

Polje	Postavke
Invoker Identifier (IID)	Nije prisutno
Link Identifier (LID)	Adresa veze određenog DSRC-VU-a
Chaining	Nema

Polje	Postavke
Element Identifier (EID)	Kako je navedeno u VST-u. Nema proširenja.
Access Credentials	Nema
AttributeIdList	Nema proširenja, 1 atribut, AttributeID = 1 (RtmData)
Fragmentation	Nema
Layer2 settings	Naredba PDU-a, provjerena naredba ACn

U tablici 14.11. prikazan je primjer očitavanja podataka RTM-a.

Tablica 14.11.

Iznošenje – primjer okvira za GET.request

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG	0111 1110	Oznaka početka
2	Private LID	xxxx xxxx	Adresa veze određenog DSRC-VU-a
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Naredba PDU-a
7	LLC Control field	n111 0111	Provjerena naredba ACn, n bitova
8	Fragmentation header	1xxx x001	Nema fragmentiranja
9	GET.request SEQUENCE {	0110	GET.request
	OPTION indicator	0	Pristupni podatci nisu prisutni
	OPTION indicator	0	IID nije prisutan
	OPTION indicator	1	AttributeIdList prisutan
	Fill BIT STRING(SIZE(1))	0	Postavljeno na 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	EID instance aplikacije RTM-a kako je navedeno u VST-u. Nema proširenja.
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Nema proširenja, broj atributa = 1
12		0000 0001	AttributeId=1, RtmData. Nema proširenja

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
13	FCS	xxxx xxxx	Slijed provjere okvira
14		xxxx xxxx	
15	Flag	0111 1110	Oznaka završetka

DSC_50 DSRC-VU, nakon primanja naredbe GET.request, šalje naredbu GET.response sa zatraženim podatcima u skladu s naredbom GET.response utvrđenom u normi EN 13372 točkama 6.2., 6.3., 6.4. i u normi EN 12834 uz postavke kako su navedene u tablici 14.12.

Tablica 14.12.

Iznošenje – postavke okvira za GET.response

Polje	Postavke
Invoker Identifier (IID)	Nije prisutno
Link Identifier (LID)	U skladu s normom EN 12834
Chaining	Nema
Element Identifier (EID)	Kako je navedeno u VST-u.
Access Credentials	Nema
Fragmentation	Nema
Layer2 settings	Odgovor PDU-a, odgovor dostupan i naredba prihvaćena, naredba ACn

U tablici 14.13. prikazan je primjer očitavanja podataka RTM-a.

Tablica 14.13.

Iznošenje – primjer sadržaja okvira odgovora

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG	0111 1110	Oznaka početka
2	Private LID	xxxx xxxx	Adresa veze određenog DSRC-VU-a
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
6	MAC Control field	1101 0000	Odgovor PDU-a
7	LLC Control field	n111 0111	Odgovor dostupan, naredba ACn, n bitova
8	LLC Status field	0000 0000	Odgovor dostupan i naredba prihvaćena
9	Fragmentation header	1xxx x001	Nema fragmentiranja
10	GET.response SEQUENCE {	0111	GET.Response
	OPTION indicator	0	IID nije prisutan
	OPTION indicator	1	Popis atributa prisutan
	OPTION indicator	0	Uzvratni status nije prisutan
	Fill BIT STRING(SIZE(1))	0	Ne upotrebljava se
11	EID INTEGER(0..127,…)	xxxx xxxx	Odgovor iz aplikacije RTM-a Instanca. Nema proširenja.
12	AttributeList SEQUENCE OF {	0000 0001	Nema proširenja, broj atributa = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Nema proširenja, AttributeID = 1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Nema proširenja, odabir spremnika = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Slijed provjere okvira
n+2		xxxx xxxx	
n+3	Flag	0111 1110	Oznaka završetka

DSC_51 REDCR zatim zatvara vezu izdavanjem naredbe EVENT_REPORT, RELEASE u skladu s normom EN 13372, točkama 6.2., 6.3., 6.4. i normom EN 12834, točkom 7.3.8., bez posebnih postavki RTM-a. U tablici 14.14. prikazan je primjer kodiranja bitova naredbe RELEASE:

Tablica 14.14.

Prekid. Sadržaj okvira naredbe EVENT_REPORT, RELEASE

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG	0111 1110	Oznaka početka
2	Private LID	xxxx xxxx	Adresa veze određenog DSRC-VU-a
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1000 s000	Okvir sadržava naredbu LPDU.
7	LLC Control field	0000 0011	Naredba UI-a
8	Fragmentation header	1xxx x001	Nema fragmentiranja.
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Pristupni podatci nisu prisutni.
	OPTION indicator	0	Parametar događaja nije prisutan.
	OPTION indicator	0	IID nije prisutan.
	Mode BOOLEAN	0	Ne očekuje se odgovor.
10	EID INTEGER (0..127,…)	0000 0000	Nema proširenja, EID = 0 (sustav)
11	EventType INTEGER (0..127,…) }	0000 0000	Vrsta događaja 0 = RELEASE
12	FCS	xxxx xxxx	Slijed provjere okvira
13		xxxx xxxx	
14	Flag	0111 1110	Oznaka završetka

DSC_52 Ne očekuje se odgovor DSRC-VU-a na naredbu RELEASE. Komunikacija se zatim zatvara.

5.4.8 *Opis ispitivanja transakcija u okviru DSRC-a*

DSC_53 Potpuna ispitivanja koja uključuju zaštitu podataka trebaju provesti, kako je utvrđeno u Dodatku 11., Zajednički sigurnosni mehanizmi, ovlaštene osobe s pristupom sigurnosnim postupcima upotrebom uobičajene naredbe GET kako je utvrđeno u prethodnom tekstu.

DSC_54 Puštanje u pogon i periodička ispitivanja koja zahtijevaju dešifriranje i razumijevanje dešifriranog sadržaja podataka provode se kako je navedeno u Dodatku 11., Zajednički sigurnosni mehanizmi, i Dodatku 9., Homologacija, Popis obveznih ispitivanja.

Međutim, temeljna komunikacija DSRC-a može se ispitati s pomoću naredbe ECHO. Takva ispitivanja mogu biti potrebna pri puštanju u pogon, pri periodičkom pregledu ili drugačije na zahtjev nadležnog nadzornog tijela ili u skladu s Uredbom (EU) br. 165/2014 (vidjeti odjeljak 6. u nastavku).

DSC_55 Kako bi se provelo ovo temeljno komunikacijsko ispitivanje, REDCR izdaje naredbu ECHO tijekom razmjene podataka, odnosno nakon uspješnog dovršetka faze inicijalizacije. Slijed interakcija stoga je sličan slijedu ispitivanja:

— 1. korak REDCR šalje „tablicu usluga radiofara" (BST) koja uključuje identifikatore aplikacije (AID-ove) na popis usluga koji podržava. U aplikacijama RTM-a to će jednostavno biti usluga s vrijednošću AID = 2.

DSRC-VU ocjenjuje primljeni BST i ako utvrdi da BST zahtijeva Freight&Fleet (AID = 2), DSRC-VU odgovara. Ako REDCR ne ponudi vrijednost AID = 2, DSRC-VU zaustavlja svoju transakciju s REDCR-om.

— 2. korak DSRC-VU šalje zahtjev za dodjelu privatnog prozora.

— 3. korak REDCR šalje dodjelu privatnog prozora.

— 4. korak DSRC-VU upotrebljava dodijeljeni privatni prozor za slanje tablice usluga vozila (eng. *Vehicle Service Table*, VST). VST uključuje popis različitih instanci aplikacija koje DSRC-VU podržava u okviru vrijednosti AID = 2. Različite instance utvrđuju se s pomoću jedinstvenih EID-ova, a svaki je povezan s vrijednošću parametra koji označava instancu podržane aplikacije.

— 5. korak Zatim REDCR analizira ponuđeni VST i prekida vezu (RELEASE) jer mu nije potrebno ništa od onoga što nudi VST (odnosno prima VST iz DSRC-VU-a koji nije VU RTM-a, ili, u slučaju da primi odgovarajući VST, pokreće instancu uređaja.

— 6. korak REDCR izdaje naredbu (ECHO) određenom DSRC-VU-u i dodjeljuje privatni prozor.

— 7. korak DSRC-VU upotrebljava nedavno dodijeljeni privatni prozor za slanje okvira za odgovor ECHO.

U sljedećoj tablici nalazi se primjer razmjene podataka ECHO u praksi.

DSC_56 Inicijalizacija se provodi u skladu s odjeljkom 5.4.7. (DSC_44 do DSC_48) i tablicama 14.4. do 14.9.

DSC_57 REDCR zatim izdaje naredbu ACTION, ECHO u skladu s normom ISO 14906, koja sadržava 100 okteta podataka, ali ne sadržava posebne postavke za RTM. U tablici 14.15. prikazan je sadržaj okvira koji šalje REDCR.

Tablica 14.15.

Primjer okvira za ACTION, zahtjev ECHO

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG	0111 1110	Oznaka početka
2	Private LID	xxxx xxxx	Adresa veze određenog DSRC-VU-a
3		xxxx xxxx	

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Naredba PDU-a
7	LLC Control field	n111 0111	Provjerena naredba ACn, n bitova
8	Fragmentation header	1xxx x001	Nema fragmentiranja.
9	ACTION.request SEQUENCE {	0000	Zahtjev za radnju (ECHO)
	OPTION indicator	0	Pristupni podatci nisu prisutni.
	OPTION indicator	1	Parametar radnje prisutan.
	OPTION indicator	0	IID nije prisutan.
	Mode BOOLEAN	1	Odgovor se očekuje.
10	EID INTEGER (0..127,…)	0000 0000	Nema proširenja, EID = 0 (sustav)
11	ActionType INTEGER (0..127,…)	0000 1111	Nema proširenja, zahtjev ECHO za vrstu radnje
12	ActionParameter CONTAINER {	0000 0010	Nema proširenja, odabir spremnika = 2
13		0110 0100	Nema proširenja, Duljina niza = 100 okteta
14		xxxx xxxx	Podatci za koje se treba izvršiti naredba ECHO
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Slijed provjere okvira
115		xxxx xxxx	
116	Flag	0111 1110	Oznaka završetka

DSC_58 DSRC-VU, nakon primanja zahtjeva ECHO, šalje odgovor ECHO od 100 okteta podataka odražavanjem primljene naredbe, u skladu s normom ISO 14906, bez posebnih postavki za RTM. U tablici 14.16. prikazan je primjer kodiranja na razini bitova.

Tablica 14.16.

Primjer okvira za ACTION, odgovor ECHO

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG	0111 1110	Oznaka početka
2	Private LID	xxxx xxxx	Adresa veze određenog VU-a
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	Odgovor PDU-a
7	LLC Control field	n111 0111	Naredba ACn, n bitova
8	LLC status field	0000 0000	Odgovor dostupan.
9	Fragmentation header	1xxx x001	Nema fragmentiranja.
10	ACTION.response SEQUENCE {	0001	Odgovor RADNJE (ECHO)
	OPTION indicator	0	IID nije prisutan.
	OPTION indicator	1	Parametar odgovora prisutan.
	OPTION indicator	0	Uzvratni status nije prisutan.
	Fill BIT STRING (SIZE (1))	0	Ne upotrebljava se.
11	EID INTEGER (0..127,…)	0000 0000	Nema proširenja, EID = 0 (sustav)
12	ResponseParameter CONTAINER {	0000 0010	Nema proširenja, odabir spremnika = 2
13		0110 0100	Nema proširenja, Duljina niza = 100 okteta
14		xxxx xxxx	Podatci za koje je izvršena naredba ECHO
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Slijed provjere okvira
115		xxxx xxxx	
116	Flag	0111 1110	Oznaka završetka

5.5 **Potpora Direktivi (EU) 2015/719**

5.5.1 *Pregled*

DSC_59 Za potporu Direktivi (EU) 2015/719 o najvećim masama i dimenzijama za teška teretna vozila, protokol transakcije za preuzimanje podataka OWS-a putem veze sučelja DSRC-a na frekvenciji od 5,8 GHz bit će jednak protokolu koji se upotrebljava za podatke RTMA-a (vidjeti odjeljak 5.4.1), a jedina je razlika u tome što će identifikator objekata koji se odnosi na normu TARV upućivati na normu ISO 15638 (TARV) Dio 20. koji se odnosi na WOB/OWS.

5.5.2 *Naredbe*

DSC_60 Naredbe koje se upotrebljavaju za transakciju OWS-a bit će jednake naredbama koje se upotrebljavaju za transakcije u okviru RTM-a.

5.5.3 *Slijed naredbi za ispitivanje*

DSC_61 Slijed naredbi za ispitivanje za podatke OWS-a bit će jednak slijedu za podatke RTM-a.

5.5.4 *Strukture podataka*

DSC_62 Korisni podatci (podatci OWS-a) sastoje se od ulančavanja

1. podataka EncryptedOwsPayload, što čini šifru OwsPayload kako je utvrđeno u modulu ASN-1 u odjeljku 5.5.5. Način šifriranja jednak je načinu donesenom za RtmData koji je naveden u Dodatku 11.,

2. podataka DSRCSecurityData, izračunano s pomoću jednakih algoritama kao i za RtmData, kako je navedeno u Dodatku 11.

5.5.5 *Modul ASN.1 za transakcije OWS-a u okviru DSRC-a*

DSC_63. Definicija modula ASN.1 za podatke DSRC-a u okviru aplikacije RTM-a utvrđuje se kako slijedi:

```
   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 *Elementi OwsData, provedene radnje i definicije*

Elementi OwsData utvrđeni su radi potpore Direktivi (EU) 2015/719 o najvećim masama i dimenzijama za teška teretna vozila. Njihovo je značenje sljedeće:

— recordedWeight predstavlja ukupnu izmjerenu masu teškog teretnog vozila uz razlučivost od 10 kg kako je utvrđeno u normi EN ISO 14906. Primjerice, vrijednost od 2 500 predstavlja masu od 25 tona.

— axlesConfiguration predstavlja konfiguraciju teškog teretnog vozila u pogledu broja osovina. Konfiguracija se utvrđuje s pomoću maske bitova od 20 bitova (u skladu s normom EN ISO 14906).

Maska bitova od 2 bita predstavlja konfiguraciju osovine sa sljedećim formatom:

— vrijednost 00B znači da je vrijednost „nedostupna" jer vozilo ne raspolaže opremom za preuzimanje mase na osovini;

— vrijednost 01B znači da osovina nije prisutna;

— vrijednost 10B znači da je osovina prisutna, a masa izračunata i preuzeta te navedena u polju axlesRecordedWeight;

— vrijednost 11B rezervirana je za buduće upotrebe.

Posljednja su četiri bita rezervirana za buduće upotrebe.

Broj osovina										
Broj osovina na jedinici vozila			Broj osovina na prikolici							
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 bita)

— axlesRecordedWeight predstavlja specifičnu masu za svaku osovinu uz razlučivost od 10 kg. Za svaku se osovinu upotrebljavaju dva okteta. Primjerice, vrijednost od 150 predstavlja masu od 1 500 Kg.

Ostale vrste podataka utvrđuju se u odjeljku 5.4.5.

5.5.7 *Mehanizmi prijenosa podataka*

DSC_64 Mehanizam prijenosa podataka za podatke OWS-a između REDCR-a i uređaja DSRC-a u vozilu jednak je mehanizmu za podatke RTM-a (vidjeti odjeljak 5.4.6).

DSC_65 Prijenos podataka između platforme na kojoj se prikupljaju podatci o najvećim masama i uređaja DSRC-a u vozilu temelji se na fizičkoj vezi i sučeljima te protokolu utvrđenom u odjeljku 5.6.

5.6 **Prijenos podataka između DSRC-VU-a i VU-a**

5.6.1 *Fizička veza i sučelja*

DSC_66 Veza između VU-a i DSRC-VU-a može se uspostaviti s pomoću fizičkog kabela ili putem bežične komunikacije kratkog dometa na temelju sustava Bluetooth v4.0 BLE.

DSC_67 Neovisno o izboru fizičke veze i sučelja, potrebno je ispuniti sljedeće zahtjeve:

DSC_68 a) Kako bi se mogli angažirati različiti dobavljači za isporuku VU-a i DSRC-VU-a te različitih serija DSRC-VU-a, veza između VU-a i DSRC-VU-a mora biti veza u okviru otvorene norme. VU se povezuje s DSRC-VU-om

i) upotrebom fiksnog kabela od najmanje 2 metra, upotrebom ravnog priključka DIN 41612 H11, odobrenog 11-pinskog muškog priključka iz DSRC-VU-a koji odgovara ženskom priključku iz uređaja VU-a;

ii) upotrebom sustava Bluetooth niske razine energije (BLE);

iii) upotrebom priključka u skladu s normom ISO 11898 ili normom SAE J1939.

DSC_69 b) Definicija sučelja i veze između VU-a i DSRC-VU-a mora podržavati naredbe protokola aplikacije utvrđene u odjeljku 5.6.2. i

DSC_70 c) VU i DSRC-VU moraju podržavati rad prijenosa podataka putem veze u pogledu učinkovitosti i napajanja.

5.6.2 *Protokol aplikacije*

DSC_71 Protokol aplikacije između uređaja jedinice u vozilu za komunikaciju na daljinu i DSRC-VU-a zadužen je za periodični prijenos podataka komunikacijom na daljinu iz VU-a DSRC-u.

DSC_72 Utvrđuju se sljedeće glavne naredbe:

1. Inicijalizacija komunikacijske veze – zahtjev
2. Inicijalizacija komunikacijske veze – odgovor
3. Slanje podataka uz identifikator aplikacije RTM-a i prijenos utvrđen u okviru podataka RTM-a
4. Potvrđivanje podataka
5. Prekid komunikacijske veze – zahtjev
6. Prekid komunikacijske veze – odgovor

DSC_73 U modulu ASN1.0, prethodne naredbe mogu se utvrditi kao:

```
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 je naredbi i parametara sljedeći:

— `RCDT-Communication Link Initialization – Request` upotrebljava se za inicijalizaciju komunikacijske veze. VU šalje naredbu DSRC-VU-u. VU postavlja LinkIdentifier i prenosi ga DSRC-VU-u za pronalaženje određene komunikacijske veze.

(Napomena: to služi za potporu budućim vezama i ostalim aplikacijama/modulima kao što je vaganje u vozilu).

— `RCDT-Communication Link Initialization – Response` upotrebljava DSRC-VU za pružanje odgovora na zahtjev za inicijalizaciju komunikacijske veze. DSRC-VU šalje naredbu VU-u. Naredbom se pruža rezultat inicijalizacije kao odgovor = 1 (uspješno) ili = 0 (neuspješno).

DSC_75 Inicijalizacija komunikacijske veze provodi se isključivo nakon ugradnje, kalibracije i pokretanja motora / uključivanja VU-a.

— `RCDT-Send Data` upotrebljava VU za slanje potpisanih podataka RCDTData (odnosno podataka u okviru komunikacije na daljinu) DSRC-VU-u. Podatci će se slati svakih 60 sekundi. Parametar DataTransactionId utvrđuje određeni prijenos podataka. Parametar LinkIdentifier također se upotrebljava kako bi se osiguralo da je odgovarajuća veza ispravna.

— `RCDT-Data Acknowledgment` šalje DSRC-VU kako bi pružio povratne informacije VU-u nakon primitka podataka s pomoću naredbe `RCDT-Send Data` koju utvrđuje parametar DataTransactionId. Parametar odgovora iznosi 1 (uspješno) ili 0 (neuspješno). Ako VU primi više od tri odgovora koji su jednaki 0 ili ako VU ne primi potvrdu podataka RCDT-a za određene prethodno poslane podatke RCDT s određenim parametrom DataTransactionId, VU će generirati i zabilježiti događaj.

— `RCDT-Communication Link Termination request` request šalje VU DSRC-VU-u za prekid veze za određeni LinkIdentifier.

DSC_76 Pri ponovnom pokretanju DSRC-VU-a ili VU-a treba ukloniti sve postojeće komunikacijske veze jer bi moglo biti „zaostalih” veza zbog iznenadna isključenja VU-a.

— `RCDT-Communication Link Termination – Response` šalje DSRC-VU VU-u za potvrđivanje zahtjeva za prekid veze za određeni LinkIdentifier koji vrši VU.

5.7 **Rješavanje pogrešaka**

5.7.1 *Bilježenje i prijenos podataka u okviru DSRC-VU-a*

DSC_77 Podatci se u već zaštićenom obliku pružaju DSRC-VU-u u okviru funkcije VUSM-a. VUSM provjerava jesu li podatci zabilježeni u DSRC-VU-u zabilježeni na ispravan način. Zapisi i izvješća o pogreškama prijenosa podataka iz VU-a u memoriju DSRC-VU-a bilježe se tipom EventFaultType i rednim brojem postavljenim na pogrešku komunikacije uređaja za komunikaciju na daljinu ‘62’H, zajedno s oznakom vremena.

DSC_78 VU zadržava datoteku utvrđenu jedinstvenim nazivom koji se lako može utvrditi provjerom u svrhu bilježenja „grešaka unutarnje komunikacije VU-a”.

DSC_79 Ako VUPM pokuša dobiti podatke VU-a iz sigurnosnog modula (kako bi ih poslao VU-DSRC-u), a u tome ne uspije, tu pogrešku bilježi tipom EventFaultType i rednim brojem postavljenim na pogrešku komunikacije ‘62’H Remote Communication Facility zajedno s oznakom vremena. Greška komunikacije otkriva se ako se za taj događaj ne primi poruka `RCDT Data Acknowledgment` (odnosno, uz iste poruke za DataTransactionId in the `in the Send Data and Acknowledgment`) `RCDT Send Data` više od tri puta zaredom.

5.7.2 *Pogreške bežične komunikacije*

DSC_80 Rješavanje pogrešaka komunikacije u skladu je s povezanim normama za DSRC, odnosno EN 300 674-1, EN 12253, EN 12795, EN 12834 i odgovarajućim parametrima norme EN 13372.

5.7.2.1 *Pogreške šifriranja i potpisa*

DSC_81 Pogreške šifriranja i potpisa rješavaju se kako je utvrđeno u Dodatku 11., Zajednički sigurnosni mehanizmi, te nisu prisutne u bilo kojoj od poruka o pogreškama povezanima s prijenosom podataka u okviru DSRC-a.

5.7.2.2 *Bilježenje pogrešaka*

Medij DSRC dinamična je bežična komunikacija u okruženju neizvjesnih atmosferskih uvjeta i uvjeta interferencija, osobito u kombinacijama „prijenosnog REDCR-a" i „vozila u pokretu" uključenima u ovu aplikaciju. Stoga je potrebno utvrditi razliku između „greške očitavanja" i stanja „pogreške". U transakciji putem bežičnog sučelja greška očitavanja uobičajena je, a posljedica je obično ponovni pokušaj odnosno ponovno slanje BST-a ili ponovni pokušaj slijeda koji će u većini okolnosti dovesti do uspješnog uspostavljanja veze u komunikaciji i prijenosa podataka, osim ako se ciljano vozilo kreće izvan dometa tijekom vremena potrebnog za ponovni prijenos. („Uspješna" instanca „očitavanja" može uključivati nekoliko ponovnih pokušaja.)

Do greške očitavanja može doći zbog neispravnog uparivanja antena (pogreška „ciljanja") jer je jedna antena zaštićena. To može biti namjerno, no može biti i uzrokovano fizičkom prisutnošću drugog vozila, interferencijama u radiokomunikaciji, osobito na frekvenciji bežične mreže od oko 5,8 GHz ili drugim bežičnim komunikacijama s javnim pristupom, ili može biti uzrokovano radarskim interferencijama ili teškim atmosferskim uvjetima (npr. tijekom oluje), ili pak jednostavno kretanjem izvan dometa komunikacije DSRC-a. Pojedinačne instance grešaka očitavanja zbog svoje se naravi ne mogu zabilježiti, jednostavno jer do komunikacije uopće nije došlo.

Međutim, ako djelatnik nadležnog nadzornog tijela cilja vozilo i pokuša ispitati njegov DSRC-VU, ali ne uslijedi uspješan prijenos podataka, do greške je moglo doći zbog namjernog neovlaštenog rukovanja i stoga su djelatniku nadležnog nadzornog tijela potrebna sredstva za bilježenje greške i upozoravanje suradnika o mogućem kršenju. Suradnici tada mogu zaustaviti vozilo i provesti fizički pregled. Međutim, s obzirom na to da nije uspostavljena uspješna komunikacija, DSRC-VU ne može poslati podatke o grešci. Takvo je je izvješćivanje stoga funkcija izvedbe opreme REDCR-a.

„Greška očitavanja" s tehničkog se gledišta razlikuje od „pogreške". U ovom kontekstu „pogrešku" čini dobivanje pogrešne vrijednosti.

Podatci preneseni u DSRC-VU dostavljaju se u već zaštićenom obliku, stoga ih mora provjeriti dostavljač podataka (vidjeti odjeljak 5.4).

Podatci koji se potom prenose putem zračnog sučelja provjeravaju se kružnim provjerama zalihosti na komunikacijskoj razini. Ako ih CRC potvrdi, podatci su ispravni. Ako ih CRC ne potvrdi, podatci se ponovno prenose. Vjerojatnost da neispravni podatci mogu uspješno proći CRC-om statistički je toliko malena da se može zanemariti.

Ako CRC ne potvrdi podatke te nema dovoljno vremena za ponovni prijenos i primitak ispravnih podataka, rezultat neće biti pogreška nego instanca određenog tipa pogreške očitavanja.

Jedina značajna „pogreška" podataka koja se može zabilježiti pogreška je broja uspješnih inicijalizacija transakcija koje se dogode i koje ne rezultiraju uspješnim prijenosom podataka u REDCR.

DSC_82 REDCR stoga bilježi, uz vremensku oznaku, broj slučajeva u kojima je faza „inicijalizacije" ispitivanja funkcije DSRC-a uspješna, ali je transakcija prekinuta prije nego što je REDCR uspješno dohvatio podatke. Ti podatci dostupni su djelatniku nadležnog nadzornog tijela i pohranjuju se u memoriju opreme REDCR-a. Način na koji se to postiže pitanje je izvedbe proizvoda ili specifikacije nadležnog nadzornog tijela.

Jedina značajna „pogreška" podataka koja se može zabilježiti broj je slučajeva u kojima REDCR ne uspije dešifrirati primljene podatke. Međutim, treba napomenuti da će se to odnositi isključivo na učinkovitost softvera REDCR-a. Podatke je moguće dešifrirati s tehničkog gledišta, no sa semantičkog gledišta oni nisu smisleni.

DSC_83 REDCR stoga bilježi, uz vremensku oznaku, broj slučajeva u kojima je pokušao dešifrirati podatke primljene putem sučelja DSRC-a, ali u tome nije uspio.

6 PUŠTANJE U POGON I PERIODIČKA ISPITIVANJA PREGLEDA ZA FUNKCIJU KOMUNIKACIJE NA DALJINU

6.1 **Opće značajke**

DSC_84 Predviđene su dvije vrste ispitivanja za funkciju komunikacije na daljinu:

1) ispitivanje ECHO za potvrđivanje komunikacijskog kanala DSRC-REDCR >>-:-<bežični DSRC-VU;

2) cjelovito sigurnosno ispitivanje kojim se osigurava da se s pomoću kartice radionice može pristupiti šifriranom i potpisanom sadržaju podataka koje je stvorio VU i koji su preneseni bežičnim komunikacijskim kanalom.

6.2 **ECHO**

U ovoj se točki nalaze odredbe posebno namijenjene ispitivanju funkcionalne aktivnosti za DSRC-REDCR >>-:-<DSRC-VU.

Cilj je naredbe ECHO omogućiti radionicama ili uređajima za homologacijsko ispitivanje da ispitaju radi li DSRC veza bez potrebe za pristupom sigurnosnim podatcima. Oprema ispitivača stoga mora biti sposobna pokrenuti komunikaciju DSRC-a (slanjem BST-a uz vrijednost AID = 2), a zatim poslati naredbu ECHO te će, ako DSRC ispravno radi, primiti odgovor ECHO. Više pojedinosti možete pronaći u odjeljku 5.4.8. Ako veza DSRC-a odgovor primi na ispravan način, može se potvrditi njezin ispravan rad (DSRC-REDCR >>-:-<DSRC-VU).

6.3 **Ispitivanja za potvrđivanje sigurnog sadržaja podataka**

DSC_85 Ovo se ispitivanje provodi za potvrđivanje cjelovitog sigurnosnog protoka podataka. Za takvo je ispitivanje potreban čitač za ispitivanje u okviru DSRC-a. Čitač za ispitivanje u okviru DSRC-a ima istu funkciju i ugrađuje se s jednakim specifikacijama kao i čitač koji upotrebljavaju nadležna tijela, uz tu razliku da se kartica radionice upotrebljava za autentifikaciju korisnika čitača za ispitivanje DSRC-a umjesto kontrolne kartice. Ispitivanje se može provesti nakon početne aktivacije pametnog tahografa ili na kraju postupka kalibracije. Nakon aktivacije jedinica u vozilu generira i prenosi DSRC-VU-u zaštićene podatke za rano otkrivanje.

DSC_86 Osoblje radionice mora postaviti čitač za ispitivanje DSRC-a na udaljenost između 2 i 10 metara ispred vozila.

DSC_87 Zatim će osoblje radionice umetnuti karticu radionice u čitač za ispitivanje u okviru DSRC-a kako bi zatražilo ispitivanje ranog otkrivanja podataka u jedinici u vozilu. Nakon uspješnog ispitivanja osoblje radionice pristupit će primljenim podatcima kako bi osigurali da je njihov integritet uspješno potvrđen i da su uspješno dešifrirani.

Dodatak 15.

MIGRACIJA: UPRAVLJANJE ISTODOBNIM POSTOJANJEM VIŠE GENERACIJA OPREME

SADRŽAJ

1. DEFINICIJE 497

2. OPĆE ODREDBE 497

2.1. Pregled prijelaza 497

2.2. Interoperabilnost između jedinice u vozilu i kartica 498

2.3. Interoperabilnost između jedinice u vozilu i senzora kretanja 498

2.4. Interoperabilnost između jedinica u vozilu, tahografskih kartica i opreme za preuzimanje podataka 498

2.4.1 Izravno preuzimanje putem IDE-a 498

2.4.2 Preuzimanje podataka s kartice putem jedinice u vozilu 499

2.4.3 Preuzimanje podataka iz jedinice u vozilu 499

2.5. Interoperabilnost između jedinice u vozilu i opreme za kalibraciju 499

3. GLAVNI KORACI TIJEKOM RAZDOBLJA KOJE PRETHODI DATUMU UVOĐENJA 499

4. ODREDBE ZA RAZDOBLJE NAKON DATUMA UVOĐENJA 499

1. DEFINICIJE

Za potrebe ovog Dodatka upotrebljavaju se sljedeće definicije:

sustav pametnog tahografa: prema definiciji u ovom Prilogu (poglavlje 1., definicija bbb));

tahografski sustav prve generacije: prema definiciji u ovoj Uredbi (članak 2., definicija 1.);

tahografski sustav druge generacije: prema definiciji u ovoj Uredbi (članak 2., definicija 7.);

datum uvođenja: prema definiciji u ovom Prilogu (poglavlje 1., definicija ccc));

inteligentna namjenska oprema (eng. *Intelligent Dedicated Equipment*, IDE): oprema koja se upotrebljava za preuzimanje podataka, prema definiciji u Dodatku 7. ovog Priloga.

2. OPĆE ODREDBE

2.1. **Pregled prijelaza**

U uvodu ovog Priloga naveden je pregled prijelaza između sustava tahografa prve i druge generacije.

Uz odredbe ovog uvoda navodi se i sljedeće:

— prva generacija senzora kretanja neće biti interoperabilna s drugom generacijom jedinica u vozilu;

— druga generacija senzora kretanja početak će se ugrađivati u vozila u isto vrijeme kada i druga generacija jedinica u vozilu;

— opremu za preuzimanje podataka i kalibraciju trebat će unaprijediti kako bi se podržale obje generacije uređaja za bilježenje podataka i tahografskih kartica.

2.2. **Interoperabilnost između jedinice u vozilu i kartica**

Podrazumijeva se da su tahografske kartice prve generacije interoperabilne s jedinicama u vozilu prve generacije (u skladu s Prilogom I.B ovoj Uredbi), dok su tahografske kartice druge generacije interoperabilne s jedinicama u vozilu druge generacije (u skladu s Prilogom I.C ovoj Uredbi). Osim toga, primjenjuju se i sljedeći zahtjevi:

MIG_001 Osim kako je predviđeno u zahtjevima MIG_004 i MIG_005, tahografske kartice prve generacije mogu se i dalje upotrebljavati u jedinicama u vozilu druge generacije do isteka valjanosti. Međutim, nositelji kartica mogu zatražiti njihovu zamjenu tahografskim karticama druge generacije čim budu dostupne.

MIG_002 Jedinice u vozilu druge generacije moraju moći upotrebljavati bilo koju umetnutu valjanu karticu vozača, kontrolnu karticu i karticu poduzeća prve generacije.

MIG_003 Tu mogućnost radionice mogu zauvijek onemogućiti u takvim jedinicama u vozilu, tako da se tahografske kartice prve generacije ne mogu više primati. To se može učiniti tek nakon što Europska komisija započne postupak kojim se od radionica zatraži da to učine, primjerice, tijekom svakog periodičnog pregleda tahografa.

MIG_004 Jedinice u vozilu druge generacije mogu upotrebljavati samo kartice radionice druge generacije.

MIG_005 Za određivanje načina rada jedinice u vozilu druge generacije u obzir uzimaju samo vrstu umetnutih valjanih kartica, bez obzira na generaciju.

MIG_006 Bilo koja valjana tahografska kartica druge generacije mora se moći upotrebljavati u jedinicama u vozilu druge generacije na potpuno isti način kao i tahografske kartice prve generacije iste vrste.

2.3. **Interoperabilnost između jedinice u vozilu i senzora kretanja**

Podrazumijeva se da su senzori kretanja prve generacije interoperabilni s jedinicama u vozilu prve generacije, dok su senzori kretanja druge generacije interoperabilni s jedinicama u vozilu druge generacije. Osim toga, primjenjuju se i sljedeći zahtjevi:

MIG_007 Jedinice u vozilu druge generacije neće se moći upariti i upotrebljavati sa senzorima kretanja prve generacije.

MIG_008 Senzori kretanja druge generacije mogu se upariti i upotrebljavati samo s jedinicama u vozilu druge generacije ili s jedinicama u vozilu obiju generacija.

2.4. **Interoperabilnost između jedinica u vozilu, tahografskih kartica i opreme za preuzimanje podataka**

MIG_009 Oprema za preuzimanje podataka može se upotrebljavati samo s jednom generacijom jedinica u vozilu i tahografskih kartica ili s objema.

2.4.1 *Izravno preuzimanje putem IDE-a*

MIG_010 Podatci se preuzimaju putem IDE-a s tahografskih kartica jedne generacije umetnutih u njihove čitače, koristeći se sigurnosnim mehanizmima i protokolom za preuzimanje podataka te generacije. Preuzeti podatci moraju biti u formatu koji je definiran za tu generaciju.

MIG_011 Kako bi se omogućilo da nadzor nad vozačima provode nadzorna tijela koja nisu iz EU-a, mora biti moguće i preuzeti podatke s kartica vozača (i radionice) druge generacije na potpuno isti način kao i s kartica vozača (i radionice) prve generacije. Takvo preuzimanje uključuje:

— nepotpisane elementarne datoteke (EF-ove) `IC` i `ICC`;

— nepotpisane EF-ove (prve generacije) `Card_Certificate` i `CA_Certificate`;

— druge EF-ove aplikacijskih podataka (unutar podatkovne datoteke (DF-a) TACHO) koje zatraži protokol preuzimanja podataka s kartice prve generacije. Te informacije zaštićuju se digitalnim potpisom u skladu sa sigurnosnim mehanizmima prve generacije.

Takvo preuzimanje ne uključuje EF-ove aplikacijskih podataka koji se nalaze samo na karticama vozača (i radionice) druge generacije (EF-ovi aplikacijskih podataka unutar DF-a TACHO_G2).

2.4.2 *Preuzimanje podataka s kartice putem jedinice u vozilu*

MIG_012 Podatci se preuzimaju s kartice druge generacije umetnute u jedinicu u vozilu prve generacije koristeći se protokolom za preuzimanje podataka prve generacije. Kartica odgovara na naredbe jedinice u vozilu na potpuno isti način kao i kartica prve generacije. Preuzeti podatci moraju biti istog formata kao i podatci preuzeti s kartice prve generacije.

MIG_013 Podatci se preuzimaju s kartice prve generacije umetnute u jedinicu u vozilu druge generacije koristeći se protokolom za preuzimanje podataka definiranim u Dodatku 7. ovog Priloga. Jedinica u vozilu šalje naredbe kartici na potpuno isti način kao i jedinica u vozilu prve generacije, a preuzeti podatci slijede format definiran za kartice prve generacije.

2.4.3 *Preuzimanje podataka iz jedinice u vozilu*

MIG_014 Podatci iz jedinica u vozilu druge generacije preuzimaju se koristeći se sigurnosnim mehanizmima druge generacije te protokolom za preuzimanje podataka određenim u Dodatku 7. ovog Priloga.

MIG_015 Kako bi se omogućilo da nadzor nad vozačima provode nadzorna tijela koja nisu iz EU-a te da podatke iz jedinice u vozilu preuzimaju radionice koje nisu iz EU-a, može postojati mogućnost da se podatci iz jedinice u vozilu druge generacije preuzmu koristeći se sigurnosnim mehanizmima prve generacije te protokolom za preuzimanje podataka prve generacije. Preuzeti podatci moraju biti istog formata kao i podatci preuzeti iz jedinica u vozilu prve generacije. Ta se mogućnost može odabrati putem naredbi u izborniku.

2.5. **Interoperabilnost između jedinice u vozilu i opreme za kalibraciju**

MIG_016 Oprema za kalibraciju mora moći izvršiti kalibraciju tahografa svih generacija koristeći se protokolom za kalibraciju te generacije. Oprema za kalibraciju može se koristiti samo s jednom generacijom tahografa ili s objema.

3. GLAVNI KORACI TIJEKOM RAZDOBLJA KOJE PRETHODI DATUMU UVOĐENJA

MIG_017 Ispitni ključevi i certifikati moraju biti dostupni proizvođačima najkasnije **30 mjeseci** prije datuma uvođenja.

MIG_018 Ispitivanja interoperabilnosti mogu započeti ako to proizvođači zatraže najkasnije **15 mjeseci** prije datuma uvođenja.

MIG_019 Službeni ključevi i certifikati moraju biti dostupni proizvođačima najkasnije **12 mjeseci** prije datuma uvođenja.

MIG_020 Države članice moraju biti u mogućnosti izdati kartice radionice druge generacije najkasnije **tri mjeseca** prije datuma uvođenja.

MIG_021 Države članice moraju biti u mogućnosti izdati sve vrste tahografskih kartica druge generacije najkasnije **mjesec dana prije datuma uvođenja**.

4. ODREDBE ZA RAZDOBLJE NAKON DATUMA UVOĐENJA

MIG_022 Nakon datuma uvođenja države članice izdaju isključivo tahografske kartice druge generacije.

MIG_023 Proizvođači jedinica u vozilu / senzora kretanja smiju proizvoditi jedinice u vozilu / senzore kretanja prve generacije sve dok se upotrebljavaju na terenu kako bi se neispravni sastavni dijelovi mogli zamijeniti.

MIG_024 Proizvođači jedinica u vozilu / senzora kretanja smiju zatražiti i dobiti zadržavanje homologacije za one vrste jedinica u vozilu / senzora kretanja prve generacije koji su već homologirani.

Dodatak 16.

ADAPTER ZA VOZILA KATEGORIJE M1 I N1

KAZALO

1. POKRATE I REFERENTNI DOKUMENTI 501

1.1. Kratice 501

1.2. Referentne norme 501

2. OPĆA OBILJEŽJA I FUNKCIJE ADAPTERA 502

2.1. Opći opis adaptera 502

2.2. Funkcije 502

2.3. Sigurnost 502

3. ZAHTJEVI ZA UREĐAJ ZA BILJEŽENJE PODATAKA KADA JE ADAPTER UGRAĐEN 502

4. ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNOSTI ADAPTERA 503

4.1. Povezivanje i prilagođavanje dolaznih impulsa brzine 503

4.2. Dovođenje dolaznih impulsa do ugrađenog senzora kretanja 503

4.3. Ugrađeni senzor kretanja 503

4.4. Sigurnosni zahtjevi 503

4.5. Karakteristike izvedivosti 504

4.6. Materijali 504

4.7. Oznake 504

5. UGRADNJA UREĐAJA ZA BILJEŽENJE PODATAKA KADA SE UPOTREBLJAVA ADAPTER 504

5.1. Ugradnja 504

5.2. Plombiranje 505

6. PROVJERE, PREGLEDI I POPRAVCI 505

6.1. Periodični pregledi 505

7. HOMOLOGACIJA UREĐAJA ZA BILJEŽENJE PODATAKA KADA SE UPOTREBLJAVA ADAPTER 505

7.1. Opći zahtjevi 505

7.2. Certifikat o ispravnosti 506

1. POKRATE I REFERENTNI DOKUMENTI

1.1. **Pokrate**

TBD bit će definirano (eng. *To Be Defined*)

VU jedinica u vozilu (eng. *Vehicle Unit*)

1.2. **Referentne norme**

ISO 16844-3 *Road vehicles – Tachograph systems – Part 3: Motion sensor interface*

2. OPĆA OBILJEŽJA I FUNKCIJE ADAPTERA

2.1. **Opći opis adaptera**

ADA_001 Adapter šalje spojenoj jedinici u vozilu zaštićene podatke o kretanju, koji trajno predstavljaju brzinu vozila i prijeđenu udaljenost.

Adapter je namijenjen samo za ona vozila koja u skladu s ovom Uredbom moraju biti opremljena uređajem za bilježenje podataka.

Ugrađuje se i upotrebljava samo u onim vrstama vozila definiranima u definiciji yy) „adapter" iz priloga I.C kada nije mehanički moguće ugraditi bilo koju drugu vrstu postojećeg senzora kretanja, koji je inače usklađen s odredbama ovog Priloga i njegovih dodataka od 1. do 16.

Adapter nije mehanički spojen s pomičnim dijelom vozila, već je povezan s impulsima brzine/udaljenosti koje proizvode integrirani senzori ili alternativna sučelja.

ADA_002 Homologirani senzor kretanja (u skladu s odredbama iz odjeljka 8. Priloga I.C, Homologacija uređaja za bilježenje podataka i tahografskih kartica) ugrađuje se u kućište adaptera, u kojem se nalazi i uređaj za pretvaranje impulsa koji dolazne impulse vodi do ugrađenog senzora kretanja. Ugrađeni senzor kretanja spojen je na jedinicu u vozilu, čime je sučelje između jedinice u vozilu i adaptera u skladu sa zahtjevima navedenima u normi ISO 16844-3.

2.2. **Funkcije**

ADA_003 Adapter ima sljedeće funkcije:

— spajanje i prilagođavanje dolaznih impulsa brzine;

— dovođenje dolaznih impulsa do ugrađenog senzora kretanja;

— sve funkcije ugrađenog senzora kretanja, slanje zaštićenih podataka o kretanju jedinici u vozilu.

2.3. **Sigurnost**

ADA_004 Adapter se sigurnosno ne certificira u skladu s generičkom sigurnosnom ciljnom vrijednosti za senzore kretanja definiranom u Dodatku 10. ovog Priloga. Umjesto toga primjenjuju se sigurnosni zahtjevi navedeni u odjeljku 4.4. ovog Dodatka.

3. ZAHTJEVI ZA UREĐAJ ZA BILJEŽENJE PODATAKA KADA JE ADAPTER UGRAĐEN

Zahtjevi navedeni u sljedećim poglavljima upućuju na to kako se tumače zahtjevi iz ovog Priloga prilikom upotrebe adaptera. Brojevi povezanih zahtjeva navedenih u Prilogu I.C navedeni su u zagradama.

ADA_005 Uređaj za bilježenje podataka bilo kojeg vozila opremljenog adapterom mora biti u skladu s odredbama navedenima u ovom Prilogu, osim ako u Dodatku nije drugačije navedeno.

ADA_006 Kada je adapter ugrađen, uređaj za bilježenje podataka sastoji se od kabela, adaptera (uključujući senzor kretanja) i jedinice u vozilu [01].

ADA_007 Funkcija za otkrivanje događaja i/ili kvarova uređaja za bilježenje podataka izmijenjena je kako slijedi:

— događaj „prekid napajanja" aktivira jedinica u vozilu, dok nije u načinu rada za kalibraciju, pri svakom prekidu napajanja ugrađenog senzora kretanja duljem od 200 milisekundi [79];

— događaj „pogreška u podacima o kretanju" aktivira jedinica u vozilu u slučaju prekida uobičajenog protoka podataka između ugrađenog senzora kretanja i jedinice u vozilu i/ili u slučaju greške u integritetu podataka ili greške u autentifikaciji podataka tijekom razmjene podataka između ugrađenog senzora kretanja i jedinice u vozilu [83];

— događaj „pokušaj probijanja zaštite” aktivira jedinica u vozilu u slučaju bilo kojeg drugog događaja koji utječe na sigurnost ugrađenog senzora kretanja dok nije u načinu rada za kalibraciju [85];

— grešku „uređaj za bilježenje podataka” aktivira jedinica u vozilu, dok nije u načinu rada za kalibraciju, u slučaju bilo kakvog kvara ugrađenog senzora kretanja [88].

ADA_008 Kvarovi adaptera koje uređaj za bilježenje podataka može otkriti kvarovi su povezani s ugrađenim senzorom kretanja [88].

ADA_009 Funkcija za kalibraciju jedinice u vozilu omogućava automatsko uparivanje ugrađenog senzora kretanja s jedinicom u vozilu [202, 204].

4. ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNOSTI ADAPTERA

4.1. **Povezivanje i prilagođavanje dolaznih impulsa brzine**

ADA_011 Ulazno sučelje adaptera prihvaća impulse frekvencije koji predstavljaju brzinu vozila i prijeđenu udaljenost. Električne karakteristike dolaznih impulsa su sljedeće: *definirat će ih proizvođač*. Prilagodbe dostupne isključivo proizvođaču adaptera te ovlaštenoj radionici koja provodi ugradnju adaptera moraju omogućiti ispravno povezivanje ulaznog sučelja adaptera s vozilom, ako je primjenjivo.

ADA_012 Ulazno sučelje adaptera mora imati mogućnost, ako je primjenjivo, pomnožiti ili podijeliti impulse frekvencije dolaznih impulsa brzine s fiksnim faktorom kako bi se signal prilagodio rasponu k faktora određenom u ovom Prilogu (4 000 do 25 000 impulsa/km). Fiksni faktor mogu programirati samo proizvođač adaptera i ovlaštena radionica koja obavlja ugradnju adaptera.

4.2. **Dovođenje dolaznih impulsa do ugrađenog senzora kretanja**

ADA_013 Dolazni impulsi, koji su eventualno prilagođeni kako je prethodno navedeno, dovode se do ugrađenog senzora kretanja tako da senzor kretanja otkrije svaki dolazni impuls.

4.3. **Ugrađeni senzor kretanja**

ADA_014 Dolazni impulsi stimuliraju ugrađeni senzor kretanja te mu time omogućavaju da generira podatke o kretanju koji točno predstavljaju kretanje vozila, kao da je mehanički spojen s pomičnim dijelom vozila.

ADA_015 Jedinica u vozilu identificira adapter s pomoću identifikacijskih podataka ugrađenog senzora kretanja [95].

ADA_016 Smatra se da instalacijski podatci spremljeni u ugrađenom senzoru kretanja predstavljaju instalacijske podatke adaptera [122].

4.4. **Sigurnosni zahtjevi**

ADA_017 Kućište adaptera mora biti oblikovano tako da se ne može otvoriti i plombirano tako da se pokušaji fizičkog neovlaštenog rukovanja mogu jednostavno otkriti (npr. vizualnim pregledom; vidjeti ADA_035). Za plombe vrijede isti zahtjevi kao i za plombe senzora kretanja [398 do 406].

ADA_018 Ne smije biti moguće ukloniti ugrađeni senzor kretanja iz adaptera bez uništavanja plombe (plombi) kućišta adaptera ili uništavanja plombe između senzora i kućišta adaptera (vidjeti ADA_034).

ADA_019 Adapterom se mora osigurati da se podatci o kretanju mogu obrađivati i dobiti samo putem ulaznog sučelja adaptera.

4.5. **Karakteristike izvedivosti**

ADA_020 Adapter mora biti u potpunosti operativan pri rasponu temperatura koji je definirao proizvođač.

ADA_021 Adapter mora biti u potpunosti operativan pri rasponu vlažnosti od 10 % do 90 % [214].

ADA_022 Adapter mora biti zaštićen od prenapona, zamjene polariteta napajanja i kratkih spojeva [216].

ADA_023 Adapter mora:

— reagirati na magnetsko polje koje ometa detekciju kretanja vozila. U takvim okolnostima jedinica u vozilu bilježi i pohranjuje kvar senzora [88] ili

— imati senzorski element koji je zaštićen od magnetskih polja ili je na njih neosjetljiv [217].

ADA_024 Adapter mora biti u skladu s međunarodnim pravilnikom UN ECE R10 koji se odnosi na elektromagnetsku kompatibilnost te mora biti zaštićen od elektrostatičkih pražnjenja i prijelaznih pojava [218].

4.6. **Materijali**

ADA_025 Adapter mora zadovoljavati stupanj zaštite (*definirat će ga proizvođač ovisno o položaju ugradnje*) [220, 221].

ADA_026 Kućište adaptera žute je boje.

4.7. **Oznake**

ADA_027 Opisna pločica pričvršćuje se na adapter te su na njoj navedene sljedeće pojedinosti:

— naziv i adresa proizvođača adaptera;

— kataloški broj proizvođača i godina proizvodnje adaptera;

— homologacijska oznaka tipa adaptera ili tipa uređaja za bilježenje podataka koji sadržava adapter;

— datum ugradnje adaptera;

— identifikacijski broj vozila na koje je ugrađen.

ADA_028 Na opisnoj pločici navode se i sljedeće pojedinosti (ako ih se ne može izravno pročitati s vanjske strane ugrađenog senzora kretanja):

— naziv proizvođača ugrađenog senzora kretanja;

— kataloški broj proizvođača i godina proizvodnje ugrađenog senzora kretanja;

— homologacijska oznaka ugrađenog senzora kretanja.

5. UGRADNJA UREĐAJA ZA BILJEŽENJE PODATAKA KADA SE UPOTREBLJAVA ADAPTER

5.1. **Ugradnja**

ADA_029 Adaptere koji se ugrađuju u vozila ugrađuju isključivo proizvođači vozila ili radionice ovlaštene za ugradnju, aktivaciju i kalibraciju digitalnih i pametnih tahografa.

ADA_030 Ovlaštene radionice koje ugrađuju adaptere izvršavaju prilagodbu ulaznog sučelja i odabiru omjer dijeljenja ulaznog signala (ako je primjenjivo).

ADA_031 Ovlaštene radionice koje ugrađuju adapter plombiraju kućište adaptera.

ADA_032 Adapter se postavlja što je bliže moguće onom dijelu vozila iz kojeg se šalju dolazni impulsi.

ADA_033 Kablovi kojima se napaja adapter crvene su (pozitivan pol) odnosno crne boje (uzemljenje).

5.2. **Plombiranje**

ADA_034 U pogledu plombiranja primjenjuju se sljedeći zahtjevi:

— kućište adaptera plombirano je (vidjeti ADA_017);

— kućište ugrađenog senzora pričvršćeno je plombom na kućište adaptera, osim ako nije moguće ukloniti senzor iz kućišta adaptera bez uništavanja plombe (plombi) kućišta adaptera (vidjeti ADA_018);

— kućište adaptera plombom je pričvršćeno na vozilo;

— veza između adaptera i uređaja koji šalje ulazne impulse mora biti plombirana na oba kraja (u mjeri u kojoj je to moguće).

6. PROVJERE, PREGLEDI I POPRAVCI

6.1. **Periodični pregledi**

ADA_035 Kada se upotrebljava adapter, svaki periodični pregled (periodični pregledi u skladu sa zahtjevima [409] do [413] Priloga I.C) uređaja za bilježenje podataka uključuje sljedeće provjere:

— nalazi li se na adapteru odgovarajuća homologacijska oznaka;

— jesu li plombe na adapteru i priključcima netaknute;

— je li adapter ugrađen na način naveden na tipskoj pločici;

— je li adapter ugrađen na način koji je naveo proizvođač adaptera i/ili vozila;

— je li postavljanje adaptera odobreno za vozilo koje se pregledava.

ADA_036 Ove provjere uključuju kalibraciju te zamjenu svih plombi, bez obzira na njihovo stanje.

7. HOMOLOGACIJA UREĐAJA ZA BILJEŽENJE PODATAKA KADA SE UPOTREBLJAVA ADAPTER

7.1. **Opći zahtjevi**

ADA_037 Uređaj za bilježenje podataka mora se predati na homologaciju u cjelovitom stanju zajedno s adapterom [425].

ADA_038 Svaki adapter može se predati na zasebnu homologaciju ili na homologaciju kao sastavni dio uređaja za bilježenje podataka.

ADA_039 Takva homologacija uključuje provjere funkcionalnosti u vezi s adapterom. Pozitivni rezultati svih tih provjera navode se u odgovarajućem certifikatu [426].

7.2. **Certifikat o ispravnosti**

ADA_040 Certifikat o ispravnosti adaptera ili uređaja za bilježenje podataka koji sadržava adapter dostavlja se proizvođaču adaptera tek nakon uspješne provedbe svih sljedećih minimalnih ispitivanja funkcionalnosti.

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativna provjera**		
1.1.	Dokumentacija	Je li dokumentacija adaptera točna?	
2.	**Vizualni pregled**		
2.1.	Je li adapter u skladu s dokumentacijom?		
2.2.	Identifikacija / oznake adaptera		ADA_027, ADA_028
2.3.	Materijali adaptera		[219] do [223] ADA_026
2.4.	Plombiranje		ADA_017, ADA_018, ADA_034
3.	**Ispitivanje funkcionalnosti**		
3.1.	Dovođenje impulsa brzine do ugrađenog senzora kretanja		ADA_013
3.2.	Povezivanje i prilagođavanje dolaznih impulsa brzine		ADA_011, ADA_012
3.3.	Preciznost mjerenja kretanja		[30] do [35], [217]
4.	**Ispitivanja u vezi s okolišem**		
4.1.	Rezultati ispitivanja proizvođača	Rezultati ispitivanja proizvođača u vezi s okolišem	ADA_020, ADA_021, ADA_022, ADA_024
5.	**EMC**		
5.1.	Emisije zračenja i osjetljivost	Provjeriti usklađenost s Uredbom 2006/28/EZ	ADA_024
5.2.	Rezultati ispitivanja proizvođača	Rezultati ispitivanja proizvođača u vezi s okolišem	ADA_024

ISSN 1977-0847 (elektroničko izdanje)
ISSN 1977-0596 (tiskano izdanje)

Ured za publikacije Europske unije
2985 Luxembourg
LUKSEMBURG

HR