II

(Nezakonodajni akti)

UREDBE

IZVEDBENA UREDBA KOMISIJE (EU) 2018/502

z dne 28. februarja 2018

o spremembi o Izvedbene uredbe (EU) 2016/799 za določitev zahtev glede konstrukcije, preskušanja, namestitve, delovanja in popravila tahografov in njihovih sestavnih delov

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 165/2014 Evropskega parlamenta in Sveta z dne 4. februarja 2014 o tahografih v cestnem prometu ([1]) ter zlasti členov 11 in 12(7) Uredbe,

ob upoštevanju naslednjega:

(1) Z Uredbo (EU) št. 165/2014 so bili uvedeni pametni tahografi, ki so druga generacija digitalnih tahografov in vključujejo opremo za povezavo z globalnim satelitskim navigacijskim sistemom (v nadaljnjem besedilu: GNSS) in komunikacijsko opremo za zgodnje odkrivanje na daljavo, lahko pa tudi vmesnik za povezavo z inteligentnimi prometnimi sistemi (v nadaljnjem besedilu: ITS).

(2) Tehnične zahteve glede konstrukcije, preskušanja, namestitve, delovanja in popravila tahografov in njihovih sestavnih delov so določene v Izvedbeni uredbi Komisije (EU) 2016/799 ([2]).

(3) V skladu s členi 8, 9 in 10 Uredbe (EU) št. 165/2014 so v vozila, ki bodo prvič registrirana 15. junija 2019 ali pozneje, vgrajeni pametni tahografi. Izvedbeno uredbo (EU) 2016/799 je zato treba spremeniti tako, da se bodo njene tehnične določbe začele uporabljati od navedenega datuma.

(4) Da se zagotovi skladnost s členom 8 Uredbe (EU) št. 165/2014, ki določa, da mora biti položaj vozila zapisan vsake tri ure v skupnem času vožnje, bi bilo treba Izvedbeno uredbo (EU) 2016/799 spremeniti tako, da bo informacije o položaju vozila mogoče shranjevati vsake tri ure z uporabo merila, ki ga ni mogoče ponastaviti, in da se odpravi možnost zamenjave s „časom neprekinjene vožnje“, ki je merilo z drugačnim namenom.

(5) Enota v vozilu lahko sestoji iz ene same enote ali več enot, porazdeljenih po vozilu. GNSS oprema in oprema za namensko komunikacijo kratkega dosega (v nadaljnjem besedilu: DSRC) je zato lahko nameščena v glavno ohišje enote v vozilu ali zunaj njega. Kadar so nameščene zunaj njega, bi moralo biti možno opremo in glavno ohišje enote v vozilu homologirati kot sestavne dele, s čimer bi se postopek homologacije pametnih tahografov prilagodil potrebam trga.

(6) Pravila o shranjevanju dogodkov časovnega navzkrižja in nastavljanja časa je treba prilagoditi, da bodo omogočala razlikovanje med samodejnim nastavljanjem časa, ki se sproži zaradi morebitnega nepooblaščenega posega v tahograf ali njegove okvare, in nastavljanjem časa, ki je bilo opravljeno zaradi drugih razlogov, na primer vzdrževanja.

(7) Identifikatorji podatkov bi morali omogočati razlikovanje med podatki, prenesenimi iz pametnih tahografov, in podatki, prenesenimi iz tahografov prejšnje generacije.

([1]) UL L 60, 28.2.2014, str. 1.

([2]) Izvedbena uredba Komisije (EU) 2016/799 z dne 18. marca 2016 o izvajanju Uredbe (EU) št. 165/2014 Evropskega parlamenta in Sveta za določitev zahtev glede konstrukcije, preskušanja, namestitve, delovanja in popravila tahografov in njihovih sestavnih delov (UL L 139, 26.5.2016, str. 1).

(8) Obdobje veljavnosti kartice podjetja je treba podaljšati z dveh na pet let, da se ga uskladi z obdobjem veljavnosti vozniške kartice.

(9) Treba bi bilo bolje opredeliti opise nekaterih napak in dogodkov, potrjevanje vnosov kraja, kjer se dnevne delovne izmene začnejo in/ali končajo, uporabo izrecne privolitve voznika za vmesnik z ITS v zvezi s podatki, ki jih enota v vozilu pošlje prek omrežja vozila, in druga tehnična vprašanja.

(10) Za zagotovitev, da je certifikacija pečatov na tahografih posodobljena, jih je treba prilagoditi novemu standardu za zaščito mehanskih pečatov, ki se uporabljajo v tahografih.

(11) Ta uredba zadeva konstrukcijo, preskušanje, namestitev in delovanje sistemov, ki vključujejo tudi radijsko opremo, kot jo ureja Direktiva 2014/53/EU Evropskega parlamenta in Sveta ([1]). Navedena direktiva ureja dajanje na trg in dajanje v uporabo elektronske ali električne opreme, ki uporablja radijske valove za namene komunikacije in/ali radijske determinacije na horizontalni ravni, zlasti ob upoštevanju električne varnosti, združljivosti z drugimi sistemi, dostopa do radiofrekvenčnega spektra, dostopa do storitev reševanja in/ali morebitnih drugih delegiranih določb. Da se zagotovi učinkovita uporaba radijskega spektra, preprečijo škodljive radijske motnje, zagotovita varnost in elektromagnetna združljivost radijske opreme ter omogočijo morebitne druge posebne delegirane zahteve, ta uredba ne bi smela posegati v določbe navedene direktive.

(12) Izvedbeno uredbo (EU) 2016/799 bi bilo zato treba spremeniti.

(13) Ukrepi, predvideni s to uredbo, so v skladu z mnenjem odbora iz člena 42(3) Uredbe (EU) št. 165/2014 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Izvedbena uredba (EU) 2016/799 se spremeni:

(1) Člen 1 se spremeni:

(a) drugi in tretji odstavek se nadomestita z naslednjim:

„2. Konstrukcija, preskušanje, namestitev, pregled, delovanje in popravilo pametnih tahografov in njihovih sestavnih delov so skladni s tehničnimi zahtevami iz Priloge IC k tej uredbi.

3. Konstrukcija, testiranje, namestitev, pregled, delovanje in popravilo tahografov, ki niso pametni tahografi, so še naprej skladni s Prilogo I k Uredbi (EU) št. 165/2014 ali Prilogo IB k Uredbi Sveta (EGS) št. 3821/85 (*), kot je ustrezno;

(*) Uredba Sveta (EGS) 3821/85 z dne 20. decembra 1985 o tahografu (nadzorni napravi) v cestnem prometu (UL L 370, 31.12.1985, str. 8).“;

(b) doda se naslednji odstavek 5:

„5. Ta uredba ne posega v Direktivo 2014/53/EU Evropskega parlamenta in Sveta (*).“;

(*) Direktiva 2014/53/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014 o harmonizaciji zakonodaj držav članic v zvezi z dostopnostjo radijske opreme na trgu in razveljavitvi Direktive 1999/5/ES (UL L 153, 22.5.2014, str. 62).

(2) člen 2 se spremeni:

(a) opredelitev pojma 3 se nadomesti z naslednjim:

„(3) ‚opisna mapa‘ pomeni popolno mapo v elektronski obliki ali na papirju, ki vsebuje vse informacije, ki jih proizvajalec ali njegov zastopnik sporoči homologacijskemu organu za namene homologacije tahografa ali njegovega dela, vključno s potrdili iz člena 12(3) Uredbe (EU) št. 165/2014, izvedbo preskusov, opredeljenih v Prilogi IC k tej uredbi, ter skicami, fotografijami in drugimi relevantnimi dokumenti;“;

([1]) Direktiva 2014/53/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014 o harmonizaciji zakonodaj držav članic v zvezi z dostopnostjo radijske opreme na trgu in razveljavitvi Direktive 1999/5/ES (UL L 153, 22.5.2014, str. 62).

(b) opredelitev pojma 7 se nadomesti z naslednjim:

„(7) ‚pametni tahograf' ali ‚tahograf druge generacije' pomeni digitalni tahograf, ki izpolnjuje določbe členov 8, 9 in 10 Uredbe (EU) št. 165/2014 ter Priloge IC k tej uredbi;";

(c) opredelitev pojma 8 se nadomesti z naslednjim:

„(8) ‚sestavni del tahografa' pomeni katerega koli od naslednjih elementov: enoto v vozilu, tipalo gibanja, tahografski vložek, zunanjo GNSS opremo in zunanjo opremo za zgodnje odkrivanje na daljavo;";

(d) doda se naslednja opredelitev pojma 10:

„(10) ‚enota v vozilu' pomeni tahograf, razen tipala gibanja in povezovalnih kablov tipala gibanja.

Zajema lahko eno samo enoto ali več enot, porazdeljenih po vozilu, in vključuje procesno enoto, pomnilnik podatkov, funkcijo merjenja časa, dve vmesniški napravi za pametni kartici voznika in sovoznika, tiskalnik, prikazovalnik, priključke in opremo za vnos uporabniških podatkov, GNSS sprejemnik in opremo za komunikacijo na daljavo.

Enoto v vozilu lahko sestavljajo naslednji homologirani sestavni deli:

— enota v vozilu kot en sam sestavni del (vključno z GNSS sprejemnikom in opremo za komunikacijo na daljavo),

— glavno ohišje enote v vozilu (vključno z opremo za komunikacijo na daljavo) in zunanja GNSS oprema,

— glavno ohišje enote v vozilu (vključno z GNSS sprejemnikom) in zunanja oprema za komunikacijo na daljavo,

— glavno ohišje enote v vozilu, zunanja GNSS oprema in zunanja oprema za komunikacijo na daljavo.

Če enota v vozilu sestoji iz več enot, porazdeljenih po vozilu, so procesna enota, pomnilnik podatkov in funkcija merjenja časa zajeti v glavnem ohišju enote v vozilu.

Izraz ‚enota v vozilu (VU)' se uporablja za ‚enoto v vozilu' ali ‚glavno ohišje enote v vozilu'.";

(3) v členu 6 se tretji odstavek nadomesti z naslednjim:

„Vendar pa se Priloga IC uporablja od 15. junija 2019, razen Dodatka 16, ki se uporablja od 2. marca 2016.";

(4) Priloga IC se spremeni v skladu s Prilogo I k tej uredbi;

(5) Priloga II se spremeni v skladu s Prilogo II k tej uredbi.

Člen 2

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 28. februarja 2018

Za Komisijo

Predsednik

Jean-Claude JUNCKER

PRILOGA I

Priloga IC k Uredbi (EU) 2016/799 se spremeni:

(1) Kazalo se spremeni:

(a) točka 3.12.5 se nadomesti z naslednjim:

„3.12.5 Kraji in položaji, kjer se dnevne delovne izmene začnejo in končajo in/ali kjer skupni čas vožnje doseže 3 ure“;

(b) točka 4.5.3.2.16 se nadomesti z naslednjim:

„4.5.3.2.16 Kraji, kjer skupni čas vožnje doseže tri ure“;

(c) točka 4.5.4.2.14 se nadomesti z naslednjim:

„4.5.4.2.14 Kraji, kjer skupni čas vožnje doseže tri ure“;

(d) točka 6.2 se nadomesti z naslednjim:

„6.2 Preverjanje novih ali popravljenih sestavnih delov“;

(2) točka 1 se spremeni:

(a) opredelitev pojma (ll) se nadomesti z naslednjim:

„(ll) ‚oprema za komunikacijo na daljavo‘ ali ‚oprema za zgodnje odkrivanje na daljavo‘ pomeni:

opremo enote v vozilu, ki se uporablja za izvedbo usmerjenega cestnega nadzora;“;

(b) opredelitev pojma (tt) se nadomesti z naslednjim:

„(tt) ‚nastavljanje časa‘ pomeni:

nastavljanje tekočega časa; to nastavljanje se lahko opravi samodejno v rednih presledkih z uporabo referenčnega časa, ki ga posreduje GNSS sprejemnik, ali v kalibracijskem načinu;“;

(c) prva alinea opredelitve pojma (yy) se nadomesti z naslednjim:

„— se namešča in uporablja samo v vozilih tipov M1 in N1 (kakor so opredeljena v Prilogi II k Direktivi 2007/46/ES Evropskega parlamenta in Sveta ([*]), kot je bila nazadnje spremenjena),“;

(d) doda se nova opredelitev pojma (fff):

„(fff) ‚skupni čas vožnje‘ pomeni:

vrednost, ki predstavlja skupno dosedanje število minut vožnje določenega vozila.

Vrednost skupnega časa vožnje je tekoča vsota vseh minut, ki se štejejo kot minute VOŽNJE, kot jih je zabeležila funkcija zapisovalne naprave za spremljanje voznikovih dejavnosti, in se uporablja samo za sprožitev zapisovanja položaja vozila, vsakič ko se doseže večkratnik treh ur skupnega časa vožnje. Štetje skupnega časa vožnje se začne ob aktivaciji zapisovalne naprave. Nanj ne vpliva nobeno drugo stanje, kot na primer stanje zunaj področja uporabe ali prevoz s trajektom/vlakom.

Vrednost skupnega časa vožnje ni predvidena za prikaz, tiskanje ali prenos;“;

(3) v točki 2.3 se zadnja alinea odstavka 13 nadomesti z naslednjim:

„— običajno obdobje veljavnosti za delovanje enot v vozilu je 15 let, z začetkom na dan datum začetka veljavnosti potrdil zanje, vendar se enote v vozilu lahko uporabljajo še nadaljnje 3 mesece, in sicer izključno za namen prenosa podatkov.“;

(4) v točki 2.4 se prvi odstavek nadomesti z naslednjim:

„Cilji varnosti sistema so zaščita pomnilnika podatkov s tem, da preprečuje nepooblaščene dostope do podatkov in nepooblaščeno manipuliranje z njimi ter da zaznava poskuse takih posegov, zaščita celovitosti in pristnosti podatkov, izmenjanih med tipalom gibanja in enoto v vozilu, zaščita celovitosti in pristnosti podatkov, izmenjanih med zapisovalno napravo in tahografskimi karticami, zaščita celovitosti in pristnosti podatkov, izmenjanih med enoto v vozilu in morebitno zunanjo GNSS opremo, zaščita zaupnosti, celovitosti in pristnosti podatkov, izmenjanih za namen nadzora prek komunikacije za zgodnje odkrivanje na daljavo, ter preverjanje celovitosti in pristnosti prenesenih podatkov.“;

(5) v točki 3.2 se druga alinea odstavka 27 nadomesti z naslednjim:

„— položajev, kjer skupni čas vožnje doseže večkratnik treh ur,“;

(6) v točki 3.4 se odstavek 49 nadomesti z naslednjim:

„(49) Za prvo spremembo dejavnosti v dejavnost ODMOR/POČITEK ali RAZPOLOŽLJIVOST v času 120 sekund od samodejne spremembe v dejavnost DELO zaradi ustavitve vozila velja, da je nastopila v trenutku, ko se je vozilo ustavilo (kar lahko prekliče prvotno spremembo v dejavnost DELO).“;

(7) v točki 3.6.1 se odstavek 59 nadomesti z naslednjim:

„(59) Voznik nato vnese trenutni kraj vozila, kar se šteje za začasni vnos.

Pod naslednjimi pogoji se začasni vnos, vpisan ob zadnjem izvleku kartice, potrdi (tj. se ne more več prepisati):

— kraj, kjer se začne trenutna dnevna delovna izmena, je vpisan med ročnim vnašanjem v skladu z zahtevo 61;

— naslednji vpis kraja, kjer se začne trenutna dnevna delovna izmena, če imetnik kartice med ročnim vnašanjem v skladu z zahtevo 61 ne vnese nobenega kraja, kjer se delovna izmena začne ali konča.

Pod naslednjimi pogoji se začasni vnos, vpisan ob zadnjem izvleku kartice, prepiše in se potrdi nova vrednost:

— naslednji vpis kraja, kjer se konča trenutna dnevna delovna izmena, če imetnik kartice med ročnim vnašanjem v skladu z zahtevo 61 ne vpiše nobenega kraja, kjer se delovna izmena začne ali konča.“;

(8) v točki 3.6.2 se šesta in sedma alinea nadomestita z naslednjim:

„— kraj, kjer se je končala prejšnja dnevna delovna izmena, v povezavi z ustreznim časom (s tem se prepiše in potrdi vpis ob zadnjem izvleku kartice),

— kraj, kjer se začne trenutna dnevna delovna izmena, v povezavi z ustreznim časom (s tem potrdi začasni vnos, vpisan ob zadnjem izvleku kartice),“;

(9) točka 3.9.15 se nadomesti z naslednjim:

„3.9.15 Dogodek ‚časovno navzkrižje‘

(86) Ta dogodek se sproži, **kadar naprava ni v kalibracijskem načinu**, če enota v vozilu med časom, ki ga beleži oprema za merjenje časa enote v vozilu, in časom, ki ga posreduje GNSS sprejemnik, zazna odstopanje, daljše od 1 minute. Ta dogodek se zapiše skupaj z internim časom enote v vozilu in ga spremlja samodejno nastavljanje časa. Po sproženju dogodka časovnega navzkrižja enota v vozilu 12 ur ne sproži drugih dogodkov časovnega navzkrižja. Ta dogodek se ne sproži, kadar GNSS sprejemnik 30 ali več dni ni mogel odkriti veljavnega GNSS signala.“;

(10) v točki 3.9.17 se doda naslednja alinea:

„— napaka na vmesniku z ITS (če je ustrezno).“;

(11) točka 3.10 se spremeni:

(i) besedilo pred preglednico v odstavku (89) se nadomesti z naslednjim:

„Zapisovalna naprava zaznava napake z izvajanjem vgrajenih preskusov in samopreskusov v skladu z naslednjo preglednico:“;

(ii) v tabeli se doda naslednja vrstica:

„Vmesnik z ITS (neobvezno)	Pravilno delovanje“	

(12) v točki 3.12 se druga alinea nadomesti z naslednjim:

„— povprečno število položajev na dan pomeni vsaj 6 položajev, kjer se začne dnevna delovna izmena, 6 položajev, kjer skupni čas vožnje doseže večkratnik treh ur, in 6 položajev, kjer se dnevna delovna izmena konča, tako da ‚365 dni‘ vključuje najmanj 6570 položajev;“;

(13) točka 3.12.5 se spremeni:

(a) naslov in odstavek 108 se nadomestita z naslednjim:

„3.12.5 Kraji in položaji, kjer se dnevne delovne izmene začnejo in končajo in/ali kjer skupni čas vožnje doseže 3 ure

(108) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani:

— kraje in položaje, kjer voznik in/ali sovoznik začne svojo dnevno delovno izmeno,

— položaje, kjer skupni čas vožnje doseže večkratnik treh ur,

— kraje in položaje, kjer voznik in/ali sovoznik konča svojo dnevno delovno izmeno.“;

(b) v odstavku 110 se četrta alinea nadomesti z naslednjim:

„— vrsto vnosa (čas začetka, čas konca ali dosežene 3 ure skupnega časa vožnje),“;

(c) odstavek 111 se nadomesti z naslednjim:

„(111) Pomnilnik podatkov je zmožen podatke o krajih in položajih, kjer se dnevne delovne izmene začnejo in končajo in/ali kjer skupni čas vožnje doseže 3 ure, hraniti najmanj 365 dni.“;

(14) v točki 3.12.7 se odstavek 116 nadomesti z naslednjim:

„(116) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani trenutno hitrost vozila ter ustrezajoči datum in čas vsako sekundo najmanj zadnjih 24 ur premikanja vozila.“;

(15) preglednica v točki 3.12.8 se spremeni:

(a) med vnosa „Ni informacij o položaju s strani GNSS sprejemnika“ in „Napaka v podatkih o gibanju“ se vstavi naslednji vnos:

„Napaka pri komuniciranju z zunanjo GNSS opremo	— Najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov, — 5 najdaljših dogodkov v zadnjih 365 dneh.	— Datum in čas začetka dogodka, — datum in čas konca dogodka, — vrsta, številka, država članica izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v danem dnevu.“

(b) vnos „časovno navzkrižje“ se nadomesti z naslednjim:

„Časovno navzkrižje	— najresnejši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov (tj. tisti z največjo razliko med datumom in časom zapisovalne naprave ter datumom in časom GNSS), — 5 najresnejših dogodkov v zadnjih 365 dneh.	— Datum in čas zapisovalne naprave, — datum in čas GNSS, — vrsta, številka, država članica izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v danem dnevu.“

(16) v točki 3.20 se odstavek (200) nadomesti z naslednjim:

„(200) Zapisovalne naprave so lahko opremljene tudi s standardiziranimi vmesniki, ki v delovnem ali kalibracijskem načinu omogočajo uporabo podatkov, ki jih je zapisal ali pripravil tahograf, z zunanjo opremo.

Neobvezni vmesnik z ITS je predpisan in standardiziran v Dodatku 13. Vzporedno s tem lahko delujejo tudi drugi vmesniki enote v vozilu, pod pogojem, da v celoti izpolnjujejo zahteve iz Dodatka 13 glede obveznih podatkov, varnosti in voznikove privolitve.

Voznikova privolitev ni potrebna v zvezi s podatki, ki se prenesejo z zapisovalne naprave v omrežje vozila. Kadar se osebni podatki, vneseni v omrežje vozila, nadalje obdelujejo zunaj omrežja vozila, mora proizvajalec vozila zagotoviti, da se ti osebni podatki obdelujejo v skladu z Uredbo (EU) 2016/679 (Splošna uredba o varstvu podatkov).

Prav tako voznikova privolitev ni potrebna v zvezi s podatki tahografa, ki se prenesejo zunanjemu podjetju (zahteva 193), saj je ta scenarij zajet v pravicah dostopa s kartico podjetja.

Za podatke ITS, ki so na voljo prek navedenega vmesnika, veljajo naslednje zahteve:

— ti podatki so niz izbranih obstoječih podatkov iz slovarja podatkov tahografa (Dodatek 1),

— podniz teh izbranih podatkov je označen kot ‚osebni podatki',

— podniz ‚osebni podatki' je na voljo samo, če je aktivirano preverljivo soglasje voznika, da njegovi osebni podatki lahko zapustijo omrežje vozila,

— privolitev voznika je možno kadar koli aktivirati ali deaktivirati z ukazi v meniju, pod pogojem, da je vstavljena vozniška kartica,

— niz in podniz podatkov se preneseta prek brezžičnega protokola Bluetooth v okolici voznikove kabine, s hitrostjo osveževanja ene minute,

— povezava zunanje naprave z vmesnikom z ITS se zaščiti z namensko in naključno določeno kodo PIN, sestavljeno iz vsaj 4 števk, ki je zapisana in posredovana preko prikazovalnika vsake od enot v vozilu,

— prisotnost vmesnika z ITS v nobenem primeru ne sme motiti ali vplivati na pravilno delovanje in varnost enote v vozilu.

Poleg niza izbranih obstoječih podatkov, ki štejejo za minimalni seznam, se lahko iznesejo tudi drugi podatki, pod pogojem, da se ne štejejo za osebne podatke.

Zapisovalna naprava je status privolitve voznika zmožna sporočiti drugim platformam v omrežju vozila.

Ko je električni kontakt vozila vključen, se ti podatki oddajajo ves čas.";

(17) v točki 3.23 se odstavek 211 nadomesti z naslednjim:

„(211) Čas notranje ure VU se samodejno nastavi vsakih 12 ur. Če taka nastavitev ni možna, ker GNSS signal ni na voljo, se nastavitev opravi takoj, ko VU dobi dostop do veljavnega časa, ki ga posreduje GNSS sprejemnik, v skladu s stanjem električnega kontakta vozila. Referenčni čas za samodejno nastavljanje časa notranje ure VU se izpelje na podlagi podatka iz GNSS sprejemnika.";

(18) v točki 3.26 se odstavka 225 in 226 nadomestita z naslednjim:

„(225) Na vsako samostojno nameščeno enoto zapisovalne naprave je pritrjena označevalna ploščica z naslednjimi podatki:

— ime in naslov proizvajalca opreme,

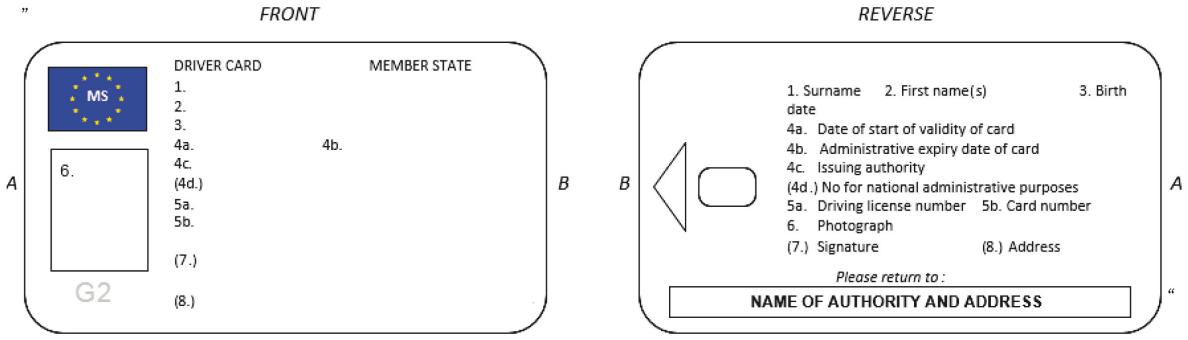
— proizvajalčeva kataloška številka dela in leto proizvodnje,

— serijska številka,

— homologacijska oznaka.

(226) Če prostor fizično ne omogoča prikaza vseh zgoraj omenjenih podatkov, označevalna ploščica prikazuje vsaj: ime ali logotip proizvajalca in kataloško številko dela.“;

(19) v točki 4.1 se slika, ki prikazuje prednjo in hrbtno stran vozniške kartice, nadomesti z naslednjo:



(20) v točki 4.5.3.1.8 se prva alinea odstavka 263 nadomesti z naslednjim:

„— napaka kartice (kjer pri napaki nastopa ta kartica),“;

(21) v točki 4.5.3.2.8 se prva alinea odstavka 288 nadomesti z naslednjim:

„— napaka kartice (kjer pri napaki nastopa ta kartica),“;

(22) točka 4.5.3.2.16 se nadomesti z naslednjim:

„4.5.3.2.16 Kraji, kjer skupni čas vožnje doseže tri ure

(305) Vozniška kartica je zmožna hraniti naslednje podatke, povezane s krajem, kjer skupni čas vožnje doseže večkratnik treh ur:

— datum in čas v trenutku, ko skupni čas vožnje doseže večkratnik treh ur,

— položaj vozila,

— točnost GNSS, datum in čas v trenutku, ko je bil določen položaj,

— vrednost števca prevožene poti.

(306) Vozniška kartica je zmožna hraniti najmanj 252 takih zapisov.“;

(23) točka 4.5.4.2.14 se nadomesti z naslednjim:

„4.5.4.2.14 Kraji, kjer skupni čas vožnje doseže tri ure

(353) Kartica servisne delavnice je zmožna hraniti naslednje podatke, povezane s krajem, kjer skupni čas vožnje doseže večkratnik treh ur:

— datum in čas v trenutku, ko skupni čas vožnje doseže večkratnik treh ur,

— položaj vozila,

— točnost GNSS, datum in čas v trenutku, ko je bil določen položaj,

— vrednost števca prevožene poti.

(354) Kartica servisne delavnice je zmožna hraniti najmanj 18 takih zapisov.“;

(24) v točki 5.2 se odstavek 396 nadomesti z naslednjim:

„(396) Na ploščici so navedeni vsaj naslednji podatki:

— ime, naslov ali trgovsko ime pooblaščenega izvajalca namestitve ali servisne delavnice,

— značilni koeficient vozila, izražen kot ‚w = … imp/km‘,

— konstanta zapisovalne naprave, izražena kot ‚k = … imp/km‘,

— dejanski obseg pnevmatik, izražen kot ‚l = … mm‘,

— velikost pnevmatik,

— datum merjenja značilnega koeficienta vozila in dejanskega obsega pnevmatik,

— identifikacijska številka vozila,

— prisotnost (ali odsotnost) zunanje GNSS opreme,

— serijska številka morebitne zunanje GNSS opreme,

— serijska številka morebitne naprave za komunikacijo na daljavo,

— serijske številke vseh nameščenih pečatov,

— del vozila, v katerega je nameščen morebitni pretvornik,

— del vozila, v katerega je nameščeno tipalo gibanja, če ni povezano z menjalnikom vozila ali če se ne uporablja pretvornik,

— barva kabla med pretvornikom in tistim delom vozila, ki zagotavlja vhodne impulze,

— serijska številka vgrajenega tipala gibanja na pretvorniku.“;

(25) točka 5.3 se spremeni:

(a) za odstavkom 398 se vstavi nov odstavek 398a:

„(398a) Zgoraj omenjeni pečati morajo biti certificirani v skladu s standardom EN 16882:2016.“;

(b) v odstavku (401) se drugi pododstavek nadomesti z naslednjim:

„Ta edinstvena identifikacijska številka je opredeljena kot: neodstranljiva oznaka MMNNNNNNNN, pri čemer je MM edinstvena identifikacija proizvajalca (vpisovanje v podatkovno zbirko izvaja Evropska komisija), NNNNNNNN pa edinstvena alfanumerična številka pečata, kot jo določi proizvajalec.“;

(c) odstavek 403 se nadomesti z naslednjim:

„(403) Ko pridobijo certifikat za model pečata v skladu s standardom EN 16882:2016, se proizvajalci pečatov vpišejo v namensko podatkovno zbirko, identifikacijske številke svojih pečatov pa javno objavijo v okviru postopka, ki ga določi Evropska komisija.“;

(d) odstavek 404 se nadomesti z naslednjim:

„(404) Pooblaščene servisne delavnice in proizvajalci vozil v okviru Uredbe (EU) št. 165/2014 uporabljajo samo v skladu s standardom EN 16882:2016 certificirane pečate tistih proizvajalcev, ki so vneseni v zgoraj omenjeni podatkovni zbirki.“;

(26) točka 6.2 se nadomesti z naslednjim:

„6.2 Preverjanje novih ali popravljenih sestavnih delov

(407) Vsako posamezno napravo, novo ali popravljeno, se preveri glede pravilnosti delovanja in točnosti odčitavanja in zapisovanja v okviru mej, predpisanih v poglavjih 3.2.1, 3.2.2, 3.2.3 in 3.3.“;

(27) v točki 6.3 se odstavek 408 nadomesti z naslednjim:

„(408) Ob namestitvi v vozilo celotna instalacija (vključno z zapisovalno napravo) izpolnjuje določbe glede največjih dovoljenih odstopanj iz poglavij 3.2.1, 3.2.2, 3.2.3 in 3.3. Celotna instalacija je zapečatena v skladu s poglavjem 5.3 in je kalibrirana.“;

(28) točka 8.1 se spremeni:

(a) v točki 8.1 se uvodno besedilo pred odstavkom 425 nadomesti z naslednjim:

„Za namen tega poglavja izraz ‚zapisovalna naprava‘ pomeni ‚zapisovalno napravo ali njene sestavne dele‘. Za kable, ki povezujejo tipalo gibanja z VU, zunanjo GNSS opremo z VU ali zunanjo opremo za komunikacijo na daljavo z VU, homologacija ni potrebna. Papir, ki ga uporablja zapisovalna naprava, se šteje za sestavni del zapisovalne naprave.

Vsak proizvajalec lahko zaprosi za homologacijo sestavnih delov zapisovalne naprave v kombinaciji s katerimi koli drugimi sestavnimi deli zapisovalne naprave pod pogojem, da so vsi takšni sestavni deli skladni z zahtevami iz te priloge. Sicer lahko proizvajalci zaprosijo tudi za homologacijo zapisovalne naprave.

Kot je opisano v opredelitvi pojma 10 v členu 2 te Uredbe, imajo enote v vozilu lahko različne sestave. Ne glede na njihovo sestavo, zunanja antena in (če se uporablja) razdelilnik za anteno, priključen na GNSS sprejemnik ali na opremo za komunikacijo na daljavo, nista vključena v homologacijo enote v vozilu.

Kljub temu proizvajalci, ki so pridobili homologacijo za zapisovalno napravo, hranijo javno dostopen seznam združljivih anten in razdelilnikov za vsako homologirano enoto v vozilu, zunanjo GNSS opremo in zunanjo opremo za komunikacijo na daljavo.“;

(b) odstavek 427 se nadomesti z naslednjim:

„(427) Pristojni homologacijski organi držav članic ne izdajo certifikata o homologaciji, dokler jim niso predloženi:

— potrdilo o varnosti (če se zahteva v skladu s to prilogo),

— potrdilo o funkcionalnosti in

— potrdilo o interoperabilnosti (če se zahteva v skladu s to prilogo)

za zapisovalno napravo ali tahografsko kartico, ki je predmet zahtevka za homologacijo.“;

(29) Dodatek 1 se spremeni:

(a) Kazalo se spremeni:

(i) točka 2.63. se nadomesti z naslednjim:

„2.63. Rezervirano za prihodnjo uporabo“;

(ii) točka 2.78. se nadomesti z naslednjim:

„2.78. GNSSAccumulatedDriving“;

(iii) točka 2.79. se nadomesti z naslednjim:

„2.79. GNSSAccumulatedDrivingRecord“;

(iv) točka 2.111. se nadomesti z naslednjim:

„2.111. NoOfGNSSADRecords“;

(v) točka 2.160. se nadomesti z naslednjim:

„2.160. Rezervirano za prihodnjo uporabo“;

(vi) točka 2.203. se nadomesti z naslednjim:

„2.203. VuGNSSADRecord“;

(vii) točka 2.204. se nadomesti z naslednjim:

„2.204. VuGNSSADRecordArray“;

(viii) točka 2.230. se nadomesti z naslednjim:

„2.230. Rezervirano za prihodnjo uporabo“;

(ix) točka 2.231. se nadomesti z naslednjim:

„2.231. Rezervirano za prihodnjo uporabo“;

(b) v točki 2 se pred točko 2.1. doda naslednje besedilo:

„Za podatkovne tipe na karticah, ki se uporabljajo za aplikacije prve ali druge generacije, je velikost, določena v tem dodatku, velikost za aplikacije druge generacije. Velikost za aplikacije prve generacije naj bi bila bralniku že znana. Zahteve iz Priloge IC, ki navajajo številke v povezavi s takšnimi podatkovnimi tipi, zajemajo aplikacije tako prve kot tudi druge generacije.“;

(c) točka 2.19. se nadomesti z naslednjim:

„2.19. **CardEventData**

Prva generacija:

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z dogodki v zvezi z imetnikom kartice (zahtevi 260 in 318 iz Priloge IC).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
  cardEventRecords                    SET SIZE(NoOfEventsPerType) OF
                                      CardEventRecord
}
```

CardEventData je niz, urejen po naraščajoči vrednosti EventFaultType, zapisov cardEventRecords (razen zapisov poskusov kršenja varnosti, ki so zbrani v zadnji množici niza).

cardEventRecords je množica zapisov dogodkov določene vrste (ali kategorije pri dogodkih poskusov kršenja varnosti).

Druga generacija:

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z dogodki v zvezi z imetnikom kartice (zahtevi 285 in 341 iz Priloge IC).

```
CardEventData ::= SEQUENCE SIZE(11) OF {
  cardEventRecords                    SET SIZE(NoOfEventsPerType) OF
                                      CardEventRecord
}
```

CardEventData je niz, urejen po naraščajoči vrednosti EventFaultType, zapisov cardEventRecords (razen zapisov poskusov kršenja varnosti, ki so zbrani v zadnji množici niza).

cardEventRecords je množica zapisov dogodkov določene vrste (ali kategorije pri dogodkih poskusov kršenja varnosti).“;

(d) točka 2.30. se nadomesti z naslednjim:

„2.30. **CardRenewalIndex**

Indeks podaljšanja kartice (opredelitev i).

```
CardRenewalIndex::= IA5String(SIZE(1))
```

Dodeljena vrednost: (glej poglavje 7 te Priloge).

„0“ Prva izdaja. ‚0‘ Prva izdaja.

Vrstni red pri povečevanju: ‚0, …, 9, A, …, Z‘“;

(e) v točki 2.61. se besedilo za podnaslovom „Druga generacija“ nadomesti z naslednjim:

```
„DriverCardApplicationIdentification ::= SEQUENCE {
typeOfTachographCardId          EquipmentType,
cardStructureVersion            CardStructureVersion,
noOfEventsPerType               NoOfEventsPerType,
noOfFaultsPerType               NoOfFaultsPerType,
activityStructureLength         CardActivityLengthRange,
noOfCardVehicleRecords          NoOfCardVehicleRecords,
noOfCardPlaceRecords            NoOfCardPlaceRecords,
noOfGNSSADRecords               NoOfGNSSADRecords,
noOfSpecificConditionRecords    NoOfSpecificConditionRecords
noOfCardVehicleUnitRecords      NoOfCardVehicleUnitRecords
}
```

Poleg elementov za prvo generacijo se uporabljajo še naslednji podatkovni elementi:

noOfGNSSADRecords je število GNSS zapisov skupnega časa vožnje, ki jih lahko hrani kartica.

noOfSpecificConditionRecords je število zapisov posebnih pogojev, ki jih lahko hrani kartica.

noOfCardVehicleRecords je število zapisov o uporabljenih enotah v vozilu, ki jih lahko hrani kartica.“;

(f) točka 2.63. se nadomesti z naslednjim:

„2.63. **Rezervirano za prihodnjo uporabo**“;

(g) v točki 2.67. se besedilo pod podnaslovom „Druga generacija“ nadomesti z naslednjim:

„uporabljajo se enake vrednosti kot pri prvi generaciji, z naslednjimi dodatki:

```
--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
--Driver Card (Sign)            (17),--only to be used in the CHA
                                field of a signing certificate
--Workshop Card (Sign)          (18), --only to be used in the CHA
                                field of a signing certificate
--Vehicle Unit (Sign)           (19), --only to be used in the CHA
                                field of a signing certificate
--RFU                           (20..255)
```

Opomba 1: vrednosti za drugo generacijo za ploščico, pretvornik in zunanjo GNSS povezavo ter vrednosti za prvo generacijo za enoto v vozilu in tipalo gibanja se lahko uporabljajo v SealRecord, tj. če se uporablja.

Opomba 2: V polju CardHolderAuthorisation (CHA) za certifikat druge generacije se vrednosti (1), (2) in (6) razumejo kot navedba certifikata za medsebojno avtentikacijo za zadevno vrsto opreme. Za navedbo ustreznega certifikata za ustvarjanje digitalnega podpisa je treba uporabiti vrednost 17, 18 ali 19.“;

(h) v točki 2.70. se besedilo pod podnaslovom „Druga generacija“ nadomesti z naslednjim:

„Druga generacija:

'0x'H	Splošni dogodki
'00'H	Ni dodatnih podrobnosti
'01'H	Vstavitev neveljavne kartice
'02'H	Navzkrižje med karticami
'03'H	Časovno prekrivanje
'04'H	Vožnja brez ustrezne kartice
'05'H	Vstavitev kartice med vožnjo
'06'H	Zadnja seja s kartico nepravilno zaključena
'07'H	Prekoračitev hitrosti
'08'H	Izpad napajanja
'09'H	Napaka v podatkih o gibanju
'0A'H	Navzkrižje v gibanju vozila
'0B'H	Časovno navzkrižje (med GNSS in notranjo uro VU)
'0C'H	Napaka pri komuniciranju z opremo za komunikacijo na daljavo
'0D'H	Ni informacij o položaju s strani GNSS sprejemnika
'0E'H	Napaka pri komuniciranju z zunanjo GNSS opremo
'0F'H	RFU
'1x'H	Dogodki poskusov kršenja varnosti, povezani z enoto v vozilu
'10'H	Ni dodatnih podrobnosti
'11'H	Neuspešna avtentikacija tipala gibanja
'12'H	Neuspešna avtentikacija tahografske kartice
'13'H	Nepooblaščena zamenjava tipala gibanja
'14'H	Napaka v celovitosti vhodnih podatkov s kartice
'15'H	Napaka v celovitosti shranjenih podatkov uporabnika
'16'H	Napaka pri notranjem prenosu podatkov
'17'H	Nepooblaščeno odprtje ohišja
'18'H	Sabotaža strojne opreme
'19'H	Zaznavanje poskusov manipulacije GNSS
'1A'H	Neuspešna avtentikacija zunanje GNSS opreme
'1B'H	Certifikat zunanje GNSS opreme je potekel
'1C'H to '1F'H	RFU
'2x'H	Dogodki poskusov kršenja varnosti, povezani s tipalom
'20'H	Ni dodatnih podrobnosti
'21'H	Neuspešna avtentikacija
'22'H	Napaka v celovitosti shranjenih podatkov
'23'H	Napaka pri notranjem prenosu podatkov
'24'H	Nepooblaščeno odprtje ohišja
'25'H	Sabotaža strojne opreme
'26'H to '2F'H	RFU
'3x'H	Napake zapisovalne naprave
'30'H	Ni dodatnih podrobnosti
'31'H	Notranja napaka VU
'32'H	Napaka na tiskalniku
'33'H	Napaka na prikazovalniku
'34'H	Napaka pri prenosu podatkov
'35'H	Napaka na tipalu
'36'H	Napaka na notranjem GNSS sprejemniku
'37'H	Napaka na zunanji GNSS opremi
'38'H	Napaka na opremi za komunikacijo na daljavo
'39'H	Napaka na vmesniku z ITS
'3A'H to '3F'H	RFU
'4x'H	Napake na kartici
'40'H	Ni dodatnih podrobnosti
'41'H to '4F'H	RFU
'50'H to '7F'H	RFU
'80'H to 'FF'H	Določi proizvajalec“;

(i) točka 2.71. se nadomesti z naslednjim:

„2.71. **ExtendedSealIdentifier**

Druga generacija:

podaljšani identifikator pečata edinstveno identificira pečat (zahteva 401 iz Priloge IC).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                OCTET STRING (SIZE(2)),
   sealIdentifier                  OCTET STRING (SIZE(8))
}
```

manufacturerCode je koda proizvajalca pečata.

sealIdentifier je identifikator za pečat, ki je glede na proizvajalca edinstven.“;

(j) točki 2.78. in 2.79. se nadomestita z naslednjim:

„2.78. **GNSSAccumulatedDriving**

Druga generacija:

informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z GNSS položajem vozila, če skupni čas vožnje doseže večkratnik treh ur (zahtevi 306 in 354 iz Priloge IC).

```
GNSSAccumulatedDriving := SEQUENCE {
   gnssADPointerNewestRecord       INTEGER(0..NoOfGNSSADRecords -1),
   gnssAccumulatedDrivingRecords   SET SIZE(NoOfGNSSADRecords) OF
                                   GNSSAccumulatedDrivingRecord
}
```

placePointerNewestRecord je indeks zadnjega posodobljenega GNSS zapisa skupnega časa vožnje.

Dodeljena vrednost je število, ki ustreza števcu GNSS zapisa skupnega časa vožnje; začne se z vrednostjo ‘0’ za prvi GNSS zapis skupnega časa vožnje v strukturi.

gnssContinuousDrivingRecords je množica podatkov, ki vsebujejo datum in čas, ko skupni čas vožnje doseže večkratnik treh ur, in informacijo o položaju vozila.

2.79. **GNSSAccumulatedDrivingRecord**

Druga generacija:

informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z GNSS položajem vozila, če skupni čas vožnje doseže večkratnik treh ur (zahtevi 305 in 353 iz Priloge IC).

```
GNSSAccumulatedDrivingRecord ::= SEQUENCE {
  timeStamp                    TimeReal,
  gnssPlaceRecord              GNSSPlaceRecord,
  vehicleOdometerValue         OdometerShort
}
```

timeStamp je datum in čas v trenutku, ko skupni čas vožnje doseže večkratnik treh ur.

gnssPlaceRecord vsebuje informacijo, povezano s položajem vozila.

vehicleOdometerValue je vrednost števca prevožene poti v trenutku, ko skupni čas vožnje doseže večkratnik treh ur.“;

(k) točka 2.86. se nadomesti z naslednjim:

„2.86. **KeyIdentifier**

Edinstveni identifikator javnega ključa, uporabljen za sklicevanje in izbiranje ključa. Identificira tudi imetnika ključa.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber          ExtendedSerialNumber,
   certificateRequestID          CertificateRequestID,
   certificationAuthorityKID     CertificationAuthorityKID
}
```

Prva oblika je primerna za sklicevanje na javni ključ enote v vozilu, tahografske kartice ali zunanje GNSS opreme.

Druga oblika je primerna za sklicevanje na javni ključ enote v vozilu (kadar v času tvorbe certifikata ni mogoče poznati serijske številke enote v vozilu).

Tretja oblika je primerna za sklicevanje na javni ključ države članice.“;

(l) točka 2.92. se nadomesti z naslednjim:

„2.92. **MAC**

Druga generacija:

kriptografska kontrolna vsota dolžine 8, 12 ali 16 bajtov, ki ustreza nizom kod iz Dodatka 11.

```
MAC ::= CHOICE {
   Mac8                 OCTET STRING (SIZE(8)),
   Mac12                OCTET STRING (SIZE(12)),
   Mac16                OCTET STRING (SIZE(16)),
}“;
```

(m) točka 2.111. se nadomesti z naslednjim:

„2.111. **NoOfGNSSADRecords**

Druga generacija:

število GNSS zapisov skupnega časa vožnje, ki jih lahko hrani kartica.

NoOfGNSSADRecords ::= INTEGER (0..2^{16}-1)

Dodeljena vrednost: glej Dodatek 2.“;

(n) v točki 2.120. se dodeljena vrednost „16H“ nadomesti z naslednjim:

„'16'H VuGNSSADRecord “;

(o) točka 2.160. se nadomesti z naslednjim:

„2.160. **Rezervirano za prihodnjo uporabo**“;

(p) točka 2.162. se nadomesti z naslednjim:

„2.162. **TimeReal**

Koda sestava datum/čas, v kateri sta datum in čas izražena kot število sekund od časa 00h.00m.00s. po UTC dne 1. januarja 1970.

```
TimeReal {INTEGER:TimeRealRange} ::= INTEGER (0..TimeRealRange)
```

Dodeljena vrednost – oktetno poravnano: Število sekund od polnoči 1. januarja 1970 po UTC.

Najpoznejši možni datum/čas je v letu 2106.“;

(q) točka 2.179. se nadomesti z naslednjim:

„2.179. **VuCardRecord**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z uporabljeno tahografsko kartico (zahteva 132 iz Priloge IC).

```
VuCardRecord ::= SEQUENCE {
cardNumberAndGenerationInformation      FullCardNumberAndGeneration,
cardExtendedSerialNumber                ExtendedSerialNumber,
cardStructureVersion                    CardStructureVersion,
cardNumber                              CardNumber
}
```

cardNumberAndGenerationInformation je celotna številka in generacija uporabljene kartice (podatkovni tip 2.74.).

cardExtendedSerialNumber, kot se prebere s kartice iz datoteke EF_ICC v MF.

cardStructureVersion, kot se prebere iz datoteke EF_Application_Identification v DF_Tachograph_G2.

cardNumber, kot se prebere iz datoteke EF_Application_Identification v DF_Tachograph_G2.“;

(r) točki 2.203. in 2.204. se nadomestita z naslednjim:

„2.203. **VuGNSSADRecord**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z GNSS položajem vozila, če skupni čas vožnje doseže večkratnik treh ur (zahtevi 108 in 110 iz Priloge IC).

```
VuGNSSADRecord ::= SEQUENCE {
   timeStamp                        TimeReal,
   cardNumberAndGenDriverSlot       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot     FullCardNumberAndGeneration,
   gnssPlaceRecord                  GNSSPlaceRecord,
   vehicleOdometerValue             OdometerShort
}
```

timeStamp je datum in čas v trenutku, ko skupni čas vožnje doseže večkratnik treh ur.

cardNumberAndGenDriverSlot identificira kartico, vstavljeno v voznikovo režo, vključno z njeno generacijo.

cardNumberAndGenCodriverSlot identificira kartico, vstavljeno v sovoznikovo režo, vključno z njeno generacijo.

gnssPlaceRecord vsebuje informacijo, povezano s položajem vozila.

vehicleOdometerValue je vrednost števca prevožene poti v trenutku, ko skupni čas vožnje doseže večkratnik treh ur.

2.204. **VuGNSSADRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z GNSS položajem vozila, če skupni čas vožnje doseže večkratnik treh ur (zahtevi 108 in 110 iz Priloge IC).

```
VuGNSSADRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF VuGNSSADRecord
}
```

recordType označuje vrsto zapisa (VuGNSSADRecord).

Dodeljena vrednost: Glej RecordType.

recordSize je v bajtih izražena velikost VuGNSSADRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica GNSS zapisov skupnega časa vožnje.“;

(s) točki 2.230. in 2.231. se nadomestita z naslednjim:

„2.230. Rezervirano za prihodnjo uporabo

2.231. Rezervirano za prihodnjo uporabo“;

(t) v točki 2.234. se besedilo pod podnaslovom „Druga generacija“ nadomesti z naslednjim:

```
„WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId               EquipmentType,
    cardStructureVersion                 CardStructureVersion,
    noOfEventsPerType                    NoOfEventsPerType,
    noOfFaultsPerType                    NoOfFaultsPerType,
    activityStructureLength              CardActivityLengthRange,
    noOfCardVehicleRecords               NoOfCardVehicleRecords,
    noOfCardPlaceRecords                 NoOfCardPlaceRecords,
    noOfCalibrationRecords               NoOfCalibrationRecords,
    noOfGNSSADRecords                    NoOfGNSSADRecords,
    noOfSpecificConditionRecords         NoOfSpecificConditionRecords,
    noOfCardVehicleUnitRecords           NoOfCardVehicleUnitRecords
}
```

Poleg elementov za prvo generacijo se uporabljajo še naslednji podatkovni elementi:

noOfGNSSADRecords je število GNSS zapisov skupnega časa vožnje, ki jih lahko hrani kartica.

noOfSpecificConditionRecords je število zapisov posebnih pogojev, ki jih lahko hrani kartica.

noOfCardVehicleRecords je število zapisov o uporabljenih enotah v vozilu, ki jih lahko hrani kartica.“;

(30) Dodatek 2 se spremeni:

(a) v točki 1.1. se dodajo naslednje kratice:

„CHA pooblastilo imetnika certifikata

DO podatkovni objekt“;

(b) točka 3.3. se spremeni:

(i) odstavek TCS_24 se nadomesti z naslednjim:

„TCS_24 Ti varnostni pogoji so lahko povezani na naslednje načine:

IN: izpolnjeni morajo biti vsi varnostni pogoji.

ALI: izpolnjen mora biti najmanj en varnostni pogoj.

Pravila dostopa za datotečni sistem, tj. ukazi SELECT, READ BINARY in UPDATE BINARY, so določena v poglavju 4. Pravila dostopa za preostale ukaze so določena v naslednjih tabelah. Izraz ‚Ni relevantno‘ se uporabi, kadar ni zahteve za podporo zadevnega ukaza. V tem primeru je ukaz lahko podprt ali ne, vendar je pogoj za dostop zunaj področja veljavnosti.“;

(ii) v odstavku TCS_25 se tabela nadomesti z naslednjim:

„Ukaz	Vozniška kartica	Kartica servisne delavnice	Nadzorna kartica	Kartica podjetja
External Authenticate				
— za avtentikacijo prve generacije	ALW	ALW	ALW	ALW
— za avtentikacijo 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	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
PSO: Compute Digital Signature	ALW ALI SM-MAC-G2	ALW ALI SM-MAC-G2	Ni relevantno	Ni relevantno
PSO: Hash	Ni relevantno	Ni relevantno	ALW	Ni relevantno

Ukaz	Vozniška kartica	Kartica servisne delavnice	Nadzorna kartica	Kartica podjetja
PERFORM HASH of FILE	ALW ALI SM-MAC-G2	ALW ALI SM-MAC-G2	Ni relevantno	Ni relevantno
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ni relevantno	Ni relevantno	ALW	Ni relevantno
Verify	Ni relevantno	ALW	Ni relevantno	Ni relevantno“

(iii) v odstavku TCS_26 se tabela nadomesti z naslednjim:

„Ukaz	Vozniška kartica	Kartica servisne delavnice	Nadzorna kartica	Kartica podjetja
External Authenticate				
— za avtentikacijo prve generacije	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
— za avtentikacijo druge generacije	ALW	PWD	ALW	ALW
Internal Authenticate	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
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	Ni relevantno	ALW	ALW	Ni relevantno
PSO: Compute Digital Signature	ALW ALI SM-MAC-G2	ALW ALI SM-MAC-G2	Ni relevantno	Ni relevantno
PSO: Hash	Ni relevantno	Ni relevantno	ALW	Ni relevantno
PERFORM HASH of FILE	ALW ALI SM-MAC-G2	ALW ALI SM-MAC-G2	Ni relevantno	Ni relevantno
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ni relevantno	Ni relevantno	ALW	Ni relevantno
Verify	Ni relevantno	ALW	Ni relevantno	Ni relevantno“

(iv) v odstavku TCS_27 se tabela nadomesti z naslednjim:

„Ukaz	Vozniška kartica	Kartica servisne delavnice	Nadzorna kartica	Kartica podjetja
External Authenticate				
— za avtentikacijo prve generacije	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
— za avtentikacijo druge generacije	ALW	PWD	ALW	ALW
Internal Authenticate	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
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	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
PSO: Compute Digital Signature	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
PSO: Hash	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
PERFORM HASH of FILE	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
Verify	Ni relevantno	ALW	Ni relevantno	Ni relevantno“

(c) v točki 3.4. se odstavek TCS_29 nadomesti z naslednjim:

„TCS_29 Opisa stanja SW1 in SW2 se vrneta v vsakem sporočilu z odzivom in označujeta stanje obdelave ukaza.

SW1	SW2	Pomen
90	00	Normalna obdelava.
61	XX	Normalna obdelava. XX = število razpoložljivih bajtov za odziv.
62	81	Opozorilo glede obdelave. Del vrnjenih podatkov je morda poškodovanih.
63	00	Neuspešna avtentikacija (opozorilo).
63	CX	Napačen CHV (PIN). Števec preostalih poskusov je podan v ‚X‘.

SW1	SW2	Pomen
64	00	Napaka pri izvedbi – stanje trajnega pomnilnika nespremenjeno. Napaka celovitosti.
65	00	Napaka pri izvedbi – stanje trajnega pomnilnika spremenjeno.
65	81	Napaka pri izvedbi – stanje trajnega pomnilnika spremenjeno – napaka pomnilnika.
66	88	Varnostna napaka: napačna kriptografska kontrolna vsota (med varnim sporočanjem) ali napačen certifikat (med preverjanjem certifikata) ali napačen kriptogram (med zunanjo avtentikacijo) ali napačen podpis (med preverjanjem podpisa).
67	00	Napačna dolžina (napačen Lc ali Le).
68	83	Pričakovan zadnji ukaz iz verige.
69	00	Prepovedan ukaz (pri T=0 ni razpoložljivega odziva)
69	82	Varnostni status ni zadovoljiv.
69	83	Metoda avtentikacije blokirana.
69	85	Pogoji uporabe niso izpolnjeni.
69	86	Ukaz ni dovoljen (ni trenutne EF).
69	87	Manjkajo pričakovani podatkovni objekti varnega sporočanja.
69	88	Nepravilni podatkovni objekti varnega sporočanja.
6A	80	Nepravilni parametri v podatkovnem polju.
6A	82	Datoteka ni najdena.
6A	86	Napačna parametra P1-P2.
6A	88	Podatki, na katere se sklicuje ukaz, niso najdeni.
6B	00	Napačni parametri (zamik zunaj EF).
6C	XX	Napačna dolžina, SW2 označuje točno dolžino. Ni vrnjeno nobeno podatkovno polje.
6D	00	Koda instrukcije ni podprta ali ni veljavna.
6E	00	Razred ni podprt.
6F	00	— Druge napake pri preverjanju.

Vrnejo se lahko drugi opisi stanja, kot so opredeljeni v standardu ISO/IEC 7816-4, če njihovo vedenje ni izrecno omenjeno v tem dodatku.

Tako se lahko na primer vrnejo naslednji opisi stanja:

6881: Logični kanal ni podprt.

6882: Varno sporočanje ni podprto.“;

(d) v točki 3.5.1.1 se zadnja alinea odstavka TCS_38 nadomesti z naslednjim:

„— Če se izbrana aplikacija šteje za poškodovano (v atributih datoteke je zaznana napaka celovitosti), se vrne stanje obdelave ‚**6400**‘ ali ‚**6500**‘.“;

(e) v točki 3.5.1.2 se zadnja alinea odstavka TCS_41 nadomesti z naslednjim:

„— Če se izbrana datoteka šteje za poškodovano (v atributih datoteke je zaznana napaka celovitosti), se vrne stanje obdelave ‚**6400**‘ ali ‚**6500**‘.“;

(f) v točki 3.5.2.1 se šesta alinea odstavka TCS_43 nadomesti z naslednjim:

„— Če je zaznana napaka celovitosti v atributih datoteke, kartica šteje datoteko za poškodovano in nepopravljivo, vrne se stanje obdelave ‚**6400**‘ ali ‚**6500**‘.“;

(g) točka 3.5.2.1.1 se spremeni:

(i) v odstavku TCS_45 se tabela nadomesti z naslednjim:

„Bajt	Dolžina	Vrednost	Opis
#1	1	‚81h‘	T_{PV}: oznaka za nešifrirane podatke
#2	L	‚NNh‘ ali ‚81 NNh‘	L_{PV}: dolžina vrnjenih podatkov (=prvotni Le) L je 2 bajta, če je L_{PV} > 127 bajtov
#(2+L) – #(1+L+NN)	NN	‚XX..XXh‘	Nešifrirana vrednost podatkov
#(2+L+NN)	1	‚99h‘	Oznaka za stanje obdelave (SW1-SW2) – neobvezno za varno sporočanje prve generacije
#(3+L+NN)	1	‚02h‘	Dolžina stanja obdelave – neobvezno za varno sporočanje prve generacije
#(4+L+NN) – #(5+L+NN)	2	‚XX XXh‘	Stanje obdelave nezaščitenega odziva APDU – neobvezno za varno sporočanje prve generacije
#(6+L+NN)	1	‚8Eh‘	TCC: oznaka za kriptografsko kontrolno vsoto
#(7+L+NN)	1	‚XXh‘	LCC: dolžina naslednje kriptografske kontrolne vsote ‚04h‘ za varno sporočanje prve generacije (glej Del A iz Dodatka 11) ‚08h‘, ‚0Ch‘ ali ‚10h‘, odvisno od dolžine ključa AES, za varno sporočanje druge generacije (glej Del B iz Dodatka 11)

Bajt	Dolžina	Vrednost	Opis
#(8+L+NN) – #(7+M+L+NN)	M	‚XX..XXh‘	Kriptografska kontrolna vsota
SW	2	‚XXXXh‘	Opis stanja (SW1, SW2)“

(ii) v odstavku TCS_46 se tabela nadomesti z naslednjim:

„Bajt	Dolžina	Vrednost	Opis
#1	1	‚87h‘	$T_{PI\ CG}$: oznaka za šifrirane podatke (kriptogram)
#2	L	‚MMh‘ ali ‚81 MMh‘	$L_{PI\ CG}$: dolžina vrnjenih šifriranih podatkov (različna od originalne vednosti Le iz ukaza zaradi zapolnitve) L je 2 bajta, če je LPI CG > 127 bajtov
#(2+L) – #(1+L+MM)	MM	‚01XX..XXh‘	Šifrirani podatki: zapolnitveni kazalnik in kriptogram
#(2+L+MM)	1	‚99h‘	Oznaka za stanje obdelave (SW1-SW2) – neobvezno za varno sporočanje prve generacije
#(3+L+MM)	1	‚02h‘	Dolžina stanja obdelave – neobvezno za varno sporočanje prve generacije
#(4+L+MM) – #(5+L+MM)	2	‚XX XXh‘	Stanje obdelave nezaščitenega odziva APDU – neobvezno za varno sporočanje prve generacije
#(6+L+MM)	1	‚8Eh‘	TCC: oznaka za kriptografsko kontrolno vsoto
#(7+L+MM)	1	‚XXh‘	LCC: dolžina naslednje kriptografske kontrolne vsote ‚04h‘ za varno sporočanje prve generacije (glej Del A iz Dodatka 11) ‚08h‘, ‚0Ch‘ ali ‚10h‘, odvisno od dolžine ključa AES, za varno sporočanje druge generacije (glej Del B iz Dodatka 11)
#(8+L+MM) – #(7+N+L+MM)	N	‚XX..XXh‘	Kriptografska kontrolna vsota
SW	2	‚XXXXh‘	Opis stanja (SW1, SW2)“

(h) v točki 3.5.2.2 se šesta alinea odstavka TCS_50 nadomesti z naslednjim:

„— Če je zaznana napaka celovitosti v atributih datoteke, kartica šteje datoteko za poškodovano in nepopravljivo, vrne se stanje obdelave ‚**6400**‘ ali ‚**6500**‘.“;

(i) v točki 3.5.2.3 se odstavek TCS_52 nadomesti z naslednjim:

(i) zadnja vrstica tabele se nadomesti z naslednjim:

„Le	1	‚XXh‘	Kakor določa ISO/IEC 7816-4.“;

(ii) doda se naslednji stavek:

„Če se ne uporablja varno sporočanje in je T = 0, kartica privzame vrednost Le = ‚00h'.

Če je T = 1 in Le = ‚01h', se vrne stanje obdelave ‚6700'.";

(j) v točki 3.5.2.3 se šesta alinea odstavka TCS_53 nadomesti z naslednjim:

„— Če je zaznana napaka celovitosti v atributih datoteke, kartica šteje datoteko za poškodovano in nepopravljivo, vrne se stanje obdelave ‚**6400**' ali ‚**6500**'.";

(k) v točki 3.5.3.2 se šesta alinea odstavka TCS_63 nadomesti z naslednjim:

„— Če je zaznana napaka celovitosti v atributih datoteke, kartica šteje datoteko za poškodovano in nepopravljivo, vrne se stanje obdelave ‚**6400**' ali ‚**6500**'.";

(l) v točki 3.5.5 se odstavek TCS_72 nadomesti z naslednjim:

„TCS_72 PIN, ki ga vnese uporabnik, mora IFD kodirati v ASCII in na desni zapolniti z bajti ‚FFh' do skupne dolžine 8 bajtov, glej tudi podatkovni tip WorkshopCardPIN iz Dodatka 1.";

(m) v točki 3.5.8 se odstavek TCS_95 nadomesti z naslednjim:

„TCS_95 Če je ukaz INTERNAL AUTHENTICATE uspešen, se trenutni ključ seje prve generacije (če obstaja) izbriše in ni več na voljo. Pogoj za razpoložljivost novega ključa seje prve generacije je uspešna izvedba ukaza EXTERNAL AUTHENTICATE za avtentikacijski mehanizem prve generacije.

Opomba: Za ključe seje druge generacije glej CSM_193 in CSM_195 v Dodatku 11. Če so vzpostavljeni ključi seje druge generacije in tahografska kartica prejme ukaz APDU INTERNAL AUTHENTICATE v neformatiranem besedilu, prekine sejo varnega sporočanja druge generacije in uniči ključe seje druge generacije.";

(n) v točki 3.5.9 se odstavek TCS_97 nadomesti z naslednjim:

„TCS_97 Različica ukaza za medsebojno avtentikacijo kartice in enote v vozilu se lahko izvede le pri MF, DF Tachograph in DF Tachograph_G2, glej tudi TCS_34. Če je ta ukaz EXTERNAL AUTHENTICATE druge generacije uspešen, se trenutni ključ seje prve generacije (če obstaja) izbriše in ni več na voljo.

Opomba: Za ključe seje druge generacije glej CSM_193 in CSM_195 v Dodatku 11. Če so vzpostavljeni ključi seje druge generacije in tahografska kartica prejme ukaz APDU EXTERNAL AUTHENTICATE v neformatiranem besedilu, prekine sejo varnega sporočanja druge generacije in uniči ključe seje druge generacije.";

(o) v točki 3.5.10 se v tabeli v odstavku TCS_101 doda naslednja vrstica:

„5 + L + 1	1	‚00h'	Kakor določa ISO/IEC 7816-4"

(p) v točki 3.5.11.2.3 se v odstavku TCS_114 doda naslednje:

„— Če je currentAuthenticatedTime kartice poznejši od datuma izteka izbranega javnega ključa, se vrne stanje obdelave **‚6A88'**.

Opomba: Če je poslan ukaz MSE:SET AT za avtentikacijo VU, je navedeni ključ javni ključ VU_MA. Če je na voljo v njenem spominu, kartica za uporabo nastavi tisti javni ključ VU_MA, ki se sklada z referenco imetnika certifikata (CHR), navedeno v polju s podatki ukaza (kartica javne ključe VU_MA lahko identificira na podlagi polja CHA v certifikatu). Kadar je na voljo samo javni ključ VU_Sign ali kadar ni na voljo noben javni ključ enote v vozilu, kartica na ta ukaz vrne stanje obdelave ‚6A 88'. Glej opredelitev polja CHA v Dodatku 11 in podatkovnega tipa equipmentType v Dodatku 1.

Če je nadzorni kartici poslan ukaz MSE:SET DST z navedbo EQT (tj. z VU ali kartico), je v skladu s CSM_234 navedeni ključ vedno ključ EQT_Sign, ki se mora uporabiti za preverjanje digitalnega podpisa. Kot je prikazano na sliki 13 v Dodatku 11, je ustrezen javni ključ EQT_Sign vedno shranjen na nadzorni kartici. V nekaterih primerih je na kontrolni kartici morda shranjen ustrezni javni ključ EQT_MA. Ko prejme ukaz MSE:SET DST, kontrolna kartica vedno za uporabo nastavi javni ključ EQT_Sign.";

(q) točka 3.5.13 se spremeni:

(i) odstavek TCS_121 se nadomesti z naslednjim:

„TCS_121 Začasno shranjena vrednost HASH of FILE se izbriše, če se z ukazom PERFORM HASH of FILE izračuna nova vrednost HASH of FILE, če je izbran DF in če se tahografska kartica ponastavi.";

(ii) odstavek TCS_123 se nadomesti z naslednjim:

„TCS_123 Tahografska aplikacija druge generacije za ključ podpisa kartice Card_Sign podpira algoritem SHA-2 SHA-256, SHA-384 ali SHA-512, določen z naborom algoritmov v Delu B Dodatka 11.";

(iii) tabela v odstavku TCS_124 se nadomesti z naslednjim:

„Bajt	Dolžina	Vrednost	Opis
CLA	1	‚80h'	CLA
INS	1	‚2Ah'	Izvedba varnostne operacije
P1	1	‚90h'	Oznaka: Hash
P2	1	‚00h'	Implicitno znan algoritem Za tahografsko aplikacijo prve generacije: SHA-1 Za tahografsko aplikacijo druge generacije: algoritem SHA-2 (SHA-256, SHA-384 ali SHA-512), opredeljen z naborom algoritmov v Delu B Dodatka 11, za ključ podpisa kartice Card_Sign"

(r) točka 3.5.14 se spremeni:

besedilo pod naslovom in do odstavka TCS_126 se nadomesti z naslednjim:

„Ta ukaz se uporablja za izračun digitalnega podpisa prej izračunane zgoščene kode (glej PERFORM HASH of FILE, poglavje 3.5.13).

Le za vozniško kartico in kartico servisne delavnice se zahteva, da podpirata ta ukaz v DF Tachograph in DF Tachograph_G2.

Druge vrste tahografskih kartic lahko izvedejo ta ukaz, lahko pa tudi ne. Pri tahografskih aplikacijah druge generacije imajo ključ podpisa samo vozniške kartice in kartice servisne delavnice, druge kartice pa ukaza ne morejo uspešno izvesti in ga zaključijo z ustrezno kodo napake.

Ukaz je lahko dostopen v MF, lahko pa tudi ni. Če ukaz ni dostopen v MF, se zaključi z ustrezno kodo napake.

Ta ukaz je v skladu s standardom ISO/IEC 7816-8. Uporaba ukaza je glede na s tem povezani standard omejena.“;

(s) točka 3.5.15 se spremeni:

(i) tabela v odstavku TCS_133 se nadomesti z naslednjim:

„Bajt	Dolžina	Vrednost	Opis
CLA	1	‚00h‘	CLA
INS	1	‚2Ah‘	Izvedba varnostne operacije
P1	1	‚00h‘	
P2	1	‚A8h‘	Oznaka: podatkovno polje vsebuje DO, pomembne za preverjanje
Lc	1	‚XXh‘	Dolžina Lc naslednjega podatkovnega polja
#6	1	‚9Eh‘	Oznaka za digitalni podpis
#7 ali #7 – #8	L	‚NNh‘ ali ‚81 NNh‘	Dolžina digitalnega podpisa (L je 2 bajta, če je digitalni podpis daljši od 127 bajtov): 128 bajtov, kodiranih v skladu z Delom A iz Dodatka 11 za tahografsko aplikacijo prve generacije. Odvisno od izbrane krivulje za tahografsko aplikacijo druge generacije (glej Del B iz Dodatka 11).
#(7+L) – #(6+L+NN)	NN	‚XX..XXh‘	Vsebina digitalnega podpisa“

(ii) v odstavku TCS_134 se doda naslednja alinea:

„– Če ima izbrani javni ključ (uporabljen za preverjanje javnega ključa) CHA.LSB (CertificateHolderAuthorisation.equipmentType), ki ni ustrezen za preverjanje javnega ključa v skladu z Dodatkom 11, se vrne stanje obdelave **‚6985‘**.“;

(t) točka 3.5.16 se spremeni:

(i) v odstavku TCS_138 se v tabeli doda naslednja vrstica:

„5 + L + 1	1	‚00h'	Kakor določa ISO/IEC 7816-4"

(ii) v odstavku TCS_139 se doda naslednji pododstavek:

„— ‚**6985**' označuje, da je 4-bajtni časovni žig, naveden v polju s podatki ukaza, zgodnejši od časa cardValidityBegin ali poznejši od časa cardExpiryDate.";

(u) točka 4.2.2 se spremeni:

(i) v podatkovni strukturi v odstavku TCS_154 se vrstice od DF Tachograph_G2 do EF CardMA_Certificate in vrstice od EF GNSS_Places do konca navedenega odstavka nadomestijo z naslednjim:

"

Datoteka/podatkovni element	Št. zapisov	Velikost (v bajtih) Min.	Maks.	Privzete vrednosti
└DF Tachograph_G2		*20268*	*40316*	
├EF Application_Identification		*17*	*17*	
└DriverCardApplicationIdentification		*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 00}
├noOfGNSSADRecords		2	2	{00 00}
├noOfSpecificConditionRecords		2	2	{00 00}
└noOfCardVehicleUnitRecords		2	2	{00 00}
├EF CardMA_Certificate		*204*	*341*	

…

EF GNSS_Places		*4538*	*6050*	
└GNSSContinuousDriving		*4538*	*6050*	
├gnssADPointerNewestRecord		2	2	{00 00}
└gnssAccumulatedDrivingRecords		4536	6048	
└GNSSContinuousDrivingRecord	n_8	*18*	*18*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		14	14	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
├geoCoordinates		6	6	{00..00}
└vehicleOdometerValue		3	3	{00..00} ;

(ii) v odstavku TCS_155 se vnos NoOfGNSSCDRecords v tabeli nadomesti z naslednjim:

„n_8	NoOfGNSSADRecords	252	336“

(v) v točki 4.3.1 se besedilo za kratico SC4 v odstavku TCS_156 nadomesti z naslednjim:

„**SC4** Za ukaz READ BINARY s sodim bajtom INS:

(SM-C-MAC-G1 IN SM-R-ENC-MAC-G1) ALI

(SM-C-MAC-G2 IN SM-R-ENC-MAC-G2)

Za ukaz READ BINARY z lihim bajtom INS: NEV“;

(w) točka 4.3.2 se spremeni:

(i) v podatkovni strukturi v odstavku TCS_162 se vrstice od DF Tachograph_G2 do EF CardMA_Certificate, vrstice od EF Calibration do extendedSealIdentifier in vrstice od EF GNSS_Places do vehicleOdometerValue nadomestijo z naslednjim:

”

Datoteka/podatkovni element	Št. zapisov	Velikost (v bajtih) Min.	Velikost (v bajtih) Maks.	Privzete vrednosti
DF Tachograph_G2	*1878*		*49787*	
EF Application_Identification	*19*		*19*	
WorkshopCardApplicationIdentificatio	*19*		*19*	
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 00}
noOfCalibrationRecords	2		2	{00 00}
noOfGNSSADRecords	2		2	{00 00}
noOfSpecificConditionRecords	2		2	{00 00}
noOfCardVehicleUnitRecords	2		2	{00 00}
EF CardMA_Certificate	*204*		*341*	
...				
EF Calibration		*15668*	*45394*	
WorkshopCardCalibrationData		*15668*	*45394*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*15664*	*45390*	
WorkshopCardCalibrationRecord	n_5	*178*	*178*	
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		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}

...

EF GNSS_Places		*326*	*434*	
└GNSSContinuousDriving		*326*	*434*	
├gnssADPointerNewestRecord		2	2	{00 00}
└gnssAccumulatedDrivingRecords		324	432	
└GNSSContinuousDrivingRecord	n_8	*18*	*18*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		14	14	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
├geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

“

(ii) vnos NoOfGNSSCDRecords v tabeli v odstavku TCS_163 se nadomesti z naslednjim:

„n_8	NoOfGNSSADRecords	18	24“

(31) v Dodatku 3 se točka 2 spremeni:

(a) po vrstici s piktogramoma „Lokacija začetka dnevne delovne izmene“ in „Lokacija konca dnevne delovne izmene“ se vstavi naslednja vrstica:

„ Položaj po 3 urah skupnega časa vožnje“;

(b) kombinacija piktogramov „Nastavljanje časa (s strani servisne delavnice)“ se nadomesti z naslednjim:

„ Časovno navzkrižje ali nastavljanje časa (s strani servisne delavnice)“;

(c) v seznam dogodkov se dodata naslednji kombinaciji piktogramov:

„ Ni informacij o položaju s strani GNSS sprejemnika ali napaka pri komuniciranju z zunanjo GNSS opremo

Napaka pri komuniciranju z opremo za komunikacijo na daljavo“;

(32) Dodatek 4 se spremeni:

(a) točka 2 se spremeni:

(i) blok številka 11.4 se nadomesti z naslednjim:

„11.4 *Vnos kraja, v katerem se dnevna delovna izmena začne in/ali konča*

pi = piktogram kraja začetka/konca, čas, država, regija	pihh:mm Cou Reg
zemljepisna dolžina zapisanega položaja	lon ±DDD°MM.M’
zemljepisna širina zapisanega položaja	lat ± DD°MM.M’
časovni žig ob določitvi položaja	hh:mm
Števec prevožene poti	x xxx xxx **km**“

(ii) blok številka 11.5 se nadomesti z naslednjim:

„11.5 *Položaji po 3 urah skupnega časa vožnje*
pi = položaj po 3 urah skupnega časa
vožnje
zemljepisna dolžina zapisanega položaja
zemljepisna širina zapisanega položaja
časovni žig ob določitvi položaja
Števec prevožene poti

```
pihh:mm
lon  ± DDD°MM.M'
lat ± DD°MM.M '
hh:mm
x xxx xxx km“
```

(b) v točki 3.1. se točka 11.5 v vzorcu dnevnega izpisa nadomesti z naslednjim:

„11.5	Položaji po 3 urah skupnega časa vožnje v časovnem zaporedju“

(c) v točki 3.2. se vzorec dnevnega izpisa nadomesti z naslednjim:

„1	Datum in čas izpisanega dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice, vstavljene v VU + GEN)
4	Identifikacija vozila (vozilo, iz katerega se opravi izpis)
5	Identifikacija VU (VU, iz katere se opravi izpis + GEN)
6	Zadnja kalibracija te VU
7	Zadnji nadzor na tem tahografu
9	Ločilo voznikovih dejavnosti
10	Ločilo voznikove reže (reža 1)
10a	Stanje zunaj področja uporabe na začetku tega dneva
10.1 / 10.2/ 10.3/ 10.3a/ 10.4	Dejavnosti v časovnem zaporedju (voznikova reža)
10	Ločilo sovoznikove reže (reža 2)
10a	Stanje zunaj področja uporabe na začetku tega dneva
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Dejavnosti v časovnem zaporedju (sovoznikova reža)
11	Ločilo dnevnega povzetka
11.1	Povzetek obdobij brez kartice v voznikovi reži
11.4	Vneseni kraji v časovnem zaporedju
11.5	Položaji po 3 urah skupnega časa vožnje v časovnem zaporedju
11.7	Skupne vrednosti dejavnosti
11.2	Povzetek obdobij brez kartice v sovoznikovi reži
11.4	Vneseni kraji v časovnem zaporedju
11.5	Položaji po 3 urah skupnega časa vožnje v časovnem zaporedju

11.8	Skupne vrednosti dejavnosti
11.3	Povzetek dejavnosti za voznika, vključno z obema režama
11.4	Vnosi krajev tega voznika v časovnem zaporedju
11.5	Položaji po 3 urah skupnega časa vožnje v časovnem zaporedju
11.9	Skupne vrednosti po dejavnostih za tega voznika
13.1	Ločilo dogodkov in napak
13.4	Zapisi dogodkov/napak (zadnjih 5 dogodkov ali napak, ki so v VU shranjene ali so v teku)
22.1	Kraj nadzora
22.2	Podpis nadzornika
22.3	Od časa (prostor, na katerem lahko voznik brez kartice označi,
22.4	Do časa katera obdobja se nanašajo nanj)
22.5	Podpis voznika“

(d) v točki 3.7 se odstavek PRT_014 nadomesti z naslednjim:

„PRT_014 Izpis zgodovine vstavljenih kartic je v skladu z naslednjim formatom:

1	Datum in čas izpisanega dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice, vstavljene v VU)
23	Najnovejše kartice, vstavljene v VU
23.1	Vstavljene kartice (do 88 zapisov)
12.3	Ločilo napak“

(33) Dodatek 7 se spremeni:

(a) točka 1.1. se nadomesti z naslednjim:

„1.1 **Področje uporabe**

Podatki se v zunanji pomnilniški medij (ESM) lahko prenesejo:

— iz enote v vozilu z inteligentno namensko opremo (IDE), priključeno na VU,

— s tahografske kartice z IDE, opremljeno z vmesniško napravo (IFD),

— s kartice preko enote v vozilu z IDE, priključeno na VU.

Da bi se lahko preverilo avtentičnost in celovitost prenesenih podatkov, shranjenih na ESM, se podatki prenesejo s pripetim podpisom v skladu z Dodatkom 11 Skupni varnostni mehanizmi. Prenesejo se tudi identifikacija in varnostni certifikati (države članice in opreme) izvorne opreme (VU ali kartice). Oseba, ki preveri podatke, mora imeti lasten varnostni evropski javni ključ, ki ga je pridobila neodvisno.

Podatki, preneseni iz VU, se podpišejo z uporabo skupnih varnostnih mehanizmov iz Dela B Dodatka 11 (Sistem tahografov druge generacije), razen kadar nadzor nad vozniki opravi nadzorni organ zunaj EU z nadzorno kartico prve generacije; v tem primeru se podatki podpišejo z uporabo skupnih varnostnih mehanizmov iz Dela A Dodatka 11 (Sistem tahografov prve generacije) v skladu z zahtevo MIG_015 iz Dodatka 15 (Migracija).

Ta dodatek zato določa dve vrsti prenosa podatkov iz VU:

— prenos podatkov iz VU druge generacije, ki ima strukturo podatkov druge generacije in se podpiše z uporabo skupnih varnostnih mehanizmov iz Dela B Dodatka 11,

— prenos podatkov iz VU prve generacije, ki ima strukturo podatkov prve generacije in se podpiše z uporabo skupnih varnostnih mehanizmov iz Dela A Dodatka 11.

Podobno sta v odstavkih 3 in 4 tega dodatka določeni tudi dve vrsti prenosa podatkov iz vozniških kartic druge generacije, vstavljenih v VU.“;

(b) točka 2.2.2 se spremeni:

(i) tabela se nadomesti z naslednjim:

„Struktura sporočil	Največ 4 bajti Glava				Največ 255 bajtov Podatki			1 bajt Kontrolna vsota
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (stage 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00,00-,00,FF,FF, FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Overview	80	EE	F0	02	36	01 or 21		97
Activities	80	EE	F0	06	36	02 or 22	Datum	CS
Events & Faults	80	EE	F0	02	36	03 ali 23		99
Detailed Speed	80	EE	F0	02	36	04 ali 24		9A
Technical Data	80	EE	F0	02	36	05 ali 25		9B
Card download	80	EE	F0	02	36	06	Reža	CS

Struktura sporočil	Največ 4 bajti Glava				Največ 255 bajtov Podatki			1 bajt Kontrolna vsota
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Podatki	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Podatki	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS“

(ii) v opombe pod tabelo se dodata naslednji alinei:

„— TRTP 21 do 25 se uporabljajo za zahtevke za prenos podatkov iz VU druge generacije, TRTP 01 do 05 se uporabljajo za zahtevke za prenos podatkov iz VU prve generacije, ki jih VU lahko sprejme samo v okviru nadzora nad vozniki, ki ga opravi nadzorni organ zunaj EU z nadzorno kartico prve generacije.

— TRTP 11 do 19 in 31 do 39 so rezervirane za prenose podatkov, kot jih določi proizvajalec.“;

(c) točka 2.2.2.9 se spremeni:

(i) odstavek DDP_011 se nadomesti z naslednjim:

„DDP_011 Sporočilo Transfer Data Request pošlje IDE, da bi VU sporočil, katera vrsta podatkov se prenese. Enobajtni parameter TRTP navaja vrsto prenosa.

Obstaja šest vrst prenosa podatkov. Za prenos podatkov iz VU se za vsako vrsto prenosa lahko uporabita dve različni vrednosti TRTP:

Vrsta prenosa podatkov	Vrednost TRTP za prenos podatkov iz VU prve generacije	Vrednost TRTP za prenos podatkov iz VU druge generacije
Pregled (*Overview*)	01	21
Dejavnosti na določen dan (*Activities of a specified date*)	02	22
Dogodki in napake (*Events and faults*)	03	23
Podrobni podatki o hitrosti (*Detailed speed*)	04	24
Tehnični podatki (*Technical data*)	05	25

Vrsta prenosa podatkov	Vrednost TRTP
Prenos podatkov s kartice	06“

(ii) odstavek DDP_054 se nadomesti z naslednjim:

„DDP_054 IDE med sejo prenosa podatkov obvezno zahteva prenos podatkov iz pregleda (TRTP 01 ali 21), saj le to zagotavlja zapis certifikatov VU v preneseno datoteko (in preverjanje digitalnega podpisa).

V drugem primeru (TRTP 02 ali 22) sporočilo *Transfer Data Request* vsebuje navedbo koledarskega dneva (v formatu `TimeReal` format), za katerega se prenesejo podatki.“;

(d) v točki 2.2.2.10 se odstavek DDP_055 nadomesti z naslednjim:

„DDP_055 V prvem primeru (TREP 01 ali 21) VU pošlje v IDE podatke, ki pomagajo operaterju izbrati podatke, ki jih želi prenesti v nadaljevanju. To sporočilo vsebuje naslednje podatke:

— varnostni certifikati,

— identifikacija vozila,

— trenutni datum in čas VU,

— najpoznejši in najzgodnejši datum, za katerega je mogoče prenesti podatke (podatki VU),

— znak prisotnosti kartic v VU,

— predhodni prenosi podatkov za potrebe podjetja,

— blokade s strani podjetja,

— predhodni nadzori.“;

(e) v točki 2.2.2.16 se zadnja alinea odstavka DDP_018 nadomesti z naslednjim:

„— FA Data not available (podatki niso na voljo)

Podatkovni objekt iz zahtevka za prenos podatkov ni na voljo v VU (npr. kartica ni vstavljena, prenos podatkov iz VU prve generacije se je zahteval zunaj okvira nadzora nad vozniki, ki ga opravi nadzorni organ zunaj EU, itd.).“;

(f) točka 2.2.6.1 se spremeni:

(i) prvi pododstavek odstavka DDP_029 se nadomesti z naslednjim:

„Podatkovno polje *Positive Response Transfer Data Overview* vsebuje naslednje podatke v naslednjem zaporedju; pri čemer je SID 76 hex, TREP 01 ali 21 hex; sporočilo je ustrezno razdeljeno na delna sporočila, ki so označena z zaporednimi številkami:“;

(ii) naslov „Struktura podatkov prve generacije“ se nadomesti z naslednjim:

„Struktura podatkov prve generacije (TREP 01 hex)“;

(iii) naslov „Struktura podatkov druge generacije“ se nadomesti z naslednjim:

„Struktura podatkov druge generacije (TREP 21 hex)“;

(g) točka 2.2.6.2 se spremeni:

(i) prvi pododstavek odstavka DDP_030 se nadomesti z naslednjim:

„Podatkovno polje *Positive Response Transfer Data Activities* vsebuje naslednje podatke v naslednjem zaporedju; pri čemer je SID 76 hex, TREP 02 ali 22 hex; sporočilo je ustrezno razdeljeno na delna sporočila, ki so označena z zaporednimi številkami:“;

(ii) naslov „Struktura podatkov prve generacije“ se nadomesti z naslednjim:

„Struktura podatkov prve generacije (TREP 02 hex)“;

(iii) naslov „Struktura podatkov druge generacije“ se nadomesti z naslednjim:

„Struktura podatkov druge generacije (TREP 22 hex)“;

(iv) vnos VuGNSSCDRecordArray pod naslovom „Struktura podatkov druge generacije (TREP 22 hex)“ se nadomesti z naslednjim:

„VuGNSSADRecordArray	Položaji GNSS vozila, kjer skupni čas vožnje doseže večkratnik treh ur. Če je razdelek prazen, se pošlje le glava tabele z noOfRecords = 0.“

(h) točka 2.2.6.3 se spremeni:

(i) prvi pododstavek odstavka DDP_031 se nadomesti z naslednjim:

„Podatkovno polje sporočila *Positive Response Transfer Data Events and Faults* vsebuje naslednje podatke v naslednjem zaporedju; pri čemer je SID 76 hex, TREP 03 ali 23 hex; sporočilo je ustrezno razdeljeno na delna sporočila, ki so označena z zaporednimi številkami:“;

(ii) naslov „Struktura podatkov prve generacije“ se nadomesti z naslednjim:

„Struktura podatkov prve generacije (TREP 03 hex)“;

(iii) naslov „Struktura podatkov druge generacije“ se nadomesti z naslednjim:

„Struktura podatkov druge generacije (TREP 23 hex)“;

(iv) vnos VuTimeAdjustmentGNSSRecordArray pod naslovom „Struktura podatkov druge generacije (TREP 23 hex)“ se črta:

(i) točka 2.2.6.4 se spremeni:

(i) prvi pododstavek odstavka DDP_032 se nadomesti z naslednjim:

„Podatkovno polje *Positive Response Transfer Data Detailed Speed* vsebuje naslednje podatke v naslednjem zaporedju; pri čemer je SID 76 hex, TREP 04 ali 24 hex; sporočilo je ustrezno razdeljeno na delna sporočila, ki so označena z zaporednimi številkami:“;

(ii) naslov „Struktura podatkov prve generacije“ se nadomesti z naslednjim:

„Struktura podatkov prve generacije (TREP 04)“;

(iii) naslov „Struktura podatkov druge generacije“ se nadomesti z naslednjim:

„Struktura podatkov druge generacije (TREP 24)“;

(j) točka 2.2.6.5 se spremeni:

(i) prvi pododstavek odstavka DDP_033 se nadomesti z naslednjim:

„Podatkovno polje *Positive Response Transfer Data Technical Data* vsebuje naslednje podatke v naslednjem zaporedju; pri čemer je SID 76 hex, TREP 05 ali 25 hex; sporočilo je ustrezno razdeljeno na delna sporočila, ki so označena z zaporednimi številkami:“;

(ii) naslov „Struktura podatkov prve generacije“ se nadomesti z naslednjim:

„Struktura podatkov prve generacije (TREP 05)“;

(iii) naslov „Struktura podatkov druge generacije“ se nadomesti z naslednjim:

„Struktura podatkov druge generacije (TREP 25)“;

(k) v točki 3.3 se odstavek DDP_035 nadomesti z naslednjim:

„DDP_035 Prenos podatkov s tahografske kartice zajema naslednje korake:

— prenos skupnih podatkov kartice iz elementarnih datotek `ICC` in `IC` Ti podatki niso obvezni in niso zavarovani z digitalnim podpisom.

— (za tahografske kartice prve in druge generacije) Prenos elementarnih datotek v okviru `Tachograph DF`:

— Prenos elementarnih datotek `Card_Certificate` in `CA_Certificate`. Ti podatki niso zavarovani z digitalnim podpisom.

Te datoteke se obvezno prenesejo v vsaki seji prenosa podatkov.

— Prenos drugih elementarnih datotek z aplikativnimi podatki(v okviru `Tachograph DF`), razen `Card_Download`. Ti podatki so zavarovani z digitalnim podpisom, in sicer z uporabo skupnih varnostnih mehanizmov iz Dela A Dodatka 11.

— V vsaki seji prenosa podatkov se obvezno preneseta vsaj elementarni datoteki `Application_Identification` in `Identification`.

— Pri prenosu podatkov z vozniške kartice je obvezen tudi prenos naslednjih elementarnih datotek:

— `Events_Data`,

— `Faults_Data`,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific_Conditions,

— (samo za tahografske kartice druge generacije) Razen če se prenos podatkov z vozniške kartice, vstavljene v VU, izvede med nadzorom nad vozniki, ki ga opravi nadzorni organ zunaj EU z nadzorno kartico prve generacije, prenos elementarnih datotek v okviru Tachograph_G2 DF:

— Prenos elementarnih datotek CardSignCertificate, CA_Certificate in Link_Certificate (če obstajajo). Ti podatki niso zavarovani z digitalnim podpisom.

Te datoteke se obvezno prenesejo v vsaki seji prenosa podatkov.

— Prenos drugih aplikativnih elementarnih datotek (v okviru Tachograph_G2 DF), razen Card_Download Ti podatki so zavarovani z digitalnim podpisom, in sicer z uporabo skupnih varnostnih mehanizmov iz Dela B Dodatka 11.

— V vsaki seji prenosa podatkov se obvezno preneseta vsaj elementarni datoteki Application_Identification in Identification.

— Pri prenosu podatkov z vozniške kartice je obvezen tudi prenos naslednjih elementarnih datotek:

— Events_Data,

— Faults_Data,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific_Conditions,

— VehicleUnits_Used,

— GNSS Places.

— Pri prenosu podatkov z vozniške kartice se posodobi datum LastCardDownload v elementarni datoteki Card_Download v namenskih datotekah Tachograph in, če je ustrezno, Tachograph_G2

— Pri prenosu podatkov s kartice servisne delavnice se ponastavi števec kalibracij v elementarni datoteki Card_Download v namenskih datotekah Tachograph in, če je ustrezno, Tachograph_G2 .

— Pri prenosu podatkov s kartice servisne delavnice se ne prenese `Sensor_Installation_Data` v namenskih datotekah `Tachograph` in, če je ustrezno, `Tachograph_G2`.“;

(l) v točki 3.3.2 se prvi pododstavek odstavka DDP_037 nadomesti z naslednjim:

„Zaporedje za prenos EF ICC, IC, Card_Certificate (ali CardSignCertificate za DF Tachograph_G2), CA_Certificate in Link_Certificate (samo za DF Tachograph_G2) je naslednje:“;

(m) v točki 3.3.3 se tabela nadomesti z naslednjim:

„Kartica	Dir	IDE/IFD	Pomen/opombe
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	— Izračun zgoščene vrednosti vsebine podatkov z uporabo predpisanega zgoščevalnega algoritma v skladu z Delom A ali B Dodatka 11. Ta ukaz ni ISO ukaz.
Izračun Hash of File in začasna shranitev zgoščene vrednosti			
OK	⇨		
	⇦	**Read Binary**	Če datoteka vsebuje več podatkov, kot je zmogljivost vmesnega pomnilnika čitalnika ali kartice, je treba ukaz ponavljati, dokler se ne prebere celotna datoteka.
Podatki datoteke OK	⇨	Shranitev sprejetih podatkov na ESM	v skladu s **3.4** Data storage format
	⇦	**PSO: Compute Digital Signature**	
Izvedba varnostne operacije *Compute Digital Signature* z začasno shranjeno zgoščeno vrednostjo			
Podpis OK	⇨	Dopis podatkov k predhodno shranjenim podatkom na ESM	v skladu s **3.4** Data storage format“

(n) v točki 3.4.2 se odstavek DDP_046 nadomesti z naslednjim:

„DDP_046 Podpis se shrani kot naslednji objekt TLV neposredno za objektom TLV, ki vsebuje podatke datoteke.

Opredelitev	Pomen	Dolžina
FID (2 bajta) || ‚00‘	Oznaka za EF (FID) v DF Tachograph ali za skupne podatke kartice	3 bajti
FID (2 bajta) || ‚01‘	Oznaka za podpis EF (FID) v DF Tachograph	3 bajti
FID (2 bajta) || ‚02‘	Oznaka za EF (FID) v DF Tachograph_G2	3 bajti
FID (2 bajta) || ‚03‘	Oznaka za podpis EF (FID) v DF Tachograph_G2	3 bajti
xx xx	Dolžina polja vrednosti	2 bajta

Primer podatkov v preneseni datoteki na ESM:

Oznaka	Dolžina	Vrednost
00 02 00	00 11	— Podatki v EF ICC
C1 00 00	00 C2	— Podatki v EF Card_Certificate
		— ...
05 05 00	0A 2E	Podatki v EF Vehicles_Used (v DF Tachograph)
05 05 01	00 80	Podpis EF Vehicles_Used (v DF Tachograph)
05 05 02	0A 2E	Podatki v EF Vehicles_Used (v DF Tachograph_G2)
05 05 03	xx xx	Podpis EF Vehicles_Used (v DF Tachograph_G2)“

(o) v točki 4. se odstavek DDP_049 nadomesti z naslednjim:

„DDP_049 Za vozniške kartice prve generacije: podatki se prenesejo z uporabo protokola za prenos podatkov prve generacije, preneseni podatki pa so v enakem formatu kot podatki, ki se prenesejo iz enote v vozilu prve generacije.

Za vozniške kartice druge generacije: VU nato po datotekah prenese celotno kartico v skladu s protokolom prenosa podatkov, opredeljenim v odstavku 3, in prepošlje IDE vse podatke, ki jih prejme s kartice, v ustreznem formatu datotek TLV in enkapsulirane v sporočilu *Positive Response Transfer Data* (glej 3.4.2).“;

(34) v točki 2. Dodatka 8 se odstavek pod podnaslovom „Vir“ nadomesti z naslednjim:

„ISO 14230-2: Road Vehicles – Diagnostic Systems – Keyword Protocol 2000 – Part 2: Data Link Layer.

Prva izdaja: 1999.“;

(35) Dodatek 9 se spremeni:

(a) v kazalu se točka 6 nadomesti z naslednjim:

„6. PRESKUSI ZUNANJE OPREME ZA KOMUNIKACIJO NA DALJAVO“;

(b) v točki 1.1. se prvi pomišljaj nadomesti z naslednjim:

„— **certificiranju zaščite** na podlagi specifikacij skupnih meril, da se ugotovi, ali so cilji zaščite v celoti izpolnjeni v skladu z Dodatkom 10 k tej prilogi,“;

(c) v točki 2. se tabela v zvezi s preskusi funkcionalnosti enote v vozilu nadomesti z naslednjim:

„Št.	Preskus	Opis	Povezane zahteve
1.	**Administrativni pregled**		
1.1	Dokumentacija	Pravilnost dokumentacije	
1.2	Rezultati preskusa proizvajalca	Rezultati preskusa proizvajalca, opravljenega med vgradnjo Papirna dokazila	88, 89, 91
2.	**Vizualni pregled**		
2.1	Skladnost z dokumentacijo		
2.2	Identifikacija/oznake		224 do 226
2.3	Materiali		219 do 223
2.4	Zapečatenje		398, 401 do 405
2.5	Zunanji vmesniki		
3.	**Preskusi funkcionalnosti**		
3.1	Možne funkcije		02, 03, 04, 05, 07, 382
3.2	Načini delovanja		09 do 11*, 134, 135
3.3	Pravice dostopa do funkcij in podatkov		12*, 13*, 382, 383, 386 do 389
3.4	Spremljanje vstavljanja in izvlečenja kartic		15, 16, 17, 18, 19*, 20*, 134
3.5	Merjenje hitrosti in razdalje		21 do 31
3.6	Merjenje časa (preskus se opravlja pri 20 °C)		38 do 43
3.7	Spremljanje voznikovih dejavnosti		44 do 53, 134
3.8	Spremljanje statusa vožnje		54, 55, 134
3.9	Ročni vnosi		56 do 62
3.10	Upravljanje blokad s strani podjetja		63 do 68
3.11	Spremljanje nadzornih dejavnosti		69, 70
3.12	Zaznavanje dogodkov in/ali napak		71 do 88, 134

Št.	Preskus	Opis	Povezane zahteve
3.13	Identifikacijski podatki naprave		93*, 94*, 97, 100
3.14	Podatki o vstavljanju in izvlečenju vozniške kartice		102* do 104*
3.15	Podatki o voznikovih dejavnostih		105* do 107*
3.16	Podatki o krajih in položajih		108* do 112*
3.17	Podatki števca prevožene poti		113* do 115*
3.18	Podrobni podatki o hitrosti		116*
3.19	Podatki o dogodkih		117*
3.20	Podatki o napakah		118*
3.21	Kalibracijski podatki		119* do 121*
3.22	Podatki o prilagajanju časa		124*, 125*
3.23	Podatki o nadzornih dejavnostih		126*, 127*
3.24	Podatki o blokadah s strani podjetja		128*
3.25	Podatki o prenosih podatkov		129*
3.26	Podatki o posebnih stanjih		130*, 131*
3.27	Zapisovanje in shranjevanje podatkov na tahografske kartice		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Prikazovanje		90, 134 151 do 168 PIC_001, DIS_001
3.29	Tiskanje		90, 134, 169 do 181, PIC_001, PRT_001 do PRT_014
3.30	Opozarjanje		134, 182 do 191 PIC_001
3.31	Prenos podatkov na zunanje medije		90, 134, 192 do 196
3.32	Komunikacija na daljavo za namen ciljnih cestnih preverjanj		197 do 199
3.33	Iznos podatkov na dodatne zunanje naprave		200, 201
3.34	Kalibracija		202 do 206*, 383, 384, 386 do 391
3.35	Cestno preverjanje kalibracije		207 do 209
3.36	Nastavljanje časa		210 do 212*
3.37	Brez interference s strani dodatnih funkcij		06, 425

Št.	Preskus	Opis	Povezane zahteve
3.38	Vmesnik tipala gibanja		02, 122
3.39	Zunanja GNSS oprema		03, 123
3.40	Preverjanje, ali VU odkrije, zapiše in shrani dogodke in/ali napake, ki jih opredeli proizvajalec VU, ko se povezano tipalo gibanja odzove na magnetna polja, ki motijo odkrivanje gibanja vozila.		217
3.41	Nabor algoritmov in standardizirani parametri domen		CSM_48, CSM_50
4.	**Okoljski preskusi**		
4.1	Temperatura	Preverjanje funkcionalnosti z naslednjimi preskusi: preskus v skladu z ISO 16750-4, poglavje 5.1.1.2: Low temperature operation test (72 h pri – – 20 °C) Ta preskus se nanaša na IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold Preskus v skladu z ISO 16750-4: poglavje 5.1.2.2: High temperature operation test (72 h pri 70 °C) Ta preskus se nanaša na IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Preskus v skladu z ISO 16750-4, poglavje 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 ciklov, čas mirovanja 2 h pri vsaki temperaturi) Skrčen nabor preskusov (izbranih med preskusi, predpisanimi v oddelku 3 te preglednice) se lahko opravi pri nižji temperaturi, pri višji temperaturi ali med temperaturnimi cikli	213
4.2	Vlažnost	Preverjanje, ali lahko enota v vozilu prenese cikle vlage (preskus s ciklično vlažno vročino) s preskusom Db po IEC 60068-2-30, šest 24-urnih ciklov, pri vsakem spreminjanje temperature od + 25 °C do + 55 °C, relativna vlažnost 97 % pri + 25 °C in 93 % pri + 55 °C	214
4.3	Mehanski	1. Sinusoidne vibracije preverjanje, ali lahko enota v vozilu prenese sinusoidne vibracije naslednjih lastnosti: konstantni premiki med 5 in 11 Hz: konica 10 mm konstantni pospeški med 11 in 300 Hz: 5g To zahtevo se preverja s preskusom Fc po IEC 60068-2-6, z najmanjšim trajanjem preskusa 3 × 12 ur (12 ur na vsako os) ISO 16750-3 za naprave, nameščene v ločeno kabino vozila, ne zahteva preskusa s sinusoidnimi vibracijami.	219

Št.	Preskus	Opis	Povezane zahteve
		2. Naključne vibracije: Preskus v skladu z ISO 16750-3, poglavje 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab Preskus z naključnimi vibracijami, 10–2 000 Hz, RMS navpično 21,3 m/s^2, RMS vodoravno 11,8 m/s^2, RMS bočno 13,1 m/s^2, 3 osi, 32 h na os, vključno s temperaturnim ciklom – 20–70 °C. Ta preskus se nanaša na IEC 60068-2-64: Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance 3. Udarci: mehanski udarec s 3 g, pol sinusni v skladu z ISO 16750. Zgoraj opisani preskusi se opravijo na različnih vzorcih preskušane opreme.	
4.4	Zaščita pred vodo in tujki	Preskus v skladu z ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (brez sprememb parametrov); najnižja vrednost IP 40	220, 221
4.5	Prenapetostna zaščita	Preverjanje, ali enota v vozilu prenese naslednje napajanje: izvedbe 24 V: 34 V pri + 40 °C 1 uro izvedbe 12 V: 17 V pri + 40 °C 1 uro(ISO 16750-2)	216
4.6	Zaščita pred zamenjavo polarnosti	Preverjanje, ali enota v vozilu prenese zamenjavo polaritete svoje napajalne napetosti (ISO 16750-2)	216
4.7	Kratkostična zaščita	Preverjanje, ali so izhodni signali zaščiteni pred kratkimi stiki z napajalno napetostjo in ozemljitvijo (ISO 16750-2)	216
5.	**Preskusi elektromagnetne združljivosti (EMC)**		
5.1	Lastna sevanja in dovzetnost	Skladnost s Pravilnikom ECE R10	218
5.2	Elektrostatična razelektritev	Skladnost z ISO 10605:2008 + Technical Corrigendum: 2010 + AMD1:2014: +/– 4 kV za kontakt in +/– 8 kV za odvod zraka	218

Št.	Preskus	Opis	Povezane zahteve
5.3	Prehodna dovzetnost za prevodne motnje	Pri izvedbah 24 V: skladnost z ISO 7637-2 + Pravilnikom ECE št. 10 Rev. 3: impulz 1a: Vs = – 450 V Ri = 50 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 20 V Ri = 0,05 ohma impulz 3a: Vs = – 150 V Ri = 50 ohmov impulz 3b: Vs = + 150 V Ri = 50 ohmov impulz 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulz 5: Vs = + 120 V Ri = 2,2 ohma td = 250 ms Pri izvedbah 12 V: skladnost z ISO 7637-1 + Pravilnikom ECE št. 10 Rev. 3: impulz 1: Vs = – 75 V Ri = 10 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 10 V Ri = 0,05 ohma impulz 3a: Vs = – 112 V Ri = 50 ohmov impulz 3b: Vs = + 75 V Ri = 50 ohmov impulz 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impulz 5: Vs = + 65 V Ri = 3 ohme td = 100 ms impulz 5 se preskuša le za enote v vozilu, namenjene za vgradnjo v vozila brez vgrajene zunanje skupne zaščite pred razbremenitvami Za predlog razbremenitve glej ISO 16750-2, 4. izdaja, poglavje 4.6.4.	218“

(d) točka 6. se nadomesti z naslednjim:

„6. PRESKUSI ZUNANJE OPREME ZA KOMUNIKACIJO NA DALJAVO

Št.	Preskus	Opis	Povezane zahteve
1.	**Administrativni pregled**		
1.1	Dokumentacija	Pravilnost dokumentacije	
2.	**Vizualni pregled**		
2.1	Skladnost z dokumentacijo		
2.2	Identifikacija/oznake		225, 226
2.3	Materiali		219 do 223
3.	**Preskusi funkcionalnosti**		
3.1	Komunikacija na daljavo za namen ciljnih cestnih preverjanj		4, 197 do 199

Št.	Preskus	Opis	Povezane zahteve
3.2	Zapisovanje in shranjevanje v pomnilniku podatkov		91
3.3	Komunikacija z enoto na vozilu		Dodatek 14 DSC_66 do DSC_70, DSC_71 do DSC_76
4.	**Okoljski preskusi**		
4.1	Temperatura	Preverjanje funkcionalnosti z naslednjimi preskusi: preskus v skladu z ISO 16750-4, poglavje 5.1.1.2: Low temperature operation test (72 h pri – 20 °C) Ta preskus se nanaša na IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold Preskus v skladu z ISO 16750-4: poglavje 5.1.2.2: High temperature operation test (72 h pri 70 °C) Ta preskus se nanaša na IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Preskus v skladu z ISO 16750-4, poglavje 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 ciklov, čas mirovanja 1 h pri vsaki temperaturi) Skrčen nabor preskusov (izbranih med preskusi, predpisanimi v oddelku 3 te preglednice) se lahko opravi pri nižji temperaturi, pri višji temperaturi ali med temperaturnimi cikli	213
4.2	Zaščita pred vodo in tujki	Preskus v skladu z ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (ciljna vrednost IP40)	220, 221
5.	**Preskusi elektromagnetne združljivosti (EMC)**		
5.1	Lastna sevanja in dovzetnost	Skladnost s Pravilnikom ECE R10	218
5.2	Elektrostatična razelektritev	Skladnost z ISO 10605:2008 + Technical Corrigendum: 2010 + AMD1:2014: +/– 4 kV za kontakt in +/– 8 kV za odvod zraka	218

Št.	Preskus	Opis	Povezane zahteve
5.3	Prehodna dovzetnost za prevodne motnje	Pri izvedbah 24 V: skladnost z ISO 7637-2 + Pravilnikom ECE št. 10 Rev. 3: impulz 1a: Vs = – 450 V Ri = 50 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 20 V Ri = 0,05 ohma impulz 3a: Vs = – 150 V Ri = 50 ohmov impulz 3b: Vs = + 150 V Ri = 50 ohmov impulz 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulz 5: Vs = + 120 V Ri = 2,2 ohma td = 250 ms Pri izvedbah 12 V: skladnost z ISO 7637-1 + Pravilnikom ECE št. 10 Rev. 3: impulz 1: Vs = – 75 V Ri = 10 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 10 V Ri = 0,05 ohma impulz 3a: Vs = – 112 V Ri = 50 ohmov impulz 3b: Vs = + 75 V Ri = 50 ohmov impulz 4: Vs = –6 V Va = – 5 V t6 = 15 ms impulz 5: Vs = +65 V Ri = 3 ohme td = 100 ms impulz 5 se preskuša le za enote v vozilu, namenjene za vgradnjo v vozila brez vgrajene zunanje skupne zaščite pred razbremenitvami Za predlog razbremenitve glej ISO 16750-2, 4. izdaja, poglavje 4.6.4.	218“

(e) tabela v točki 8. v zvezi s preskusi interoperabilnosti se nadomesti z naslednjim:

„Št.	Preskus	Opis
	8.1 Preskusi interoperabilnosti med enotami v vozilu in tahografskimi karticami	
1.	Medsebojna avtentikacija	Preverjanje normalnega poteka medsebojne avtentikacije enote v vozilu in tahografske kartice
2.	Preskusi pisanja/branja	Izvedba značilnega scenarija uporabe enote v vozilu. Scenarij mora biti prilagojen vrsti preskušane kartice in mora obsegati vpise v kar največ elementarnih datotek na kartici. Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov z enote v vozilu Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov s kartice Preverjanje, ali je mogoče vse zapise pravilno prebrati, z dnevnimi izpisi

Št.	Preskus	Opis
		8.2 Preskusi interoperabilnosti med enotami v vozilu in tipali gibanja
1.	Povezovanje	Preverjanje normalnega poteka povezave med enotami v vozilu in tipali gibanja
2.	Preskusi delovanja	Izvedba značilnega scenarija uporabe tipala gibanja. Scenarij vključuje običajno delovanje in ustvarjanje čim več dogodkov in napak. Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov z enote v vozilu Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov s kartice Preverjanje, ali je mogoče vse zapise pravilno prebrati, z dnevnim izpisom
		8.3 Preskusi interoperabilnosti med enotami v vozilu in zunanjo GNSS opremo (če je primerno)
1.	Medsebojna avtentikacija	Preverjanje normalnega poteka medsebojne avtentikacije (povezave) med enoto v vozilu in zunanjim GNSS modulom
2.	Preskusi delovanja	Izvedba značilnega scenarija delovanja zunanje GNSS opreme. Scenarij vključuje običajno delovanje in ustvarjanje čim več dogodkov in napak. Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov z enote v vozilu Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov s kartice Preverjanje, ali je mogoče vse zapise pravilno prebrati, z dnevnim izpisom“

(36) Dodatek 11 se spremeni:

(a) v točki 8.2.3 se odstavek CSM_49 nadomesti z naslednjim:

„CSM_49 Enote v vozilu, tahografske kartice in zunanja GNSS oprema morajo podpirati algoritme SHA-256, SHA-384 in SHA-512, določene v [SHS].“;

(b) v točki 9.1.2 se prvi pododstavek odstavka CSM_58 nadomesti z naslednjim:

„CSM_58 Kadar koli ERCA ustvari nov evropski korenski par ključev, mora pripraviti vezni certifikat za nov evropski javni ključ in ga podpisati s predhodnim evropskim zasebnim ključem. Veljavnost veznega certifikata je 17 let in 3 mesece. To je prikazano tudi na sliki 1 v oddelku 9.1.7.“;

(c) v točki 9.1.4 se odstavek CSM_72 nadomesti z naslednjim:

„CSM_72 Za vsako enoto v vozilu se ustvarita dva edinstvena para ključev ECC, označena kot VU_MA in VU_Sign. To nalogo prevzamejo proizvajalci enote v vozilu. Kadar koli se ustvari par ključev VU, mora stran, ki ga ustvari, javni ključ poslati svojemu MSCA, da pridobi pripadajoči certifikat za enoto v vozilu, podpisan s strani MSCA. Zasebni ključ uporablja samo enota v vozilu.“;

(d) točka 9.1.5 se spremeni:

(i) odstavek CSM_83 se nadomesti z naslednjim:

„CSM_83 Za vsako tahografsko kartico se ustvari en edinstven par ključev ECC, označen kot Card_MA. Poleg tega se za vsako vozniško kartico in vsako kartico servisne delavnice ustvari drug edinstven par ključev ESS, označen kot Card_Sign. To nalogo lahko prevzamejo proizvajalci ali personalizatorji kartic. Kadar koli se ustvari par ključev kartice, mora stran, ki ga ustvari, javni ključ poslati svojemu MSCA, da pridobi pripadajoči certifikat kartice, podpisan s strani MSCA. Zasebni ključ uporablja samo tahografska kartica.“;

(ii) odstavek CSM_88 se nadomesti z naslednjim:

„CSM_88 Veljavnost certifikata Card_MA je:

— za vozniške kartice: 5 let

— za kartice podjetja: 5 let

— za nadzorne kartice: 2 leti

— za kartice servisne delavnice: 1 leto“;

(iii) v odstavku CSM_91 se doda naslednje besedilo:

„— poleg tega izključno za nadzorne kartice, kartice podjetja in kartice servisne delavnice, in to samo v primeru, da so take kartice izdane v prvih treh mesecih obdobja veljavnosti novega certifikata EUR: dve generaciji starejši certifikat EUR, če obstaja.

Opomba k zadnji alinei: na primer, v prvih treh mesecih veljavnosti certifikata ERCA(3) (glej sliko 1), morajo zadevne kartice vsebovati certifikat ERCA(1). To je potrebno, da se zagotovi, da se te kartice lahko uporabljajo za prenose podatkov z enot v vozilu ERCA(1), katerih običajna 15-letna življenjska doba in 3-mesečno obdobje za prenos podatkov se izteče v teh mesecih; glej zadnjo točko zahteve 13) iz Priloge IC.“;

(e) točka 9.1.6 se spremeni:

(i) odstavek CSM_93 se nadomesti z naslednjim:

„CSM_93 Za vsako zunanjo GNSS opremo se ustvari en edinstven par ključev ECC, označen kot EGF_MA. To nalogo prevzamejo proizvajalci zunanje GNSS opreme. Kadar koli se ustvari par ključev EGF_MA, mora stran, ki ga ustvari, javni ključ poslati svojemu MSCA, da pridobi pripadajoči certifikat EGF_MA, podpisan s strani MSCA. Zasebni ključ uporablja samo zunanja GNSS oprema.“;

(ii) odstavek CSM_95 se nadomesti z naslednjim:

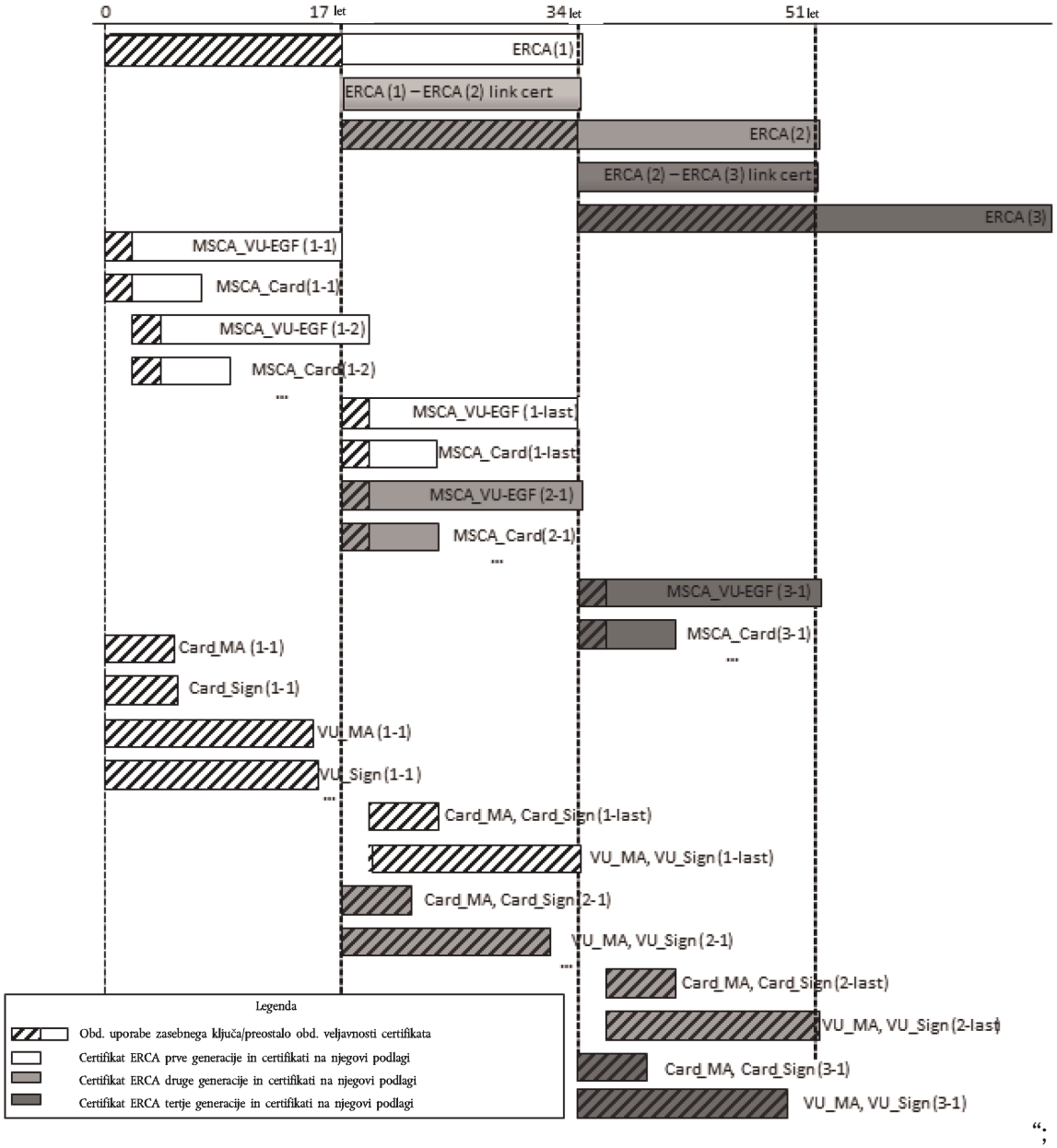
„CSM_95 Zunanja GNSS oprema svoj par ključev EGF_MA, ki je sestavljen iz zasebnega ključa EGF_MA.SK in javnega ključa EGF_MA.PK, uporablja izključno za medsebojno avtentikacijo in uskladitev ključa seje glede na enote v vozilu, kot je določeno v oddelku 11.4 tega dodatka.“;

(f) točka 9.1.7 se spremeni:

(i) slika 1 se nadomesti z naslednjim:

„Slika 1

Izdajanje in uporaba različnih generacij korenskih certifikatov ERCA, veznih certifikatov ERCA, certifikatov MSCA in certifikatov opreme



“;

(ii) odstavek 6 v opombah k sliki 1 se nadomesti z naslednjim:

„6. Da se prihrani prostor, je razlika med obdobjem veljavnosti certifikatov Card_MA in Card_Sign prikazana samo za prvo generacijo.“;

(g) točka 9.2.1.1 se spremeni:

(i) v odstavku CSM_106 se prva alinea nadomesti z naslednjim:

„— za 128-bitne glavne ključe tipala gibanja: CV = ‚B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83‘ “;

(ii) v odstavku CSM_107 se prvi pododstavek nadomesti z naslednjim:

„Vsak proizvajalec tipal gibanja za vsako tipalo gibanja ustvari naključen in edinstven povezovalni ključ K_P in vsak povezovalni ključ pošlje certifikacijskemu organu svoje države članice. MSCA z glavnim ključem tipala gibanja K_M šifrira vsak povezovalni ključ posebej in šifriran ključ vrne proizvajalcu tipala gibanja. Za vsak šifriran ključ MSCA proizvajalca tipala gibanja obvesti o številki različice ustrezajočega K_M.“;

(iii) odstavek CSM_108 se nadomesti z naslednjim:

„CSM_108 Vsak proizvajalec tipal gibanja za vsako tipalo gibanja ustvari edinstveno serijsko številko in vse serijske številke pošlje certifikacijskemu organu svoje države članice. MSCA vsako serijsko številko posebej šifrira z identifikacijskim ključem K_{ID} in šifrirano serijsko številko vrne proizvajalcu tipala gibanja. Za vsako šifrirano serijsko številko MSCA proizvajalca tipala gibanja obvesti o številki različice ustrezajočega K_{ID}.“;

(h) točka 9.2.2.1 se spremeni:

(i) odstavek CSM_123 se nadomesti z naslednjim:

„CSM_123 Proizvajalec enote v vozilu za vsako enoto v vozilu ustvari edinstveno serijsko številko VU in jo pošlje certifikacijskemu organu države članice, v kateri ima sedež, z zahtevkom za pridobitev dveh posebnih ključev DSRC enote v vozilu. Serijska številka VU ima podatkovni tip VuSerialNumber.

Opomba:

— Ta serijska številka VU je identična podatkovnemu elementu vuSerialNumber zapisa VuIdentification, glej Dodatek 1, in referenci imetnika certifikata v certifikatih VU.

— Serijska številka VU v trenutku, ko proizvajalec enote v vozilu zahteva posebne ključe DSRC enote v vozilu, morda ni znana. V tem primeru proizvajalec enote v vozilu namesto tega pošlje edinstveni identifikator zahtevka za certifikat, ki ga je uporabil, ko je zahteval certifikate VU; glej CSM_153. Ta identifikator zahtevka za certifikat je zato enakovreden referenci imetnika certifikata iz certifikatov VU.“;

(ii) v odstavku CSM_124 se alinea „info“ v koraku 2 nadomesti z naslednjim:

„info = serijska številka VU ali identifikator zahtevka za certifikat, kot je določeno v CSM_123“;

(iii) odstavek CSM_128 se nadomesti z naslednjim:

„CSM_128 MSCA vodi evidenco vseh posebnih ključev DSRC VU, ki jih je ustvaril, njihovih številk različice in serijskih številk VU ali identifikatorjev zahtevka za certifikat, uporabljenih pri njihovi izpeljavi.“;

(i) v točki 9.3.1 se prvi pododstavek odstavka CSM_135 nadomesti z naslednjim:

„Posebna pravila kodiranja (DER) v skladu z [ISO 8825-1] se uporabljajo za označevanje podatkovnih objektov v certifikatih. Tabela 4 prikazuje celotno kodiranje certifikata, vključno z vsemi bajti oznak in dolžine.“;

(j) v točki 9.3.2.3 se odstavek CSM_141 nadomesti z naslednjim:

„CSM_141 Pooblastilo imetnika certifikata se uporablja za identifikacijo tipa certifikata. Sestavljeno je iz šestih bitov z največjo težo ID aplikacije tahografa, povezane s tipom opreme, ki določa tip opreme, za katero je certifikat namenjen. V primeru certifikata VU, certifikata vozniške kartice ali certifikata kartice servisne delavnice se tip opreme uporablja tudi za razlikovanje med certifikatom za medsebojno avtentikacijo in certifikatom za ustvarjanje digitalnih podpisov (glej oddelek 9.1 in Dodatek 1, podatkovni tip equipmentType).“;

(k) v točki 9.3.2.5 se v odstavku CSM_146 doda naslednji pododstavek:

„*Opomba:* Za certifikat kartice je vrednost CHR enaka vrednosti cardExtendedSerialNumber v EF_ICC; glej Dodatek 2. Za certifikat EGF je vrednost CHR enaka vrednosti sensorGNSSSerialNumber v EF_ICC; glej Dodatek 14. Za certifikat VU je vrednost CHR enaka podatkovnemu elementu vuSerialNumber v zapisu VuIdentification, glej Dodatek 1, razen če proizvajalec v trenutku, ko se certifikat zahteva, ne pozna posebne serijske številke proizvajalca.“;

(l) v točki 9.3.2.6 se odstavek CSM_148 nadomesti z naslednjim:

„CSM_148 Datum začetka veljavnosti certifikata označuje datum začetka in čas veljavnosti certifikata.“;

(m) točka 9.3.3 se spremeni:

(i) v odstavku CSM_151 se prvi pododstavek nadomesti z naslednjim:

„Pri zahtevku za certifikat mora MSCA ERCA poslati naslednje podatke:“;

(ii) odstavek CSM_153 se nadomesti z naslednjim:

„CSM_153 Proizvajalec opreme mora v zahtevku za certifikat MSCA poslati naslednje podatke, ki MSCA omogočijo, da ustvari referenco imetnika certifikata novega certifikata za opremo:

— serijsko številko naprave, edinstveno za proizvajalca, vrsto naprave in mesec proizvodnje (če jih pozna, glej CSM_154), sicer pa edinstven identifikator zahtevka za certifikat.

— mesec in leto izdelave opreme ali zahtevka za certifikat.

Proizvajalec zagotovi, da so ti podatki pravilni in da se certifikat, ki ga MSCA vrne, vnese v opremo, za katero je namenjen.“;

(n) točka 10.2.1 se spremeni:

(i) v odstavku CSM_157 se besedilo pred opombami k sliki 4 nadomesti z naslednjim:

„Enote v vozilu za preverjanje verige certifikatov tahografske kartice uporabljajo protokol, prikazan na sliki 4. Za vsak certifikat, ki ga VU prebere iz kartice, VU preveri, da je polje ‚pooblastilo imetnika certifikata‘ (CHA) pravilno:

— v polju CHA certifikata Card mora biti naveden certifikat kartice za medsebojno avtentikacijo (glej Dodatek 1, podatkovni tip EquipmentType);

— v polju CHA certifikata Card.CA mora biti naveden MSCA;

— v polju CHA certifikata Card.Link mora biti naveden ERCA.“;

(ii) v odstavku CSM_159 se doda naslednji stavek:

„Medtem ko je shranjevanje vseh drugih tipov certifikatov neobvezno, pa mora VU obvezno shraniti nov vezni certifikat, ki ga predloži kartica.“;

(o) točka 10.2.2 se spremeni:

(i) v odstavku CSM_161 se besedilo pred sliko 5 nadomesti z naslednjim:

„Tahografske kartice za preverjanje verige certifikatov VU uporabljajo protokol, prikazan na sliki 5. Za vsak certifikat, ki ga predloži VU, kartica preveri, da je polje „pooblastilo imetnika kartice“ (CHA) pravilno:

— v polju CHA certifikata VU.Link mora biti naveden ERCA;

— v polju CHA certifikata VU.CA mora biti naveden MSCA;

— v polju CHA certifikata VU mora biti naveden certifikat VU za medsebojno avtentikacijo (glej Dodatek 1, podatkovni tip EquipmentType).“;

(ii) odstavek CSM_165 se nadomesti z naslednjim:

„CSM_165 Če je ukaz MSE: Set AT neuspešen, kartica navedeni VU.PK nastavi za poznejšo uporabo med avtentikacijo v vozilu in začasno shrani Comp(VU.PKeph). Če sta pred uskladitvijo ključa seje poslana dva ali več ukazov MSA: Set AT, kartica shrani samo zadnji prejeti Comp(VU.PKeph). Kartica ponastavi Comp(VU.PKeph) po uspešnem ukazu GENERAL AUTHENTICATE.“;

(p) točka 10.3 se spremeni:

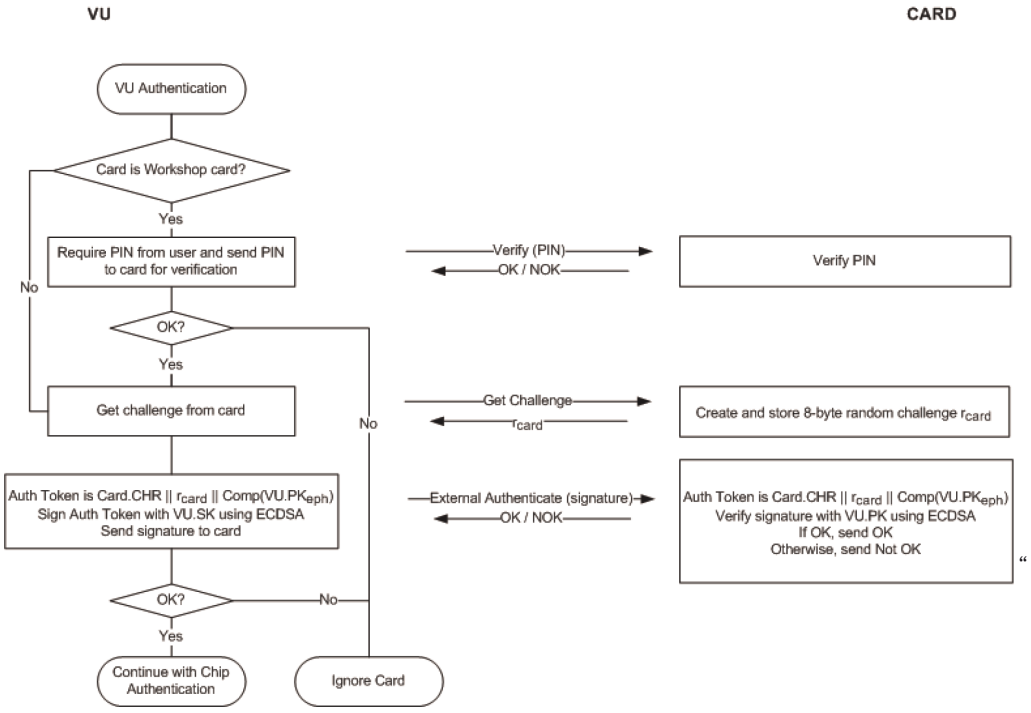
(i) prvi pododstavek odstavka CSM_170 se nadomesti z naslednjim:

„Poleg poziva kartica VU v podpis vključi referenco imetnika certifikata, ki jo pridobi iz certifikata kartice.“;

(ii) v odstavku CSM_171 se slika 6 nadomesti z naslednjim:

„Slika 6

Protokol avtentikacije VU



“

(iii) odstavek CSM_174 se nadomesti z naslednjim:

„CSM_174 Po prejemu podpisa VU v ukazu EXTERNAL AUTHENTICATE kartica:

— izračuna avtentikacijski žeton tako, da poveže Card.CHR, poziv kartice rcard in identifikator kratkotrajnega javnega ključa VU Comp(VU.PKeph),

— preveri podpis VU z uporabo algoritma ECDSA in zgoščevalnega algoritma, povezanega z velikostjo ključa para ključev VU VU_MA, kot je določeno v CSM_50, v povezavi z VU.PK in izračunanim avtentikacijskim žetonom.“;

(q) v točki 10.4 se odstavek CSM_176 spremeni:

(i) pododstavek 2. se nadomesti z naslednjim:

„2. VU kartici pošlje javno točko $VU.PK_{eph}$ svojega kratkotrajnega para ključev. Javna točka se pretvori v oktetni niz, kot je določeno v [TR-03111]. Uporabi se nestisnjeni format kodiranja. Kot je pojasnjeno v CSM_164, je VU ta kratkotrajni par ključev ustvarila pred preverjanjem verige certifikatov VU. VU je identifikator kratkotrajnega javnega ključa Comp($VU.PK_{eph}$) poslala kartici, ta pa ga je shranila.“;

(ii) pododstavek 6. se nadomesti z naslednjim:

„6. Z uporabo K_{MAC} kartica izračuna avtentikacijski žeton glede na kratkotrajno javno točko VU: T_{PICC} = CMAC(K_{MAC}, $VU.PK_{eph}$). Javna točka je v formatu, ki ga uporablja VU (glej točko 2 zgoraj). Kartica enoti v vozilu pošlje N_{PICC} in T_{PICC}.“;

(r) v točki 10.5.2 se odstavek CSM_191 nadomesti z naslednjim:

„CSM_191 Vsak podatkovni objekt, ki ga je treba šifrirati, se zapolni v skladu z [ISO 7816-4] z uporabo indikatorja vsebine zapolnjevanja ‚01'. Za izračun MAC se podatkovni objekt v APDU zapolni v skladu z [ISO 7816-4].

Opomba: Zapolnjevanje za varno sporočanje se vedno opravi s plastjo varnega sporočanja, ne pa z algoritmom CMAC ali CBC.

Povzetek in primeri

Ukaz APDU z uporabo varnega sporočanja bo imel naslednjo strukturo, odvisno od ustreznega nezavarovanega ukaza (DO je podatkovni objekt):

Primer 1: CLA INS P1 P2 || Lc' || DO '8E' || Le

Primer 2: CLA INS P1 P2 || Lc' || DO '97' || DO '8E' || Le

Primer 3 (sodi INS bajt): CLA INS P1 P2 || Lc' || DO '81' || DO '8E' || Le

Primer 3 (lihi INS bajt): CLA INS P1 P2 || Lc' || DO 'B3' || DO '8E' || Le

Primer 4 (sodi INS bajt): CLA INS P1 P2 || Lc' || DO '81' || DO '97' || DO'8E' || Le

Primer 4 (lihi INS bajt): CLA INS P1 P2 || Lc' || DO 'B3' || DO '97' || DO'8E' || Le

pri čemer je Le = '00' ali '00 00', odvisno od tega, ali se uporabljajo kratka podatkovna polja ali podaljšana podatkovna polja; glej [ISO 7816-4].

Odziv APDU z uporabo varnega sporočanja bo imel naslednjo strukturo, odvisno od ustreznega nezavarovanega odziva:

Primer 1 ali 3: DO '99' || DO '8E' || SW1SW2

Primer 2 ali 4 (sodi INS bajt) brez šifriranja: DO '81' || DO '99' || DO '8E' || SW1SW2

Primer 2 ali 4 (sodi INS bajt) s šifriranjem: DO '87' || DO '99' || DO '8E' || SW1SW2

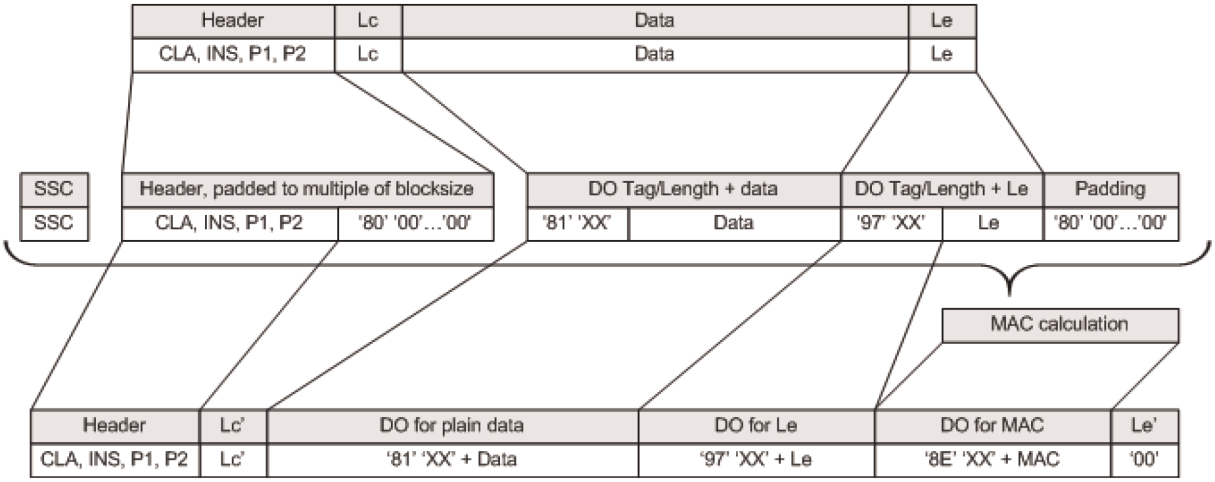
Primer 2 ali 4 (lihi INS bajt) brez šifriranja: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Opomba: Primer 2 ali 4 (lihi INS bajt) s šifriranjem se v komunikaciji med VU in kartico nikoli ne uporablja.

V nadaljevanju so navedeni trije primeri transformacij APDU za ukaze s sodo INS kodo. Slika 8 prikazuje avtenticiran ukaz APDU za primer 4, slika 9 avtenticiran odziv APDU za primer 1/primer 3, slika 10 pa šifriran in avtenticiran odziv APDU za primer 2/primer 4.

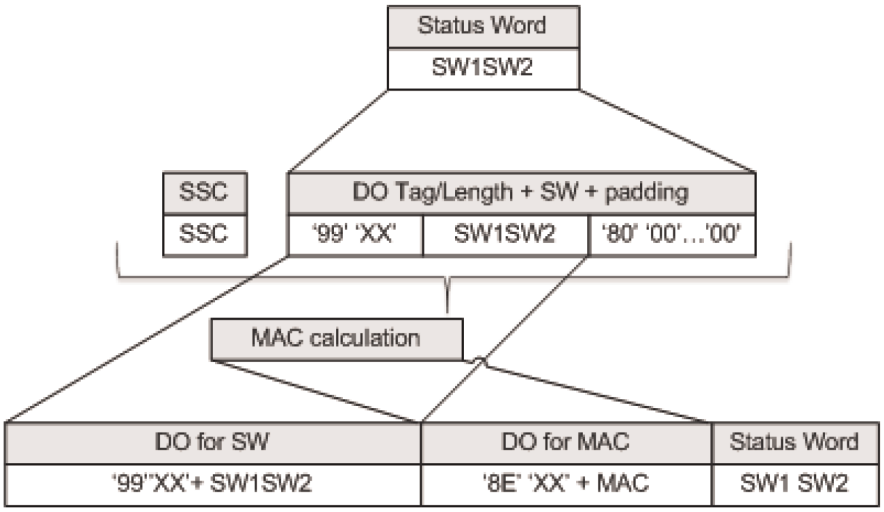
Slika 8

Transformacija avtenticiranega ukaza APDU za primer 4



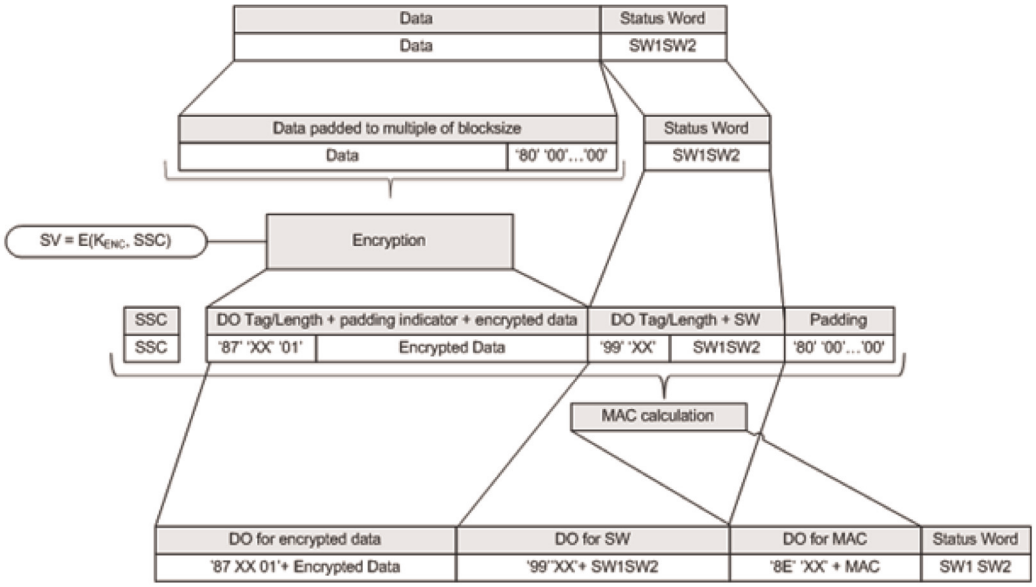
Slika 9

Transformacija avtenticiranega odziva APDU za primer 1/primer 3



Slika 10

Transformacija šifriranega in avtenticiranega odziva APDU za primer 2/primer 4



“

(s) v točki 10.5.3 se odstavek CSM_193 nadomesti z naslednjim:

„CSM_193 Tahografska kartica prekine sejo varnega sporočanja samo v primeru, da se zgodi kar koli od naslednjega:

— Tahografska kartica prejme ukaz APDU v neformatiranem besedilu.

— Tahografska kartica v ukazu APDU zazna napako v varnem sporočanju:

— ni pričakovanega podatkovnega objekta varnega sporočanja, vrstni red podatkovnih objektov je nepravilen, vključen je nepoznan podatkovni objekt,

— podatkovni objekt varnega sporočanja je nepravilen, npr. nepravilna vrednost MAC, nepravilna struktura TLV.

— Tahografska kartica ostane brez napajanja ali se ponastavi.

— VU izbere aplikacijo na kartici.

— Dosežena je mejna vrednost števila ukazov in povezanih odzivov v trenutni seji. Za posamezno kartico to mejno vrednost določi proizvajalec ob upoštevanju varnostnih zahtev uporabljene strojne opreme, pri čemer je največja vrednost 240 ukazov in povezanih odzivov SM na sejo.“;

(t) točka 11.3.2 se spremeni:

(i) prvi pododstavek odstavka CSM_208 se nadomesti z naslednjim:

„Med povezovanjem z VU zunanja GNSS oprema uporabi protokol, prikazan na sliki 5 (oddelek 10.2.2), da preveri verigo certifikatov VU.“;

(ii) odstavek CSM_210 se nadomesti z naslednjim:

„CSM_210 Ko zunanja GNSS oprema preveri certifikat VU_MA, ga shrani za uporabo med običajnim delovanjem; glej oddelek 11.3.3.“;

(u) v točki 11.3.3 se prvi pododstavek odstavka CSM_211 nadomesti z naslednjim:

„Med običajnim delovanjem enota v vozilu in EGF za preverjanje časovne veljavnosti shranjenega certifikata EGF_MA in za nastavitev javnega ključa VU_MA za kasnejšo avtentikacijo VU uporabljata protokol s slike 11. Med običajnim delovanjem se ne opravi nobeno dodatno medsebojno preverjanje.“;

(v) v točki 12.3. se preglednica 6 nadomesti z naslednjim:

„Preglednica 6

Število podatkovnih bajtov (v neformatiranem besedilu in šifriranih) na posamezno navodilo v skladu z [ISO 16844-3]

Navodilo	Zahtevek/ odziv	Opis podatkov	Št. podatkovnih bajtov v neformatiranem besedilu v skladu z [ISO 16844-3]	Št. podatkovnih bajtov v neformatiranem besedilu pri uporabi ključev AES	Št. šifriranih podatkovnih bajtov pri uporabi ključev AES dolžine		
					128	192	256
10	zahtevek	podatki za avtentikacijo + številka datoteke	8	8	16	16	16
11	odziv	podatki za avtentikacijo + vsebina datoteke	16 ali 32, odvisno od datoteke	16 ali 32, odvisno od datoteke	32/48	32/48	32/48
41	zahtevek	serijska številka tipala gibanja	8	8	16	16	16
41	odziv	povezovalni ključ	16	16/24/32	16	32	32
42	zahtevek	ključ seje	16	16/24/32	16	32	32
43	zahtevek	informacije o povezavi	24	24	32	32	32
50	odziv	informacije o povezavi	24	24	32	32	32
70	zahtevek	podatki za avtentikacijo	8	8	16	16	16
80	odziv	vrednost števca tipala gibanja + podatki za avtentikacijo	8	8	16	16	16“

(w) v točki 13.1. se zahteva glede serijske številke VU v pododstavku CSM_224 nadomesti z naslednjim:

„**Serijska številka VU** serijska številka VU ali identifikator zahtevka za certifikat (podatkovni tip VuSerialNumber ali CertificateRequestID) – glej CSM_123“;

(x) v točki 13.3. se druga alinea odstavka CSM_228 nadomesti z naslednjim:

„2. Nadzorna kartica uporabi navedeni glavni ključ DSRC v kombinaciji s serijsko številko VU ali identifikatorjem zahtevka za certifikat v zaščitnih podatkih DSRC, da ustvari posebna ključa DSRC $K\_VU_{DSR}C\_ENC$ in $K\_VU_{DSRC}\_MAC$ za VU, kot je navedeno v CSM_124.“;

(y) točka 14.3 se spremeni:

(i) v odstavku CSM_234 se besedilo pred opombami k sliki 13 nadomesti z naslednjim:

„IDE lahko preverjanje podpisa na podlagi prenesenih podatkov opravi sama, ali pa za ta namen uporabi nadzorno kartico. Če uporablja nadzorno kartico, se preverjanje podpisa opravi, kot je prikazano na Figure 13. Za preverjanje časovne veljavnosti certifikata, ki ga predloži IDE, nadzorna kartica uporabi svoj interni trenutni čas, kot je določeno v CSM_167. Nadzorna kartica posodobi trenutni čas, če je datum začetka veljavnosti avtentičnega certifikata, ki predstavlja veljaven časovni vir, novejši od trenutnega časa kartice. Kartica kot veljaven časovni vir sprejme samo naslednje certifikate:

— vezne certifikate ERCA druge generacije,

— vezne certifikate MSCA druge generacije,

— certifikate VU_Sign ali Card_Sign druge generacije, ki jih izda ista država kot certifikate nadzorne kartice.

Če preverjanje podpisa opravi sama, IDE preveri avtentičnost in veljavnost vseh certifikatov v verigi certifikatov v podatkovni datoteki ter podpis glede na shemo podpisovanja, določeno v [DSS]. V obeh primerih je treba za vsak certifikat, prebran iz podatkovne datoteke, preveriti, da je polje ‚pooblastilo imetnika certifikata‘ (CHA) pravilno:

— v polju CHA certifikata EQT mora biti naveden certifikat VU ali Card (kot je primerno) za podpis (glej Dodatek 1, podatkovni tip EquipmentType),

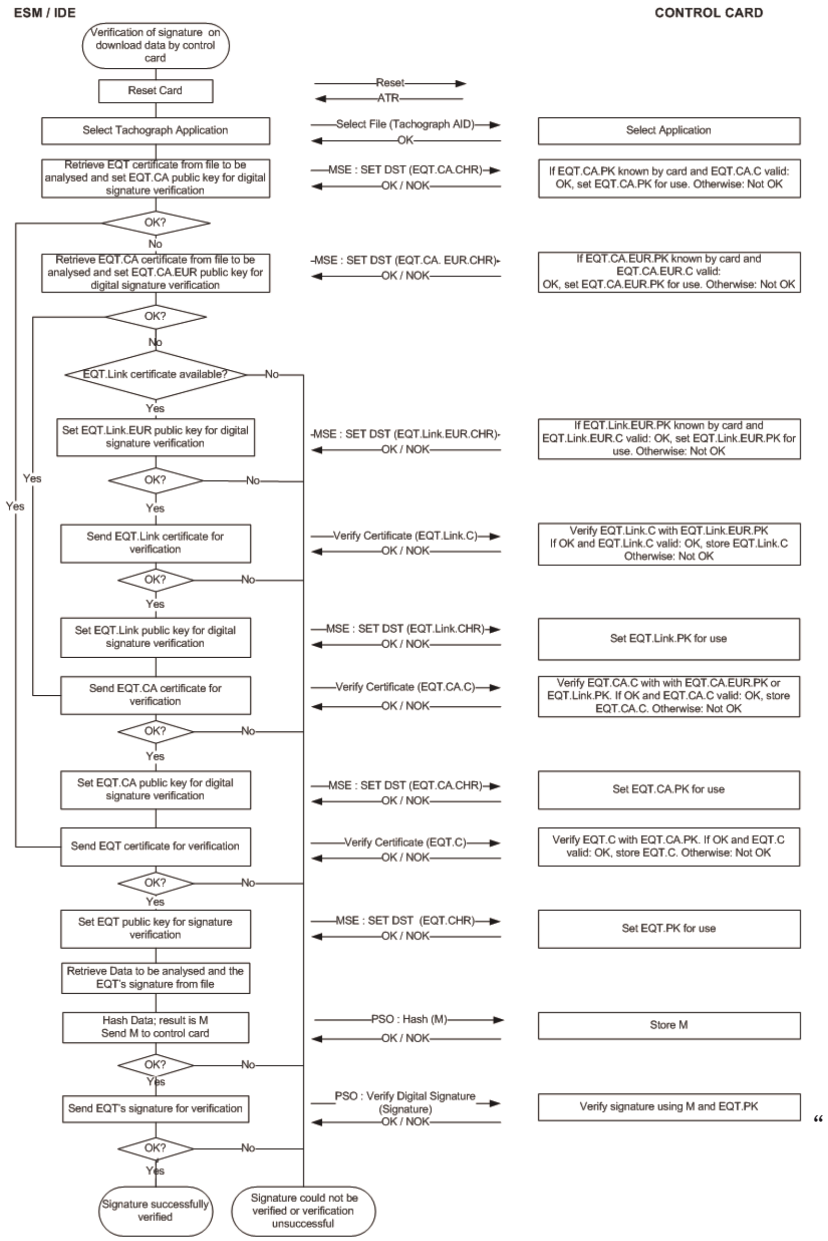
— v polju CHA certifikata EQT.CA mora biti naveden MSCA,

— v polju CHA certifikata EQT.Link mora biti naveden ERCA.“;

(ii) slika 13 se nadomesti z naslednjim:

„Slika 13

Protokol za preverjanje podpisa glede na preneseno podatkovno datoteko



“

(37) Dodatek 12 se spremeni:

(a) točka 3. se spremeni:

(i) v odstavku GNS_4, se drugi pododstavek za sliko 2 nadomesti z naslednjim:

„Ločljivost določitve položaja temelji na formatu zgoraj opisanega RMC sporočila. Prvi del polja 3 in polja 5 predstavljata stopinje. Preostala mesta predstavljajo minute s tremi decimalnimi mesti. Ločljivost je tako 1/1 000 minute ali 1/60 000 stopinje (kajti ena minuta je 1/60 stopinje).“;

(ii) odstavek GNS_5 se nadomesti z naslednjim:

„GNS_5 Enota v vozilu v svoj pomnilnik shrani informacijo o položaju glede na zemljepisno širino in dolžino z ločljivostjo 1/10 minute ali 1/600 stopinje, kot je opisano v Dodatku 1 za tip GeoCo-ordinates.

VU lahko uporabi ukaz GPS DOP in aktivni sateliti (GSA), da določi in zapiše razpoložljivost signala in točnost meritve. Za oceno ravni točnosti zapisanih podatkov o lokaciji se uporablja zlasti HDOP (glej 4.2.2). VU shrani vrednost napake pri določanju horizontalnega položaja (HDOP), izračunano kot minimalno vrednost HDOP, pridobljeno od razpoložljivih sistemov GNSS.

GNSS Id. označuje ustrezno NMEA Id. za vsak satelitski sistem GNSS in satelitski dopolnilni sistem (SBAS).

Slika 3

Struktura sporočila GSA

1234 1415 16 17 18

$<GNSS Id.>GSA,a,a,x,x,x,x,x,x,x,x,x,x,x,x,x,x.x,x.x,x.x*hh

1) Izbirni način
2) Način
3) ID 1. satelita, ki se uporablja za določitev položaja
4) ID 2. satelita, ki se uporablja za določitev položaja
...
14) ID 12. satelita, ki se uporablja za določitev položaja
15) PDOP
16) HDOP
17) VDOP
18) Kontrolna vsota “

(iii) odstavek GNS_6 se nadomesti z naslednjim:

„GNS_6 Sporočilo GSA se shrani pod številko zapisa ‚02‘ do ‚06‘“.

(b) točka 4.2.1 se spremeni:

(i) odstavek GNS_16 se nadomesti z naslednjim:

„GNS_16 V komunikacijskem protokolu podaljšana podatkovna polja niso podprta.“;

(ii) odstavek GNS_18 se nadomesti z naslednjim:

„GNS_18 V zvezi s funkcijami 1 (zbiranje in distribucija GNSS podatkov), 2 (zbiranje podatkov o konfiguraciji zunanje GNSS opreme) in 3 (protokol za upravljanje) zaščiteni GNSS oddajnik-sprejemnik simulira pametno kartico, katere arhitektura datotečnega sistema sestoji iz glavne datoteke (MF), namenske datoteke (DF) z identifikatorjem aplikacije v skladu s poglavjem 6.2 Dodatka 1 (‚FF 44 54 45 47 4D') ter tremi elementarnimi datotekami, ki vsebujejo certifikate, in eno samo elementarno datoteko (EF.EGF) z identifikatorjem datotek ‚2F2F', kot je opisano v tabeli 1.";

(iii) odstavek GNS_20 se nadomesti z naslednjim:

„GNS_20 Zaščiteni GNSS oddajnik-sprejemnik za shranjevanje podatkov uporablja pomnilnik, ki je zmožen opraviti vsaj 20 milijonov bralno/pisalnih ciklov. Razen tega sta zasnova notranjosti in izvedba zaščitenega GNSS oddajnika-sprejemnika v domeni proizvajalcev.

Preslikava zapisanih števil in podatkov je določena v tabeli 1. Treba je opozoriti, da obstaja pet sporočil GSA za konstelacije GNSS in satelitski dopolnilni sistem (SBAS)".

(c) v točki 4.2.2 se pododstavek 5 odstavka GNS_23 nadomesti z naslednjim:

„5. Procesor VU preveri prejete podatke z izluščenjem informacij (npr. o zemljepisni širini in dolžini, času) iz RMC sporočila NMEA. RMC sporočilo NMEA vključuje informacijo o tem, ali je položaj veljaven. Če položaj ni veljaven, podatki o lokaciji še niso na voljo in se jih ne sme uporabiti za zapisovanje položaja vozila. Če je položaj veljaven, procesor VU iz stavkov GSA NMEA izlušči tudi vrednosti HDOP in izračuna najnižjo vrednost za razpoložljive satelitske sisteme (tj. ko je določitev položaja na voljo).";

(d) v točki 4.4.1 se odstavek GNS_28 nadomesti z naslednjim:

„GNS_28 Če VU povezani zunanji GNSS opremi več kot 20 zaporednih minut ne uspe sporočiti ničesar, VU ustvari in v VU zapiše dogodek vrste EventFaultType z vrednostjo enum ‚0E'H ‚napaka pri komuniciranju z zunanjo GNSS opremo', ki mu dodeli časovni žig s trenutnim časom. Dogodek bo ustvarjen samo, če sta izpolnjena naslednja pogoja: a) pametni tahograf ni v kalibracijskem načinu in b) vozilo se premika. V tem kontekstu se napaka pri komuniciranju sproži, kadar zaščiteni oddajnik-sprejemnik VU ne prejme sporočila odziva po poslanem sporočilu z zahtevkom, kot je opisano v oddelku 4.2.";

(e) v točki 4.4.2 se odstavek GNS_29 nadomesti z naslednjim:

„GNS_29 Če je prekršena celovitost zunanje GNSS opreme, zaščiteni GNSS oddajnik-sprejemnik v celoti izbriše svoj pomnilnik, vključno s kriptografskimi gradivi. Kot je opisano v GNS_25 in GNS_26, VU zazna poskus manipulacije, če je stanje odziva ‚6690'. VU nato ustvari dogodek vrste EventFaultType z vrednostjo enum ‚19'H ‚zaznavanje poskusov manipulacije GNSS'. Druga možnost je, da se zunanja GNSS oprema ne odzove na nobeno zunanjo zahtevo več.";

(f) v točki 4.4.3 se odstavek GNS_30 nadomesti z naslednjim:

„GNS_30 Če zaščiteni GNSS oddajnik-sprejemnik več kot 3 zaporedne ure od GNSS sprejemnika ne prejme nobenih podatkov, zaščiteni GNSS oddajnik-sprejemnik na ukaz READ RECORD ustvari sporočilo odziva s številko RECORD ‚01' in podatkovnim poljem v dolžini 12 bajtov, ki so vsi nastavljeni na 0xFF. Po prejemu sporočila odziva s to vrednostjo podatkovnega polja, VU ustvari in zapiše dogodek vrste EventFaultType z vrednostjo enum ‚0D'H ‚ni informacij o položaju s strani GNSS sprejemnika', ki mu dodeli časovni žig s trenutnim časom, samo, če sta izpolnjena naslednja pogoja: a) pametni tahograf ni v kalibracijskem načinu in b) vozilo se premika.";

(g) v točki 4.4.4 se besedilo odstavka GNS_31 do slike 4 nadomesti z naslednjim:

„Če VU zazna, da certifikat EGF, ki se uporablja za medsebojno avtentikacijo, ni več veljaven, VU ustvari in zapiše dogodek na zapisovalni napravi vrste EventFaultType z vrednostjo enum *‚1B'H ‚certifikat zunanje GNSS opreme je potekel'*, ki ji dodeli časovni žig s trenutnim časom. VU kljub temu uporabi prejete GNSS podatke o položaju.“;

(h) v točki 5.2.1 se odstavek GNS_34 nadomesti z naslednjim:

„GNS_34 Če VU več kot 3 zaporedne ure od GNSS sprejemnika ne prejme nobenih podatkov, VU ustvari in zapiše dogodek vrste EventFaultType z vrednostjo enum ‚0D'H ‚ni informacij o položaju s strani GNSS sprejemnika', ki mu dodeli časovni žig s trenutnim časom, samo, če sta izpolnjena naslednja pogoja: a) pametni tahograf ni v kalibracijskem načinu in b) vozilo se premika.“;

(i) točka 6. se nadomesti z naslednjim:

„6. ČASOVNO NAVZKRIŽJE Z GNSS

Če VU zazna odstopanje, večje od 1 minute, med časom, ki ga beleži funkcija za merjenje časa enote v vozilu, in časom, ki ga posreduje GNSS sprejemnik, VU zapiše dogodek vrste EventFaultType z vrednostjo enum *‚0B'H ‚časovno navzkrižje (med GNSS in notranjo uro VU)'*. Po sproženju dogodka časovnega navzkrižja enota v vozilu naslednjih 12 ur ne preverja časovnega navzkrižja. Ta dogodek se ne sproži, kadar GNSS sprejemnik v zadnjih 30 dneh ni mogel odkriti veljavnega GNSS signala.“;

(38) Dodatek 13 se spremeni:

(a) v točki 2. se četrti odstavek nadomesti z naslednjim:

„Pojasnilo: ta dodatek ne določa:

— operacij in vodenja v zvezi z zbiranjem *podatkov* v VU (to je opredeljeno drugje *v Uredbi* ali pa je odvisno od zasnove izdelka),

— oblike predstavitve zbranih podatkov v aplikaciji na zunanji napravi,

— določb o varnosti podatkov, ki presegajo Bluetooth® (npr. šifriranje) in zadevajo vsebino *podatkov* (te so določene drugje v *Uredbi* [Dodatek 11 Skupni varnostni mehanizmi]).

— protokolov Bluetooth®, ki jih uporablja vmesnik z ITS“;

(b) v točki 4.2. se tretji odstavek nadomesti z naslednjim:

„Ko zunanja naprava prvič pride v območje dosega VU, se postopek povezave Bluetooth® lahko začne (glej tudi Prilogo 2). Napravi si izmenjata naslova, imeni, profila in skupni zaupni ključ, tako da se lahko v prihodnosti kadar koli povežeta. Ko je ta korak zaključen, VU zaupa zunanji napravi, ki lahko začne pošiljati zahtevke za prenos podatkov s tahografa. Dodatni šifrirni mehanizmi, ki presegajo Bluetooth®, niso predvideni. Če pa so potrebni dodatni varnostni mehanizmi, se določijo v skladu z Dodatkom 11 Skupni varnostni mehanizmi.“;

(c) točka 4.3. se spremeni:

(i) prvi odstavek se nadomesti z naslednjim:

„Iz varnostnih razlogov bo za VU potreben avtorizacijski sistem s kodo PIN, ločen od povezave Bluetooth. Vsaka VU mora biti za namene avtentikacije zmožna ustvariti kode PIN iz vsaj 4 števk. Vsakič, ko se zunanja naprava poveže z VU, mora vnesti pravilno kodo PIN, preden lahko prejme katere koli podatke.“;

(ii) tretji odstavek za tabelo 1 se nadomesti z naslednjim:

„Proizvajalec lahko ponudi možnost za neposredno zamenjavo kode PIN v VU, kode PUC pa ne sme biti možno zamenjati. Za spremembo kode PIN, če je mogoča, je treba vnesti veljavno kodo PIN neposredno v VU.“;

(d) v točki 4.4 se drugi odstavek za podnaslovom „Podatkovno polje“ nadomesti z naslednjim:

„Če podatki, ki jih je treba obdelati, presegajo razpoložljivi prostor v enem sporočilu, se razdelijo na več delnih sporočil. Vsako delno sporočilo ima enako glavo in SID, vendar za navedbo številke sporočila vsebuje 2-bajtni števec, tj. Counter Current (CC) in Counter Max (CM). Da se omogoči preverjanje napak in prekinitev prenosa, sprejemna naprava potrdi vsako delno sporočilo. Sprejemna naprava lahko delno sporočilo sprejme, zahteva njegov ponovni prenos, zahteva od naprave pošiljateljice, naj začne prenos znova, ali prekine prenos.“;

(e) Priloga 1 se spremeni:

(i) naslov se nadomesti z naslednjim:

„(1) SEZNAM RAZPOLOŽLJIVIH PODATKOV PREK VMESNIKA Z ITS“;

(ii) v tabelo se v točki (3) za postavko „Ni informacij o položaju s strani GNSS sprejemnika“ vstavi naslednja postavka:

„Napaka pri komuniciranju z zunanjo GNSS opremo	— najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov, — 5 najdaljših dogodkov v zadnjih 365 dneh.	— datum in čas začetka dogodka, — datum in čas konca dogodka, — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v danem dnevu.“

(iii) v točki (5) se doda naslednja alinea:

„— napaka vmesnika z ITS (če je ustrezno)“;

(f) specifikacije ASN.1 v Prilogi 3 se spremenijo:

(i) za vrstico 206 se dodajo naslednje vrstice 206a–206e:

```
“206a
206b       DriverID ::= SEQUENCE{
206c       issuingMemberState OCTET STRING (SIZE(3)),
206d       cardNumber OCTET STRING (SIZE(16))
206e }“;
```

(ii) vrstice 262–264 se nadomestijo z naslednjim:

```
„262    driveRecognize BIT STRING ('00'B UNION '01'B),
263     driverCardDriver1 BIT STRING ('00'B UNION '01'B),
264     driverCardDriver2 BIT STRING ('00'B UNION '01'B), “;
```

(iii) vrstica 275 se nadomesti z naslednjim:

```
„275    outOfScopeCondition BIT STRING ('00'B UNION '01'B),„;
```

(iv) vrstice 288–310 se nadomestijo z naslednjim:

```
„288    driver1WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
289     '011'B UNION '100'B UNION '101'B …),
290     driver2WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
291     '011'B UNION '100'B UNION '101'B …),
292
293     driver1TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
294     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
295     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
296     UNION '1011'B UNION '1100'B UNION '1101'B …),
297
298
299     driver2TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
300     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
301     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
302     UNION '1011'B UNION '1100'B UNION '1101'B …),
303
304
305
306     overSpeed BIT STRING ('00 'B UNION '01 'B),
307     driver1Identification DriverID,
308     driver2Identification DriverID,
309
310“
```

(v) vrstici 362 in 363 se nadomestita z naslednjim:

```
„362    driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363     driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),“;
```

(vi) za vrstico 410 se vstavita naslednji vrstici 410a in 410b:

```
„410a   comErrorWithExternalGNSSFacility
410b    CommunicationErrorWithTheExternalGNSSFacility,“;
```

(vii) za vrstico 539 se dodajo naslednje vrstice 539 a–539j:

```
„539a     CommunicationErrorWithTheExternalGNSSFacility ::= SEQUENCE{
539b      beginDate GeneralizedTime,
539c      endDate GeneralizedTime,
539d      cardsType SEQUENCE OF UTF8String,
539e      cardsNumber SEQUENCE OF INTEGER,
539f      issuingMemberState SEQUENCE OF NationAlpha,
539g      cardsGeneration SEQUENCE OF INTEGER,
539h      numberOfSimilarEvent INTEGER
539i            }
539j“;
```

(39) Dodatek 14 se spremeni:

(a) postavka 5.5 v kazalu se nadomesti z naslednjim:

„5.5 Podpora za Direktivo (EU) 2015/719 ..... 490“;

(b) v točki 2 se tretji odstavek nadomesti z naslednjim:

„V tem scenariju je čas, ki je na razpolago za *komunikacijo*, omejen, ker je komunikacija ciljno usmerjena in je po svoji zasnovi kratkega dosega. Poleg tega lahko pristojni nadzorni organi ista komunikacijska sredstva, ki se uporabljajo za nadzor tahografov na daljavo (RTM), uporabljajo tudi za druge namene (kot je največja teža in dimenzije težkih tovornih vozil, opredeljene v Direktivi (EU) 2015/719), take operacije pa so lahko po presoji pristojnih nadzornih organov ločene ali zaporedne.“;

(c) točka 5.1 se spremeni:

(i) v odstavku DSC_19 se dvanajsta alinea nadomesti z naslednjim:

„– Antena DSRC-VU je nameščena na mestu, na katerem omogoča najboljšo možno komunikacijo DSRC med vozilom in obcestno anteno, če je bralnik nameščen v razdalji 15 metrov pred vozilom in na višini 2 metra ter je usmerjen proti vodoravnemu in navpičnemu središču vetrobranskega stekla. Pri lahkih vozilih je primerna namestitev, ki ustreza zgornjemu delu vetrobranskega stekla. Pri vseh drugih vozilih se antena DSRC namesti blizu spodnjega ali zgornjega dela vetrobranskega stekla.“;

(ii) v odstavku DSC_22 se prvi pododstavek nadomesti z naslednjim:

„Faktor oblike antene ni opredeljen in je poslovna odločitev, vendar mora nameščeni DSRC-VU izpolnjevati zahteve o skladnosti, opredeljene v oddelku 5. Antena mora biti nameščena na položaju, ki je določen v DSC_19, in mora učinkovito podpirati primere uporabe iz 4.1.2 in 4.1.3.“;

(d) v točki 5.4.3 se zaporedje 7 nadomesti z naslednjim:

„7 REDCR > DSRC-VU Pošlje GET.request za podatke drugega atributa (če je primerno).“

(e) v točki 5.4.4 se opredelitev modula ASN.1 v odstavku DCS_40 spremeni:

(i) prva vrstica zaporedja za `TachographPayload` se nadomesti z naslednjim:

„`tp15638VehicleRegistrationPlate LPN – Vehicle Registration Plate as per EN 15509`[1]“

(ii) doda se opomba [1]:

„1. Če LPN vsebuje AlphabetIndicator LatinAlphabetNo2 ali latinCyrillicAlphabet, se posebni znaki ponovno preslikajo v enoto cestnega prikazovalnika z uporabo posebnih pravil v skladu s Prilogo E standarda ISO/DIS 14 906,2“;

(iii) v vrstici, kjer je opredeljen časovni žig tekočega zapisa, se črta nadpisana številka 2;

(iv) definicija modula ASN.1 za `RtmTransferAck` se nadomesti z naslednjim:

„
```
RtmTransferAck ::= INTEGER {
                   Ok (1),
                   NoK (2)
                   } (1..255)
```
“;

(f) v točki 5.4.5 se postavka RTM12 v tabeli 14.3 nadomesti z naslednjim:

„**RTM12** **Napaka na tipalu**	VU ustvari celoštevilčno vrednost za podatkovni element RTM12. VU spremenljivki sensorFault dodeli vrednost: — 1 če je bil v zadnjih 10 dneh zabeležen dogodek tipa ‚napaka na tipalu' ‚35H'; — 2 če je bil v zadnjih 10 dneh zabeležen dogodek tipa ‚napaka na GNSS sprejemniku' (notranja ali zunanja z vrednostjo enum ‚36'H ali ‚37'H); — 3 če je bil v zadnjih 10 dneh zapisan dogodek tipa ‚0E'H ‚napaka pri komuniciranju z zunanjo GNSS opremo'; — 4 če sta bila v zadnjih 10 dneh zapisana ‚napaka na tipalu' in ‚napaka GNSS sprejemnika'; — 5 če sta bila v zadnjih 10 dneh zapisana dogodka tipa ‚napaka na tipalu' in ‚napaka pri komuniciranju z zunanjo GNSS opremo'; — 6 če sta bila v zadnjih 10 dneh zapisana ‚napaka GNSS sprejemnika' in ‚napaka pri komuniciranju z zunanjo GNSS opremo'; — 7 če so bile v zadnjih 10 dneh zapisane vse tri napake na tipalu. ELSE dodeli vrednost 0,če v zadnjih 10 dneh ni bilo zapisanih nobenih dogodkov.	– Napaka na tipalu, en oktet v skladu s slovarjem podatkov.	`sensorFault INTEGER (0..255),` “

(g) v točki 5.4.6 se odstavek DSC_43 nadomesti z naslednjim:

„DSC_43 Pri vseh izmenjavah DSRC se podatki kodirajo z uporabo PER (Packed Encoding Rules) NEPORAVNANO, razen `TachographPayload` in `OwsPayload`;, ki se kodirata z OER (Octet Encoding Rules), kot so opredeljeni v ISO/IEC 8825-7, priporočilo ITU-T X.696.“;

(h) v točki 5.4.7 se v četrtem stolpcu tabele 14.9 besedilo v polju, ki opisuje `Rtm-ContextMark`; nadomesti z naslednjim:

„identifikator objekta podprtega standarda, dela in različice. Primer: ISO (1) standard (0) TARV (15638) del9 (9) različica1 (1).

Prvi oktet je 06H, to je identifikator objekta. Drugi oktet je 06H, to je njegova dolžina. V naslednjih 6 oktetih je kodiran identifikator objekta iz primera.“;

(i) točki 5.5 in 5.5.1 se nadomestita z naslednjim:

„5.5 **Podpora za Direktivo (EU) 2015/719**

5.5.1 *Pregled (Overview)*

DSC_59 Za podporo za Direktivo (EU) 2015/719 o največji teži in dimenzijah težkih tovornih vozil bo protokol transakcije za prenos podatkov OWS preko povezave z vmesnikom 5,8 GHz DSRC enak kot protokol za podatke RTM (glej 5.4.1) z edino razliko, da se bo z identifikatorjem objekta, ki se nanaša na standard TARV, naslavljal del 20 standarda ISO 15638 (TARV), ki se nanaša na WOB/OWS.“;

(j) v točki 5.6.1 se pododstavek a) odstavka DSC_68 nadomesti z naslednjim:

„(a) da bi bilo mogoče naročilo za dobavo VU in DSRC-VU, pa tudi različnih serij DSRC-VU, oddati različnim dobaviteljem, mora biti povezava med VU in DSRC-VU, ki ni del VU, v skladu z odprtimi standardi. Povezava med VU in DSRC-VU mora biti“;

(k) v točki 5.7.1 se odstavek DSC_77 nadomesti z naslednjim:

„DSC_77 Funkcija *VUSM podatke*, ki so že zaščiteni, posreduje *DSRC-VU*. *VUSM* preveri, da so bili podatki, ki so bili zapisani v *DSRC-VU*, zapisani pravilno. Zapis napak v prenosu podatkov od *VU* v pomnilnik *DSRC-VU* in poročanje o njih se zapisuje s tipom EventFaultType in nastavitvijo vrednosti enum na ‚0C'H ‚napaka pri komuniciranju z opremo za komunikacijo na daljavo' skupaj s časovnim žigom.“;

(40) Dodatek 15 se spremeni:

(a) prvi odstavek točke 2.2 se nadomesti z naslednjim:

„Razume se, da so tahografske kartice prve generacije interoperabilne z enotami v vozilu prve generacije v skladu s Prilogo IB k Uredbi (EGS) št. 3821/85 ter da so tahografske kartice druge generacije interoperabilne z enotami v vozilu druge generacije v skladu s Prilogo IC k tej uredbi. Poleg tega veljajo tudi spodnje zahteve.“;

(b) v točki 2.4.1 se odstavek MIG_11 spremeni:

(i) prva alinea se nadomesti z naslednjim:

„— nepodpisani EF ic in icc (neobvezno),“;

(ii) tretja alinea se nadomesti z naslednjim:

„— druge EF z aplikativnimi podatki (v DF tahografu), ki se zahtevajo v protokolu za prenos podatkov s kartice prve generacije. Ti podatki so v skladu z varnostnimi mehanizmi prve generacije zaščiteni z digitalnim podpisom.

Tak prenos ne vključuje EF z aplikativnimi podatki, prisotnih na vozniških karticah (in karticah servisnih delavnic) druge generacije (EF z aplikativnimi podatki znotraj DF tahografa druge generacije).“;

(c) v točki 2.4.3 se odstavka MIG_014 in MIG_015 nadomestita z naslednjim:

„MIG_014 Izven okvira kontrole voznikov s strani kontrolnih organov zunaj EU se iz enot v vozilu druge generacije podatki prenesejo ob uporabi varnostnih mehanizmov druge generacije in protokola za prenos podatkov, kot je določen v Dodatku 7 k tej prilogi.

MIG_015 Da se omogoči nadzor nad vozniki tudi nadzornim organom zunaj EU, je neobvezno lahko omogočen tudi prenos podatkov iz enot v vozilu druge generacije ob uporabi varnostnih mehanizmov prve generacije. Preneseni podatki so v tem primeru v enakem formatu kot podatki, preneseni iz enote v vozilu prve generacije. Ta funkcija se lahko izbere prek ukazov v meniju.“

PRILOGA II

Priloga II k Uredbi (EU) 2016/799 se spremeni:

(1) v poglavju I se odstavek b) točke 1 nadomesti z naslednjim:

„(b) homologacijske številke, ki ustreza številki certifikata o homologaciji za prototip zapisovalne naprave ali tahografskega vložka ali tahografske kartice in je nameščena v neposredni bližini tega pravokotnika.“;

(2) v poglavju III se točka 5 nadomesti z naslednjim:

„5. Predloženo v homologacijo dne .....“;

(3) v poglavju IV se točka 5 nadomesti z naslednjim:

„5. Predloženo v homologacijo dne .....“.