32002R1360

UREDBA KOMISIJE (EZ) br. 1360/2002

od 13. lipnja 2002.

o sedmoj prilagodbi tehničkom napretku Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u cestovnom prometu

(Tekst značajan za EGP)

KOMISIJA EUROPSKIH ZAJEDNICA,

uzimajući u obzir Ugovor o osnivanju Europske zajednice,

uzimajući u obzir Uredbu (EEZ) br. 3821/85 od 20. prosinca 1985. o tahografu u cestovnom prometu [1] kako je zadnje izmijenjena Uredbom (EZ) br. 2135/98 [2], a posebno njezine članke 17. i 18.,

budući da:

(1) Tehničke specifikacije iz Priloga I. točke (B) Uredbe (EEZ) br. 3821/85 trebalo bi prilagoditi tehničkom napretku obraćajući posebnu pozornost ukupnoj sigurnosti sustava i interoperabilnosti između tahografa i vozačkih kartica.

(2) Prilagodba opreme također zahtijeva prilagodbu Priloga II. Uredbi (EEZ) br. 3821/85 koji određuje oznake i potvrde o odobrenju.

(3) Odbor osnovan sukladno članku 18. Uredbe (EEZ) br. 3821/85 nije dao mišljenje u vezi mjera utvrđenih u prijedlogu, te je stoga Komisija podnijela Vijeću prijedlog u pogledu navedenih mjera.

(4) Istekom razdoblja utvrđenog u članku 18. stavku 5. točki (b) Uredbe (EEZ) br. 3821/85, Vijeće nije djelovalo, te je stoga na Komisiji donošenje tih mjera,

DONIJELA JE OVU UREDBU:

Članak 1.

Prilog Uredbi (EZ) br. 2135/98 zamjenjuje se Prilogom ovoj Uredbi.

Članak 2.

Prilog II. Uredbi (EEZ) br. 3821/85 mijenja se kako slijedi:

1. poglavlje I. točka 1. prvi podstavak mijenja se kako slijedi:
   — standardna oznaka Grčke „GR” zamjenjuje se s „23”,
   — standardna oznaka Irske „IRL” zamjenjuje se s „24”,
   — dodaje se standardna oznaka „12” za Austriju,
   — dodaje se standardna oznaka „17” za Finsku,
   — dodaje se standardna oznaka „5” za Švedsku.
2. Poglavlje I. točka 1. drugi podstavak mijenja se kako slijedi:
   — riječi „ili kartice tahografa” umeću se iza riječi „tahografski listić”.
3. Poglavlje I. točka 2. mijenja se kako slijedi:
   — riječi „na svakoj kartici tahografa” se umeću iza riječi „tahografski listić”.
4. U poglavlju II. sljedeće riječi se dodaju naslovu: „ZA PROIZVODE USKLAĐENE S PRILOGOM I.”.

[1] SL L 370, 31.12.1985., str. 8.
[2] SL L 274, 9.10.1998., str. 1.

5. Dodaje se sljedeće poglavlje III.:

„III. POTVRDA O ODOBRENJU ZA PROIZVODE USKLAĐENE S PRILOGOM I. B

Nakon davanja odobrenja, država tražitelju izdaje potvrdu o odobrenju čiji je obrazac predočen u nastavku. Pri izvješćivanju drugih država članica o izdanim ili moguće oduzetim odobrenjima, država članica mora koristiti preslike takve potvrde.

POTVRDA O ODOBRENJU ZA PROIZVODE USKLAĐENE S PRILOGOM I. B

Naziv nadležne uprave .....

Izvješće o ([3]):

☐ odobrenju

☐ oduzimanju odobrenja

☐ modelu tahografa

☐ sastavnom dijelu tahografa ([4]) .....

☐ kartici vozača

☐ kartici radionice

☐ kartici prijevoznika

☐ nadzornoj kartici

Odobrenje br. .....

1. Tvornička oznaka ili zaštitni znak .....
2. Naziv modela .....
3. Naziv proizvođača .....
4. Adresa proizvođača .....
5. Podnosi se na odobrenje za .....
6. Laboratorij(i) .....
7. Datum i broj provjere(a) .....
8. Datum odobrenja .....
9. Datum oduzimanja odobrenja .....
10. Model sastavnog dijela (sastavnih dijelova) tahografa s kojim dio namjerava koristiti .....
11. Mjesto .....
12. Datum .....
13. Priloženi opisni dokumenti .....

---

14. Napomene (uključujući i mjesto žigova prema potrebi)

.....

Potpis

([3]) Označiti odgovarajuće polje.

([4]) Navesti sastavni dio na koji se odnosi izvješće."

Članak 3.

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europskih zajednica*.

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

Sastavljeno u Bruxellesu 13. lipnja 2002.

Za Komisiju
Loyola DE PALACIO
Potpredsjednica

PRILOG

„PRILOG I. B

ZAHTJEVI U POGLEDU IZRADE, ISPITIVANJA, UGRADNJE I NADZORA

SADRŽAJ

I. DEFINICIJE

U ovom Prilogu:

(a) **‚aktivacija' znači:**

faza u kojoj tahograf dostiže punu radnu sposobnost i izvršava sve funkcije, uključujući i sigurnosne funkcije;

Za aktiviranje tahografa potrebna je kartica radionice i unos njenog PIN-a;

(b) **‚autentifikacija' znači:**

funkcija namijenjena utvrđivanju i provjeri identiteta osobe;

(c) **‚autentičnost' znači:**

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

(d) **‚ugrađeni test' (BIT) znači:**

provjera koja se provodi na zahtjev i koju aktivira operater ili vanjska oprema;

(e) **‚kalendarski dan' znači:**

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

(f) **‚kalibriranje' znači:**

ažuriranje ili potvrđivanje parametara vozila koji se čuvaju u podatkovnoj memoriji. Parametri vozila uključuju identifikaciju vozila (VIN, VRN i državu članicu u kojoj je vozilo registrirano) i značajke vozila (w, k, l, dimenzije guma, podešenje ograničivača brzine (ako se zahtijeva), trenutačno UTC vrijeme, trenutačno stanje na brojaču kilometara);

za kalibriranje tahografa potrebna je kartica radionice;

(g) **‚broj kartice' znači:**

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

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

(h) **‚indeks rednog broja kartice' znači:**

14. alfanumerički znak broja kartice koji se koristi za razlikovanje kartica izdanih tvrtki ili tijelu koje ima pravo na više kartica tahografa. Tvrtka ili tijelo se na jedinstven način identificira pomoću prvih 13 znakova broja kartice;

(i) **‚indeks obnavljanja kartice' znači:**

16. alfanumerički znak broja kartice koji se uvećava prilikom svakog obnavljanja kartice tahografa;

(j) **‚indeks zamjene kartice' znači:**

15. alfanumerički znak broja kartice koji se uvećava prilikom svake zamjene kartice tahografa;

(k) **‚karakteristični koeficijent vozila' znači:**

numerička vrijednost koja označuje karakteristiku izlaznog signala koja nastaje na priključnom mjestu vozila s tahografom (izlazno vratilo mjenjača ili pogonska osovina vozila) dok vozilo prelazi udaljenost od jednog kilometra pod standardnim ispitnim uvjetima (v. poglavlje VI. točku (5)). Karakteristični koeficijent izražava se u impulsima po kilometru (w = … imp/km);

(l) **‚kartica prijevoznika' znači:**

kartica tahografa koju tijela države članice izdaju vlasniku ili posjedniku vozila opremljenog tahografom;

kartica prijevoznika identificira tvrtku i omogućuje prikaz, preuzimanje i ispis podataka pohranjenih u tahografu koje je blokirala ta tvrtka;

(m) **‚konstanta tahografa' znači:**

numerička vrijednost koja označuje karakteristiku ulaznog signala potrebnog za prikaz i zapis prijeđene udaljenosti od jednog kilometra; konstanta se izražava u impulsima po kilometru (k = … imp/km);

(n) **‚neprekidno vrijeme vožnje' izračunava se u tahografu kao ([1]):**

neprekidno vrijeme vožnje se izračunava kao trenutačno akumulirano vrijeme vožnje određenog vozača od završetka posljednjeg razdoblja PRIPRAVNOSTI ili STANKE/ODMORA ili NEPOZNATO ([2]) u trajanju od najmanje 45 minuta (navedeno razdoblje može biti podijeljeno na nekoliko razdoblja od najmanje 15 minuta). Navedeni izračuni prema potrebi uzimaju u obzir i prethodne aktivnosti pohranjene na kartici vozača. Ako vozač nije umetnuo svoju karticu, izračun se temelji na zapisima iz podatkovne memorije koji se odnose na tekuće razdoblje u kojemu kartica nije bila umetnuta u odgovarajući utor za kartice (slot);

(o) **‚nadzorna kartica' znači:**

kartica tahografa koju tijela države članice izdaju domaćem nadležnom nadzornom tijelu;

nadzorna kartica identificira kontrolno tijelo i po mogućnosti službenika za kontrolu i omogućuje pristup podacima pohranjenim u podatkovnoj memoriji ili karticama vozača radi očitavanja, ispisa i/ili preuzimanja;

(p) **‚zbirno vrijeme stanke' izračunava se pomoću tahografa kao ([1]):**

zbirno vrijeme stanke od vremena vožnje se izračunava kao tekuće akumulirano vrijeme PRIPRAVNOSTI ili STANKE/ODMORA ili NEPOZNATO ([2]) u trajanju od najmanje 15 minuta za pojedinog vozača, od završetka posljednjeg razdoblja njegove PRIPRAVNOSTI ili STANKE/ODMORA ili NEPOZNATO ([2]) u trajanju od najmanje 45 minuta (to razdoblje može biti podijeljeno na nekoliko razdoblja od najmanje 15 minuta).

Navedeni izračun prema potrebi uzima u obzir prethodne aktivnosti pohranjene na vozačkoj kartici. Nepoznata razdoblja negativnog vremenskog izračuna (početak nepoznatog razdoblja je vremenski kasniji od završetka nepoznatog razdoblja) zbog vremenskih preklapanja između dva različita tahografa se ne uzimaju u obzir za izračun.

Ako vozač nije umetnuo svoju karticu, izračun se temelji na zapisima iz podatkovne memorije vezanim za tekuće razdoblje u kojemu kartica nije bila umetnuta u odgovarajući utor za kartice (slot);

(q) **‚podatkovna memorija' znači:**

elektronsko sredstvo za pohranjivanje podataka ugrađeno u tahografu;

(r) **‚digitalni potpis' znači:**

podaci stavljeni na blok podataka ili kriptografsku pretvorbu bloka podataka koja omogućuje primatelju bloka podataka dokazivanje autentičnosti i cjelovitosti bloka podataka;

(s) **‚preuzimanje podataka' znači:**

kopiranje zajedno s digitalnim potpisom dijela ili čitave skupine podataka pohranjenih u podatkovnoj memoriji vozila ili u memoriji kartice tahografa;

pri preuzimanju se pohranjeni podaci ne mogu mijenjani niti brisati;

([1]) Ovaj način izračuna neprekidnog vremena vožnje i ukupnog vremena pauze služi tahografu za izračun upozorenja o vremenu neprekidne vožnje. Isti ne dovodi u pitanje pravno tumačenje navedenih vremena.

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

(t) **‚kartica vozača' znači:**

kartica tahografa koju su izdala tijela države članice određenom vozaču;

kartica vozača identificira vozača i omogućava pohranjivanje podataka o aktivnosti vozača;

(u) **‚djelatni opseg pogonskih kotača' znači:**

prosjek udaljenosti koju prijeđe svaki od kotača koji pokreću vozilo (pogonski kotači) tijekom jednog potpunog okretaja. Mjerenje tih udaljenosti obavlja se pod standardnim ispitnim uvjetima (poglavlje VI. točka 5.) i izražava se u obliku ‚l = … mm'. Proizvođači vozila mogu nadomjestiti mjerenje takvih udaljenosti teoretskim izračunom koji uzima u obzir raspored opterećenja po osovinama za prazno vozilo i uobičajeno radno stanje ([1]). Metode takvog teoretskog izračuna odobrava nadležno tijelo države članice;

(v) **‚događaj' znači:**

nepravilan rad tahografa koji može biti posljedica pokušaja prijevare;

(w) **‚greška' znači:**

nepravilan rad ustanovljen od tahografa koji može biti posljedica nepravilnog rada ili kvara;

(x) **‚ugradnja' znači:**

postavljanje tahografa u vozilo;

(y) **‚senzor kretanja' znači:**

dio tahografa koji daje signal koji predstavlja brzinu kretanja vozila i/ili prijeđenu udaljenost;

(z) **‚nevažeća kartica' znači:**

kartica za koju je ustanovljeno da je neispravna ili čija početna autentifikacija nije uspjela ili čiji datum početka važenja još nije nastupio ili čiji je datum važenja istekao;

(aa) **‚izvan djelokruga' znači:**

kad tahograf nije potrebno koristiti u skladu s odredbama Uredbe Vijeća (EEZ) br. 3820/85;

(bb) **‚prekoračenje brzine' znači:**

prekoračenje dopuštene brzine vozila koja se utvrđuje u bilo kojem razdoblju duljem od 60 sekundi, tijekom kojega izmjerena brzina vozila prelazi graničnu brzinu podešenu ograničavačem brzine, a utvrđenu Direktivom Vijeća 92/6/EEZ od 10. veljače 1992. o ugradnji i uporabi uređaja za ograničenje brzine za određene kategorije motornih vozila u Zajednici ([2]);

(cc) **‚periodični pregled' znači:**

niz postupaka koji se provode radi provjere ispravnosti rada tahografa i usklađenosti podešenih vrijednosti s parametrima vozila;

(dd) **‚pisač' znači:**

sastavni dio tahografa koji daje ispis pohranjenih podataka;

(ee) **‚tahograf' znači:**

svu opremu namijenjenu ugradnji u cestovna vozila radi prikaza, bilježenja i automatskog ili poluautomatskog pohranjivanja podataka o kretanju takvih vozila i o određenim razdobljima aktivnosti njihovih vozača;

([1]) Direktiva 97/27/EZ od 22. srpnja 1997. o masama i dimenzijama određenih kategorija motornih vozila i njihovih prikolica i o izmjeni Direktive 70/156/EEZ (SL L 233, 25.8.1997., str. 1.).
([2]) SL L 57, 2.3.1992., str. 27.

(ff) **‚obnavljanje' znači:**

izdavanje nove kartice tahografa kada postojećoj kartici istekne valjanost ili kada postane neispravna pa je vraćena tijelu koje ju je izdalo. Obnavljanje uvijek podrazumijeva nedvojbenost da postoje dvije važeće kartice;

(gg) **‚popravak' znači:**

svaki popravak senzora kretanja ili jedinice u vozilu koji zahtijeva isključivanje njegovog napajanja ili isključivanje s drugih sastavnih dijelova tahografa ili njegovo otvaranje;

(hh) **‚zamjena' znači:**

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

(ii) **‚sigurnosna potvrda' znači:**

postupak koji je potvrdilo certifikacijsko tijelo ITSEC ([1]) da tahograf (ili njegov dio) ili kartica tahografa koja se ispituje zadovoljava sigurnosne zahtjeve utvrđene u Dodatku 10.: Generički sigurnosni ciljevi;

(jj) **‚samoprovjera' znači:**

ispitivanje koje tahograf provodi ciklički i automatski radi otkrivanja pogrešaka;

(kk) **‚kartica tahografa' znači:**

pametna kartica namijenjena korištenju uz tahograf. Kartica tahografa omogućuje tahografu prepoznavanje identiteta (ili skupine identiteta) nositelja kartice, te omogućuje prijenos i pohranjivanje podataka. Kartica tahografa može biti sljedećeg tipa:

— kartica vozača,

— nadzorna kartica,

— kartica radionice,

— kartica prijevoznika;

(ll) **‚tipno odobrenje' znači:**

postupak u kojem država članica potvrđuje da tahograf (ili njegov sastavni dio) ili kartica tahografa koja se ispituje zadovoljava zahtjeve ove Uredbe;

(mm) **‚dimenzije guma' znači:**

oznaka dimenzije guma (vanjskih pogonskih kotača) u skladu s Direktivom 92/23/EEZ od 31. ožujka 1992. ([2]);

(nn) **‚identifikacija vozila' znači:**

brojevi kojima se identificira vozilo: registracijski broj vozila (VRN) s oznakom države članice registracije i identifikacijski broj vozila (VIN) ([3]);

(oo) **‚jedinica u vozilu' (VU) znači:**

tahograf bez senzora kretanja i vodiča priključenih na senzor kretanja. Jedinica u vozilu može biti bilo jedna jedinica ili više jedinica raspoređenih u vozilu, ako udovoljava sigurnosnim zahtjevima iz ove Uredbe;

([1]) Preporuka Vijeća 95/144/EZ od 7. travnja 1995. o zajedničkim kriterijima procjene sigurnosti informatičke tehnologije (SL L 93, 26.4.1995., str. 27.).
([2]) SL L 129, 14.5.1992., str. 95.
([3]) Direktiva 76/114/EEZ od 18. prosinca 1975. o usklađivanju zakonodavstava država članica u odnosu na propisane pločice i natpise za motorna vozila i njihove prikolice te na njihov položaj i način pričvršćivanja (SL L 24, 30.1.1976., str. 1.).

(pp) **za potrebe izračunavanja u tahografu ‚tjedan' znači:**

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

(qq) **‚kartica radionice' znači:**

kartica tahografa koju su izdala tijela države članice proizvođaču tahografa, ugraditelju, proizvođaču vozila ili servisu koji je ovlastila takva država članica.

Servisna kartica identificira nositelja kartice i omogućava provjeru, kalibraciju i/ili preuzimanje podataka s tahografa.

II. OPĆA OBILJEŽJA I FUNKCIJE TAHOGRAFA

000 Svako vozilo opremljeno tahografom u skladu s odredbama ovog Priloga mora imati pokazivač brzine i brojač kilometara. Ove funkcije mogu biti ugrađene u tahograf.

1. **Opća obilježja**

Svrha tahografa je bilježenje, čuvanje, prikazivanje, ispis i davanje podataka o aktivnosti vozača.

001 Tahograf se sastoji od vodiča, senzora kretanja i jedinice u vozilu.

002 Jedinica u vozilu sastoji se od jedinice za obradu podataka, podatkovne memorije, sata za prikaz realnog vremena, sučelja za dvije pametne kartice (za vozača i suvozača), pisača, zaslona, vizualnog upozorenja, priključka za kalibraciju/preuzimanje podataka i uređaja za unos korisničkih ulaznih podataka.

Tahograf se može priključiti na druge uređaje pomoću dodatnih priključaka.

003 Svako odobreno ili bilo koje drugo priključivanje ili spajanje na tahograf, neke funkcije, jednog ili više uređaja, ne smije ometati ili imati mogućnost ometanja pravilnog i sigurnog rada tahografa i odredbi ove Uredbe.

Korisnici tahografa identificiraju se uz pomoć kartice tahografa.

004 Tahograf daje pravo selektivnog pristupa podacima i funkcijama u skladu s vrstom i/ili identitetom korisnika.

Tahograf bilježi i pohranjuje podatke u podatkovnu memoriju i na kartice tahografa.

To se odvija u skladu s Direktivom 95/46/EZ od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom prijenosu takvih podataka ([1]).

2. **Funkcije:**

005 Tahograf osigurava sljedeće funkcije:

— praćenje umetanja i vađenja kartice,

— mjerenje brzine i udaljenosti,

— mjerenje vremena,

— praćenje aktivnosti vozača,

— praćenje stanja vožnje,

— ručne unose vozača,

  — unos mjesta početka i/ili završetka dnevnog razdoblja rada,

  — ručni unos aktivnosti vozača,

  — unos posebnih uvjeta,

([1]) SL L 281, 23.11.1995., str. 31.

— upravljanje zaključavanjem podataka o tvrtki,

— praćenje aktivnosti nadzora,

— otkrivanje događaja i/ili pogrešaka,

— ugrađene provjere i samoprovjere,

— očitavanje iz podatkovne memorije,

— zapis i spremanje u podatkovnoj memoriji,

— očitavanje iz kartica tahografa,

— zapis i spremanje na karticama tahografa,

— prikaz,

— ispis,

— upozorenja,

— preuzimanje podataka na vanjske medije,

— izlaz podataka na dodatne vanjske uređaje,

— kalibracija,

— podešavanje vremena.

3. **Načini rada**

006 Tahograf mora ima četiri načina rada:

— radni način,

— nadzorni način,

— kalibracijski način,

— prijevoznički način.

007 Tahograf se prebacuje na sljedeći način rada u skladu s umetnutim valjanim karticama tahografa u kartično sučelje (utore):

Način rada		Utor vozača				
		Bez kartice	Kartica vozača	Nadzorna kartica	Kartica radionice	Kartica prijevoznika
Utor suvozača	Bez kartice	Radni	Radni	Nadzorni	Kalibracijski	Prijevozнички
	Kartica vozača	Radni	Radni	Nadzorni	Kalibracijski	Prijevozнички
	Nadzorna kartica	Nadzorni	Nadzorni	Nadzorni (*)	Radni	Radni
	Kartica radionice	Kalibracijski	Kalibracijski	Radni	Kalibracijski (*)	Radni
	Kartica prijevoznika	Prijevozнички	Prijevozнички	Radni	Radni	Prijevozнички (*)

008 (*) U ovim situacijama tahograf mora koristiti samo karticu tahografa umetnutu u utor vozača.

009 Tahograf zanemaruje umetnutu nevažeću karticu, osim prikaza, ispisa ili preuzimanja podataka s istekle kartice, što mora biti omogućeno.

010 Sve funkcije navedene pod II.2 moraju raditi u svim načinima rada, uz sljedeće iznimke:

— funkcija kalibracije je dostupna samo u kalibracijskom načinu rada,

— funkcija podešavanja vremena je ograničena kada nije u kalibracijskom načinu rada,

— funkcije ručnog unosa vozača su dostupne samo u radnom načinu i kalibracijskom načinu rada,

— upravljanje zaključavanjem podataka tvrtke je dostupno samo u prijevozničkom načinu rada,

— funkcija praćenje nadzornih aktivnosti radi samo u nadzornom načinu rada,

— funkcija preuzimanja podataka nije dostupna u radnom načinu (osim kako je predviđeno u Zahtjevu 150).

011 Tahograf može prenijeti sve podatke na zaslon, pisač ili vanjska sučelja uz sljedeće iznimke:

— u radnom načinu, sve osobne identifikacije (prezime i ime(na)) koji ne odgovaraju umetnutoj kartici tahografa ostaju nevidljivi, a svaki broj kartice koji ne odgovara umetnutoj kartici tahografa ostaju djelomično nevidljivi (nevidljiva je svaka neparna znamenka slijeva nadesno),

— u prijevozničkom načinu, podaci o vozaču (zahtjevi 081, 084 i 087) se mogu prenijeti samo za razdoblja koja nije zaključala neka druga tvrtka (koja je identificirana s prvih 13 znamenaka broja kartice prijevoznika),

— kad u tahograf nije umetnuta kartica, podaci o vozaču se mogu prenijeti samo za tekući i prethodnih osam kalendarskih dana.

4. **Sigurnost**

Sigurnost sustava ima za cilj zaštitu podatkovne memorije tako da spriječi neovlašten pristup i manipuliranje podacima i otkrivanje svakog takvog pokušaja, zaštitu cjelovitosti i autentičnosti podataka koji se razmjenjuju između senzora kretanja i jedinice u vozilu, zaštitu cjelovitosti i autentičnosti podataka koji se razmjenjuju između tahografa i kartica tahografa, te provjeru cjelovitosti i autentičnosti preuzetih podataka.

012 Kako bi se postigla sigurnost sustava, tahograf mora udovoljiti sigurnosnim zahtjevima navedenim u generičkim sigurnosnim ciljevima za senzor kretanja i jedinicu u vozilu (Dodatak 10.).

III. ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNI ZAHTJEVI ZA TAHOGRAFE

1. **Praćenje umetanja i vađenja kartica**

013 Tahograf mora nadgledati kartične utore tako da registrira umetanje i vađenje kartice.

014 Po umetanju kartice tahograf mora ustanoviti je li umetnuta kartica važeća kartica tahografa i u tom slučaju identificirati vrstu kartice.

015 Tahograf mora biti tako projektiran da se kartice tahografa zaključaju pri pravilnom umetanju u kartične utore.

016 Oslobađanje kartice tahografa može funkcionirati samo kada je vozilo zaustavljeno i nakon što su odgovarajući podaci spremljeni na kartice. Oslobađanje kartice zahtijeva aktivnost korisnika.

2. **Mjerenje brzine i udaljenosti**

017 Ova funkcija mora neprekidno mjeriti i biti u stanju dati stanje brojača kilometara koje odgovara ukupnoj udaljenosti koju je vozilo prešlo.

018 Ova funkcija mora neprekidno mjeriti i biti u stanju dati brzinu vozila.

019 Funkcija mjerenja brzine također daje informaciju kreće li se vozilo ili stoji. Smatra se da se vozilo kreće čim funkcija utvrdi više od 1 imp/sek u trajanju od najmanje pet sekundi na senzoru kretanja, u protivnom se smatra da vozilo stoji.

Uređaji za prikaz brzine (brzinomjer) i ukupno prijeđene udaljenosti (brojač kilometara) ugrađeni na svako vozilo opremljeno tahografom koji je sukladan odredbama ove Uredbe moraju udovoljavati zahtjevima u pogledu maksimalnih odstupanja utvrđenih u ovom Prilogu (poglavlje III. odjeljak 2. točka 1. i poglavlje III. odjeljak 2. točka 2.).

2.1. ***Mjerenje prijeđene udaljenosti***

020 Prijeđena udaljenost se može mjeriti:

— tako da se zbraja kretanje prema naprijed i prema natrag, ili

— tako da se računaju samo kretanja prema naprijed.

021 Tahograf mora mjeriti udaljenost od 0 do 9 999 999,9 km.

022 Izmjerena udaljenost mora biti u granicama sljedećih odstupanja (na najmanjoj udaljenosti od 1,000 m):

— ± 1 % prije ugradnje,

— ± 2 % pri ugradnji i periodičnom pregledu,

— ± 4 % pri korištenju.

023 Izmjerena udaljenost mora imati razlučivost jednaku ili veću od 0,1 km.

2.2. ***Mjerenje brzine***

024 Tahograf mora mjeriti brzinu od 0 do 220 km/h.

025 Kako bi se osigurala najveća tolerancija prikazane brzine od ± 6 km/h pri korištenju, a s obzirom na:

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

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

tahograf mora, kod brzina između 20 i 180 km/h i za karakteristične koeficijente vozila između 4,000 i 25,000 imp/km mjeriti brzinu uz toleranciju od ± 1 km/h (pri konstantnoj brzini).

Napomena: Razlučivost spremanja podataka ima dodatnu toleranciju od ± 0,5 km/h za brzinu koju sprema tahograf.

025a Brzina se mora mjeriti ispravno unutar uobičajenih tolerancija u roku od 2 sekunde od kraja promjene brzine kada se brzina mijenjala više od 2 m/s^2.

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

3. **Mjerenje vremena**

027 Funkcija mjerenja vremena mora trajno mjeriti i digitalno iskazivati UTC datum i vrijeme.

028 UTC datum i vrijeme se moraju koristiti za iskazivanje datuma u svim segmentima uređaja za bilježenje (zapisi, ispisi, razmjena podataka, prikaz, …).

029 Kako bi se prikazalo lokalno vrijeme, mora biti omogućeno mijenjanje pomaka prikazanog vremena u koracima od pola sata.

030 Odstupanje vremena može biti unutar vrijednosti od ± 2 sekunde po danu za uvjete tipnog odobrenja.

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

032 Na mjerenje vremena ne smije utjecati prekid vanjskog napajanja kraći od 12 mjeseci u uvjetima tipnog odobrenja.

4. **Praćenje aktivnosti vozača**

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

034 Aktivnosti vozača su VOŽNJA, RAD, PRIPRAVNOST ili PAUZA/ODMOR.

035 Vozač i/ili suvozač moraju imati mogućnost ručnog odabira između RADA, PRIPRAVNOSTI ili STANKE/ODMORA.

036 Kada se vozilo kreće, za vozača se automatski odabire VOŽNJA, a za suvozača se automatski odabire PRIPRAVNOST.

037 Kad se vozilo zaustavi, za vozača se automatski odabire RAD.

038 Pri prvoj automatskoj promjeni aktivnosti u RAD, u roku od 120 sekundi od zaustavljanja vozila, treba pretpostaviti da se dogodila nakon zaustavljanja vozila (čime je moguće poništiti promjenu aktivnosti u RAD).

039 Ova funkcija mora bilježiti podatke o promjenama aktivnosti u razlučivost od jedne minute.

040 Uzimajući u obzir kalendarsku minutu, ako je neka aktivnost VOŽNJE nastupila tijekom te minute, čitava minuta se smatra VOŽNJOM.

041 Uzimajući u obzir kalendarsku minutu, ako je neka aktivnost VOŽNJE nastupila tijekom netom protekle minute i minute koja neposredno slijedi, i ta cijela minuta se smatra VOŽNJOM.

042 Uzimajući u obzir kalendarsku minutu koja se ne smatra VOŽNJOM, sukladno prethodnim zahtjevima, cijela minuta se smatra istom vrstom aktivnosti kao i najdulja neprekidna aktivnost unutar minute (ili posljednja aktivnost od jednako dugih).

043 Ova funkcija također mora trajno pratiti neprekidno vrijeme vožnje i zbirno vrijeme pauze vozača.

5. **Praćenje stanja vožnje**

044 Ova funkcija mora neprekidno i automatski pratiti stanje vožnje.

045 Stanje vožnje POSADA se odabire kada se dvije valjane vozačke kartice umetnu u tahograf, a u svim drugim slučajevima se odabire stanje vožnje JEDAN VOZAČ.

6. **Ručni unos od strane vozača**

6.1. ***Unos mjesta početka i/ili kraja dnevnog razdoblja rada***

046 Ova funkcija omogućava unos mjesta početka i/ili završetka dnevnog razdoblja rada vozača i/ili suvozača.

047 Mjesta se definiraju kao država, te dodatno prema potrebi, kao regija.

048 U vrijeme vađenja kartice vozača (ili kartice radionice) tahograf mora potaknuti (su)vozača da unese ‚mjesto završetka dnevnog razdoblja rada'.

049 Tahograf mora omogućiti zanemarivanje ovog zahtjeva.

050 Mora postojati mogućnost unosa mjesta početka i/ili kraja dnevnog razdoblja rada bez kartice ili u vremena različitog od vremena umetanja ili vađenja.

6.2. ***Ručni unos aktivnosti vozača***

050a Nakon umetanja kartice vozača (ili kartice radionice) i samo tada, tahograf će:

— podsjetiti nositelja kartice o datumu i vremenu posljednjeg vađenja kartice, i

— zatražiti od nositelja kartice da naznači predstavlja li trenutačno umetanje kartice nastavak tekućeg razdoblja dnevnog rada.

Tahograf omogućuje nositelju kartice da pitanje zanemari bez davanja odgovora, ili da na pitanje odgovori pozitivno ili negativno:

— u slučaju kada nositelj kartice zanemari pitanje, tahograf ga upozorava na ‚mjesto početka dnevnog razdoblja rada'. Tahograf omogućuje da se ovo pitanje zanemari. Ako se mjesto unese, ono se bilježi u podatkovnoj memoriji i na kartici tahografa i odnosi se na vrijeme umetanja kartice,

— u slučaju negativnog ili pozitivnog odgovora, tahograf poziva nositelja kartice da ručno unese aktivnosti, uz datum i vrijeme njihovog početka i završetka, izabirući samo između aktivnosti RADA, PRIPRAVNOSTI ili PAUZE/ODMORA, strogo obuhvaćenih samo u razdoblju između posljednjeg vađenja kartice i trenutačnog umetanja kartice i ne dopuštajući da se navedene aktivnosti međusobno preklope. Ovo se vrši na sljedeći način:

  — u slučaju da nositelj kartice na pitanje odgovori pozitivno, tahograf poziva nositelja kartice da aktivnosti unese ručno kronološkim redom za razdoblje od posljednjeg vađenja kartice do tekućeg umetanja kartice. Postupak završava kad se vrijeme završetka ručno unesene aktivnosti izjednači s vremenom umetanja kartice.

  — u slučaju kada nositelj kartice na pitanje odgovori negativno, tahograf:

    — poziva nositelja kartice da aktivnosti unese ručno kronološkim redom od vremena vađenja kartice do vremena završetka dotičnog dnevnog razdoblja rada (ili aktivnosti vezanih uz predmetno vozilo u slučaju kada se dnevno razdoblje nastavlja na tahografskom listiću). Prije nego što nositelju kartice omogući ručno unošenje svake aktivnosti tahograf će pozvati nositelja kartice da naznači predstavlja li vrijeme završetka posljednje zabilježene aktivnosti kraj prethodnog razdoblja rada (vidjeti napomenu u nastavku),

    Napomene: u slučaju kada nositelj kartice ne naznači kada je završilo prethodno razdoblje rada i ručno unese aktivnost čije je vrijeme završetka jednako vremenu umetanja kartice, tahograf:

      — pretpostavlja da je dnevno razdoblje rada završilo početkom prvog ODMORA (ili ostaje NEPOZNATO) nakon vađenja kartice ili u trenutku vađenja kartice, ako nije bilo uneseno vrijeme odmora (i ako niti jedno razdoblje nije NEPOZNATO),

      — pretpostavlja da je vrijeme početka (vidjeti dolje) jednako vremenu umetanja kartice,

      — postupiti na niže opisani način;

    — potom, ako je vrijeme završetka dotičnog razdoblja rada različito od vremena vađenja kartice, ili ako mjesto završetka dnevnog razdoblja rada nije u to vrijeme bilo uneseno, poziva nositelja kartice da ‚potvrdi ili unese mjesto završetka dnevnog razdoblja rada' (tahograf omogućuje zanemarivanje ovog zahtjeva). Ako se mjesto unese ono se bilježi samo na kartici tahografa i to samo ako je različito od onoga koje je uneseno pri vađenju kartice (ako je uneseno), i ako se odnosi na vrijeme završetka razdoblja rada,

    — potom poziva nositelja kartice da unese ‚vrijeme početka' tekućeg dnevnog razdoblja rada (ili aktivnosti vezanih uz trenutačno vozilo u slučaju da je nositelj kartice prethodno tijekom istog razdoblja koristio tahografski listić), te nositelja kartice upozorava da unese ‚mjesto početka dnevnog razdoblja rada' (tahograf omogućuje zanemarivanje ovog zahtjeva). Ako se mjesto unese, ono se bilježi samo na kartici tahografa i odnosi se na navedeno vrijeme početka. Ako je to vrijeme početka jednako vremenu umetanja kartice, mjesto se također bilježi u podatkovnoj memoriji,

    — potom, ako je vrijeme početka različito od vremena umetanja kartice, poziva nositelja kartice da ručno unese aktivnosti kronološkim redom od takvog vremena početka do vremena umetanja kartice. Postupak završava kada je vrijeme završetka ručno unesene aktivnosti jednako vremenu umetanja kartice,

  — tahograf potom omogućuje nositelju kartice izmjenu svake ručno unesene aktivnosti, do potvrđivanja odabirom posebne naredbe, a nakon toga zabranjuje svaku izmjenu,

  — takve odgovore na početno pitanje, nakon kojih nema unosa aktivnosti, tahograf tumači kao da je nositelj kartice zanemario pitanje.

Tijekom čitavog postupka unosa podataka tahograf čeka na unos ne dulje od sljedećih prekida:

— ako nema nikakve interakcije s ljudskim sučeljem tahografa tijekom jedne minute (uz vizualno i po mogućnosti zvučno upozorenje nakon 30 sekundi), ili

— ako se kartica izvadi i umetne druga kartica vozača (ili kartica radionice), ili

— dokle god se vozilo ne pokrene,

u ovom slučaju tahograf potvrđuje sve već izvršene unose.

6.3. ***Unos posebnih stanja***

050b Tahograf omogućuje vozaču unos, u realnom vremenu, sljedeća dva posebna stanja:

— ‚IZVAN DJELOKRUGA' (početak, kraj)

— ‚VOŽNJA TRAJEKTOM/VLAKOM'

‚VOŽNJA TRAJEKTOM/VLAKOM' ne može nastati ako je stanje ‚IZVAN DJELOKRUGA' aktivno.

Započeto stanje ‚IZVAN DJELOKRUGA' tahograf mora automatski zatvoriti ako se kartica vozača umeće ili vadi.

7. **Upravljanje blokadom tvrtke**

051 Ova funkcija omogućuje upravljanje blokadama koje postavi tvrtka kako bi ograničila pristup podacima tvrtke za sebe.

052 Blokade tvrtke se sastoje od datuma/vremena početka (postavljanje blokade) i datuma/vremena završetka (skidanje blokade) pridruženih identifikaciji tvrtke naznačenoj u broju kartice tvrtke (pri postavljanju blokade).

053 Blokade se mogu postaviti odnosno skinuti samo u realnom vremenu.

054 Skidanje blokade može izvršiti samo tvrtka čija je blokada postavljena (što određuje prvih 13 znamenki broja kartice tvrtke) ili,

055 Skidanje blokade je automatsko kada druga tvrtka izvrši postavljanje blokade.

055a U slučaju postavljanja blokade od strane tvrtke kada je prethodna blokada bila za istu tvrtku, pretpostavlja se da prethodna blokada nije bila skinuta, te da je i dalje postavljena.

8. **Praćenje nadzornih aktivnosti**

056 Ova funkcija prati aktivnosti PRIKAZA, ISPISA i PREUZIMANJA podataka iz tahografa i kartice dok je u načinu nadzora.

057 Ova funkcija također prati aktivnosti KONTROLE PREKORAČENJA BRZINE dok je u načinu nadzora. Smatra se da je kontrola prekoračenja brzine nastala ako je u načinu nadzora ispis ‚prekoračenja brzine' poslan na pisač ili na zaslon ili ako su podaci o ‚događajima i pogreškama' preuzeti iz podatkovne memorije tahografa.

9. **Prepoznavanje događaja i/ili pogrešaka**

058 Ova funkcija otkriva sljedeće događaje i/ili pogreške:

9.1. ***Događaj ‚umetanje nevažeće kartice'***

059 Ovaj događaj se aktivira umetanjem bilo koje nevažeće kartice i/ili ako istekne valjanost umetnute važeće kartice.

9.2. ***Događaj ‚sukob kartica'***

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

Sukob kartica		Utor vozača				
		Bez kartice	Kartica vozača	Nadzorna kartica	Kartica radionice	Kartica prijevoznika
Utor suvozača	Bez kartice					
	Kartica vozača				X	
	Nadzorna kartica			X	X	X
	Kartica radionice		X	X	X	X
	Kartica prijevoznika			X	X	X

9.3. ***Događaj ‚vremensko preklapanje'***

061 Ovaj slučaj se aktivira kada su datum/vrijeme posljednjeg vađenja vozačke kartice, očitani s kartice, kasniji nego tekući datum/vrijeme tahografa u koji je umetnuta kartica.

9.4 ***Događaj ‚vožnja bez odgovarajuće kartice'***

062 Ovaj događaj se aktivira za bilo koju kombinaciju kartica tahografa označenu s X u sljedećoj tablici ako se aktivnost vozača promijeni na VOŽNJU ili ako dođe do promjene načina rada kada je aktivnost vozača VOŽNJA:

Vožnja bez odgovarajuće kartice		Utor vozača				
		Bez kartice (ili nevažeća kartica)	Kartica vozača	Nadzorna kartica	Kartica radionice	Kartica prijevoznika
Utor suvozača	Bez kartice (ili nevažeća kartica)	X		X		X
	Kartica vozača	X		X	X	X
	Nadzorna kartica	X	X	X	X	X
	Kartica radionice	X	X	X		X
	Kartica prijevoznika	X	X	X	X	X

9.5. ***Događaj ‚umetanje kartice tijekom vožnje'***

063 Ovaj događaj se aktivira ako se kartica tahografa umetne u bilo koji utor u vrijeme dok je aktivnost vozača VOŽNJA.

9.6. ***Događaj ‚neispravno zatvaranje posljednje razmjene podataka s karticom'***

064 Ovaj događaj se aktivira kada pri umetanju kartice tahograf utvrdi da unatoč odredbama utvrđenim u stavku III. točki 1. prethodna razmjena podataka s karticom nije pravilno završena (kartica je izvađena prije nego su svi potrebni podaci spremljeni na karticu). Ovaj događaj se aktivira samo s karticom vozača i karticom radionice.

9.7. ***Događaj ‚prekoračenje brzine'***

065 Ovaj događaj se aktivira pri svakom prekoračenju brzine.

9.8. ***Događaj ‚prekid napajanja'***

066 Ovaj događaj se aktivira izvan kalibracije pri svakom prekidu napajanja senzora kretanja i/ili jedinice u vozilu duljeg od 200 milisekundi. Prag prekida utvrđuje proizvođač. Pad napajanja zbog pokretanja motora vozila ne aktivira ovaj događaj.

9.9. ***Događaj ‚pogreška podataka kretanja'***

067 Ovaj događaj se aktivira u slučaju prekida redovnog protoka podataka između senzora kretanja i jedinice u vozilu i/ili u slučaju pogreške cjelovitosti podataka ili pogreške autentifikacije podataka tijekom razmjene podataka između senzora kretanja i jedinice u vozilu.

9.10. ***Događaj ‚pokušaj probijanja zaštite'***

068 Ovaj događaj se aktivira za sve ostale događaje koji utječu na sigurnost senzora kretanja i/ili jedinice u vozilu kako je navedeno u generičkim sigurnosnim ciljevima za takve sastavne dijelove dok nisu u načinu kalibracije.

9.11. ***Pogreška ‚kartica'***

069 Ova pogreška se aktivira ako se tijekom rada javi pogreška na kartici tahografa.

9.12. ***Pogreška ‚tahograf'***

070 Ova pogreška se aktivira za neku od sljedećih pogrešaka, dok nije u načinu kalibracije:

— interna pogreška jedinice u vozilu,

— pogreška pisača,

— pogreška zaslona,

— pogreška pri preuzimanju podataka,

— pogreška senzora.

10. **Postupak provjere i samoprovjere**

071 Tahograf sam otkriva pogreške samoprovjerom i provjerama prema sljedećoj tablici:

Podsustav koji se provjerava	Samoprovjera	Provjera
Program		Cjelovitost
Podatkovna memorija	Pristup	Pristup, cjelovitost podataka
Uređaji kartičnog sučelja	Pristup	Pristup
Tipkovnica		Ručna provjera
Pisač	(ovisi o proizvođaču)	Ispis
Zaslon		Vizualna provjera
Preuzimanje podataka (vrši se samo tijekom preuzimanja podataka)	Pravilan rad	
Senzor	Pravilan rad	Pravilan rad

11. **Očitavanje podataka iz memorije**

072 Tahograf mora biti u stanju očitati sve podatke pohranjene u njegovoj podatkovnoj memoriji.

12. **Zapis i spremanje u podatkovnoj memoriji**

Za potrebe ovog stavka:

— ‚365 dana' se definira kao 365 kalendarskih dana prosječne aktivnosti vozača u vozilu. Prosječna dnevna aktivnost u vozilu definira se kao najmanje šest vozača ili suvozača, šest ciklusa umetanja i vađenja kartice i 256 promjena aktivnosti. Tako ‚365 dana' uključuje najmanje 2,190 (su)vozača, 2,190 ciklusa umetanja i vađenja kartice i 93,440 promjene aktivnosti,

— vremena se bilježe s razlučivošću od jedne minute, osim ako nije drukčije propisano,

— stanje brojača kilometara se bilježi s razlučivošću od jednog kilometra,

— brzine se bilježe s razlučivošću od 1 km/h.

073 Na podatke pohranjene u podatkovnoj memoriji ne smije utjecati nikakav vanjski prekid napajanja kraći od dvanaest mjeseci u tipno odobrenim uvjetima.

074 Tahograf mora moći zapisivati i spremati izravno ili neizravno sljedeće podatke u svojoj podatkovnoj memoriji:

12.1. ***Identifikacijski podaci o uređaju***

12.1.1. *Identifikacijski podaci jedinice u vozilu*

075 Tahograf mora moći spremiti sljedeće identifikacijske podatke jedinice u vozilu u svojoj podatkovnoj memoriji:

— naziv proizvođača,

— adresa proizvođača,

— broj dijela,

— serijski broj,

— broj verzije programa,

— datum ugradnje verzije programa,

— godina proizvodnje uređaja,

— broj tipnog odobrenja.

076 Identifikacijske podatke jedinice u vozilu bilježi i pohranjuje jednom zauvijek proizvođač jedinice u vozilu, osim podataka vezanih uz program i broja tipnog odobrenja koji se mogu mijenjati kod ažuriranja programa.

12.1.2. *Identifikacijski podaci senzora kretanja*

077 Senzor kretanja mora biti u stanju čuvati u svojoj memoriji sljedeće identifikacijske podatke:

— naziv proizvođača,

— broj dijela,

— serijski broj,

— broj tipnog odobrenja,

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

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

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

079 Jedinica u vozilu mora biti u stanju čuvati u svojoj podatkovnoj memoriji sljedeće identifikacijske podatke senzora kretanja s kojim je trenutačno uparena:

— serijski broj,

— broj tipnog odobrenja,

— datum prvog uparivanja.

12.2. ***Sigurnosni elementi***

080 Tahograf mora biti u stanju pohraniti sljedeće sigurnosne elemente:

— europski javni ključ,

— certifikat države članice,

— certifikat tahografa,

— privatni ključ tahografa.

Proizvođač jedinice u vozilu ugrađuje u tahograf sigurnosne elemente.

12.3. ***Podaci o umetanju i vađenju kartice vozača***

081 Za svaki ciklus umetanja i vađenja kartice vozača ili kartice radionice u/iz uređaja, tahograf mora zabilježiti i pohraniti u svoju podatkovnu memoriju:

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

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

— datum i vrijeme umetanja,

— stanje brojača kilometara vozila pri umetanju kartice,

— utor u koji je kartica umetnuta,

— datum i vrijeme vađenja,

— stanje brojača kilometara vozila pri vađenju kartice,

— sljedeće informacije pohranjene na kartici o prethodnom vozilu koje je vozač koristio:

  — registracijski broj vozila i državu članicu u kojoj je vozilo registrirano,

  — datum i vrijeme vađenja kartice,

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

082 Podatkovna memorija mora biti u stanju čuvati te podatke najmanje 365 dana.

083 Kad se iscrpi kapacitet memorije za spremanje, novi podaci zamjenjuju najstarije podatke.

12.4. ***Podaci o aktivnosti vozača***

084 Tahograf zapisuje i sprema u svoju podatkovnu memoriju svaku promjenu aktivnosti vozača i/ili suvozača i/ili svaku promjenu stanja vožnje i/ili svako umetanje ili vađenje kartice vozača ili kartice radionice:

— stanje vožnje (POSADA, JEDAN VOZAČ),

— utor (VOZAČ, SUVOZAČ),

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

— aktivnost (VOŽNJA, PRIPRAVNOST, RAD, PAUZA/ODMOR),

— datum i vrijeme promjene.

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

Napomena: podaci o aktivnosti koje ručno unosi vozač se ne bilježe u podatkovnoj memoriji.

085 Podatkovna memorija mora biti u stanju čuvati podatke o aktivnosti vozača najmanje 365 dana.

086 Kada se iscrpi kapacitet memorije za pohranu, novi podaci zamjenjuju najstarije podatke.

12.5. ***Mjesta početka i/ili završetka dnevnog razdoblja rada***

087 Tahograf bilježi i pohranjuje u svoju podatkovnu memoriju svaki unos mjesta početka i/ili završetka dnevnog razdoblja rada od strane (su)vozača:

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

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

— vrsta unosa (početak ili završetak, stanje unosa),

— državu i regiju u koju se ulazi,

— stanje brojača kilometara vozila.

088 Podatkovna memorija mora biti u stanju čuvati podatke o početku i/ili završetku dnevnog razdoblja rada najmanje 365 dana (uz pretpostavku da jedan vozač izvrši dva unosa dnevno).

089 Kada se iscrpi kapacitet memorije za spremanje, novi podaci zamjenjuju najstarije podatke.

12.6. ***Stanje brojača prijeđenih kilometara***

090 Tahograf zapisuje i sprema u svoju podatkovnu memoriju stanje brojača prijeđenih kilometara i pripadajući datum u ponoć svakog kalendarskog dana.

091 Podatkovna memorija može biti u stanju pohranjivati ponoćna stanja brojača kilometara najmanje 365 kalendarskih dana.

092 Kada se iscrpi kapacitet memorije za spremanje, novi podaci zamjenjuju najstarije podatke.

12.7. ***Detaljni podaci o brzini***

093 Tahograf zapisuje i sprema u podatkovnu memoriju trenutačnu brzinu vozila i pripadajući datum i vrijeme u svakoj sekundi tijekom najmanje posljednja 24 sata kretanja vozila.

12.8. ***Podaci o događanjima***

Za potrebe ovog podstavka, vrijeme se bilježi s razlučivošću od jedne sekunde.

094 Za svaki otkriveni događaj, tahograf zapisuje i sprema u svoju podatkovnu memoriju sljedeće podatke prema sljedećim pravilima spremanja:

Događaj	Pravila spremanja	Podaci koji se zapisuju za svaki događaj
Sukob kartica	— 10 posljednjih događaja	— datum i vrijeme početka događaja, — datum i vrijeme kraja događaja, — vrsta kartica, broj i država članica izdavatelj dviju sukobljenih kartica.
Vožnja bez odgovarajuće kartice	— najdulji događaj od svih događaja u posljednjih 10 dana nastanka, — pet najduljih događaja tijekom posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme kraja događaja, — vrsta kartice, broj i država članica izdavatelj bilo koje kartice umetnute na početku i/ili kraju događaja, — broj sličnih događaja tog dana.
Umetanje kartice tijekom vožnje	— posljednji događaj od svih događaja u posljednjih 10 dana nastanka.	— datum i vrijeme događaja, — vrsta kartice, broj i država članica izdavanja, — broj sličnih događaja tog dana.
Posljednje razdoblje razmjene podataka s karticom nije pravilno završeno	— 10 posljednjih događaja	— datum i vrijeme umetanja kartice, — vrsta kartice, broj i država članica izdavatelj, — podaci o posljednjem razdoblju razmjene podataka očitani s kartice: — datum i vrijeme umetanja kartice, — registracijski broj vozila i država članica registracije.
Prekoračenje brzine [1]	— najteži događaj od svih događaja u posljednjih 10 dana nastanka (tj. onaj s najvećom prosječnom brzinom), — pet najtežih događaja tijekom posljednjih 365 dana, — prvi slučaj koji se desio nakon posljednje kalibracije.	— datum i vrijeme početka događaja, — datum i vrijeme kraja događaja, — maksimalna brzina izmjerena tijekom događaja, — aritmetička prosječna brzina izmjerena tijekom događaja, — vrsta kartice, broj i država članica izdavatelj kartice vozača (prema potrebi), — broj sličnih događaja tog dana.

Događaj	Pravila spremanja	Podaci koji se zapisuju za svaki događaj
Prekid napajanja ([2])	— najdulji događaj od svih događaja u posljednjih 10 dana nastanka, — pet najduljih događaja tijekom posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme kraja događaja, — vrsta kartica, broj i država članica izdavatelj bilo koje kartice umetnute na početku i/ili kraju događaja, — broj sličnih događaja tog dana.
Pogreška u podacima o kretanju	— najdulji događaj od svih događaja u posljednjih 10 dana nastanka, — pet najduljih događaja tijekom posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme kraja događaja, — vrsta kartica, broj i država članica izdavatelj bilo koje kartice umetnute na početku i/ili kraju događaja, — broj sličnih događaja tog dana.
Pokušaj probijanja zaštite	— 10 posljednjih događaja po vrsti događaja	— datum i vrijeme početka događaja, — datum i vrijeme kraja događaja (ako je bitno), — vrsta kartica, broj i država članica izdavatelj bilo koje kartice umetnute na početku i/ili kraju događaja, — broj sličnih događaja tog dana.

095 ([1]) Tahograf također zapisuje i sprema u svoju podatkovnu memoriju:
— datum i vrijeme posljednje KONTROLE PREKORAČENJA BRZINE,
— datum i vrijeme prvog prekoračenja brzine nakon navedene KONTROLE PREKORAČENJA BRZINE,
— broj događanja prekoračenja brzine od posljednje KONTROLE PREKORAČENJA BRZINE.
([2]) Ovi podaci se mogu bilježiti samo po ponovnom priključenju na napajanje, vremena mogu biti poznata s točnošću do minute.

12.9. ***Podaci o pogreškama***

U smislu ovog podstavka, vrijeme se bilježi s razlučivošću od jedne sekunde.

096 Za svaku otkrivenu pogrešku tahograf mora pokušati zapisati i spremiti u svoju podatkovnu memoriju sljedeće podatke prema sljedećim pravilima spremanja:

Događaj	Pravila spremanja	Podaci koji se zapisuju za događaj
Pogreška kartice	— 10 posljednjih pogrešaka kartice vozača	— datum i vrijeme početka pogreške, — datum i vrijeme završetka pogreške, — vrsta kartice, broj i država članica izdavatelj.
Pogreška tahografa	— 10 posljednjih pogrešaka za svaku vrstu pogreške, — prva pogreška nakon posljednje kalibracije.	— datum i vrijeme početka pogreške, — datum i vrijeme završetka pogreške, — vrsta pogreške, — vrsta kartice, broj i država članica izdavatelj bilo koje kartice koja je umetnuta na početku i/ili kraju pogreške.

12.10. ***Podaci o kalibraciji***

097 Tahograf zapisuje i sprema u svojoj podatkovnoj memoriji podatke od važnosti za:

— poznate parametre kalibracije u trenutku aktivacije,

— njegovu prvu kalibraciju nakon aktivacije,

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

— pet posljednjih kalibracija (ako je tijekom jednog kalendarskog dana izvršeno više kalibracija, sprema se samo posljednja izvršena tog dana).

098 Za svaku od spomenutih kalibracija se bilježe sljedeći podaci:

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

— naziv i adresa radionice,

— broj kartice radionice, država članica izdavanja kartice i datum isteka valjanosti kartice,

— identifikacija vozila,

— ažurirani ili potvrđeni parametri: w, k, l, dimenzije guma, podešenost ograničavača brzine, brojač kilometara (stare i nove vrijednosti), datum i vrijeme (stare i nove vrijednosti).

099 Senzor kretanja zapisuje i sprema u svoju memoriju sljedeće podatke o ugradnji senzora kretanja:

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

— posljednje uparivanje s jedinicom u vozilu (datum, vrijeme, broj tipnog odobrenja jedince u vozilu, serijski broj jedince u vozilu).

12.11. ***Podaci o podešavanju vremena***

100 Tahograf zapisuje i sprema u svojoj podatkovnoj memoriji podatke od važnosti za:

— posljednje podešavanje vremena,

— pet podešavanja vremena najvećih razmjera nakon posljednje kalibracije,

obavljenih u načinu kalibracije izvan redovne kalibracije (definicija (f)).

101 Za svako od tih podešavanja vremena bilježe se sljedeći podaci:

— datum i vrijeme, stara vrijednost,

— datum i vrijeme, nova vrijednost,

— naziv i adresa radionice,

— broj kartice radionice, država članica izdavanja kartice i datum isteka valjanosti kartice.

12.12. ***Podaci o nadzornim aktivnostima***

102 Tahograf zapisuje i sprema u svoju memoriju sljedeće podatke od važnosti za 20 posljednjih nadzornih aktivnosti:

— datum i vrijeme nadzora,

— broj nadzorne kartice i državu članicu izdavatelja kartice,

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

103 U slučaju preuzimanja podataka, bilježe se također datumi prvog i posljednjeg dana za koje se preuzimaju podaci.

12.13. ***Podaci o zaključavanju podataka tvrtke***

104 Tahograf zapisuje i sprema u svoju memoriju sljedeće podatke od važnosti za 20 posljednjih zaključavanja podataka tvrtke:

— datum i vrijeme zaključavanja,

— datum i vrijeme otključavanja,

— broj kartice prijevoznika i država članica izdavanja kartice,

— naziv i adresa prijevoznika.

12.14. ***Podaci o aktivnostima preuzimanja podataka***

105 Tahograf zapisuje i sprema u svojoj podatkovnoj memoriji sljedeće podatke od važnosti za posljednje preuzimanje podataka iz podatkovne memorije na vanjske medije u načinu rada prijevoznika ili kalibracije:

— datum i vrijeme preuzimanja podataka,

— broj kartice prijevoznika ili kartice radionice i država članica izdavatelja kartice,

— naziv prijevoznika ili radionice.

12.15. ***Podaci o posebnim uvjetima***

105a Tahograf zapisuje u svoju podatkovnu memoriju sljedeće podatke od važnosti za posebna stanja:

— datum i vrijeme unosa,

— vrsta posebnog stanja.

105b Podatkovna memorija mora biti u stanju čuvati podatke o posebnim uvjetima najmanje 365 dana (uz pretpostavku da se dnevno u prosjeku otvara i zatvara jedno stanje). Kada se iscrpi kapacitet za spremanje, novi podaci zamjenjuju najstarije podatke.

13. **Očitavanje kartica tahografa**

106 Tahograf mora biti u stanju očitavati s kartica tahografa, ako je primjereno, sljedeće potrebne podatke:

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

— provjeriti je li posljednje razdoblje rada s karticom pravilno završeno,

— izračunati neprekidno vrijeme vožnje vozača, zbirno vrijeme pauze i zbirno vrijeme vožnje za prethodni i tekući tjedan,

— izraditi ispise prema podacima zapisanim na kartici vozača,

— preuzeti podatke s kartice vozača na vanjske medije.

107 U slučaju pogreške pri očitavanju, tahograf mora ponovo pokušati, najviše tri puta, istu naredbu očitavanja, te će tada, ako je očitavanje ponovno bilo neuspješno, karticu proglasiti neispravnom i nevažećom.

14. **Zapisivanje i spremanje podataka na tahografske kartice**

108 Tahograf postavlja ‚podatke o razmjeni podataka s karticom' u karticu vozača ili karticu radionice odmah nakon umetanja kartice.

109 Tahograf ažurira podatke pohranjene na valjanoj kartici vozača, radionice i/ili nadzornoj kartici sa svim podacima koji su bitni za razdoblje u kojem je kartica umetnuta i koji se odnose na nositelja kartice. Podaci pohranjeni na tim karticama navedeni su u poglavlju IV.

109a Tahograf ažurira podatke o aktivnosti vozača i lokaciji (kako je navedeno u poglavlju IV, stavcima 5.2.5. i 5.2.6.) pohranjene na valjanim karticama vozača i/ili karticama radionice s podacima o aktivnosti i lokaciji koje je nositelj kartice unio ručno.

110 Ažuriranje kartica tahografa mora biti takvo da, prema potrebi i uzimajući u obzir stvarni kapacitet za spremanje, najnoviji podaci zamjenjuju najstarije.

111 U slučaju pogreške zapisa, tahograf mora pokušati ponovno, najviše tri puta, izvršiti istu naredbu zapisivanja, te će ako je i dalje neuspješna, proglasiti karticu neispravnom i nevažećom.

112 Prije oslobađanja vozačke kartice, a nakon što su svi potrebni podaci spremljeni na karticu, tahograf će poništiti podatke iz razdoblja rada s tom karticom.

15. **Prikaz**

113 Zaslon mora imati najmanje 20 znakova.

114 Minimalna veličina znaka je 5 mm u visinu i 3,5 mm u širinu.

114a Zaslon podržava skupine slovnih znakova latinski 1 i grčki utvrđene normom ISO 8859, dijelovi 1 i 7, kako je navedeno u poglavlju 4. Dodatka 1. ‚Skupine slovnih znakova'. Zaslon može koristiti pojednostavnjene znakove (npr. slovni znakovi s naglaskom se mogu prikazivati bez naglaska ili se mala slova mogu prikazivati kao velika slova).

115 Zaslon mora imati odgovarajuće neblješteće osvjetljenje.

116 Oznake moraju biti vidljive s vanjske strane tahografa.

117 Tahograf mora biti u stanju prikazati:

— standardne podatke,

— podatke upozorenja,

— podatke o pristupu izbornicima,

— ostale podatke koje korisnik zatraži.

Tahograf može prikazati dodatne informacije ako ih je moguće jasno razlikovati od gore navedenih podataka.

118 Zaslon tahografa koristi piktograme ili kombinacije piktograma navedene u Dodatku 3. Na zaslonu se mogu također prikazati dodatni piktogrami ili kombinacije piktograma, ako ih je moguće jasno razlikovati od ranije spomenutih piktograma ili kombinacija piktograma.

119 Zaslon mora biti uključen uvijek kada se vozilo kreće.

120 Tahograf može imati ručnu ili automatsku mogućnost isključivanja zaslona kada se vozilo ne kreće.

Oblik prikaza naveden je u Dodatku 5.

15.1. ***Standardni prikaz***

121 Kada nije potrebno prikazivati nikakve druge informacije, tahograf mora standardno prikazivati sljedeće:

— lokalno vrijeme (kao rezultat UTC vremena + pomaci koje podešava vozač),

— način rada,

— trenutačnu aktivnost vozača i trenutačnu aktivnost suvozača,

— informacije vezane uz vozača:

— ako je njegova trenutačna aktivnost VOŽNJA, njegovo trenutačno neprekidno vrijeme vožnje i njegovo trenutačno zbirno vrijeme pauze,

— ako njegova trenutačna aktivnost nije VOŽNJA, trenutačno trajanje te aktivnosti (otkad je odabrana) i njegovo trenutačno zbirno vrijeme pauze,

— informacije vezane uz suvozača:

— trenutačno trajanje njegove aktivnosti (otkad je odabrana).

122 Prikaz podataka vezanih uz svakog vozača mora biti jasan, jednostavan i nedvosmislen. U slučaju kada se informacije o vozaču i suvozaču ne mogu prikazati istodobno, tahograf mora standardno prikazivati informacije u vezi vozača, a korisniku mora omogućiti da prikaže i informacije u vezi suvozača.

123 U slučaju kad širina zaslona ne omogućuje standardno prikazivanje načina rada, tahograf mora nakratko prikazati novi način rada kad se on izmijeni.

124 Tahograf nakratko prikazuje ime nositelja kartice pri umetanju kartice.

124a Kad je započelo stanje ‚IZVAN DJELOKRUGA' standardni zaslon mora, koristeći odgovarajući piktogram, prikazati da je takvo stanje započelo (prihvatljivo je da se tekuća aktivnost vozača ne mora prikazati istodobno).

15.2. ***Prikaz upozorenja***

125 Tahograf prikazuje informaciju upozorenja koristeći prvenstveno piktograme iz Dodatka 3., dopunjene prema potrebi dodatnim numerički šifriranim informacijama. Može se također dodati tekstualni opis upozorenja na jeziku po odabiru vozača.

15.3. ***Pristup izbornicima***

126 Tahograf mora osigurati potrebne naredbe putem odgovarajuće strukture izbornika.

15.4. ***Ostali prikazi***

127 Na zahtjev mora biti moguće selektivno prikazivanje:

— UTC datuma i vremena,

— način rada (ako nije standardno predviđeno),

— neprekidno vrijeme vožnje i zbirno vrijeme pauze vozača,

— neprekidno vrijeme vožnje i zbirno vrijeme pauze suvozača,

— zbirno vrijeme vožnje vozača za prethodni i tekući tjedan,

— zbirno vrijeme vožnje suvozača za prethodni i tekući tjedan,

— sadržaj bilo kojeg od šest ispisa u istom obliku kao što izgledaju sami ispisi.

128 Prikaz sadržaja ispisa je u slijedu, redak po redak. Ako je širina zaslona manja od 14 slovnih znakova, korisniku se pruža potpuna informacija na primjeren način (nekoliko redaka, klizni prikaz teksta, …). Reci ispisa koji se odnose na ručno unesene informacije mogu se izostaviti iz prikaza.

16. **Ispis**

129 Tahograf mora biti u stanju ispisati informacije iz svoje podatkovne memorije i/ili kartica tahografa u obliku šest sljedećih ispisa:

— dnevni ispis aktivnosti vozača s kartice,

— dnevni ispis aktivnosti vozača iz jedinice u vozilu,

— ispis događaja i pogrešaka s kartice,

— ispis događaja i pogrešaka iz jedinice u vozilu,

— ispis tehničkih podataka,

— ispis prekoračenja brzine.

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

Na kraju ispisa mogu se dati dodatni podaci.

Tahograf može omogućiti i druge ispise, ako se oni jasno razlikuju od šest gore spomenutih ispisa.

130 ‚Dnevni ispis aktivnosti vozača s kartice' i ‚ispis događaja i pogrešaka s kartice' moraju biti dostupni samo kada je kartica vozača ili kartica radionice umetnuta u tahograf. Tahograf zapisuje do tada pohranjene podatke na odgovarajućoj kartici prije početka ispisa.

131 Kako bi se izradio ‚dnevni ispis aktivnosti vozača s kartice' i ‚ispis događaja i pogrešaka iz kartice', tahograf mora:

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

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

132 Pisač mora moći ispisati 24 slovna znaka po retku.

133 Minimalna veličina slovnih znakova mora biti 2,1 mm u visinu i 1,5 mm u širinu.

133a Pisač mora podržavati skupinu slova Latin 1 i skupinu grčkih slova utvrđene normom ISO 8859, dio 1. i 7., kako je navedeno u poglavlju 4. Dodatka 1.: ‚Skupine slova'.

134 Pisači moraju biti tako izrađeni da daju ispise s takvom oštrinom da se izbjegne svaka nejasnoća pri njihovom čitanju.

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

136 Papir za korištenje u tahografu mora nositi odgovarajuću oznaku tipnog odobrenja i oznaku vrste ili vrsta tahografa u kojima se može koristiti. Ispisi moraju ostati jasno čitljivi i prepoznatljivi u normalnim uvjetima čuvanja, s obzirom na jakost svjetla, vlažnost i temperaturu, najmanje godinu dana.

137 Također mora postojati mogućnost da se u ove dokumente dodaju rukom pisane zabilješke, kao što je potpis vozača.

138 Slučajeve nestanka papira pri ispisu tahograf mora riješiti tako da nakon ponovnog umetanja papira, ponovno počne ispis od početka ili se ispis nastavi uz jasno upućivanje na prethodno ispisan dio.

17. **Upozorenja**

139 Tahograf upozorava vozača pri otkrivanju svakog događaja ili pogreške.

140 Upozorenje o prekidu napajanja može se odgoditi do ponovne uspostave napajanja.

141 Tahograf mora upozoriti vozača 15 minuta prije i u trenutku prekoračenja 4 sata i 30 minuta neprekidne vožnje.

142 Upozorenja moraju biti vizualna. Pored vizualnih upozorenja moguće je predvidjeti i davanje zvučnog signala.

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

144 Vizualna upozorenja mogu biti ugrađena u tahograf i/ili odvojena od tahografa.

145 U potonjem slučaju ono mora biti označeno oznakom ‚T' i mora biti žute ili narančaste boje.

146 Upozorenja moraju trajati najmanje 30 sekundi, osim ako ih korisnik ne potvrdi pritiskom na bilo koju tipku tahografa: Prva potvrda ne smije izbrisati prikaz uzroka upozorenja iz sljedećeg stavka.

147 Uzrok upozorenja se mora prikazati na tahografu i ostati vidljiv dok ga korisnik ne potvrdi korištenjem posebne tipke ili naredbe u tahografu.

148 Dodatna upozorenja se mogu predvidjeti dokle god ona ne zbunjuju vozače u vezi s prethodno danim upozorenjima.

18. **Preuzimanje podataka na vanjske medije**

149 Tahograf mora moći na zahtjev preuzeti podatke iz svoje podatkovne memorije ili s kartice vozača na vanjske medije za spremanje preko svog priključka za kalibraciju/preuzimanje podataka. Tahograf mora ažurirati podatke spremljene na predmetnu karticu prije početka preuzimanja podataka.

150 Pored toga, kao neobavezna funkcija, tahograf može, u bilo kojem načinu rada preuzimati podatke preko drugog priključka za tvrtku koja se identificirala preko tog kanala. U tom slučaju se na takvo preuzimanje podataka primjenjuju prava pristupa podacima u načinu rada tvrtke.

151 Preuzimanje podataka ne izmijenjuje ili briše niti jedan pohranjeni podatak.

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

Protokoli preuzimanja podataka su opisani u Dodatku 7.

19. **Izlazni podaci za dodatne vanjske uređaje**

152 Kad tahograf ne posjeduje funkcije prikaza brzine i/ili brojača kilometara, tahograf mora imati izlazni signal ili signale koji omogućuju prikaz brzine vozila (brzinomjer) i/ili ukupne prijeđene udaljenosti vozila (brojač kilometara).

153 Jedinica u vozilu mora također biti u stanju osigurati izlaz sljedećih podataka preko odgovarajuće serijske veze neovisne o neobveznoj CAN bus sabirnici (ISO 11898 Cestovna vozila – Razmjena digitalnih informacija – Controller Area Network (CAN) za brzu komunikaciju), kako bi se omogućila njihova obrada pomoću drugih elektronskih jedinica ugrađenih u vozilu:

— tekući UTC datum i vrijeme,

— brzina vozila,

— ukupno prijeđena udaljenost vozila (brojač kilometara),

— trenutačno odabrana aktivnost vozača i suvozača,

— informacija o tome je li bilo koja kartica tahografa trenutačno umetnuta u utor vozača odnosno suvozača i (prema potrebi) informacije o identifikaciji odgovarajućih kartica (broj kartice i država članica izdavatelj).

Pored ovog popisa minimalnih informacija mogu se prenijeti i drugi podaci.

Kad je vozilu dan kontakt, ovi se podaci neprekidno šalju. Kad vozilu nije dan kontakt, šalje se najmanje svaka izmjena aktivnosti vozača ili suvozača i/ili svako umetanje ili vađenje kartice iz tahografa. U slučaju da pojedini podaci nisu poslani zbog toga što nije dan kontakt u vozilu, podaci se moraju poslati pri ponovnom davanju kontakta vozila.

20. **Kalibracija**

154 Funkcija kalibracije mora omogućavati:

— automatsko uparivanje senzora kretanja s jedinicom u vozilu,

— digitalnu prilagodbu konstante tahografa (k) karakterističnom koeficijentu vozila (w) (vozila s dva ili više završnih osovinskih prijenosnih omjera moraju biti opremljena sklopnim uređajem pomoću koje se ti različiti omjeri automatski usklađuju s omjerom za koji je tahograf prilagođen vozilu),

— podešavanje (bez ograničenja) trenutačnog vremena,

— podešavanje trenutačne vrijednosti brojača kilometara,

— ažuriranje identifikacijskih podataka senzora kretanja spremljenih u podatkovnoj memoriji,

— ažuriranje ili potvrđivanje ostalih parametara poznatih tahografu: identifikacija vozila, w, l, dimenzije guma i prema potrebi podešavanje ograničavača brzine.

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

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

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

156 Funkcija kalibriranja mora biti u stanju unijeti potrebne podatke preko priključnice za kalibraciju/preuzimanje podataka u skladu s protokolom kalibracije utvrđenim u Dodatku 8. Funkcija kalibriranja također može unositi potrebne podatke preko drugih priključnica.

21. **Podešavanje vremena**

157 Funkcija podešavanja vremena mora omogućavati podešavanje trenutačnog vremena za najviše jednu minutu u razmacima od najmanje sedam dana.

158 Funkcija podešavanja vremena mora u načinu kalibracije omogućavati podešavanje trenutačnog vremena bez ograničenja.

22. **Radna obilježja**

159 Jedinica u vozilu mora biti u potpunosti spremna za pogon u temperaturnom rasponu od - 20 °C do 70 °C a senzor kretanja u temperaturnom rasponu od - 40 °C do 135 °C. Sadržaj podatkovne memorije se mora očuvati pri temperaturi do – 40 °C.

160 Tahograf mora biti u potpunosti spreman za pogon pri rasponu vlažnosti od 10 % do 90 %.

161 Tahograf mora biti zaštićen od prenapona, zamjene polariteta napajanja i kratkih spojeva.

162 Tahograf mora udovoljavati Direktivi Komisije 95/54/EZ od 31. listopada 1995. ([1]) o prilagodbi tehničkom napretku Direktive Vijeća 72/245/EEZ ([2]) o usklađivanju zakonodavstava država članica u odnosu na elektromagnetsku kompatibilnost, te mora biti zaštićen od elektrostatskih pražnjenja i prijelaznih stanja.

23. **Materijali**

163 Svi sastavni dijelovi tahografa moraju biti izrađeni od materijala dostatne stabilnosti i mehaničke čvrstoće i stabilnih električnih i magnetskih osobina.

164 U normalnim uvjetima korištenja svi unutarnji dijelovi tahografa moraju biti zaštićeni od vlage i prašine.

165 Jedinica u vozilu mora zadovoljavati stupanj zaštite IP 40, a senzor kretanja mora zadovoljavati stupanj zaštite IP 64 prema normi IEC 529.

([1]) SL L 266, 8.11.1995., str. 1.
([2]) SL L 152, 6.7.1972., str. 15.

166 Tahograf mora odgovarati važećim tehničkim specifikacijama u odnosu na ergonomsku izvedbu.

167 Tahograf mora biti zaštićen od slučajnog oštećenja.

24. **Oznake**

168 Ako tahograf prikazuje stanje brojača kilometara i brzinu vozila, na zaslonu se pojavljuju sljedeće pojedinosti:

— pokraj broja koji označuje udaljenost, jedinicu mjere za udaljenost označenu kraticom ‚km',

— pokraj broja koji pokazuje brzinu, oznaku ‚km/h'.

Tahograf se također može prebaciti na prikaz brzine u miljama na sat, u kojem slučaju se jedinica mjere za brzinu prikazuje kraticom ‚mph'.

169 Identifikacijska pločica pričvršćuje se na svakom odvojenom sastavnom dijelu tahografa i prikazuje sljedeće podatke:

— naziv i adresu proizvođača uređaja,

— kataloški broj proizvođača i godinu proizvodnje uređaja,

— serijski broj uređaja,

— tipno odobrenje uređaja.

170 Kad fizički prostor nije dostatan za prikaz svih gore navedenih podataka, identifikacijska pločica mora prikazivati barem naziv i zaštitni znak proizvođača i kataloški broj tahografa.

IV. ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNI ZAHTJEVI ZA KARTICE TAHOGRAFA

1. **Vidljivi podaci**

Prednja strana mora sadržavati:

171 riječi ‚kartica vozača' ili ‚nadzorna kartica' ili ‚kartica radionice' ili ‚kartica prijevoznika' tiskane velikim slovima na službenom jeziku ili jezicima države članice koja izdaje karticu, prema vrsti kartice;

172 iste riječi na drugim službenim jezicima Zajednice, tiskane u pozadini kartice:

ES	TARJETA DEL CONDUCTOR	TARJETA DE CONTROL	TARJETA DEL CENTRO DE ENSAYO	TARJETA DE LA EMPRESA
DK	FØRERKORT	KONTROLKORT	VÆRKSTEDSKORT	VIRKSOMHEDSKORT
DE	FAHRERKARTE	KONTROLLKARTE	WERKSTATTKARTE	UNTERNEHMENSKARTE
EL	ΚΑΡΤΑ ΟΔΗΟΥ	ΚΑΡΤΑ ΕΛΕΓΧΟΥ	ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΗΣ
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTRÔLEUR	CARTE D'ATELIER	CARTE D'ENTREPRISE
GA	CÁRTA TIOMÁNAÍ	CÁRTA STIÚRTHA	CÁRTA CEARDLAINNE	CÁRTA COMHLACHTA
IT	CARTA DEL CONDUCENTE	CARTA DI CONTROLLO	CARTA DELL'OFFICINA	CARTA DELL'AZIENDA
NL	BESTUURDERS KAART	CONTROLEKAART	WERKPLAATSKAART	BEDRIJFSKAART
PT	CARTÃO DE CONDUTOR	CARTÃO DE CONTROLO	CARTÃO DO ENSAIO	CARTÃO DE EMPRESA
FI	KULJETTAJA KORTTILLA	VALVONTAKORTTI	KORJAAMOKORTTI	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

173 naziv države članice koja je izdala karticu (nije obvezno);

174 razlikovnu oznaku države članice koja je izdala karticu, tiskanu u negativu u plavom pravokutniku i okruženu s 12 žutih zvjezdica. Razlikovne oznake su sljedeće:

B Belgija

DK Danska

D Njemačka

GR Grčka

E Španjolska

F Francuska

IRL Irska

I Italija

L Luksemburg

NL Nizozemska

A Austrija

P Portugal

FIN Finska

S Švedska

UK Ujedinjena Kraljevina;

175 informacije karakteristične za izdanu karticu, označene kako slijedi:

	Kartica vozača	Nadzorna kartica	Kartica radionice ili kartica prijevoznika
1.	Prezime vozača	Naziv nadzornog tijela	Naziv tvrtke ili radionice
2.	Ime(na) vozača	Prezime nadzornika (prema potrebi)	Prezime nositelja kartice (prema potrebi)
3.	Datum rođenja vozača	Ime(na) nadzornika (prema potrebi)	Ime(na) nositelja kartice (prema potrebi)
4.(a)	Datum početka valjanosti kartice		
(b)	Datum isteka valjanosti kartice (ako postoji)		
(c)	Naziv tijela koja izdaje karticu (može biti tiskano na 2. stranici)		
(d)	Broj različit od navedenoga pod točkom 5. za administrativne potrebe (nije obvezno)		
5.(a)	Broj vozačke dozvole (na datum izdavanja kartice vozača)		
5.(b)	Broj kartice		
6.	Fotografija vozača	Fotografija nadzornika (nije obvezna)	—
7.	Potpis vozača	Potpis nositelja kartice (nije obvezno)	
8.	Uobičajeno mjesto prebivališta ili poštanska adresa nositelja (nije obvezno	Poštanska adresa nadzornog tijela	Poštanska adresa prijevoznika ili radionice

176 datumi se pišu u obliku ‚dd/mm/gggg' ili ‚dd.mm.gggg.' (dan, mjesec, godina).

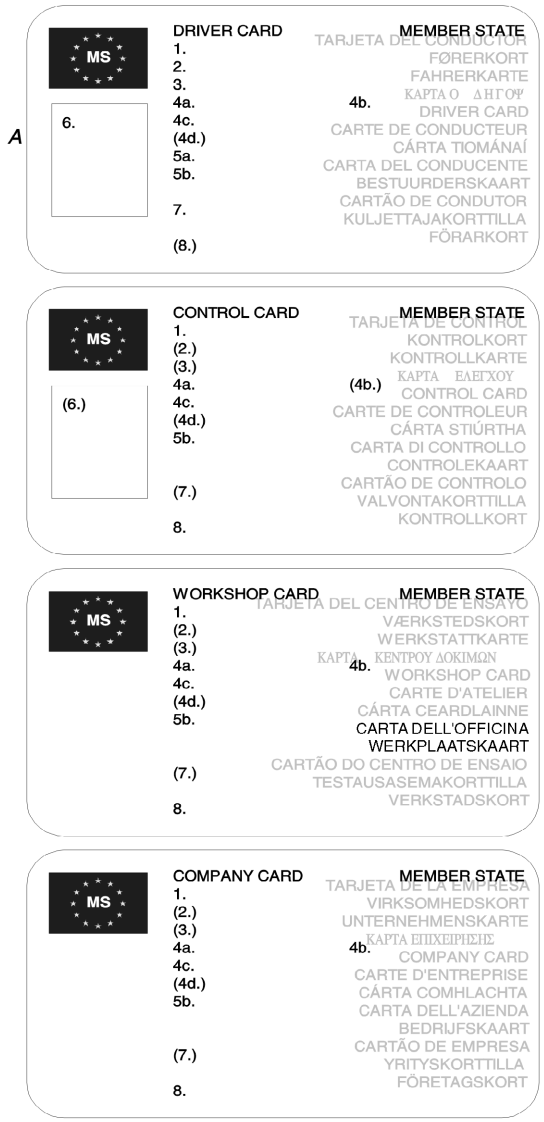
stražnja strana mora sadržavati:

177 pojašnjenja navedenih stavki na prednjoj strani kartice;

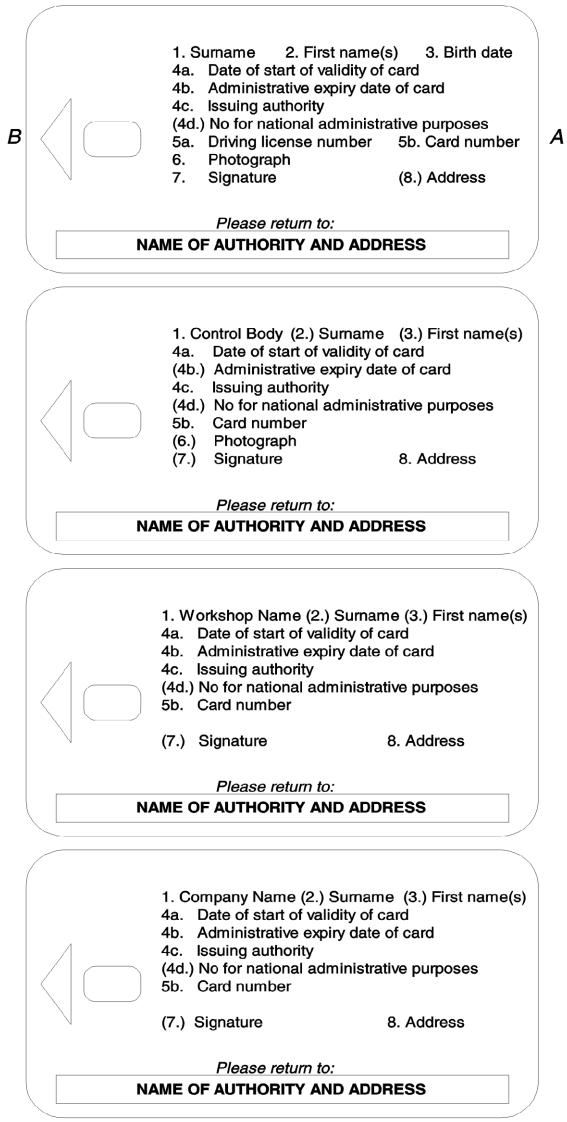
178 uz poseban pisani pristanak nositelja mogu se dodati i informacije koje se ne odnose na vođenje kartice, pri čemu njihovo dodavanje ni na koji način neće izmijeniti korištenje obrasca kao kartice tahografa.

OBRAZAC ZAJEDNICE ZA KARTICE TAHOGRAFA

PREDNJA STRANA



POLEĐINA



179 Kartice tahografa se moraju tiskati sa sljedećim prevladavajućim bojama pozadine:

— kartica vozača: bijela,

— nadzorna kartica: plava,

— kartica radionice: crvena,

— kartica prijevoznika: žuta.

180 Kartice tahografa moraju imati barem sljedeća obilježja za zaštitu tijela kartice od krivotvorenja i neovlaštenog rukovanja:

— sigurnosno izvedenu pozadinu s finim guilloche uzorcima i nijansiranim tiskom,

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

— barem jedna dvobojna linija u mikrotisku.

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

2. **Sigurnost**

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

182 Kako bi se postigla sigurnost sustava, kartice tahografa moraju zadovoljavati sigurnosne zahtjeve utvrđene u generičkim sigurnosnim ciljevima za kartice tahografa (Dodatak 10.).

183 Kartice tahografa moraju biti čitljive od strane druge opreme, kao što su osobna računala.

3. **Norme**

184 Kartice tahografa moraju zadovoljavati sljedeće norme:

— ISO/IEC 7810 Identifikacijske kartice – fizičke značajke,

— ISO/IEC 7816 Identifikacijske kartice – integrirani krugovi s kontaktima,

  — 1. dio: Fizička obilježja,

  — 2. dio: Dimenzije i smještaj kontakata,

  — 3. dio: Elektronski signali i protokoli prijenosa,

  — 4. dio: Međugranske naredbe za razmjenu,

  — 8. dio: Međugranske naredbe koje se odnose na sigurnost,

— ISO/IEC 10573 Identifikacijske kartice – metode provjere.

4. **Okoliš i električne karakteristike**

185 Kartice tahografa moraju biti u stanju ispravno raditi u svim klimatskim uvjetima uobičajenim na teritoriju Zajednice, pri temperaturnom rasponu od najmanje - 25 °C do + 70 °C s povremenim vršnim porastom do + 85 °C, pri čemu ‚povremeno' označuje ne dulje od 4 sata svaki puta i ne više od 100 puta tijekom vijeka trajanja kartice.

186 Kartice tahografa moraju biti u stanju ispravno raditi u rasponu vlažnosti između 10 % i 90 %.

187 Kartice tahografa moraju biti u stanju ispravno raditi tijekom razdoblja od pet godina ako se koriste u skladu sa specifikacijama okruženja i elektrotehničkim specifikacijama.

188 Tijekom korištenja kartice tahografa moraju biti u skladu s Direktivom Komisije 95/54/EZ od 31. listopada 1995. ([1]) o elektromagnetskoj kompatibilnosti, te moraju biti zaštićene od elektrostatskih pražnjenja.

5. **Spremanje podataka**

Za potrebe ovog stavka,

— vremena se bilježe s razlučivošću od jedne minute, osim ako nije drukčije određeno,

— stanje brojača kilometara se bilježi s razlučivošću od 1 kilometra,

— brzine se bilježe s razlučivošću od 1 km/h.

Funkcije, naredbe i logičke strukture kartice tahografa koje ispunjavaju zahtjeve u pogledu spremanja podataka su navedene u Dodatku 2.

([1]) SL L 266, 8.11.1995., str. 1.

189 Ovaj stavak navodi minimalan kapacitet spremanja podataka za različite podatkovne datoteke. Kartice tahografa moraju biti u stanju prikazati tahografu stvarni kapacitet spremanja tih podatkovnih datoteka.

Svi dodatni podaci koji se mogu spremiti na karticama tahografa, a koji se odnose na druge podatke eventualno spremljene na kartici, moraju se čuvati u skladu s Direktivom 95/46/EZ od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka ([1]).

5.1. ***Identifikacija kartice i sigurnosni podaci***

5.1.1. *Identifikacija programa*

190 Kartice tahografa moraju biti u stanju pohraniti sljedeće programske identifikacijske podatke:

— identifikaciju tahografskog programa,

— identifikaciju vrste kartice tahografa.

5.1.2. *Identifikacija čipa*

191 Kartice tahografa moraju biti u stanju pohraniti sljedeće identifikacijske podatke o integriranom krugu (IC):

— serijski broj IC,

— proizvodne reference IC.

5.1.3. *IC identifikacija kartice*

192 Kartice tahografa moraju biti u stanju pohraniti sljedeće identifikacijske podatke pametnih kartica:

— serijski broj kartice (s proizvodnim referencama),

— broj tipskog odobrenja kartice,

— identifikaciju (ID) personalizatora kartice,

— identifikaciju ugraditelja (ID),

— identifikator IC.

5.1.4. *Sigurnosni elementi*

193 Kartice tahografa moraju biti u stanju pohraniti sljedeće podatke o sigurnosnim elementima:

— europski javni ključ,

— certifikat države članice,

— certifikat kartice,

— privatni ključ kartice.

5.2. ***Kartica vozača***

5.2.1. *Identifikacija kartice*

194 Kartica vozača mora biti u stanju pohraniti sljedeće identifikacijske podatke kartice:

— broj kartice,

— država članica izdavatelj, naziv tijela izdavatelja, datum izdavanja,

— datum početka valjanosti i isteka kartice.

([1]) SL L 281, 23.11.1995., str. 31.

5.2.2. *Identifikacija nositelja kartice*

195 Kartica vozača mora biti u stanju pohraniti sljedeće identifikacijske podatke nositelja kartice:

— prezime nositelja,

— ime(na) nositelja,

— datum rođenja,

— izabrani jezik.

5.2.3. *Podaci o vozačkoj dozvoli*

196 Kartica vozača mora biti u stanju pohraniti sljedeće podatke o vozačkoj dozvoli:

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

— broj vozačke dozvole (na datum izdavanja kartice).

5.2.4. *Podaci o korištenim vozilima*

197 Kartica vozača mora biti u stanju spremiti sljedeće podatke za svaki kalendarski dan korištenja kartice i za svako razdoblje korištenja dotičnog vozila tog dana (razdoblje korištenja obuhvaća sve uzastopne cikluse umetanja i vađenja kartice u tom vozilu s gledišta kartice):

— datum i vrijeme prvog korištenja vozila (tj. prvog umetanja kartice u navedenom razdoblju korištenja vozila ili 00:00 ako je kartica korištena u to vrijeme),

— stanje brojača kilometara vozila u to vrijeme,

— datum i vrijeme posljednjeg korištenja vozila (tj. posljednjeg vađenja kartice u tom razdoblju korištenja vozila ili 23:59 ako je kartica korištena u to vrijeme)

— stanje brojača kilometara vozila u to vrijeme,

— registracijski broj vozila i država članica registracije vozila.

198 Kartica vozača mora biti u stanju pohraniti najmanje 84 takva zapisa.

5.2.5. *Podaci o aktivnostima vozača*

199 Kartica vozača mora biti u stanju pohraniti, za svaki kalendarski dan korištenja kartice ili za koji je vozač ručno unio podatke, sljedeće podatke:

— datum,

— dnevni brojač prisustva (uvećan za 1 za svaki od navedenih kalendarskih dana),

— ukupnu udaljenost koju je vozač prešao u tom danu,

— status vozača u 00:00,

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

  — status vožnje (POSADA, JEDAN VOZAČ),

  — utor (VOZAČ, SUVOZAČ),

  — status kartice (UMETNUTA, NIJE UMETNUTA),

  — aktivnost (VOŽNJA, PRIPRAVNOST, RAD, PAUZA/ODMOR),

  — vrijeme promjene.

200 Memorija vozačke kartice mora biti u stanju zadržati podatke o aktivnosti vozača najmanje 28 dana (pri čemu se prosječna aktivnost vozača utvrđuje na 93 promjene dnevno).

201 Podaci navedeni u zahtjevima 197 i 199 pohranjuju se na način koji omogućuje učitavanje aktivnosti redoslijedom njihovog pojavljivanja, čak i u slučaju vremenskog preklapanja.

5.2.6. *Mjesta početka i/ili završetka dnevnih aktivnosti*

202 Kartica vozača mora biti u stanju pohraniti sljedeće podatke vezane uz mjesto početka i/ili završetka dnevnih aktivnosti koje unese vozač:

— datum i vrijeme unosa (ili datum/vrijeme vezane uz ručni unos),

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

— državu i regiju ulaska,

— stanje brojača kilometara vozila.

203 Memorija vozačke kartice mora biti u stanju pohraniti najmanje 42 parova takvih zapisa.

5.2.7. *Podaci o događajima*

Za potrebe ovog podstavka, vrijeme se pohranjuje s razlučivošću od jedne sekunde.

204 Kartica vozača mora biti u stanju pohraniti podatke vezane uz sljedeće događaje koje je tahograf otkrio dok je bila umetnuta kartica:

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

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

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

— prekid napajanja,

— pogreška u podacima o kretanju,

— pokušaji probijanja zaštite.

205 Kartica vozača mora biti u stanju pohraniti sljedeće podatke za navedene događaje:

— šifru događaja,

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

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

— registracijsku oznaku vozila i državu članicu registracije vozila u kojemu je nastao događaj.

Napomena: Kod događaja ‚vremenskog preklapanja':

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

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

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

Napomena: Kod događaja ‚neispravnog završetka posljednjeg korištenja kartice':

— datum i vrijeme početka događaja moraju odgovarati datumu i vremenu umetanja kartice koji nije pravilno završen,

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

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

206 Kartica vozača mora biti u stanju pohraniti podatke za šest posljednjih događaja za svaku vrstu (tj. 36 događaja).

5.2.8. *Podaci o pogreškama*

Za potrebe ovog podstavka, vrijeme se bilježi s razlučivošću od jedne sekunde.

207 Kartica vozača mora biti u stanju spremiti podatke vezane uz sljedeće pogreške koje je tahograf otkrio dok je kartica bila umetnuta:

— pogreška kartice (kada je ta kartica predmet događaja),

— pogreška tahografa.

208 Kartica vozača mora biti u stanju spremiti sljedeće podatke za navedene pogreške:

— šifru pogreške,

— datum i vrijeme početka pogreške (ili umetanja kartice ako je u tom trenutku pogreška bila u tijeku),

— datum i vrijeme završetka pogreške (ili vađenja kartice ako je u tom trenutku pogreška bila u tijeku),

— registracijski broj vozila i državu članicu registracije vozila u kojemu je došlo do pogreške.

209 Kartica vozača mora biti u stanju spremiti podatke za dvanaest posljednjih pogrešaka za svaku vrstu (tj. 24 pogreške).

5.2.9. *Podaci o nadzornim aktivnostima*

210 Kartica vozača mora biti u stanju spremiti sljedeće podatke vezane uz nadzorne aktivnosti:

— datum i vrijeme nadzora,

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

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

— razdoblje preuzimanja podataka (u slučaju preuzimanja podataka),

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

Napomena: sigurnosni zahtjevi podrazumijevaju da se preuzimanje podataka s kartice bilježi samo ako je izvršeno preko tahografa.

211 Kartica vozača mora biti u stanju spremiti jedan takav zapis.

5.2.10. *Podaci o upotrebi kartice*

212 Kartica vozača mora biti u stanju pohraniti podatke vezane o vozilu u kojem je započela upotreba kartice:

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

— registracijski broj vozila i državu članicu registracije vozila.

5.2.11. *Podaci o posebnim stanjima*

212a Kartica vozača mora biti u stanju spremiti sljedeće podatke vezane uz posebna stanja koja su unesena dok je kartica bila umetnuta (bez obzira u koji utor):

— datum i vrijeme unosa,

— vrsta posebnog stanja.

212b Kartica vozača mora biti u stanju spremiti 56 takvih zapisa.

5.3. ***Kartica radionice***

5.3.1. *Sigurnosni elementi*

213 Kartica radionice mora biti u stanju spremiti osobni identifikacijski broj (PIN oznaku).

214 Kartica radionice mora biti u stanju spremiti kriptografske ključeve potrebne za uparivanje senzora kretanja s jedinicama u vozilu.

5.3.2. *Identifikacija kartice*

215 Kartica radionice mora moći spremiti sljedeće identifikacijske podatke kartice:

— broj kartice,

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

— datum početka i isteka valjanosti kartice.

5.3.3. *Identifikacija nositelja kartice*

216 Kartica radionice mora biti u stanju spremiti sljedeće identifikacijske podatke nositelja kartice:

— ime radionice,

— adresu radionice,

— prezime nositelja,

— ime(na) nositelja,

— izabrani jezik.

5.3.4. *Podaci o korištenim vozilima*

217 Kartica radionice mora biti u stanju spremiti podatke o korištenim vozilima na isti način kao i kartica vozača.

218 Kartica radionice mora biti u stanju čuvati najmanje 4 takva zapisa.

5.3.5. *Podaci o aktivnosti vozača*

219 Kartica radionice mora biti u stanju spremiti podatke o aktivnostima vozača na isti način kao i kartica vozača.

220 Kartica radionice mora biti u stanju čuvati podatke o aktivnostima vozača barem tijekom jednog dana prosječne aktivnosti vozača.

5.3.6. *Podaci o početku i/ili završetku dnevnog razdoblja rada*

221 Kartica radionice mora biti u stanju spremiti podatke o početku i/ili završetku dnevnog razdoblja rada na isti način kao i kartica vozača.

222 Kartica radionice mora biti u stanju čuvati najmanje tri para takvih zapisa.

5.3.7. *Podaci o događajima i pogreškama*

223 Kartica radionice mora biti u stanju spremiti podatke o događajima i pogreškama na isti način kao i kartica vozača.

224 Kartica radionice mora biti u stanju čuvati podatke za tri posljednja događaja svake vrste (tj. 18 događaja) i šest posljednjih pogrešaka svake vrste (tj. 12 pogrešaka).

5.3.8. *Podaci o nadzornim aktivnostima*

225 Kartica radionice mora biti u stanju spremiti podatke o aktivnostima nadzora na isti način kao i kartica vozača.

5.3.9. *Podaci o kalibraciji i podešavanju vremena*

226 Kartica radionice mora biti u stanju spremiti zapise o kalibraciji i/ili vremenskim podešenjima izvršenim dok je kartica bila umetnuta u tahograf.

227 Svaki zapis o kalibraciji mora sadržavati sljedeće podatke:

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

— identifikaciju vozila,

— parametre koji se ažuriraju ili potvrđuju (w, k, l, dimenzije guma, postavke ograničavača brzine, stanje brojača kilometara (novu i staru vrijednost), datum i vrijeme (nove i stare vrijednosti),

— identifikaciju tahografa (kataloški broj jedinice vozila, serijski broj jedinice vozila, serijski broj senzora kretanja).

228 Kartica radionica mora biti u stanju spremiti barem 88 takvih zapisa.

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

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

5.3.10. *Podaci o posebnim uvjetima*

230a Kartica radionice mora biti u stanju spremiti podatke o posebnim uvjetima na isti način kao i kartica vozača. Kartica radionice mora biti u stanju čuvati dva takva zapisa.

5.4. ***Nadzorna kartica***

5.4.1. *Identifikacija kartice*

231 Nadzorna kartica mora moći spremiti sljedeće identifikacijske podatke kartice:

— broj kartice,

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

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

5.4.2. *Identifikacija nositelja kartice*

232 Nadzorna kartica mora moći spremiti sljedeće identifikacijske podatke nositelja kartice:

— naziv nadzornog tijela,

— adresu nadzornog tijela,

— prezime nositelja,

— ime(na) nositelja,

— izabrani jezik.

5.4.3. *Podaci o nadzornim aktivnostima*

233 Nadzorna kartica mora moći spremiti sljedeće podatke o nadzornim aktivnostima:

— datum i vrijeme nadzora,

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

— razdoblje preuzimanja podataka (ako postoji),

— registracijski broj vozila i država članica registracije kontroliranog vozila.

— broj kartice i država članica koja je izdala kontroliranu vozačku karticu.

234 Nadzorna kartica mora moći spremiti najmanje 230 takvih zapisa.

5.5. ***Kartica prijevoznika***

5.5.1. *Identifikacija kartice*

235 Kartica prijevoznika mora moći spremiti sljedeće identifikacijske podatke kartice:

— broj kartice,

— država članica izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,

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

5.5.2. *Identifikacija nositelja kartice*

236 Kartica tvrtke mora moći spremiti sljedeće identifikacijske podatke nositelja kartice:

— naziv tvrtke,

— adresu tvrtke.

5.5.3. *Podaci o aktivnostima prijevoznika*

237 Kartica prijevoznika mora moći spremiti sljedeće podatke o aktivnostima prijevoznika:

— datum i vrijeme aktivnosti,

— vrstu aktivnosti (zaključavanje ili otključavanje blokade jedinice vozila, preuzimanje podataka s jedinice vozila i/ili s kartice),

— razdoblje preuzimanja podataka (ako postoji),

— registracijski broj vozila i država registracije vozila,

— broj kartice i državu članicu izdavanja kartice (u slučaju preuzimanja podataka s kartice).

238 Kartica prijevoznika mora moći spremiti barem 230 takvih zapisa.

V. UGRADNJA TAHOGRAFA

1. **Ugradnja**

239 Novi tahograf se isporučuje neaktiviran ugraditeljima ili proizvođačima vozila sa svim parametrima za kalibraciju navedenim u poglavlju III, odjeljak 20., podešenim na odgovarajuće i osnovne vrijednosti. Ako neka određena vrijednost nije podešena, slovni parametri se zamjenjuju nizom znakova '?' a numerički parametri se postavljaju na ‚0'.

240 Prije aktivacije, tahograf mora imati pristup funkciji kalibracije, čak i kada nije u režimu kalibracije.

241 Prije aktivacije, tahograf ne smije zapisivati niti spremati podatke iz točaka III.12.3 do III.12.9, te III.12.12 do i uključujući III.12.14.

242 Tijekom ugradnje proizvođači vozila moraju unaprijed podesiti sve poznate parametre.

243 Proizvođači vozila ili ugraditelji tahograf moraju aktivirati prije nego što vozilo napusti službene prostorije u kojima je izvršena ugradnja.

244 Stavljanje tahografa u pogon se vrši automatski prvim umetanjem kartice radionice u bilo koji uređaj kartičnog sučelja.

245 Posebne operacije uparivanja senzora kretanja i jedinice u vozilu, ako ih ima, se vrše automatski prije ili tijekom aktivacije.

246 Nakon aktivacije, tahograf mora u potpunosti izvršavati funkcije i prava pristupa podacima.

247 Funkcije zapisivanja i spremanja u tahografu postižu punu radnu sposobnost nakon njegove aktivacije.

248 Nakon ugradnje slijedi kalibracija. Prva kalibracija uključuje unos registracijskog broja vozila i vrši se u roku od dva tjedna nakon spomenute ugradnje ili dodjele registracijske broja vozila, što god je kasnije.

248a Tahograf mora biti smješten u vozilu tako da omogući vozaču pristup potrebnim funkcijama iz svog sjedala.

2. **Ugradbena pločica**

249 Nakon što se pri ugradnji izvrši provjera tahografa, na, u ili pored tahografa se učvršćuje ugradbena pločica koja je jasno vidljiva i lako dostupna. Nakon svakog pregleda od strane ovlaštenog ugraditelja ili radionice na mjesto prethodne postavlja se nova pločica.

250 Pločica mora sadržavati sljedeće podatke:

— naziv, adresu ili zaštitni znak ovlaštenog ugraditelja ili radionice,

— karakteristični koeficijent vozila u obliku ‚w = … imp/km',

— konstanta tahografa u obliku ‚k = … imp/km',

— djelatni opseg guma kotača u obliku ‚l = … mm',

— dimenzije guma,

— datum utvrđivanja karakterističnog koeficijenta vozila i mjerenja djelatnog opsega guma kotača,

— identifikacijski broj vozila.

3. **Postavljanje žigova**

251 Sljedeći dijelovi moraju zaštićeni žigom:

— svaki spoj čije bi razdvajanje uzrokovalo izmjene ili gubitak podataka koje ne bi bilo moguće otkriti,

— ugradbena pločica, osim ako je pričvršćena na takav način da ju je nemoguće ukloniti bez uništavanja oznaka na istoj.

252 Gore spomenuta žigovi se mogu ukloniti:

— u izvanrednom slučaju,

— pri ugradnji, podešavanju ili popravku ograničavača brzine ili nekog drugog uređaja koji doprinosi sigurnosti na cesti, pod uvjetom da tahograf nastavi raditi pouzdano i ispravno, te da ovlašteni ugraditelj ili radionica ponovno postavi žigove (u skladu s poglavljem VI.), odmah nakon postavljanja ograničavača brzine ili nekog drugog uređaja koji doprinosi sigurnosti na cestama ili u roku od sedam dana u drugim slučajevima.

253 Svaki put kada se ti žigovi skidaju, sastavlja se pisana izjava u kojoj se navode razlozi zbog kojih je to učinjeno i koja mora biti dostupna nadležnom tijelu.

VI. ISPITIVANJE, PREGLEDI I POPRAVCI

Zahtjevi u pogledu okolnosti u kojima se žigovi mogu skidati sukladno članku 12.5 Uredbe (EEZ) br. 3821/85 kako je zadnje izmijenjena Uredbom (EZ) br. 2135/98, utvrđeni su u poglavlju V. odjeljku 3. ovog Priloga.

1. **Ovlaštenje ugraditelja ili radionica**

Države članice ovlašćuju, redovito nadziru i potvrđuju tijela koja obavljaju:

— ugradnju,

— ispitivanje,

— preglede,

— popravke.

U okviru članka 12. stavka 1. ove Uredbe, kartice radionice se izdaju samo ugraditeljima i/ili radionicama ovlaštenim za stavljanje u pogon i/ili kalibraciju tahografa u skladu s ovim Prilogom i, osim ukoliko ne postoji valjano opravdanje:

— onima koji nemaju pravo na kartice prijevoznika,

— i čija druga poslovna djelatnost ne dovodi u pitanje sveukupnu sigurnost sustava kako je utvrđeno u Dodatku 10.

2. **Ispitivanje novih ili popravljenih uređaja**

254 Svaki pojedini uređaj, bilo da je nov ili popravljen, provjerava se u pogledu njegovog ispravnog rada i točnosti očitavanja i zapisa, u granicama utvrđenim u poglavlju III.2.1. i III.2.2., putem stavljanja žigova u skladu s poglavljem V.3 i kalibracije.

3. **Nadzor pri ugradnji**

255 Pri postavljanju u vozilo, čitava instalacija (uključujući i tahograf) mora udovoljiti odredbama koje se tiču maksimalnih odstupanja utvrđenih u poglavlju III.2.1. i III.2.2.

4. **Periodični pregledi**

256 Periodični pregled tahografa u vozilu se obavlja nakon svakog popravka uređaja ili nakon svake izmjene karakterističnog koeficijenta vozila ili djelatnog opsega guma ili nakon pogreške UTC vremena veće od 20 minuta, ili pri promjeni registracijske oznake vozila, te bar jednom svake dvije godine (24 mjeseca) nakon posljednjeg pregleda.

257 Ti pregledi obuhvaćaju sljedeće provjere:

— da tahograf radi ispravno, uključujući funkciju spremanja podataka na kartice tahografa,

— sukladnost s odredbama poglavlja III.2.1. i III.2.2. o najvećem odstupanju,

— ima li tahograf oznaku tipnog odobrenja,

— da je pričvršćena ugradbena pločica,

— da su svi žigovi na uređaju i na drugim dijelovima instalacije netaknuti,

— dimenziju i djelatni opseg guma kotača.

258 Ovi pregledu moraju obuhvatiti i kalibraciju.

5. **Mjerenje pogrešaka**

259 Mjerenje pogrešaka pri ugradnji i tijekom korištenja se provodi prema sljedećim uvjetima, za koje se smatra da predstavljaju standardne ispitne uvjete:

— vozilo prazno, u normalnom stanju rada,

— pritisak u gumama u skladu s uputama proizvođača,

— potrošenost gaznog sloja guma u granicama dopuštenim nacionalnim propisima,

— kretanje vozila:

  — vozilo se kreće snagom vlastitog motora pravocrtno i na ravnom terenu, pri brzini od 50 ± 5 km/h. Mjerna udaljenost je najmanje 1,000 m,

— pod uvjetom da im je točnost usporedljiva, za provjeru se mogu koristiti i alternativne metode kao što je odgovarajuće ispitivanje na stolu.

6. **Popravci**

260 Radionice moraju biti u stanju preuzeti podatke s tahografa kako bi ih mogli dostaviti odgovarajućem prijevozniku.

261 Ovlaštene radionice izdaju prijevoznicima potvrdu o nemogućnosti preuzimanja podataka kada neispravnost tahografa sprečava preuzimanje prethodno zabilježenih podataka, čak i nakon popravka u radionici. Radionice čuvaju presliku svake izdane potvrde u trajanju od najmanje godinu dana.

VII. IZDAVANJE KARTICA

Postupci izdavanja kartica ustrojeni u državama članicama moraju biti u skladu sa sljedećim:

262 Broj kartice prvog izdavanja kartice tahografa tražitelju mora imati redni indeks (ako je primjereno) i indeks zamjene, te indeks ponovnog izdavanja postavljen na ‚0'.

263 Brojevi kartica svih nepersonaliziranih kartica tahografa koje se izdaju jednom nadzornom tijelu ili jednoj radionici ili jednom prijevozniku moraju imati istih prvih 13 znamenaka, te različit redni indeks.

264 Kartica tahografa koja se izdaje kao zamjena za postojeću karticu tahografa mora imati isti broj kartice kao i kartica koju zamjenjuje, osim indeksa zamjene koji se uvećava za 1 (redoslijedom 0, …, 9, A, …, Z).

265 Kartica tahografa koja se izdaje kao zamjena za postojeću karticu tahografa mora imati isti datum isteka valjanosti kartice kao i kartica koju zamjenjuje.

266 Kartica tahografa koja se izdaje zbog ponovnog izdavanja postojeće kartice tahografa mora imati isti broj kartice kao i kartica koja se obnavlja, osim indeksa ponovnog izdavanja koji se uvećava za 1 (redoslijedom 0, …, 9, A, …, Z).

267 Zamjena postojeće kartice tahografa radi izmjene administrativnih podataka slijedi ista pravila obnavljanja ako se obavlja unutar iste države članice odnosno pravila prvog izdavanja ako istu obavlja druga država članica.

268 Rubrika ‚prezime nositelja kartice' za personalizirane kartice radionice ili nadzorne kartice se popunjavaju nazivom radionice ili nadzornog tijela.

VIII. TIPNO ODOBRENJE TAHOGRAFA I KARTICA TAHOGRAFA

1. **Općenito**

Za potrebe ovog poglavlja, riječ ‚tahograf' znači ‚tahograf ili njegove sastavne dijelove'. Tipno odobrenje nije potrebno za vodiče koji povezuju senzor kretanja s jedinom u vozilu. Papir koji se koristi u tahografu smatra se sastavnim dijelom tahografa.

269 Tahograf se podnosi za tipno odobrenje zajedno sa svim integriranim dodatnim uređajima.

270 Tipno odobrenje tahografa i kartica tahografa mora uključivati sigurnosne provjere, provjere funkcionalnosti i interoperabilnosti. Pozitivni rezultati svih ovih provjera se utvrđuju u odgovarajućoj potvrdi.

271 Tijelo vlasti država članica zaduženo za tipno odobrenje neće izdati potvrdu o tipnom odobrenju u skladu s člankom 5. ove Uredbe ako nemaju:

— sigurnosnu potvrdu,

— potvrdu o funkcionalnosti,

— i potvrdu o interoperabilnosti

za tahograf ili karticu tahografa koja je predmet zahtjeva za tipno odobrenje.

272 Svaka izmjena softverske ili hardverske opreme tahografa, ili naravi materijala korištenih za njegovu izradu mora prije korištenja biti prijavljena tijelu koje je izvršilo tipno odobrenje opreme. To nadležno tijelo mora potvrditi proizvođaču proširenje tipnog odobrenja ili može zatražiti ažuriranje ili odgovarajuće potvrde o funkcionalnosti, sigurnosti i/ili interoperabilnosti.

273 Postupak softverske nadogradnje tahografa na licu mjesta, odobrava tijelo koje je izvršilo tipno odobrenje tahografa. Nadogradnja softvera ne smije mijenjati ili brisati niti jedan podatak o aktivnosti vozača pohranjen u tahografu. Softver se može nadograđivati samo pod odgovornosti proizvođača uređaja.

2. **Sigurnosna potvrda**

274 Sigurnosna potvrda se izdaje u skladu s odredbama Dodatka 10. ovom Prilogu.

3. **Potvrda o funkcionalnosti**

275 Svaki pristupnik za tipno odobrenje mora dostaviti tijelu države članice odgovornom za tipno odobrenje sve materijale i dokumente koje tijelo smatra potrebnima.

276 Potvrda o funkcionalnosti se izdaje proizvođaču tek nakon uspješnog okončanja najmanje onih provjera funkcionalnosti koje su navedene u Dodatku 9.

277 Tijelo za tipno odobrenje izdaje potvrdu o funkcionalnosti. Osim naziva korisnika i identifikacije modela, ta potvrda detaljno opisuje izvršene provjere i postignute rezultate.

4. **Potvrda o interoperabilnosti**

278 Provjera interoperabilnosti se provodi u jednom od laboratorija pod nadležnošću i odgovornosti Europske komisije.

279 Laboratorij mora upisati zahtjeve za provjeru interoperabilnosti koje podnose proizvođači kronološkim redom njihovog pristizanja.

280 Zahtjevi se službeno upisuju samo kada laboratorij dođe u posjed:

— cjelokupnog niza materijala i dokumenata potrebnih za takvo ispitivanje interoperabilnosti,

— odgovarajuće potvrde o sigurnosti,

— odgovarajuće potvrde o funkcionalnosti.

Datum upisa zahtjeva se prijavljuje proizvođaču.

281 Laboratorij ne smije izvršiti provjeru interoperabilnosti tahografa ili kartice tahografa za koje nije izdan sigurnosna potvrda i potvrda o funkcionalnosti.

282 Svaki proizvođač koji traži provjeru interoperabilnosti mora se obvezati da će laboratoriju zaduženom za takve provjere ostaviti cjelokupan niz materijala i dokumenata koje je pribavio radi provedbe provjera.

283 Provjere interoperabilnosti moraju se izvesti u skladu s odredbama točke 5. Dodatka 9. ovom Prilogu, na svim vrstama tahografa odnosno kartica tahografa:

— za koje tipno odobrenje još vrijedi, ili

— za koje je tipno odobrenje u tijeku i koji imaju važeću potvrdu o interoperabilnosti.

284 Potvrdu o interoperabilnosti laboratorij izdaje proizvođaču tek nakon uspješnog prolaska svih provjera interoperabilnosti.

285 Ako provjere interoperabilnosti na jednom ili više tahografa ili kartice(a) tahografa nisu bila uspješne prema zahtjevu 283, potvrda o interoperabilnosti se ne smije izdati prije nego proizvođač koji je podnio zahtjev ne izvrši potrebne izmjene i prođe provjeru interoperabilnosti. Laboratorij uz pomoć proizvođača kojih se tiče ova pogreška interoperabilnosti utvrđuje uzrok problema te pokušava pomoći proizvođaču podnositelju zahtjeva da iznađe tehničko rješenje. Ako je proizvođač izmijenio svoj proizvod, odgovornost je proizvođača da utvrdi kod nadležnih tijela vrijede li još uvijek potvrde o sigurnosti i uvjerenje o funkcionalnosti.

286 Potvrda o interoperabilnosti vrijedi šest mjeseci. Na kraju tog razdoblja ona se opoziva ako proizvođač nije dobio odgovarajuću potvrdu o tipnom odobrenju. Proizvođač ga dostavlja tijelu države članice ovlaštenom za tipno odobrenje koje je izdalo potvrdu o funkcionalnosti.

287 Niti jedan element koji bi mogao biti ishodište neuspjeha provjere interoperabilnosti se ne smije koristiti za postizanje dobiti ili za preuzimanje vodećeg položaja.

5. **Potvrda o tipnom odobrenju**

288 Tijelo države članice ovlašteno za tipno odobrenje može izdati potvrdu o tipnom odobrenju čim zaprimi tri potrebna uvjerenja.

289 Tijelo ovlašteno za izdavanje tipnog odobrenja, potvrdu o tipnom odobrenju mora istodobno dostaviti laboratoriju zaduženom za provjeru interoperabilnosti i proizvođaču.

290 Laboratorij nadležan za provjeru interoperabilnosti mora imati javnu internet stranicu na kojoj će se ažurirati popis modela tahografa ili kartica tahografa:

— za koje je upisan zahtjev za provjeru interoperabilnosti,

— kojima je izdana potvrda o interoperabilnosti (čak i privremena),

— kojima je izdana potvrda o tipnom odobrenju.

6. **Izvanredni postupak: prva provjera interoperabilnosti**

291 Do isteka četiri mjeseca od izdavanja potvrde o interoperabilnosti za prvi par tahografa i kartica tahografa (kartica vozača, kartica radionice, nadzorna kartica i kartica prijevoznika), svaka izdana potvrda (uključujući i prvu) u vezi zahtjeva upisanih u tom razdoblju se smatra privremenom.

292 Ako na kraju tog razdoblja svi predmetni proizvodi budu međusobno interoperabilni, sve odgovarajuće potvrde o interoperabilnosti postaju konačne.

293 Ako se tijekom tog razdoblja utvrde pogreške interoperabilnosti, laboratorij zadužen za provjeru interoperabilnosti mora utvrditi uz pomoć svih uključenih proizvođača uzroke problema, te ih mora pozvati da izvrše potrebne izmjene.

294 Ako se po isteku tog razdoblja problemi interoperabilnosti nastave, laboratorij zadužen za provjeru interoperabilnosti, u suradnji sa svim zainteresiranim proizvođačima i tijelima ovlaštenim za tipno odobrenje koja su izdala odgovarajuće potvrde o funkcionalnosti moraju iznaći uzrok pogrešaka interoperabilnosti i utvrditi koje izmjene svaki od dotičnih proizvođača treba izvršiti. Iznalaženje tehničkih rješenja može trajati najdulje dva mjeseca, nakon čega će Komisija, ako se ne iznađe nikakvo zajedničko rješenje, nakon dogovora s laboratorijem zaduženim za provjeru interoperabilnosti, odlučiti koji će tahograf(i) i kartice dobiti konačnu potvrdu o interoperabilnosti i navesti razloge.

295 Svaki zahtjev za provjeru interoperabilnosti upisan od strane laboratorija između kraja četveromjesečnog razdoblja nakon izdavanja prve privremene potvrde o interoperabilnosti i datuma odluke Komisije iz zahtjeva 294 se mora odgoditi dok se ne riješe prvi problemi interoperabilnosti. Takvi zahtjevi se potom obrađuju kronološkim redom njihovog upisivanja.

Dodatak 1.

PODATKOVNI RJEČNIK

SADRŽAJ

1. UVOD

Ovaj Dodatak definira format podataka, elemente podataka i strukturu podataka za primjenu u tahografima i karticama tahografa.

1.1. **Pristup definiranju vrsta podataka**

U ovom se dodatku za definiranje vrsta podataka koristi ASN.1 (Abstract Syntax Notation One). To omogućuje definiranje jednostavnih i strukturiranih podataka, bez impliciranja posebne sintakse prijenosa (pravila šifriranja) koja bi bila ovisna o aplikaciji i okruženju.

Dogovori o nazivlju tipa ASN.l su u skladu s normom ISO/IEC 8824-1. To znači da:

— gdje je moguće, značenje vrste podataka se naslućuje iz odabranih naziva,

— ako je vrsta podataka kombinacija različitih vrsta podataka, naziv vrste podataka i dalje je jedinstveni niz slovnih znakova koji počinje velikim slovom, međutim velika slova se u imenima koriste kako bi naglasilo odgovarajuće značenje,

— nazivi vrsta podataka općenito su vezani uz naziv vrste podataka iz kojih su izvedeni, uređaj u kojemu su podaci pohranjeni, te funkciju vezanu uz podatke.

Ako je vrsta podataka po ASN.l već definirana u okviru neke druge norme, a važna je za korištenje u tahografu, ta ASN.1 vrsta podataka definirat će se u ovom Dodatku.

Kako bi se dopustilo više vrsta pravila šifriranja, neke ASN.1 vrste podataka, u ovom Dodatku su ograničene identifikatorima raspona vrijednosti. Identifikatori raspona vrijednosti su definirani u stavku 3.

1.2. **Literatura**

U ovom Dodatku koriste se sljedeći izvori:

ISO 639	Kodeks o prikazivanju naziva jezika. Prvo izdanje: 1988
EN 726-3	Sistemi identifikacijskih kartica – Telekomunikacijske kartice i terminali s integriranim krugovima – 3. dio: Zahtjevi za kartice, koje ne ovise o aplikaciji, prosinac 1994.
ISO 3779	Cestovna vozila – Identifikacijski broj vozila (VIN) – Sadržaj i struktura. 3. izdanje: 1983.
ISO/IEC 7816-5	Informacijska tehnologija – Identifikacijske kartice – Kontaktna(e) kartica(e) s integriranim krugovima – 5. dio: Sustav numeriranja i postupak registracije za identifikatore aplikacija. Prvo izdanje: 1994. + Dopuna 1: 1996.
ISO/IEC 8824-1	Informacijska tehnologija – Sažeti sintaktički zapis 1 (ASN.l): Specifikacije osnovnog zapisa. 2. izdanje: 1998.
ISO/IEC 8825-2	Informacijska tehnologija – Pravila šifriranja ASN.l: specifikacije pravila paketnog kodiranja (PER).2. izdanje: 1998.
ISO/IEC 8859-1	Informacijska tehnologija – Skupine 8-bitnih jednobajtnih šifriranih grafičkih znakova – 1. dio: skupina latinica br. 1. Prvo izdanje: 1998.
ISO/IEC 8859-7	Informacijska tehnologija – Skupine 8-bitnih jednobajtnih šifriranih grafičkih znakova – 7. dio: latinica/grčka abeceda. Prvo izdanje: 1987.
ISO 16844-3	Cestovna vozila – Tahografski sustavi – Sučelje senzora kretanja WD 3-20/05/99.

2. DEFINICIJE VRSTA PODATAKA

Za svaku od sljedećih vrsta podataka standardna vrijednost sadržaja ‚nepoznato' ili ‚ne primjenjuje se' se sastoji u popunjavanju elementa s ‚FF' bajtima.

2.1. **ActivityChangeInfo**

Ova vrsta podataka omogućuje šifriranje, u okviru dvobajtne riječi, statusa utora u 00:00 sati i/ili statusa vozača u 00:00 sati i/ili promjene aktivnosti i/ili promjene statusa vožnje i/ili promjene statusa kartice vozača ili kartice suvozača. Ova se vrsta podataka odnosi na zahtjeve 084, 109a, 199 i 219.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Dodjela vrijednosti – oktetno poravnanje: 'scpaattttttttttt'B (16 bita)

Za zapise u podatkovnoj memoriji (ili status utora):

's'B	utor:
	'0'B: VOZAČ,
	'1'B: SUVOZAČ,
'c'B	Status vožnje:
	'0'B: JEDAN VOZAČ,
	'1'B: POSADA,
'p'B	Status kartice vozača (ili kartice radionice) u odgovarajućem utoru:
	'0'B: UMETNUTA, kartica je umetnuta,
	'1'B: NIJE UMETNUTA, kartica nije umetnuta (ili je kartica izvađena),
'aa'B	Aktivnost:
	'OO'B: PAUZA/ODMOR,
	'O1'B: PRIPRAVNOST,
	'10'B: RAD,
	'11'B: VOŽNJA,
'ttttttttttt'B	Vrijeme promjene: broj minuta od 00h00 određenog dana.

Za zapise na kartici vozača (ili kartici radionice) (i status vozača):

's'B	Utor (ne vrijedi kada je 'p' = 1, osim prema donjoj napomeni):	
	'0'B: VOZAČ,	
	'1'B: 2. SUVOZAČ,	
'c'B	Status vožnje (slučaj 'p' = 0) ili	Naredni status aktivnosti (slučaj 'p' = 1):
	'0'B: JEDAN VOZAČ,	'0'B: NEPOZNATO
	'1'B: POSADA,	'1'B: POZNATO (= ručno uneseno)
'p'B	Status kartice:	
	'0'B: UMETNUTA, kartica je umetnuta u tahograf;	
	'1'B: NIJE UMETNUTA, kartica nije umetnuta (ili je kartica izvađena),	

'aa'B Aktivnost (ne vrijedi kada je 'p' = 1 i ‚c ‚= 0, osim prema donjoj napomeni:

'00'B: PAUZA/ODMOR,

'01'B: PRIPRAVNOST,

'10'B: RAD,

'11'B: VOŽNJA,

'ttttttttttt' B Vrijeme promjene: broj minuta nakon 00h00 određenog dana.

Napomena za slučaj ‚vađenja kartice':

Kad se kartica izvadi:

— ‚s' vrijedi i označuje utor iz kojeg je kartica izvađena,

— ‚c' se mora postaviti na 0,

— ‚p' se mora postaviti na 1,

— ‚aa' mora šifrirati tekuću aktivnost, izabranu u to vrijeme,

Kao rezultat ručnog unosa, bitovi riječi ‚c' i ‚aa' (pohranjeni na kartici) mogu se kasnije prepisati preko postojećih zapisa.

2.2. **Address**

Adrese.

```
Address ::= SEQUENCE {
    codePage                                    INTEGER (0..255),
    address                                     OCTET STRING (SIZE(35))
}
```

codePage navodi dio ISO/IEC 8859 koji se koristi za šifriranje adrese.

address je adresa šifrirana u skladu s ISO/IEC 8859 kodnom stranicom.

2.3. **BCDString**

BCDString se primjenjuje za prikaz binarno kodiranih decimalnih brojeva (BCD). Ova podatkovna vrsta se koristi za predstavljanje jednodecimalne znamenke u jednom poluoktetu (4 bita). BCDString se temelji na ISO/IEC 8824-1 ‚CharacterString Type'.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
    identification ( WITH COMPONENTS {
    fixed PRESENT }) })
```

BCDString koristi zapis ‚hstring'. Krajnja lijeva heksadecimalna znamenka mora biti najznačajniji poluoktet prvog okteta. Višekratnik okteta tvori se tako da se prema potrebi umetne poluoktet sa završnim nulama od mjesta lijevog poluokteta u prvom oktetu.

Dopuštene znamenke su: 0, 1, … 9.

2.4. **CalibrationPurpose**

Šifra pojašnjava zašto je zabilježen niz parametara kalibriranja. Ova podatkovna vrsta je vezana uz zahtjeve 097 i 098.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti:

‚00'H rezervirana vrijednost,

‚01'H aktivacija: bilježenje poznatih parametara kalibracije u trenutku aktivacije jedinice vozila,

‚02'H prva ugradnja: prva kalibracija u jedinici vozila nakon aktivacije,

‚03'H ugradnja: prva kalibracija jedinice vozila u sadašnjem vozilu,

‚04'H periodični nadzor.

2.5 **CardActivityDailyRecord**

Informacija pohranjena na kartici koja se odnosi na aktivnost vozača na određeni kalendarski dan. Ova vrsta podataka je povezana sa zahtjevima 199 i 219.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength            INTEGER(0..CardActivityLengthRange),
   activityRecordLength                    INTEGER(0..CardActivityLengthRange),
   activityRecordDate                      TimeReal,
   activityDailyPresenceCounter            DailyPresenceCounter,
   activityDayDistance                     Distance,
   activityChangeInfo                      SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength je ukupna duljina prethodnog dnevnog zapisa u bajtima. Najveća vrijednost je iskazana u duljini OCTET STRING koja sadrži takve zapise (vidjeti CardActivityLengthRange, stavak 3). Kad je taj zapis najstariji dnevni zapis, vrijednost activityPreviousRecordLength mora biti postavljena na 0.

activityRecordLength je ukupna duljina tog zapisa u bajtima. Najveća vrijednost je dana duljinom OCTET STRING koja sadrži navedene zapise.

activityRecordDate je datum zapisa.

activityDailyPresenceCounter je dnevni brojač prisutnosti kartica za taj dan.

activityDayDistance je ukupna prijeđena udaljenost na taj dan.

activityChangeInfo je skupina podataka ActivityChangeInfo za vozača za taj dan. Može sadržavati najviše 1 440 vrijednosti (jedna promjena aktivnosti na minutu). Ta skupina uvijek uključuje i activityChangeInfo koja šifrira status vozača u 00:00.

2.6 **CardActivityLengthRange**

Broj bajta na kartici vozača ili kartici radionice raspoloživih za spremanje zapisa o aktivnosti vozača.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: vidjeti stavak 3.

2.7. **CardApprovalNumber**

Broj tipnog odobrenja kartice.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: Nije utvrđeno.

2.8. **CardCertificate**

Certifikat javnog ključa kartice.

```
CardCertificate ::= Certificate
```

2.9 **CardChipIdentification**

Informacija pohranjena na kartici koja se odnosi na identifikaciju integriranog kruga (IC) kartice (zahtjev 191).

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                  OCTET STRING (SIZE(4)),
   icManufacturingReferences       OCTET STRING (SIZE(4))
}
```

icSerialNumber je serijski broj IC, kako je utvrđeno u EN 726-3.

icManufacturingReferences je identifikator proizvođača IC i ugradbenih elemenata, kako je utvrđeno u EN 726-3.

2.10. **CardConsecutiveIndex**

Redni indeks kartice (definicija h).

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

Dodjela vrijednosti: (vidjeti poglavlje VII. ovog Priloga).

Redoslijed uvećavanja:: ‚0…9, A…Z, a…z'.

2.11. **CardControlActivityDataRecord**

Informacija pohranjena na kartici vozačaj ili kartici radionice koja se odnosi na posljednju kontrolu kojoj je vozač bio podvrgnut (zahtjevi 210 i 225).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                          controlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   controlVehicleRegistration           VehicleRegistrationIdentification,
   controlDownloadPeriodBegin           TimeReal,
   controlDownloadPeriodEnd             TimeReal
}
```

controlType je vrsta nadzora.

controlTime je datum i vrijeme nadzora.

controlCardNumber je FullCardNumber službenika za nadzor koji je izvršio nadzor.

controlVehicleRegistration je registracijski broj vozila i država članica registracije vozila na kojemu je obavljen nadzor.

controlDownloadPeriodBegin i **controlDownloadPeriodEnd** je razdoblje za koje su preuzeti podaci, u slučaju preuzimanja podataka.

2.12. **CardCurrentUse**

Informacija o trenutačnom korištenju kartice (zahtjev 212).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                      TimeReal,
   sessionOpenVehicle                   VehicleRegistrationIdentification
}
```

sessionOpenTime je vrijeme kada je kartica umetnuta radi trenutačnog korištenja. Pri vađenju kartice ovaj se element postavlja na nulu.

sessionOpenVehicle je identifikacija trenutačno korištenog vozila koja se postavlja umetanjem kartice. Pri vađenju kartice ovaj se element postavlja na nulu.

2.13. **CardDriverActivity**

Informacija pohranjena na kartici vozača ili kartici radionice koja se odnosi na aktivnosti vozača (zahtjevi 199 i 219).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord       INTEGER(0..CardActivityLengthRange-1),
   activityPointerNewestRecord          INTEGER(0..CardActivityLengthRange-1),
   activityDailyRecords                 OCTET STRING
                                        (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord je određivanje početka prostora za spremanje (broj bajta od početka niza) najstarijeg punog dnevnog zapisa u nizu activityDailyRecords. Najveću vrijednost prikazuje duljina niza.

activityPointerOldestDayRecord je određivanje početka prostora za spremanje (broj bajta od početka niza) najnovijeg dnevnog zapisa u nizu activityDailyRecords. Najveću vrijednost prikazuje duljina niza.

activityDailyRecords je prostor raspoloživ za čuvanje podataka o aktivnostima vozača (struktura podataka: CardActivityDailyRecord) za svaki kalendarski dan u kojemu je kartica korištena.

Dodjela vrijednosti: taj se oktetni niz ciklički popunjava zapisima CardActivityDailyRecord. Pri prvom korištenju spremanje započinje s prvim bajtom niza. Svi novi zapisi se stavljaju na kraj prethodnog. Kad se niz popuni, spremanje se nastavlja u prvi bajt niza bez obzira na prekid u podatkovnom elementu. Prije stavljanja u niz novih podataka o aktivnostima (povećanje postojeće activityDailyRecord ili stavljanje nove activityDailyRecord), koji zamjenjuju stare podatke o aktivnostima, potrebno je ažurirati activityPointerOldestDayRecord tako da odražava novo mjesto najstarijeg punog dnevnog zapisa, a activityPreviousRecordLength takvog (novog) najstarijeg potpunog dnevnog zapisa ponovo postaviti na 0.

2.14. **CardDrivingLicenceInformation**

Informacija pohranjena na kartici vozača, koja se odnosi na podatke o vozačkoj dozvoli nositelja kartice (zahtjev 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority          Name,
   drivingLicenceIssuingNation             NationNumeric,
   drivingLicenceNumber                    IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority je tijelo ovlašteno za izdavanje vozačke dozvole.

drivingLicenceIssuingNation je državna pripadnost tijela koje je izdalo vozačku dozvolu.

drivingLicenceNumber je broj vozačke dozvole.

2.15. **CardEventData**

Informacija pohranjena na kartici vozača ili kartici radionice koja se odnosi na slučajeve vezane uz nositelja kartice (zahtjevi 204 i 223).

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

CardEventData je slijed, poredan prema rastućoj vrijednosti EventFaultType, zapisa cardEventRecords (osim o pokušajima probijanja zaštite koji su skupljeni u posljednjem nizu slijeda).

cardEventRecords je niz zapisa o događajima određene vrste (ili kategorija događaja pokušaja probijanja zaštite).

2.16. **CardEventRecord**

Informacija pohranjena na kartici vozača ili kartici radionice koja se odnosi na slučaj vezan uz nositelja kartice (zahtjevi 205 i 223).

```
CardEventRecord ::= SEQUENCE {
   eventType                               EventFaultType,
   eventBeginTime                          TimeReal,
   eventEndTime                            TimeReal,
   eventVehicleRegistration                VehicleRegistrationIdentification
}
```

eventType je vrsta događaja.

eventBeginTime je datum i vrijeme početka događaja.

eventEndTime je datum i vrijeme završetka događaja.

eventVehicleRegistration je registracijska oznaka vozila i država članica registracije vozila u kojem se događaj dogodio.

2.17. **CardFaultData**

Informacija pohranjena na kartici vozača ili kartici radionice koja se odnosi na pogreške vezane uz nositelja kartice (zahtjevi 207 i 223).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                    SET SIZE(NoOfFaultsPerType) OF
                                       CardFaultRecord
}
```

cardFaultData je slijed niza zapisa o pogreškama tahografa iza kojeg slijedi niz zapisa o pogreškama kartice.

cardFaultRecords je niz zapisa o pogreškama određene kategorije pogrešaka (tahografa ili kartica).

2.18. **CardFaultRecord**

Informacija pohranjena na kartici vozača ili kartici radionice koja se odnosi na pogreške vezane uz nositelja kartice (zahtjevi 208 i 223).

```
CardFaultRecord ::= SEQUENCE {
   faultType                           EventFaultType,
   faultBeginTime                      TimeReal,
   faultEndTime                        TimeReal,
   faultVehicleRegistration            VehicleRegistrationIdentification
}
```

faultType je vrsta pogreške.

faultBeginTime je datum i vrijeme početka pogreške.

faultEndTime je datum i vrijeme završetka pogreške.

faultVehicleRegistration je registracijski broj vozila i država članica registracije vozila u kojemu je nastala pogreška.

2.19. **CardIccIdentification**

Informacija pohranjena na kartici koja se odnosi na identifikaciju integriranog kruga (IC) kartice (zahtjev 192).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                           OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardApprovalNumber                  CardApprovalNumber
   cardPersonaliserID                  OCTET STRING (SIZE(1)),
   embedderIcAssemblerId               OCTET STRING (SIZE(5)),
   icIdentifier                        OCTET STRING (SIZE(2))
}
```

clockStop je režim Clockstop definiran u EN 726-3.

cardExtendedSerialNumber obuhvaća serijski broj IC i podatke o proizvodnji IC utvrđene u EN 726-3 i kako je podrobnije određeno vrstom podataka ExtendedSerialNumber.

cardApprovalNumber je broj tipnog odobrenja kartice.

cardPersonaliserID je ID personalizatora kartice, definiran u EN 726-3.

embedderIcAssemblerId je identifikator ugraditelja/instalatera IC, kako je definirano u EN 726-3.

icIdentifier je identifikator IC na kartici i proizvođača njezinog IC, kako je definirano u EN 726-3.

2.20. **CardIdentification**

Informacija pohranjena na kartici koja se odnosi na identifikaciju kartice (zahtjevi 194, 215, 231, 235).

```
CardIdentification ::= SEQUENCE
   cardIssuingMemberState                  NationNumeric,
   cardNumber                              CardNumber,
   cardIssuingAuthorityName                Name,
   cardIssueDate                           TimeReal,
   cardValidityBegin                       TimeReal,
   cardExpiryDate                          TimeReal
}
```

cardIssuingMemberState je oznaka države članice koja je izdala karticu.

cardNumber je broj kartice.

cardIssuingAuthorityName je naziv tijela koje je izdalo karticu.

cardIssueDate je datum izdavanja kartice sadašnjem nositelju.

cardValidityBegin je datum početka valjanosti kartice.

cardExpiryDate je datum isteka valjanosti kartice.

2.21. **CardNumber**

Broj kartice prema definiciji g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification                 IA5String(SIZE(14)),
      cardReplacementIndex                 CardReplacementIndex,
      cardRenewalIndex                     CardRenewalIndex
   }
   SEQUENCE {
      ownerIdentification                  IA5String(SIZE(13)),
      cardConsecutiveIndex                 CardConsecutiveIndex,
      cardReplacementIndex                 CardReplacementIndex,
      cardRenewalIndex                     CardRenewalIndex
   }
}
```

driverIdentification je jedinstvena identifikacija vozača u državi članici.

ownerIdentification je jedinstvena identifikacija prijevoznika ili radionice ili nadzornog tijela u državi članici.

cardConsecutiveIndex je redni indeks kartice.

cardConsecutiveIndex je zamjenski indeks kartice.

cardConsecutiveIndex je indeks obnavljanja kartice.

Prvi slijed izbora je prikladan za šifriranje broja kartice vozača, drugi slijed izbora je prikladan za šifriranje brojeva kartice radionice, nadzorne kartice i kartice prijevoznika.

2.22. **CardPlaceDailyWorkPeriod**

Informacija pohranjena na kartici vozača ili kartici radionice koja se odnosi na mjesta početka i/ili završetka dnevnog razdoblja rada (zahtjevi 202 i 221).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord                INTEGER(0..NoOfCardPlaceRecords-1),
   placeRecords                            SET SIZE(NoOfCardPlaceRecords) OF PlaceRe-
                                           cord
}
```

placePointerNewestRecord je indeks posljednjeg ažuriranog zapisa mjesta.

Pripisivanje vrijednosti: Broj koji odgovara numeratoru zapisa mjesta, koji počinje s ‚0' za prvu pojavu zapisa mjesta u strukturi.

placeRecords je niz zapisa koja sadrži informacije o upisanim mjestima.

2.23. **CardPrivateKey**

Privatni ključ kartice.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24. **CardPublicKey**

Javni ključ kartice.

```
CardPublicKey ::= PublicKey
```

2.25. **CardRenewalIndex**

Indeks obnavljanja kartice (definicija i).

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

Dodjela vrijednosti: (vidjeti poglavlje VII. ovog Priloga).

‚0' prvo izdavanje.

Redoslijed uvećavanja: ‚0, …,9, A, …,Z'.

2.26. **CardReplacementIndex**

Indeks zamjene kartice (definicija j).

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

Dodjela vrijednosti: (vidjeti poglavlje VII. ovog Priloga).

‚0' izvorna kartica.

Redoslijed uvećavanja: ‚0, …,9, A, …,Z'.

2.27. **CardSlotNumber**

Razlikovna šifra za raspoznavanje između dvaju utora jedinice u vozilu.

```
CardSlotNumber ::= INTEGER {
   driverSlot                              (0),
   co-driverSlot                           (1)
}
```

Dodjela vrijednosti: nije podrobnije određena.

2.28. **CardSlotsStatus**

Šifra koja označuje vrstu kartica umetnutih u dva utora jedinice u vozilu.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti – oktetni poredak: 'ccccdddd'B:

'cccc'B Identifikacija vrste kartice umetnute u utor suvozača,

'dddd'B Identifikacija vrste kartice umetnute u utor vozača,

sa sljedećim identifikacijskim šiframa:

'0000'B nije umetnuta kartica,

'0001'B umetnuta je kartica vozača,

'0010'B umetnuta je kartica radionice,

'0011'B umetnuta je nadzorna kartica,

'0100'B umetnuta je kartica prijevoznika.

2.29. **CardStructureVersion**

Oznaka koja prikazuje inačicu primijenjene strukture na kartici tahografa.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Dodjela vrijednosti: 'aabb'H:

'aa'H indeks izmjena strukture,

'bb'H indeks izmjena pri korištenju podatkovnih elemenata utvrđenih za strukturu prikazanu gornjim bajtom.

2.30. **CardVehicleRecord**

Informacija pohranjena na kartici vozača ili kartici radionice, koja se odnosi na razdoblje korištenja vozila tijekom jednog kalendarskog dana (zahtjevi 197 i 217).

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin je stanje brojača kilometara vozila na početku razdoblja korištenja vozila.

vehicleOdometerEnd je stanje brojača kilometara vozila na kraju razdoblja korištenja vozila.

vehicleFirstUse je datum i vrijeme početka razdoblja korištenja vozila.

vehicleLastUse je datum i vrijeme završetka razdoblja korištenja vozila.

vehicleRegistration je registracijska oznaka vozila i država registracije vozila.

vuDataBlockCounter je vrijednost VuDataBlockCounter pri posljednjem razdoblju korištenja vozila.

2.31. **CardVehiclesUsed**

Informacija pohranjena na kartici vozača ili kartici radionice, koja se odnosi na vozila koja je koristio nositelj kartice (zahtjevi 197 i 217).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord              INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                      SET SIZE(NoOfCardVehicleRecords) OF
                                           CardVehicleRecord
}
```

vehiclePointerNewestRecord je indeks posljednjeg ažuriranog zapisa o vozilu.

Pripisivanje vrijednosti: Broj koji odgovara numeratoru zapisa o vozilu koji počinje s ‚0' za prvo pojavljivanje u strukturi zapisa o vozilu.

cardVehicleRecords je niz zapisa s podacima o korištenim vozilima.

2.32. **Certificate**

Certifikat javnog ključa, izdan od certifikacijske vlasti.

```
Certificate ::= OCTET STRING (SIZE(194))
```

Dodjela vrijednosti: digitalni potpis s djelomičnim obnavljanjem CertificateContent u skladu s Dodatkom 11. ‚Zajednički sigurnosni mehanizmi': Potpis (128 bajta) || Preostali dio javnog ključa (58 bajta) || Oznaka certifikacijske vlasti (8 bajta).

2.33. **CertificateContent**

(Jasan) sadržaj certifikata javnog ključa u skladu s Dodatkom 11. ‚Zajednički sigurnosni mehanizmi'.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier             INTEGER(0..255),
   certificationAuthorityReference          KeyIdentifier,
   certificateHolderAuthorisation           CertificateHolderAuthorisation,
   certificateEndOfValidity                 TimeReal,
   certificateHolderReference               KeyIdentifier,
   publicKey                                PublicKey
}
```

certificateProfileIdentifier je inačica odgovarajućeg certifikata.

Dodjela vrijednosti: ‚01h' za takvu inačicu.

certificationAuthorityReference identificira certifikacijsku vlast koja je izdala certifikat. Također upućuje na javni ključ te certifikacijske vlasti.

certificateHolderAuthorisation identificira prava nositelja certifikata.

certificateEndOfValidity je datum administrativnog isteka valjanosti certifikata.

certificateHolderReference identificira nositelja certifikata. Također upućuje na njegov javni ključ.

publicKey je javni ključ koji se potvrđuje tim certifikatom.

2.34. **CertificateHolderAuthorisation**

Identifikacija prava nositelja certifikata.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID                  OCTET STRING(SIZE(6))
   equipmentType                            EquipmentType
}
```

tachographApplicationID je identifikator aplikacije za tahografsku aplikaciju.

Dodjela vrijednosti: ‚FFh' ‚54h' ‚41h' ‚43h' ‚48h' ‚4Fh'. Taj AID je vlasnički neregistrirani identifikator aplikacije u skladu s ISO/IEC 7816-5.

equipmentType je identifikacija tipa uređaja za koji je certifikat namijenjen.

dodjela vrijednosti: u skladu s vrstom podatka EquipmentType. Vrijednost 0 ako je certifikat od jedne države članice.

2.35. **CertificateRequestID**

Jedinstveni identifikator zahtjeva za certifikat. Može se također koristiti kao identifikator javnog ključa jedinice u vozilu ako u trenutku generiranja certifikata nije poznat serijski broj jedinice u vozilu za koju je ključ namijenjen.

```
CertificateRequestID ::= SEQUENCE {
   requestSerialNumber                    INTEGER(0..2^32-1)
   requestMonthYear                       BCDString(SIZE(2))
   crIdentifier                           OCTET STRING(SIZE(1))
   manufacturerCode                       ManufacturerCode
}
```

requestSerialNumber je serijski broj zahtjeva za certifikat, jedinstven za proizvođača i niže navedeni mjesec.

requestMonthYear je identifikacija mjeseca i godine zahtjeva za certifikat.

Dodjela vrijednosti: šifra BCD za mjesec (dvije znamenke) i godinu (zadnje dvije znamenke).

crIdentifier: je identifikator za raspoznavanje zahtjeva za certifikat od proširenog serijskog broja.

Dodjela vrijednosti: ‚FFh'.

manufacturerCode: je brojčana šifra proizvođača koji traži certifikat.

2.36. **CertificationAuthorityKID**

Identifikator javnog ključa certifikacijske vlasti (države članice ili europske certifikacijske vlasti).

```
CertificationAuthorityKID ::= SEQUENCE {
   nationNumeric                          NationNumeric
   nationAlpha                            NationAlpha
   keySerialNumber                        INTEGER(0..255)
   additionalInfo                         OCTET STRING(SIZE(2))
   caIdentifier                           OCTET STRING(SIZE(1))
}
```

nationNumeric je brojčana nacionalna šifra certifikacijske vlasti.

nationAlpha je alfanumerička nacionalna šifra certifikacijske vlasti.

keySerialNumber je serijski broj za raspoznavanje različitih ključeva certifikacijske vlasti ako dođe do promjene ključeva.

additionalInfo je dvobajtno polje za dodatno šifriranje (specifično za certifikacijsku vlast).

caIdentifier je identifikator za raspoznavanje identifikatora ključa certifikacijske vlasti od drugih identifikatora ključeva.

Pripisivanje vrijednosti: ‚01h'.

2.37. **CompanyActivityData**

Informacija pohranjena na kartici prijevoznika koja se odnosi na aktivnosti izvršene s karticom (zahtjev 237).

```
CompanyActivityData ::= SEQUENCE {
  companyPointerNewestRecord          INTEGER(0..NoOfCompanyActivityRecords-1),
  companyActivityRecords              SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord               SEQUENCE {
      companyActivityType                 CompanyActivityType,
      companyActivityTime                 TimeReal,
      cardNumberInformation               FullCardNumber,
```

```
        vehicleRegistrationInformation      VehicleRegistrationIdentification,
        downloadPeriodBegin                 TimeReal,
        downloadPeriodEnd                   TimeReal
    }
}
```

companyPointerNewestRecord je indeks posljednjeg ažuriranja companyActivityRecord.

Dodjela vrijednosti: Broj koji odgovara brojaču zapisa o aktivnostima tvrtke, a koji započinje s ‚0' za prvu pojavu zapisa o aktivnostima tvrtke u strukturi.

companyActivityRecords je niz svih zapisa o aktivnostima tvrtke.

companyActivityRecord je redoslijed informacija vezanih uz jednu aktivnost tvrtke.

companyActivityType je vrsta aktivnosti tvrtke.

companyActivityTime je datum i vrijeme aktivnosti tvrtke.

cardNumberInformation je broj kartice i država članica izdavanja kartice s koje se podaci preuzimaju, ako postoji.

vehicleRegistrationInformation je registracijska oznaka vozila i država članica registracije vozila u kojemu je izvršeno preuzimanje podataka odnosno zaključavanje ili otključavanje blokade.

downloadPeriodBegin i **downloadPeriodEnd** je razdoblje preuzimanja podataka iz jedinice vozila, ako postoji.

2.38. **CompanyActivityType**

Šifra koja označuje aktivnost koju obavlja tvrtka korištenjem svoje kartice prijevoznika.

```
CompanyActivityType ::= INTEGER {
   card downloading                    (1),
   VU downloading                      (2),
   VU lock-in                          (3),
   VU lock-out                         (4)
}
```

2.39. **CompanyCardApplicationIdentification**

Informacija pohranjena na kartici prijevoznika koja se odnosi na identifikaciju primjene kartice (zahtjev 190).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId označuje vrstu primijenjene kartice.

cardStructureVersion označuje inačicu strukture primijenjene na kartici.

noOfCompanyActivityRecords je broj zapisa o aktivnostima tvrtke koje kartica može pohraniti.

2.40. **CompanyCardHolderIdentification**

Informacija pohranjena na kartici prijevoznika koja se odnosi na identifikaciju nositelja kartice (zahtjev 236).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName je naziv poduzeća nositelja kartice.

companyAddress je adresa tvrtke nositelja.

cardHolderPreferredLanguage je odabrani jezik nositelja kartice.

2.41. **ControlCardApplicationIdentification**

Informacija pohranjena na nadzornoj kartici koja se odnosi na identifikaciju primjene kartice (zahtjev 190).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                    EquipmentType,
   cardStructureVersion                      CardStructureVersion,
   noOfControlActivityRecords                NoOfControlActivityRecords
}
```

typeOfTachographCardId označuje primijenjenu vrstu kartice.

cardStructureVersion označuje inačicu strukture primijenjene na kartici.

noOfControlActivityRecords je broj zapisa o nadzornim aktivnostima koji se mogu pohraniti na kartici.

2.42. **ControlCardControlActivityData**

Informacija pohranjena na nadzornoj kartici, koja se odnosi na aktivnosti nadzora izvršene s karticom (zahtjev 233).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord             INTEGER(0..NoOfControlActivityRecords-1),
   controlActivityRecords                 SET SIZE(NoOfControlActivityRecords) OF
     controlActivityRecord                  SEQUENCE {
       controlType                            ControlType,
       controlTime                            TimeReal,
       controlledCardNumber                   FullCardNumber,
       controlledVehicleRegistration          VehicleRegistrationIdentification,
       controlDownloadPeriodBegin             TimeReal,
       controlDownloadPeriodEnd               TimeReal
     }
}
```

controlPointerNewestRecord je indeks posljednjeg ažuriranog zapisa o aktivnostima nadzora.

Dodjela vrijednosti: broj koji odgovara brojaču zapisa o aktivnostima nadzora koji počinje s ‚0' za prvu pojavu zapisa o aktivnosti nadzora u strukturi.

controlActivityRecords je niz svih zapisa o aktivnostima nadzora.

controlActivityRecord je redoslijed informacija vezanih uz jedan nadzor.

controlType je vrsta nadzora.

controlTime je datum i vrijeme nadzora.

controlledCardNumber je broj kartice i država članica izdavanja kartice koja je nadzorana.

controlledVehicleRegistration je VRN i država članica registracije vozila u kojemu je izvršen nadzor.

controlDownloadPeriodBegin i **controlDownloadPeriodEnd** je razdoblje za koje su moguće preuzeti podaci.

2.43. **ControlCardHolderIdentification**

Informacija pohranjena na nadzornoj kartici koja se odnosi na identifikaciju nositelja kartice (zahtjev 232).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                    Name,
   controlBodyAddress                 Address,
   cardHolderName                     HolderName,
   cardHolderPreferredLanguage        Language
}
```

controlBodyName je naziv nadzornog tijela nositelja kartice.

controlBodyAddress je adresa nadzornog tijela nositelja kartice.

cardHolderName je prezime i ime(na) nositelja kontrolne kartice.

cardHolderPreferredLanguage je odabrani jezik nositelja kartice.

2.44. **ControlType**

Šifra koja označuje aktivnosti koje se vrše u sklopu nadzora. Ova vrsta podataka je vezana uz zahtjeve 102, 210 i 225.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti – oktetni poredak: 'cvpdxxxx'B (8 bita)

'c'B	Identifikacija vrste kartice umetnute u utor suvozača,
	'0'B: tijekom ove aktivnosti nadzora nisu preuzeti podaci sa kartice,
	'1'B: tijekom ove aktivnosti nadzora preuzeti su podaci sa kartice
'v'B	preuzimanje podataka s jedinice vozila:
	'0'B: tijekom ove aktivnosti nadzora nisu preuzeti podaci iz jedinice vozila,
	'1'B: tijekom ove aktivnosti nadzora preuzeti su podaci iz jedinice vozila
'p'B	ispis:
	'B': tijekom ove aktivnosti nadzora nije bilo ispisa,
	'1'B: tijekom ove aktivnosti nadzora izvršen ispis
'd'B	prikaz:
	'0'B: tijekom ove aktivnosti nadzora se nije koristio zaslon,
	'1'B: tijekom ove aktivnosti nadzora se je koristio zaslon
'xxxx'B	nije korišteno.

2.45. **CurrentDateTime**

Tekući datum i vrijeme tahografa

```
CurrentDateTime ::= TimeReal
```

Dodjela vrijednosti: nije podrobnije određeno.

2.46. **DailyPresenceCounter**

Brojač pohranjen na kartici vozača ili kartici radionice uvećan za 1 za svaki kalendarski dan kada je kartica bila umetnuta u jedinicu vozila. Ova vrsta podataka je vezana uz zahtjeve 199 i 219.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Dodjela vrijednosti: Redni broj s najvišom vrijednosti = 9 999; nakon čega ponovo počinje od 0. Pri prvom izdavanju kartice broj se postavlja na 0.

2.47. **Datef**

Datum iskazan u brojčanom obliku spremnom za ispis.

```
Datef ::= SEQUENCE {
   year       BCDString(SIZE(2)),
   month      BCDString(SIZE(1)),
   day        BCDString(SIZE(1))
}
```

Dodjela vrijednosti:

yyyy	Godina
mm	Mjesec
dd	Dan

'00000000'H izričito označuje da nema datuma

2.48. **Distance**

Prijeđena udaljenost (rezultat izračuna razlike između dvaju stanja brojača kilometara u kilometrima).

```
Distance ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: nepotpisani binarni broj. Vrijednost u km u djelatnom rasponu od 0 do 9 999 km.

2.49. **DriverCardApplicationIdentification**

Informacija pohranjena na kartici vozača koja se odnosi na identifikaciju primjene kartice (zahtjev 190).

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                  EquipmentType,
   cardStructureVersion                    CardStructureVersion,
   noOfEventsPerType                       NoOfEventsPerType,
   noOfFaultsPerType                       NoOfFaultsPerType,
   activityStructureLength                 CardActivityLengthRange,
   noOfCardVehicleRecords                  NoOfCardVehicleRecords,
   noOfCardPlaceRecords                    NoOfCardPlaceRecords
}
```

typeOfTachographCardId označuje primijenjenu vrstu kartice.

cardStructureVersion označuje inačicu primijenjene strukture na kartici.

noOfEventsPerType je broj događaja po vrsti događaja koji kartica može zabilježiti.

noOfFaultsPerType je broj pogrešaka po vrsti pogreške koje kartica može zabilježiti.

activityStructureLength označuje broj raspoloživih bajtova za spremanje zapisa o aktivnostima.

noOfCardVehicleRecords je broj zapisa o vozilu koje kartica može sadržavati.

noOfCardPlaceRecords je broj mjesta koje kartica može zabilježiti.

2.50. **DriverCardHolderIdentification**

Informacija pohranjena na kartici vozača koja se odnosi na identifikaciju nositelja kartice (zahtjev 195).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                          HolderName,
   cardHolderBirthDate                     Datef,
   cardHolderPreferredLanguage             Language
}
```

cardHolderName je prezime i ime(na) nositelja kartice vozača.

cardHolderBirthDate je datum rođenja nositelja kartice vozača.

cardHolderPreferredLanguage je izabrani jezik nositelja kartice.

2.51. **EntryTypeDailyWorkPeriod**

Oznaka za raspoznavanje između početka i kraja zapisa o dnevnom razdoblju rada i stanja unosa.

```
EntryTypeDailyWorkPeriod ::= INTEGER
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Dodjela vrijednosti: prema ISO/IEC8824-1.

2.52. **EquipmentType**

Oznaka po kojoj se razlikuju vrste uređaja za tahografsku primjenu.

```
EquipmentType ::= INTEGER(0..255)
- - Reserved                          (0),
- - Driver Card                       (1),
- - Workshop Card                     (2),
- - Control Card                      (3),
- - Company Card                      (4),
- - Manufacturing Card                (5),
- - Vehicle Unit                      (6),
- - Motion Sensor                     (7),
- - RFU                               (8..255)
```

Dodjela vrijednosti: prema ISO/IEC8824-1.

Vrijednost 0 je rezervirana za označivanje države članice ili Europe u certifikacijskom polju CHA.

2.53. **EuropeanPublicKey**

Europski javni ključ.

```
EuropeanPublicKey ::= PublicKey
```

2.54. **EventFaultType**

Šifra koja određuje događaj ili pogrešku.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti:

'0x'H	Opći događaji,
'00'H	Nema podrobnijih podataka,
'01'H	Umetanje nevažeće kartice,
'02'H	Sukob kartica,
'03'H	Vremensko preklapanje,
'04'H	Vožnja bez odgovarajuće kartice,
'05'H	Umetanje kartice tijekom vožnje,
'06'H	Posljednja razmjena podataka s karticom nije pravilno završena,
'07'H	Prekoračenje brzine,

'08'H	Prekid napajanja,
'09'H	Pogreška podataka o kretanju,
'0A'H do '0F'H	RFU,
'1x'H	Slučajevi pokušaja probijanja zaštite vezani uz jedinicu u vozilu,
'10'H	Nema podrobnijih podataka,
'11'H	Neuspjela autentifikacija senzora kretanja,
'12'H	Neuspjela autentifikacija kartice tahografa,
'13'H	Neovlaštena zamjena senzora kretanja,
'14'H	Pogreška cjelovitosti ulaza podataka s kartice,
'15'H	Pogreška cjelovitosti pohranjenih podataka korisnika,
'16'H	Pogreška pri unutarnjem prijenosu podataka,
'17'H	Neovlašteno otvaranje kućišta,
'18'H	Ometanje rada softvera,
'19'H do '1F'H	RFU,
'2x'H	Događaji pokušaja probijanja zaštite vezani uz senzor,
'20'H	Nema podrobnijih podataka,
'21'H	Neuspjela autentifikacija,
'22'H	Pogreška cjelovitosti pohranjenih podataka,
'23'H	Pogreška pri unutarnjem prijenosu podataka,
'24'H	Neovlašteno otvaranje kućišta,
'25'H	Ometanja rada softvera,
'26'H do '2F'H	RFU,
'3x'H	Pogreške tahografa,
'30'H	Nema podrobnijih podataka,
'31'H	Interna pogreška jedinice vozila,
'32'H	Pogreška pisača,
'33'H	Pogreška zaslona,
'34'H	Pogreška pri preuzimanju podataka,
'35'H	Pogreška senzora,
'36'H do'3F'H	RFU
'4x'H	Pogreške kartice,
'40'H	Nema podrobnijih podataka,
'41'H do '4F'H	RFU
'50'H do '7F'H	RFU,
'80'H do 'FF'H	specifično za proizvođača.

2.55. **EventFaultRecordPurpose**

Šifra koja pojašnjava zašto su događaj ili pogreška zabilježeni.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti:

'00'H	jedan od 10 najnovijih (ili posljednjih) događaja ili pogrešaka.
'01'H	najdulji događaj u jednom od 10 posljednjih dana nastanka,
'02'H	jedan od 5 najduljih događaja u posljednjih 365 dana,
'03'H	posljednji događaj u jednom od 10 posljednjih dana nastanka,
'04'H	najozbiljniji događaj u jednom od 10 posljednjih dana nastanka,
'05'H	jedan od 5 najozbiljnijih događaja u posljednjih 365 dana,
'06'H	prvi događaj ili pogreška do kojih je došlo nakon posljednje kalibracije,
'07'H	aktivni/tekući događaj ili pogreška,
'08'H do '7F'H	RFU,
'80'H do 'FF'H	specifično za proizvođača.

2.56. **ExtendedSerialNumber**

Jedinstvena identifikacija uređaja. Može se također koristiti i kao identifikator javnog ključa uređaja.

```
ExtendedSerialNumber ::= SEQUENCE {
    serialNumber                    INTEGER(0..2^32-1)
    monthYear                       BCDString(SIZE(2))
    type OCTET                      STRING(SIZE(1))
    manufacturerCode                ManufacturerCode
}
```

serialNumber je serijski broj uređaja, jedinstven za proizvođača, vrstu uređaja i mjesec proizvodnje.

monthYear je identifikacija mjeseca i godine proizvodnje (ili dodjele serijskog broja).

Dodjela vrijednosti: BCD šifra mjeseca (dvije znamenke) i godine (zadnje dvije znamenke).

type je identifikator vrste uređaja.

Dodjela vrijednosti: odnosi se na proizvođača; vrijednost ‚FFh' je rezervirana.

manufacturerCode: je brojčana šifra proizvođača uređaja.

2.57. **FullCardNumber**

Šifra kojom se potpuno identificira kartica tahografa.

```
FullCardNumber ::= SEQUENCE {
    cardType                        EquipmentType,
    cardIssuingMemberState          NationNumeric,
    cardNumber                      CardNumber
}
```

cardType je vrsta kartice tahografa.

cardIssuingMemberState je šifra države članice koja je izdala karticu.

cardNumber je broj kartice.

2.58. **HighResOdometer**

Stanje brojača kilometara vozila: Ukupna udaljenost koju je vozilo prešlo tijekom korištenja.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Dodjela vrijednosti: nepotpisan binarni broj. Vrijednost u 1/200 km, u rasponu od 0 do 21 055 406 km.

2.59. **HighResTripDistance**

Udaljenost prijeđena tijekom cjelokupne vožnje ili jednog njezinog dijela.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Dodjela vrijednosti: nepotpisan binarni broj. Vrijednost u 1/200 km, u rasponu od 0 do 21 055 406 km.

2.60. **HolderName**

Prezime i ime(na) nositelja kartice.

```
HolderName ::= SEQUENCE {
    holderSurname                   Name,
    holderFirstNames                Name
}
```

holderSurname je prezime nositelja. Prezime ne uključuje titule.

Dodjela vrijednosti: Ako se ne radi o osobnoj kartici, holderSurname sadrži istu informaciju kao i companyName ili workshopName ili controlBodyName.

holderFirstNames su ime(na) i inicijali nositelja.

2.61. **K-ConstantOfRecordingEquipment**

Konstanta tahografa (definicija m)).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: Broj impulsa po kilometru, u djelatnom rasponu od 0 do 64 255 impulsa/km.

2.62. **KeyIdentifier**

Jedinstveni identifikator javnog ključa koji se koristi pri navođenju i izboru ključa. Također identificira i nositelja ključa.

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

Prvi odabir je prikladan za navođenje javnog ključa jedinice u vozilu ili kartice tahografa.

Drugi oblik je prikladan za navođenje javnog ključa jedinice u vozilu (u slučaju da u trenutku generiranja potvrde nije poznat serijski broj jedinice u vozilu).

Treći odabir je prikladan za navođenje javnog ključa države članice.

2.63. **L-TyreCircumference**

Djelatni opseg guma kotača (definicija u)).

```
L-TyreCircumference ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: nepotpisan binarni broj, vrijednost u 1/8 mm u djelatnom rasponu od 0 do 8 031 mm.

2.64. **Language**

Šifra koja označuje jezik.

```
Language ::= IA5String(SIZE(2))
```

Dodjela vrijednosti: šifriranje s dva mala slova u skladu s ISO 639.

2.65. **LastCardDownload**

Datum i vrijeme pohranjeni na vozačkoj kartici, o posljednjem preuzimanju podataka s kartice (za svrhe drukčije od nadzora). Taj datum može ažurirati jedinica vozila ili neki drugi čitač kartica.

```
LastCardDownload ::= TimeReal
```

Dodjela vrijednosti: nije podrobnije određeno.

2.66. **ManualInputFlag**

Šifra koja označuje je li nositelj kartice pri njenom umetanju ručno unio aktivnosti vozača ili nije (zahtjev 081).

```
ManualInputFlag ::= INTEGER {
   noEntry                          (0)
   manualEntries                    (1)
}
```

Dodjela vrijednosti: nije podrobnije određeno.

2.67. **ManufacturerCode**

Šifra koja označuje proizvođača.

```
ManufacturerCode ::= INTEGER(0..255)
```

Dodjela vrijednosti:

'00'H	Nema podataka
'01'H	Rezervirana vrijednost
'02'H .. '0F'H	Rezervirano za buduću primjenu
'10'H	ACTIA
'11'H .. '17'H	Rezervirano za proizvođače čiji nazivi počinju s 'A'
'18'H .. '1F'H	Rezervirano za proizvođače čiji nazivi počinju s 'B'
'20'H .. '27'H	Rezervirano za proizvođače čiji nazivi počinju sa 'C'
'28'H .. '2F'H	Rezervirano za proizvođače čiji nazivi počinju s 'D'
'30'H .. '37'H	Rezervirano za proizvođače čiji nazivi počinju s 'E'
'38'H .. '3F'H	Rezervirano za proizvođače čiji nazivi počinju s 'F'
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Rezervirano za proizvođače čiji nazivi počinju s 'G'
'48'H .. '4F'H	Rezervirano za proizvođače čiji nazivi počinju s 'H'
'50'H .. '57'H	Rezervirano za proizvođače čiji nazivi počinju s 'I'
'58'H .. '5F'H	Rezervirano za proizvođače čiji nazivi počinju s 'J'
'60'H .. '67'H	Rezervirano za proizvođače čiji nazivi počinju s 'K'
'68'H .. '6F'H	Rezervirano za proizvođače čiji nazivi počinju s 'L'
'70'H .. '77'H	Rezervirano za proizvođače čiji nazivi počinju s 'M'
'78'H .. '7F'H	Rezervirano za proizvođače čiji nazivi počinju s 'N'
'80'H	OSCARD
'81'H .. '87'H	Rezervirano za proizvođače čiji nazivi počinju s 'O'
'88'H .. '8F'H	Rezervirano za proizvođače čiji nazivi počinju s 'P'
'90'H .. '97'H	Rezervirano za proizvođače čiji nazivi počinju s 'Q'
'98'H .. '9F'H	Rezervirano za proizvođače čiji nazivi počinju s 'R'
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	Rezervirano za proizvođače čiji nazivi počinju sa 'S'
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Rezervirano za proizvođače čiji nazivi počinju s 'T'
'B0'H .. 'B7'H	Rezervirano za proizvođače čiji nazivi počinju s 'U'
'B8'H .. 'BF'H	Rezervirano za proizvođače čiji nazivi počinju s 'V'
'C0'H .. 'C7'H	Rezervirano za proizvođače čiji nazivi počinju s 'W'
'C8'H .. 'CF'H	Rezervirano za proizvođače čiji nazivi počinju s 'X'
'D0'H .. 'D7'H	Rezervirano za proizvođače čiji nazivi počinju s 'Y'
'D8'H .. 'DF'H	Rezervirano za proizvođače čiji nazivi počinju sa 'Z'

2.68. **MemberStateCertificate**

Certifikat javnog ključa države članice koji izdaje Europsko certifikacijsko tijelo.

```
MemberStateCertificate ::= Certificate
```

2.69. **MemberStatePublicKey**

Javni ključ države članice.

```
MemberStatePublicKey ::= PublicKey
```

2.70. **Name**

Ime.

```
Name ::= SEQUENCE {
   codePage                                INTEGER (0..255),
   name                                    OCTET STRING (SIZE(35))
}
```

codePage označuje dio ISO/IEC 8859 korišten pri šifriranju imena.

name je ime šifrirano u skladu s ISO/IEC 8859-codePage.

2.71. **NationAlpha**

Abecedna oznaka države u skladu s dogovorenim šifriranjem država na naljepnicama branika vozila i/ili kako se koristi u međunarodno usklađenim ispravama o osiguranju vozila (zelena karta).

```
NationAlpha ::= IA5String(SIZE(3))
```

Dodjela vrijednosti:

	Nema podataka
'A'	Austrija
'AL'	Albanija
'AND'	Andora
'ARM'	Armenija
'AZ'	Azerbajdžan
'B'	Belgija
'BG'	Bugarska
'BIH'	Bosna i Hercegovina
'BY'	Bjelarus
'CH'	Švicarska
'CY'	Cipar
'CZ'	Ceška
'D'	Njemacka
'DK'	Danska
'E'	Španjolska
'EST'	Estonija
'F'	Francuska
'FIN'	Finska
'FL'	Lihtenštajn
'FR'	Farski otoci
'UK'	Ujedinjena Kraljevina, Alderney, Guernsey, Jersey, Otok Man, Gibraltar
'GE'	Gruzija
'GR'	Grcka
'H'	Madarska
'HR'	Hrvatska
'I'	Italija
'IRL'	Irska
'IS'	Island
'KZ'	Kazakstan
'L'	Luksemburg
'LT'	Litva
'LV'	Latvija
'M'	Malta
'MC'	Monako

'MD'	Republika Moldova
'MK'	Makedonija
'N'	Norveška
'NL'	Nizozemska
'P'	Portugal
'PL'	Poljska
'RO'	Rumunjska
'RSM'	San Marino
'RUS'	Ruska Federacija
'S'	Švedska
'SK'	Slovacka
'SLO'	Slovenija
'TM'	Turkmenistan
'TR'	Turska
'UA'	Ukrajina
'V'	Vatikan
'YU'	Jugoslavija
'UNK'	Nepoznato
'EC'	Europska zajednica
'EUR'	Drugi dijelovi Europe
'WLD'	Drugi dijelovi svijeta.

2.72. **NationNumeric**

Brojčana oznaka države.

```
NationNumeric ::= INTEGER(0..255)
```

Dodjela vrijednosti:

- - Nema raspoloživih informacija	(00) H,
- - Austrija	(01) H,
- - Albanija	(02) H,
- - Andora	(03) H,
- - Armenija	(04) H,
- - Azerbajdžan	(05) H,
- - Belgija	(06) H,
- - Bugarska	(07) H,
- - Bosna i Hercegovina	(08) H,
- - Bjelarus	(09) H,
- - Švicarska	(0A) H,
- - Cipar	(0B) H,
- - Češka	(0C) H,
- - Njemačka	(0D) H,
- - Danska	(0E) H,
- - Španjolska	(0F) H,
- - Estonija	(10) H,
- - Francuska	(11) H,
- - Finska	(12) H,
- - Lihtenštajn	(13) H,
- - Farski otoci	(14) H,
- - Ujedinjena Kraljevina	(15) H,
- - Gruzija	(16) H,
- - Grčka	(17) H,
- - Mađarska	(18) H,
- - Hrvatska	(19) H,
- - Italija	(1A) H,
- - Irska	(1B) H,
- - Island	(1C) H,

-- Kazakstan	(1D) H,
-- Luksemburg	(1E) H,
-- Litva	(1F) H,
-- Latvija	(20) H,
-- Malta	(21) H,
-- Monako	(22) H,
-- Republika Moldova	(23) H,
-- Makedonija	(24) H,
-- Norveška	(25) H,
-- Nizozemska	(26) H,
-- Portugal	(27) H,
-- Poljska	(28) H,
-- Rumunjska	(29) H,
-- San Marino	(2A) H,
-- Ruska Federacija	(2B) H,
-- Švedska	(2C) H,
-- Slovačka	(2D) H,
-- Slovenija	(2E) H,
-- Turkmenistan	(2F) H,
-- Turska	(30) H,
-- Ukrajina	(31) H,
-- Vatikan	(32) H,
-- Jugoslavija	(33) H,
-- RFU	(34..FC) H,
-- Europska zajednica	(FD) H,
-- Drugi dijelovi Europe	(FE) H,
-- Drugi dijelovi svijeta	(FF) H

2.73. **NoOfCalibrationRecords**

Broj zapisa o umjeravanju koje može pohraniti kartica radionice.

`NoOfCalibrationRecords ::= INTEGER(0..255)`

Dodjela vrijednosti: vidjeti stavak 3.

2.74. **NoOfCalibrationsSinceDownload**

Brojač koji pokazuje broj kalibracija izvršenih s karticom radionice od posljednjeg preuzimanja podataka (zahtjev 230).

`NoOfCalibrationsSinceDownload ::= INTEGER(0..2`^{16}`-1),`

dodjela vrijednosti: nije podrobnije određeno.

2.75. **NoOfCardPlaceRecords**

Broj zapisa o mjestima koji može spremiti kartica vozača ili kartica radionice.

`NoOfCardPlaceRecords ::= INTEGER(0..255)`

Dodjela vrijednosti: vidjeti stavak 3.

2.76. **NoOfCardVehicleRecords**

Broj zapisa o korištenim vozilima koje može spremiti kartica vozača ili kartica radionice.

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

Dodjela vrijednosti: vidjeti stavak 3.

2.77. **NoOfCompanyActivityRecords**

Broj zapisa o aktivnostima tvrtke koji može spremiti kartica prijevoznika.

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

Pripisivanje vrijednosti: vidjeti stavak 3.

2.78. **NoOfControlActivityRecords**

Broj zapisa o aktivnostima nadzora koje nadzorna kartica može spremiti.

```
NoOfControlActivityRecords ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: vidjeti stavak 3.

2.79. **NoOfEventsPerType**

Broj događanja po vrstama događaja koji kartica može spremiti.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Dodjela vrijednosti: vidjeti stavak 3.

2.80. **NoOfFaultsPerType**

Broj događanja po vrsti događaja koje kartica može spremiti.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Dodjela vrijednosti: vidjeti stavak 3.

2.81. **OdometerValueMidnight**

Stanje brojača kilometara u ponoć određenog dana (zahtjev 090).

```
OdometerValueMidnight ::= OdometerShort
```

Dodjela vrijednosti: nije podrobnije određeno.

2.82. **OdometerShort**

Stanje brojača kilometara u kratkom obliku.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Dodjela vrijednosti: neoznačen binarni broj. Vrijednost u km u djelatnom rasponu od 0 do 9 999 999 km.

2.83. **OverspeedNumber**

Broj događaja prekoračenja brzine od posljednje kontrole prekoračenja brzine.

```
OverspeedNumber ::= INTEGER(0..255)
```

Dodjela vrijednosti: 0 označuje da od posljednje kontrole prekoračenja brzine nije bilo prekoračenja brzine; 1 označuje da se od posljednje kontrole prekoračenja brzine dogodio jedan događaj prekoračenja brzine, … 255 označuje da se od posljednje kontrole prekoračenja brzine desilo 255 ili više događaja prekoračenja brzine.

2.84. **PlaceRecord**

Informacija koja se odnosi na mjesto početka ili završetka dnevnog razdoblja rada (zahtjevi 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort
}
```

entryTime je datum i vrijeme unosa.

entryTypeDailyWorkPeriod je vrsta unosa.

dailyWorkPeriodCountry je unesena država.

dailyWorkPeriodRegion je unesena regija.

vehicleOdometerValue je stanje brojača kilometara u trenutku unosa mjesta.

2.85. **PreviousVehicleInfo**

Informacija koja se odnosi na vozilo koje je vozač prethodno koristio pri umetanju kartice u jedinicu vozila (zahtjev 081).

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification        VehicleRegistrationIdentification,
   cardWithdrawalTime                       TimeReal
}
```

vehicleRegistrationIdentification je registracijska oznaka vozila i država registracije vozila.
cardWithdrawalTime je datum i vrijeme vađenja kartice.

2.86. **PublicKey**

Javni ključ RSA.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                            RSAKeyModulus,
   rsaKeyPublicExponent                     RSAKeyPublicExponent
}
```

rsaKeyModulus je modul para ključeva.
rsaKeyPublicExponent je javni eksponent para ključeva.

2.87. **RegionAlpha**

Slovna oznaka regije u određenoj državi.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Dodjela vrijednosti:

	Nema raspoloživih informacija
Španjolska:	
'AN'	Andaluzija
'AR'	Aragon
'AST'	Asturija
'C'	Kantabrija
'CAT'	Katalonija
'CL'	Kastilja-Leon
'CM'	Kastilja-Mancha
'CV'	Valencija
'EXT'	Ekstremadura
'G'	Galicija
'IB'	Baleari
'IC'	Kanarski otoci
'LR'	La Rioja
'M'	Madrid
'MU'	Murcia
'NA'	Navara
'PV'	Baskija.

2.88. **RegionNumeric**

Brojčana oznaka regije u određenoj državi.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti:

'00'H	Nema podataka
Španjolska:	
'01'H	Andaluzija
'02'H	Aragon
'03'H	Asturija
'04'H	Kantabrija
'05'H	Katalonija
'06'H	Kastilja-Leon
'07'H	Kastilja-Mancha
'08'H	Valencija
'09'H	Extremadura
'0A'H	Galicija
'0B'H	Baleari
'0C'H	Kanarski otoci
'0D'H	La Rioja
'0E'H	Madrid
'0F'H	Murcia
'10'H	Navara
'11'H	Baskija.

2.89. **RSAKeyModulus**

Modul para ključeva RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Dodjela vrijednosti: Nije određeno.

2.90. **RSAKeyPrivateExponent**

Javni eksponent para ključeva RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Dodjela vrijednosti: Nije određeno.

2.91. **RSAKeyPublicExponent**

Javni eksponent para ključeva RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Dodjela vrijednosti: Nije određeno.

2.92. **SensorApprovalNumber**

Broj tipnog odobrenja senzora.

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: Nije određeno.

2.93. **SensorIdentification**

Informacija pohranjena u senzoru kretanja koja se odnosi na identifikaciju senzora kretanja (zahtjev 077).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorSCIdentifier                    SensorSCIdentifier,
   sensorOSIdentifier                    SensorOSIdentifier
}
```

sensorSerialNumber je prošireni serijski broj senzora kretanja (uključujući kataloški broj i šifru proizvođača).

sensorApprovalNumber je broj tipnog odobrenja senzora kretanja.

sensorSCIdentifier je identifikator sigurnosnog sastavnog dijela senzora kretanja.

sensorOSIdentifier je identifikator operativnog sustava senzora kretanja.

2.94. **SensorInstallation**

Informacija spremljena u senzoru kretanja koja se odnosi na ugradnju senzora kretanja (zahtjev 099).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                  SensorPairingDate,
   firstVuApprovalNumber                   VuApprovalNumber,
   firstVuSerialNumber                     VuSerialNumber,
   sensorPairingDateCurrent                SensorPairingDate,
   currentVuApprovalNumber                 VuApprovalNumber,
   currentVUSerialNumber                   VuSerialNumber
}
```

sensorPairingDateFirst je datum prvog uparivanja senzora kretanja s jedinicom u vozilu.

firstVuApprovalNumber je broj tipnog odobrenja prve jedinice u vozilu uparene sa senzorom kretanja.

firstVuSerialNumber je serijski broj prve jedinice u vozilu uparene sa senzorom kretanja.

sensorPairingDateCurrent je datum trenutačnog uparivanja senzora kretanja s jedinicom u vozilu.

currentVuApprovalNumber je broj tipnog odobrenja jedinice u vozilu s kojom je senzor kretanja trenutačno uparen.

currentVUSerialNumber je serijski broj jedinice u vozilu s kojom je trenutačno uparen senzor kretanja.

2.95. **SensorInstallationSecData**

Informacija pohranjena na kartici radionice koja se odnosi na sigurnosne podatke potrebne za uparivanje senzora kretanja s jedinicama u vozilu (zahtjev 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Dodjela vrijednosti: u skladu s ISO 16844-3.

2.96. **SensorOSIdentifier**

Identifikator operativnog sustava senzora kretanja.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Dodjela vrijednosti: utvrđuje proizvođač.

2.97. **SensorPaired**

Informacija spremljena u jedinici u vozilu koja se odnosi na identifikaciju senzora kretanja uparenog s jedinicom u vozilu (zahtjev 079).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                      SensorSerialNumber,
   sensorApprovalNumber                    SensorApprovalNumber,
   sensorPairingDateFirst                  SensorPairingDate
}
```

sensorSerialNumber je serijski broj senzora kretanja trenutačno uparenog s jedinicom u vozilu.

sensorApprovalNumber je broj tipnog odobrenja senzora kretanja koji je trenutačno uparen s jedinicom u vozilu.

sensorPairingDateFirst je datum prvog uparivanja jedinice u vozilu sa senzorom kretanja koje je trenutačno upareno s jedinicom u vozilu.

2.98. **SensorPairingDate**

Datum uparivanja senzora kretanja s jedinicom u vozilu.

```
SensorPairingDate ::= TimeReal
```

Dodjela vrijednosti: Nije određeno.

2.99. **SensorSerialNumber**

Serijski broj senzora kretanja.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.100. **SensorSCIdentifier**

Identifikator sigurnosnog sastavnog dijela senzora kretanja.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: utvrđuje proizvođač dijela.

2.101. **Signature**

Digitalni potpis.

```
Signature ::= OCTET STRING (SIZE(128))
```

Dodjela vrijednosti: u skladu s Dodatkom 11. ‚Zajednički sigurnosni mehanizmi'.

2.102. **SimilarEventsNumber**

Broj sličnih događaja u određenom danu. (zahtjev 094).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Dodjela vrijednosti: 0 se ne koristi, 1 označuje da se tog dana dogodio samo jedan događaj, 2 označuje da su se dogodila 2 događaja te vrste (spremljen je samo jedan), … 255 označuje da se tog dana dogodilo 255 ili više slučajeva takve vrste.

2.103. **SpecificConditionType**

Šifra koja označuje posebna stanja (zahtjevi 050b, 105a, 212a i 230a).

```
SpecificConditionType ::= INTEGER(0..255)
```

Dodjela vrijednosti:

'00'H	Nema podataka
'01'H	Izvan djelokruga - početak
'02'H	Izvan djelokruga - kraj
'03'H	Vožnja trajektom/vlakom
'04'H .. 'FF'	HRFU

2.104. **SpecificConditionRecord**

Informacija pohranjena na kartici vozača, kartici radionice ili u jedinici u vozilu koja se odnosi na posebne uvjete (zahtjevi 105a, 212a in 230a).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                                TimeReal,
   specificConditionType                    SpecificConditionType
}
```

entryTime je datum i vrijeme unosa.

specificConditionType je šifra koja označuje posebno stanje.

2.105. **Speed**

Brzina vozila (km/h).

```
Speed ::= INTEGER(0..255)
```

Dodjela vrijednosti: kilometar na sat u djelatnom rasponu od 0 do 220 km/h.

2.106. **SpeedAuthorised**

Najveća dopuštena brzina vozila (definicija bb).

```
SpeedAuthorised ::= Speed
```

2.107. **SpeedAverage**

Prosječna brzina u prethodno određenom trajanju (km/h).

```
SpeedAverage ::= Speed
```

2.108. **SpeedMax**

Najveća brzina izmjerena u prethodno određenom trajanju.

```
SpeedMax ::= Speed
```

2.109. **TDesSessionKey**

Trojni ključ DES razmjene podataka.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                                 OCTET STRING (SIZE(8))
   tDesKeyB                                 OCTET STRING (SIZE(8))
}
```

Dodjela vrijednosti: nije podrobnije određeno.

2.110. **TimeReal**

Šifra kombiniranog područja datuma i vremena u kojoj su datum i vrijeme izraženi kao broj sekundi nakon 00h00m00s na dan 1. siječnja 1970. GMT.

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

Dodjela vrijednosti – oktetni poredak: Broj sekundi od ponoći 1. siječnja 1970. po GMT.

Najkasniji mogući datum i vrijeme su u 2106. godini

2.111. **TyreSize**

Oznaka dimenzija guma.

```
TyreSize ::= IA5String(SIZE(15))
```

Dodjela vrijednosti: u skladu s Direktivom 92/23 (EEZ) od 31.3.1992., SL L 129, str. 95.

2.112. **VehicleIdentificationNumber**

Identifikacijski broj vozila (VIN) koji se odnosi na vozilo kao cjelinu; obično serijski broj šasije ili broj okvira.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Dodjela vrijednosti: kako je utvrđeno u ISO 3779.

2.113. **VehicleRegistrationIdentification**

Identifikacija vozila jedinstvena za cijelu Europu (registracijska oznaka vozila i država članica registracije).

```
VehicleRegistrationIdentification ::= SEQUENCE {
    vehicleRegistrationNation                NationNumeric,
    vehicleRegistrationNumber                VehicleRegistrationNumber
}
```

vehicleRegistrationNation je država u kojoj je vozilo registrirano.

vehicleRegistrationNumber je registracijska oznaka vozila (VRN).

2.114. **VehicleRegistrationNumber**

Registracijska oznaka vozila (VRN). Registacijsku oznaku dodjeljuje tijelo nadležno za registraciju.

```
VehicleRegistrationNumber ::= SEQUENCE {
    codePage                                 INTEGER (0..255),
    vehicleRegNumber                         OCTET STRING (SIZE(13))
}
```

codePage označuje dio ISO/IEC 8859 koji se koristi za šifriranje vehicleRegNumber,

vehicleRegNumber je registracijska oznaka vozila, šifrirana u skladu s ISO/IEC 8859-codePage.

Dodjela vrijednosti: utvrđuje pojedina država.

2.115. **VuActivityDailyData**

Informacija pohranjena u jedinici vozila koja se odnosi na promjene aktivnosti i/ili promjene statusa vožnje i/ili promjene statusa kartice za određeni kalendarski dan (zahtjev 084) i na status utora u 00:00 sati tog dana.

```
VuActivityDailyData ::= SEQUENCE {
    noOfActivityChanges                      INTEGER SIZE(0..1440),
    activityChangeInfos                      SET SIZE(noOfActivityChanges) OF
                                             ActivityChangeInfo
}
```

noOfActivityChanges je broj riječi ActivityChangeInfo u nizu activityChangeInfos.

activityChangeInfos je niz riječi ActivityChangeInfo pohranjen u jedinici vozila za određeni dan. Uvijek uključuje dvije riječi ActivityChangeInfo koje određuju status utora u 00:00 tog dana.

2.116. **VuApprovalNumber**

Broj tipnog odobrenja jedinice u vozilu.

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: Nije određeno.

2.117. **VuCalibrationData**

Informacija pohranjena u jedinici u vozilu koja se odnosi na kalibraciju tahografa (zahtjev 098).

```
VuCalibrationData ::= SEQUENCE {
    noOfVuCalibrationRecords                 INTEGER(0..255),
    vuCalibrationRecords SET                 SIZE(noOfVuCalibrationRecords) OF
                                             VuCalibrationRecord
}
```

noOfVuCalibrationRecords je broj zapisa sadržanih u nizu vuCalibrationRecords.

vuCalibrationRecords je niz zapisa o kalibraciji.

2.118 **VuCalibrationRecord**

Informacija spremljena u jedinici u vozilu, povezana s kalibracijom tahografa (zahtjev 098).

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal
}
```

calibrationPurpose je svrha kalibracije.

workshopName, workshopAddress su naziv i adresa radionice.

workshopCardNumber identificira karticu radionice koja se koristi pri kalibraciji.

workshopCardExpiryDate je datum isteka valjanosti kartice.

vehicleIdentificationNumber je VIN.

vehicleRegistrationIdentification sadrži registracijsku oznaku vozila i državu registracije vozila.

wVehicleCharacteristicConstant je karakteristični koeficijent vozila.

kConstantOfRecordingEquipment je konstanta tahografa.

lTyreCircumference je djelatni opseg guma kotača.

tyreSize je oznaka dimenzija guma na vozilu.

authorisedSpeed je dopuštena brzina vozila.

oldOdometerValue, newOdometerValue su staro i novo stanje brojača kilometara.

oldTimeValue, newTimeValue su stara i nova vrijednost datuma i vremena.

nextCalibrationDate je datum sljedeće kalibracije tipa naznačenog u CalibrationPurpose provedena od ovlaštenog tijela za nadzor.

2.119 **VuCardIWData**

Informacija spremljena u jedinici u vozilu povezana s ciklusima umetanja i vađenja kartice vozača ili kartice radionice u jedinici u vozilu (zahtjev 081).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                         INTEGER(0..216-1),
   vuCardIWRecords                       SET SIZE(noOfIWRecords) OF
                                         VuCardIWRecord
}
```

noOfIWRecords je broj zapisa u nizu vuCardIWRecords.

vuCardIWRecords je niz zapisa povezanih s ciklusima umetanja i vađenja kartice.

2.120 **VuCardIWRecord**

Informacija spremljena u jedinicu u vozilu, povezana s ciklusom umetanja i vađenja kartice vozača ili kartice radionice u jedinici u vozilu (zahtjev 081).

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                          HolderName,
   fullCardNumber                          FullCardNumber,
   cardExpiryDate                          TimeReal,
   cardInsertionTime                       TimeReal,
   vehicleOdometerValueAtInsertion         OdometerShort,
   cardSlotNumber                          CardSlotNumber,
   cardWithdrawalTime                      TimeReal,
   vehicleOdometerValueAtWithdrawal        OdometerShort,
   previousVehicleInfo                     PreviousVehicleInfo
   manualInputFlag                         ManualInputFlag
}
```

cardHolderName je prezime i ime(na) nositelja kartice vozača ili kartice radionice, spremljenih na kartici.

fullCardNumber je vrsta kartice, država članica izdavatelj i broj kartice, spremljenih na kartici.

cardExpiryDate je datum isteka kartice, pohranjen na kartici.

cardInsertionTime je datum i vrijeme umetanja.

vehicleOdometerValueAtInsertion je stanje brojača kilometara pri umetanju kartice.

cardSlotNumber je utor u kojeg je umetnuta kartica.

cardWithdrawalTime je datum i vrijeme vađenja.

vehicleOdometerValueAtWithdrawal je stanje brojača kilometara pri vađenju kartice.

previousVehicleInfo sadrži podatke o vozilu koje je vozač prethodno koristio spremljene na kartici.

manualInputFlag je oznaka koja naznačuje je li je nositelj kartice pri umetanju kartice ručno unio aktivnosti vozača.

2.121. **VuCertificate**

Certifikat javnog ključa jedinice u vozilu.

```
VuCertificate ::= Certificate
```

2.122. **VuCompanyLocksData**

Informacija pohranjena u jedinici u vozilu, povezana s blokadama tvrtke (zahtjev 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                               INTEGER(0..20),
   vuCompanyLocksRecords                   SET SIZE(noOfLocks) OF
                                           VuCompanyLocksRecord
}
```

noOfLocks je broj zaključavanja naveden u vuCompanyLocksRecords.

vuCompanyLocksRecords je niz zapisa zaključavanja tvrtke.

2.123. **VuCompanyLocksRecord**

Informacija pohranjena u jedinici u vozilu, povezana s jednim zaključavanjem tvrtke (zahtjev 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
    lockInTime                          TimeReal,
    lockOutTime                         TimeReal,
    companyName                         Name,
    companyAddress                      Address,
    companyCardNumber                   FullCardNumber
}
```

lockInTime, **lockOutTime** su datum i vrijeme zaključavanja i otključavanja podataka.

companyName, companyAddress su naziv i adresa tvrtke, povezani sa zaključavanjem podataka.

companyCardNumber identificira karticu korištenu pri zaključavanju.

2.124. **VuControlActivityData**

Informacija pohranjena u jedinici u vozilu, povezana s nadzorom provedenim uz korištenje ove jedinice vozila (zahtjev 102).

```
VuControlActivityData ::= SEQUENCE {
    noOfControls                        INTEGER(0..20),
    vuControlActivityRecords            SET SIZE(noOfControls) OF
                                        VuControlActivityRecord
}
```

noOfControls je broj nadzora navedenih u vuControlActivityRecords.

vuControlActivityRecords je niz zapisa o aktivnostima nadzora.

2.125. **VuControlActivityRecord**

Informacija pohranjena u jedinici u vozilu povezana s nadzorom provedenim uz korištenje ove jedinice vozila (zahtjev 102).

```
VuControlActivityRecord ::= SEQUENCE {
    controlType                         ControlType,
    controlTime                         TimeReal,
    controlCardNumber                   FullCardNumber,
    downloadPeriodBeginTime             TimeReal,
    downloadPeriodEndTime               TimeReal
}
```

controlType je vrsta nadzora.

controlTime je datum i vrijeme nadzora.

ControlCardNumber identificira nadzornu karticu korištenu za nadzor.

downloadPeriodBeginTime je početak razdoblja za koje se obavlja preuzimanje podataka, ako je došlo do preuzimanja podataka.

downloadPeriodEndTime je kraj razdoblja za koje se obavlja preuzimanje podataka, ako je došlo do preuzimanja podataka.

2.126. **VuDataBlockCounter**

Brojač pohranjen na kartici koji redom utvrđuje cikluse umetanja i vađenja kartice u jedinicama u vozilu.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Dodjela vrijednosti: Redni broj, s najvećom vrijednošću 9 999, nakon čega opet kreće od 0.

2.127. **VuDetailedSpeedBlock**

Informacija pohranjena u jedinici u vozilu, povezana s detaljnom brzinom vozila u minuti tijekom koje se vozilo kretalo (zahtjev 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate                    TimeReal,
   speedsPerSecond                        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate je datum i vrijeme prve vrijednosti brzine unutar bloka.

speedsPerSecond je kronološki slijed izmjerenih brzina svake sekunde u minuti koja počne u speedBlockBeginDate (uključeno).

2.128. **VuDetailedSpeedData**

Informacija pohranjena u jedinici u vozilu povezana s podrobnim podacima o brzini vozila.

```
VuDetailedSpeedData ::= SEQUENCE
   noOfSpeedBlocks                        INTEGER(0.2^16-1),
   vuDetailedSpeedBlocks                  SET SIZE(noOfSpeedBlocks) OF
                                          VuDetailedSpeedBlock
}
```

noOfSpeedBlocks je broj blokova brzina u nizu vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks je niz detaljnih blokova brzina.

2.129. **VuDownloadablePeriod**

Najstariji i najnoviji datum za koji jedinica u vozilu sadrži podatke vezane uz aktivnosti vozača (zahtjevi 081, 084 ili 087).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                    TimeReal
   maxDownloadableTime                    TimeReal
}
```

minDownloadableTime je najstariji datum i vrijeme pohranjeni u jedinici vozila umetanja kartice ili promjene aktivnosti ili unosa mjesta.

MaxDownloadableTime je najnoviji datum i vrijeme pohranjeni u jednici vozila vađenja kartice ili promjene aktivnosti ili unosa mjesta.

2.130. **VuDownloadActivityData**

Informacija pohranjena u jedinici u vozilu povezana sa zadnjim preuzimanjem podataka iz iste (zahtjev 105).

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumber                         FullCardNumber,
   companyOrWorkshopName                  Name
}
```

downloadingTime je datum i vrijeme preuzimanja podataka.

fullCardNumber identificira karticu korištenu za odobrenje preuzimanja podataka.

companyOrWorkshopName je naziv tvrtke ili radionice.

2.131. **VuEventData**

Informacija pohranjena u jedinici u vozilu, povezana s događajima (zahtjev 094, osim u slučaju prekoračenja brzine).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                           INTEGER(0..255),
   vuEventRecords                         SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents je broj događaja navedenih u nizu vuEventRecords.

vuEventRecords je niz zapisa događaja.

2.132. **VuEventRecord**

Informacija pohranjena u jedinicu u vozilu povezana s događajem (zahtjev 094, osim u slučaju prekoračenja brzine).

```
VuEventRecord ::= SEQUENCE {
    eventType                           EventFaultType,
    eventRecordPurpose                  EventFaultRecordPurpose,
    eventBeginTime                      TimeReal,
    eventEndTime                        TimeReal,
    cardNumberDriverSlotBegin           FullCardNumber,
    cardNumberCodriverSlotBegin         FullCardNumber,
    cardNumberDriverSlotEnd             FullCardNumber,
    cardNumberCodriverSlotEnd           FullCardNumber,
    similarEventsNumber                 SimilarEventsNumber
}
```

eventType je vrsta događaja.

eventRecordPurpose je svrha s kojom je taj događaj zabilježen.

eventBeginTime je datum i vrijeme početka događaja.

eventEndTime je datum i vrijeme kraja događaja.

cardNumberDriverSlotBegin identificira karticu umetnutu u utor vozača na početku događaja.

cardNumberCodriverSlotBegin identificira karticu umetnutu u utor suvozača na početku događaja.

cardNumberDriverSlotEnd identificira karticu umetnutu u utor vozača na kraju događaja.

cardNumberCodriverSlotEnd identificira karticu umetnutu u utor suvozača pri kraju događaja.

similarEventsNumber je broj sličnih događaja u tom danu.

Ovaj slijed se može koristiti za sve događaje, osim za događaje prekoračenja brzine.

2.133. **VuFaultData**

Informacija pohranjena u jedinicu u vozilu, povezana s pogreškama (zahtjev 096).

```
VuFaultData ::= SEQUENCE {
    noOfVuFaults                        INTEGER(0..255),
    vuFaultRecords SET                  SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults je broj pogrešaka navedenih u nizu vuFaultRecords.

vuFaultRecords je niz zapisa o pogreškama.

2.134. **VuFaultRecord**

Informacija spremljena u jedinici u vozilu, povezana s pogreškom (zahtjev 096).

```
VuFaultRecord ::= SEQUENCE {
    faultType                           EventFaultType,
    faultRecordPurpose                  EventFaultRecordPurpose,
    faultBeginTime                      TimeReal,
    faultEndTime                        TimeReal,
    cardNumberDriverSlotBegin           FullCardNumber,
    cardNumberCodriverSlotBegin         FullCardNumber,
    cardNumberDriverSlotEnd             FullCardNumber,
    cardNumberCodriverSlotEnd           FullCardNumber
}
```

faultType je vrsta pogreške tahografa.

faultRecordPurpose je svrha s kojom je ta pogreška bila zabilježena.

faultBeginTime je datum i vrijeme početka pogreške.

faultEndTime je datum i vrijeme kraja pogreške.

cardNumberDriverSlotBegin identificira karticu umetnutu u utor vozača na početku pogreške.

cardNumberCodriverSlotBegin identificira karticu umetnutu u utor suvozača na početku pogreške.

cardNumberDriverSlotEnd identificira karticu umetnutu u utor vozača na kraju pogreške.

cardNumberCodriverSlotEnd identificira karticu umetnutu u utor suvozača na kraju pogreške.

2.135. **VuIdentification**

Informacija pohranjena u jedinici u vozilu, povezana s identifikacijom jedinice u vozilu (zahtjev 075).

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                VuManufacturerName,
   vuManufacturerAddress             VuManufacturerAddress,
   vuPartNumber                      VuPartNumber,
   vuSerialNumber                    VuSerialNumber,
   vuSoftwareIdentification          VuSoftwareIdentification,
   vuManufacturingDate               VuManufacturingDate,
   vuApprovalNumber                  VuApprovalNumber
}
```

vuManufacturerName je naziv proizvođača jedinice u vozilu.

vuManufacturerAddress je adresa proizvođača jedinice u vozilu.

vuPartNumber je kataloški broj jedinice u vozilu.

vuSerialNumber je serijski broj jedinice u vozilu.

vuSoftwareIdentification identificira softver instaliran u jedinici u vozilu.

vuManufacturingDate je datum proizvodnje jedinice u vozilu.

vuApprovalNumber je broj tipnog odobrenja jedinice u vozilu.

2.136. **VuManufacturerAddress**

Adresa proizvođača jedinice u vozilu.

```
VuManufacturerAddress ::= Address
```

Dodjela vrijednosti: Nije određeno.

2.137. **VuManufacturerName**

Naziv proizvođača jedinice u vozilu.

```
VuManufacturerName ::= Name
```

Dodjela vrijednosti: Nije određeno.

2.138. **VuManufacturingDate**

Datum proizvodnje jedinice u vozilu.

```
VuManufacturingDate ::= TimeReal
```

Dodjela vrijednosti: Nije određeno.

2.139. **VuOverSpeedingControlData**

Informacija pohranjena u jedinici u vozilu, povezana s događajima prekoračenja brzine nakon zadnje kontrole prekoračenja brzine (zahtjev 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
    lastOverspeedControlTime                TimeReal,
    firstOverspeedSince                     TimeReal,
    numberOfOverspeedSince                  OverspeedNumber
}
```

lastOverspeedControlTime je datum i vrijeme zadnje kontrole prekoračenja brzine.

firstOverspeedSince je datum i vrijeme prvog prekoračenja brzine nakon ove kontrole prekoračenja brzine.

numberOfOverspeedSince je broj događaja prekoračenja brzine od zadnje kontrole prekoračenja brzine.

2.140. **VuOverSpeedingEventData**

Informacija pohranjena u jedinici u vozilu povezana s događajima prekoračenja brzine (zahtjev 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
    noOfVuOverSpeedingEvents                INTEGER(0..255),
    vuOverSpeedingEventRecords              SET SIZE(noOfVuOverSpeedingEvents) OF
                                            VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents je broj događaja navedenih u nizu vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords je niz zapisa o događajima prekoračenja brzine.

2.141. **VuOverSpeedingEventRecord**

Informacija pohranjena u jedinici u vozilu, povezana s događajima prekoračenja brzine (zahtjev 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    eventType                               EventFaultType,
    eventRecordPurpose                      EventFaultRecordPurpose,
    eventBeginTime                          TimeReal,
    eventEndTime                            TimeReal,
    maxSpeedValue                           SpeedMax,
    averageSpeedValue                       SpeedAverage,
    cardNumberDriverSlotBegin               FullCardNumber,
    similarEventsNumber                     SimilarEventsNumber
}
```

eventType je vrsta događaja.

eventRecordPurpose je svrha zbog koje je taj događaj bio zabilježen.

eventBeginTime je datum i vrijeme početka događaja.

eventEndTime je datum i vrijeme kraja događaja.

maxSpeedValue je najviša brzina izmjerena tijekom događaja.

averageSpeedValue je aritmetička prosječna brzina izmjerena tijekom događaja.

cardNumberDriverSlotBegin identificira karticu umetnutu u utor vozača na početku događaja.

similarEventsNumber je broj sličnih događaja u tom danu.

2.142. **VuPartNumber**

Kataloški broj jedinice u vozilu.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Dodjela vrijednosti: određuje proizvođač jedinice vozila.

2.143. **VuPlaceDailyWorkPeriodData**

Informacija pohranjena u jedinici u vozilu povezana s mjestima početka ili kraja dnevnih perioda aktivnosti vozača (zahtjev 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {

   noOfPlaceRecords                          INTEGER(0..255),

   vuPlaceDailyWorkPeriodRecords             SET SIZE(noOfPlaceRecords) OF
                                             VuPlaceDailyWorkPeriodRecord

}
```

noOfPlaceRecords je broj zapisa navedenih u nizu vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords je niz zapisa vezanih uz mjesta.

2.144. **VuPlaceDailyWorkPeriodRecord**

Informacija spremljena u jedinici u vozilu povezana s mjestom početka ili kraja dnevnih razdoblja aktivnosti vozača (zahtjev 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {

   fullCardNumber                            FullCardNumber,

   placeRecord                               PlaceRecord

}
```

fullCardNumber je vrsta kartice vozača, država članica izdavatelj kartice i broj kartice.

placeRecord sadrži informacije povezane s unesenim mjestom.

2.145. **VuPrivateKey**

Privatni ključ jedinice u vozilu.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. **VuPublicKey**

Javni ključ jedinice u vozilu.

```
VuPublicKey ::= PublicKey
```

2.147. **VuSerialNumber**

Serijski broj jedinice u vozilu (zahtjev 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. **VuSoftInstallationDate**

Datum ugradnje verzije softvera u jedinicu u vozilu.

```
VuSoftInstallationDate ::= TimeReal
```

Dodjela vrijednosti: Nije određeno.

2.149. **VuSoftwareIdentification**

Informacija spremljena u jedinici u vozilu, povezana s instaliranim softverom.

```
VuSoftwareIdentification ::= SEQUENCE {

   vuSoftwareVersion                         VuSoftwareVersion,

   vuSoftInstallationDate                    VuSoftInstallationDate

}
```

vuSoftwareVersion je broj verzije softvera instaliranog u jedinicu u vozilu.

vuSoftInstallationDate je datum instalacije softvera.

2.150. **VuSoftwareVersion**

Verzija softvera jedinice u vozilu.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Dodjela vrijednosti: Nije određeno.

2.151. **VuSpecificConditionData**

Informacija pohranjena u jedinici u vozilu, povezana s posebnim stanjima.

```
VuSpecificConditionData ::= SEQUENCE {
    noOfSpecificConditionRecords            INTEGER(0..2^16-1)
    specificConditionRecords                SET SIZE (noOfSpecificConditionRecords) OF
                                            SpecificConditionRecord
}
```

noOfSpecificConditionRecords je broj zapisa u nizu specificConditionRecords.

specificConditionRecords je niz zapisa povezanih s posebnim stanjima.

2.152. **VuTimeAdjustmentData**

Informacija spremljena u jedinici u vozilu, povezana s podešenjima vremena provedenim izvan okvira redovnih kalibracija (zahtjev 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
    noOfVuTimeAdjRecords                    INTEGER(0..6),
    vuTimeAdjustmentRecords                 SET SIZE(noOfVuTimeAdjRecords) OF
                                            VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords je broj zapisa u vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords je niz zapisa o podešavanju vremena.

2.153. **VuTimeAdjustmentRecord**

Informacija spremljena u jedinici u vozilu, povezana s podešavanjem vremena provedenim izvan okvira redovnih kalibriranja (zahtjev 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
    oldTimeValue                            TimeReal,
    oldTimeValue                            TimeReal,
    newTimeValue                            TimeReal,
    workshopName                            Name,
    workshopAddress                         Address,
    workshopCardNumber                      FullCardNumber
}
```

oldTimeValue, newTimeValue su stara i nova vrijednost datuma i vremena.

workshopName, workshopAddress su naziv i adresa radionice.

workshopCardNumber identificira karticu radionice korištenu za podešavanje vremena.

2.154. **W-VehicleCharacteristicConstant**

Karakteristični koeficijent vozila (definicija k).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Dodjela vrijednosti: Impulsi po kilometru u djelatnom rasponu od 0 do 64 255 impulsa/km.

2.155. **WorkshopCardApplicationIdentification**

Informacija pohranjena na kartici radionice, povezana s identifikacijom primjene kartice (zahtjev 190).

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId                  EquipmentType,
    cardStructureVersion                    CardStructureVersion,
    noOfEventsPerType                       NoOfEventsPerType,
    noOfFaultsPerType                       NoOfFaultsPerType,
    activityStructureLength                 CardActivityLengthRange,
    noOfCardVehicleRecords                  NoOfCardVehicleRecords,
    noOfCardPlaceRecords                    NoOfCardPlaceRecords,
    noOfCalibrationRecords                  NoOfCalibrationRecords
}
```

typeOfTachographCardId naznačuje vrstu primijenjene kartice.

cardStructureVersion naznačuje verziju strukture primijenjenu na kartici.

noOfEventsPerType je broj događaja po tipu događaja koje kartica može zabilježiti.

noOfFaultsPerType je broj pogrešaka po tipu pogrešaka koje kartica može zabilježiti.

activityStructureLength označuje broj bajtova raspoloživih za spremanje zapisa o aktivnosti.

noOfCardVehicleRecords je broj zapisa vozila koje može sadržavati kartica.

noOfCardPlaceRecords je broj mjesta koje može zabilježiti kartica.

noOfCalibrationRecords je broj zapisa kalibracija koje može spremiti kartica.

2.156. **WorkshopCardCalibrationData**

Informacija spremljena na kartici radionice, povezana s radioničkim radom s karticom (zahtjevi 227 i 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
    calibrationTotalNumber                  INTEGER(0..2^16-1),
    calibrationPointerNewestRecord          INTEGER(0..NoOfCalibrationRecords-1),
    calibrationRecords                      SET SIZE(NoOfCalibrationRecords) OF
                                            WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber je ukupni broj kalibracija obavljenih s karticom.

calibrationPointerNewestRecord je indeks zadnjeg ažuriranog zapisa kalibracije.

Dodjela vrijednosti: Broj koji odgovara brojaču evidencije kalibracije, počevši s ‚0' za prvu pojavu zapisa kalibriranja u strukturi.

calibrationRecords je niz zapisa koji sadrže informacije o kalibraciji i/ili podešavanju vremena.

2.157. **WorkshopCardCalibrationRecord**

Informacija spremljena na kartici radionice povezana s obavljenim kalibriranjem s tom karticom (zahtjev 227).

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
    calibrationPurpose                      CalibrationPurpose,
    vehicleIdentificationNumber             VehicleIdentificationNumber,
    vehicleRegistration                     VehicleRegistrationIdentification,
    wVehicleCharacteristicConstant          W-VehicleCharacteristicConstant,
    kConstantOfRecordingEquipment           K-ConstantOfRecordingEquipment,
    lTyreCircumference                      L-TyreCircumference,
    tyreSize                                TyreSize,
```

```
    authorisedSpeed                 SpeedAuthorised,
    oldOdometerValue                OdometerShort,
    newOdometerValue                OdometerShort,
    oldTimeValue                    TimeReal,
    newTimeValue                    TimeReal,
    nextCalibrationDate             TimeReal,
    vuPartNumber                    VuPartNumber,
    vuSerialNumber                  VuSerialNumber,
    sensorSerialNumber              SensorSerialNumber
}
```

calibrationPurpose je svrha kalibracije.

vehicleIdentificationNumber je VIN.

vehicleRegistration sadrži registracijsku oznaku vozila i državu članicu registracije vozila.

wVehicleCharacteristicConstant je karakteristični koeficijent vozila.

kConstantOfRecordingEquipment je konstanta tahografa.

lTyreCircumference je djelatni opseg guma kotača.

tyreSize je oznaka dimenzija guma na vozilu.

authorisedSpeed je najviša dopuštena brzina vozila.

oldOdometerValue, newOdometerValue su staro i novo stanje brojača kilometara.

oldTimeValue, newTimeValue su stara i nova vrijednost datuma i vremena.

nextCalibrationDate je datum sljedeće kalibracije, tipa naznačenog u CalibrationPurpose pri ovlaštenom tijelu za kalibraciju.

vuPartNumber, vuSerialNumber i **sensorSerialNumber** su podatkovni elementi za identifikaciju tahografa.

2.158. **WorkshopCardHolderIdentification**

Informacija pohranjena na kartici radionice, povezana s identifikacijom nositelja kartice (zahtjev 216).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
    workshopName                    Name,
    workshopAddress                 Address,
    cardHolderName                  HolderName,
    cardHolderPreferredLanguage     Language
}
```

workshopName je naziv radionice nositelja kartice.

workshopAddress je adresa radionice nositelja kartice.

cardHolderName je prezime i ime(na) nositelja kartice (npr. ime mehaničara).

cardHolderPreferredLanguage je odabrani jezik nositelja kartice.

2.159. **WorkshopCardPIN**

Osobni identifikacijski broj nadzorne kartice (zahtjev 213).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: PIN poznat nositelju kartice, desno popunjeno ‚FF' bajtima do 8 bajta.

3. DEFINICIJE RASPONA VRIJEDNOSTI I VELIČINA

Definicija promjenjivih vrijednosti korištenih za definicije u stavku 2.

TimeRealRange::= 2^{32}-1

3.1. **Definicije za karticu vozača:**

Naziv promjenjive vrijednosti	Minimum	Maksimum
CardActivityLengthRange	5 544 bajta (28 dana po 93 promjena aktivnosti na dan)	13 776 bajta (28 dana po 240 promjena aktivnosti na dan)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2. **Definicije za karticu radionice:**

Naziv promjenjive vrijednosti	Minimum	Maksimum
CardActivityLengthRange	198 bajta (1 dan s 93 promjena aktivnosti)	492 bajta (1 dan s 240 promjena aktivnosti)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfEventsPerType	6	6
NoOfCalibrationRecords	88	255

3.3. **Definicije za nadzornu karticu:**

Naziv promjenjive vrijednosti	Minimum	Maksimum
NoOfControlActivityRecords	230	520

3.4. **Definicije za karticu prijevoznika:**

Naziv promjenjive vrijednosti	Minimum	Maksimum
NoOfCompanyActivityRecords	230	520

4. NIZOVI ZNAKOVA

IA5Strings koriste ASCII znakove definirane u ISO/IEC 8824-1. Za čitljivost i lakši osvrt dodjela vrijednosti navedena je u nastavku. U slučaju nepodudarnosti ISO/IEC 8824-1 ima prednost pred ovom informativnom bilješkom.

```
! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Drugi nizovi znakova (Address, Name, VehicleRegistrationNumber) uz to koriste znakove definirane šiframa 192 do 255 u ISO/IEC 8859-1 (skup slova Latin1) ili u ISO/IEC 8859-7 (skup grčkih slova).

5. ŠIFRIRANJE

Kad su šifrirani prema pravilima šifriranja ASN.1, sve definirane vrste podataka se moraju šifrirati prema ISO/IEC 8825-2 (usklađena inačica).

Dodatak 2.

OPIS KARTICA TAHOGRAFA

Sadržaj

1. UVOD

1.1. **Kratice**

Za potrebe ovog Dodatka, primjenjuju se sljedeće kratice:

AC	uvjeti pristupa
AID	identifikator aplikacije
ALW	uvijek
APDU	podatkovna jedinica aplikacijskog protokola (struktura naredbe)
ATR	odaziv na povrat u početno stanje
AUT	autentificirano
C6, C7	kontakti br. 6 i 7 kartice opisani u ISO/IEC 7816-2
cc	satni ciklusi
CHV	informacija o provjeri nositelja kartice
CLA	bajt razreda naredbe APDU
DF	namjenska datoteka; DF može sadržavati druge datoteke (EF ili DF)
EF	elementarna datoteka
ENC	šifrirano: pristup moguć samo šifriranjem podataka
etu	elementarna jedinica vremena
IC	integrirani krug
ICC	kartica s integriranim krugom
ID	identifikator
IFD	naprava sučelja
IFS	veličina informacijskog polja
IFSC	veličina informacijskog polja za karticu
IFSD	veličina informacijskog polja naprave (za terminal)
INS	bajt instrukcije APDU naredbe
Lc	dužina ulaznih podataka za naredbu APDU
Le	dužina očekivanih podataka (izlazni podaci za naredbu)
MF	glavna datoteka (temeljna DF)
P1-P2	parametarski bajti
NAD	adresa čvora korištena u protokolu T = 1
NEV	nikad
PIN	osobni identifikacijski broj
PRO SM	zaštićeno sigurnim prijenosom poruka
PTS	odabir prijenosa protokola
RFU	namijenjeno budućoj uporabi

RST	vraćanje u prijašnje stanje (kartice)
SM	siguran prijenos poruka
SW1-SW2	statusni bajti
TS	početni ATR znak
VPP	napon programiranja
XXh	vrijednost XX u heksadecimalnom zapisu
||	simbol ulančavanja 03||04 = 0304.

1.2. **Literatura**

U ovom su Dodatku korišteni sljedeći naslovi:

EN 726-3	Sustavi identifikacijskih kartica - Telekomunikacijske kartice s integriranim krugom (krugovima) i terminali - Dio 3: Zahtjevi za karticu neovisni od aplikacije. Prosinac, 1994.
ISO/IEC 7816-2	Informacijska tehnologija - Identifikacijske kartice — Kontaktne kartice s integriranim krugom (krugovima) - Dio 2: Dimenzije i položaj kontakata. Prvo izdanje: 1999.
ISO/IEC 7816-3	Informacijska tehnologija - Identifikacijske kartice - Kontaktne kartice s integriranim krugom (krugovima) - Dio 3: Elektronski signali i protokoli prijenosa. 2.izdanje: 1997.
ISO/IEC 7816-4	Informacijska tehnologija - Identifikacijske kartice — Kontaktne kartice s integriranim krugom (krugovima) - Dio 4: Međugranske naredbe za razmjenu. Prvo izdanje: 1995 + 1. dopuna: 1997.
ISO/IEC 7816-6	Informacijska tehnologija - Identifikacijske kartice - Kontaktne kartice s integriranim krugovima - Dio 6: Međugranski podatkovni elementi. Prvo izdanje: 1996 + 1. korekcija: 1998.
ISO/IEC 7816-8	Informacijska tehnologija - Identifikacijske kartice - Kontaktne kartice s integriranim krugom (krugovima) - Dio 8: Zaštitne međugranske naredbe. Prvo izdanje: 1999.
ISO/IEC 9797	Informacijska tehnologija - Zaštitne tehnike - Mehanizam podatkovne cjelovitosti uporabom funkcije kriptografske provjere s blok šifarskim algoritmom. 2. izdanje: 1994.

2. ELEKTRIČNA I FIZIČKA OBILJEŽJA

TCS_200 Ako nije drukčije propisano, svi elektronski signali moraju biti u skladu s ISO/IEC 7816-3.

TCS_201 Položaj i dimenzije kontakata kartice moraju biti u skladu s ISO/IEC 7816-2.

2.1. **Napon napajanja i potrošnja struje**

TCS_202 Kartica mora raditi prema specifikacijama unutar granica potrošnje naznačenim u ISO/IEC 7816-3.

TCS_203 Kartica mora raditi sa V_{cc} = 3 V (± 0,3 V) ili sa V_{cc} = 5 V (± 0,5 V).

Odabir napona se vrši prema ISO/IEC 7816-3.

2.2. **Napon programiranja V_{pp}**

TCS_204 Kartica ne zahtijeva napon programiranja na pinu C6. Očekuje se da pin C6 nije priključen na IFD. Kontakt C6 se može priključiti na V_{cc} u kartici, ali ne i uzemljiti. Ovaj napon se ni u kojem slučaju ne smije obrađivati.

2.3. **Generiranje i frekvencija sata**

TCS_205 Kartica radi u frekventnom području od 1 do 5 MHz. Unutar jedne razmjene podataka s karticom frekvencija sata može odstupati za ± 2 %. Frekvenciju sata generira jedinica u vozilu a ne sama kartica. Radni ciklus se može izmjenjivati između 40 i 60 %.

TCS_206 U uvjetima sadržanim u datoteci kartice EF_{ICC}, se može zaustaviti vanjski sat. Prvi bajt sadržaja datoteke EF_{ICC} šifrira uvjete režima Clockstop (za pojedinosti pogledati EN 726-3).

Niska	Visoka		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop dopušten, nema povlaštene razine
0	1	1	Clockstop dopušten, povlaštena visoka razina.
1	0	1	Clockstop dopušten, povlaštena niska razina.
0	0	0	Clockstop nije dopušten
0	1	0	Clockstop dopušten samo na visokoj razini.
1	0	0	Clockstop dopušten samo na niskoj razini.

Bitovi od 4 do 8 se ne koriste.

2.4. **Kontakt I/O**

TCS_207 Kontakt I/O C7 se koristi za prijem podataka iz IFD i odašiljanje podataka u IFD. Tijekom rada, samo kartica ili IFD mora biti u režimu odašiljanja. Ako su obje jedinice u režimu odašiljanja, to ne uzrokuje oštećenje kartice. Kad ne odašilje, kartica ulazi u režim prijema.

2.5. **Stanja kartice**

TCS_208 Dok je priključeno napajanje kartica radi u dva stanja:

— radno stanje dok izvršava naredbe ili se spaja s digitalnom jedinicom,

— stanje mirovanja u svako drugo vrijeme; u tom stanju kartica zadržava sve podatke.

3. HARDVER I KOMUNIKACIJA

3.1. **Uvod**

Ovaj stavak opisuje minimalnu funkcionalnost za kartice tahografa i jedinice u vozilu kojima se osigurava ispravan rad i interoperabilnost.

Kartice tahografa su što je više moguće sukladne raspoloživim primjenjivim ISO/IEC normama (posebno ISO/IEC 7816). No ipak, naredbe i protokoli su u cijelosti opisani kako bi se odredila neka ograničena uporaba ili neke razlike ako ih ima. Ako nije drukčije naznačeno, navedene naredbe su u cijelosti u skladu sa spomenutim normama.

3.2. **Protokol prijenosa**

TCS_300 Protokol prijenosa je u skladu s ISO/IEC 7816-3. Konkretno, jedinica vozila mora raspoznati produljenja vremena čekanja koje odašilje kartica.

3.2.1. ***Protokoli***

TCS_301 Kartica mora predvidjeti i protokol T = 0 i protokol T = 1.

TCS_302 T = 0 je standardni protokol, stoga je potrebna naredba PTS za prijelaz na protokol T = 1.

TCS_303 Naprave podržavaju neposrednu konvenciju u oba protokola, pa je stoga za karticu obavezna neposredna konvencija.

TCS_304 Bajt ‚Informacija o veličini kartičnog polja' je prisutan pri ATR u znaku TA3. Ta vrijednost iznosi najmanje ‚F0h' (= 240 bajta).

Na protokole se primjenjuju sljedeća ograničenja:

TCS_305 T = 0

— Naprava sučelja podržava odgovor na I/O nakon vršnog signala na RST od 400 cc.

— Naprava sučelja čita znakove s razmakom od 12 etu.

— Naprava sučelja čita pogrešan znak i njegovo ponavljanje ako su razmaci 13 etu. Ako je otkriven pogrešan znak, može se pojaviti signal pogreške na I/O između 1 etu i 2 etu. Naprava podržava kašnjenje od 1 etu.

— Naprava sučelja prihvaća 33-bajtni ATR (TS + 32).

— Ako je u ATR prisutan TC1, za znakove koje šalje naprava sučelja prisutan je dodatni zaštitno vrijeme, iako znakovi koje šalje kartica još uvijek mogu biti razmaknuti 12 etu. Ovo također vrijedi i za znak ACK, kojeg kartica šalje nakon znaka P3 kojeg odašilje naprava sučelja.

— Naprava sučelja uzima u obzir znak NUL kojega odašilje kartica.

— Naprava sučelja prihvaća komplementarne režime za ACK.

— Naredba traži odgovor te se ne može koristiti u režimu ulančavanja za dobivanje podataka čija bi dužina mogla prelaziti 255 bajta.

TCS_306 T = 1

— Bajt NAD: ne koristi se (NAD se postavlja na ‚00').

— ABORT S-bloka: ne koristi se.

— Pogreška stanja VPP S-bloka: ne koristi se.

— Ukupna dužina ulančavanja podatkovnog polja ne prelazi 255 bajta (što osigurava IFD).

— Veličinu podatkovnog polja za uređaj (IFSD) navodi IFD odmah nakon ATR: IFD šalje zahtjev za IFS S-blokanakon ATR, a kartica šalje natrag IFS S-bloka. Preporučena vrijednost za IFSD je 254 bajta.

— Kartica ne traži ponovno podešavanje IFS-a.

3.2.2. ***ATR***

TCS_307 Naprava provjerava bajte ATR prema ISO/IEC 7816-3. Ne vrši se provjera na povijesnim znakovima ATR.

Primjer osnovnog biprotokola ATR prema ISO/IEC 7816-3

Znak	Vrijednost	Napomene
TS	‚3Bh'	Označuje neposrednu konvenciju
T0	‚85h'	Prisutan TD1; prisutno 5 povijesnih bajtova
TD1	‚80h'	Prisutan TD2; koristi se T = 0
TD2	‚11h'	Prisutan TA3; koristi se T = 1
TA3	‚XXh' (min. ‚F0h')	Veličina informacijskog polja na kartici (IFSC)
TH1 do TH5	‚XXh'	Povijesni znakovi
TCK	‚XXh'	Znak za provjeravanje (bez OR)

TCS_308 Nakon odaziva na povrat u početno stanje (ATR) implicitno se odabire glavna datoteka (MF) i ona postaje tekući imenik.

3.2.3. ***PTS***

TCS_309 T = 0 je standardni protokol. Za postavljanje protokola T = 1 uređaj šalje kartici PTS (poznat i kao PPS).

TCS_310 Kako su oba protokola T = 0 i T = 1 obavezni, temeljni PTS za izmjenu protokola je obavezan za karticu.

Kako je naznačeno u ISO/IEC 7816-3, PTS se može koristiti za prijelaz na brzine prijenosa podataka više od standardne brzine prijenosa podataka koju predlaže kartica u ATR (bajt TA(1)), ako postoji.

Za karticu su više brzine prijenosa podataka neobvezne.

TCS_311 Ako nije podržana niti jedna brzina prijenosa podataka osim standardne (ili ako odabrana brzina prijenosa podataka nije podržana), kartica ispravno odgovara na PTS prema ISO/IEC 7816-3 ispuštajući bajt PPS1.

Primjeri osnovnih PTS za odabir protokola su sljedeći:

Znak	Vrijednost	Napomene
PPSS	‚FFh'	Znak za početak
PPS0	‚00h' ili ‚01h'	Nema PPS1 do PPS3; ‚00h' za odabir T0, ‚01h' za odabir T1
PK	‚XXh'	Znak provjere: ‚XXh' = ‚FFh' ako je PPS0 = ‚00h' ‚XXh' = ‚FEh' ako je PPS0 = ‚01h'

3.3. **Uvjeti pristupa (AC)**

Uvjeti pristupa (AC) za naredbe UPDATE_BINARY i READ_BINARY su određeni za svaku elementarnu datoteku.

TCS_312 AC tekuće datoteke moraju biti zadovoljene prije pristupanja datoteci putem tih naredbi.

Definicije raspoloživih uvjeta pristupa su sljedeće:

— ALW: Radnja je uvijek moguća i može se provesti bez ograničenja.

— NEV: Radnja nije moguća nikada.

— AUT: Pravo koje odgovara uspješnoj vanjskoj autentifikaciji mora biti otvoreno (vrši se naredbom EXTERNAL_AUTHENTICATE).

— PRO SM: Naredba se mora odaslati s dodatnim kriptografskim ispitnim zbrojem putem sigurnog prijenosa poruka (vidjeti Prilog 11.).

— AUT i PRO-SM: (kombinirani).

Za naredbe obrade (UPDATE_BINARY i READ_BINARY) se na kartici mogu postaviti sljedeći uvjeti pristupa:

	UPDATE_BINARY	READ_BINARY
ALW	Da	Da
NEV	Da	Da
AUT	Da	Da
PRO SM	Da	Ne
AUT i PRO SM	Da	Ne

Uvjet pristupa PRO SM nije raspoloživ za naredbu READ_BINARY. To znači da prisutstvo kriptografske provjere ispitnog zbroja za naredbu READ nije nikad obavezno. No korištenjem vrijednosti ‚OC' za razred, moguće je primijeniti naredbu READ_BINARY sa sigurnosnim prijenosom poruka, kako je opisano u stavku 3.6.2.

3.4. **Šifriranje podataka**

Kada treba zaštititi povjerljivost podataka za čitanje iz datoteke, datoteka se označuje kao ‚šifrirana'. Šifriranje se vrši putem sigurnog prijenosa poruka (vidjeti Dodatak 11.).

3.5. **Pregled šifri naredbi i pogrešaka**

Naredbe i ustroj datoteka su izvedeni i usklađeni sa ISO/IEC 7816-4.

TCS_313 Ovaj odjeljak opisuje sljedeće parove naredbi i odgovora APDU:

Naredba	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 Statusne riječi SW1 SW2 su uključene u svaku poruku odgovora i označivaju stanje obrade naredbe.

SW1	SW2	Značenje
90	00	Normalna obrada
61	XX	Normalna obrada. XX = broj raspoloživih bajtova odgovora
62	81	Obrada uz upozorenje. Dio vraćenih podataka može biti neispravan.
63	CX	Pogrešan CHV (PIN). ‚X' osigurava brojač preostalih pokušaja.
64	00	Pogreška u izvedbi – Stanje postojane memorije nepromijenjeno. Pogreška cjelovitosti.
65	00	Pogreška u izvedbi – Stanje postojane memorije promijenjeno.
65	81	Pogreška u izvedbi – Stanje postojane memorije promijenjeno. Pogreška memorije
66	88	Sigurnosna pogreška: pogrešan kriptografski ispitni zbroj (prilikom sigurnosnog prijenosa poruka) ili pogrešan certifikat (prilikom provjere certifikata) ili pogrešan kriptogram (prilikom vanjske autentifikacije) ili pogrešan potpis (prilikom provjere potpisa)
67	00	Pogrešna dužina (pogrešan Lc ili Le)
69	00	Zabranjena naredba (nema odgovora u T = 0)
69	82	Sigurnosni status nije zadovoljen
69	83	Blokiran način autentifikacije
69	85	Uvjeti uporabe nisu zadovoljeni
69	86	Naredba nije dopuštena (nema tekuće EF)
69	87	Nedostaju očekivani podatkovni objekti sigurnog prijenosa poruka
69	88	Neispravni podatkovni objekti sigurnog prijenosa poruka
6A	82	Datoteka nije pronađena
6A	86	Pogrešni parametri P1-P2
6A	88	Podaci na koje upućuje naredba nisu pronađeni
6B	00	Pogrešni parametri (protuvrijednost izvan EF)

SW1	SW2	Značenje
6C	XX	Pogrešna dužina, SW2 označuje točnu dužinu. Podatkovno polje ne uzvraća
6D	00	Naredbena šifra nije podržana ili nije valjana
6E	00	Razred nije podržan
6F	00	Ostale pogreške provjere

3.6. **Opis naredbi**

U ovom su poglavlju opisane obavezne naredbe za kartice tahografa.

Daljnje predmetne pojedinosti, povezane s obuhvaćenim kriptografskim radnjama su navedene u Dodatku 11. ‚Zajednički sigurnosni mehanizmi'.

Sve naredbe su opisane neovisno o korištenom protokolu (T = 0 ili T = 1). Uvijek su naznačeni APDU bajtovi CLA, INS, PI, P2, Lc i Le. Ako Lc ili Le nisu potrebni za opisanu naredbu, pridružena duljina, vrijednost i opis su prazni.

TCS_315 Ako se zahtijevaju oba bajta dužine (Lc i Le), opisana naredba se mora podijeliti u dva dijela ako IFD koristi protokol T = 0: IFD šalje naredbu opisanu s P3 = Lc + podaci, a potom šalje naredbu GET_RESPONSE (vidjeti točku 3.6.6.) uz P3 = Le.

TCS_316 Ako se zahtijevaju oba bajta dužine, a Le = 0 (sigurni prijenos poruka):

— Prilikom korištenja protokola T = 1, kartica odgovara na Le = 0 slanjem svih raspoloživih izlaznih podataka.

— Prilikom korištenja protokola T = 0, IFD šalje prvu naredbu s P3 = Lc + podaci, kartica (na taj implicitni Le = 0) odgovara statusnim bajtovima ‚61La', pri čemu je La broj raspoloživih bajtova odgovora. IFD potom generira naredbu GET RESPONSE sa P3 = La za čitanje podataka.

3.6.1. ***Odabir datoteke***

Ova naredba je u skladu s ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom definiranom u normi.

Naredba SELECT FILE se koristi:

— za odabir aplikacijske DF (obvezan odabir po imenu),

— za odabir elementarne datoteke koja odgovara ID predane datoteke.

3.6.1.1. *Odabir po nazivu (AID)*

Ova naredba omogućuje odabir aplikacijske DF na kartici.

TCS_317 Ova naredba može se izvoditi sa svakog mjesta u strukturi datoteke (poslije ATR ili u bilo koje drugo vrijeme).

TCS_318 Odabir aplikacije ponovo vraća tekuće sigurnosno okruženje. Nakon izvršenog odabira aplikacije ne bira se više niti jedan javni ključ, a ključ iz prethodne razmjene podataka više nije na raspolaganju za siguran prijenos poruka. Gubi se i uvjet pristupa AUT.

TCS_319 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	
INS	1	‚A4h'	
P1	1	‚A4h'	Odabir po nazivu (AID)
P2	1	‚0Ch'	Ne očekuje se nikakav odgovor
Lc	1	‚NNh'	Broj bajtova poslanih na karticu (dužina AID): ‚06h' za tahografsku aplikaciju
#6-#(5 + NN)	NN	‚XX..XXh'	AID: ‚FF 54 41 43 48 4F' za tahografsku aplikaciju

Za naredbu SELECT FILE nije potreban nikakav odgovor (nema Le u T = 1, ili se u T = 0 ne traži odgovor).

TCS_320 Odgovor na poruku (ne traži se odgovor)

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća ‚9000',

— Ako nije nađena aplikacija koja odgovara AID, uzvraćeno stanje obrade je ‚6A82',

— u T = 1, ako je prisutan bajt Le, uzvraćeno stanje obrade je ‚6700',

— u T = 0, ako se traži odziv poslije naredbe SELECT FILE, uzvraćeno stanje je ‚6900',

— ako se izabrana aplikacija smatra neispravnom (u atributima datoteke je otkrivena pogreška cjelovitosti), uzvraćeno stanje obrade je ‚6400' ili ‚6581'.

3.6.1.2. *Odabir elementarne datoteke korištenjem njezinog identifikatora datoteke*

TCS_321 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	
INS'	1	‚A4h'	
P1	1	‚02h'	Izbor EF u okviru tekuće DF
P2	1	‚0Ch'	Ne očekuje se nikakav odgovor
Lc	1	‚02h'	Broj bajta poslanih na karticu
#6-#7	2	‚XXXXh'	Identifikator datoteke

Za naredbu SELECT FILE nije potreban nikakav odgovor (Kod T = 1 nema Le, ili se ne traži odgovor kod T = 0).

TCS_322 Poruka odgovora (ne traži se odgovor)

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna kartica uzvraća ‚9000',

— ako nije nađena datoteka koja odgovara identifikatoru datoteke, uzvraćeno stanje obrade je ‚6A82',

— u T = 1, ako je prisutan bajt Le, uzvraćeno stanje je ‚6700',

— u T = 0, ako se traži odgovor poslije naredbe SELECT FILE, uzvraćeno stanje je ‚6900'

— ako se izabrana datoteka smatra neispravnom (u atributima datoteke je otkrivena pogreška cjelovitosti), uzvraćeno stanje je ‚6400' ili ‚6581'.

3.6.2. ***Binarno čitanje***

Ova naredba je u skladu s ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenoj u normi.

Naredba Read Binary se koristi za čitanje podataka iz transparentne datoteke.

Odgovor kartice se sastoji od uzvraćanja pročitanih podataka koji se mogu neobvezno zatvoriti u strukturu sigurnog čitanja poruke.

TCS_323 Ova naredba se može izvesti samo ako sigurnosni status zadovoljava sigurnosne atribute utvrđene za EF za funkciju READ:

3.6.2.1. *Naredba bez sigurnog prijenosa poruke*

Ova naredba omogućuje IFD-u čitanje podataka iz trenutačno odabrane EF bez sigurnog prijenosa poruka.

TCS_324 Čitanje podataka iz datoteke označene ‚Encrypted' nije moguće preko ove naredbe

TCS_325 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	Ne traži se siguran prijenos poruke
INS	1	‚B0h'	
P1	1	‚XXh'	Pomak u bajtima od početka datoteke: najznačajniji bajt
P2	1	‚XXh'	Pomak u bajtima od početka datoteke: najmanje značajan bajt
Le	1	‚XXh'	Duljina očekivanih podataka, broj bajtova koje treba pročitati

Napomena: bit 8 u P1 mora biti postavljen na 0.

TCS_326 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
#1-#X	X	‚XX..XXh'	Čitanje podataka
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna kartica uzvraća ‚9000',

— ako EF nije izabrana, uzvraćeno stanje obrade je ‚6986',

— ako kontrola pristupa odabrane datoteke nije zadovoljena, naredba se prekida s ‚6982',

— ako pomak ne odgovara veličini EF (pomak > veličina EF), uzvraćeno stanje obrade je ‚6B00',

— ako veličina podataka koje treba pročitati ne odgovara veličini EF (pomak + Le > veličina EF), stanje obrade je ‚6700' ili ‚6Cxx', pri čemu je ‚xx' točna duljina,

— ako je otkrivena pogreška cjelovitosti unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade ‚6400' ili ‚6581',

— ako je otkrivena pogreška cjelovitosti u pohranjenim podacima, kartica uzvraća tražene podatke, a uzvraćeno stanje obrade je ‚6281'.

3.6.2.2. *Naredba sa sigurnim prijenosom poruke*

Ova naredba omogućuje IDF-u čitanje podataka iz trenutačno odabranog EF uz siguran prijenos poruka radi povjere cjelovitosti primljenih podataka i zaštite povjerljivosti podataka u slučaju da je EF označena s ‚Encrypted'

TCS_327 Naredbena poruka

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚0Ch'	Traži se siguran prijenos poruka
INS	1	‚B0h'	INS
P1	1	‚XXh'	P1 (pomak u bajtima od početka datoteke): najznačajniji bajt
P2	1	‚XXh'	P2 (pomak u bajtima od početka datoteke): najmanje značajan bajt
Lc	1	‚09h'	Duljina ulaznih podatka za siguran prijenos poruka
#6	1	‚97h'	T_{LE}: oznaka za određivanje očekivane duljine specifikacije
#7	1	‚01h'	T_{LE}: oznaka očekivane duljine
#8	1	‚NNh'	Određivanje očekivane duljina (originalni Le): broj bajtova koje treba pročitati

Bajt	Duljina	Vrijednost	Opis
#9	1	‚8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#10	1	‚04h'	LCC: duljina sljedećeg kriptografskog kontrolnog zbroja
#11-#14	4	‚XX..XXh'	Kriptografski kontrolni zbroj (4 najznačajnija bajta)
Le	1	‚00h'	Utvrđeno u ISO/IEC 7816-4

TCS_328 Poruka odgovora na poruku ako EF nije označen s ‚Encrypted' i ako je format ulaza za siguran prijenos poruka točan:

Bajt	Duljina	Vrijednost	Opis
#1	1	‚81h'	T_{PV}: oznaka za nešifrirane podatke
#2	L	‚NNh' ili ‚81 NNh'	L_{PV}: duljina uzvraćenih podataka (= izvorni Le) L je 2 bajta, ako je L_{PV} < 127 bajta
#(2 + L)-#(1 + L+NN)	NN	‚XX..XXh'	Vrijednost nešifriranih podataka
#(2 + L+NN)	1	‚8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#(3 + L+NN)	1	‚04h'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja
#(4 + L+NN)-#(7 + L+NN)	4	‚XX..XXh'	Kriptografski kontrolni zbroj (4 najznačajnija bajta)
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

TCS_329 Odgovor na poruku ako je EF označen kao ‚Encrypted' i ako je ulazni format za siguran prijenos poruka točan:

Bajt	Duljina	Vrijednost	Opis
#1	1	‚87h'	$T_{PI\ CG}$: oznaka za šifrirane podatke (kriptogram)
#2	L	‚MMh' ili ‚81 MMh'	$L_{PI\ CG}$: duljina uzvraćenih šifriranih podataka (različita od izvorne Le naredbe zbog popunjenja) L je 2 bajta, ako je $L_{PI\ CG}$ > 127 bajtova
#(2 + L)-#(1 + L+MM)	MM	‚01XX..XXh'	Šifrirani podaci: indikator popunjenja i kriptogram
#(2 + L+MM)	1	‚8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#(3 + L+MM)	1	‚04h'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja
#(4 + L+MM)-#(7 + L+MM)	4	‚XX..XXh'	Kriptografski kontrolni zbroj (4 najznačajnija bajta)
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

Uzvraćeni šifrirani podaci sadrže prvi bajt koji prikazuje korišteni režim popunjenja. Za tahografsku primjenu indikator popunjenja uvijek ima vrijednost ‚01h', što znači da je primijenjen režim popunjenja utvrđen u ISO/IEC 7816-4 (jedan bajt koji ima vrijednost ‚80h', iza kojeg slijedi nekoliko nultih bajtova: metoda 2 po ISO/IEC 9797).

Stanja ‚normalne' obrade, opisana u naredbi READ BINARY bez sigurnog prijenosa poruka (vidjeti točku 3.6.2.1.), mogu se uzvratiti tako da se koriste gore opisane strukture poruka odgovora, pod oznakom ‚99h' (opisano u TCS_335).

Osim toga mogu se dogoditi i neke pogreške posebno vezane uz siguran prijenos poruka. U tom slučaju se stanje obrade jednostavno uzvraća bez uključivanja strukture sigurnog prijenosa poruka.

TCS_330 Poruka odgovora kod netočnog ulaznog formata za siguran prijenos poruka

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako ne postoji ključ tekuće razmjene podataka, uzvraća se stanje obrade ‚6A88'. To se može dogoditi ako još nije napravljen ključ razmjene podataka ili ako je valjanost ključa razmjene podataka istekla (u tom slučaju IFD mora ponovo pokrenuti postupak međusobne autentifikacije za postavljanje novog ključa za razmjenu podataka).

— Ako neki očekivani podatkovni objekti (gore navedeni) nedostaju u formatu sigurnog prijenosa poruka, uzvraća se stanje obrade ‚6987': ova pogreška se događa ako nema očekivane oznake ili ako naredbodavni sadržaj nije pravilno izrađen.

— Ako neki podatkovni objekti nisu točni, uzvraćeno stanje obrade je ‚6988': ova pogreška se događa ako su prisutne sve tražene oznake, ali su neke duljine različite od onih očekivanih.

— Ako ne uspije provjera kriptografskog kontrolnog zbroja, uzvraćeno stanje obrade je ‚6688'.

3.6.3. ***Binarno ažuriranje***

Ova naredba je u skladu s ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenoj u normi.

Poruka naredbe UPDATE BINARY započinje ažuriranjem (brisanje + pisanje) bitova koji su već sadržani u binarnom obliku EF, s bitovima danim u naredbi APDU.

TCS_331 Naredba se može izvoditi samo ako sigurnosni status zadovoljava sigurnosne atribute utvrđene za EF za funkciju UPDATE (Ako pristupna kontrola funkcije UPDATE obuhvaća PRO SM, tada u naredbu mora biti dodan siguran prijenos poruka).

3.6.3.1. *Naredba bez sigurnog prijenosa poruke*

Ova naredba omogućuje IFD-u upisivanje podataka u trenutačno odabran EF bez da kartica provjerava cjelovitost primljenih podataka. Ovaj nešifrirani način je dopušten samo ako predmetna datoteka nije označena kao ‚Encrypted".

TCS_332 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	Ne traži se siguran prijenos poruka
INS	1	‚D6h'	
P1	1	‚XXh'	
P2	1	‚XXh'	Pomak u bajtovima od početka datoteke: najmanje značajan bajt
Lc	1	‚NNh'	Lc: duljina podataka koji se ažuriraju. Broj bajovta koje treba upisati
#6-#(5 + NN)	NN	‚XX..XXh'	Podaci koje treba upisati

Napomena bit 8 u P1 mora biti postavljen na 0.

TCS_333 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna kartica uzvraća ‚9000',

— ako nije izabran EF, uzvraćeno stanje obrade je ‚6986',

— ako nije udovoljeno pristupnoj kontroli za izabranu datoteku, naredba se prekida s ‚6982',

— ako pomak nije kompatibilan s veličinom EF (pomak > veličina EF), uzvraćeno stanje obrade je ‚6B00',

— ako veličina podataka koje treba upisati nije u skladu s veličinom EF (pomak + Le > veličina EF), uzvraćeni status obrade je ‚6700',

— ako je otkrivena pogreška cjelovitosti atributa datoteke, kartica smatra da je datoteka neispravna i nepopravljiva, a uzvraćeno stanje obrade je ‚6400' ili ‚6500',

— ako zapisivanje nije uspješno, uzvraćeno stanje obrade je ‚6581'.

3.6.3.2. *Naredba sa sigurnim prijenosom poruke*

Ova naredba omogućuje IFD-u upisivanje podataka u trenutačno izabranu EF, a kartica provjerava cjelovitost primljenih podataka. Obzirom da nije tražena povjerljivost podataka, podaci nisu šifrirani.

TCS_334 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚0Ch'	Siguran prijenos poruka. Zatraženo
INS	1	‚D6h'	INS
P1	1	‚XXh'	Pomak u bajtovima od početka datoteke: najznačajniji bajt
P2	1	‚XXh'	Pomak u bajtovima od početka datoteke: najmanje značajan bajt
Lc	1	‚XXh'	Duljina polja zaštićenih podataka
#6	1	‚81h'	T_{PV}: oznaka za vrijednost nešifriranih podataka
#7	L	‚NNh' ili ‚81 NNh'	L_{PV}: duljina odaslanih podataka L je 2 bajta, ako je L_{PV} > 127 bajtova
#(7 + L)-#(6 + L+NN)	NN	‚XX..XXh'	Vrijednost nešifriranih podataka (koje treba upisati)
#(7 + L+NN)	1	‚8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#(8 + L+NN)	1	‚04h'	L_{CC}: duljina sljedećeg kriptografskog kontrolnog zbroja
#(9 + L+NN)-#(12 + L+NN)	4	‚XX..XXh'	Kriptografski kontrolni zbroj (4 najznačajnija bajta)
Le	1	‚00h'	Kako je u utvrđeno u ISO/IEC 7816-4

TCS_335 Poruka odgovor pri pravilnom ulaznom formatu sigurnog prijenosa poruka

Bajt	Duljina	Vrijednost	Opis
#1	1	‚99h'	T_{SW}: oznaka za statusne riječi (koje treba zaštiti sa CC)
#2	1	‚02h'	L_{SW}: duljina uzvraćenih statusnih riječi
#3-#4	2	‚XXXXh'	Statusne riječi (SW1, SW2)
#5	1	‚8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbroj
#6	1	‚04h'	LCC: duljina sljedećeg kriptografskog kontrolnog zbroja
#7-#10	4	‚XX..XXh'	Kriptografski kontrolni zbroj (4 najznačajnija bajta)
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

‚Redovna' stanja obrade opisana za naredbu UPDATE BINARY bez sigurnog prijenosa poruka (vidjeti točku 3.6.3.1.) se mogu uzvratiti tako da se koristi gore opisana struktura poruka odgovora.

Osim toga, mogu se dogoditi i neke pogreške karakteristične za siguran prijenos poruka. U tom slučaju se stanje obrade jednostavno vraća bez uključivanja strukture sigurnog prijenosa poruka.

TCS_336 Poruka odgovora ako je u sigurnom prijenosu poruka došlo do pogreške

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako nema ključa tekuće razmjene podataka, uzvraćeno stanje obrade je ‚6A88',

— ako neki očekivani podatkovni objekti (gore navedeni) nedostaju u formatu sigurnog prijenosa poruka, uzvraća se stanje obrade ‚6987': ova pogreška se događa ako nedostaje očekivana oznaka ili ako naredbodavni sadržaj nije pravilno sastavljen,

— ako su neki podatkovni objekti neispravni, uzvraćeno stanje obrade je ‚6988': ova se pogreška događa ako postoje sve tražene oznake, ali su neke duljine različite od očekivanih,

— ako ne uspije provjera kriptografskih kontrolnih zbrojeva, stanje obrade je ‚6688'.

3.6.4. ***Traži zahtjev za lozinku***

Ova naredba je u skladu s ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Naredbom GET CHALLENGE se od kartice traži izdavanje zahtjeva za lozinku radi korištenja u sigurnosnom postupku u kojem se kartici šalju kriptogram ili šifrirani podaci.

TCS_337 Zahtjev za lozinku kojega izdaje kartica vrijedi samo za sljedeću naredbu koja koristi zahtjev za lozinku poslan kartici.

TCS_338 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	CLA
INS	1	‚84h'	INS
P1	1	‚00h'	P1
P2	1	‚00h'	P2
Le	1	‚08h'	Le (duljina očekivanog zahtjeva za lozinku)

TCS_339 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
#1-#8	8	‚XX..XXh'	Zahtjev za lozinku
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća ‚9000',

— ako se Le razlikuje od ‚08h', stanje obrade je ‚6700',

— ako parametri P1-P2 nisu točni, stanje obrade je ‚6A86'.

3.6.5. ***Provjeri***

Ova naredba je u skladu s ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Naredba Provjeri na kartici započinje usporedbu između CHV (PIN) podataka koji su poslani iz naredbe sa referentnih CHV pohranjenih na kartici.

Napomena: PIN koji unosi korisnik mora biti desno popunjen s bajtima ‚FFh' do duljine od 8 bajtova IFD-a.

TCS_340 Ako je naredba uspješna, otvaraju se prava koja odgovaraju predočenju CHV, a brojač preostalih pokušaja CHV se pokreće iznova.

TCS_341 Neuspješna usporedba se registrira na kartici kako bi se ograničio broj daljnjih pokušaja korištenja referentnog CHV.

TCS_342 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	CLA
INS	1	‚20h'	INS
P1	1	‚00h'	P1
P2	1	‚00h'	P2 (provjereni CHV je implicitno poznat)
Lc	1	‚08h'	Duljina odaslane šifre CHV
#6-#13	8	‚XX..XXh'	CHV

TCS_343 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna kartica uzvraća ‚9000',

— ako nije pronađen referentni CHV, uzvraćeno stanje obrade je ‚6A88',

— ako je CHV blokiran (brojač preostalih pokušaja za CHV je nula), uzvraćeno stanje obrade je ‚6983'. Kada se jednom nađe u tom stanju, CHV se više nikada ne može uspješno predočiti.

— ako je usporedba neuspješna, brojač preostalih pokušaja se smanjuje i uzvraća se status obrade ‚63CX' (X > 0, pri čemu je X jednak brojaču preostalih pokušaja CHV. X = ‚F', brojač preostalih pokušaja CHV je veći od ‚F'),

— ako se referentni CHV smatra neispravnim, uzvraćeno stanje obrade je ‚6400' ili ‚6581'.

3.6.6. ***Traži odgovor***

Ova naredba je u skladu sa ISO/IEC 7816-4.

Ova naredba (potrebna i dostupna samo za protokol T = 0) se koristi za prijenos pripremljenih podataka s kartice na sučelje tahografa (primjer gdje naredba uključuje i Lc i Le).

Naredba GET_RESPONSE mora biti izdana neposredno nakon naredbe za pripremu podataka, inače se podaci gube. Nakon izvršenja naredbe GET_RESPONSE (osim ako nastupi pogreška ‚61xx' ili ‚6Cxx', vidjeti dolje), ranije pripremljeni podaci više nisu dostupni.

TCS_344 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	
INS	1	‚C0h'	
P1	1	‚00h'	
P2	1	‚00h'	
Le	1	‚XXh'	Broj očekivanih bajtova

TCS_345 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
#1-#X	X	‚XX..XXh'	Podaci
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna kartica uzvraća ‚9000'.

— Ako kartica nije pripremila nikakve podatke, uzvraćeno stanje obrade je ‚6900' ili ‚6F00'.

— Ako Le prekorači broj raspoloživih bajtova ili ako je Le nula, uzvraćeno stanje obrade je ‚6Cxx', pri čemu ‚xx' označuje točan broj raspoloživih bajtova. U tom su slučaju pripremljeni podaci još uvijek dostupni za iduću naredbu GET_RESPONSE.

— Ako Le nije nula, a manji je od broja raspoloživih bajtova, kartica normalno šalje tražene podatke, a uzvraćeno stanje obrade je ‚61xx', pri čemu ‚xx' označuje broj dodatnih bajtova koji su još uvijek dostupni za iduću naredbu GET_RESPONSE.

— Ako naredba nije podržana (protokol T = 1), kartica uzvraća ‚6D00'.

3.6.7. ***PSO: provjeri certifikat***

Ova naredba je u skladu s ISO/IEC 7816-8, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Naredbu VERIFY CERTIFICATE kartica koristi za dobivanje javnog ključa i provjeru njegove valjanosti.

TCS_346 Ako je naredba VERIFY CERTIFICATE uspješna, javni ključ se pohranjuje za buduću uporabu u sigurno okruženje. Ovaj se ključ izričito postavlja za primjenu u sigurnosnim naredbama (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE ili VERIFY CERTIFICATE) za MSE naredbe (vidjeti točku 3.6.10.) tako da koristi svoj identifikator ključa.

TCS_347 U svakom slučaju, naredba VERIFY CERTIFICATE koristi javni ključ koji je ranije odabran u sklopu MSE naredbe za otvaranje certifikata. Ovaj javni ključ mora biti onaj države članice ili europski.

TCS_348 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	CLA
INS	1	‚2Ah'	Izvedba sigurnosne operacije
P1	1	‚00h'	P1
P2	1	‚AEh'	P2: podaci koji nisu šifrirani po BER-TLV (ulančavanje podatkovnih elemenata)
Lc	1	‚CEh'	Lc: duljina certifikata, 194 bajtova
#6-#199	194	‚XX..XXh'	Certifikat: ulančavanje podatkovnih elemenata (opisano u Dodatku 11.)

TCS_349 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća ‚9000',

— ako provjera certifikata nije uspjela, uzvraća se stanje obrade ‚6688'. Postupak provjere i otvaranja certifikata opisan je u Dodatku 11.,

— ako u sigurnosnom okruženju nije prisutan javni ključ, uzvraća se stanje obrade ‚6A88',

— ako se izabrani javni ključ (uporabljen za otvaranje certifikata) smatra oštećenim, uzvraćeno stanje obrade je ‚6400' ili ‚6581',

— ako je izabrani javni ključ (uporabljen za otvaranje certifikata) CHA.LSB (CertificateHolderAuthorisation.equipment-Type) različit od ‚00' (odnosno nije onaj države članice ili europski), uzvraćeno stanje obrade je ‚6985'.

3.6.8. ***Unutarnja autentifikacija***

Ova naredba je u skladu s ISO/IEC 7816-4.

Primjenom INTERNAL AUTHENTICATE naredbe, IFD može autentificirati karticu.

Postupak autentifikacije je opisan je u Dodatku 11. Obuhvaća sljedeća očitovanja:

TCS_350 Naredba INTERNAL AUTHENTICATE koristi privatni ključ kartice (izabran implicitno) za potpisivanje autentifikacijskih podataka, uključujući K1 (prvi element za dogovor o ključu za razmjenu podataka) i RND1, te koristi trenutačno izabrani javni ključ (putem posljednje narede MSE) za šifriranje potpisa i oblikovanje autentifikacijskog tokena (podrobnije u Dodatku 11.).

TCS_351 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	CLA
INS	1	‚88h'	INS
P1	1	‚00h'	P1
P2	1	‚00h'	P2
Lc	1	‚10h'	Duljina podataka poslanih kartici
#6-#13 |	8	‚XX..XXh'	Poziv uporabljen za autentifikaciju kartice
#14-#21	8	‚XX..XXh'	VU.CHR (vidjeti Dodatak 11.)
Le	1	‚80h'	Duljina podataka koji se očekuju od kartice

TCS_352 Odgovor na poruku

Bajt	Duljina	Vrijednost	Opis
#1-#128	128	‚XX..XXh'	Token autentifikacije kartice (vidjeti Dodatak 11.)
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna kartica uzvraća ‚9000',

— ako u sigurnosnom okruženju nema javnog ključa, uzvraćeno stanje obrade je ‚6A88',

— ako u sigurnosnom okruženju nema privatnog ključa, uzvraćeno stanje obrade je ‚6A88',

— ako VU.CHR ne odgovara identifikatoru trenutačnog javnoga ključa, uzvraćeno stanje obrade je ‚6A88',

— ako se izabrani privatni ključ smatra neispravnim, uzvraćeno stanje obrade je ‚6400' ili ‚6581'.

TCS_353 Ako je naredba INTERNAL_AUTHENTICATE uspješna, trenutačni ključ razmjene podataka, ako postoji, se briše i više nije dostupan. Za novi ključ razmjene podataka naredba EXTERNAL_AUTHENTICATE treba biti uspješno izvršena.

3.6.9. ***Vanjska autentifikacija***

Ova naredba je u skladu s ISO/IEC 7816-4.

S naredbom EXTERNAL AUTHENTICATE kartica može autentificirati IFD.

Postupak autentifikacije je opisan je u Dodatku 11. Sadrži sljedeća očitovanja:

TCS_354 Naredba GET CHALLENGE mora neposredno prethoditi naredbi EXTERNAL_AUTHENTICATE. Kartica izdaje zahtjev za lozinku izvana (RND3).

TCS_355 Provjera kriptograma koristi RND3 (zahtjev za lozinku koji šalje kartica), privatni ključ kartice (implicitno izabran) i javni ključ prethodno izabran naredbom MSE.

TCS_356 Kartica provjerava kriptogram; ako je točan, otvara se pristupni uvjet AUT.

TCS_357 Kriptogram ulaznih podataka nosi drugi element za dogovor o ključu razmjene podataka K2.

TCS_358 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	CLA
INS	1	‚82h'	INS
P1	1	‚00h'	P1
P2	1	‚00h'	P2 (javni ključ kojega treba koristiti je implicitno poznat, a prethodno je postavljen naredbom MSE)
Lc	1	‚80h'	Lc (dužina podataka poslanih na karticu)
#6-#133	128	‚XX..XXh'	Kriptogram (vidjeti Dodatak 11.)

TCS_359 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (statusne riječi (SW1, SW2))

— Ako je naredba uspješna kartica uzvraća ‚9000',

— ako u sigurnosnom okruženju nema javnog ključa, uzvraća se ‚6A88',

— ako CHA trenutačno postavljenog javnog ključa nije ulančavanje AID tahografskog programa i tipa opreme jedinice vozila, uzvraćeno stanje obrade je ‚6F00' (vidjeti Dodatak 11.),

— ako u sigurnosnom okruženju nije prisutan nikakav privatni ključ, uzvraćeno stanje obrade je ‚6A88',

— ako je provjera kriptograma pogrešna, uzvraćeno stanje obrade je ‚6688',

— ako ovoj naredbi neposredno ne prethodi naredba GET CHALLENGE, uzvraćeno stanje obrade je ‚6985',

— ako se izabrani privatni ključ smatra neispravnim, uzvraćeno stanje obrade je ‚6400' ili ‚6581'.

TCS_360 Ako je naredba EXTERNAL AUTHENTICATE uspješna, i ako je prvi dio ključa razmjene podataka dostupan iz uspješnog ranije izvršenog INTERNAL AUTHENTICATE, ključ razmjene podataka je postavljen za buduće naredbe uz siguran prijenos poruka.

TCS_361 Ako prvi dio ključa razmjene podataka nije dostupan iz prethodne naredbe INTERNAL AUTHENTICATE, onda se drugi dio ključa razmjene podataka, koji šalje IFD, ne pohranjuje na kartici. Tim se mehanizmom osigurava da se postupak međusobne autentifikacije obavlja redoslijedom utvrđenim u Dodatku 11.

3.6.10. ***Upravljanje sigurnosnim okruženjem***

Ova se naredba koristi za postavljanje javnoga ključa za potrebe autentifikacije.

Ova je naredba u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe je ograničena u smislu odgovarajuće norme.

TCS_362 Ključ naveden u podatkovnom polju MSE vrijedi za svaku datoteku DF tahografa.

TCS_363 Ključ naveden u podatkovnom polju MSE ostaje tekući javni ključ do sljedeće ispravne naredbe MSE.

TCS_364 Ako navedeni ključ (već) nije na kartici, sigurno okruženje ostaje nepromijenjeno.

TCS_365 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	CLA
INS	1	‚22h'	INS
P1	1	‚C1h'	P1: navedeni ključ vrijedi za sve kriptografske radnje
P2	1	‚B6h'	P2 (navedeni podaci u vezi digitalnog potpisa)
Lc	1	‚0Ah'	Lc: duljina idućeg podatkovnog polja
#6	1	‚83h'	Oznaka za navođenje javnoga ključa u asimetričnim slučajevima
#7	1	‚08h'	Duljina navedenog ključa (identifikatora ključa)
#8-#15	08h	‚XX..XXh'	Identifikator ključa utvrđen u Dodatku 11.

TCS_366 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna kartica uzvraća ‚9000',

— ako navedeni ključ nije na kartici, uzvraćeno stanje obrade je ‚6A88',

— ako nedostaju neki očekivani podatkovni objekti u formatu sigurnog prijenosa poruka, uzvraćeno stanje obrade je ‚6987'. To se može dogoditi ako nema oznake ‚83h',

— ako su neki podatkovni objekti netočni, uzvraćeno stanje obrade je ‚6988'. To se može dogoditi ako duljina identifikatora ključa nije ‚08h',

— ako se izabrani ključ smatra neispravnim, uzvraćeno stanje obrade je ‚6400' ili ‚6581'.

3.6.11. ***PSO: funkcija kompresije podataka***

Ova naredba služi za prijenos na karticu rezultata izračuna kompresije podataka. Ova se naredba koristi za provjeru digitalnog potpisa.

Vrijednost funkcije kompresije se pohranjuje u EEPROM za iduću naredbu provjere digitalnog potpisa.

Ova naredba je u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe je ograničena u odnosu na odgovarajuću normu.

TCS_367 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	CLA
INS	1	‚2Ah'	Izvedba sigurnosne operacije
P1	1	‚90h'	Vraćanje šifre funkcije kompresije podataka
P2	1	‚A0h'	Oznaka: podatkovno polje sadrži DO potreban za kompresiju podataka
Lc	1	‚16h'	Duljina Lc narednog podatkovnog polja
#6	1	‚90h'	Oznaka za šifru funkcije kompresije podataka
#7	1	‚14h'	Duljina šifre funkcije kompresije podataka
#8-#27	20	‚XX..XXh'	šifra funkcije kompresije

TCS_368 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna kartica uzvraća ‚9000',

— ako nedostaju neki očekivani podatkovni objekti (gore navedeni), uzvraća se stanje obrade ‚6987'. To se može dogoditi ako nema jedne od oznaka ‚90h',

— ako neki podatkovni objekti nisu točni, uzvraćeno stanje obrade je ‚6988'. Ova se pogreška javlja ako postoji tražena oznaka, ali duljine različite od ‚14h'.

3.6.12. ***Komprimiraj datoteku***

Ova naredba nije u skladu s ISO/IEC 7816-8. Stoga bajt CLA ove naredbe ukazuje da slijedi vlasnička uporaba PERFORM SECURITY OPERATION/HASH.

TCS_369 Naredba izvrši kompresiju datoteke se koristi za komprimiranje podatkovnog područja trenutačno izabranog transparentnog EF.

TCS_370 Rezultat postupka komprimiranja se sprema na kartici. Nakon toga se može koristiti za ishođenje digitalnog potpisa datoteke korištenjem naredbe PSO-COMPUTE_DIGITAL_ SIGNATURE. Ovaj rezultat ostaje na raspolaganju za naredbu COMPUTE DIGITAL SIGNATURE do sljedeće uspješne naredbe Perform Hash of File.

TCS_371 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚80h'	CLA
INS	1	‚2Ah'	Izvedba sigurnosne operacije
P1	1	‚90h'	Oznaka: kompresija
P2	1	‚00h'	P2: kompresija podataka trenutačno odabrane transparentne datoteke

TCS_372 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna kartica uzvraća ‚9000',

— ako nije izabrana niti jedna aplikacija, uzvraća se stanje obrade ‚6985',

— ako se izabrani EF smatra neispravnim (pogreške cjelovitosti atributa datoteke ili spremljenih podataka), uzvraćeno stanje obrade je ‚6400' ili ‚6581',

— ako izabrana datoteka nije transparentna, uzvraćeno stanje obrade je ‚6986'.

3.6.13. ***PSO: izračunaj digitalni potpis***

Ova se naredba koristi za izračun digitalnog potpisa iz šifre ranije izračunate funkcije kompresije podataka (vidjeti točku 3.6.12 PERFORM HASH of FILE).

Ova naredba je u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe je ograničena u smislu predmetne norme.

TCS_373 Za izračun digitalnog potpisa se koristi privatni ključ kartice koji je kartici implicitno poznat.

TCS_374 Kartica izvodi digitalni potpis korištenjem metode popunjenja, u skladu sa PKCS1 (za pojedinosti vidjeti Dodatak 11.).

TCS_375 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	CLA
INS	1	‚2Ah'	Izvedba sigurnosne radnje
P1	1	‚9Eh'	Digitalni potpis koji treba uzvratiti
P2	1	‚9Ah'	Oznaka: podatkovno polje sadrži podatke koje treba potpisati. Ako nije obuhvaćeno podatkovno polje, pretpostavlja se da su podaci već na kartici (komprimiranje datoteke).
Le	1	‚80h'	Duljina očekivanog potpisa

TCS_376 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
#1-#128	128	‚XX..XXh'	Potpis prethodno izračunate funkcije komprimiranja
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća ‚9000',

— ako se implicitno izabrani privatni ključ smatra neispravnim, uzvraćeno stanje obrade je ‚6400' ili ‚6581'.

3.6.14. ***PSO: provjeri digitalni potpis***

Ova naredba služi za provjeravanje digitalnog potpisa koji se pruža kao ulazni podatak, prema PKCS1 poruci, čija funkcija kompresije je poznata kartici. Kartica implicitno poznaje algoritam potpisa.

Ova naredba je u skladu s ISO/IEC 7816-8. Primjena ove naredbe je ograničena u usporedbi s odgovarajućom normom.

TCS_377 Naredba provjere digitalnog potpisa uvijek koristi javni ključ koji je odabran prethodnom naredbom upravljana sigurnim okruženjem i prethodnom šifrom kompresije unesenom naredbom PSO: funkcija kompresije.

TCS_378 Poruka naredbe

Bajt	Duljina	Vrijednost	Opis
CLA	1	‚00h'	CLA
INS	1	‚2Ah'	Izvedba sigurnosne operacije
P1	1	‚00h'	
P2	1	‚A8h'	Oznaka: podatkovno polje sadrži DO mjerodavnu za provjeru
Lc	1	‚83h'	Duljina Lc narednog podatkovnog polja
#28	1	‚9Eh'	Oznaka za digitalni potpis
#29-#30	2	‚8180h'	Duljina digitalnog potpisa (128 bajtova, šifriranih po ISO/IEC 7816-6)
#31-#158		‚XX..XXh'	Sadržaj digitalnog potpisa

TCS_379 Poruka odgovora

Bajt	Duljina	Vrijednost	Opis
SW	2	‚XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna kartica uzvraća ‚9000',

— ako ne uspije provjera potpisa, uzvraćeno stanje obrade je ‚6688'. Postupak provjeravanja je opisan ju Dodatku 11.,

— ako nije izabran javni ključ, uzvraćeno stanje obrade je ‚6A88',

— ako nedostaju neki očekivani podatkovni objekti (gore navedeni), uzvraćeno stanje obrade je ‚6987'. To se može dogoditi ako nema jedne od traženih oznaka,

— ako nema šifre funkcije komprimiranja za obradu naredbe (rezultat prethodne naredbe PSO: funkcija komprimiranja uzvraćeno stanje obrade je ‚6985',

— ako su neki podatkovni objekti netočni, uzvraćeno stanje obrade je ‚6988'. To se može dogoditi ako je duljina traženih podatkovnih objekata netočna,

— ako se izabrani javni ključ smatra neispravnim, uzvraćeno stanje obrade je ‚6400' ili ‚6581'.

4. STRUKTURA KARTICA TAHOGRAFA

Ovaj stavak propisuje strukture datoteka kartica tahografa za pohranjivanje dostupnih podataka.

Ne propisuje obvezne unutarnje strukture koje ovise o proizvođaču kartice, npr. zaglavlja datoteke, niti pohranjivanje i postupanje s podatkovnim elementima potrebnim samo za internu uporabu, kao npr. EuropeanPublicKey, CardPrivateKey, TDesSessionKey ili WorkshopCardPin.

Korisni memorijski kapacitet kartica tahografa iznosi najmanje 11 kilobajta. Mogu se koristiti i veći kapaciteti. U tom slučaju struktura kartice ostaje ista, ali se povećava broj zapisa nekih elemenata strukture. Ovaj stavak navodi najmanje i najveće vrijednosti brojeva ovih zapisa.

4.1. ***Struktura kartice vozača***

TCS_400 Kartica vozača nakon personalizacije mora imati sljedeću strukturu trajnih datoteka i uvjete pristupa datoteci.

datoteke	identifikacija datoteke	uvjeti pristupa: čitanje	uvjeti pristupa: ažuriranje	uvjeti pristupa: šifrirano
MF	3F00			
├─EF ICC	0002	INT	NIC	Ne
├─EF IC	0005	INT	NIC	Ne
└─DF Tachograph	0500			
├─EF Application_Identification	0501	INT	NIC	Ne
├─EF Card_Certificate	C100	INT	NIC	Ne
├─EF CA_Certificate	C108	INT	NIC	Ne
├─EF Identification	0520	INT	NIC	Ne
├─EF Card_Download	050E	INT	INT	Ne
├─EF Driving_Licence_Info	0521	INT	NIC	Ne
├─EF Events_Data	0502	INT	PRO MS/AUT	Ne
├─EF Faults_Data	0503	INT	PRO MS/AUT	Ne
├─EF Driver_Activity_Data	0504	INT	PRO MS/AUT	Ne
├─EF Vehicles_Used	0505	INT	PRO MS/AUT	Ne
├─EF Places	0506	INT	PRO MS/AUT	Ne
├─EF Current_Usage	0507	INT	PRO MS/AUT	Ne
├─EF Control_Activity_Data	0508	INT	PRO MS/AUT	Ne
└─EF Specific_Conditions	0522	INT	PRO MS/AUT	Ne

TCS_401 Strukture svih EF moraju biti transparentne.

TCS_402 Čitanje sa sigurnim prijenosom poruke mora biti omogućeno za sve datoteke u DF Tahograf.

TCS_403 Kartica vozača mora imati sljedeću podatkovnu strukturu:

element datoteke/podatka	broj zapisa	veličina (bajtova) min	veličina (bajtova) maks	unaprijed zadane vrijednosti
MF	*11411*	*24959*		
╠═EF ICC	*25*	*25*		
╚═CardIccIdentification	*25*	*25*		
├─clockStop	1	1	{00}	
├─cardExtendedSerialNumber	8	8	{00..00}	
├─cardApprovalNumber	8	8	{20..20}	
├─cardPersonaliserID	1	1	{00}	
├─embedderIcAssemblerId	5	5	{00..00}	
└─icIdentifier	2	2	{00..00}	
╠═EF IC	*8*	*8*		
╚═CardChipIdentification	*8*	*8*		
├─icSerialNumber	4	4	{00..00}	
└─icManufacturingReferences	4	4	{00..00}	
╚═DF Tachograph	*11378*	*24926*		
╠═EF Application_Identification	*10*	*10*		
╚═DriverCardApplicationIdentification	*10*	*10*		
├─typeOfTachographCardId	1	1	{00}	
├─cardStructureVersion	2	2	{00..00}	
├─noOfEventsPerType	1	1	{00}	
├─noOfFaultsPerType	1	1	{00}	
├─activityStructureLength	2	2	{00..00}	
├─noOfCardVehicleRecords	2	2	{00..00}	
└─noOfCardPlaceRecords	1	1	{00}	
╠═EF Card_Certificate	*194*	*194*		
╚═CardCertificate	194	194	{00..00}	
╠═EF CA_Certificate	*194*	*194*		
╚═MemberStateCertificate	194	194	{00..00}	
╠═EF Identification	*143*	*143*		
├─CardIdentification	*65*	*65*		
├─cardIssuingMemberState	1	1	{00}	
├─cardNumber	16	16	{20..20}	
├─cardIssuingAuthorityName	36	36	{20..20}	
├─cardIssueDate	4	4	{00..00}	
├─cardValidityBegin	4	4	{00..00}	
└─cardExpiryDate	4	4	{00..00}	
└─DriverCardHolderIdentification	*78*	*78*		
├─cardHolderName	*72*	*72*		
├─holderSurname	36	36	{00, 20..20}	
└─holderFirstNames	36	36	{00, 20..20}	
├─cardHolderBirthDate	4	4	{00..00}	
└─cardHolderPreferredLanguage	2	2	{20 20}	

EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_404 Sljedeće vrijednosti, koje se koriste za prikaz veličina u gornjoj tabeli, predstavljaju najmanje i najveće vrijednosti broja zapisa koje mora koristiti podatkovna struktura kartice vozača:

		min	maks
n_1	NoOfEventsPerType	**6**	12
n_2	NoOfFaultsPerType	**12**	24
n_3	NoOfCardVehicleRecords	**84**	200
n_4	NoOfCardPlaceRecords	**84**	112
n_6	CardActivityLengthRange	5 554 bajtova (28 dana * 93 promjene aktivnosti)	13 776 bajtova (28 dana *240 promjene aktivnosti)

4.2. ***Struktura kartice radionice***

TCS_405 Kartica radionice nakon personalizacije mora imati sljedeću strukturu trajnih datoteka i sljedeće uvjete pristupa datoteci:

		uvjeti pristupa		
datoteke	identifikacija datoteke	čitanje	ažuriranje	šifrirano
MF	3F00	INT		
├─EF ICC	0002	INT	NIC	Ne
├─EF IC	0005	INT	NIC	Ne
└─DF Tachograph	0500			
├─EF Application_Identification	0501	INT	NIC	Ne
├─EF Card_Certificate	C100	INT	NIC	Ne
├─EF CA_Certificate	C108	INT	NIC	Ne
├─EF Identification	0520	INT	NIC	Ne
├─EF Card_Download	0509	INT	INT	Ne
├─EF Calibration	050A	INT	PRO MS/AUT	Ne
├─EF Sensor_Installation_Data	050B	INT	NIC	Ne
├─EF Events_Data	0502	INT	PRO MS/AUT	Ne
├─EF Faults_Data	0503	INT	PRO MS/AUT	Ne
├─EF Driver_Activity_Data	0504	INT	PRO MS/AUT	Ne
├─EF Vehicles_Used	0505	INT	PRO MS/AUT	Ne
├─EF Places	0506	INT	PRO MS/AUT	Ne
├─EF Current_Usage	0507	INT	PRO MS/AUT	Ne
├─EF Control_Activity_Data	0508	INT	PRO MS/AUT	Ne
└─EF Specific_Conditions	0522	INT	PRO MS/AUT	Ne

TCS_406 Strukture svih EF moraju biti transparentne.

TCS_407 Čitanje sa sigurnim prijenosom poruke mora biti omogućeno za sve datoteke u DF Tahograf.

TCS_408 Kartica radionice mora imati sljedeću podatkovnu strukturu:

element datoteke/podatka	broj zapisa	veličina (bajtova) min	veličina (bajtova) maks	unaprijed zadane vrijednosti
MF		*11088*	*29061*	
╠═EF ICC		*25*	*25*	
╚═CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─icIdentifier		2	2	{00..00}
╠═EF IC		*8*	*8*	
╚═CardChipIdentification		*8*	*8*	
├─icSerialNumber		4	4	{00..00}
└─icManufacturingReferences		4	4	{00..00}
╚═DF Tachograph		*11055*	*29028*	
╠═EF Application_Identification		*11*	*11*	
╚═WorkshopCardApplicationIdentification		*11*	*11*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
├─noOfEventsPerType		1	1	{00}
├─noOfFaultsPerType		1	1	{00}
├─activityStructureLength		2	2	{00 00}
├─noOfCardVehicleRecords		2	2	{00 00}
├─noOfCardPlaceRecords		1	1	{00}
└─noOfCalibrationRecords		1	1	{00}

EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
EF Sensor_Installation_Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}

├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
═EF Places		*61*	*81*	
└─CardPlaceDailyWorkPeriod		*61*	*81*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*60*	*80*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
═EF Current_Usage		*19*	*19*	
└─CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
═EF Control_Activity_Data		*46*	*46*	
└─CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
│ ├─cardType		1	1	{00}
│ ├─cardIssuingMemberState		1	1	{00}
│ └─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
═EF Specific_Conditions		*10*	*10*	
└─SpecificConditionRecord	2	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_409 Sljedeće vrijednosti, koje se koriste za prikaz veličina u gornjoj tabeli, predstavljaju najmanje i najveće vrijednosti broja zapisa koje mora koristiti podatkovna struktura kartice radionice:

		min	maks
n_1	NoOfEventsPerType	**3**	3
n_2	NoOfFaultsPerType	**6**	6
n_3	NoOfCardVehicleRecords	**4**	8
n_4	NoOfCardPlaceRecords	**6**	8
n_6	CardActivityLengthRange	**88**	255
n_5	NoOfCalibrationRecords	198 bajtova (1 dan * 93 promjene aktivnosti)	492 bajtova (1 dan * 240 promjena aktivnosti)

4.3. ***Struktura nadzorne kartice***

TCS_410 Nakon personalizacije nadzorna kartica mora imati sljedeću strukturu trajnih datoteka i uvjete pristupa datoteci:

		uvjeti pristupa		
datoteke	identifikacija datoteke	čitanje	ažuriranje	šifrirano
MF	3F00			
├─EF ICC	0002	ALW	NEV	Ne
├─EF IC	0005	ALW	NEV	Ne
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	Ne
├─EF Card_Certificate	C100	ALW	NEV	Ne
├─EF CA_Certificate	C108	ALW	NEV	Ne
├─EF Identification	0520	AUT	NEV	Ne
└─EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	Ne

TCS_411 Strukture svih EF moraju biti transparentne.

TCS_412 Čitanje sa sigurnim prijenosom poruke mora biti omogućeno za sve datoteke u DF Tahograf.

TCS_413 Nadzorna kartica mora imati sljedeću podatkovnu strukturu:

element datoteke/podatka	broj zapisa	veličina (bajtova) min	veličina (bajtova) max	unaprijed zadane vrijednosti
MF		*11219*	*24559*	
╠═EF ICC		*25*	*25*	
╚═CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─icIdentifier		2	2	{00 00}
╠═EF IC		*8*	*8*	
╚═CardChipIdentification		*8*	*8*	
├─icSerialNumber		4	4	{00..00}
└─icManufacturingReferences		4	4	{00..00}
╚═DF Tachograph		*11186*	*24526*	
╠═EF Application_Identification		*5*	*5*	
╚═ControlCardApplicationIdentification		*5*	*5*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
└─noOfControlActivityRecords		2	2	{00 00}
╠═EF Card_Certificate		*194*	*194*	
╚═CardCertificate		194	194	{00..00}
╠═EF CA_Certificate		*194*	*194*	
╚═MemberStateCertificate		194	194	{00..00}
╠═EF Identification		*211*	*211*	
├─CardIdentification		*65*	*65*	
├─cardIssuingMemberState		1	1	{00}
├─cardNumber		16	16	{20..20}
├─cardIssuingAuthorityName		36	36	{00, 20..20}
├─cardIssueDate		4	4	{00..00}
├─cardValidityBegin		4	4	{00..00}
└─cardExpiryDate		4	4	{00..00}
└─ControlCardHolderIdentification		*146*	*146*	
├─controlBodyName		36	36	{00, 20..20}
├─controlBodyAddress		36	36	{00, 20..20}
├─cardHolderName				
├─holderSurname		36	36	{00, 20..20}
└─holderFirstNames		36	36	{00, 20..20}
└─cardHolderPreferredLanguage		2	2	{20 20}
╚═EF Controller_Activity_Data		*10582*	*23922*	
╚═ControlCardControlActivityData		*10582*	*23922*	
├─controlPointerNewestRecord		2	2	{00 00}
└─controlActivityRecords		*10580*	*23920*	
└─controlActivityRecord	n_7	*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlledCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlledVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}

TCS_414 Sljedeće vrijednosti koje se koriste za prikaz veličina u gornjoj tabeli su najmanje i najveće vrijednosti koje mora imati podatkovna struktura nadzorne kartice.

		min	maks
n_7	NoOfControlActivityRecords	230	520

4.4. *Struktura kartice prijevoznika*

TCS_415 Kartica prijevoznika nakon personalizacije mora imati sljedeću strukturu trajnih datoteka i sljedeće uvjete pristupa datoteci:

datoteke	identifikacija datoteke	uvjeti pristupa: čitanje	uvjeti pristupa: ažuriranje	uvjeti pristupa: šifrirano
MF	3F00			
├─EF ICC	0002	ALW	NEV	Ne
├─EF IC	0005	ALW	NEV	Ne
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	Ne
├─EF Card_Certificate	C100	ALW	NEV	Ne
├─EF CA_Certificate	C108	ALW	NEV	Ne
├─EF Identification	0520	AUT	NEV	Ne
└─EF Company_Activity_Data	050D	ALW	PRO SM / AUT	Ne

TCS_416 Strukture svih EF moraju biti transparentne.

TCS_417 Čitanje sa sigurnim prijenosom poruke mora biti omogućeno za sve datoteke u DF Tahograf.

TCS_418 Kartica prijevoznika mora imati sljedeću podatkovnu strukturu:

element datoteke/podatka	broj zapisa	veličina (bajtova) min	veličina (bajtova) maks	unaprijed zadane vrijednosti
MF		*11147*	*24487*	
╠EF ICC		*25*	*25*	
└CardIccIdentification		*25*	*25*	
├clockStop		1	1	{00}
├cardExtendedSerialNumber		8	8	{00..00}
├cardApprovalNumber		8	8	{20..20}
├cardPersonaliserID		1	1	{00}
├embedderIcAssemblerId		5	5	{00..00}
└icIdentifier		2	2	{00 00}
╠EF IC		*8*	*8*	
└CardChipIdentification		*8*	*8*	
├icSerialNumber		4	4	{00..00}
└icManufacturingReferences		4	4	{00..00}
╠DF Tachograph		*11114*	*24454*	
╠EF Application_Identification		*5*	*5*	
└CompanyCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfCompanyActivityRecords		2	2	{00 00}
╠EF Card_Certificate		*194*	*194*	
└CardCertificate		194	194	{00..00}
╠EF CA_Certificate		*194*	*194*	
└MemberStateCertificate		194	194	{00..00}
╠EF Identification		*139*	*139*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└CompanyCardHolderIdentification		*74*	*74*	
├companyName		36	36	{00, 20..20}
├companyAddress		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}
╠EF Company_Activity_Data		*10582*	*23922*	
└CompanyActivityData		*10582*	*23922*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*23920*	
└companyActivityRecord	n_8	46	46	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}

├─cardNumberInformation			
│ ├─cardType	1	1	{00}
│ ├─cardIssuingMemberState	1	1	{00}
│ └─cardNumber	16	16	{20..20}
├─downloadPeriodBegin	4	4	{00..00}
└─downloadPeriodEnd	4	4	{00..00}

TCS_419 Sljedeće vrijednosti koje se koriste za prikaz veličina u gornjoj tabeli predstavljaju najmanje i najveće vrijednosti broja zapisa koje mora imati podatkovna struktura kartice prijevoznika.

		min	maks
n8	NoOfCompanyActivityRecords	230	520

Dodatak 3.

PIKTOGRAMI

PIC_001 Tahograf može koristiti sljedeće piktograme i kombinacije piktograma:

1. OSNOVNI PIKTROGRAMI

	Osobe	**Radnje**	**Načini rada**
	Poduzeće		Prijevozni način
	Nadzornik	Nadzor	Nadzorni način
	Vozač	Vozač	Radni način
	Radionica/Ispitno mjesto	Ispitivanje/kalibracija	Kalibracijski način
	Proizvođač		

	Aktivnosti	**Trajanje**
	Pripravnost	Razdoblje tekuće pripravnosti
	Vožnja	Vrijeme neprekidne vožnje
	Odmor	Razdoblje tekućeg odmora
	Rad	Razdoblje tekućeg rada
	Pauza	Zbirno vrijeme pauza
	Nepoznato	

	Oprema	**Funcije**
1	Utor vozača	
2	Utor suvozača	
	Kartica	
	Sat	
	Prikaz	Prikazivanje
	Vanjsko spremanje	Preuzimanje podataka
	Napajanje	
	Pisač/Ispis	Ispisivanje
	Senzor	
	Dimenzije guma	
	Vozilo/Jedinica vozila	

	Posebni uvjeti
OUT	Izvan djelokruga
	Boravak na trajektu/vlaku

	Razno		
!	Događaji		Pogreške
	Početak dnevnog razdoblja aktivnosti		Kraj dnevnog razdoblja aktivnosti
	Mjesto	M	Ručni unos aktivnosti vozača
	Osiguranje		Brzina
	Vrijeme	Σ	Ukupno/sažetak

	Oznake
24h	Dnevno
I	Tjedno
II	dva tjedna
	Od ili do

2. KOMBINACIJE PIKTOGRAMA

	Razno		
	Mjesto nadzora		
	Mjesto početka dnevnog razdoblja aktivnosti		Mjesto kraja dnevnog razdoblja aktivnosti
	Od vremena		Do vremena
	U vozilu		
OUT	Početak aktivnosti izvan djelokruga	OUT	Kraj aktivnosti izvan djelokruga

Kartice

Kartica vozača
Kartica prijevoznika
Nadzorna kartica
Kartica radionice
Bez kartice

Vožnja

Vožnja u posadi
Vrijeme vožnje u tjedan dana
Vrijeme vožnje u dva tjedna

Ispisi

Dnevni ispis aktivnosti vozača s kartice
Dnevni ispis aktivnosti svih vozača iz jedinice u vozilu
Ispis događaja i pogrešaka s kartice
Ispis događaja i pogrešaka iz jedinice vozila
Ispis tehničkih podataka
Ispis prekoračenja brzine

Događaji

Umetanje nevažeće kartice
Sukob kartica
Preklapanje vremena
Vožnja bez odgovarajuće kartice
Umetanje kartice tijekom vožnje
Zadnja razmjena podataka s karticom nije pravilno završena
Prekoračenje brzine
Prekid napajanja
Pogreška podataka kretanja
Proboj zaštite
Podešavanje vremena (u radionici)
Kontrola prekoračenja brzine

Pogreške

Pogreška kartice (utor vozača)
Pogreška kartice (utor suvozača)
Pogreška prikaza
Pogreška preuzimanja podataka
Pogreška pisača
Pogreška senzora
Interna pogreška jedinice vozila

Postupak ručnog unosa

I dalje isto dnevno razdoblje aktivnosti?
Kraj prethodnog razdoblja aktivnosti?
Potvrdi ili unesi mjesto kraja razdoblja aktivnosti
Unesi vrijeme početka
Unesi mjesto početka razdoblja aktivnosti.

Napomena: Dodatne kombinacija piktograma za formiranje bloka ispisa ili identifikatora zapisa su utvrđene u Dodatku 4.

Dodatak 4.

ISPISI

SADRŽAJ

1. OPĆENITO

Svaki ispis nastaje povezivanjem raznih podatkovnih blokova koji se identificiraju identifikatorom bloka.

Jedan podatkovni blok sadrži jedan ili više zapisa, koji se mogu identificirati pomoću identifikatora zapisa.

PRT_001 Ako identifikator zapisa neposredno prethodi identifikatoru bloka, identifikator zapisa se ne ispisuje.

PRT_002 Ako je neka podatkovna stavka nepoznata ili se ne smije ispisati radi zaštite prava na pristup podacima, umjesto nje se ispisuju praznine.

PRT_003 Ako je sadržaj cijelog reda nepoznat ili ga ne treba ispisivati, tada se izostavlja cijeli red.

PRT_004 Numerička podatkovna polja se ispisuju u desnom poravnanju, s razmakom za tisuće i milijune i bez vodećih nula.

PRT_005 Polja s podatkovnim nizovima se ispisuju u lijevom poravnanju i pune prazninama do duljine podatkovnog elementa ili se skraćuju na duljinu podatkovnog elementa prema potrebi (imena i adrese).

2. SPECIFIKACIJA PODATKOVNOG BLOKA

U ovom poglavlju se koriste sljedeći dogovoreni formati bilježenja:

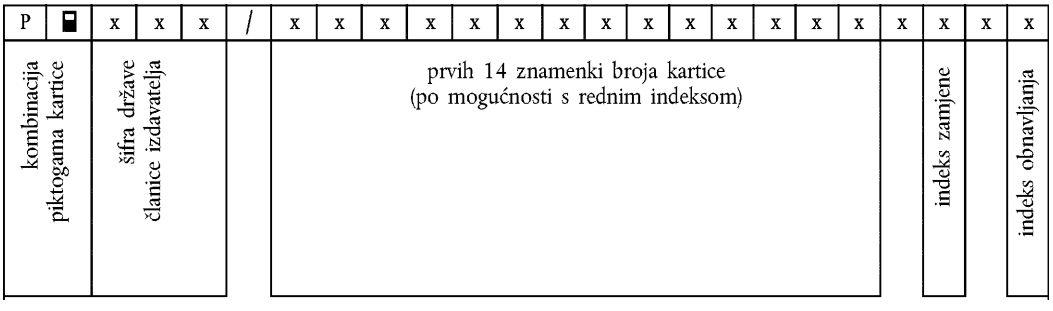
— Podebljano tiskana slova označivaju običan tekst koji se ispisuje (ispis ostaje u normalnim slovima),

— Normalna slova stoje za varijable (piktogrami ili podaci), koji se kod ispisa zamjenjuju njihovim vrijednostima,

— Imena varijabli su nadopunjena podcrtavanjem za prikaz duljine podatkovnog elementa raspoložive za primjenu,

— Datumi su prikazani u formatu ‚dd/mm/gggg' (dan, mjesec, godina). Može se koristiti i oblik ‚dd.mm.gggg',

— Izraz ‚Identifikator kartice' označuje slog koji se sastoji od sljedećeg: vrsta kartice prikazana kombinacijom piktograma, šifra države članice izdavatelja, kosa crta i broj kartice s indeksom zamjene i indeksom obnavljanja odvojenim razmakom:



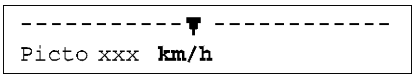
PRT_006 Za ispis se koriste sljedeći podatkovni blokovi i/ili podatkovni zapisi, sukladno sljedećim značenjima i formatima:

Broj bloka ili zapisa Znacenje	Format Podataka
1. **Datum i vrijeme ispisa dokumenta**	dd/mm/yyyy hh:mm **(UTC)**

2. **Vrsta ispisa**

Identifikator bloka

Kombinacija piktograma ispisa (vidjeti Dodatak 3.), podešenje ogranicavaca brzine (samo pri ispisu prekoracenja brzine).



3. **Identifikacija nositelja kartice**

Identifikator bloka P = Piktogram osoba

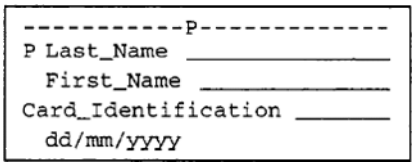
Prezime nositelja kartice

Ime(na) nositelja kartice (ako postoji)

Identifikacija kartice

Datum isteka valjanosti (ako postoji)

Ako kartica nije personalizirana ili ako ne sadrži prezime nositelja, umjesto toga se tiska naziv tvrtke, radionice ili nadzornog tijela.

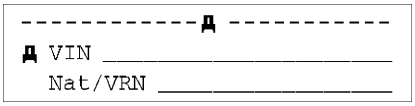


4. **Identifikacija vozila**

Identifikator bloka

Identifikacijska oznaka vozila

Država clanica registracije i registracijska oznaka vozila

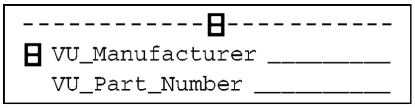


5. **Identifikacija jedinice vozila**

Identifikator bloka

Naziv proizvodaca jedinice vozila

Kataloški broj jedinice vozila.



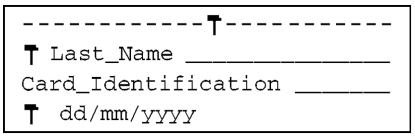
6. **Zadnja kalibracija tahografa**

Identifikator bloka

Naziv radionice

Identifikacija kartice radionice

Datum kalibracije



7. **Zadnji nadzor (od strane službenika za nadzor)**

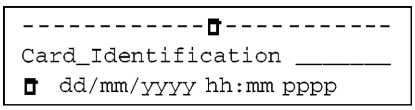
Identifikator bloka

Identifikacija nadzorne kartice

Datum, vrijeme i vrsta nadzora

Tip nadzora: Do cetiri piktograma. Tip nadzora može biti (kombinacija) sljedeceg:

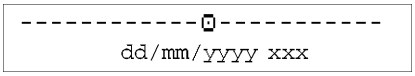
: Preuzimanje podataka s kartice : Preuzimanje podataka s jedinice vozila : Ispis : Prikaz.



8. **Aktivnosti vozaca pohranjene na kartici prema redoslijedu nastajanja**

Identifikator bloka

Datum upita (kalendarski dan predmet ispisa) + brojac dnevne nazocnosti kartice



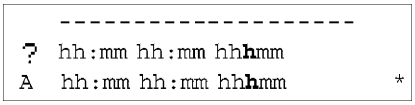
8.1. *Razdoblje u kojem kartica nije bila umetnuta*

8.1.a Identifikator bloka (pocetak razdoblja)

8.1.b *Nepoznato razdoblje.* Vrijeme pocetka i kraja, trajanje

8.1.c *Rucno unesena aktivnost*

Piktogram aktivnosti, vrijeme pocetka i kraja (ukljucivo), trajanje, razdoblje odmora od najmanje sat vremena je oznaceno zvjezdicom.

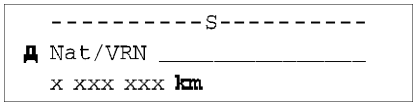


8.2. *Stavljanje kartice u utor S*

Identifikator bloka; S = piktogram utora

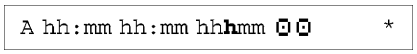
Država clanica registracije vozila i registracijska oznaka vozila

Stanje brojaca kilometara vozila kod umetanja kartice.

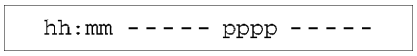


8.3. *Aktivnost (dok je kartica bila umetnuta)*

Piktogram aktivnosti, vrijeme pocetka i kraja (ukljucivo), trajanje, stanje posade (piktogram posade ako je stanje CREW, bez piktograma ako je stanje SINGLE, razdoblje odmora u trajanju od najmanje jedan sat je oznaceno zvjezdicom.

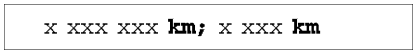


8.3.a *Posebno stanje*. Vrijeme unosa, piktogram posebnoga stanja (ili kombinacija piktograma).



8.4. *Izvlacenje kartice*

Brojac kilometara vozila i prijedena udaljenost od zadnjeg umetanja za koje je brojac kilometara poznat.

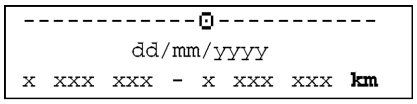


9. **Aktivnosti vozaca pohranjene u jedinici vozila, po utoru, kronološkim redom**

Identifikator bloka

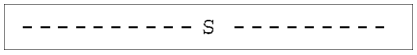
Datum upita (kalendarski dan ispisa)

Brojac kilometara vozila u 00:00 i 24:00.



10. **Aktivnosti koje se obavljaju u utoru S**

Identifikator bloka.



10.1. *Razdoblje kada u utoru S nema kartice*

Identifikator zapisa

Nije umetnuta kartica

Brojac kilometara vozila na pocetku razdoblja.

10.2. *Umetanje kartice*

Identifikator zapisa o umetanju kartice

Prezime vozaca

Ime vozaca

Identifikacija kartice vozaca

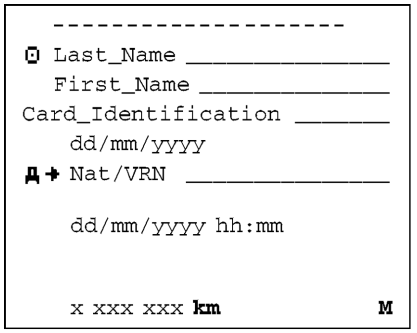
Datum isteka kartice vozaca

Država clanica registracije i registracijska oznaka prethodno korištenog vozila

Datum i vrijeme izvlacenja kartice iz prethodnog vozila

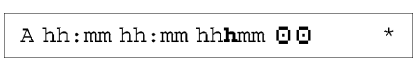
Prazna linija

Stanje brojaca kilometara vozila kod umetanja kartice, znak rucnog unosa aktivnosti vozaca (M ako rucni unos postoji, bez znaka ako rucni unio ne postoji).



10.3. *Aktivnost*

Piktogram aktivnosti, vrijeme pocetka i kraja (ukljucivo), trajanje, stanje posade (piktogram posade ako je CREW, bez oznake ako je SINGLE, odmori u trajanju od najmanje jedan sat oznaceni su zvjezdicom.



10.3.a *Posebno stanje*

Vrijeme unosa, piktogram posebnoga stanja (ili kombinacija piktograma).

```
hh:mm ----- pppp -----
```

10.4. *Izvlacenje kartice ili kraj razdoblja ‚bez kartice'*

Brojac kilometara vozila pri izvlacenju kartice ili na kraju razdoblja ‚bez kartice' i prijedena udaljenost od umetanja kartice ili od pocetka razdoblja ‚bez kartice".

```
x xxx xxx km; x xxx km
```

11. **Dnevni sažetak**

Identifikator bloka

```
----------Σ ---------
```

11.1. *Dnevni sažetak jedinice vozila za razdoblja bez kartice u utoru vozaca*

Identifikator bloka

```
10■ - - -
```

11.2. *Dnevni sažetak jedinice vozila za razdoblja bez kartice u utoru suvozaca*

Identifikator bloka

```
20■ - - -
```

11.3. *Dnevni sažetak jedinice vozila po vozacu*

Identifikator zapisa

Prezime vozaca

Ime(na) vozaca

Identifikacija vozacke kartice

```
  --------------------
0 Last_Name ________________
  First_Name ________________
Card_Identification _______
```

11.4. *Unos mjesta gdje dnevno razdoblje aktivnosti pocinje i/ili završava*

pi = piktogram mjesta pocetka/kraja, vrijeme, država, regija, stanje brojaca kilometara

```
pihh:mm  Cou  Reg
  x xxx  xxx  km
```

11.5. *Aktivnosti ukupno (s kartice)*

Ukupno trajanje vožnje, prijedena udaljenost

Ukupno trajanje rada i pripravnost

Ukupno trajanje odmora i nepoznato

Ukupno trajanje aktivnosti u posadi.

```
0  hhhmm x xxx km
⚒  hhhmm ⧈ hhhmm
⊢  hhhmm ? hhhmm
00 hhhmm
```

11.6. *Aktivnosti ukupno (razdoblje bez kartice u utoru vozaca)*

Ukupno trajanje vožnje, prijedena udaljenost

Ukupno trajanje rada i pripravnosti

Ukupno trajanje odmora.

```
0  hhhmm x xxx km
⚒  hhhmm ⧈ hhhmm
⊢  hhhmm
```

11.7. *Aktivnosti ukupno (razdoblje bez kartice u utoru suvozaca)*

Ukupno trajanje rada i pripravnosti

Ukupno trajanje odmora.

```
⚒  hhhmm ⧈ hhhmm
⊢  hhhmm
```

11.8. *Aktivnosti ukupno (po vozacu, ukljucuje oba utora)*

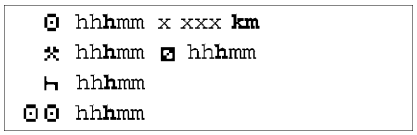
Ukupno trajanje vožnje, prijedena udaljenost

Ukupno trajanje rada i pripravnosti

Ukupno trajanje odmora

Ukupno trajanje aktivnosti u posadi

Ako se traži dnevni ispis za tekuci dan, dnevna sažeta informacija se izracunava iz dostupnih podataka u trenutku ispisa.



12. **Dogadaji i/ili pogreške spremljene na kartici**

12.1. Identifikator bloka 5 zadnjih ‚dogadaja i pogrešaka' s kartice

12.2. Identifikator bloka svih zabilježenih ‚dogadaja' na kartici

12.3. Identifikator bloka svih zabilježenih ‚pogrešaka' na kartici

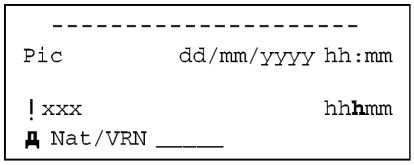
12.4. *Zapis dogadaja i/ili pogreške*

Identifikator zapisa

Piktogram dogadaj/pogreška, svrha zapisa, datum i vrijeme pocetka,

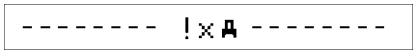
Dodatna šifra dogadaja/pogreške (ako postoji), trajanje

Država clanica registracije i registracijska oznaka vozila na kojem se dogodio dogadaj ili pogreška.



13. **Dogadaji i/ili pogreške, pohranjene ili se trenutacno dogadaju u jedinici vozila**

13.1. Identifikator bloka 5 zadnjih ‚dogadaja i pogrešaka' iz jedinice vozila



13.2. Identifikator bloka svi zabilježeni ili trenutacni ‚dogadaji' u jedinici vozila

13.3. Identifikator bloka sve zabilježene ili trenutacnih ‚pogrešaka" u jedinici vozila

13.4. *Zapis dogadaja i/ili pogreške*

Identifikator zapisa

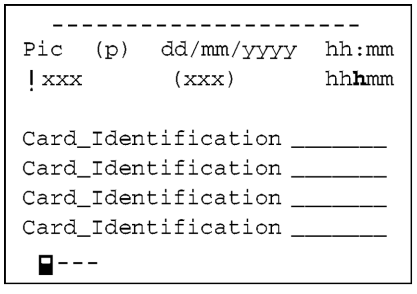
Piktogram dogadaja/pogreške, svrha zapisa, datum i vrijeme pocetka

Dodatna šifra dogadaja/pogreške (ako postoji), broj slicnih dogadaja tog dana, trajanje

Identifikacija kartica umetnutih na pocetku ili na kraju dogadaja ili pogreške (do 4 reda bez ponavljanja istih brojeva kartica dva puta)

Slucaj kada kartica nije umetnuta

Svrha zapisa (p) je numericka šifra, koja objašnjava zašto je dogadaj ili pogreška zabilježen; šifriranje u skladu s podatkovnim elementom EventFaultRecordPurpose.



14. **Identifikacija jedinice vozila**

Identifikator bloka

Naziv proizvodaca jedinice vozila

Adresa proizvodaca jedinice vozila

Kataloški broj jedinice vozila

Broj odobrenja jedinice vozila

Serijski broj jedinice vozila

Godina proizvodnje jedinice vozila

Verzija softvera instaliranog u jedinici vozila i datum instalacije

```
----------⊟----------
⊟ Name _____________________
  Address ___________________
  PartNumber ________
  Apprv _____________
  S/N ________
  yyyy
  V    xx.xx.xx   dd/mm/yyyy
```

15. **Identifikacija senzora**

Identifikator bloka

Serijski broj senzora

Broj odobrenja senzora

Datum prve ugradnje senzora.

```
-----------Л-----------
Л S/N ________
  Apprv _____________
  dd/mm/yyyy
```

16. **Kalibracjski podaci**

Identifikator bloka

```
----------┳ ---------
```

16.1. *Zapis o kalibraciji*

Identifikator zapisa

Radionica koja je obavila kalibraciju

Adresa radionice

Identifikacija kartice radionice

Datum isteka valjanosti kartice radionice

Prazan red

Datum kalibracije + svrha kalibracije

Idenitifikacijski broj vozila

Država clanica registracije i registracijska oznaka vozila

Karakteristicni koeficijent vozila

Konstanta tahografa

Djelatni promjer guma kotaca

Dimenzije postavljenih guma

Postavke ogranicavaca brzine

Staro i novo stanje brojaca kilometara

Svrha kalibracije (p) je numericka šifra kojom se objašnjava zašto su ovi parametri kalibracije zabilježeni, šifrirani u skladu s podatkovnim elementom CalibrationPurpose.

```
   --------------------
┳ Workshop_name _____________
  Workshop_address _________
Card-Identification ________
  dd/mm/yyyy

┳ dd/mm/yyyy   (p)
Д VIN ________________________
  Nat/VRN __________
w xx xxx Imp/km
k xx xxx Imp/km
l xx xxx mm
● TyreSize __________
› xxx km/h
x xxx xxx – x xxx xxx km
```

17. **Podešavanje vremena**

Identifikator bloka

```
----------◷ ---------
```

17.1. *Zapis o podešavanja vremena*

Identifikator zapisa

Stari datum i vrijeme

Novi datum i vrijeme

Radionica koja je obavila podešavanje vremena

Adresa radionice

Identifikacija kartice radionice

Datum isteka valjanosti kartice radionice.

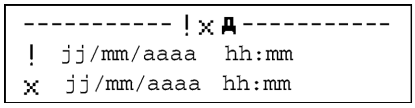
```
   --------------------
! ◷ dd/mm/yyyy hh:mm
  ◷ dd/mm/yyyy hh:mm
┳ Workshop_name __________
  Workshop_address _______
Card_Identification _____
  dd/mm/yyyy
```

18. **Najnoviji događaj i pogreška zapisana u jedinici vozila**

Identifikator bloka

Datum i vrijeme najnovijeg događaja

Datum i vrijeme najnovije pogreške.

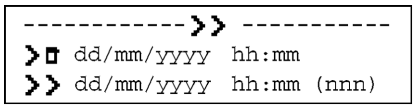


19. **Informacije o kontroli prekoračenja brzine**

Identifikator bloka

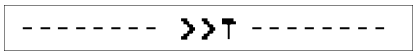
Datum i vrijeme zadnje KONTROLE PREKORAČENJA BRZINE

Datum/vrijeme prvog prekoračenja brzine i broj događaja prekoračenja brzine od tada.



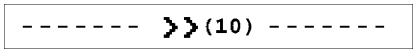
20. **Zapis o prekoračenju brzine**

20.1. Identifikator bloka ‚Prvo prekoračenje brzine nakon zadnje kalibracije'



20.2. Identifikator bloka ‚5 najozbiljnijih u zadnjih 365 dana.'

20.3. Identifikator bloka ‚Najozbiljniji za svaki od zadnjih deset dana nastanka.'



20.4. Identifikator zapisa

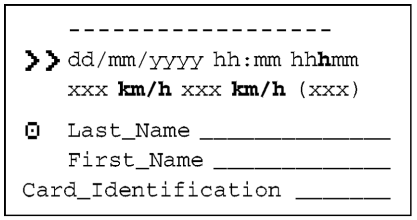
Datum, vrijeme i trajanje

Najveća i prosječna brzina, broj sličnih događaja tog dana

Prezime vozača

Ime(na) vozača

Identifikacija kartice vozača



20.5. Ako u bloku nema zapisa o prekoračenju brzine.

21. **Ručno upisani podaci**

Identifikator bloka

21.1. Mjesto nadzora

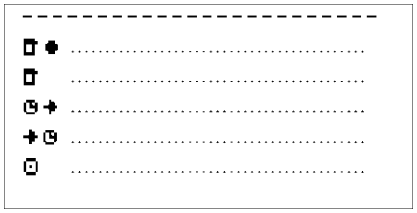
21.2. Potpis kontrolora

21.3. Od trenutka

21.4. Do trenutka

21.5. Potpis vozača

‚Ručno upisani podaci' Umetnuti dovoljno praznih linija iznad prostora za ručni upis, tako da se stvarno mogu upisati traženi podaci ili staviti potpis.



3. SPECIFIKACIJE ISPISA

U ovom se poglavlju koriste sljedeći dogovoreni zapisi:

N	Ispis bloka ili broja zapisa N
N	Ispis bloka ili broja zapisa N ponovljeno onoliko puta koliko je potrebno
X/Y	Ispis bloka ili zapisa X i/ili Y prema potrebi ponavljajući onoliko puta koliko je potrebno

3.1. **Aktivnosti vozača iz dnevnog ispisa kartice**

PRT_007 Aktivnosti vozača iz dnevnog ispisa kartice mora biti u skladu sa sljedećim formatom:

1	Datum i vrijeme ispisa dokumenta
2	Vrsta ispisa
3	Identifikacija kontrolora (ako je u jedinicu vozila umetnuta nadzorna kartica)
3	Identifikacija vozača (iz kartice s koje se vrši ispis)
4	Identifikacija vozila (vozilo iz kojeg se vrši ispis)
5	Identifikacija jedinice vozila (jedinica vozila iz koje se vrši ispis)
6	Zadnja kalibracija jedinice ove vozila
7	Zadnji nadzor kojemu je pregledavani vozač bio podvrgnut
8	Razdvajatelj aktivnosti vozača
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Aktivnosti vozača po redoslijedu nastanka
11	Razdvajatelj dnevnog sažetka
11.4	Mjesta unijeta kronološkim redom
11.5	Aktivnosti ukupno
12.1	Događaji ili pogreške od razdvajatelja kartice
12.4	Zapisi događaja/pogrešaka (zadnjih 5 događaja ili pogrešaka spremljenih na kartici)
	Događaji ili pogreške od razdvajatelja jedinice vozila
13.1	Zapisi događaja/pogrešaka (zadnjih 5 događaja ili pogrešaka spremljenih ili trenutačno aktivnih u jedinici vozila)
13.4	Mjesto nadzora
21.1	Potpis kontrolora
21.2	Potpis vozača
21.5	

3.2. **Aktivnosti vozača iz dnevnog ispisa jedinice vozila**

PRT_008 Aktivnosti vozača iz dnevnog ispisa jedinice vozila mora biti u skladu sa sljedećim formatom:

1	Datum i vrijeme ispisa dokumenta
2	Vrsta ispisa
3	Identifikacija nositelja kartice (za sve kartice umetnute u jedinicu vozila)
4	Identifikacija vozila (vozilo iz kojeg se radi ispis)
5	Identifikacija jedinice vozila (jedinica vozila iz koje se radi ispis)
6	Zadnja kalibracija ove jedinice vozila
7	Zadnji nadzor na tom tahografu
9	Razdvajatelj aktivnosti vozača
10	Razdvajatelj utora vozača (utor 1)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Aktivnosti kronološkim redom (utor vozača)
10	Razdvajatelj utora suvozača (utor 2)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Aktivnosti kronološkim redom (utor suvozača)
11	Razdvajatelj dnevnog sažetka
11.1	Sažetak razdoblja bez kartice u utoru vozača
11.4	Mjesta unijeta kronološkim redom
11.6	Aktivnosti ukupno

11.2	Sažetak razdoblja bez kartice u utoru suvozača
11.4	Mjesta unijeta kronološkim redom
11.7	Aktivnosti ukupno
11.3	Sažetak aktivnosti za vozača, uključena oba utora
11.4	Mjesta koja je taj vozač unio kronološkim redom
11.7	Aktivnosti ukupno za tog vozača
13.1	Razdvajatelj događaja i pogrešaka
13.4	Zapisi događaja/pogrešaka (zadnjih 5 događaja ili pogrešaka pohranjenih ili se trenutačno događajau u jedinici vozila)
21.1	Mjesto nadzora
21.2	Potpis kontrolora
21.3	Od vremena (prostor za vozača bez kartice kako bi se naznačilo koja razdoblja se odnose na njega)
21.4	Do vremena
21.5	Potpis vozača

3.3. **Događaji i pogreške iz ispisa kartice**

PRT_009 Događaji i pogreške iz ispisa kartice moraju biti u skladu sa sljedećim formatom:

1	Datum i vrijeme ispisa dokumenta
2	Vrsta ispisa
3	Identifikacija kontrolora (ako je u jedinicu vozila umetnuta nadzorna kartica)
3	Identifikacija vozača (iz kartice za koju se radi ispis)
4	Identifikacija vozila (vozilo za koje se radi ispis)
12.2	Razdvajatelj događaja
12.4	Zapisi događaja (svi događaji pohranjeni na kartici)
12.3	Razdvajatelj pogrešaka
12.4	Zapisi o pogreškama (sve pogreške pohranjene na kartici)
21.1	Mjesto nadzora
21.2	Potpis kontrolora
21.5	Potpis vozača

3.4. **Događaji i pogreške iz ispisa jedinice vozila**

PRT_10 Događaji i pogreške iz ispisa jedinice vozila moraju biti u skladu sa sljedećim formatom:

1	Datum i vrijeme ispisa dokumenta
2	Vrsta ispisa
3	Identifikacija nositelja kartice (za sve kartice umetnute u jedinicu vozila)
4	Identifikacija vozila (vozilo za koje se radi ispis)
13.2	Razdvajatelj događaja
13.4	Zapisi događaja (svi događaji pohranjeni ili koji se trenutačno događaju u jedinici vozila)
13.3	Razdvajatelj pogrešaka
13.4	Zapisi o pogreškama (sve pogreške pohranjene ili se trenutačno događaju u jedinici vozila)
21.1	Mjesto nadzora
21.2	Potpis kontrolora
21.5	Potpis vozača

3.5. **Ispis tehničkih podataka**

PRT_011 Ispis tehničkih podataka mora biti u skladu sa sljedećim formatom:

1	Datum i vrijeme ispisa dokumenta
2	Vrsta ispisa
3	Identifikacija nositelja kartice (za sve kartice umetnute u jedinicu vozila)
4	Identifikacija vozila (vozilo iz kojeg se radi ispis)
14	Identifikacija jedinice vozila
15	Identifikacija senzora
16	Razdvajatelj podataka o kalibraciji
16.1	Zapisi kalibracije (svi raspoloživi zapisi kronološkim redom)
17	Razdvajatelj podešavanja vremena
17.1	Zapisi o podešavanju vremena (svi raspoloživi zapisi od zapisa o podešavanju vremena i od zapisa o kalibraciji)
18	Najnoviji događaj i pogreška zapisani u jedinici vozila

3.6. **Ispis prekoračenja brzine**

PRT_012 Ispis prekoračenja brzine mora biti u sljedećem formatu:

1	Datum i vrijeme ispisa dokumenta
2	Vrsta ispisa
3	Identifikacija nositelja kartice (za sve kartice umetnute u jedinicu vozila)
4	Identifikacija vozila (vozilo iz kojeg se radi ispis)
19	Informacije o kontroli prekoračenja brzine
20.1	Identifikator podataka o prekoračenju brzine
20.4 / 20.5	Prvo prekoračenje brzine poslije zadnje kalibracije
20.2	Identifikator podataka o prekoračenju brzine
20.4 / 20.5	5 najtežih prekoračenja brzine u zadnjih 365 dana
20.3	Identifikator podataka o prekoračenju brzine
20.4 / 20.5	Najteže prekoračenje brzine za svaki od posljednjih 10 dana nastanka
21.1	Mjesto nadzora
21.2	Potpis kontrolora
21.5	Potpis vozača

Dodatak 5.

PRIKAZ

U ovom se Dodatku koriste sljedeći dogovorni oblici bilježenja:

— podebljano tiskana slova označivaju običan teksta za prikaz (prikaz je u normalnim slovima),

— normalna slova označivaju promjenjive varijable (piktogrami ili podaci), koji se za prikaz zamjenjuju njihovim vrijednostima:

dd mm gggg: dan, mjesec, godina,

hh: sati,

mm: minute,

D: piktogram trajanje,

EF: kombinacija piktograma događaja ili pogrešaka,

O: piktogram načina rada.

DIS_001 Tahograf prikazuje podatke primjenom sljedećeg formata:

Podaci	Oblik
standardni prikaz	
Lokalno vrijeme	Hh:mm
Način rada	O
Podaci o vozaču	1 Dhh**h**mm ▮▮hh**h**mm
Podaci o suvozaču	2 Dhh**h**mm
Uključeno stanje ‚Izvan djelokruga'	OUT
Upozorenje	
Prekoračenje vremena neprekidne vožnje	10 hh**h**mm ▮▮hh**h**mm
Događaj ili pogreška	EF
Ostali prikazi	
UTC datum vrijeme	UTC gg/mm/aaaa o UTC gg.mm.aaaa Hh:mm
Neprekidno vrijeme vožnje i zbirno vrijeme stanke vozača	10 hh**h**mm ▮▮hh**h**mm
Neprekidno vrijeme vožnje i zbirno vrijeme stanke suvozača	20 hh**h**mm ▮▮hh**h**mm
Zbirno vrijeme vožnje vozača za protekli i tekući tjedan	10 ‖ hhh**h**mm
Zbirno vrijeme vožnje suvozača za protekli i tekući tjedan	20 ‖ hhh**h**mm

Dodatak 6.

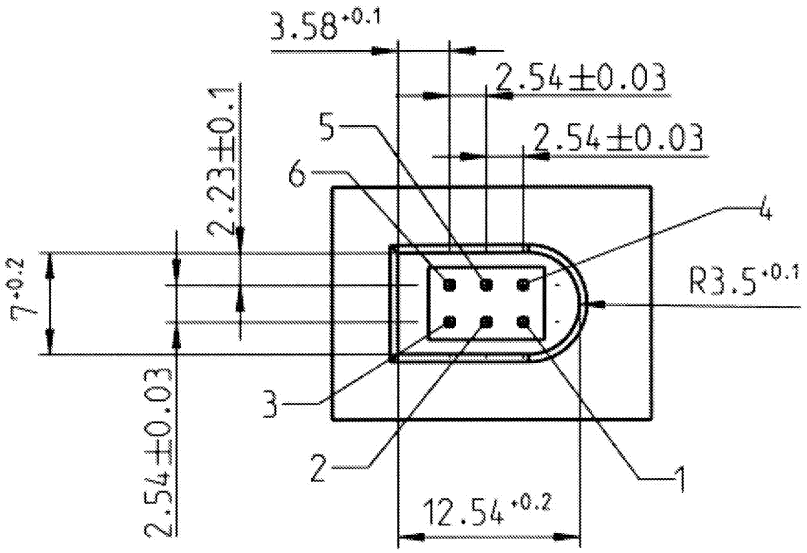
VANJSKA SUČELJA

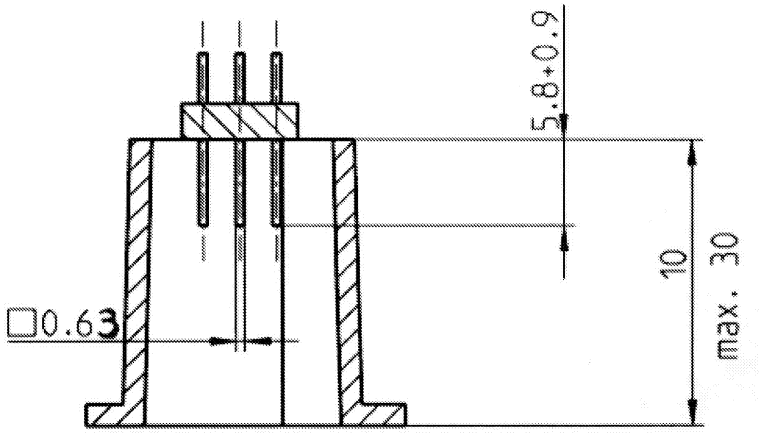
SADRŽAJ

1. HARDVER

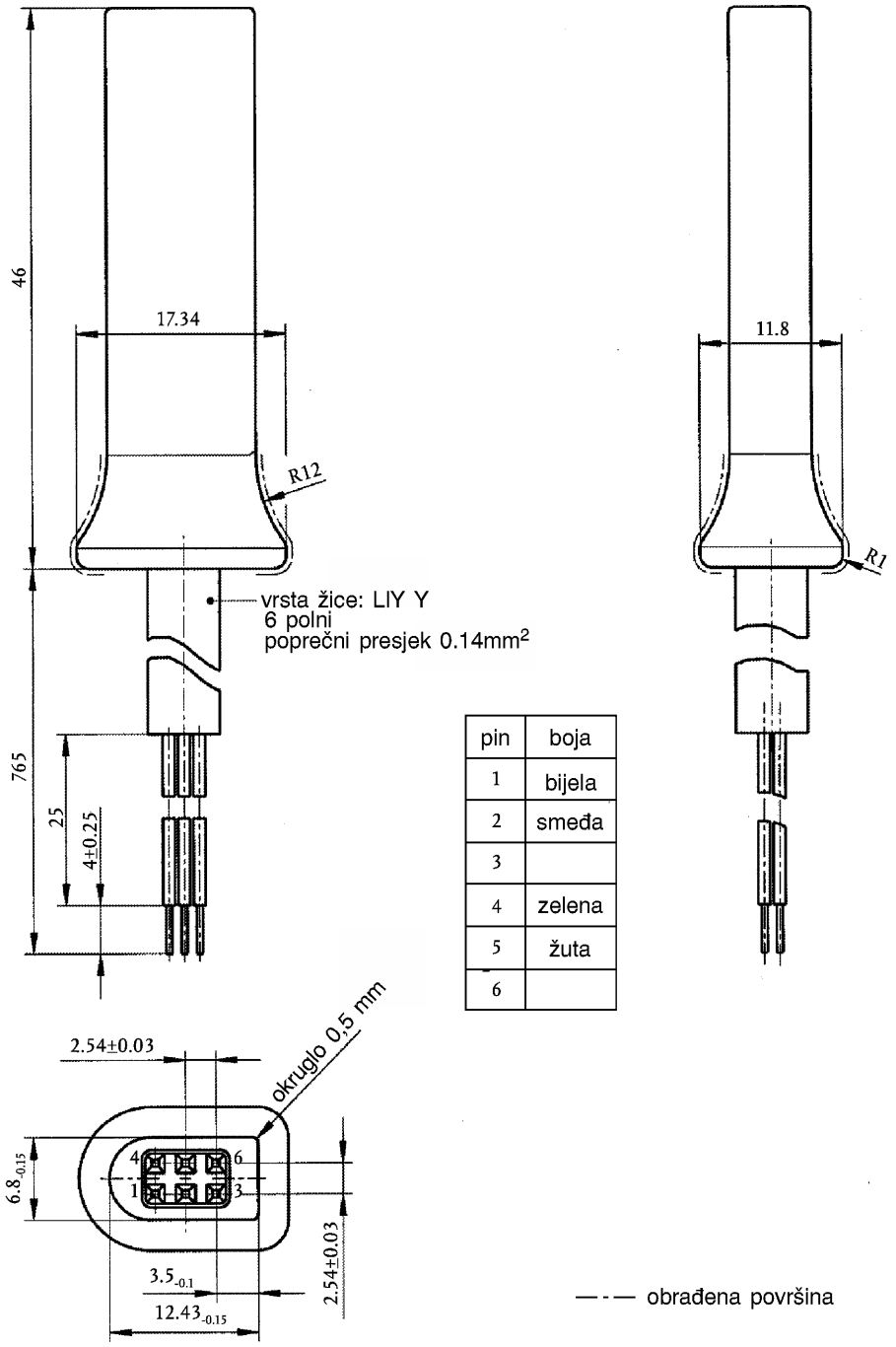
1.1. **Utičnica**

INT_001 Utičnica za preuzimanje podataka/kalibraciju je 6-pinski konektor, koji je dostupan s prednje strane tahografa bez potrebe isključivanja bilo kojeg dijela tahografa, i koji udovoljava sljedećem nacrtu (sve dimenzije su izražene u milimetrima):





Sljedeći dijagram prikazuje tipičan utikač za 6-pinsko uparivanje:



pin	boja
1	bijela
2	smeđa
3	
4	zelena
5	žuta
6	

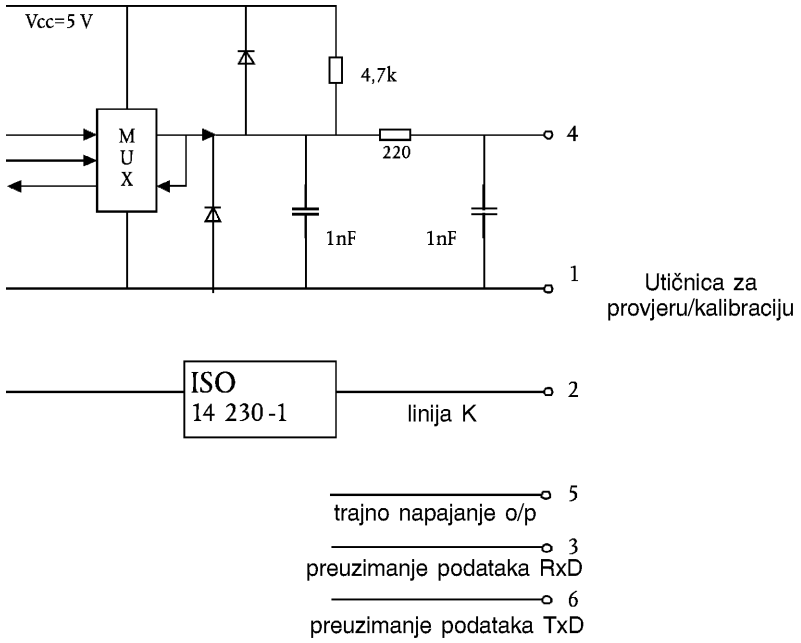
1.2. **Raspored kontakata**

INT_002 Kontakti se raspoređuju prema sljedećoj tablici:

Pin	Opis	Napomena
1	Akumulator - minus	Priključeno na negativni pol akumulatora vozila
2	Podatkovna komunikacija	Linija K (po ISO 14 230-1)
3	RxD – preuzimanje podataka	Unos podataka u tahograf
4	Ulazno/izlazni signal	Kalibracija
5	Stalni izlaz napajanja	Raspon napona je onaj koji je na vozilu minus 3 V kako bi se omogućio pad napona na zaštitnim strujnim krugovima Izlaz 40 mA
6	TxD - preuzimanje podataka	Izlaz podataka iz tahografa

1.3. **Blok dijagram**

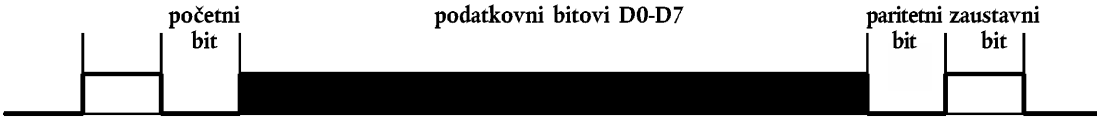
INT_003 Blok dijagram udovoljava sljedećem:



2. SUČELJE ZA PREUZIMANJE PODATAKA

INT_004 Sučelje za preuzimanje podataka udovoljava specifikacijama RS232.

INT_005 Sučelje za preuzimanje podataka koristi jedan početni bit, 8 podatkovnih bitova, s LSB (najmanje značajnim bitom) na početku, jedan parno paritetni bit i 1 zaustavni bit.



Organizacija podatkovnih bajtova

Početni bit: jedan bit na logičkoj razini 0

Podatkovni bitovi: prenose se s LSB (najmanje značajnim bitom) na početku

Paritetni bit: paran paritet

Zaustavni bit: jedan bit na logičkoj razini 1

Kod prijenosa numeričkih podataka sastavljenih od više bajtova, najznačajniji bajt se prenosi prvi, a najmanje značajan bajt posljednji.

INT_006 Brzine prijenosa podataka moraju biti prilagodljive od 9 600 bps do 115 200 bps. Prijenos se mora postići pri najvišoj mogućoj brzini prijenosa, kod čega je početna brzina prijenosa podataka nakon početka komunikacije postavljena na 9 600 bps.

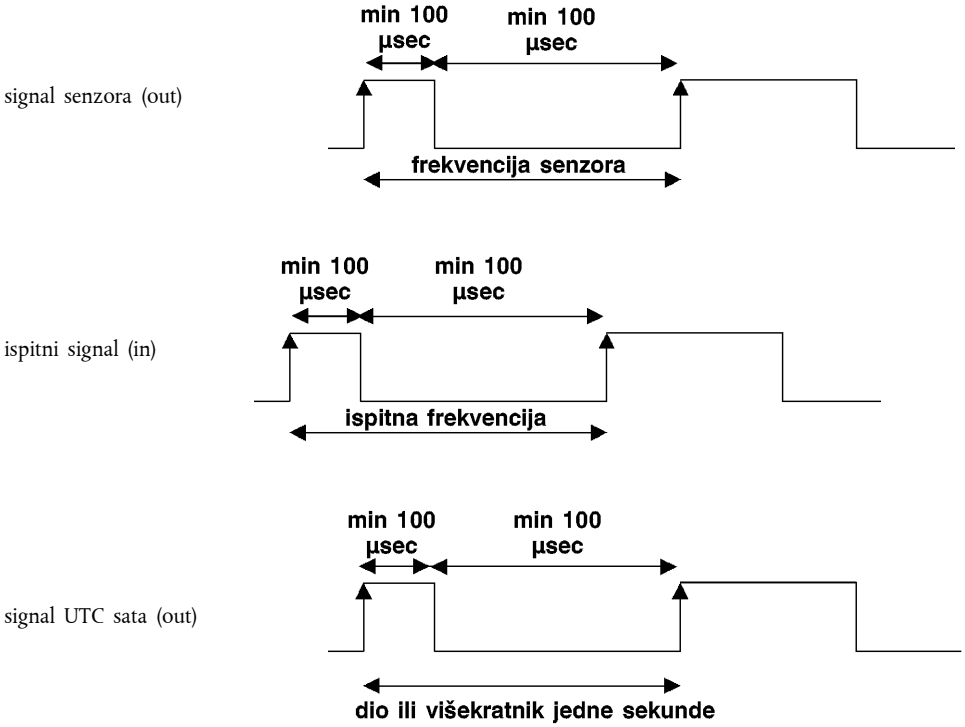
3. SUČELJE KALIBRACIJE

INT_007 Podatkovna komunikacija mora udovoljavati ISO 14 230-1 Cestovna vozila – dijagnostički sustavi – protokol s ključnom riječi 2000 - Dio 1.: Fizička razina, Prvo izdanje: 1999.

INT_008 Ulazno/izlazni signal mora udovoljavati sljedećem električnom opisu:

Parametar	Minimalno	Tipično	Maksimalno	Napomena
U_{low} (in)			1,0 V	I = 750 µA
U_{high} (in)	4 V			I = 200 µA
Frekvencija			4 kHz	
U_{low} (in)			1,0 V	I = 1 mA
U_{high} (out)	4 V			I = 1 mA

INT_009 Ulazno/izlazni signal mora udovoljavati sljedećim vremenskim dijagramima:



Dodatak 7.

PROTOKOLI PREUZIMANJA PODATAKA

SADRŽAJ

1. UVOD

Ovaj Dodatak navodi postupke za obavljanje različitih vrsta preuzimanja podataka na vanjski medij za spremanje, zajedno s protokolima koje treba provesti kako bi se osigurao ispravan prijenos podataka i potpuna sukladnost formata preuzetih podataka koji omogućava svakom kontroloru da pregleda takve podatke i da može kontrolirati njihovu vjerodostojnost i cjelovitost prije analize.

1.1. **Područje primjene**

Podaci se mogu preuzeti na ESM:

— iz jedinice u vozilu posebnom namjenskom opremom (IDE) priključenom na jedinicu vozila,

— s kartice tahografa putem IDE opremljenom uređajem kartičnog sučelja (IFD),

— s kartice tahografa preko jedinice u vozilu putem IDE priključenim na jedinicu vozila.

Da bi se omogućila provjera vjerodostojnosti i cjelovitosti preuzetih podataka spremljenih na ESM, podaci se preuzimaju potpisom stavljenim sukladno Dodatku 11. Zajednički sigurnosni mehanizmi. Identifikacija uređaja izvora (jedinica vozila ili kartica) i njegovi sigurnosni certifikati (države članice i opreme) se također preuzimaju. Onaj tko provjerava podatke mora neovisno posjedovati povjerljiv europski javni ključ.

DDP_001 Podaci preuzeti tijekom jednog procesa preuzimanja podataka se moraju spremiti u ESM unutar jedne datoteke.

1.2. **Skraćenice i zabilješke**

U ovom se Dodatku koriste sljedeće skraćenice:

AID	identifikator aplikacije
ATR	odziv na vraćanje u početno stanje
CS	bajt kontrolnog zbroja
DF	namjenska datoteka
DS_	dijagnostički proces
EF	elementarna datoteka
ESM	vanjski medij za spremanje podataka
FID	identifikator datoteke (ID datoteke)
FMT	formatni bajt (prvi bajt glave poruke)
ICC	kartica s integriranim sklopom
IDE	posebna namjenska oprema: Oprema koja se koristi za preuzimanje podataka na ESM (npr. osobno računalo)
IFD	uređaj sučelja
KWP	protokol s ključnom riječi 2000
LEN	bajt duljine (posljednji bajt glave poruke)
PPS	protokol odabira parametra
PSO	izvođenje sigurnosne radnje
SID	identifikator službe
SRC	izvorni bajt
TGT	ciljni bajt
TLV	vrijednost duljine oznake
TREP	parametar odziva prijenosa
TRTP	parametar zahtjeva za prijenos
VU	jedinica u vozilu.

2. PREUZIMANJE PODATAKA S JEDINICE VOZILA

2.1. **Postupak preuzimanja podataka**

Za preuzimanje podataka s jedinice vozila operator mora obaviti sljedeće radnje:

— umetnuti svoju karticu tahografa unutar utora jedinice vozila ([1]),

— priključiti IDE na priključnicu za preuzimanje podataka jedinice vozila,

— uspostaviti vezu između IDE i jedinice vozila,

— odabrati na IDE podatke za preuzimanje i poslati zahtjev u jedinicu vozila,

— zaključiti sesiju preuzimanja podataka.

2.2. **Protokol preuzimanja podataka**

Protokol je strukturiran na načelu nadređen-podređen, kod čega IDE ima nadređenu, a jedinica vozila podređenu ulogu.

Struktura, vrste i protok poruka su načelno utemeljena na protokolu ključne riječi 2000 (KWP) (ISO 14230-2 Cestovna vozila – Dijagnostički sustavi – Protokol ključne riječi 2000 - Dio 2.: Razina podatkovnih veza).

Aplikacijska razina se u načelu temelji na sadašnjem nacrtu ISO 14229-1 (Cestovna vozila – Dijagnostički sustavi – Dio 1. Dijagnostičke službe, verzija 6. od 22. veljače 2001.).

2.2.1. ***Struktura poruke***

DDP_002 Sve poruke koje se razmjenjuju između IDE i jedinice vozila su formatirane u strukturi koja se sastoji od tri dijela:

— glava koju čini formatni bajt (FMT), ciljni bajt (TGT), izvorni bajt (SRC) i moguće bajt za duljinu (LEN),

— podatkovno polje koje čine bajt identifikatora službe (SID) i promjenjiv broj podatkovnih bajtova koji može obuhvaćati neobavezni bajt dijagnostičkog procesa (DS_) ili neobavezni bajt parametara prijenosa (TRTP ili TREP),

— kontrolni zbroj kojega čini bajt kontrolnog zbroja (CS).

Zaglavlje				Podatkovno polje					Kontrolni zbroj
FMT	TGT	SRC	LEN	SID	Podaci	…	…	…	CS
4 bajta				najviše 225 bajtova					1 bajt

Bajt TGT i SRC predstavljaju fizičku adresu primatelja i tvorca poruke. Vrijednosti su F0 Hex za IDE i EE Hex za jedinicu vozila.

Bajt LEN je duljina dijela podatkovnog polja.

Bajt ispitnog zbroja je 8-bitni zbroj serije modula 256 svih bajtova poruke s izuzetkom samog CS.

Bajtovi FMT, SID, DS_, TRTP i TREP su definirani u nastavku ovog dokumenta.

([1]) Umetnuta kartica aktivira odgovarajuća prava na pristup funkciji preuzimanja podataka i podacima.

DDP_003 Kada su podaci koje prenosi poruka dulji od prostora koji je raspoloživ u dijelu podatkovnog polja, poruka se u stvarnosti šalje u nekoliko dijelova poruke. Svaki dio poruke nosi glavu, isti SID, TREP i 2-bajtni brojač dijelova poruke koji označuje broj dijelova poruke u cjelokupnoj poruci. Kako bi se omogućilo provjeravanje pogrešaka i prekid, IDE potvrđuje svaki dio poruke. IDE može primiti dio poruke, tražiti da se ona ponovo prenese, zahtijevati od jedinice vozila da ponovo počne ili prekine prijenos.

DDP_004 Ako posljednji dio poruke sadrži točno 255 bajtova u podatkovnom polju, zadnji dio poruke se mora staviti s praznim podatkovnim poljem (osim SID TREP i brojača dijelova poruke) kako bi se označio kraj poruke.

Primjer:

Zaglavlje	SID	TREP	Poruka	CS
4 bajta	Više od 255 bajtova			

ce se prenijeti kao:

Zaglavlje	SID	TREP	00	01	Dio poruke1	CS
4 bajta	255 bajtova					

Zaglavlje	SID	TREP	00	01	Dio poruke 2	CS
4 bajta	255 bajtova					

…

Zaglavlje	SID	TREP	xx	yy	Dio poruke n	CS
4 bajta	Manje od 255 bajtova					

ili kao:

Zaglavlje	SID	TREP	00	01	Dio poruke1	CS
4 bajta	255 bajtova					

Zaglavlje	SID	TREP	00	02	Dio poruke2	CS
4 bajta	255 bajtova					

…

Zaglavlje	SID	TREP	xx	yy	Dio poruke n	CS
4 bajta	255 bajtova					

Zaglavlje	SID	TREP	xx	yy + 1	CS
4 bajta	4 bajta				

2.2.2. ***Vrste poruka***

Komunikacijski protokol za preuzimanje podataka između jedinice vozila i IDE zahtijeva razmjenu osam različitih vrsta poruka.

Sljedeća tablica prikazuje sažeti prikaz takvih poruka.

Struktura poruke	Najviše 4 bajta Zaglavlje				Najviše 255 bajtova Podaci			1 bajt Kontrolni zbroj
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Zahtjev za početak komunikacije	81	EE	F0		81			E0
Pozitivan odgovor za početak komunikacije	80	F0	EE	03	C1		8F,EA	9B
Zahtjev za početak dijagnostičkog procesa	80	EE	F0	02	10	81		F1
Pozitivan odgovor za početak dijagnostike	80	F0	EE	02	50	81		31
Parametri kontrolne veze								
Provjera brzine prijenosa podataka (stadij 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Pozitivan odgovor na zahtjev za provjeru brzine prijenosa podataka	80	F0	EE	02	C7		01	28
Prijelazna brzina prijenosa podataka (stadij 2)	80	EE	F0	03	87		02,03	ED
Zahtjev za prihvat podataka	80	EE	F0	0A	35		00,00,00, 00,00,FF,- FF, FF,FF	99
Pozitivan odgovor na zahtjev za prihvat podataka	80	F0	EE	03	75		00,FF	D5
Zahtjev za prijenos podataka								
Pregled	80	EE	F0	02	36	01		97
Aktivnosti	80	EE	F0	06	36	02	Datum	CS
Događaji i pogreške	80	EE	F0	02	36	03		99
Detaljna brzina	80	EE	F0	02	36	04		9A
Tehnički podaci	80	EE	F0	02	36	05		9B
Preuzimanje podataka sa kartice	80	EE	F0	02	36	06		9C
Pozitivan odgovor za prijenos podataka	80	F0	EE	Len	76	TREP	Podatak	CS
Zahtjev za prekid prijenosa podataka	80	EE	F0	01	37			96
Pozitivan odgovor na zahtjev za prekid prijenosa	80	F0	EE	01	77			D6
Zahtjev za prekid komunikacije	80	EE	F0	01	82			El
Pozitivan odgovor na za prekid komunikacije	80	F0	EE	01	C2			21
Potvrda dijela poruke	80	EE	F0	Len	83		Podatak	CS
Negativni odgovori								
Opće odbacivanje	80	F0	EE	03	7F	Sid Req	10	CS
Servis nije podržan	80	F0	EE	03	7F	Sid Req	11	CS
Podfunkcija nije podržana	80	F0	EE	03	7F	Sid Req	12	CS
Neispravna duljina poruke	80	FO	EE	03	7F	Sid Req	13	CS
Neispravni uvjeti ili pogreška slijeda zahtjeva	80	F0	EE	03	7F	Sid Req	22	CS
Zahtjev izvan dosega	80	F0	EE	03	7F	Sid Req	31	CS
Prihvat podataka nije prihvaćen	80	F0	EE	03	7F	Sid Req	50	CS
Čekanje na odgovor	80	F0	EE	03	7F	Sid Req	78	CS
Podaci nisu dostupni	80	F0	EE	03	7F	Sid Req	FA	CS

Napomene:

— Sid Req = Sid odgovarajućeg zahtjeva.
— TREP = TRTP odgovarajućeg zahtjeva.
— Osjenčana polja označivaju da se ne prenosi ništa.
— Izraz prihvat (s gledišta IDE) se koristi zbog usklađenosti s ISO 14229. Znači isto što i preuzimanje podataka (s gledišta VU).
— Potencijalni 2-bitni brojači dijelova poruke nisu prikazani u ovoj tablici.

2.2.2.1. *Zahtjev za početak komunikacije (SID 81)*

DDP_005 Ovu poruku izdaje IDE za uspostavljanje komunikacijske veze s jedinicom vozila. Početne komunikacije se uvijek obavljaju pri brzini od 9 600 bauda (dok se brzina prijenosa podataka eventualno ne promijeni korištenjem odgovarajućih servisa za upravljanje vezom).

2.2.2.2. *Pozitivan odgovor za početak komunikacije (SID C1)*

DDP_006 Ovu poruku izdaje jedinica vozila kao pozitivan odgovor na zahtjev za početak komunikacije. Ona sadrži 2 ključna bajta ‚8F' ‚EA' koji označivaju da jedinica podržava protokol sa zaglavljem koje sadrži podatke o ciljanom,izvoru i duljini.

2.2.2.3. *Zahtjev za početak dijagnostičkog procesa (SID 10)*

DDP_007 Poruku sa zahtjevom za početak dijagnostičkog procesa šalje IDE kako bi zahtijevao novi dijagnostički proces sa jedinicom vozila. Podfunkcija ‚zadani proces' (81 Hex) označuje da je potrebno otvoriti standardni dijagnostički proces.

2.2.2.4. *Pozitivan odgovor za početak dijagnostike (SID 50)*

DDP_008 Pozitivan odgovor na poruku za početak dijagnostike šalje jedinica vozila kao pozitivan odgovor na zahtjev za početak dijagnostičkog procesa.

2.2.2.5. *Servis upravljanja vezom (SID 87)*

DDP_052 Servis kontrole veze koristi IDE da bi započela s promjenom brzine prijenosa podataka. Ovo se odvija u dva koraka. U prvom koraku IDE predlaže promjenu brzine prijenosa podataka navodeći novu brzinu. Po primitku pozitivne poruke iz jedinice vozila, IDE odašilje potvrdu promjene brzine prijenosa podataka u jedinicu vozila (drugi korak). IDE potom prelazi na novu brzinu prijenosa podataka. Po primitku potvrde jedinica vozila prelazi na novu brzinu prijenosa podataka.

2.2.2.6. *Pozitivan odgovor na zahtjev za upravljanje vezom (SID C7)*

DDP_053 Pozitivan odgovor na zahtjev za upravljanje vezom izdaje jedinica vozila kao pozitivan odgovor na zahtjev za servis upravljanja vezama (prvi korak). Napominje se da nema odgovora na zahtjev za potvrdom (drugi korak).

2.2.2.7. *Zahtjev za prihvat podataka (SID 35)*

DDP_009 Poruku sa zahtjevom za prihvat podataka izdaje IDE kako bi je jedinica vozila obavijestila da je radnja prihvata podatka zatražena. Za zadovoljavanje uvjeta ISO14229, obuhvaćeni su podaci koji sadrže pojedinosti o adresi, veličini i formatu zahtijevanih podataka. Obzirom da ih IDE ne poznaje prije prihvata podatka, adresa memorije se postavlja na 0, format je nešifriran i nekomprimiran i veličina memorije je postavljena na maksimum.

2.2.2.8. *Pozitivan odgovor na zahtjev za prihvat podataka (SID 75)*

DDP_010 Poruku s pozitivnim odgovorom na zahtjev za prihvat podataka šalje jedinica vozila kako bi ukazala IDE da je jedinica vozila spremna za preuzimanje podataka. Za udovoljavanje zahtjeva ISO 14229, podaci su obuhvaćeni u ovoj poruci s pozitivnim odgovorom, ukazujući IDE da će daljnje poruke s pozitivnim odgovorom na zahtjev za prijenos podataka sadržavati najviše 00FFh bajtova.

2.2.2.9. *Zahtjev za prijenos podataka (SID 36)*

DDP_011 Zahtjev za prijenos podataka šalje IDE da bi jedinica vozila ukazala na vrstu podataka koje treba preuzeti. Jednobajtni parametar zahtjeva za prijenos podataka (TRTP) označuje vrstu prijenosa.

Postoji šest vrsta prijenosa podataka:

— pregled (TRTP 01),

— aktivnosti navedenog dana (TRTP 02),

— događaji i pogreške (TRTP 03),

— detaljna brzina (TRTP 04),

— tehnički podaci (TRTP 05),

— preuzimanje podataka sa kartice (TRTP 06).

DDP_054 IDE mora obavezno zahtijevati prijenos pregleda podataka (TRTP 01) tijekom procesa preuzimanja podataka obzirom da će samo to osigurati da se certifikati jedinice vozila zabilježe unutar preuzete datoteke (i omogućiti provjeru digitalnog potpisa).

U drugom slučaju (TRTP 02) poruka sa zahtjevom za prijenos podataka obuhvaća oznaku kalendarskog dana (u formatu `TimeReal`) za kojega treba preuzeti podatke.

2.2.2.10. *Pozitivan odgovor za prijenos podataka (SID 76)*

DDP_012 Pozitivan odgovor za prijenos podataka šalje jedinica vozila kao odgovor na zahtjev za prijenos podataka. Poruka sadrži zahtijevane podatke, s parametrom odgovora za prijenos (TREP) koji odgovara TRTP-u zahtjeva.

DDP_055 U prvom slučaju (TREP 01), jedinica vozila će poslati podatke koji pomažu operatoru IDE da izabere podatke koje želi dalje preuzeti. Informacija sadržana u ovoj poruci je sljedeća:

— sigurnosni certifikati,

— identifikacija vozila,

— tekući datum i vrijeme jedinice vozila,

— najstariji i najraniji datum za koje je moguće preuzeti podatke (podaci iz jedinice vozila),

— oznaka prisustva kartice u jedinici vozila,

— prethodno preuzimanje podataka za potrebe tvrtke,

— zaključavanja podataka tvrtke,

— prethodni nadzor.

2.2.2.11. *Zahtjev za prekid prijenosa (SID 37)*

DDP_013 Zahtjev za prijekid prijenosa šalje IDE kako bi obavijestio jedinicu vozila da je proces preuzimanja podataka završen.

2.2.2.12. *Pozitivan odgovor na zahtjev za prekid prijenosa (SID 77)*

DDP_014 Poruku s pozitivnim odgovorom na zahtjev za prijekid prijenosa šalje jedinica vozila kako bi potvrdila zahtjev za prekid prijenosa.

2.2.2.13. *Zahtjev za prekid komunikacije (SID 82)*

DDP_015 Poruka sa zahtjevom za prekid komunikacije šalje IDE za prekid komunikacijske veze s jedinicom vozila.

2.2.2.14. *Pozitivan odgovor na zahtjev za prekid komunikacije (SID C2)*

DDP_016 Poruku s pozitivnim odgovorom na prekid komunikacije šalje jedinica vozila za potvrdu zahtjeva za prekid komunikacije.

2.2.2.15. *Potvrda dijela poruke (SID 83)*

DDP_017 Potvrdu dijela poruke šalje IDE za potvrdu primitka svakog dijela poruke koji se prenosi u više dijelova poruka. Podatkovno polje sadrži SID koji se prima sa jedinice vozila i 2-bajtnu šifru kako slijedi:

— MsgC + 1 potvrđuje ispravan prijem broja dijela poruke MsgC.

Zahtjev šalje IDE prema jedinici vozila da pošalje sljedeći dio poruke.

— MsgC ukazuje na problem s prijemom broja dijela poruke MsgC.

Zahtjev ponovno šalje IDE prema jedinici vozila da pošalje dio poruke.

— FFFF zahtijeva kraj poruke.

Ovim se postupkom može služiti IDE za okončanje prijenosa poruke iz jedinice vozila iz bilo kojeg razloga.

Posljednji dio neke poruke (bajt LEN < 255) se može potvrditi korištenjem bilo koje od ovih šifri ili se ne mora potvrditi.

Odgovori jedinice vozila koji se sastoje od više dijelova poruke su sljedeći:

— pozitivan odgovor na prijenos podataka (SID 76)

2.2.2.16. *Negativan odgovor (SID 7F)*

DDP_018 Poruku s negativnim odgovorom jedinica vozila šalje kao odgovor na gore navedene poruke zahtjeva ako jedinica vozila ne može udovoljiti zahtjevu. Podatkovna polja poruke sadrže SID odgovore (7F), SID zahtjeva i šifru koja označuje razlog za negativan odgovor. Na raspolaganju su sljedeće šifre:

— 10 opće odbacivanje

Radnja se ne može obaviti zbog razloga koji nije dolje naveden

— 11 servis nije podržan

SID zahtjeva nije razumljiv

— 12 podfunkcija se ne podržava

DS_ ili TRTP zahtjeva nije razumljiv ili nema daljnjih dijelova poruke koje treba prenijeti

— 13 neispravna duljina poruke

Duljina primljene poruke je pogrešna

— 22 uvjeti nisu ispravni ili pogreška slijeda zahtjeva

Zahtijevani servis nije aktivan ili slijed poruka zahtjeva nije ispravan

— 31 zahtjev izvan djelokruga

Zapis parametra zahtjeva (podatkovno polje) nije valjan

— 50 prihvat podataka se ne prihvaća

Zahtjev se ne može izvršiti (jedinica vozila u neprimjerenom režimu rada ili unutarnja pogreška jedinice vozila)

— 78 čekanje na odgovor

Zahtijevana radnja se ne može pravovremeno dovršiti i jedinica vozila nije spremna za prihvaćanje drugog zahtjeva

— FA podaci nisu dostupni

Podatkovni objekt zahtjeva za prijenos podataka nije dostupan u jedinici vozila (npr. nije umetnuta kartica, …)

2.2.3. ***Protok poruke***

Tipičan protok poruke tijekom redovnog postupka preuzimanja podataka je sljedeći:

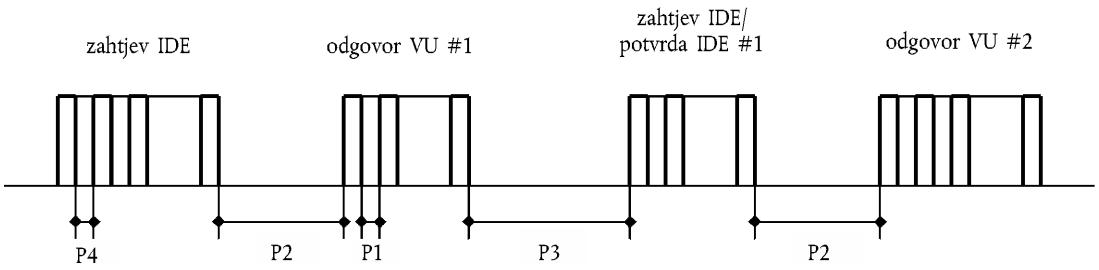
IDE		VU
Zahtjev za početak komunikacije	⇨	
	⇦	Pozitivan odgovor
Zahtjev za početak dijagnostičke aktivnosti	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prihvat podataka	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prijenos pregleda podataka	⇨	
	⇦	Pozitivan odgovor
Zahtjev za podatke #2	⇨	
	⇦	Pozitivan odgovor #1
Potvrda dijela poruke #1	⇨	
	⇦	Pozitivan odgovor #2
Potvrda dijela poruke #2	⇨	
	⇦	Pozitivni odgovor #m
Potvrda dijela poruke #m	⇨	
	⇦	Pozitivan odgovor (podatkovno polje < 255 bajtova)
Potvrda dijela poruke (neobvezno)	⇨	
…		
Zahtjev za prijenos podataka #n	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prekid prijenosa	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prekid komunikacije	⇨	
	⇦	Pozitivan odgovor

2.2.4. ***Vremenski termini***

DDP_019 Tijekom redovnog rada mjerodavni su vremenski parametri prikazani na sljedećoj slici:

Slika 1.

Protok poruke, vremenski termini



Gdje je:

P1 = međubajtno vrijeme za odgovor VU.

P2 = vrijeme između kraja zahtjeva IDE i početka odziva VU, ili između kraja potvrde IDE i početka sljedećeg odgovora VU.

P3 = vrijeme između kraja odziva VU i početka novog zahtjeva IDE ili između kraja odgovora VU i početka potvrde IDE, ili između kraja zahtjeva IDE i početka novog zahtjeva IED ako VU ne odgovori.

P4 = međubajtno vrijeme za zahtjev IDE.

P5 = produljena vrijednost P3 za preuzimanje podataka s kartice.

Dopuštene vrijednosti vremenskih parametara su prikazane u sljedećoj tablici (proširenI niz parametara tempiranja KWP, koriste se u slučaju fizičkog adresiranja za bržu komunikaciju).

Vremenski parametar	Donja granična vrijednost (ms)	Gornja granična vrijednost (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minuta

(*) Ako VU pošalje negativan odgovor sa šifrom koja znači ‚zahtjev uredno primljen, čekanje na odgovor', ova vrijednost se proteže na istu gornju graničnu vrijednost P3.

2.2.5. ***Obrada pogrešaka***

Ako tijekom razmjene poruka dođe do pogreške, shema protoka poruke se mijenja ovisno o tome koja oprema je ustanovila pogrešku i o poruci koja uzrokuje pogrešku.

Na slikama 2. i 3. prikazani su postupci obrade pogreške za jedinicu vozila odnosno IDE.

2.2.5.1. *Stadij početka komunikacije*

DDP_020 Ako IDE ustanovi pogrešku u stadiju početka komunikacije, zbog vremena ili zbog protoka bitova, čekat će u trajanju od P3 min prije ponovnog izdavanja zahtjeva.

DDP_021 Ako jedinica vozila ustanovi pogrešku u slijedu koji dolazi iz IDE, ona neće poslati odgovor i čekat će u trajanju od najviše P3 drugu poruku sa zahtjevom za početak komunikacije.

2.2.5.2. *Stadij komunikacije*

Mogu se odrediti dva različita područja obrade pogrešaka:

1. Jedinica vozila utvrđuje pogrešku prijenosa iz IDE.

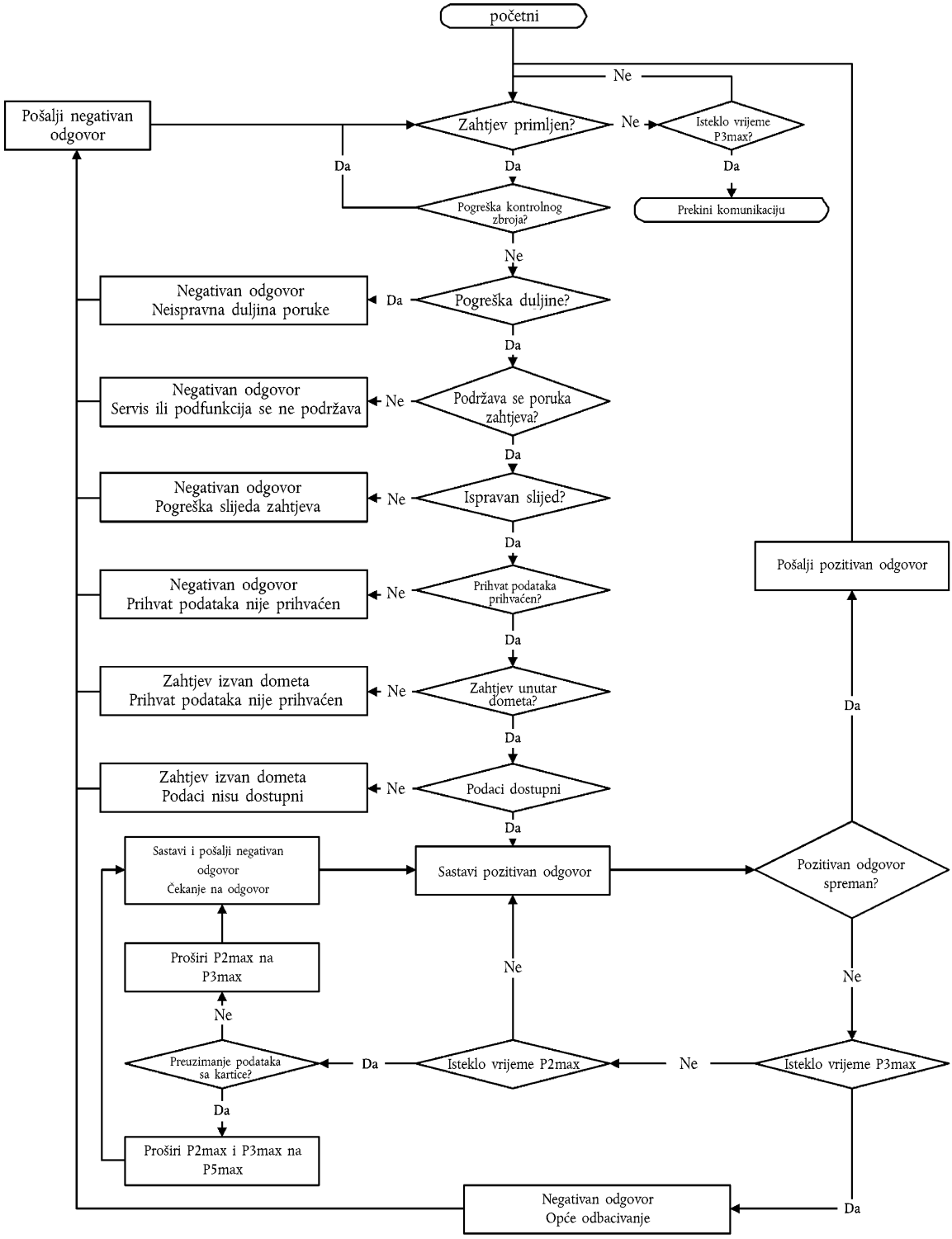
DDP_022 Za svaku primljenu poruku jedinica vozila mora ustanoviti pogreške proteka vremena, pogreške bajtnih formata (npr. kršenje početnog i zaustavnog bita) i okvirne pogreške (pogrešan broj primljenih bajtova, pogrešan bajt kontrolnog zbroja).

DDP_023 Ako jedinica vozila uoči jednu od gore spomenutih pogrešaka, ona ne šalje nikakav odgovor i zanemaruje primljenu poruku.

DDP_024 Jedinica vozila može ustanoviti ostale pogreške u formatu ili sadržaju primljene poruke (npr. poruka se ne podržava) čak i ako poruka udovoljava zahtjevima duljine i ispitnog zbroja; u tom slučaju jedinica vozila mora odgovoriti IDE porukom s negativnim odgovorom koja navodi narav pogreške.

Slika 2.

Obrada pogrešaka u jedinici vozila



2. IDE uočava pogrešku prijenosa iz jedinice vozila.

DDP_025 Za svaku primljenu poruku IDE mora ustanoviti vremenske pogreške, pogreške u formatu bajtova (npr. kršenja početnog i završnog bita) i okvirne pogreške (pogrešan broj primljenih bajtova, pogrešan bajt kontrolnog zbroja).

DDP_026 IDE mora uočiti pogreške slijeda, npr. neispravan korak povećanja brojača dijelova poruke za naredne primljene poruke.

DDP_027 Ako IDE utvrdi pogrešku ili nema odgovora iz jedinice vozila u vremenu P2max, poruka sa zahtjevom će se ponovo poslati u najviše tri prijenosa ukupno. Za potrebe ovog uočavanja pogreške, potvrda dijela poruke će se smatrati zahtjevom upućenim jedinici vozila.

DDP_028 IDE mora čekati u trajanju od najmanje P3min prije početka svakog prijenosa; razdoblje čekanja se mjeri od posljednjeg izračunatog javljanja zaustavnog bita nakon otkrivanja pogreške.

Slika 3.

Obrada pogrešaka u IDE

2.2.6. ***Sadržaj poruke odgovora***

Ovaj stavak navodi sadržaj podatkovnih polja različitih poruka s pozitivnim odgovorom.

Podatkovni elementi su definirani u rječnika podataka Dodatka 1..

2.2.6.1. *Pozitivan odgovor za prijenos pregleda podataka*

DDP_029 Podatkovno polje poruke ‚pozitivnog odgovora za prijenos pregleda podataka' mora pružiti sljedeće podatke sljedećim redom prema SID 76h, TREP 01h i odgovarajućem prelamanju i brojanju dijelova poruke:

Podatkovni element	Duljina (u bajtovima)	Napomena
MemberStateCertificate	194	Certifikati sigurnosti VU
VUCertificate	194	
VehicleIdentificationNumber	17	Identifikacija vozila
VehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
CurrentDateTime	4	Tekući datum i vrijeme VU
VuDownloadablePeriod		Razdoblje u kojem je moguće preuzimati podatke
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Vrsta kartica umetnutih u VU
VuDownloadActivityData		Prethodno preuzimanje podataka sa VU
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData		Sve blokade za potrebe tvrtke su spremljene. Ako je odjeljak prazan, šalje se samo noOfLocks = 0
noOfLocks	1	
...	(98)	
VuCompanyLocksRecord: lockInTime	4	
VuCompanyLocksRecord: lockOutTime	4	
VuCompanyLocksRecord: companyName	36	
VuCompanyLocksRecord: companyAddress	36	
VuCompanyLocksRecord: companyCardNumber	18	
...		
VuControlActivityData		Svi kontrolni zapisi su spremljeni u VU. Ako je odjeljak prazan, šalje se samo noOfControls = 0
noOfControls	1	
...	(31)	
VuControlActivityRecord: controlType	1	
VuControlActivityRecord: controlTime	4	
VuControlActivityRecord: controlCardNumber	18	
VuControlActivityRecord: downloadPeriodBeginTime	4	
VuControlActivityRecord: downloadPeriodEndTime	4	
...		
Signature	128	RSA potpis svih podataka (osim certifikata) od VehicleIdentificationNumber do posljednjeg bajta zadnjeg VuControlActivityREcord

2.2.6.2. *Pozitivan odgovor za prijenos podataka o aktivnostima*

DDP_030 Podatkovno polje poruke ‚pozitivnog odgovora za prijenos podataka o aktivnostima' pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 02h i odgovarajućem prelamanju i brojanju dijelova poruke:

Podatkovni element	Duljina (u bajtovima)	Napomena
TimeReal	4	Datum dana kada su preuzeti podaci
OdometerValueMidnight	3	Stanje brojača kilometara na kraju dana preuzimanja podataka
VuCardIWData		Podaci o broju ciklusa umetanja i izvlačenja kartice.
noOfVuCardIWRecords	2	
...	(129)	— Ako ovaj odjeljak nema raspoloživih podatka, šalje se samo noOfVuCardIWRecords = 0.
VuCardIWRecord: cardHolderName		— Kada se VuCardIWRecord proteže preko 00:00 (umetanje kartice prethodnog dana) ili preko 24:00 (izvlačenje kartice sljedećeg dana), javlja se u cijelosti oba dana.
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		Stanje utora u 00:00 i promjene aktivnosti zabilježene na dan preuzimanja podataka.
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Evidencija podataka koja se odnose na mjesta za dan kada su preuzeti podaci. Ako je odjeljak prazan, šalje se samo noOfPlaceRecords = 0.
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord: fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		Podaci o posebnim uvjetima zabilježeni za dan za koji se preuzimaju podaci. Ako je odjeljak prazan, šalje se samo noOfSpecificConditionRecords = 0.
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	RSA potpis svih podataka od TimeReal do posljednjeg bajta zadnjeg zapisa o posebnim uvjetima.

2.2.6.3. *Pozitivan odgovor za prijenos podataka o događajima i pogreškama*

DDP_031 Podatkovno polje poruke ‚pozitivnog odgovora za prijenos podataka o događajima i pogreškama' pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 03h i odgovarajućem prelamanju i brojanju dijelova poruke:

Podatkovni element	Duljina (u bajtovima)	Napomena
VuFaultData		Sve pogreške pohranjene ili se trenutačno događaju u VU. Ako ovaj odjeljak nema podatka, šalje se samo noOfVuFaults = 0.
NoOfVuFaults	1	
...	(82)	
VuFaultRecord: FaultType	1	
VuFaultRecord: FaultRecordPurpose	1	
VuFaultRecord: FaultBeginTime	4	
VuFaultRecord: FaultEndTime	4	
VuFaultRecord: CardNumberDriverSlotBegin	18	
VuFaultRecord: cardNumberCodriverSlotBegin	18	
VuFaultRecord: CardNumberDriverSlotEnd	18	
VuFaultRecord: CardNumberCodriverSlotEnd	18	
...		
VuEventData		Svi događaji (osim prekoračenja brzine) pohranjeni ili se trenutačno događaju. Ako ovaj odjeljak nema podatka, šalje se samo noOfVuEvents = 0.
NoOfVuEvents	1	
...	(83)	
VuEventRecord: EventType	1	
VuEventRecord: EventRecordPurpose	1	
VuEventRecord: EventBeginTime	4	
VuEventRecord: EventEndTime	4	
VuEventRecord: CardNumberDriverSlotBegin	18	
VuEventRecord: cardNumberCodriverSlotBegin	18	
VuEventRecord: CardNumberDriverSlotEnd	18	
VuEventRecord: CardNumberCodriverSlotEnd	18	
VuEventRecord: SimilarEventsNumber	1	
...		
VuOverSpeedingControlData		Podaci koji se odnose na posljednju kontrolu prekoračenja brzine (standardni podaci ako nema podataka).
LastOverspeedControlTime	4	
FirstOverspeedSince	4	
NumberOfOverspeedSince	1	
VuOverSpeedingEventData		Svi podaci o prekoračenju brzine pohranjeni u VU. Ako je ovaj odjeljak prazan, šalje se samo noOfVuOverSpeedingEvents = 0.
NoOfVuOverSpeedingEvents	1	
...	(31)	
VuOverSpeedingEventRecord: EventType	1	
VuOverSpeedingEventRecord: EventRecordPurpose	1	
VuOverSpeedingEventRecord: EventBeginTime	4	
VuOverSpeedingEventRecord: EventEndTime	4	
VuOverSpeedingEventRecord: MaxSpeedValue	1	
VuOverSpeedingEventRecord: AverageSpeedValue	1	
VuOverSpeedingEventRecord: CardNumberDriverSlotBegin	18	
VuOverSpeedingEventRecord: SimilarEventsNumber	1	
...		
VuTimeAdjustmentData		Svi događaji o podešavanju vremena se pohranjuju u VU (izvan okvira punog kalibriranja). Ako ovaj odjeljak nema podatka, šalje se samo noOfVuTimeAdjuRecords = 0.
NoOfVuTimeAdjRecords	1	
...	(98)	
VuTimeAdjustmentRecord: OldTimeValue	4	
VuTimeAdjustmentRecord: NewTimeValue	4	
VuTimeAdjustmentRecord: WorkshopName	36	
VuTimeAdjustmentRecord: WorkshopAddress	36	
VuTimeAdjustmentRecord: WorkshopCardNumber	18	
...		
Signature	128	RSA potpis svih podataka počevši od noOfVuFaults do posljednjeg bajta zadnjeg zapisa o podešavanju vremena.

2.2.6.4. *Pozitivan odgovor za prijenos podrobnih podataka o brzini*

DDP_032 Podatkovno polje poruke ‚pozitivan odgovor za prijenos podrobnih podataka o brzini' pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 04h i odgovarajućem prelamanju i brojanju dijelova poruke:

Podatkovni element	Duljina (u bajtovima)	Napomena
VuDetailedSpeedData		Svi podrobni podaci o brzini pohranjeni u VU (jedan blok brzine u minuti tijekom koje se vozilo kretalo). 60 vrijednosti brzine u minuti (jedna u sekundi).
NoOfSpeedBlocks	2	
...		
VuDeatailedSpeedBlock		
SpeedBlockBeginDate	4	
speedsPerSecond	60	
...		
Signature	128	RSA potpis svih podataka počevši od noOfSpeedBlocks do posljednjeg bajta zadnjeg bloka brzine

2.2.6.5. *Pozitivan odgovor za prijenos tehničkih podataka*

DDP_033 Podatkovno polje ‚pozitivnog odgovora za prijenos tehničkih podataka' pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 05h i odgovarajućem prelamanju i brojanju dijelova poruke:

Podatkovni element	Duljina (u bajtovima)	Napomena
VuIdentification		
vuManufacturerName	36	
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		svi zapisi o kalibraciji pohranjeni u VU.
noOfVuCalibrationRecords	1	
...	(164)	
VuCalibrationRecord		
calibrationPurpose	1	
workshopName	36	
workshopAddress	36	
workshopCardNumber	18	
workshopCardExpiryDate	4	
vehicleIdentificationNumber	17	
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
wVehicleCharacteristicConstant	2	
kConstantOfRecordingEquipment	2	
lTyreCircumference	2	
tyreSize	15	
authorisedSpeed	1	
oldOdometerValue	3	
newOdometerValue	3	
oldTimeValue	4	
newTimeValue	4	
nextCalibrationDate	4	
...		
Signature	128	RSA potpis svih podataka počevši od vuManufacturerName do posljednjeg bajta zadnjeg VuCalibrationRecord

2.3. **Spremanje datoteke ESM**

DDP_034 Ako je proces preuzimanja podataka obuhvatio i prijenos podataka iz jedinice vozila, IDE mora pohraniti unutar jedne fizičke datoteke sve podatke koje je primio sa jedinicie vozila tijekom procesa preuzimanja podataka u okviru poruka s pozitivnim odgovorom na zahtjev za prijenos podataka. Pohranjeni podaci ne sadrže glave poruka, brojače dijelova poruke, prazne dijelove poruka i kontrolne zbrojeve, ali obuhvaćaju SID i TREP (prvog dijela poruke samo ako ima više dijelova poruka).

3. PROTOKOL PREUZIMANJA PODATAKA S KARTICE TAHOGRAFA

3.1. **Područje primjene**

Ovaj stavak opisuje izravno preuzimanje podataka s kartice tahografa na IDE. IDE nije dio sigurnog okruženja; stoga se ne vrši nikakva autentifikacija između kartice i IDE.

3.2. **Definicije**

Proces preuzimanja podataka: Svaki put se obavlja preuzimanje podataka s ICC. Proces obuhvaća cjelokupan postupak od vraćanja u početno stanje ICC od strane IFD do stavljanja izvan pogona ICC (izvlačenje kartice ili sljedeće vraćanje u početno stanje).

Potpisana podatkovna datoteka: Datoteka se prenosi na IFD u običnom tekstu. Na ICC se datoteka sažima i potpisuje, a potpis se prenosi na IFD.

3.3. **Preuzimanje podataka s kartice**

DDP_035 Preuzimanje podataka s kartice tahografa obuhvaća sljedeće korake:

— preuzimanje zajedničkih podataka kartice u EFICC i IC Ovi podaci su neobvezni i nisu zaštićeni digitalnim potpisom,

— preuzimanje EF Card_Certificate i CA_Certificate Ovaj podatak nije zaštićen digitalnim potpisom,

Obvezno je preuzeti ove datoteke u svakom procesu preuzimanja podataka.

— preuzimanje drugih podataka aplikacije EF (unutar DF Tahografa) osim EF Card_Download. Ovi podaci su zaštićeni digitalnim potpisom,

— obavezno je preuzeti najmanje EF Application_Identification i ID: u svakom procesu preuzimanja podataka,

— prilikom preuzimanja podataka s kartice vozača također je obvezno preuzeti sljedeće EF:

— Events_Data,

— Faults_Data,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific Conditions

— prilikom preuzimanja podataka s kartice vozača, ažuriranje LastCardDownload u Card_Download EF.,

— prilikom preuzimanja podataka s kartice radionice, vraćanje u početno stanje brojača kalibracija u EF Card_Download.Card_Download.

3.3.1. ***Slijed inicijalizacije***

DDP_036 IDE započinje sljedećim slijedom:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	Vraćanje hardvera u početno stanje	
ATR	⇨		

Može se koristiti PPS za prijelaz na veću brzinu prijenosa podataka ako ICC to podržava.

3.3.2. ***Slijed za nepotpisane podatkovne datoteke***

DDP_037 Slijed prijenosa ICC, IC, Card_Certificate i CA_Certificate je sljedeći: je sljedeći:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	Odabir datoteke	Odabrati datoteku selektirajući je pomoću identifikatora datoteka
OK	⇨		
	⇦	Binarno čitanje	Ako datoteka sadrži više podataka nego što je veličina međumemorije čitača ili kartice, naredbu treba ponoviti dok se ne pročita cijela datoteka.
Podaci sa datoteke OK	⇨	Spremanje podataka u ESM	prema 3.4. (Format spremanja podataka)

Napomena: Prije odabira `Card_Certificate` EF, mora se odabrati tahografska aplikacija (odabir putem AID).

3.3.3. ***Slijed za potpisane podatkovne datoteke***

DDP_038 Koristi se sljedeći slijed za svaku od sljedećih datoteka koju treba preuzeti sa njihovim potpisom:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	Odabir datoteke	
OK	⇨		
	⇦	Sažimanje datoteke	Izračunava vrijednost sažimanja nad sadržajem podataka odabrane datoteke korištenjem propisanog algoritma funkcije sažimanja prema Prilogu 11. Ova naredba nije ISO-naredba.
Izračun vrijednosti sažimanja datoteke i privremeno pohranjivanje vrijednost sažimanja			
OK	⇨		
	⇦	Binarno čitanje	Ako datoteka sadrži više podataka nego što je veličina međumemorije čitača ili kartice, naredbu treba ponoviti dok se ne pročita cijela datoteka.
Podaci datoteke OK	⇨	Spremanje primljenih podataka u ESM	prema 3.4. (Format za spremanje podataka
OK	⇦	PSO: Izračun digitalnog potpisa	
Zaštitna radnja ‚izračuna digitalnog potpisa' korištenjem privremeno pohranjene vrijednosti sažimanja			
Potpis OK	⇨	Stavljanje podataka uz prethodno pohranjene podatke na ESM	prema 3.4. (Format za spremanje podataka)

3.3.4. ***Slijed vraćanja brojača kalibracija u početno stanje***

DDP_039 Slijed vraćanja u početno stanje brojača NoOfCalibrationsSinceDownload u Card_Download EF na kartici radionice je sljedeći:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	Select File EF Card_Download	Odabir pomoću identifikatora datoteke
OK	⇦		
	⇦	Binarno ažuriranje NoOfCalibrations-SinceDownload = '00 00'	
Vraćanje broja preuzimanja podataka s kartice u početno stanje			
OK	⇨		

3.4. **Format spremanja podataka**

3.4.1. ***Uvod***

DDP_040 Preuzeti podaci se moraju pohranjivati u skladu sa sljedećim uvjetima:

— podatke se sprema transparentno. To znači da se poredak bajtova kao i poredak bitova unutar bajtova koji se prenose s kartice mora očuvati tijekom pohranjivanja,

— svi podaci s kartice koji su preuzeti tijekom procesa preuzimanja se spremaju u jednoj datoteci na ESM.

3.4.2. ***Format datoteke***

DDP_041 Format datoteke je niz više TLV objekata.

DDP_042 Znak za EF je FID plus dodatak ‚00'.

DDP_043 Znak potpisa EF je FID datoteke plus dodatak ‚01'.

DDP_044 Duljina je dvobajtna vrijednost. Vrijednost određuje broj bajtova u polju vrijednosti. Vrijednost ‚FF FF' u polju duljine je rezervirana za buduću uporabu.

DDP_045 Ako datoteka nije preuzeta, ništa što se odnosi na datoteku se ne smije pohraniti (nikakva oznaka i nikakva nulta duljina).

DDP_046 Potpis se pohranjuje kao sljedeći objekt TLV izravno nakon TLV objekta koji sadrži podatke datoteke.

Definicija	Značenje	Dužina
FID (2 bajta) || ‚00'	Oznaka za EF (FID)	3 bajta
FID (2 bajta) || ‚01'	Znak za potpis EF(FID)	3 bajta
XX XX	Duljina polja vrijednosti	2 bajta

Primjer podataka u preuzetoj datoteci na ESM:

Oznaka:	Duljina:	Vrijednost
00 02 00	00 11	Podaci EF ICC
C1 00 00	00 C2	Podaci EF Card_Certificate
		…
05 05 00	0A 2E	Podaci EF Vehicles_Used
05 05 01	00 80	Potpis EF Vehicles_Used

4. PREUZIMANJE PODATAKA S KARTICE TAHOGRAFA PREKO JEDINICE U VOZILU

DDP_047 Jedinica vozila mora omogućiti preuzimanje sadržaja kartice vozača umetnute u priključeni IDE.

DDP_048 IDE mora poslati poruku ‚zahtjev za prijenos podataka s kartice' na jedinicu vozila za pokretanje tog načina rada (vidjeti 2.2.2.9.).

DDP_049 Jedinica vozila potom mora preuzeti sve podatke sa kartice, datoteku po datoteku, u skladu s protokolom preuzimanja s kartice definiranim u stavku 3. i dostaviti sve podatke primljene s kartice na IDE unutar odgovarajućeg formata datoteke TLV (vidjeti 3.4.2.) i komprimirane unutar poruke ‚pozitivan odgovor za prijenos podataka'.

DDP_050 IDE mora vratiti podatke s kartice iz poruke ‚pozitivan odgovor za prijenos podataka' (uklanjanje svih zaglavlja, SID, TREP, brojača dijelova poruke i kontrolnih zbrojeva) i pohraniti ih u jednu fizičku datoteku kako je opisano u stavku 2.3.

DDP_051 Jedinica vozila nakon toga, prema potrebi, ažurira datoteku Control_Activity_Data ili Card_Download na kartici vozača.

Dodatak 8.

PROTOKOL KALIBRACIJE

SADRŽAJ

1. UVOD

Ovaj Dodatak opisuje način razmjene podataka između jedinice u vozilu i ispitnog uređaja putem K-linije koja čini sastavni dio sučelja za kalibraciju opisanog u Dodatku 6. Također opisuje upravljanje linijom ulazno/izlaznih signala na utičnici za kalibraciju.

Uspostavljanje komunikacije K-linijom je opisano u odjeljku 4. ‚Servis komunikacije'.

Ovaj Prilog upotrebljava pojam dijagnostičkih ‚aktivnost' za određivanje opsega upravljanja putem K-linije u različitim uvjetima. Standardna aktivnost je ‚StandardDiagnosticSession' u kojoj se svi podaci mogu čitati s jedinice u vozilu, ali niti jedan podatak nije moguće upisati u jedinicu u vozilu.

Odabir dijagnostičke aktivnosti se opisuje u odjeljku 5. ‚Servis upravljanja'.

CPR_001 ‚ECUProgrammingSession' omogućava upisivanje podataka u jedinicu u vozilu. Kod upisa podataka za kalibraciju (zahtjevi 097 i 098), jedinica u vozilu također mora biti u načinu rada KALIBRACIJA.

Prijenos podataka putem K-linije je opisan u odjeljku 6. ‚Servis prijenosa podataka'. Formati prenesenih podataka su detaljno izloženi u odjeljku 8. ‚Formati dataRecords'.

CPR_002 ‚ECUAdjustmentSession' omogućava izbor kalibracijskog načina rada preko U/I signala sučelja K-linije. Upravljanje kalibriranjem U/I signala je opisano u odjeljku 7. ‚Upravljanje ispitnim impulsima – funkcionalna jedinica upravljanja ulazom/izlazom'.

CPR_003 U ovom dokumentu se ‚tt' odnosi na adresu ispitnog uređaja.Iako može postojati povlaštena adresa ispitnih uređaja, jedinica vozila se ispravno odaziva na svaku adresu ispitnog uređaja. Fizička adresa jedinice vozila je 0xEE.

2. IZRAZI, DEFINICIJE I LITERATURA

Protokoli, poruke i šifre pogreške se u načelu temelje na dosadašnjem nacrtu ISO 14229-1 (Cestovna vozila - dijagnostički sustavi - dio 1.: dijagnostički servis, inačica 6. od 22. veljače 2001.).

Za identifikatore servisa, zahtjevi za servise i odzive, te za standardne parametre koriste se bajtno šifriranje i heksadecimalne vrijednosti.

Izraz ‚ispitni uređaj' se odnosi na uređaj koji se koristi za upisivanje podataka za programiranje/kalibraciju jedinice vozila.

Izrazi ‚korisnik' i ‚poslužitelj' se odnose na ispitni uređaj odnosno jedinicu vozila.

Izraz ECU označuje ‚elektronsku upravljačku jedinicu' i odnosi se na jedinicu vozila.

Literatura:

ISO 14230-2: Cestovna vozila - Dijagnostički sustavi – Protokol s ključnim riječima 2000. - Dio 2: Razina podatkovnih veza. Prvo izdanje: 1999. Vozila - dijagnostički sustavi

3. PREGLED SERVISA

3.1. **Raspoloživi servisi**

Sljedeća tablica daje pregled servisa koje će biti dostupni na tahografu i koji su definirani u ovom dokumentu.

CPR_004 Tablica prikazuje servise koji su dostupni u aktiviranoj dijagnostičkom procesu.

— Prvi stupac navodi servise koji su dostupni,

— drugi stupac obuhvaća broj točke ovog Priloga ako je servis detaljnije definiran,

— treći stupac pridružuje vrijednosti identifikatora servisa za poruke zahtjeva,

— četvrti stupac navodi servise ‚StandardDiagnosticSession' (SD) koje moraju biti ugrađene u svaku jedinicu vozila,

— peti stupac navodi servisne procese ‚ECUAdjustmentSession' (ECUAS) koji moraju biti ugrađeni da bi se upravljalo U/I signalnom linijom u utičnici za kalibraciju na prednjoj strani jedinice vozila,

— šesti stupac navodi servise ‚ECUProgrammingSession' (ECUPS) koji moraju biti ugrađeni da bi se programiralo parametre u jedinici vozila.

Tablica 1.

Tablica s pregledom vrijednosti identifikatora servisa

			Dijagnostički procesi		
Naziv servisa za dijagnostiku	Odjeljak br.	Zahtijevana Sid vrijednost	SD	ECUAS	ECUPS
StartCommunication	4.1.	81	■	■	■
StopCommunication	4.2.	82	■		
TesterPresent	4.3.	3E	■	■	■
StartDiagnosticSession	5.1.	10	■	■	■
SecurityAccess	5.2.	27	■	■	■
ReadDataByIdentifier	6.1.	22	■	■	■
WriteDataByIdentifier	6.2.	2E			■
InputOutputControlByIdentifier	7.1.	2F		■	

■ Ovaj simbol označuje da je servis obvezan u ovom dijagnostičkom procesu.
Izostanak simbola označuje da ovaj servis nije dozvoljen u ovom dijagnostičkom procesu.

3.2. **Šifre odziva**

Šifre odziva se definiraju za svaki servis.

4. SERVIS KOMUNIKACIJE

Neki servisi su potrebni za uspostavljanje i održavanje komunikacije. Oni se ne javljaju na izvršnom nivou. Raspoloživi servisi su navedeni u sljedećoj tablici:

Tablica 2.

Servisi komunikacije

Naziv servisa	Opis
StartCommunication	Korisnik zahtjeva početak komunikacijskog procesa s poslužiteljem (poslužiteljima)
StopCommunication	Korisnik zahtijeva prekid tekućeg komunikacijskog procesa
TesterPresent	Korisnik poručuje poslužitelju da je još uvijek prisutan

CPR_005 Servis StartCommunication se koristi da bi započela komunikacija. Da bi se obavio neki servis, komunikaciju se mora pokrenuti, a komunikacijski parametri moraju biti primjereni željenom načinu rada.

4.1. **Servis StartCommunication**

CPR_006 Po prijemu znaka primitiva StartCommunication, jedinica vozila mora provjeriti može li se zahtijevana komunikacijska veza pokrenuti u trenutačnim uvjetima. Važeći uvjeti za početak komunikacijske veze su opisani u dokumentu ISO 14230-2.

CPR_007 Potom jedinica vozila mora obaviti sve potrebne radnje za početak komunikacijske veze i šalje primitiv odziva Start-Communication s odabranim pozitivnim parametrima odziva.

CPR_008 Ako jedinica vozila koja je već pokrenuta (i započela je dijagnostičku aktivnost) primi novi zahtjev StartCommunication (npr. zbog ispravljanja pogreške u dijagnostičkom uređaju) zahtjev mora biti prihvaćen i jedinica vozila se mora ponovo pokrenuti.

CPR_009 Ako zbog nekog razloga komunikacijska veza ne može biti pokrenuta, jedinica vozila će i dalje raditi kao i neposredno prije pokušaja pokretanja komunikacijske veze.

CPR_010 Poruka sa zahtjevom StartCommunication mora biti fizički naslovljena.

CPR_011 Inicijalizacija jedinice vozila za servise se obavlja u postupku ‚brze inicijalizacije':

— prije svake aktivnosti postoji razdoblje neaktivnosti sabirnice,

— dijagnostički uređaj potom šalje obrazac za inicijalizaciju,

— svi podaci koji su potrebni za uspostavljanje komunikacije su sadržani u odzivu jedinice vozila.

CPR_012 Po završetku inicijalizacije,

— svi komunikacijski parametri se postavljaju na vrijednosti definirane u tablici 4. prema ključnim bajtovima,

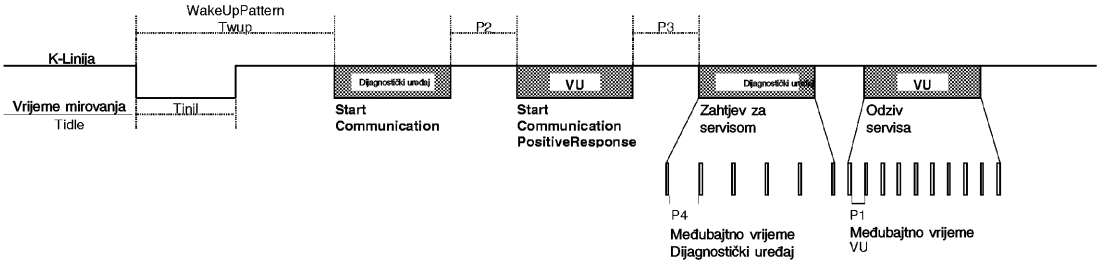
— jedinica vozila čeka na prvi zahtjev dijagnostičkog uređaja,

— jedinica vozila je u standardnom dijagnostičkom načinu rada, tj. StandardDiagnosticSession,

— U/I signalna linija kalibracije je u standardnom načinu rada, tj. u načinu rada izvan pogona.

CPR_014 Brzina podataka na K-liniji mora biti 10 400 Bauda.

CPR_016 Brza inicijalizacija započinje kada dijagnostički uređaj prenese obrazac pobude (Wup) na K-liniji. Obrazac započinje nakon vremena mirovanja na K-liniji u vremenu smanjene aktivnosti Tinil. Ispitna jedinica prenosi prvi bit servisa StartCommunication nakon razdoblja Twup i prvog prekida.



CPR_017 Vremenski termini za prvo pokretanje i općenito termini veze su navedeni u tablicama u nastavku. Postoje različite mogućnosti za razdoblje mirovanja:

— prvi prijenos nakon uključivanja T_{idle} = 300 ms.

— nakon okončanja servisa StopCommunication, T_{idle} = P3 min.

— nakon prekida komunikacije zbog isteka vremena P3 max, T_{idle} = 0.

Tablica 3.

Vremenski termini za brzo pokretanje

Parametar		najmanja vrijednost	najveća vrijednost
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tablica 4.

Vremenski termini komunikacije

Vremenski parametar	Opis parametra	Donje granične vrijednosti (ms)	Gornje granične vrijednosti (ms)
		najmanja	najveća
P1	Međubajtna vrijednost za odziv jedinice vozila	0	20
P2	Vrijeme između zahtjeva dijagnostičkog uređaja i odziva VU ili dva odziva VU	25	250
P3	Vrijeme između kraja odziva VU i početka novog zahtjeva dijagnostičkog uređaja	55	5 000
P4	Međubajtno vrijeme za zahtjev dijagnostičkog uređaja	5	20

CPR_018 Format poruka za brzo pokretanje je naveden u sljedećim tablicama:

Tablica 5.

Poruka StartCommunication zahtjeva

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	81	FMT
#2	Bajt ciljne adrese	EE-	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Zahtjev za servis StarCommunication	81	SCR
#5	Kontrolni zbroj	00-FF	CS

Tablica 6.

Poruka StartCommunication s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id servisa StartCommunication s pozitivnim odgovorom	C1	SCRPR
#6	Bajt ključa 1	EA	KB1
#7	Bajt ključa 2	8F	KB 2
#8	Kontrolni zbroj	00-FF	CS

CPR_019 Nema negativnog odgovora na poruku StartCommunication zahtjeva, ako nema poruke s pozitivnim odgovorom za prijenos, tada se jedinica vozila ne pokreće, ništa se ne prenosi i ona nastavlja s redovnim radom.

4.2. **Servis StopCommunication**

4.2.1. ***Opis poruke***

Svrha ove razine servisne komunikacije je okončanje komunikacijske aktivnosti.

CPR_020 Po prijemu znaka primitiva StopCommunication, jedinica vozila mora provjeriti omogućavaju li prevladavajući uvjeti okončanje ove komunikacije. U tom slučaju jedinica vozila mora obaviti sve radnje potrebne za okončanje ove komunikacije.

CPR_021 Ako je moguće okončati komunikaciju, jedinica vozila mora izdati primitiv odziva StopCommunication s odabranim parametrima pozitivnog odgovora prije okončanja komunikacije.

CPR_022 Ako se komunikacija iz nekog razloga ne može okončati, jedinica vozila mora izdati primitiv odziva StopCommunication s odabranim parametrom negativnog odgovora.

CPR_023 Ako jedinica vozila ustanovi istek vremena P3max, komunikacija se okončava bez izdavanja primitiva bilo kakvog odgovora.

4.2.2. ***Format poruka***

CPR_024 Formati poruke za primitive StopCommunication se navode u sljedećim tablicama:

Tablica 7.

Poruka StopCommunication zahtjeva

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt adrese izvora	tt	SRC
#4	Bajt za dodatnu duljinu	01	LEN
#5	Id servisa StopCommunication zahtjeva	82	SPR
#6	Kontrolni zbroj	00-FF	CS

Tablica 8.

StopCommunication poruka s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu dužinu	01	LEN
#5	Servis StopCommunication s pozitivnim odgovorom	C2	SPRPR
#6	Kontrolni zbroj	00-FF	CS

Tablica 9.

Poruka StopCommunication s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id servisa negativnog odgovora	7F	NR
#6	Identifikacija servisa StopCommuinication zahtjeva	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Kontrolni zbroj	00-FF	CS

4.2.3. ***Određivanje parametara***

Ovaj servis ne zahtijeva nikakvo određivanje parametara.

4.3. **Servis TesterPresent**

4.3.1. ***Opis poruka***

Servis TesterPresent koristi dijagnostički uređaj kako bi ukazao poslužitelju da je još uvijek prisutan, kako bi spriječila automatsko vraćanje poslužitelja u redovan rad i moguće prekidanje komunikacije. Ovaj poslani servis povremeno održava dijagnostički proces/komunikaciju aktivnim ponovnim postavljanjem sata P3 prilikom svakog primitka zahtjeva za ovaj servis.

4.3.2. ***Format poruka***

CPR_079 Format poruka za primitive TesterPresent je prikazan u sljedećim tablicama:

Tablica 10.

Poruka TesterPresent zahtjeva

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt adrese izvora	tt	SRC
#4	Bajt za dodatnu duljinu	02	LEN
#5	Id servisa TesterPresent zahtjeva	3E	TP
#6	Podfunkcija = responseRequired = [da	01	RESPREQ_Y
	ne]	02	RESPREQ_NO
#7	Kontrolni zbroj	00-FF	CS

CPR_080 Ako je parametar responseRequired postavljen na ‚da', poslužitelj mora odgovoriti porukom sa sljedećim pozitivnim odgovorom. Ako je postavljen na ‚ne', poslužitelj ne šalje nikakav odgovor.

Tablica 11.

Poruka TesterPresent s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	01	LEN
#5	Id servisa TesterPresent s pozitivnim odgovorom	7E	TPPR
#6	Kontrolni zbroj	00-FF	CS

CPR_081 Servis mora podržavati sljedeće šifre negativnih odgovora:

Tablica 12.

Poruka TesterPresent s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id službe negativnog odgovora	7F	NR
#6	Identifikacija službe TesterPresent zahtjeva	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RCJML
#8	Kontrolni zbroj	00-FF	CS

5. SERVIS UPRAVLJANJA

Raspoloživi servisi su navedeni u sljedećoj tabeli:

Tabela 13.

Servisi upravljanja

Naziv servisa	Opis
StartDiagnosticSession	Korisnik zahtijeva pokretanje dijagnostičkog procesa s VU
SecurityAccess	Korisnik zahtijeva pristupanje funkcijama koje su ograničene na ovlaštene korisnike

5.1. **Servis StartDiagnosticSession**

5.1.1. ***Opis poruka***

CPR_025 Servis StartDiagnosticSession se koristi kako bi omogućio dijagnostičke procese u poslužitelju. Dijagnostički proces omogućava poseban skup servisa prema tablici 17. Proces može proizvođačima vozila omogućiti posebne servise koje nisu dio ovog dokumenta. Provedbena pravila moraju odgovarati sljedećim zahtjevima:

— uvijek je samo jedan dijagnostički proces aktivan u jedinici vozila,

— prilikom uključenja jedinica vozila mora uvijek pokrenuti StandardDiagnosticSession. Ako nije pokrenut niti jedan drugi dijagnostički proces, StandardDiagnosticSession mora biti aktivan sve dok je uključena jedinica vozila,

— ako je ispitni uređaj zatražio dijagnostički proces koji je već aktivan, jedinica vozila mora poslati poruku s pozitivnim odgovorom,

— kada god ispitni uređaj zatraži novi dijagnostički proces, jedinica vozila mora najprije poslati poruku StartDiagnosticSession s pozitivnim odgovorom prije nego li novi proces postane aktivan u jedinici vozila. Ako jedinica vozila nije u stanju započeti zatraženi novi dijagnostički proces, ona će odgovoriti porukom StartDiagnosticSession s negativnim odgovorom, te će se nastaviti odvijati tekući proces.

CPR_026 Dijagnostički proces započinje samo ako je uspostavljena komunikacija između korisnika i jedinice vozila.

CPR_027 Vremenski parametri opisani u tablici 4. moraju biti aktivni nakon uspješne StartDiagnosticSession s parametrom diagnosticSession postavljenim na ‚StandardDiagnosticSession' u poruci zahtjeva ako je prethodno bio aktivan drugi dijagnostički proces.

5.1.2. ***Format poruka***

CPR_028 Formati poruka za primitive StartDiagnosticSession su prikazani u sljedećim tablicama:

Tablica 14.

Poruka StartDiagnosticSession zahtjeva

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt adrese izvora	tt	SRC
#4	Bajt za dodatnu duljinu	02	LEN
#5	Id servisa StartDiagnosticSession zahtjeva	10	STDS
#6	diagnosticSession = (jedna vrijednost iz tablice 17.)	XX	DS_…
#7	Kontrolni zbroj	00-FF	CS

Tablica 15.

Poruka StartDiagnosticSession s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Dodatni bajt za duljinu	02	LEN
#5	ID servisa pozitivnog odziva StartDiagnosticSession	50	STDSPR
#6	DiagnosticSession = (ista vrijednost kao u bajtu #6 u tabeli 14.)	XX	DS_…
#7	Kontrolni zbroj	00-FF	CS

Tablica 16.

Poruka StartDiagnosticSession s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id servisa negativnog odgovora	7F	NR
#6	Id servis StartDiagnosticSession zahtjeva	10	STDS
#7	ResponseCode = (subFunctionNotSupported [a])	12	RC_SFNS
	incorrectMessageLength [b]	13	RC_IML
	conditionsNotCorrect [c])	22	RC_CNC
#8	Kontrolni zbroj	00-FF	CS

[a] Vrijednost unesena u bajt #6 poruke zahtjeva se ne podržava, tj. nije u tablici 17.
[b] Duljina poruke je pogrešna.
[c] Kriteriji za zahtjev StartDiagnosticSession nisu zadovoljeni.

5.1.3. ***Određivanje parametara***

CPR_029 Parametar diagnosticSession (DS_) koristi servis StartDiagnosticSession za odabir posebnog postupka jednog ili više poslužitelja. U ovom dokumentu su opisani sljedeći dijagnostički procesi:

Tablica 17.

Određivanje vrijednosti diagnosticSession

Heksadecimalna vrijednost	Opis	Mnemonik
81	StandardDiagnosticSession Ovaj dijagnostički proces uključuje sve servise navedene u tablici 1. stupcu 4. ‚SD'. Ovi servisi omogućavaju čitanje svih podataka s poslužitelja (VU). Ovaj dijagnostički proces je aktivan nakon što je uspješno obavljeno pokretanje između korisnika (dijagnostičkog uređaja) i poslužitelja (VU). Preko ovog dijagnostičkog procesa mogu se memorirati drugi dijagnostički procesi navedeni u ovoj točki.	SD
85	ECUProgrammingSession Ovaj dijagnostički proces uključuje sve servise navedene u tablici 1. stupcu 6. ‚ECUPS'. Ovi servisi podržavaju programiranje memorije poslužitelja (VU). Preko ovog dijagnostičkog procesa se mogu memorirati drugi dijagnostički procesi navedeni u ovoj točki.	ECUPS
87	ECUAdjustmentSession Ovaj dijagnostički proces uključuje sve servise navedene u tablici 1. stupcu 5. ‚ECUAS'. Ovi servisi podržavaju upravljanje ulazom/izlazom poslužitelja (VU). Preko ovog dijagnostičkog procesa se mogu memorirati drugi dijagnostički procesi navedeni u ovoj točki.	ECUAS

5.2. **Servis SecurityAccess**

Upisivanje podataka kalibracije ili pristup ulazu/izlazu liniji kalibracije nije moguće osim ako je jedinica vozila u načinu rada KALIBRACIJA. Pored unošenja važeće kartice radionice u jedinicu vozila, u jedinicu vozila je potrebno upisati odgovarajući PIN prije dobivanja dozvole za pristup načinu rada KALIBRACIJA.

Servis SecurityAccess osigurava način upisivanja PIN-a i ukazivanje dijagnostičkom uređaju je li jedinica vozila u načinu rada KALIBRACIJA ili nije.

Dopušteno je upisivanje PIN-a na neki drugi način.

5.2.1. ***Opis poruka***

Servis SecurityAccess se sastoji od SecurityAccess poruke ‚requestSeed', nakon čega može slijediti SecurityAccess poruka ‚sendKey'. Servis SecurityAccess se mora obavljati nakon servisa StartDiagnosticSession.

CPR_033 Dijagnostički uređaj može koristiti SecurityAccess poruku ‚requestSeed' za provjeru je li je jedinica u vozilu spremna za prihvaćanje PIN-a.

CPR_034 Ako je jedinica u vozilu već u načinu rada KALIBRACIJA, ona odgovara na zahtjev upućivanjem ‚signala' od 0x0000 korištenjem servisa SecurityAccess s pozitivnim odgovorom.

CPR_035 Ako je jedinica u vozilu spremna prihvatiti PIN za provjeru putem kartice radionice, ona odgovara na zahtjev slanjem ‚signala' koje je veće od 0x0000 korištenjem servisa SecurityAccess s pozitivnim odgovorom.

CPR_036 Ako jedinica u vozilu nije spremna prihvatiti PIN iz dijagnostičkog uređaja, bilo zato što umetnuta kartica radionice nije valjana ili zato što kartica radionice nije umetnuta, ili stoga što jedinica u vozilu očekuje PIN na neki drugi način, ona mora odgovoriti na zahtjev negativnim odgovorom sa šifrom odziva koji je postavljen na conditionsNotCorrectOrRequestSequenceError.

CPR_037 Dijagnostički uređaj može potom koristiti SecurityAccess poruku ‚sendKey' za slanje PIN-a jedinici u vozilu. Da bi se dalo vremena za provođenje postupka autentifikacije kartice, jedinica vozila mora koristiti šifru negativnog odgovora requestCorrectlyReceived-ResponsePending kako bi se produljilo vrijeme za davanje odgovora. Međutim, dopušteno vrijeme odziva ne smije biti dulje od pet minuta. Čim se zahtijevani servis okonča, jedinica vozila mora poslati poruku s pozitivnim odgovorom ili poruku s negativnim odgovorom sa šifrom odgovora koja je različita od ove. Jedinica vozila može ponavljati šifru requestCorrectlyReceived-ResponsePending s negativnim odgovorom do okončanja traženog servisa i do upućivanja poruke s konačnim odgovorom.

CPR_038 Jedinica u vozilu mora odgovarati na ovaj zahtjev korištenjem servisa SecurityAccess s pozitivnim odgovorom samo kada je u načinu rada KALIBRACIJA.

CPR_039 U sljedećim slučajevima, jedinica u vozilu se odaziva na ovaj zahtjev negativnim odgovorom sa šifrom odgovora postavljenom na:

— subFunctionNot supported: nepravilan format parametra podfunkcije (accessType),

— conditionsNotCorrectOrRequestSequenceError: jedinica u vozilu nije spremna za prihvaćanje unosa PIN,

— invalidKey: PIN nije valjan i broj pokušaja provjere PIN-a nije premašen,

— exceededNumberOfAttempts: PIN nije valjan i broj pokušaja provjere PIN-a je premašen,

— generalReject: ispravan PIN, ali uzajamna autentifikacija s karticom radionice nije uspjela.

5.2.2. ***Format poruka – SecurityAccess – requestSeed***

CPR_040 Formati poruka za SecurityAccess primitive ‚requestSeed' je prikazan u sljedećim tablicama:

Tablica 18.

Zahtjev SecurityAccess – poruka requestSeed

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt adrese izvora	tt	SRC
#4	Bajt za dodatnu duljinu	02	LEN
#5	Id servisa SecurityAccess zahtjeva	27	SA
#6	accessType – requestSeed	7D	AT_RSD
#7	Kontrolni zbroj	00-FF	CS

Tablica 19.

Poruka SecurityAccess – requestSeed s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	04	LEN
#5	Id servisa SecurityAccess s pozitivnim odgovorom	67	SAPR
#6	accessType – requestSeed	7D	AT_RSD
#7	SeedHigh	00-FF	SEEDH
#8	SeedLow	00-FF	SEEDL
#9	Kontrolni zbroj	00-FF	CS

Tablica 20.

Poruka SecurityAccess s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id servisa negativnog odgovora	7F	NR
#6	Id servisa SecurityAccess zahtjeva	27	SA
#7	responseCode = (conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Kontrolni zbroj	00-FF	CS

5.2.3. ***Formati poruka – SecurityAccess – sendKey***

CPR_041 Formati poruka za SecurityAccess primitive ‚sendKey' su prikazani u sljedećim tablicama:

Tablica 21.

Zahtjev SecurityAccess– poruka sendKey

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt adrese izvora	tt	SRC
#4	Bajt za dodatnu duljinu	m + 2	LEN
#5	Id servisa SecurityAccess zahtjeva	27	SA
#6	accessType – sendKey	7E	AT_SK
#7 do #m + 6	Key#1 (viši)	xx	KEY
	…	…	
	Key #m (niži, m mora biti najmanje 4, a najviše 8)	xx	
#m + 7	Kontrolni zbroj	00-FF	CS

Tablica 22.

Poruka SecurityAccess – sendKey s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	02	LEN
#5	Id servisa SecurityAccess s pozitivnim odgovorom	67	SAPR
#6	accessType – sendKey	7E	AT_SK
#7	Kontrolni zbroj	00-FF	CS

Tablica 23.

Poruka SecurityAccess s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id servisa negativnog odgovora	7F	NR
#6	Id servisa SecurityAccess zahtjeva	27	SA
#7	responseCode = generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending)	78	RC_RCR_RP
#8	Kontrolni zbroj	00-FF	CS

6. SERVIS PRIJENOSA PODATAKA

Raspoloživi servisi su opisani u sljedećoj tablici:

Tablica 24.

Servisi prijenosa podataka

Naziv servisa	Opis
ReadDataByIdentifier	Korisnik zahtjeva prijenos tekuće vrijednosti zapisa koji je dostupan za recordDataIdentifier
WriteDataByIdentifier	Korisnik zahtijeva upisivanje zapisa kojem je pristupio recordDataIdentifier

6.1. **Servis ReadDataByIdentifier**

6.1.1. ***Opis poruka***

CPR_050 Servisom ReadDataByIdentifier se služi korisnik za traženje vrijednosti podatkovnog zapisa iz poslužitelja. Podatke prepoznaje recordDataIdentifier. Odgovornost proizvođača jedinice vozila je da udovolji uvjetima poslužitelja prilikom obavljanja servisa.

6.1.2. ***Format poruka***

CPR_051 Formati poruka za primitive ReadDataByIdentifier su prikazani u sljedećim tablicama:

Tablica 25.

Poruka ReadDataByIdentifier zahtjeva

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt adrese izvora	tt	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id servisa ReadDataByIdentifier zahtjeva	22	RDBI
#6 i #7	recordDataIdentifier = (vrijednost iz tablice 28.)	xxxx	RDI_…
#8	Kontrolni zbroj	00-FF	CS

Tablica 26.

Poruka ReadDataByIdentifier s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	m + 3	LEN
#5	Id servisa ReadDataByIdentifier s pozitivnim odgovorom	62	RDBIPR
#6 i #7	recordDataIdentifier = (ista vrijednost kao bajtovi #6 i #7 iz tabele 25.)	xxxx	RDI_…
#8 do #m + 7	dataRecordO = (data#l : data#m)	xx : xx	DREC_DATA1 : DREC_DATAm
#m + 8	Kontrolni zbroj	00-FF	CS

Tablica 27.

Poruka ReadDataByIdentifier s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id servisa negativnog odgovora	7F	NR
#6	Id servisa ReadDataByIdentifier zahtjeva	22	RDBI
#7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Kontrolni zbroj	00-FF	CS

6.1.3. ***Opis parametara***

CPR_052 Parametar recordDataIdentifier (RDI_) u poruci ReadDataByIdentifier zahtjeva prepoznaje podatkovni zapis.

CPR_053 Vrijednosti recordDataIdentifier definirane ovim dokumentom prikazuje tablica u nastavku.

Tabelu recordDataIdentifier čine četiri stupca i više redova.

— Prvi stupac (Heksadecimalna vrijednost) obuhvaća ‚heksadecimalnu vrijednost' dodijeljenu recordDataIdentifier opisanom u trećem stupcu.

— Drugi stupac (Podatkovni element) prikazuje podatkovni element iz Dodatka 1. na kojem se temelji recordDataIdentifier (ponekad je potrebno prešifriranje).

— Treći stupac (Opis) navodi odgovarajući naziv recordDataIdentifier.

— Četvrti stupac (Mnemonik) navodi mnemonik ovog recordDataIdentifier.

Tablica 28.

Određivanje vrijednosti recordDataIdentifier

Heksadecimalna vrijednost	Podatkovni element	Naziv recordDataIdentifier (vidjeti format u točki 8.2.)	Mnemonik
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

CPR_054 Parametar dataRecord (DREC_) koristi ReadDataByIdentifier poruka s pozitivnim odgovorom za pružanje korisniku (dijagnostičkom uređaju) vrijednosti podatkovnog zapisa kojeg je prepoznao recordDataIdentifier. Formati podataka su opisani u odjeljku 8. Mogu se ugraditi dodatni korisnički neobvezni dataRecords uključujući posebne ulazne, unutarnje i izlazne podatke, ali nisu definirani u ovom dokumentu.

6.2. **Servis WriteDataByIdentifier**

6.2.1. ***Opis poruka***

CPR_056 Servis WriteDataByIdentifier korisnik koristi za upisivanje vrijednosti podatkovnih zapisa u poslužitelj. Podatke prepoznaje recordDataIdentifier. Odgovornost je proizvođača jedinice vozila da udovolji uvjetima poslužitelja prilikom obavljanja ovog serisa. Za ažuriranje parametara navedenih u tablici 28., jednica vozila mora biti u načinu rada KALIBRACIJA.

6.2.2. ***Format poruka***

CPR_057 Formati poruka za primitive WriteDataByIdentifier su navedeni u sljedećim tablicama:

Tablica 29.

Poruka WriteDataByIdentifier zahtjeva

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt adrese izvora	tt	SRC
#4	Bajt za dodatnu duljinu	m+3	LEN
#5	Id servisa WriteDataByIdentifier zahtjeva	2E	WDBI
#6 i #7	recordDataIdentifier = (vrijednost iz tabele 28.)	xxxx	RDI_…
#8 do #m + 7	dataRecord() = (data#1 : data#m)	xx xx	DREC_DATA1 DREC_DATAm
#m+8	Kontrolni zbroj	00-FF	CS

Tablica 30.

Poruka WriteDataByIdentifier s pozitivnom odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id servisa WriteDataByIdentifier s pozitivnim odgovorom	6E	WDBIPR
#6 i #7	recordDataIdentifier = (ista vrijednost kao i bajti #6 i #7 iz tabele 29.)	xxxx	RDI_…
#8	Kontrolni zbroj	00-FF	CS

Tablica 31.

WriteDataByIdentifier poruka s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id servisa negativnog odgovora	7F	NR
#6	Id servisa WriteDataByIdentifier zahtjeva	2E	WDBI
#7	responseCode = (requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect)	22	RC_CNC
#8	Kontrolni zbroj	00-FF	CS

6.2.3. ***Određivanje parametara***

Parametar recordDataIdentifier (RDI_) je određen u tablici 28.

Parametar dataRecord (DREC_) koristi poruka WriteDataByIdentifier zahtjeva za davanje poslužitelju (VU) vrijednosti podatkovnih zapisa koje je prepoznao recordDataIdentifier. Formati podataka su navedeni u odjeljku 8.

7. UPRAVLJANJE ISPITNIM IMPULSIMA – FUNKCIONALNA JEDINICA ZA UPRAVLJANJE ULAZOM/IZLAZOM

Raspoloživi servisi su navedeni u sljedećoj tablici:

Tablica 32.

Funkcionalna jedinica za upravljanje ulazom/izlazom

Naziv usluge	Opis
InputOutputControlByIdentifier	Korisnik zahtijeva upravljanje ulazom/izlazom koje je specifično za poslužitelj

7.1. **Opis poruka**

7.1.1. ***Opis poruka***

Postoji veza putem priključka na prednjoj strani tahografa koja omogućava upravljanje ili praćenje ispitnih impulsa korištenjem odgovarajuće dijagnostičke opreme.

CPR_058 Ova linija kalibracije U/I signala se može konfigurirati naredbom iz K-linije korištenjem servisa InputOutputControlByIdentifier za odabir tražene funkcije ulaza ili izlaza za liniju. Raspoloživa stanja linije su:

— izvan pogona,

— speedSignalInput, pri čemu se linija kalibracije U/I signala koristi za ulaz signala brzine (ispitni signal) koji nadomješta signal brzine senzora kretanja,

— realTimeSpeedSignalOutputSensor, pri čemu se linija kalibracije signala U/I koristi za izlaz signala brzine senzora kretanja,

— RTCOutput, pri čemu se linija kalibracije U/I signala koristi za izlaz signala UTC sata.

CPR_059 Jedinica u vozilu je morala pristupiti postupku podešavanja i mora biti u načinu rada KALIBRACIJA za konfiguraciju stanja linije. Prilikom izlaza iz postupka podešavanja ili načina rada KALIBRACIJA, jedinica u vozilu mora osigurati da se linija kalibracije U/I signala vrati u stanje ‚izvan pogona' (standardno).

CPR_060 Ako se impulsi brzine primaju u liniju ulaza signala brzine u realnom vremenu jedinice vozila dok je linija kalibracije U/I signala postavljena na ulaz, linija kalibracije U/I signala se mora postaviti na izlaz ili vratiti u stanje izvan pogona.

CPR_061 Redoslijed je sljedeći:

— uspostaviti komunikaciju od strane servisa StartCommunication,

— ući u postupak kalibracije putem servisa StartDiagnosticSession Service i biti u načinu rada KALIBRACIJA (redoslijed ove dvije operacije nije bitan),

— promjena stanja izlaza od strane servisa InputOutputControlByIdentifier.

7.1.2. ***Format poruka***

CPR_062 Formati poruka za InputOutputControlByIdentifier su prikazani u sljedećim tablicama:

Tablica 33.

Poruka zahtjeva InputOutputControlByIdentifier

Bajt #	Naziv parametra	Heksadecimalne vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt adrese izvora	tt	SRC
#4	Bajt za dodatnu duljinu	xx	LEN
#5	Sid InputOutputControlByIdentifier zahtjeva	2F	IOCBI
#6 i #7	InputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 ili # #8 do #9	ControlOptionRecord = (		COR_…
	inputOutputControlParameter – jedna vrijednost iz tabele 36.	xx	IOCP_…
	controlState – jedna vrijednost iz tabele 38. (vidjeti donju napomenu))	xx	CS_…
#9 ili #10	Kontrolni zbroj	00-FF	CS

Napomena: Parametar controlState je prisutan samo u nekim slučajevima (vidjeti točku 7.1.3.).

Tablica 34.

InputOutputControlByIdentifier poruka s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	xx	LEN
#5	SId InputOutputControlByIdentifier s pozitivnim odgovorom	6F	IOCBIPR
#6 i #7	inputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 ili # #8 do #9	controlStatusRecord = (		CSR_
	inputOutputControlParameter (ista vrijednost kao bajt #8 u tabeli 33.)	xx	IOCP_…
	controlState (ista vrijednost kao bajt #9 u tablici 33.)) (ako je primjenjivo)	xx	CS_…
#9 ili #10	Kontrolni zbroj	00-FF	CS

Tablica 35.

InputOutputControlByIdentifier poruka s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt adrese izvora	EE	SRC
#4	Bajt za dodatnu duljinu	03	LEN
#5	Id servisa negativnog odgovora	7F	NR
#6	SId InputOutputControlByIdentifier zahtjeva	2F	IOCBI
#7	responseCode = (		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded)	7A	RC_DCLE
#8	Kontrolni zbroj	00-FF	CS

7.1.3. ***Određivanje parametara***

CPR_064 Parametar inputOutputControlParameter (IOCP_) je određen u sljedećoj tablici:

Tablica 36.

Određivanje vrijednosti inputOutputControlParameter

Heksadecimalna vrijednost	Opis	Mnemonik
00	ReturnControlToECU Ova vrijednost upozorava poslužitelja (VU) da dijagnostički uređaj više ne upravlja linijom kalibracije U/I signala.	RCTECU
01	ResetToDefault Ova vrijednost upozorava poslužitelja (VU) da se od njega zahtijeva povrat linije kalibracije U/I signala u standardno stanje.	RTD
03	ShortTermAdjustment Ova vrijednost upozorava poslužitelja (VU) da se od njega traži podešavanje linije kalibracije U/I signala sa vrijednošću obuhvaćenom parametrom controlState.	STA

CPR_065 Parametar controlState je prisutan samo kada je inputOutputControlParameter postavljen na ShortTermAdjustment i određen je u sljedećoj tablici:

Tablica 37.

Određivanje vrijednosti controlState

Način rada	Heksadecimalna vrijednost	Opis
Stavi izvan pogona	00	U/I linija je izvan pogona (standardno stanje)
Stavi u pogon	01	Stavlja u pogon U/I liniju kalibracije kao speedSignalInput
Stavi u pogon	02	Stavlja u pogon U/I liniju kalibracije kao TimeSpeedSignalOutputSensor
Stavi u pogon	03	Stavlja u pogon U/I liniju kalibracije kao RTCOutput

8. FORMATI DATARECORDS

Ova točka opisuje:

— opća pravila koja se moraju primijeniti na raspon parametara koje jedinica u vozilu prenosi dijagnostičkom uređaju,

— formate koji se moraju koristiti za podatke koji se prenose putem servisa prijenosa podataka opisanih u odjeljku 6.

CPR_067 jedinica vozila mora podržavati sve utvrđene parametre.

CPR_068 Podaci koje jedinica vozila prenosi dijagnostičkom uređaju kao odgovor na poruku zahtjeva moraju biti izmjereni podaci (tj. tekuća vrijednost traženog parametra kojega je jednica vozila izmjerila ili uočila).

8.1. **Rasponi prenesenih parametara**

CPR_069 Tablica 38. određuje raspone koja se koriste za određivanje valjanosti prenesenog parametra.

CPR_070 Vrijednosti u rasponu ‚indikator pogreške' omogućavaju jedinici u vozilu da odmah upozori da valjan parametarski podatak trenutačno nije dostupan zbog neke pogreške tahografa.

CPR_071 Vrijednosti u rasponu ‚nije dostupan' omogućavaju jedinici u vozilu da prenese poruku koja sadrži parametar koji nije dostupan ili ga taj modul ne podržava. Vrijednosti u području ‚nije traženo' omogućavaju uređaju da prenese poruku naredbe i odredi one parametre kod kojih se odziv s prijemnika ne očekuje.

CPR_072 Ako pogreška sastavnog dijela spriječi prijenos valjanog podatka za parametar, umjesto podatka za takav parametar treba koristiti indikator pogreške opisan tablici 38. Međutim, ako izmjeren ili izračunan podatak daje ispravnu vrijednost, ali premašuje definirani raspon parametra, ne smije se koristiti indikator pogreške. Podatke treba prenositi upotrebljavajući odgovarajuće najmanje ili najveće vrijednosti parametra.

Tablica 38.

Rasponi dataRecords

Naziv raspona	1 bajt (heksadecimalna vrijednost)	2 bajta (heksadecimalna vrijednost)	4 bajta (heksadecimalna vrijednost)	ASCII
Ispravni signal	00 do FA	0000 do FAFF	00000000 do FAFFFFFF	1 do 254
Specifičan indikator parametra	FB	FB00 do FBFF	FB000000 do FBFFFFFF	niti jedan
Rezervirani rasponi za buduće bitove indikatora	FC do FD	FC00 do FDFF	FC000000 do FDFFFFFF	niti jedan
Indikator pogreške	FE	FE00 do FEFF	FE000000 do FEFFFFFF	0
Nije raspoloživ ili zatražen	FF	FF00 do FFFF	FF000000 do FFFFFFFF	FF

CPR_073 Za parametre šifrirane u ASCII, ASCII znak ‚*' je rezerviran kao razdjelnik.

8.2. **Formati dataRecords**

Dolje navedene tablice 39. do 42. detaljno prikazuju formate koji se moraju koristiti putem servisa ReadDataByIdentifier i WriteDataByIdentifier.

CPR_074 Tablica 39. daje duljinu, razlučivost i radno područje za svaki parametar koji je identificirao recordDataIdentifier:

Tablica 39.

Format dataRecords

Naziv parametra	Duljina podatka (u bajtovima)	Razlučivost	Radno područje
TimeDate	8	(Vidjeti pojedinosti u tablici 40.)	
HighResolutionTotalVehicleDistance	4	uvećanje 5 m/bit, pomak 0 m	0 do + 21 055 406 km
Kfactor	2	uvećanje 0,001 impulsa/m/bit, pomak 0	0 do 6,255 impulsa/m
LfactorTyreCircumference	2	uvećanje 0,125 10^{-3}/bit, pomak 0	0 do 8,031 m
WvehicleCharacteristicFactor	2	uvećanje 0,001 impulsa/m/bit, pomak 0	0 do 64,255 impulsa/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	(Vidjeti pojedinosti u tabeli 41.)	
SpeedAuthorised	2	uvećanje 1/256 km/h/bit, pomak 0	0 do 250, 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	(Vidjeti pojedinosti u tabeli 42.)	
VIN	17	ASCII	ASCII

CPR_075 Tablica 40. opisuje formate različitih bajtova parametra TimeDate:

Tablica 40.

Podrobni format TimeDate (vrijednost recordDataIdentifier # F00B)

Bajt	Određivanje parametra	Razlučivost	Radno područje
1	Sekunde	uvećanje 0,25 s/bit, pomak 0 s	0 do 59,75 s
2	Minute	uvećanje 1 min/bit, pomak 0 min	0 do 59 min
3	Sati	uvećanje 1 h/bit, pomak 0 h	0 do 23 h
4	Mjesec	uvećanje 1 mjesec/bit, pomak 0 mjeseci	mjesec 1 do 12
5	Dan	uvećanje 0,25 dana/bit, pomak 0 dana (vidjeti napomenu ispod tabele 41.)	0,25 do 31,75 dana
6	Godina	uvećanje 1 godina/bit, pomak + 1985 godina (vidjeti napomenu ispod tabele 41.)	godina 1985. do 2235.
7	Lokalni pomak minuta	uvećanje 1 min/bit, pomak -125 min	-59 do 59 min
8	Lokalni pomak sati	uvećanje 1 h/bit, pomak -125 h	-23 do + 23 h

CPR_076 Tablica 41. detaljno opisuje formate različitih bajtova parametra NextCalibrationDate:

Tablica 41.

Podroban format NextCalibrationDate (vrijednost recordDataIdentifier # F022)

Bajt	Određivanje parametra	Razlučivost	Radno područje
1	Mjesec	uvećanje 1 mjesec/bit, pomak 0 mjeseci	mjesec 1 do 12
2	Dan	uvećanje 0,25 dana/bit, pomak 0 dana (vidjeti donju napomenu)	0,25 do 31,75 dana
3	Godina	uvećanje 1 godina/bit, +1985 godina (vidjeti donju napomenu)	godina 1985 do 2235

Napomena u vezi s korištenja parametra ‚Dan':
1. Vrijednost 0 u datumu je prazna vrijednost. Vrijednosti 1, 2, 3 i 4 se koriste za označivanje prvog dana u mjesecu; 5, 6, 7 i 8 određuju drugi dan u mjesecu itd.
2. Ovaj parametar ne utječe niti mijenja gornji parametar sati.

Napomena u vezi korištenja bajta parametra ‚Godina':
Vrijednost 0 za godinu određuje 1985. godinu; vrijednost 1 određuje 1986.; itd.

CPR_078 Tablica 42. opisuje formate različitih bajtova parametra VehicleRegistrationNumber:

Tablica 42.

Podroban format parametra VehicleRegistrationNumber (vrijednost recordDataIdentifier # F07E)

Bajt	Označivanje parametra	Razlučivost	Radno područje
1	Kodna stranica (određena u Dodatku 1.)	ASCII	01 do 0A
2 do 14	Registarska oznaka vozila (određena u Dodatku 1.)	ASCII	ASCII

Dodatak 9.

TIPNO ODOBRENJE – POPIS NAJMANJEG OBIMA OBVEZNIH ISPITIVANJA

SADRŽAJ

1. UVOD

1.1. **Tipno odobrenje**

EEZ tipno odobrenje tahografa (ili njegov dio) ili karticu tahografa se temelji na:

— atestiranju sigurnosti koje provodi ITSEC vlast, u donosu na sigurnosni cilj koji u potpunosti udovoljava Dodatku 10. ovom Prilogu,

— potvrđivanje funkcionalnosti koje provodi tijelo države članice koje potvrđuje da ispitivani predmet udovoljava zahtjevima ovog Priloga u smislu izvršenih funkcija, točnosti mjerenja i obilježja okruženja,

— potvrđivanje interoperabilnosti koju obavlja nadležno tijelo koje potvrđuje da je tahograf (ili kartica tahografa) u cijelosti interoperabilan/interoperabilna sa zahtijevanim modelom kartice tahografa (ili tahografa) (vidjeti poglavlje VIII. ovog Priloga).

Ovaj Dodatak propisuje najmanji obim ispitivanja koji tijelo države članice mora obaviti tijekom funkcionalnih ispitivanja, te koji najmanji obim ispitivanja mora obaviti nadležno tijelo tijekom ispitivanja interoperabilnosti. Postupci koji se provode za obavljanje ispitivanja ili vrsta ispitivanja nisu podrobnije propisani.

Ovaj Dodatak ne obuhvaća ispitivanje značajki sigurnosti. Ako se neka ispitivanja neophodna za tipno odobrenje obavljaju tijekom procjene sigurnosti i postupka ispitivanja, tada takva ispitivanja ne treba ponavljati. U tom slučaju mogu se kontrolirati samo rezultati takvih sigurnosnih ispitivanja. Za informaciju, zahtjevi koje treba ispitati tijekom ispitivanja sigurnosti (ili koji su blisko povezani sa ispitivanjima koje treba obaviti) su u ovom Dodatku označeni sa ‚*'.

Ovaj Dodatak razmatra odvojeno tipno odobrenje senzora kretanja i jedinice u vozilu, kao sastavne dijelove tahografa. Interoperabilnost svakog modela senzora kretanja i svakog modela jedinice u vozilu nije obveza, stoga se tipno odobrenje za senzor kretanja može izdati samo u kombinaciji s tipnim odobrenje za jedinicu u vozilu i obrnuto.

1.2. **Literatura**

U ovom su Dodatku korišteni sljedeći izvori:

IEC 68-2-1 Ispitivanje u odnosu na okruženje - Dio 2.: Ispitivanja – Ispitivanje A: Hladno. 1990 + Izmjena 2.: 1994.

IEC 68-2-2 Ispitivanje u odnosu na okruženje - Dio 2.: Ispitivanja - Ispitivanje B: Suho i toplo. 1974 + Izmjena 2.: 1994.

IEC 68-2-6 Osnovni postupci ispitivanja u odnosu na okruženje – Metode ispitivanja – Fc ispitivanje i smjernice: Vibracije (sinusoidalne). 6. izdanje: 1985.

IEC 68-2-14 Osnovni postupci ispitivanja u odnosu na okruženje – Metode ispitivanja – N ispitivanje: Promjena temperature. Izmjena 1.: 1986.

IEC 68-2-27 Osnovni postupci ispitivanja u odnosu na okruženje – Metode ispitivanja – Ea ispitivanje i smjernice: Udaranje. 3. izdanje: 1987.

IEC 68-2-30 Osnovni postupci ispitivanja u odnosu na okruženje – Metode ispitivanja – Db ispitivanje i smjernice: Vlažno toplinsko, ciklično ispitivanje (12 + 12 – satni ciklus). Izmjena 1.: 1985.

IEC 68-2-35 Osnovni postupak ispitivanja u odnosu na okruženje – Metode ispitivanja – Fda ispitivanje: Nasumične vibracije širokog pojasa visoke ponovljivosti. Izmjena 1.: 1983.

IEC 529 Stupnjevi zaštite koje osiguravaju kućišta (pravilnik IP). 2. izdanje: 1989.

IEC 61000-4-2 Elektromagnetna kompatibilnost (EMC) – Postupci ispitivanja i mjerenja – Ispitivanje otpornosti na elektrostatsko pražnjenje: 1995./Izmjena 1.:1998.

ISO 7637-1 Cestovna vozila – Elektro smetnje zbog provođenja i spajanja – Dio 1.: Putnička vozila i laka gospodarska vozila nazivnog napona napajanja12 V – Prijelazna električna provodljivost u vodovima napajanja. 2. izdanje: 1990.

ISO 7637-2 Cestovna vozila – Elektro smetnje zbog provođenja i spajanja – Dio 2.: Gospodarska vozila nazivnog napona napajanja 24 V – Prijelazna električna provodljivost u vodovima napajanja. Prvo izdanje: 1990.

ISO 7637-3 Cestovna vozila – Elektro smetnje zbog provođenja i spajanja – Dio 3.: Vozila s naponom napajanja 12V ili 24 V – Prijelazni elektro prijenos s kapacitivnim i induktivnim spojevima putem vodića koji nisu vodovi napajanja. Prvo izdanje: 1995. + ispravak 1.: 1995.

ISO/IEC 7816-1 Identifikacijske kartice – Kontaktne kartice s integriranim krugom/krugovima – Dio 1.: Fizička obilježja. Prvo izdanje: 1998.

ISO/IEC 7816-2 Informacijska tehnologija - Identifikacijske kartice – Kontaktne kartice s integriranim krugom/krugovima – Dio 2.: Dimenzije i mjesto kontakata. Prvo izdanje: 1999.

ISO/IEC 7816-3 Informacijska tehnologija - Identifikacijske kartice – Kontaktne kartice s integriranim krugom/krugovima – Dio 3.: Elektronski signali i protokol prijenosa. 2. izdanje: 1997.

ISO/IEC 10373 Identifikacijske kartice – Metode ispitivanja. Prvo izdanje: 1993.

2. FUNKCIONALNA ISPITIVANJA JEDINICE U VOZILU

Br.	Ispitivanje	Opis	Predmetni zahtjevi
1.	**Administrativni pregled**		
1.1.	Dokumentacija	Ispravnost dokumentacije	
1.2.	Rezultati ispitivanja proizvođača	Rezultati ispitivanja proizvođača obavljenih tijekom sklapanja. Dokumentacijski iskazi	070,071,073
2.	**Vizualni pregled**		
2.1.	Sukladnost s dokumentacijom		
2.2.	Identifikacija/oznake		168, 169
2.3.	Materijali		163 do 167
2.4.	Pečaćenje		251
2.5.	Vanjska sučelja		
3.	**Funkcionalna ispitivanja**		
3.1.	Predviđene funkcije		002, 004, 244
3.2.	Načini rada		006*, 007*, 008*, 009*, 106, 107
3.3.	Funkcije i prava na pristup podacima		010*, 01l*, 240, 246, 247
3.4.	Praćenje umetanja i vađenja kartica		013, 014, 015*, 016*, 106
3.5.	Mjerenje brzine i udaljenosti		017 do 026
3.6.	Mjerenje vremena (pokus se obavlja na 20 °C)		027 do 032
3.7.	Praćenje aktivnosti vozača		033 do 043, 106
3.8.	Praćenje statusa vožnje		044, 045, 106
3.9.	Ručni unos		046 do 050b
3.10.	Upravljanje zaključavanjem podataka tvrtke		051 do 055
3.11.	Praćenje djelatnosti nadzora		056,057
3.12.	Otkrivanje događaja i/ili pogrešaka		059 do 069, 106

Br.	Ispitivanje	Opis	Predmetni zahtjevi
3.13.	Identifikacijski podaci o uređaju		075*, 076*, 079
3.14.	Podaci o umetanju i vađenju vozačke kartice		081* do 083*
3.15.	Podaci o aktivnostima vozača		084* do 086*
3.16.	Podaci o mjestima		087* do 089*
3.17.	Podaci o brojaču kilometara		090* do 092*
3.18.	Podrobni podaci o brzini		093*
3.19.	Podaci o događajima		094*, 095
3.20.	Podaci o pogreškama		096*
3.21.	Podaci o kalibraciji		097*, 098*
3.22.	Podaci o podešavanju vremena		100*, 101*
3.23.	Podaci o nadzornim aktivnostima		102*, 103*
3.24.	Podaci o zaključavanju podataka tvrtke		104*
3.25.	Podaci o aktivnosti preuzimanja podataka		105*
3.26.	Podaci o posebnim uvjetima		105a*, 105b*
3.27.	Zapisivanje i čuvanje na karticama tahografa		108, 109*, 109a*, 110*, 111, 112
3.28.	Prikaz		072, 106, 113 do 128, PIC_001, DIS_001
3.29.	Ispis		072, 106, 129 do 138, PIC_001, PRT_001 do PRT_012
3.30.	Upozorenje		106, 139 do 148, PIC_001
3.31.	Preuzimanje podataka na vanjski uređaj		072, 106, 149 do 151
3.32.	Izlaz podataka na dodatne vanjske uređaje		152, 153
3.33.	Kalibracija		154*, 155*, 156*, 245
3.34.	Podešavanje vremena		157*, 158*
3.35.	Neometanje dodatnih funkcija		003, 269

Br.	Ispitivanje	Opis	Predmetni zahtjevi
4.	**Ispitivanja u odnosu na okolinu**		
4.1.	Temperatura	Provjerava funkcionalnost putem: — IEC 68-2-1, Ad ispitavanje, trajanje testa 72 sata pri niskoj temperaturi (- 20 °C), 1 h u radu, 1 h izvan rada, — IEC 68-2-2, Bd ispistivanje, trajanje testa 72 sata pri visokoj temperaturi (+ 70 °C), 1 h u radu, 1 h izvan rada, Temperaturni ciklusi: provjeravanje može li jedinica u vozilu izdržati brze promjene temperature okoline putem Na ispitivanja IEC 68-2-14, 20 ciklusa, svaki s temperaturom koja se kreće od niske temperature (- 20 °C) do visoke temperature (+ 70 °C) i 2 sata držanja na niskoj i na visokoj temperaturi Može se obaviti skraćena serija ispitivanja (između onih propisanih u točki 3. ove tablice) pri niskoj temperaturi, viskoj temperaturi i tijekom temperaturnih ciklusa.	159
4.2.	Vlaga	Provjerava može li jedinica u vozilu izdržati cikličnu vlažnost (toplo ispitivanje) putem IEC 68-2-30, pokus Db, šest ciklusa u trajanju od 24 sata, pri svakom primjena temperature od + 25 °C do + 55 °C i relativna vlažnost od 97 % pri + 25 °C i od 93 % pri + 55 °C	160
4.3.	Vibracije	1. Sinusoidalne vibracije: provjerava može li jedinica u vozilu izdržati sinusoidalne vibracije sa sljedećim obilježjima: konstantan pomak između 5 i 11 Hz: vršna amplituda 10 mm konstantno ubrzanje između 11 i 300 Hz: 5 g Ovaj zahtjev se provjerava putem IEC 68-2-6, Fc ispitivanje, uz minimalno trajanje ispitivanja od 3 × 12 sati (12 sati po osi) 2. Nasumične vibracije: provjerava se može li jedinica u vozilu izdržati nasumične vibracije sa sljedećim obilježjima: frekvencija 5-150 Hz, razina 0,02 g^2/Hz Ovaj zahtjev se provjerava putem IEC 68-2-35, Ffda ispitivanje, uz minimalno trajanje ispitivanja od 3 × 12 sati (12 sati po osi), 1 sat u radu, 1 sat izvan rada Dva gore opisana ispitivanja se obavljaju na dva različita uzorka tipa uređaja koji se ispituje	163
4.4.	Zaštita od vode i stranih tijela	Provjerava je li indeks zaštite jedinice u vozilu sukladan IEC 529 i iznosi najmanje IP 40, kada je ugrađena u radnom stanju na vozilo	164, 165
4.5.	Prednaponska zaštita	Provjerava može li jedinica u vozilu izdržati snagu napajanja od: izvedbe od 24V: 34 V pri + 40 °C 1 sat izvedbe od 12V: 17 V pri + 40 °C 1 sat	161
4.6.	Zaštita od zamjene polariteta	Provjerava može li jedinica u vozilu izdržati inverziju svojeg napajanja.	161

Br.	Ispitivanje	Opis	Predmetni zahtjevi
4.7.	Zaštita od kratkog spoja	Provjerava jesu li signali ulaza i izlaza zaštićeni od kratkog spoja u odnosu na napajanje i uzemljenje	161
5.	**EMC ispitivanja**		
5.1.	Emitiranje zračenja i osjetljivost	Sukladnost s Direktivom 95/54/EEZ	162
5.2.	Elektrostatičko pražnjenje	Sukladnost s IEC 61000-4-2, ± 2 kV (razina 1)	162
5.3.	Provođenje prijelazne osjetljivosti pri napajanju	Za izvedbu od 24V: sukladnost s ISO 7637-2: puls 1a: Vs = - 100 V, Ri = 10 ohm puls 2: Vs = + 100 V, Ri = 10 ohm puls 3a: Vs = - 100 V, Ri = 50 ohm puls 3b: Vs = + 100 V, Ri = 50 ohm puls 4: Vs = - 16 V, Va = - 12 V, t6 = 100 ms puls 5: Vs = + 120 V, Ri = 2,2 ohm, td = 250 ms Za izvedbu 12V: sukladnost s ISO 7637-1: puls 1: Vs = - 100 V, Ri = 10 ohm puls 2: Vs = + 100 V, Ri = 10 ohm puls 3a: Vs = - 100 V, Ri = 50 ohm puls 3b: Vs = + 100 V, Ri = 50 ohm puls 4: Vs = - 6 V, Va = - 5 V, t6 = 15 ms puls 5: Vs = + 65 V, Ri = 3 Ohm, td = 100 ms Puls 5 se ispituje samo za jedinice u vozilima namijenjenima ugradnji na vozila na kojima se ne provodi jedinstvena vanjska zaštita od rasterećenja	162

3. FUNKCIONALNA ISPITIVANJA SENZORA KRETANJA

Br.	Pokus	Opis	Predmetni zahtjevi
1.	**Administrativni pregled**		
1.1.	Dokumentacija	Pravilnost dokumentacije	
2.	**Vizualni pregled**		
2.1.	Sukladnost s dokumentacijom		
2.2.	Identifikacija/oznake		169, 170
2.3.	Materijali		163 do 167
2.4.	Pečaćenje		251
3.	**Funkcionalni pokusi**		
3.1.	Identifikacijski podaci za senzor		077*
3.2.	Senzor kretanja – uparivanje jedinice u vozilu		099*, 155
3.3.	Detektiranje kretanja		
	Točnost mjerenja kretanja		022 do 026

Br.	Pokus	Opis	Predmetni zahtjevi
4.	**Ispitivanja u odnosu na okolinu**		
4.1.	Radna temperatura	Provjerava se funkcionalnost (određeno u ispitivanju br. 3.3.) u temperaturnom intrevalu [- 40 °C; + 135 °C] prema: — IEC 68-2-1, Ad ispitivanje, trajanje ispitivanja 96 sati pri najnižoj temperaturi To_{min} — IEC 68-2-2, Bd ispitivanje, trajanje ispitivanja 96 sati pri najvišoj temperaturi To_{max}	159
4.2.	Temperaturni ciklusi:	Provjerava se funkcionalnost (određeno u ispitivanje br. 3.3.) prema IEC 68-2-14 Na ispitivanje, 20 ciklusa, svaki s temperaturnom koja se izmjenjuje od najniže temperature (- 40 °C) do najviše temperature (+ 135 °C) i 2 sata održavanja na najnižoj i na najvišoj temperaturi Može se provesti skraćena serija ispitivanja (među onima koji su određeni u ispitivanju 3.3.) na najnižoj temperaturi, najvišoj temperaturi i tijekom temperaturnih ciklusa	159
4.3.	Ciklusi vlažnosti	Provjerava se funkcionalnost (određeno u ispitivanju br. 3.3.) putem IEC 68-2-30, Db ispitivanje, šest 24-satnih ciklusa, svaka temperatura se mijenja od + 25 °C do + 55 °C, relativna vlažnost od 97 % pri + 25 °C i od 93 % pri + 55 °C	160
4.4.	Vibracije	Provjerava se funkcionalnost (određeno u ispitivanju br. 3.3.) putem IEC 68-2-6, Fc ispitivanje, s trajanjem ispitivanja od 100 ciklusa frekvencije: konstantan pomak između 10 i 57 Hz: 1,5 mm amplituda vršno konstantno ubrzanje između 57 i 500 Hz: 20 g	163
4.5.	Mehanički udar	Provjerava se funkcionalnost (određeno u ispitivanju br. 3.3.) putem IEC 68-2-27 Ea ispitivanje, 3 udarca u oba smjera 3 okomite osi	163
4.6.	Zaštita od vode i stranih tijela	Provjerava se iznosi li pokazatelj zaštite senzora kretanja prema IEC 529 najmanje IP 64, kada je ugrađen u radnom stanju na vozilo	165
4.7.	Zaštita od zamjene polariteta	Provjerava se može li senzor kretanja izdržati inverziju svog energetskog napajanja	161
4.8.	Zaštita od kratkog spoja	Provjerava se jesu li signali ulaza i izlaza zaštićeni od kratkog spoja u odnosu na napajanje i uzemljenje	161
5.	**EMC**		
5.1.	Emitiranje zračenja i osjetljivost	Provjerava sukladnosti s Direktivom 95/54/EEZ	162
5.2.	Elektrostatičko pražnjenje	Sukladnost s IEC 61000-4-2, ± 2 kV (razina 1)	162
5.3.	Provedena prijelazna osjetljivosti na vodićima napajanja	Sukladnost s ISO 7637-3 (razina III)	162

4. FUNKCIONALNA ISPITIVANJA KARTICA TAHOGRAFA

Br.	Pokus	Opis	Predmetni zahtjevi
1.	**Administrativni pregled**		
1.1.	Dokumentacija	Pravilnost dokumentacije	
2.	**Vizualni pregled**		
2.1.		Osigurava da su sva obilježja zaštite i vidljivi podaci ispravno tiskani na kartici i da su sukladni	171 do 181
3.	**Fizičko ispitivanje**		
3.1.		Provjerava se dimenzija kartice i položaj kontakata	184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	**Ispitivanje protokola**		
4.1.	ATR	Provjerava se sukladnost ATR	ISO/IEC 7816-3 TCS 304, 307, 308
4.2.	T = 0	Provjerava se sukladnost protokola T = 0	ISO/IEC 7816-3 TCS 302, 303, 305
4.3.	PTS	Provjerava se sukladnost PTS naredbe postavljanjem na T = 1 sa T = 0	ISO/IEC 7816-3 TCS 309 do 311
4.4.	T = l	Provjerava se sukladnost protokola T = 1	ISO/IEC 7816-3 TCS 303,/306
5.	**Struktura kartice**		
5.1.		Ispituje se je li podatkovna struktura kartice sukladna provjerom prisustva obveznih datoteka na kartici i uvjeta pristupanju istima	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	**Funkcionalna ispitivanja**		
6.1.	Normalna obrada	Ispituje se najmanje jednom svaka dopuštena upotreba naredbe (npr. ispitati naredbu UPTDATE BINARY sa CLA = ‚00', CLA = OC' i s različitim parametrima P1, P2 i Lc) Provjerava se na kartici jesu li radnje stvarno obavljene (npr.: čitanjem datoteke na kojoj je izvedena naredba)	TCS 313 do TCS 379
6.2.	Poruke pogreške	Ispituje se najmanje jednom svaka poruka pogreške (kako je definirano u Dodatku 2.) za svaku naredbu Ispituje se najmanje jednom svaka generička pogreška (osim pogrešaka cjelovitosti ‚6400' koje su provjerene tijekom ispitivanja sigurnosti)	
7.	**Ispitivanja u odnosu na okoliš**		
7.1.		Osigurava se da kartice rade unutar graničnih uvjeta koju su određeni sukladno ISO/IEC 10373.	185 do 188 ISO/IEC 7816-1

5. ISPITIVANJA INTEROPERABILNOSTI

Br.	Pokus	Opis
1.	Uzajamna autentifikacija	Provjerava se odvija li se uzajamna autentifikacija između jedinice u vozilu i kartice tahografa normalno
2.	Ispitivanje upisivanja/očitavanja	Izvodi se scenarij tipičnog rada jedinice u vozilu. Scenarij mora biti prilagođen vrsti kartice koja se ispituje i obuhvaća upisivanje u čim je moguće više EF na kartici. Provjera se vrši preuzimanjem podataka s kartice i provjerom da su svi odgovarajući zapisi obavljeni pravilno Provjerava se dnevni ispis kartice i mogu li svi odgovarajući zapisi biti pravilno očitani

Dodatak 10.

GENERIČKI SIGURNOSNI CILJEVI

Ovaj Dodatak propisuje najmanji obvezan sadržaj sigurnosnih ciljeva senzora kretanja, jedinice u vozilu i kartice tahografa.

Kako bi definirali sigurnosne ciljeve u odnosu na koje mogu zatražiti certifikate sigurnosti, proizvođači moraju prema potrebi dopuniti i popuniti dokumente, bez izmjena ili brisanja postojećih opasnosti, ciljeva, načina postupanja i propisanih funkcija za provodbu sigurnosti.

SADRŽAJ

Generički sigurnosni cilj senzora kretanja

Generički sigurnosni cilj jedinice u vozilu

Generički sigurnosni cilj kartice tahografa

GENERIČKI SIGURNOSNI CILJ SENZORA KRETANJA

1. **Uvod**

Ovaj dokument sadrži opis senzora kretanja, opasnosti koje mora prevladati i sigurnosnih ciljeva koje mora postići, propisuje tražene funkcije provedbe sigurnosti, te navodi zahtijevanu najmanju otpornost sigurnosnih mehanizama i zahtijevanu razinu sigurnosti za razvoj i ocjenu.

Zahtjevi iz ovog dokumenta su oni iz teksta Priloga I.B. U pogledu jasnoće čitanja ponekad dolazi do ponavljanja zahtjeva u tekstu Priloga I.B i zahtjeva u vezi sigurnosnih ciljeva. Ako postoje dvojbe između zahtjeva u vezi sigurnosnog cilja i zahtjeva iz teksta Priloga I.B na koji se poziva navedeni zahtjev u vezi sigurnosnog cilja, vrijedi zahtjev iz teksta Priloga I.B.

Zahtjevi iz teksta Priloga I.B na koje se ne pozivaju sigurnosni ciljevi ne podliježu funkcijama provedbe sigurnosti.

Jednoznačne oznake se pripisuju opasnostima, ciljevima, načinima postupanja i SEF specifikacijama u svrhu pronalaženja dokumentacije razvoja i ocjene.

2. **Kratice, definicije i literatura**

2.1. ***Kratice***

ROM	Stalna memorija
SEF	Funkcija provedbe sigurnosti
TBD	Odredit će se
TOE	Predmet vrednovanja
VU	Jedinica u vozilu.

2.2. ***Definicije***

Digitalni tahograf	Uređaj za bilježenje
Jedinica	Naprava priključena na senzor kretanja
Podaci o kretanju	Podaci koji se razmjenjuju sa VU, koji iskazuju brzinu i prijeđenu udaljenost
Fizički odvojeni dijelovi	Fizički sastavni dijelovi senzora kretanja koji su raspoređeni u vozilu nasuprot fizičkih sastavnih dijelova koji su spojeni u kućištu senzora kretanja
Sigurnosni podaci	Posebni podaci potrebni za podržavanje funkcija provedbe sigurnosti (npr. kriptografski ključevi)
Sustav	Oprema, osoblje ili organizacije koji su na bilo koji način povezani s tahografom
Korisnik	Čovjek-korisnik senzora kretanja (kada se ne koristi u izrazu ‚korisnički podaci')
Korisnički podaci	Svi podaci, drugačiji od podatka o kretanju ili sigurnosti, koje upisuje ili sprema senzor kretanja

2.3. ***Literatura***

ITSEC Kriteriji vrednovanja sigurnosti informatičke tehnologije ITSEC 1991.

3. **Obrazloženje proizvoda**

3.1. ***Opis i način korištenja senzora kretanja***

Senzor kretanja je namijenjen ugradnji u vozila za cestovni prijevoz. Namijenjen je pružanju sigurnih podataka jedinici vozila o kretanju vozila, iskazujući brzinu i prijeđenu udaljenost vozila.

Senzor kretanja je u mehaničkom sučelju s dijelom vozila koji se kreće, a čije kretanje može predstavljati brzinu vozila i prijeđenu udaljenost. Može biti smješten u mjenjaču vozila ili u bilo kojem drugom dijelu vozila.

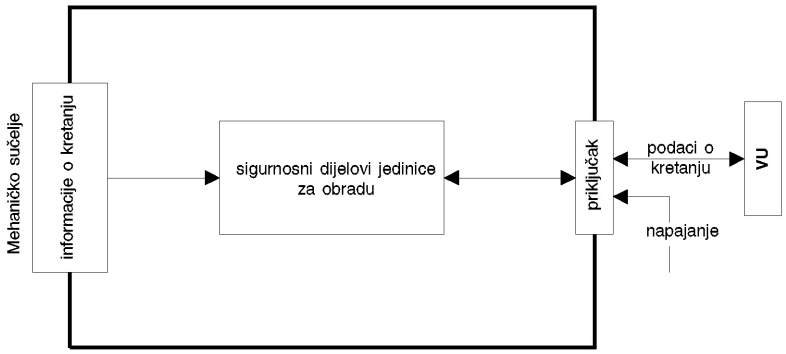
U svom radnom načinu rada, senzor kretanja je povezan s jedinicom vozila.

Također, on može biti povezan i s posebnom opremom koja služi za upravljanje (određuje proizvođač).

Sljedeća slika prikazuje tipični senzor kretanja:

Slika 1.

Tipični senzor kretanja

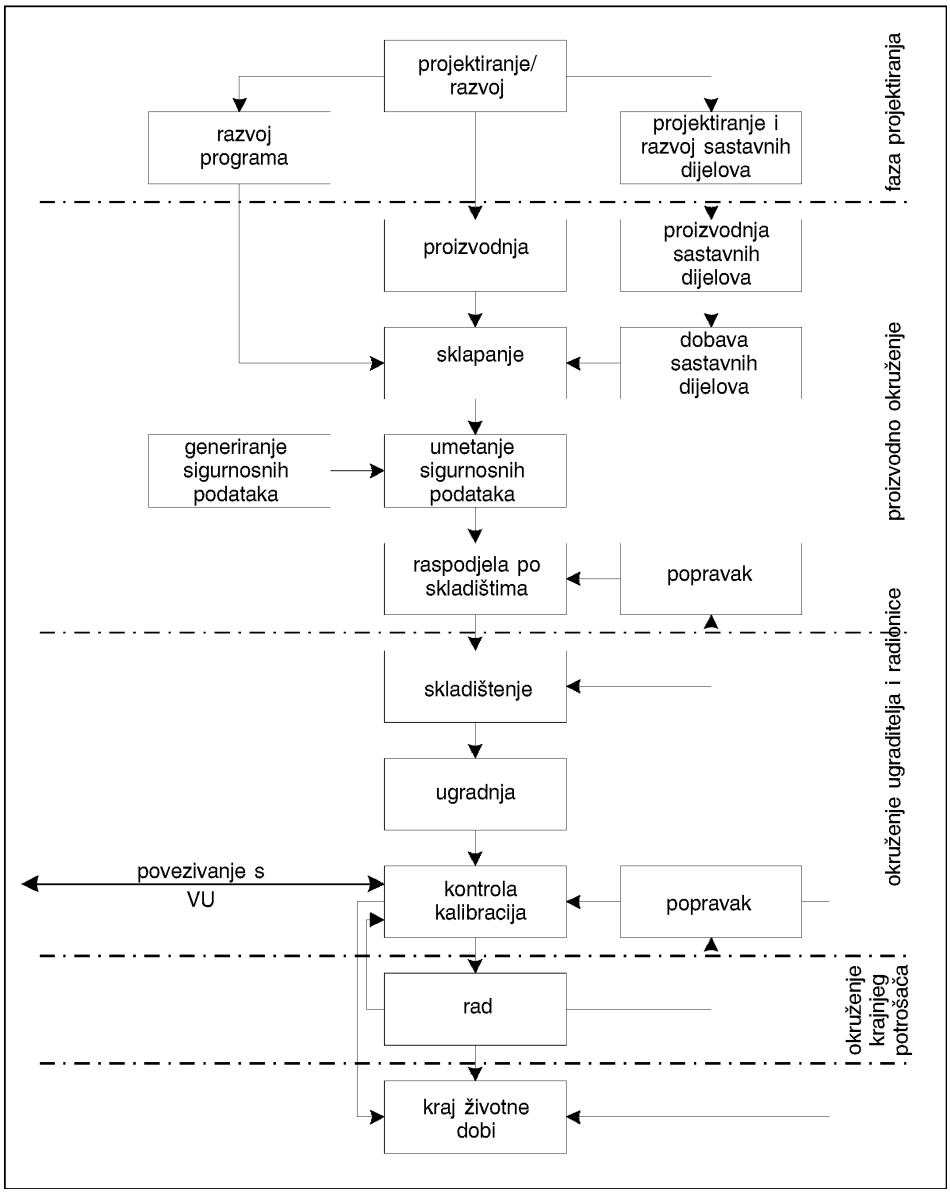


3.2. ***Životni vijek senzora kretanja***

Tipičan životni vijek senzora kretanja opisuje sljedeća slika:

Slika 2.

Tipični životni vijek senzora kretanja



3.3. ***Opasnosti***

Ovaj stavak opisuje opasnosti s kojima se može suočiti senzor kretanja.

3.3.1. *Opasnosti u odnosu na politiku upravljanja pristupom*

T.Access	Korisnici mogu pokušati pristupiti funkcijama za koje nemaju dozvolu.

3.3.2. *Opasnosti u odnosu na projektiranje*

T. Faults	Pogreške strojne opreme, programa i komunikacijskih postupaka mogu senzor kretanja dovesti u nepredviđeno stanje koje ugrožava njegovu sigurnost
T.Tests	Korištenje neprovjerenih načina ispitivanja ili postojećih ‚stražnjih ulaza' može ugroziti sigurnost senzora kretanja
T.Design	Korisnici mogu pokušati steći nezakonite spoznaje o projektu bilo iz materijala proizvođača (putem krađe, mita,…) ili putem obrnutog inženjerstva

3.3.3. *Opasnosti vezane uz rad*

T.Environment	Korisnici mogu ugroziti sigurnost senzora kretanja putem djelovanja iz neposredne okoline (toplinsko, elektromagnetsko, optičko, kemijsko, mehaničko, …)
T.Hardware	Korisnici mogu pokušati preraditi strojnu opremu senzora kretanja
T.Mechanical_Origin	Korisnici mogu pokušati utjecati na ulazne podatke osjetila kretanja (npr. odvrtanjem s mjenjača, …)
T.Motion_Data	Korisnici mogu pokušati promijeniti podatke o kretanju vozila (dodavanje, izmjena, brisanje, reprodukcija signala)
T.Power_Supply	Korisnici mogu pokušati poremetiti sigurnosne ciljeve senzora kretanja izmjenom (prekidom, smanjenjem, povećanjem) napajanja
T.Security_Data	Korisnici mogu pokušati steći nezakonito saznanje o sigurnosnim podacima u opremi tijekom generiranja sigurnosnih podataka ili prijevoza ili skladištenja
T.Software	Korisnici mogu pokušati izmijeniti program senzora kretanja
T.Stored_Data	Korisnici mogu pokušati izmijeniti spremljene podatke (sigurnosni ili korisnički podaci).

3.4. ***Sigurnosni ciljevi***

Glavni sigurnosni cilj sustava digitalnog tahografa je sljedeći:

O.Main	Podaci koje provjeravaju kontrolna tijela moraju biti dostupni i u potpunosti i točno odražavati aktivnosti vozača i vozila koji su pod nadzorom u smislu vožnje, rada, vremena pripravnosti i odmora i u smislu brzine vozila

Sigurnosni cilj senzora kretanja koji doprinosi sveukupnom sigurnosnom cilju je stoga:

O.Sensor_Main	Podaci koje prenosi senzor kretanja moraju biti dostupni VU kako bi VU omogućili da odredi potpuno i točno kretanje vozila u smislu brzine i prijeđene udaljenosti.

3.5. ***Sigurnosni ciljevi informatičke tehnologije***

Posebni sigurnosni ciljevi informatičke tehnologije za senzor kretanja koji doprinose njegovom glavnom sigurnosnom cilju su sljedeći:

O.Access	Senzor kretanja mora nadzirati pristup priključenih jedinica funkcijama i podacima
O.Audit	Senzor kretanja mora provjeravati pokušaje ugrožavanje njegove sigurnosti i treba ih proslijediti do odgovarajućih jedinica
O.Authentication	Senzor kretanja mora autentificirati priključene jedinice

O.Processing	Senzor kretanja mora osigurati da je obrada ulaznih podataka za izvođenje podataka o kretanju točna
O.Reliability	Senzor kretanja mora osigurati pouzdan servis
O.Secured_Data_Exchange	Senzor kretanja mora osiguravati razmjenu podataka s VU.

3.6. ***Fizička sredstva, osoblje ili načini postupanja***

Ovaj stavak opisuje fizičke zahtjeve, uvjete za osoblje ili načine postupanja koji doprinose sigurnosti senzora kretanja.

3.6.1. *Projektiranje opreme*

M.Development	Projektanti senzora kretanja moraju voditi računa da se dodjela odgovornosti tijekom projektiranja vrši na način koji održava sigurnost IT
M.Manufacturing	Proizvođači senzora kretanja moraju osigurati da se odgovornosti tijekom izrade dodijeli na način koji održava sigurnost IT, te da tijekom postupka izrade senzor bude zaštićen od fizičkih napada koji bi mogli ugroziti sigurnost IT.

3.6.2. *Isporuka opreme*

M.Delivery	Proizvođači senzora kretanja, proizvođači vozila i ugraditelji ili radionice moraju osigurati da se rukovanje senzorom kretanja obavlja na način koji održava sigurnost IT.

3.6.3. *Generiranje i isporuka sigurnosnih podataka*

M.Sec_Data_Generation	Algoritmi za generiranje sigurnosnih podataka moraju biti dostupni samo ovlaštenim i povjerljivim osobama
M.Sec_Data_Transport	Sigurnosni podaci moraju se dobivati, prenositi i unositi u senzor kretanja tako da se očuva njegova vlastita povjerljivost i cjelovitost.

3.6.4. *Ugradnja, kalibracija i kontrola tahografa*

M.Approved_Workshops	Ugradnju, kalibriranje i popravak tahografa mogu obavljati pouzdani i ovlašteni ugraditelji ili radionice.
M.Mechanical_Interface	Sredstva za otkrivanje neovlaštenog interveniranja u mehaničko sučelje trebaju biti osigurana (npr. pečaćenje)
M.Regular_Inpections	Tahograf se mora periodično nadzirati i kalibrirati.

3.6.5. *Nadzor nad provedbom zakona*

M.Controls	Nadzor nad provedbom zakona se mora obavljati redovito i nasumice, te mora obuhvaćati ispitivanja sigurnosti.

3.6.6. *Nadograđivanje softvera*

M.Software_Upgrade	Prije ugradnje u senzor kretanja, izmjene programa moraju biti atestirane sa stanovišta sigurnosti.

4. **Funkcije provedbe sigurnosti**

4.1. ***Identifikacija i autentifikacija***

UIA_101 Senzor kretanja mora moći utvrditi, za svaku interakciju, identitet svake jedinice na koju je bio priključen.

UIA_102 Identitet priključene jedinice se sastoji od:

— grupe jedinica:

— VU,

— dijagnostičkog uređaja,

— ostalog

— ID jedinice (samo VU).

UIA_103 ID priključene VU jedinice se sastoji od broja odobrenja VU i serijskog broja VU.

UIA_104 Senzor kretanja mora biti sposobno autentificirati svaku VU ili dijagnostički uređaj koji je priključen:

— prilikom priključenja jedinice,

— prilikom obnove napajanja.

UIA_105 Senzor kretanja mora biti sposoban za periodično ponovno autentificiranje VU na koju je priključen.

UIA_106 Senzor kretanja mora prepoznati i spriječiti korištenje podataka za autentifikaciju koji su kopirani i već upotrijebljeni.

UIA_107 Nakon utvrđivanja uzastopnih neuspješnih pokušaja autentifikacije (broj određuje proizvođač, ali ne smije biti veći od 20), SEF mora:

— generirati revizijski zapis događaja,

— upozoriti jedinicu,

— nastaviti predavati podatke o kretanju u neosiguranom načinu rada.

4.2. ***Upravljanje pristupom***

Pristupni dijagnostički uređaji osiguravaju da podaci učitani iz, stvoreni u ili promjenjeni u TOE, mogu obaviti samo oni koji su za to ovlašteni.

4.2.1. *Politika upravljanja pristupom*

ACC_101 Senzor kretanja mora upravljati pravima na pristup funkciji i podacima.

4.2.2. *Prava na pristup podacima*

ACC_102 Senzor kretanja mora osigurati da se identifikacijski podaci senzora kretanja mogu upisati samo jednom (zahtjev 078).

ACC_103 Senzor kretanja mora prihvatiti i/ili spremiti korisničke podatke samo iz autentificiranih jedinica.

ACC_104 Senzor kretanja mora provesti odgovarajuća prava pristupa čitanju i upisivanju sigurnosnih podataka.

4.2.3. *Struktura datoteke i uvjeti pristupa*

ACC_105 Struktura programa i podatkovnih datoteka te uvjeti pristupa se moraju osmisliti u postupku proizvodnje i potom blokirati u odnosu na sve buduće promjene ili brisanja.

4.3. ***Odgovornost***

ACT_101 Senzor kretanja mora u svojoj memoriji čuvati identifikacijske podatke senzora kretanja (zahtjev 077).

ACT_102 Senzor kretanja mora u svojoj memoriji čuvati ugradbene podatke (zahtjev 099).

ACT_103 Senzor kretanja mora imati mogućnost davanja podataka o odgovornosti autentificiranim jedinicama na njihov zahtjev.

4.4. ***Revizija***

AUD_101 Senzor kretanja mora, u slučajevima ugroze njegove sigurnosti, generirati revizijske zapise događaja.

AUD_102 Slučajevi koji utječu na sigurnost senzora kretanja su sljedeći:

— pokušaji narušavanja sigurnosti,

— neuspješna autentifikacija,

— pogreška cjelovitosti spremljenih podataka,

— pogreška pri unutarnjem prijenosu podataka,

— neovlašteno otvaranje kućišta,

— sabotaža strojne opreme

— hardversko manipuliranje.

AUD_103 Revizijski zapisi moraju obuhvatiti sljedeće podatke:

— datum i vrijeme događaja,

— vrsta događaja,

— identitet priključene jedinice.

Ako zahtijevani podaci nisu dostupni, daje se odgovarajući standardni znak (TBD od proizvođača).

AUD_104 Senzor kretanja mora poslati generirane revizijske zapise u VU u trenutku njihovog generiranja i može ih također spremiti u memoriju.

AUD_105 Ako senzor kretanja spremi revizijske zapise, on osigurava da se 20 revizijskih zapisa održava neovisno o veličini kapaciteta za čuvanje revizija, te mora moći isporučiti pohranjene revizijske zapise autentificiranim jedinicama na njihov zahtjev.

4.5. ***Točnost***

4.5.1. *Politika upravljanja informacijskim tokom*

ACR_101 Senzor kretanja mora osigurati da se podaci o kretanju mogu obrađivati i izvoditi samo iz mehaničkog ulaza u osjetilo.

4.5.2. *Unutarnji prijenos podataka*

Zahtjevi iz ovog stavka vrijede samo ako senzor kretanja koristi fizički odvojene dijelove.

ACR_102 Ako se podaci prenose između fizički odvojenih dijelova senzora kretanja, podaci moraju biti zaštićeni od promjena.

ACR_103 Prilikom utvrđivanja pogreške prijenosa podataka tijekom unutarnjeg prijenosa, prijenos se ponavlja i SEF mora generirati revizijski zapis o događaju.

4.5.3. *Cjelovitost pohranjenih podataka*

ACR_104 Senzor kretanja mora provjeriti korisničke podatke pohranjene u njegovoj memoriji u smislu pogrešaka cjelovitosti.

ACR_105 Po otkrivanju pogreške cjelovitosti pohranjenih korisničkih podataka, SEG mora generirati revizijski zapis.

4.6. ***Pouzdanost servisa***

4.6.1. *Ispitivanja*

RLB_101 Sve naredbe, aktivnosti ili mjesta ispitivanja karakteristična za potrebe ispitivanja u fazi proizvodnje moraju biti stavljeni izvan funkcije ili uklonjeni prije kraja faze proizvodnje. Ne smije biti moguće njihovo obnavljanje za kasniju upotrebu.

RLB_102 Senzor kretanja mora provoditi samoispitivanja tijekom početnog pogona, te tijekom redovnog rada kako bi provjerio ispravnost svog rada. Samoispitivanja senzora kretanja moraju obuhvaćati provjeru cjelovitosti sigurnosnih podataka i provjeru cjelovitosti pohranjenog izvršnog logaritma (ako nije u ROM-u).

RLB_103 Po otkrivanju unutarnje pogreške tijekom samoispitivanja, SEF mora generirati revizijski zapis (pogreška osjetila).

4.6.2. *Softver*

RLB_104 Ne smije postojati mogućnost analiziranja ili ispravljanja programa senzora kretanja na terenu.

RLB_105 Unos podataka iz vanjskih izvora se ne smije prihvatiti kao izvršni kod.

4.6.3. *Fizička zaštita*

RKB_106 Ako je senzor kretanja projektiran tako da se može otvarati, senzor kretanja mora detektirati svako otvaranje kućišta, čak i bez vanjskog napajanja u trajanju od najmanje 6 mjeseci. U tom slučaju SEF mora generirati revizijski zapis o događaju (prihvatljivo je da se revizijski zapis generira i spremi nakon ponovnog priključenja napajanja).

Ako je senzor kretanja osmišljen tako da se ne može otvoriti, projektira se tako da se pokušaji neovlaštene fizičke intervencije mogu lako utvrditi (npr. vizualnim pregledom).

RLB_107 Senzor kretanja mora detektirati određeni (određuje proizvođač) utjecaj na hardverske komponente.

RLB_108 U gore opisanom slučaju, SEF mora generirati revizijski zapis i senzor kretanja mora: (određuje proizvođač).

4.6.4. *Prekidi napajanja*

RLB_109 Senzor kretanja mora održavati sigurno stanje tijekom prekida ili kolebanja napajanja.

4.6.5. *Uvjeti povrata u početno stanje*

RLB_110 Prilikom prekida napajanja, ili ako se operacija prekine prije dovršetka, ili u nekim drugim uvjetima povrata u početno stanje, senzor kretanja se mora na pravilan način vratiti u početno stanje.

4.6.6. *Dostupnost podataka*

RLB_111 Senzor kretanja mora osigurati dobivanje pristupa izvorima podataka na zahtjev i da se izvori podataka ne traže i ne zadržavaju bez potrebe.

4.6.7. *Višestruka primjena*

RLB_112 Ako senzor kretanja osigurava primjenu podataka drukčiju od tahografske primjene, svi programi se moraju fizički i/ili logički odvojiti jedni od drugih. Ovi programi ne koriste sigurnosne podatke zajednički. Samo jedan posao smije biti aktivan u određenom trenutku.

4.7. ***Razmjena podataka***

DEX_101 Senzor kretanja mora isporučiti VU podatke o kretanju s pridruženim sigurnosnim obilježjima, kako bi VU bila u mogućnosti provjeriti njihovu cjelovitost i autentičnost.

4.8. ***Kriptografska podrška***

Zahtjevi iz ovog stavka vrijede samo prema potrebi, ovisno o korištenim sigurnosnim mehanizmima i o rješenjima proizvođača.

CSP_101 Svaka kriptografska radnja koju obavlja senzor kretanja mora biti u skladu s propisanim algoritmom i propisanom duljinom ključa.

CSP_102 Ako senzor kretanja generira kriptografske ključeve, to mora biti u skladu s propisanim algoritmima generiranja kriptografskih ključeva i propisanim veličinama kriptografskog ključa.

CSP_103 Ako senzor kretanja raspodjeljuje kriptografske ključeve, to mora biti u skladu s propisanim metodama raspodjele ključeva.

CSP_104 Ako senzor kretanja pristupi kriptografskim ključevima, to mora biti u skladu s utvrđenim metodama pristupa kriptografskim ključevima.

CSP_105 Ako senzor kretanja uništi kriptografske ključeve, to mora biti u skladu s utvrđenim metodama uništenja kriptografskih ključeva.

5. **Određivanje sigurnosnih mehanizama**

Sigurnosne mehanizme koji zadovoljavaju funkcije provedbe sigurnosti senzora kretanja određuju proizvođači senzora kretanja.

6. **Minimalna otpornost sigurnosnih mehanizama**

Minimalna otpornost sigurnosnih mehanizama senzora kretanja je ‚visoka', kako je određeno u (ITSEC).

7. **Razina sigurnosti**

Ciljna razina sigurnosti senzora kretanja je razina ITSEC E3, kako je određeno u (ITSEC).

8. **Obrazloženje**

Sljedeće matrice logički obrazlažu SEF iskazivanjem:

— koji SEF ili sredstva suzbijaju koje opasnosti,

— koji SEF ispunjavaju koje sigurnosne ciljeve IT.

	Opasnosti												Ciljevi IT					
	Dostupnost	Pogreške	Ispitivanja	Konstrukcija	Okruženje	Hardver	Mechanical_Origin	Motion_Data	Power_Supply	Security_Data	Softver	Stored_Data	Dostupnost	Revizija	Autentifikacija	Obrada	Pouzdanost	Secured_Data_Exchange
Fizička sredstva, osoblje i načini postupanja																		
Razvoj		x	x	x														
Proizvodnja			x	x														
Isporuka						x					x	x						
Generiranje sigurnosnih podataka										x								
Prijenos sigurnosnih podataka										x								
Ovlaštene radionice							x											
Mehaničko sučelje							x											
Redovna kontrola						x	x		x		x							
Nadzor nad provedbom zakona					x	x	x		x	x	x							
Nadogradnja programa											x							
Funkcije provedbe sigurnosti																		
Identifikacija i autentifikacija																		
UIA_101 Identificiranje jedinica	x							x					x		x			x
UIA_102 Identitet jedinica	x												x		x			
UIA_103 Identitet VU														x				
UIA_104 Autentifikacija jedinica	x							x					x		x			x
UIA_105 Ponovna autentifikacija	x							x					x		x			x
UIA_106 Nekrivotvoriva autentifikacija	x							x					x		x			
UIA_107 Neuspjela autentifikacija								x						x			x	
Upravljanje pristupom																		
ACC_101 Politika upravljanja pristupom	x									x		x	x					
ACC_102 ID senzora kretanja												x	x					

	Opasnosti												Ciljevi IT					
	Dostupnost	Pogreške	Ispitivanja	Konstrukcija	Okruženje	Hardver	Mechanical_Origin	Motion_Data	Power_Supply	Security_Data	Softver	Stored_Data	Dostupnost	Revizija	Autentifikacija	Obrada	Pouzdanost	Secured_Data_Exchange
ACC_103 Korisnički podaci												x	x					
ACC_104 Sigurnosni podaci										x		x	x					
ACC_105 Struktura datoteke i uvjeti pristupa	x									x		x	x					
Odgovornost																		
ACT_101 ID podaci o senzoru kretanja														x				
ACT_102 Podaci o povezivanju														x				
ACT_103 Podaci o odgovornosti														x				
Revizija																		
AUD_101 Revizijski zapisi														x				
AUD_102 Popis revizijskih događaja	x				x	x						x		x				
AUD_103 Revizijski podaci														x				
AUD_104 Revizijski alati														x				
AUD_105 Spremanje revizijskih zapisa														x				
Točnost																		
ACR_101 Politika upravljanja informacijskim tokom								x								x	x	
ACR_102 Unutarnji prijenosi																x	x	
ACR_103 Unutarnji prijenosi														x				
ACR_104 Cjelovitost spremljenih podataka												x					x	
ACR_105 Cjelovitost spremljenih podataka												x		x				
Pouzdanost																		
RLB_101 Ispitivanja u proizvodnji			x	x													x	
RLB_102 Samoispitivanja		x				x			x		x						x	
RLB_103 Samoispitivanja						x			x		x			x				
RLB_104 Analiza programa				x							x						x	
RLB_105 Instalacija programa											x					x	x	
RLB_106 Otvaranje kućišta				x	x	x				x	x	x					x	
RLB_107 Nedopuštena preinaka hardvera						x											x	
RLB_108 Nedopuštena preinaka hardvera						x								x				
RLB_109 Prekidi napajanja									x								x	
RLB_110 Povrat u početno stanje		x															x	
RLB_111 Dostupnost podataka																x	x	
RLB_112 Višestruki programi																	x	
Razmjena podataka																		
DEX_101 Isporuka sigurnosnih podataka o kretanju								x										x
Kriptografska podrška																		
CSP_101 Algoritmi																	x	x
CSP_102 Generiranje ključeva																	x	x
CSP_103 Raspodjela ključeva																	x	x
CSP_104 Dostupnost ključeva																	x	x
CSP_105 Uništenje ključeva																	x	x

GENERIČKI SIGURNOSNI CILJ JEDINICE U VOZILU

1. **Uvod**

Ovaj dokument sadrži opis jedinice u vozilu, opasnosti koje mora prevladati i sigurnosnih ciljeva koje mora postići, propisuje tražene funkcije provedbe sigurnosti, te navodi zahtijevanu najmanju otpornost sigurnosnih mehanizama i zahtijevanu razinu sigurnosti za razvoj i ocjenjivanje.

Zahtjevi iz ovog dokumenta su oni iz teksta Priloga I.B. U svrhu jasnoće čitanja ponekad dolazi do ponavljanja zahtjeva u tekstu Priloga I.B i zahtjeva u vezi sa sigurnosnim ciljevima. Ako postoje dvojbe između zahtjeva u vezi sa sigurnosnim ciljevima i zahtjeva iz Priloga I.B na koji se poziva navedeni zahtjev u vezi sa sigurnosnim ciljem, vrijedi zahtjev iz teksta Priloga I.B.

Zahtjevi iz teksta Priloga I.B na koje se ne pozivaju sigurnosni ciljevi ne podliježu funkcijama provedbe sigurnosti.

Jednoznačne oznake se pripisuju opasnostima, ciljevima, načinima postupanja i specifikacijama SEF u svrhu pronalaženja dokumentacije razrade i ocjene.

2. **Kratice, definicije i literatura**

2.1. ***Kratice***

PIN	Osobni identifikacijski broj
ROM	Stalna memorija
SEF	Funkcija provedbe sigurnosti
TBD	Odredit će se
TOE	Predmet vrednovanja
VU	Jedinica u vozilu.

2.2. ***Definicije***

Digitalni tahograf	Uređaj za bilježenje
Podaci o kretanju	Podaci koji se razmjenjuju sa senzorom kretanja, koji iskazuju brzinu i prijeđenu udaljenost
Fizički odvojeni dijelovi	Fizički sastavni dijelovi VU koji su raspoređeni u vozilu naspram fizičkih sastavnih dijelova koji su spojeni u kućištu VU
Sigurnosni podaci	Posebni podaci potrebni za podržavanje funkcija provedbe sigurnosti (npr. kriptografski ključevi)
Sustav	Oprema, osoblje ili organizacije koji su na bilo koji način povezani s tahografom
Korisnik	Korisnici su čovjek-korisnik opreme. Uobičajeni korisnici jedinice u vozilu obuhvaćaju vozače, kontrolore, radionice i tvrtke
Korisnički podaci	Svi podaci, drugačiji od sigurnosnih podataka, koje se zapisuje ili sprema u VU, prema zahtjevu u poglavlju III.12.

2.3. ***Literatura***

ITSEC	Kriteriji vrednovanja sigurnosti informatičke tehnologije ITSEC 1991.

3. **Obrazloženje proizvoda**

3.1. ***Opis jedinice u vozilu i način upotrebe***

VU je namijenjena ugradnji u vozila za cestovni prijevoz. Njezina namjena je zapisivanje, spremanje, reprodukcija, ispis i isporuka podataka koji se odnose na aktivnosti vozača.

Povezana je sa senzorom kretanja s kojim razmjenjuje podatke o kretanju vozila.

Korisnici se identificiraju u odnosu na VU korištenjem kartica tahografa.

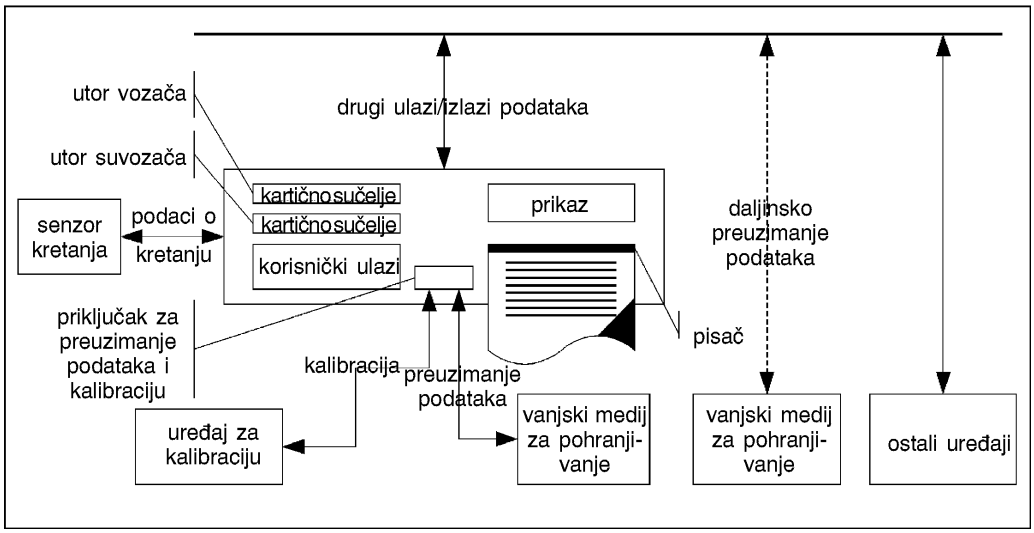
VU zapisuje i sprema podatke o aktivnosti korisnika u svoju podatkovnu memoriju, te također zapisuje podatke o aktivnosti korisnika na kartice tahografa.

VU predaje podatke na prikaz, štampač i vanjske uređaje.

Radno okruženje jedinice u vozilu kada je ugrađena u vozilo je opisana sljedećom slikom:

Slika 1.

Radno okruženje VU



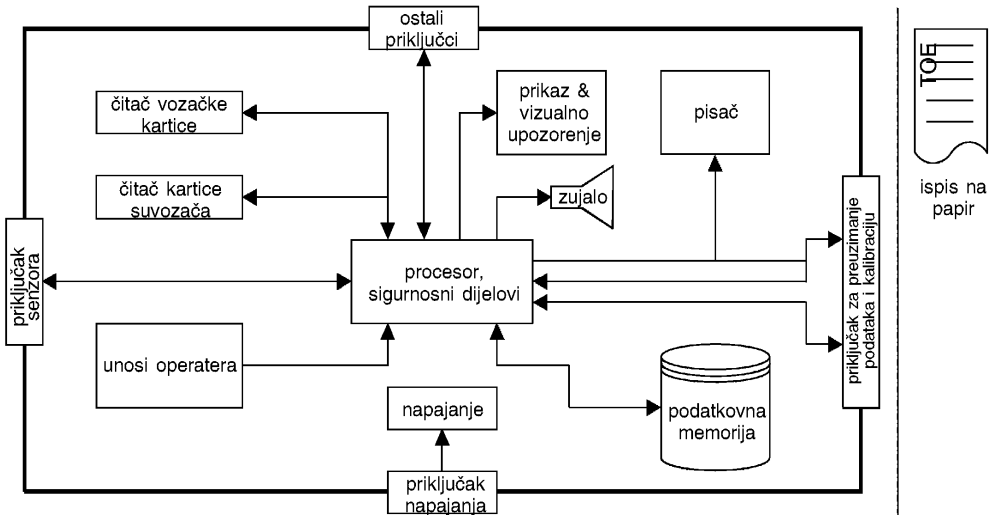
Opća obilježja VU, funkcije i načini rada su opisani u poglavlju II. Priloga I.B.

Funkcionalni zahtjevi za VU su propisani u poglavlju III. Priloga I.B.

Tipična VU je opisana na sljedećoj slici:

Slika 2.

Tipična VU […] neobavezno



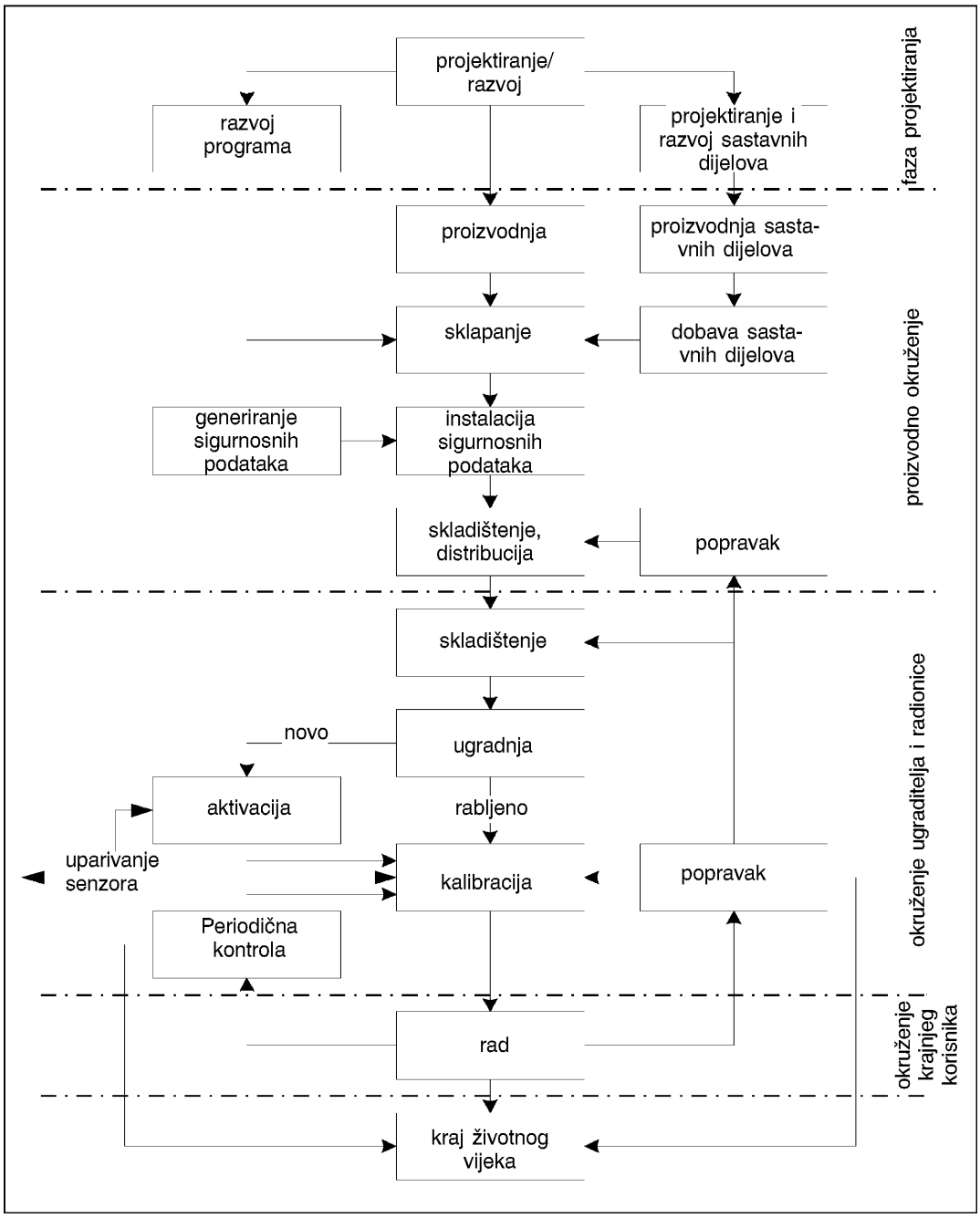
Treba naglasiti da iako je mehanizam pisača dio TOE, to nije i papirnati ispis.

3.2. ***Životni vijek jedinice u vozilu***

Tipični životni vijek VU opisuje sljedeća slika:

Slika 3.

Tipični životni vijek VU



3.3. ***Opasnosti***

Ovaj stavak opisuje opasnosti kojima je izložena VU.

3.3.1. *Opasnosti u odnosu na politiku identifikacije i upravljanja pristupom*

T.Access	Korisnici mogu pokušati pristupiti funkcijama za koje nemaju dopuštenje (npr. funkcija kolibracije dostupna vozačima)
T.Identification	Korisnici mogu pokušati koristiti nekoliko identifikacija ili nikakvu identifikaciju.

3.3.2. *Opasnosti u odnosu na projektiranje*

T.Faults	Pogreške hardvera, softvera i komunikacijskih postupaka mogu VU dovesti u nepredviđeno stanje koje ugrožava njezinu sigurnost
T.Tests	Korištenje neprovjerenih načina ispitivanja ili postojećih ‚stražnjih vrata' može ugroziti sigurnost VU
T.Design	Korisnici mogu pokušati steći nezakonite spoznaje o projektu bilo iz materijala proizvođača (putem krađe, mita,…) ili putem obrnutog inženjerstva

3.3.3. *Opasnosti vezane uz rad*

T.Calibration_Parameters	Korisnici mogu pokušati koristiti pogrešno kalibriran uređaj (putem izmjene podataka kalibracije ili organizacijskih slabosti).
T.Card_Data_Exchange	Korisnici mogu pokušati izmijeniti podatke dok se razmjenjuju između VU i kartica tahografa (dodavanje, izmjena, brisanje, reprodukcija signala)
T.Clock	Korisnici mogu pokušati učiniti izmjenu na unutarnjem satu
T.Environment	Korisnici mogu ugroziti sigurnost VU putem djelovanja iz okruženja (toplinski, elektromagnetski, optički, kemijski, mehanički, …)
T.Fake_Devices	Korisnici mogu pokušati priključiti krivotvorene uređaje na VU (senzor kretanja, pametne kartice)
T.Hardware	Korisnici mogu pokušati izmijeniti hardver VU
T.Motion_Data	Korisnici mogu pokušati izmijeniti podatke o kretanju vozila (dodavanje, izmjena, brisanje, reprodukcija signala)
T.Non_Activated	Korisnici mogu koristiti opremu koja nije aktivirana
T.Output_Data	Korisnici mogu pokušati izmijeniti isporuku podataka (ispis, prikaz ili preuzimanje podataka)
T.Power_Supply	Korisnici mogu pokušati poremetiti sigurnosne ciljeve VU izmjenom napajanja (prekid, smanjenje, povećanje)
T.Security_Data	Korisnici mogu pokušati steći nezakonito saznanje o sigurnosnim podacima tijekom generiranja podataka ili prijenosa ili instalacije u opremi
T.Software	Korisnici mogu pokušati izmijeniti softver VU
T.Stored_Data	Korisnici mogu pokušati izmijeniti spremljene podatke (sigurnosni ili korisnički podaci).

3.4. ***Sigurnosni ciljevi***

Glavni sigurnosni cilj sustava s digitalnim tahografom je sljedeći:

O.Main	Podaci koje provjeravaju kontrolna tijela moraju biti na raspolaganju i u potpunosti i točno odražavati aktivnosti vozača i vozila koji su pod nadzorom u smislu vožnje, rada, vremena pripravnosti i odmora i u smislu brzine vozila

Zato su sigurnosni ciljevi VU koji doprinose općem sigurnosnom cilju sljedeći:

O.VU_Main	Podaci koji se mjere i zapisuju i potom provjeravaju od strane kontrolnih tijela moraju biti dostupni i točno odražavati aktivnosti nadziranih vozača i vozila u smislu vožnje, rada, vremena pripravnosti i odmora i u smislu brzine vozila
O.VU_Export	VU mora biti u stanju isporučiti podatke u vanjski medij za spremanje na način koji omogućava provjeru njihove cjelovitosti i autentičnosti.

3.5. ***Sigurnosni ciljevi informatičke tehnologije***

Posebni sigurnosni ciljevi informatičke tehnologije VU koji doprinose njezinom glavnom sigurnosnom cilju su sljedeći:

O.Access	VU mora nadzirati korisnički pristup funkcijama i podacima
O.Accountability	VU mora prikupiti točne podatke u vezi odgovornosti
O.Audit	VU mora ispitati pokušaje narušavanja sigurnosti sustava i ići njihovim tragom do odgovarajućih korisnika
O.Authentication	VU mora autentificirati priključene jedinice (kada između jedinica trebaju postojati pouzdane veze)
O.Integrity	VU mora održavati cjelovitost pohranjenih podataka
O.Output	VU mora osigurati da izlazni podaci točno odražavaju izmjerene ili pohranjene podatke.
O.Processing	VU mora osigurati da obrada ulaza za izvođenje korisničkih podataka bude točna
O.Reliability	VU mora osigurati pouzdane servise
O.Secured_Data_Exchange	VU mora osiguravati razmjenu podataka sa senzorom kretanja i karticama tahografa.

3.6. ***Fizička sredstva, osoblje ili načini postupanja***

Ovaj stavak opisuje fizičke i kadrovske zahtjeve ili zahtjeve za postupak koji doprinose sigurnosti VU.

3.6.1. *Projektiranje opreme*

M.Development	Projektanti VU moraju voditi računa da se dodjela odgovornosti tijekom projektiranja vrši na način koji održava sigurnost IT
M.Manufacturing	Proizvođači VU moraju osigurati da se odgovornosti tijekom izrade dodijele na način koji održava sigurnost IT, te da tijekom postupka izrade VU bude zaštićena od fizičkih napada koji bi mogli ugroziti sigurnost IT.

3.6.2. *Isporuka opreme i stavljanje u pogon*

M.Delivery	Proizvođači VU, proizvođači vozila i radionice ili servisi moraju osigurati da se rukovanje s VU koja nije stavljena u pogon obavlja na način koji održava sigurnost IT.
M.Activation	Proizvođači vozila i ugraditelji ili radionice moraju VU staviti u pogon nakon njezine ugradnje prije nego što vozač vozila napusti poslovni prostor u kojem je izvršena ugradnja.

3.6.3. *Generiranje i isporuka sigurnosnih podataka*

M.Sec_Data_Generation	Algoritmi generiranja sigurnosnih podataka moraju biti dostupni samo ovlaštenim i pouzdanim osobama.
M.Sec_Data_Transport	Sigurnosni podaci moraju se generirati, prenositi i unositi u VU tako da se očuva njihovu povjerljivost i cjelovitost.

3.6.4. *Isporuka kartica*

M.Card_Availability	Kartice tahografa moraju biti dostupne i isporučivati se samo ovlaštenim osobama
M.Driver_Card_Uniqueness	Vozači u jednom trenutku smiju imati samo jednu valjanu vozačku karticu
M.Card_Traceability	Mora postojati mogućnost praćenja kartica (bijeli popisi, crni popisi), a crne popise se mora koristiti tijekom sigurnosnih revizija.

3.6.5. *Ugradnja, kalibracija i kontrola tahografa*

M.Approved_Workshops	Ugradnju, kalibraciju i popravak tahografa moraju obavljati pouzdani i ovlašteni ugraditelji ili radionice
M.Regular_Inpections	Tahograf se mora periodično nadzirati i kalibrirati
M.Faithful_Calibration	Ovlašteni ugraditelji i radionice moraju upisati odgovarajuće parametre vozila u tahograf tijekom kalibracije.

3.6.6. *Rad opreme*

M.Faithful_Drivers	Vozači se moraju pridržavati pravila i postupati odgovorno (npr. koristiti svoje vozačke kartice, pravilno odabrati svoju djelatnost kod ručnog odabira, …).

3.6.7. *Nadzor nad provedbom zakona*

M.Controls	Nadzor nad provedbom zakona se mora obavljati redovito i nasumice, te mora obuhvaćati ispitivanja sigurnosti.

3.6.8. *Nadogradnja programa*

M.Software_Upgrade	Prije ugradnje u VU, izmjene programa moraju biti atestirane sa stanovišta sigurnosti.

4. **Funkcije provedbe sigurnosti**

4.1. ***Identifikacija i autentifikacija***

4.1.1. *Identifikacija i autentifikacija senzora kretanja*

UIA_201 VU mora moći utvrditi, za svaku interakciju, identitet senzora kretanja na koji je priključena.

UIA_202 Identitet senzora kretanja čini broj odobrenja senzora i serijski broj senzora.

UIA_203 VU mora autentificirati senzor kretanja na koji je priključena:

— prilikom priključenja na senzor kretanja,

— prilikom svake kalibracije tahografa,

— prilikom uspostave napajanja.

Autentifikacija mora biti uzajamna i aktivirana od strane VU.

UIA_204 VU mora periodično (razdoblje određuje proizvođač i iz učestalost veću od jednom u sat vremena) ponovo identificirati i ponovo autentificirati senzor kretanja na koji je priključena i osigurati da senzor kretanja koji je identificiran tijekom posljednje kalibracije tahografa nije promijenjen.

UIA_205 VU mora ustanoviti i spriječiti korištenje podataka za autentifikaciju koji su kopirani i reproducirani.

UIA_206 Nakon što su utvrđeni uzastopni neuspješni pokušaji autentifikacije (broj određuje proizvođač, ali ne smije biti veći od 20) i/ili nakon utvrđivanja da je identitet senzora kretanja promijenjen kada to nije dopušteno (tj. izvan vremena kalibracije tahografa), SEF mora:

— generirati revizijski zapis događaja,

— upozoriti korisnika,

— nastaviti prihvaćati i koristiti neosigurane podatke o kretanju koje dostavlja senzor kretanja.

4.1.2. *Identifikacija i autentifikacija korisnika*

UIA_207 VU mora stalno i selektivno pratiti identitet dva korisnika tahografa, praćenjem umetnutih kartica tahografa u utoru vozača odnosno suvozača.

UIA_208 Identitet korisnika se sastoji od:

— skupina korisnika:

— VOZAČ (kartica vozača),

— KONTROLOR (nadzorna kartica),

— RADIONICA (kartica radionice),

— TVRTKA (kartica prijevoznika),

— NEPOZNAT (kartica nije umetnuta),

— ID korisnika koji se sastoji od:

— šifre države članice koja izdaje karticu i broja kartice,

— NEPOZNAT ako je korisnička skupina NEPOZNATA.

NEPOZNATI identiteti mogu biti poznati implicitno ili eksplicitno.

UIA_209 VU mora autentificirati svoje korisnike prilikom umetanja kartice.

UIA_210 VU mora ponovo autentificirati svoje korisnike:

— prilikom ponovne uspostave napajanja,

— periodično ili nakon nastupa posebnih događaja (određuju proizvođači i učestalije nego jednom dnevno).

UIA_211 Autentifikacija se obavlja tako da se dokaže da je umetnuta kartica valjana kartica tahografa koja posjeduje sigurnosne podatke koje je mogao samo sustav dodijeliti. Autentifikacija mora biti uzajamna i aktivirana od strane VU.

UIA_212 Pored gore navedenog, od radionice se zahtjeva da se uspješno autentificiraju putem provjere PIN-a. PIN mora imati najmanje četiri znaka.

Napomena: Kada se PIN prenosi u VU iz vanjske opreme koja se nalazi u blizini VU, pouzdanost PIN-a nije potrebno štititi tijekom prijenosa.

UIA_213 VU mora prepoznati i spriječiti korištenje autentifikacijskih podataka koji su kopirani i reproducirani.

UIA_214 Nakon otkrivanja pet uzastopnih neuspješnih pokušaja autentifikacije, SEF mora:

— generirati revizijski zapis o događaju,

— upozoriti korisnika,

— smatrati korisnika NEPOZNATIM, a karticu nevažećom (opis pod (z) i zahtjev 007).

4.1.3. *Daljinska identifikacija i autentifikacija tvrtke*

Mogućnost daljinskog priključka tvrtke je neobvezna. Ovaj stavak stoga vrijedi samo ako je takva mogućnost ugrađena.

UIA_215 Svaku interakciju s daljinski priključenom tvrtkom, VU mora moći utvrditi identitet tvrtke.

UIA_216 Daljinski priključen identitet tvrtke se sastoji od šifre države članice koja izdaje karticu tvrtke i broja njezine kartice tvrtke.

UIA_217 VU mora uspješno autentificirati daljinski priključenu tvrtku prije nego dopusti bilo kakvu isporuku podataka u istu.

UIA_218 Autentifikacija se izvodi dokazivanjem da tvrtka posjeduje valjanu karticu tvrtke koja ima sigurnosne podatke koje je samo sustav mogao dodijeliti.

UIA_219 VU mora prepoznati i spriječiti korištenje podataka za autentifikaciju koji su kopirani i reproducirani.

UIA_220 Nakon pet uzastopnih neuspješnih pokušaja autentifikacije, VU mora:

— upozoriti daljinski priključenu tvrtku.

4.1.4. *Identifikacija i autentifikacija upravljačke naprave*

Proizvođači VU mogu predvidjeti namjenske uređaje za dodatne funkcije upravljanja VU (npr. nadograđivanje programa, ponovno unošenje sigurnosnih podataka, …). Ovaj stavak stoga vrijedi samo ako je ugrađena ovakva mogućnost.

UIA_221 Za svaku interakciju s upravljačkim uređajem, VU mora moći utvrditi identitet uređaja.

UIA_222 Prije omogućavanja svake daljnje interakcije, VU mora uspješno autentificirati upravljački uređaj.

UIA_223 VU mora ustanoviti i spriječiti korištenje podataka za autentifikaciju koji su kopirani i reproducirani.

4.2. ***Upravljanje pristupom***

Upravljački uređaji za pristup osiguravaju da podatke učitavaju iz, upisuju u ili mijenjaju u TOE samo oni koji su za to ovlašteni.

Potrebno je napomenuti da korisnički podaci koje zapisuje VU, iako iskazuju privatnost ili obilježja komercijalne osjetljivosti, nisu povjerljive naravi. Stoga funkcionalni zahtjev koji se odnosi na prava pristupa učitavanju podataka (zahtjev 011) ne podliježe funkciji provedbe sigurnosti.

4.2.1. *Politika upravljanja pristupom*

ACC_201 VU mora upravljati i provjeriti prava upravljanja pristupom funkcijama i podacima.

4.2.2. *Prava pristupa funkcijama*

ACC_202 VU mora provoditi pravila izbora načina rada (zahtjevi 006 do 009).

ACC_203 VU mora koristiti način rada za provedbu pravila upravljanja pristupom funkcijama (zahtjev 010).

4.2.3. *Prava na pristup podacima*

ACC_204 VU mora provoditi pravila pristupa upisu identifikacijskih podataka VU (zahtjev 076).

ACC_205 VU mora izvršavati pravila o pristupu upisu identifikacijskih podataka uparenog senzora kretanja (zahtjevi 079 i 155).

ACC_206 Nakon aktivacije VU, VU osigurava da se podaci o kalibraciji mogu unositi u VU i pohraniti u njezinu podatkovnu memoriju (zahtjevi 154 i 156) samo u režimu kalibracije.

ACC_207 Nakon aktivacije VU, VU provodi pravila pristupa upisivanju i brisanju podataka o kalibraciji (zahtjev 097).

ACC_208 Nakon aktivacije VU, VU mora osigurati da je samo u kalibracijskom načinu rada moguć unos podataka o podešavanju vremena i spremanje u njenu podatkovnu memoriju (Ovaj zahtjev ne vrijedi za mala vremenska poravnanja omogućena zahtjevima 157 i 158).

ACC_209 Nakon aktivacije VU, VU provodi pravila pristupa upisivanju i brisanju podataka o podešavanju vremena (zahtjev 100).

ACC_210 VU mora provoditi odgovarajuća prava pristupa čitanju i brisanju sigurnosnih podataka (zahtjev 080).

4.2.4. *Struktura datoteke i uvjeti pristupa*

ACC_211 Struktura aplikacija i podatkovnih datoteka i uvjeti pristupa se moraju oblikovati tijekom proizvodnog postupka i potom blokirati u odnosu na sve buduće promjene ili brisanja.

4.3. ***Odgovornost***

ACT_201 VU mora osigurati da vozači budu odgovorni za svoje aktivnosti (zahtjevi 081, 084, 087, 105a, 105b, 109 i 109a).

ACT_202 VU mora trajno čuvati identifikacijske podatke (zahtjev 075).

ACT_203 VU mora osigurati da radionice budu odgovorne za svoje aktivnosti (zahtjevi 098, 101 i 109).

ACT_204 VU mora osigurati da kontrolori budu odgovorni za svoje aktivnosti (zahtjevi 102, 103 i 109).

ACT_205 VU mora bilježiti podatke iz brojača prijeđenih kilometara (zahtjev 090) i podrobne podatke o brzini (zahtjev 093).

ACT_206 VU mora osigurati da se korisnički podaci koji se odnose na zahtjeve 081, 093 i 102 do uključivo 105b ne mijenjaju jednom kada se upišu, osim kada postanu najstariji pohranjeni podaci koje treba zamijeniti novim podacima.

ACT_207 VU mora voditi računa da ne izmijeni podatke koji su već spremljeni na karticu tahografa (zahtjevi 109 i 109a) osim zamjene najstarijih podataka novim podacima (zahtjev 110) ili u slučaju opisanom u bilješci točke 2.1 Dodatka 1.

4.4. ***Revizija***

Mogućnosti revizije su obvezne samo za slučajeve koji mogu ukazivati na manipulaciju ili pokušaj ugrožavanja sigurnosti. Ovo se ne traži kod redovnog izvršavanja prava čak i ako se tiče sigurnosti.

AUD_201 VU mora, za događaje koji ugrožavaju sigurnost VU, zapisati takve slučajeve sa pridruženim podacima (zahtjevi 094, 096 i 109).

AUD_202 Događaji koji utječu na sigurnost VU su sljedeći:

— pokušaji ugrožavanja sigurnosti,

— neuspjela autentifikacija senzora kretanja,

— neuspjela autentifikacija kartice tahografa,

— neovlaštena promjena senzora kretanja,

— pogreška cjelovitosti unosa podataka na karticu,

— pogreška cjelovitosti pohranjenih korisničkih podataka,

— pogreška unutarnjeg prijenosa podataka,

— neovlašteno otvaranje kućišta.

— preinake hardvera,

— posljednja razmjena podataka s karticom koja nije ispravno zatvorena,

— slučaj pogreške podataka o kretanju,

— slučaj prekida napajanja,

— interna pogreška VU.

AUD_203 VU mora izvršavati pravila pohranjivanja revizijskih zapisa (zahtjev 094 i 096).

AUD_204 VU mora u svojoj memoriji pohranjivati revizijske zapise koje generira senzor kretanja.

AUD_205 Mora postojati mogućnost ispisa, prikaza i preuzimanja revizijskih zapisa.

4.5. ***Ponovno korištenje predmeta***

REU_201 VU mora osigurati da se predmeti za privremeno pohranjivanje mogu ponovo koristiti bez da to za posljedicu ima neprihvatljiv protok informacija.

4.6. ***Točnost***

4.6.1. *Politika upravljanja tokom informacija*

ACR_201 VU mora osigurati da se mogu obrađivati korisnički podaci koji se odnose na zahtjeve 081, 084, 087, 090, 093, 102, 104, 105, 105a i 109 samo iz prikladnih izvora unosa:

— podaci o kretanju vozila,

— sat VU u realnom vremenu,

— parametri kalibracije tahografa,

— kartice tahografa,

— korisnički unosi.

ACR_201a VU mora osigurati da se korisnički podaci koji se odnose na zahtjev 109a mogu unositi samo u razdoblju između posljednjeg izvlačenja kartice i trenutačog umetanja (zahtjev 050a).

4.6.2. *Unutarnji prijenos podataka*

Zahtjevi iz ovog stavka vrijede samo ako VU koristi fizički odvojene dijelove.

ACR_202 Ako se prenose podaci između fizički odvojenih dijelova VU, podaci se moraju zaštititi od izmjena.

ACR_203 Po uočavanju pogreške u prijenosu podataka tijekom unutarnjeg prijenosa, prijenos se mora ponoviti i SEF mora generirati revizijski zapis događaja.

4.6.3. *Cjelovitost pohranjenih podataka*

ACR_204 VU mora provjeriti korisničke podatke spremljene u podatkovnoj memoriji u pogledu pogrešaka cjelovitosti.

ACR_205 Po uočavanju pogreške cjelovitosti pohranjenih korisničkih podataka, SEF mora generirati revizijski zapis.

4.7. ***Pouzdanost servisa***

4.7.1. *Ispitivanja*

RLB_201 Sve naredbe, radnje ili mjesta ispitivanja koja specifična za ispitivanja u fazi izrade VU moraju biti stavljene izvan pogona ili uklonjene prije aktivacije VU. Ne smije biti moguća njihova uspostava za kasnije korištenje.

RLB_202 VU mora provesti samoispitivanja tijekom početnog puštanja u pogon i tijekom normalnog rada za provjeru ispravnosti svog rada. Samoispitivanja VU moraju obuhvaćati provjeru cjelovitosti sigurnosnih podataka i provjeru cjelovitosti pohranjenog izvršnog koda (ako nije u stalnoj memoriji).

RLB_203 Po otkrivanju unutarnje pogreške tijekom samoispitivanja, SEF mora:

— generirati revizijski zapis (osim u kalibracijskom načinu rada) (interna pogreška VU),

— očuvati cjelovitost pohranjenih podataka.

4.7.2. *Softver*

RLB_204 Ne smije biti moguće analizirati ili ispravljati pogreške programa na terenu nakon aktivacije VU.

RLB_205 Ulazni podaci iz vanjskih izvora ne smiju biti prihvaćeni kao izvršni kod.

4.7.3. *Fizička zaštita*

RLB_206 Ako je VU projektirana tako da se može otvoriti, VU mora detektirati svako otvaranje kućišta, osim u kalibracijskom načinu rada, čak i bez vanjskog napajanja, u trajanju od najmanje šest mjeseci. U takvom slučaju, SEF mora generirati revizijski zapis (Prihvatljivo je da se revizijski zapis generira i pohrani nakon ponovnog priključenja napajanja).

Ako je VU projektirana tako da se ne može otvoriti, ona se projektira tako da se pokušaji neovlaštene fizičke intervencije mogu jednostavno utvrditi (npr. putem vizualnog nadzora).

RLB_207 Nakon aktivacije, VU mora ustanoviti unaprijed određenu (određuje proizvođač) hardversku izmjenu.

RLB_208 U gore opisanom slučaju, SEF mora generirati revizijski zapis i VU mora: (određuje proizvođač).

4.7.4. *Prekidi napajanja*

RLB_209 VU mora ustanoviti odstupanja od propisanih vrijednosti napajanja, uključujući prekid napajanja.

RLB_210 U gore opisanom slučaju, SEF mora:

— generirati revizijski zapis (osim u kalibracijskom načinu rada),

— očuvati sigurno stanje VU,

— održavati sigurnosne funkcije koje se odnose na sastavne dijelove ili postupke koji su još uvijek u funkciji,

— očuvati cjelovitost pohranjenih podataka.

4.7.5. *Uvjeti povrata u početno stanje*

RLB_211 Prilikom prekida napajanja, ili ako je neka aktivnost zaustavljena prije završetka, ili u bilo kojim drugim uvjetima povrata u početno stanje, VU se mora propisno vratiti u početno stanje.

4.7.6. *Dostupnost podataka*

RLB_212 VU mora osigurati da se pristup izvorima dobije kada se to zatraži i da se izvori bez potrebe ne traže i ne zadržavaju.

RLB_213 VU mora osigurati da se kartice ne mogu izvaditi prije nego se relevantni podaci ne pohrane na kartice (zahtjevi 015 i 016).

RLB_214 U gore opisanom slučaju, SEF mora generirati revizijski zapis događaja.

4.7.7. *Višestruke aplikacije*

RLB_215 Ako VU osigurava podatke i za druge aplikacije od tahografske aplikacije, sve aplikacije se moraju fizički i/ili logički odvojiti jedna od druge. Ove aplikacije međusobno ne dijele sigurnosne podatke. U određenom trenutku smije biti aktivan samo jedan posao.

4.8. ***Razmjena podataka***

Ovaj stavak se odnosi na razmjenu podataka između VU i priključenih uređaja.

4.8.1. *Razmjena podataka sa senzorom kretanja*

DEX_201 VU mora provjeriti cjelovitost i autentičnost podataka o kretanju preuzetih sa senzora kretanja.

DEX_202 Po otkrivanju pogreške cjelovitosti ili autentičnosti podataka o kretanju, SEF mora:

— generirati revizijski zapis,

— nastaviti koristiti preuzete podatke.

4.8.2. *Razmjena podataka sa karticama tahografa*

DEX_203 VU mora provjeriti cjelovitost i autentičnost podataka koji se preuzimaju s kartica tahografa.

DEX_204 Po otkrivanju pogreške cjelovitosti i autentičnosti podataka na kartici, VU mora:

— generirati revizijski zapis,

— ne koristiti podatke.

DEX_205 VU mora u pametne kartice tahografa isporučiti podatke s odgovarajućim sigurnosnim obilježjima tako da kartica može provjeriti njihovu cjelovitost i autentičnost.

4.8.3. *Razmjena podataka s vanjskim medijima za spremanje podataka (funkcija preuzimanja podataka)*

DEX_206 VU mora generirati dokaz o podrijetlu za podatke koje preuzimaju vanjski mediji.

DEX_207 VU mora osigurati mogućnost provjere dokaza o podrijetlu podataka preuzetih s primatelja.

DEX_208 VU mora predati podatke na vanjske medije za spremanje podataka s odgovarajućim sigurnosnim obilježjima tako da se može provjeriti cjelovitost i autentičnost preuzetih podataka.

4.9. ***Kriptografska podrška***

Zahtjevi iz ovog stavka su primjenjivi samo ako su potrebni, ovisno o korištenim sigurnosnim mehanizmima i o rješenjima proizvođača.

CSP_201 Svaka kriptografska radnja koju obavlja VU mora biti u skladu s propisanim algoritmom i utvrđenom veličinom ključa.

CSP_202 Ako VU generira kriptografske ključeve, to će biti u skladu s propisanim algoritmima generiranja kriptografskih ključeva i propisanim veličinama kriptografskog ključa.

CSP_203 Ako VU raspodjeljuje kriptografske ključeve, to mora biti u skladu s propisanim metodama raspodjele ključeva.

CSP_204 Ako VU pristupa kriptografskih ključevima, to će biti u skladu s propisanim metodama pristupa kriptografskim ključevima.

CSP_205 Ako VU uništi kriptografske ključeve, to će biti u skladu s propisanim metodama uništenja kriptografskih ključeva.

5. **Određivanje sigurnosnih mehanizama**

Zahtijevani sigurnosni mehanizmi su propisani u Dodatku 11.

Sve druge sigurnosne mehanizme moraju odrediti proizvođači.

6. **Minimalna otpornost sigurnosnih mehanizama**

Minimalna otpornost sigurnosnih mehanizama jedince u vozilu je ‚visoka', kako je određeno u (ITSEC).

7. **Razina sigurnosti**

Ciljna razina osiguranja jedinice u vozilu je razina ITSEC E3, kako je određeno u (ITSEC).

8. **Obrazloženje**

Sljedeće matrice logički obrazlažu SEF pomoću prikaza:

— koji SEF ili sredstva suzbijaju koje opasnosti,

— koji SEF ispunjavaju sigurnosni ciljevi IT.

	Opasnosti																		Ciljevi IT								
	Dostupnost	Identifikacija	Pogreške	Ispitivanja	Konstrukcija	Calibration_Parameters	Card_Data_Exchange	Sat	Okruženje	Fake_Devices	Hardver	Motion_Data	Non_Activated	Outpot_DAta	Power_Supply (namjerno ostavljeno prazno)		Security_Data	Sofver	Stored_Data	Dostupnost	Odgovornost	Revizija	Autentifikacija	Cjelovitost	Izlaz	Obrada	Pouzdanost	Secured_Data_Exchange
Fizička sredstva, osoblje i načini postupanja																												
Razvoj			x	x	x																						
Proizvodnja				x	x																						
Isporuka													x														
Aktivacija	x												x														
Generiranje sigurnosnih podataka																	x										
Prijenos sigurnosnih podataka																	x										
Raspoloživost kartice		x																									
Jedna kartica vozača		x																									
Mogućnost sljedivosti kartice		x																									
Ovlaštene radionice						x		x																			
Redovna kontrolna kalibracija						x		x				x	x			x											
Pouzdane radionice						x		x																			
Pouzdani vozači		x																									
Nadzor nad provedbom zakona		x				x		x	x		x		x		x			x	x								
Nadogradnja programa																			x								
Funkcije provedbe sigurnosti																											
Identifikacija i autentifikacija																											
UIA_201 Identifikacija senzora										x		x											x				x
UIA_202 Identitet senzora										x		x											x				x
UIA_203 Autentifikacija senzora										x		x											x				x
UIA_204 Ponovna identifikacija i ponovna autentifikacija senzora										x		x											x				x
UIA_205 Trajna autentifikacija										x		x											x				
UIA_206 Neuspjela autentifikacija										x		x									x					x	
UIA_207 Identifikacija korisnika	x	x								x										x			x				x
UIA_208 Identitet korisnika	x	x								x										x			x				x
UIA_209 Autentifikacija korisnika	x	x								x										x			x				x
UIA_210 Ponovna autentifikacija korisnika	x	x								x										x			x				x
UIA_211 Sredstva autentifikacije	x	x								x										x			x				
UIA_212 Provjere PIN	x	x				x		x												x			x				
UIA_213 Trajna autentifikacija	x	x								x										x			x				

	Opasnosti																				Ciljevi IT								
	Dostupnost	Identifikacija	Pogreške	Ispitivanja	Konstrukcija	Calibration_Parameters	Card_Data_Exchange	Sat	Okruženje	Fake_Devices	Hardver	Motion_Data	Non_Activated	Outpot_DAta	Power_Supply (namjerno ostavljeno prazno)	Security_Data	Sofver	Stored_Data	Dostupnost	Odgovornost	Revizija	Autentifikacija	Cjelovitost	Izlaz	Obrada	Pouzdanost	Secured_Data_Exchange
UIA_214 Neuspjela autentifikacija	x	x								x											x							
UIA_215 Daljinska identifikacija korisnika	x	x																	x			x					x	
UIA_216 Daljinski identitet korisnika	x	x																	x			x						
UIA_217 Daljinska autentifikacija korisnika	x	x																	x			x					x	
UIA_218 Sredstva autentifikacije	x	x																	x			x						
UIA_219 Trajna autentifikacija	x	x																	x			x						
UIA_220 Neuspjela autentifikacija	x	x																										
UIA_221 Identifikacija upravljačkog uređaja	x	x																	x			x						
UIA_222 Autentifikacija upravljačkog uređaja	x	x																	x			x						
UIA_223 Trajna autentifikacija	x	x																	x			x						
Upravljanje pristupom																												
ACC_201 Politika upravljanja pristupom	x					x		x								x		x	x									
ACC_202 Prava pristupa funkcijama	x					x		x											x									
ACC_203 Prava pristupa funkcijama	x					x		x											x									
ACC_204 VU ID																		x	x									
ACC_205 ID priključenog senzora										x								x	x									
ACC_206 Podaci o kalibraciji	x					x												x	x									
ACC_207 Podaci o kalibraciji						x												x	x									
ACC_208 Podaci o podešavanju vremena								x										x	x									
ACC_209 Podaci o podešavanju vremena								x										x	x									
ACC_210 Sigurnosni podaci																x		x	x									
ACC_211 Struktura datoteke i uvjeti pristupa	x					x										x		x	x									
Odgovornost																												
ACT_201 Odgovornost vozača																				x								
ACT_202 ID podaci o VU																				x	x							
ACT_203 Odgovornost radionice																				x								
ACT_204 Odgovornost kontrolora																				x								
ACT_205 Odgovornost za kretanja vozila:																				x								
ACT_206 Izmjena podataka o odgovornosti																		x					x			x		
ACT_207 Izmjena podataka o odgovornosti																		x					x			x		

	Opasnosti																		Ciljevi IT								
	Dostupnost	Identifikacija	Pogreške	Ispitivanja	Konstrukcija	Calibration_Parameters	Card_Data_Exchange	Sat	Okruženje	Fake_Devices	Hardver	Motion_Data	Non_Activated	Outpot_DAta	Power_Supply (namjerno ostavljeno prazno)		Security_Data	Sofver	Stored_Data	Dostupnost	Odgovornost	Revizija	Autentifikacija	Cjelovitost	Izlaz	Obrada	Pouzdanost	Secured_Data_Exchange
Revizija																												
AUD_201 Revizijski zapisi																						x						
AUD_202 Popis revizijskih slučajeva	x						x				x	x		x	x				x			x						
AUD_203 Pravila pohranjivanja revizijskih zapisa																						x						
AUD_204 Revizijski zapisi senzora																						x						
AUD_205 Sredstva za reviziju																						x						
Ponovno korištenje																												
REU_201 Ponovno korištenje																	x									x	x	
Točnost																												
ACR_201 Politika upravljanja tokom informacija						x			x		x															x	x	
ACR_202 Unutarnji prijenos														x											x	x	x	
ACR_203 Unutarnji prijenos														x								x						
ACR_204 Cjelovitost pohranjenih podataka																			x					x			x	
ACR_205 Cjelovitost pohranjenih podataka																			x			x						
Pouzdanost																												
RLB_201 Ispitivanja u proizvodnji				x	x																						x	
RLB_202 Samoispitivanja			x								x				x			x									x	
RLB_203 Samoispitivanja											x				x			x				x						
RLB_204 Analiza programa					x													x									x	
RLB_205 Unos programa																		x							x	x	x	
RLB_206 Otvaranje kućišta					x				x		x			x			x	x	x						x		x	
RLB_207 Preinake hardvera											x																x	
RLB_208 Preinake hardvera											x											x						
RLB_209 Prekidi napajanja															x												x	
RLB_210 Prekidi napajanja															x							x						
RLB_211 Vraćanje u početno stanje			x																								x	
RLB_212 Dostupnost podataka																										x	x	
RLB_213 Izvlačenje kartice																											x	
RLB_214 Razmjena podataka s karticom nije ispravno završeno																							x					
RLB_215 Višestruke aplikacije																											x	
Razmjena podataka																												
DEX_201 Osiguran unos podataka o kretanju												x																x
DEX_202 Osiguran unos podataka o kretanju												x							x									
DEX_203 Osiguran unos podataka s kartice							x																					x

	Opasnosti																			Ciljevi IT							
	Dostupnost	Identifikacija	Pogreške	Ispitivanja	Konstrukcija	Calibration_Parameters	Card_Data_Exchange	Sat	Okruženje	Fake_Devices	Hardver	Motion_Data	Non_Activated	Outpot_DAta	Power_Supply (namjerno ostavljeno prazno)		Security_Data	Sofver	Stored_Data	Dostupnost	Odgovornost	Revizija	Autentifikacija	Cjelovitost	Izlaz	Obrada	Pouzdanost	Secured_Data_Exchange
DEX_204 Osiguran unos podataka s kartice							x															x						
DEX_205 Osigurana isporuka podataka na kartice							x																					x
DEX_206 Dokaz o podrijetlu														x											x			
DEX_207 Dokaz o podrijetlu														x											x			
DEX_208 Osigurana isporuka na vanjske medije														x											x			
Kriptografska podrška																												
CSP_201 Algoritmi																											x	x
CSP_202 Generiranje ključa																											x	x
CSP_203 Raspodjela ključa																											x	x
CSP_204 Dostupnost ključa																											x	x
CSP_205 Unošenje ključa																											x	x

GENERIČKI SIGURNOSNI CILJ KARTICE TAHOGRAFA

1. **Uvod**

Ovaj dokument sadrži opis kartice tahografa, opasnosti koje mora prevladati i sigurnosne ciljeve koje mora postići, propisuje tražene funkcije provedbe sigurnosti, te navodi zahtijevanu najmanju otpornost sigurnosnih mehanizama i zahtijevanu razinu sigurnosti za razvoj i ocjenjivanje.

Zahtjevi iz ovog dokumenta su oni iz teksta Priloga I.B. U svrhu jasnoće čitanja ponekad dolazi do ponavljanja zahtjeva u tekstu Priloga I.B i zahtjeva u vezi sigurnosnih ciljeva. Ako postoje dvojbe između zahtjeva u vezi sigurnosnog cilja i zahtjeva iz Priloga I.B na koji se poziva ovaj zahtjev u vezi sigurnosnog cilja, vrijedi zahtjev iz teksta Priloga I.B.

Zahtjevi iz teksta Priloga I.B na koje se ne pozivaju sigurnosni ciljevi ne podliježu funkcijama provedbe sigurnosti.

Kartica tahografa je standardna pametna kartica koja sadrži namjensku tahografsku aplikaciju i mora udovoljavati najnovijim funkcionalnim i sigurnosnim zahtjevima koji vrijede za pametne kartice. Ovaj sigurnosni cilj stoga utjelovljuje samo dodatne sigurnosne zahtjeve potrebne za tahografsku aplikaciju.

Jednoznačne oznake su pripisane opasnostima, ciljevima, načinima postupanja i specifikacijama SEF u svrhu pronalaženja dokumentacije za razvoj i ocjenu.

2. **Kratice, definicije i literatura**

2.1. ***Kratice***

IC	integrirani krug (elektronski sastavni dio namijenjen funkcijama obrade podataka i/ili memorije)
OS	operativni sustav
PIN	osobni identifikacijski broj
ROM	stalna memorija
SFP	politika sigurnosnih funkcija
TBD	odredit će se
TOE	predmet ocjenjivanja
TSF	sigurnosna funkcija TOE
VU	jedinica u vozilu.

2.2. ***Definicije***

Digitalni tahograf	Uređaj za bilježenje
Osjetljivi podaci	Podaci koje pohranjuje kartica tahografa koje treba zaštititi u smislu cjelovitosti, neovlaštene izmjene i pouzdanosti (ako vrijedi za sigurnosne podatke). Osjetljivi podaci obuhvaćaju sigurnosne podatke i korisničke podatke.
Sigurnosni podaci	Posebni podaci potrebni za podržavanje funkcija provedbe sigurnosti (npr. kriptografski ključevi).
Sustav	Oprema, osoblje ili organizacije koje su na bilo koji način povezane s tahografom.
Korisnik	Svaka jedinica (čovjek korisnik ili vanjska jedinica IT) izvan TOE koja je u međudjelovanju s TOE (kada se ne koristi u izrazu ‚korisnički podaci').

Korisnički podaci	Osjetljivi podaci koji se pohranjuju na karticu tahografa, drugačiji od sigurnosnih podataka. Korisnički podaci obuhvaćaju identifikacijske podatke i podatke o aktivnosti.
Identifikacijski podaci	Identifikacijski podaci obuhvaćaju identifikacijske podatke za karticu i identifikacijske podatke nositelja kartice.
Identifikacijski podaci kartice	Korisnički podaci koji se odnose na identifikaciju kartice određenu zahtjevima 190, 191, 192, 194, 215, 231 i 235.
Identifikacijski podaci nositelja kartice	Korisnički podaci koji se odnose na identifikaciju nositelja kartice određenu zahtjevima 195, 196, 216, 232 i 236.
Podaci o aktivnosti	Podaci o aktivnosti obuhvaćaju podatke o aktivnostima nositelja kartice, podatke o događajima i pogreškama i podatke o aktivnostima nadzora.
Podaci o aktivnostima nositelja kartice	Korisnički podaci koji se odnose na aktivnosti nositelja kartice određene zahtjevima 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 i 237.
Podaci o događajima i pogreškama	Korisnički podaci koji se odnose na događaje ili pogreške određene u zahtjevima 204, 205, 207, 208 i 223.
Podaci o aktivnostima nadzora	Korisnički podaci koji se odnose na kontrolu provedbe zakona propisanu u zahtjevima 210 i 225.

2.3. ***Literatura***

ITSEC	Kriteriji vrednovanja sigurnosti informacijske tehnologije ITSEC 1991.
IC PP	Profil zaštite integriranog kruga pametne kartice – verzija 2.0 – izdanje rujan 1998. Registrirano pri francuskom certifikacijskom tijelu pod brojem PP/9806
ES PP	Integrirani krug pametne kartice sa ugrađenim profilom zaštite programa – verzija 2.0 – izdanje lipanj 1999. Registrirano pri francuskom certifikacijskom tijelu pod brojem PP/9911

3. **Obrazloženje proizvoda**

3.1. ***Opis kartice tahografa i način korištenja***

Kartica tahografa je pametna kartica, opisana u (IC PP) i (ES PP), koja sadrži program namijenjen njenom korištenju s tahografom.

Osnovne funkcije kartice tahografa su:

— pohranjivati identifikacijske podatke kartice i nositelja kartice. Ove podatke koristi jedinica u vozilu za identifikaciju nositelja kartice, pružanje odgovarajućih funkcija i prava na pristup podacima, te jamčenje odgovornosti nositelja kartice za svoje aktivnosti,

— pohranjivati podatke o aktivnostima nositelja kartice, podatke o događajima i pogreškama i podatke o nadzornim aktivnostima, koji se odnose na nositelje podataka.

Kartica tahografa je stoga namijenjena korištenju od strane uređaja za kartično sučelje jedinice u vozilu. Može je također koristiti svaki čitač kartica (npr. osobno računalo) koje ima puno pravo na pristup čitanju svakog korisničkog podatka.

Tijekom konačnog stadija korištenja u životnom vijeku kartice tahografa (stadij 7 životnog vijeka prema (ES PP), samo jedinice u vozilu mogu upisivati korisničke podatke u karticu.

Funkcionalni zahtjevi za karticu tahografa su propisani u tekstu Prilogu I.B i Dodatku 2.

3.2. ***Životni vijek kartice tahografa***

Životni vijek kartice tahografa odgovara životnom vijeku pametne kartice opisane u (ES PP).

3.3. ***Opasnosti***

Pored općih opasnosti za pametnu karticu koji su navedeni u (ES PP) i (IC PP), kartica tahografa može se suočiti sa sljedećim opasnostima:

3.3.1. *Krajnji ciljevi*

Krajnji cilj napadača je izmjena korisničkih podataka pohranjenih unutar TOE.

T.Ident_Data	Uspješna izmjena identifikacijskih podataka koje nosi TOE (npr. vrsta kartice ili datum isteka valjanosti kartice ili identifikacijski podaci nositelja kartice) bi mogla omogućiti prijevarno korištenje TOE i mogla bi predstavljati veću opasnost za sveopći sigurnosni cilj sustava.
T.Activity_Data	Uspješna izmjena podataka o aktivnostima pohranjenih u TOE bi predstavljala opasnost za sigurnost TOE.
T.Data_Exchange	Uspješna izmjena podataka o aktivnostima (dodavanje, brisanje, izmjena) tijekom unosa ili isporuke podataka bi mogla predstavljati opasnost za sigurnost TOE.

3.3.2. *Putovi napada*

Stavke TOE se može napasti:

— pokušajem nezakonitog stjecanja saznanja o hardverskom i softverskom projektu opreme TOE i posebno o njezinim sigurnosnim funkcijama ili sigurnosnim podacima. Nedopušteno saznanje se može steći putem napada na materijal projektanta ili proizvođača materijala (krađa, mito, …) ili putem izravnog pregleda TOE (fizički uzorci, analiza zaključaka, …),

— korištenjem slabosti u osmišljanju ili ostvarenju TOE (iskorištavanje pogrešaka hardvera, pogrešaka u softveru, propusta prijenosa, pogrešaka koje izaziva TOE opterećenjem iz okruženja, iskorištavanje slabosti sigurnosnih funkcija kao što su postupci autentifikacije, upravljanje pristupu podacima, kriptografske radnje, …),

— izmjenom TOE ili njezinih sigurnosnih funkcija putem fizičkih, električnih ili logičkih napada ili kombinacija istih.

3.4. ***Sigurnosni ciljevi***

Glavni sigurnosni cilj cjelokupnog sustava digitalnog tahografa je sljedeći:

O.Main	Podaci koje provjeravaju kontrolna tijela moraju biti dostupni i u potpunosti i točno odražavati aktivnost nadziranih vozača i vozila u pogledu vožnje, rada, razdoblja pripravnosti i odmora, te u pogledu brzine vozila.

Stoga su glavni sigurnosni ciljevi TOE koji doprinose sveopćem sigurnosnom cilju sljedeći:

O.Card_Identification_Data	TOE mora očuvati identifikacijske podatke o kartici i nositelju kartice pohranjene u postupku personalizacije kartice,
O.Card_Activity_Storage	TOE mora očuvati korisničke podatke koji su pohranjeni na karticu od strane jedinica u vozilu.

3.5. ***Sigurnosni ciljevi informatičke tehnologije***

Pored općih sigurnosnih ciljeva pametne kartice navedenih u (ES PP) i (IC PP), posebni sigurnosni ciljevi IT TOE koji doprinose njegovim glavnim sigurnosnim ciljevima tijekom faze njegovog konačnog životnog vijeka korištenja su sljedeći:

O.Data_Access	TOE mora ograničiti pravo pristupa upisivanju korisničkih podataka na autentificirane jedinice u vozilu,
O.Secure_Communications	TOE mora biti u stanju podržavati sigurne komunikacijske protokole i postupke između kartice i uređaja kartičnog sučelja kada to nalaže program.

3.6. ***Fizička sredstva, osoblje ili načini postupanja***

Fizička sredstva, osoblje ili načini postupanja koji doprinose sigurnosti TOE su navedeni u (ES PP) i (IC PP) (poglavlja o sigurnosnim ciljevima za okruženje).

4. **Funkcije provedbe sigurnosti**

Ovaj stavak podrobnije opisuje neke od dopuštenih radnji kao što su dodjela ili odabir (ES PP) i osigurava dodatne funkcionalne zahtjeve za SEF.

4.1. ***Udovoljavanje profilu zaštite***

CPP_301 TOE mora biti sukladan s (IC PP).

CPP_302 TOE mora biti sukladan s (ES PP), kako je podrobnije opisano u nastavku.

4.2. ***Identifikacija i autentifikacija korisnika***

Kartica mora identificirati jedinicu u koju je umetnuta i znati je li to autentificirana jedinica u vozilu ili nije. Kartica može isporučivati sve korisničke podatke bez obzira na jedinicu na koju je povezana, osim kontrolne kartice koja može isporučiti identifikacijske podatke nositelja kartice samo autentificiranim jedinicama u vozilu (tako da kontrolor bude siguran da jedinica u vozilu nije lažna uočavanjem svojeg imena na prikazu ili ispisu).

4.2.1. *Identifikacija korisnika*

Zadatak (FIA_UID.1.1) *Popis aktivnosti uz posredovanje TSF: niti jedna.*

Zadatak (FIA_ATD.1.1) *Popis sigurnosnih obilježja*:

USER_GROUP: VEHICLE_UNIT, NON_VEHICLE_UNIT,

USER_ID: registracijski broj vozila (VRN) i šifra države članice registracije (USER_ID je poznat samo za USER_GROUP = VEHICLE_UNIT).

4.2.2. *Autentifikacija korisnika*

Zadatak (FIA_UAU.1.1) *Popis aktivnosti uz posredovanje TSF*:

— kartice vozača i radionice: isporuka korisničkih podataka sa sigurnosnim obilježjima (funkcija preuzimanja podataka sa kartice),

— nadzorna kartica: isporuka korisničkih podataka bez sigurnosnih obilježja osim za identifikacijske podatke vozača.

UIA_301 Autentifikacija jedinice u vozilu se obavlja putem dokazivanja da posjeduje sigurnosne podatke koje može raspoređivati samo sustav.

Odabir (FIA_UAU.3.1 i FIA_UAU.3.2): spriječiti.

Zadatak (FIA_UAU.4.1) *Identificirani autentifikacijski mehanizam/mehanizmi*: svaki autentifikacijski mehanizam.

UIA_302 Kartica radionice mora osigurati dodatni autentifikacijski mehanizam provjerom šifre PIN (Svrha ovog mehanizma je da jedinica u vozilu osigura identitet nositelja kartice, a nije namijenjen zaštiti sadržaja kartice radionice).

4.2.3. *Neuspjela autentifikacija*

Sljedeći zadaci opisuju reakciju kartice za svaki pojedini propust autentifikacije korisnika.

Zadatak (FIA_AFL.1.1) *Broj: 1, popis autentifikacijskih slučajeva: autentifikacija uređaja kartičnog sučelja.*

Zadatak (FIA_AFL.1.2) *Popis radnji*:

— upozoriti priključenu jedinicu,

— smatrati korisnika kao NON_VEHICLE_UNIT.

Sljedeći zadaci opisuju reakciju kartice kod propusta dodatnog autentifikacijskog mehanizma prema zahtjevu UIA_302.

Zadatak (FIA_AFL.1.1) *Broj: 5, popis autentifikacijskih slučajeva: provjere PIN (kartica radionice).*

Zadatak (FIA_AFL.1.2) *Popis radnji*:

— upozoriti priključenu jedinicu,

— blokirati postupak provjere PIN-a tako da svaki sljedeći pokušaj provjere PIN-a bude neuspješan,

— biti u stanju naznačiti narednim korisnicima razlog blokiranja.

4.3. ***Upravljanje pristupom***

4.3.1. *Politika upravljanja pristupom*

Na kraju svog životnog vijeka, kartica tahografa podliježe politici jedne jedine sigurnosne funkcije upravljanja pristupom (SFP) koja se naziva AC_SFP.

Zadatak (FDP_ACC.2.1) SFP upravljanje pristupom: AC_SFP.

4.3.2. *Funkcije upravljanja pristupom*

Zadatak (FDP_ACF.1.1) *SFP upravljanje pristupom: AC_SFP.*

Zadatak (FDP_ACF.1.1) *Imenovana skupina sigurnosnih obilježja:* USER_GROUP.

Zadatak (FDP_ACF.1.2) *Pravila koja uređuju pristup kod nadziranih subjekata i nadziranih objekata koji koriste nadzirane radnje na nadziranim objektima:*

GENERAL_READ:	Korisnički podatak može učitati iz TOE svaki korisnik, osim identifikacijskih podataka korisnika kartice koje s kontrolnih kartica može učitati samo VEHICLE_UNIT.
IDENTIF_WRITE:	Identifikacijski podaci se mogu upisati samo jednom i prije kraja faze 6 životnog vijeka kartice. Niti jedan korisnik ne može upisivati ili mijenjati identifikacijske podatke tijekom životnog vijeka kartice.
ACTIVITY_WRITE:	Podatke o aktivnostima može na TOE upisivati samo VEHICLE_UNIT.
SOFT_UPGRADE:	Niti jedan korisnik ne može nadograđivati softver TOE.
FILE_STRUCTURE:	Struktrura datoteka i uvjeti pristupa stvaraju se prije kraja faze 6 životnog vijeka TOE i potom se blokiraju protiv svake daljnje izmjene ili brisanja od strane bilo kojeg korisnika.

4.4. ***Odgovornost***

ACT_301 TOE mora sadržavate trajne identifikacijske podatke.

ACT_302 Moraju biti naznačeni vrijeme i datum personalizacije TOE. Takva oznaka mora ostati neizmjenjiva.

4.5. ***Revizija***

TOE mora pratiti slučajeve koji označivaju potencijalnu ugrozu njegove sigurnosti.

Zadatak (FAU_SAA.1.2) *Podskup propisanih revizijskih događaja.*

— neuspjeh u autentifikaciji nositelja kartice (5 uzastopnih neuspješnih provjera PIN),

— pogreška samoispitivanja,

— pogreška cjelovitosti pohranjenih podataka,

— pogreška cjelovitosti unosa podataka o aktivnosti.

4.6. ***Točnost***

4.6.1. *Cjelovitost pohranjenih podataka*

Zadatak (FDP_SDI.2.2) *Radnje koje treba poduzeti: upozoriti priključenu jedinicu,*

4.6.2. *Temeljna autentifikacija podataka*

Zadatak (FDP_DAU.1.1) *Popis objekata ili tipovi informacija: podaci o aktivnosti.*

Zadatak (FDP_DAU.1.2) *Popis subjekata: bilo koji.*

4.7. ***Pouzdanost servisa***

4.7.1. *Ispitivanja*

Odabir (FPT_TST.1.1): tijekom početnog pokretanja, periodično tijekom redovnog rada.

Napomena: tijekom početnog pokretanja znači prije nego što se izvrši kod programa (i ne nužno tijekom postupka odziva na povrat u početno stanje).

RLB_301 Samoispitivanja TOE moraju obuhvatiti provjeru cjelovitosti svakog programskog koda softvera koji nije pohranjen u ROM.

RLB_302 Po otkrivanju pogreške samoispitivanja, TSF mora upozoriti priključenu jedinicu.

RLB_303 Nakon provedenog ispitivanja OS, sve naredbe i radnje svojstvene ispitivanju se moraju staviti izvan funkcije ili ukloniti. Ne smije biti moguće premostiti ove kontrolne uređaje i vratiti ih u uporabno stanje. Naredbi koja je pridružena isključivo jednoj fazi životnog vijeka nikada se ne smije pristupiti tijekom nekog druge faze.

4.7.2. *Softver*

RLB_304 Ne smije biti moguće analizirati, ispravljati pogreške ili izmijeniti program TOE na terenu.

RLB_305 Unos podataka iz vanjskih izvora se ne smije prihvatiti kao izvršni kod.

4.7.3. *Napajanje*

RLB_306 TOE mora održavati sigurno stanje tijekom prekida ili kolebanja napajanja.

4.7.4. *Uvjeti povrata u početno stanje*

RLB_307 Ako se prekine napajanje TOE (ili ako dođe do kolebanja napajanja) ili ako se postupak prekine prije okončanja ili u svim drugim uvjetima vraćanja u početno stanje, TOE se mora uredno vratiti u početno stanje.

4.8. ***Razmjena podataka***

4.8.1. *Razmjena podataka s jedinicom u vozilu*

DEX_301 TOE mora provjeriti cjelovitost i autentičnost podataka koji se unose sa jedince u vozilu.

DEX_302 Po otkrivanju pogreške cjelovitosti unesenih podataka, TOE mora:

— upozoriti jedinicu koja šalje podatke,

— ne koristiti podatke.

DEX_303 TOE mora isporučivati korisničke podatke jedinici u vozilu s odgovarajućim sigurnosnim značajkama, tako da jedinica u vozilu može provjeriti cjelovitost i autentičnost primljenih podataka.

4.8.2. *Isporučivanje podataka jedinici izvan vozila (funkcija preuzimanja podataka)*

DEX_304 TOE mora biti u stanju generirati dokaz o podrijetlu za podatke preuzete na vanjske medije.

DEX_305 TOE mora moći osigurati mogućnost provjere dokaza o podrijetlu podataka preuzetih na primatelja.

DEX_306 TOE mora biti u stanju preuzeti podatke na vanjske medije za spremanje podataka s odgovarajućim sigurnosnim obilježjima tako da se može provjeriti cjelovitost preuzetih podataka.

4.9. ***Kriptografska podrška***

CSP_301 Ako TSF generira kriptografske ključeve, to će biti u skladu s propisanim algoritmima generiranja kriptografskih ključeva i propisanim duljinama kriptografskih ključeva. Generirani ključevi kriptografske faze moraju imati ograničen broj mogućih uporaba (koje određuje proizvođač i ne više od 240).

CSP_302 Ako TSF raspodjeljuje kriptografske ključeve, to mora biti u skladu sa specifičnim metodama raspodjele kriptografskih ključeva.

5. **Određivanje sigurnosnih mehanizama**

Zahtijevani sigurnosni mehanizmi su navedeni u Dodatku 11.

Sve ostale sigurnosne mehanizme mora definirati proizvođač TOE.

6. **Tražena najmanja otpornost mehanizama**

Najmanja otpornost mehanizama za karticu tahografa je ‚visoka' u skladu sa (ITSEC).

7. **Razina sigurnosti**

Ciljna razina sigurnosti za karticu tahografa je razina ITSEC E3 prema definiciji u (ITSEC).

8. **Obrazloženje**

Sljedeće matrice daju obrazloženje SEF pomoću prikaza:

— koji SEF sprečava koje opasnosti,

— koji SEF ispunjava koje sigurnosne ciljeve IT.

	Opasnosti											Ciljevi IT								
	T.CLON*	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	Ident_Data	Activity_Data	Data_Exchange	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FI.AW*	O.DIS_MECJANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Data_Access	Secured_Communications
UIA_301 Značenje autentifikacije																			x	
UIA_302 Provjere PIN																			x	
ACT_301 Identifikacijski podaci																				
ACT_302 Datum personalizacije																				
RLB_301 Cjelovitost softvera												x		x						
RLB_302 Samoispitivanja												x		x						
RLB_303 Ispitivanja u proizvodnji					x	x						x		x						
RLB_304 Analiza softvera					x		x	x				x		x						
RLB_305 Instalacija softvera					x	x		x				x		x						
RLB_306 Napajanje									x	x		x		x						
RLB_307 Vraćanje u početno stanje												x		x						
DEX_301 Siguran unos podataka											x									x
DEX_302 Siguran unos podataka											x									x
DEX_303 Sigurna isporuka podataka u VU											x									x
DEX_304 Dokaz o podrijetlu											x									x
DEX_305 Dokaz o podrijetlu											x									x
DEX_306 Sigurna isporuka vanjskim medijima											x									x
CSP_301 Generiranje ključeva												x								x
CSP_302 Raspodjela ključeva												x								x

Dodatak 11.

ZAJEDNIČKI SIGURNOSNI MEHANIZMI

SADRŽAJ

1. OPĆENITO

Ovaj Dodatak propisuje sigurnosne mehanizme koji osiguravaju:

— uzajamnu autentifikaciju između jedinice vozila i kartica tahografa, uključujući dogovaranje ključa razmjene podataka,

— povjerljivost, cjelovitost i autentifikaciju podataka koji se prenose između jedinice vozila i kartica tahografa,

— cjelovitost i autentifikaciju podataka preuzetih s jedinice vozila na vanjske medije za pohranjivanje,

— cjelovitost i autentifikaciju podataka preuzetih sa kartica tahografa na vanjske medije za pohranjivanje.

1.1. **Literatura**

U ovom su Dodatku korišteni sljedeći izvori:

SHA-1	Nacionalni institut za norme i tehnologiju (NIST): Publikacija FIPS 180-1: Norma sigurnosne kompresije. Travanj 1995.
PKCS1	Laboratoriji RSA. PKCS # 1: Norme šifriranja RSA. Verzija 2.0. listopad 1998.
TDES	Nacionalni institut za norme i tehnologiju (NIST): Publikacija FIPS 46-3: Norma šifriranja podataka. Nacrt 1999.
TDES-OP	ANSI X9.52, Načini rada algoritma za trostruko šifriranje podataka. 1998.
ISO/IEC 7816-4	Informacijska tehnologija – Identifikacijske kartice – Kontaktne kartice s integriranim krugom/krugovima – Dio 4.: Međugranske naredbe za razmjenu: Prvo izdanje 1995. + Izmjena 1.: 1997.
ISO/IEC 7816-6	Informacijska tehnologija - Identifikacijske kartice - Kontaktne kartice s integriranim krugom/krugovima - Dio 6.: Međugranski podatkovni elementi. Prvi izdanje: 1996 + ispravak. 1: 1998.
ISO/IEC 7816-8	Informacijska tehnologija - Identifikacijske kartice - Kontaktne kartice s integriranim krugom/krugovima - Dio 8.: Međugranske naredbe u vezi sigurnosti. Prvo izdanje 1999.
ISO/IEC 9796-2	Informacijska tehnologija – Sigurnosne tehnike – Sustavi digitalnog potpisa za obnavljanje poruka – Dio 2.: Mehanizmi koji koriste funkciju kompresije podataka. Prvo izdanje: 1997.
ISO/IEC 9798-3	Informacijska tehnologija – Sigurnosne tehnike – Mehanizmi autentifikacije jedinice – Dio 3.: Identifikacija jedinice korištenjem algoritma javnog ključa. Drugo izdanje 1998.
ISO 16844-3	Cestovna vozila – Tahografski sustavi Dio 3.: Sučelje senzora kretanja.

1.2. **Označivanje i skraćenice**

U ovom se Dodatku koriste sljedeće oznake i skraćenice:

(K_a, K_b, CZK)	Snop ključeva kojega koristi algoritam za trostruko šifriranje podataka
CA	Certifikacijsko tijelo
CAR	Upućivanje na certifikacijsko tijelo
CC	Kriptografski kontrolni zbroj
CG	Kriptogram
CH	Glava naredbe
CHA	Ovlaštenje nositelja certifikata
CHR	Upućivanje na nositelja certifikata
D()	Dešifriranje pomoću DES
DE	Podatkovni element
DO	Podatkovni objekt
d	Privatni ključ RSA, privatni eksponent
e	Javni ključ RSA, javni eksponent
E()	Šifriranje pomoću DES
EQT	Oprema
Hash()	vrijednost komprimirane poruke, izlazni podatak funkcije komprimiranja
Hash	funkcija komprimiranja
KID	identifikator ključa
Km	Ključ TDES. Glavni ključ određen u ISO 16844-3
Km_{vu}	Ključ TDES unesen u jedinice u vozilu
Km_{wc}	Ključ TDES unesen u kartice radionice
m	Predstavnik poruke, cjelobrojne brojeve između 0 i n-1
n	Ključevi RSA, modul
PB	Bajtovi za popunjenje
PI	Bajt indikatora popunjenja (za kriptograme povjerljivih DO)
PV	Nešifrirana vrijednost
s	Predstavnik potpisa, cijelobrojni broj između 0 i n-1
SSC	Brojač redoslijeda slanja
SM	Sigurno upućivanje poruka
TCBC	Način rada ulančavanjem šifarskih blokova TDEA
TDEA	Algoritam trostrukog šifriranja podataka
TLV	Vrijednost duljine oznake
VU	Jedinica u vozilu
X.C	certifikat korisnika X koji izdaje certifikacijsko tijelo
X.CA	certifikacijsko tijelo korisnika X
X.CA.PK_0X.C	radnja razvijanja certifikata za izdvajanje javnog ključa. To je infiksni operator čiji je lijevi operand javni ključ certifikacijskog tijela, a desni operand je certifikat koju izdaje navedeno certifikacijsko tijelo. Ishod je javni ključ korisnika X čiji certifikat je desni operand,

X.PK	javni ključ korisnika X
X.PK[I]	šifra RSA nekog podatka I, korištenjem javnog ključa korisnika X
X.SK	privatni ključ RSA korisnika X
X.SK[I]	šifra RSA nekog podatka I, korištenjem privatnog ključa korisnika X
‚xx'	heksadecimalna vrijednost
||	operator ulančavanja.

2. KRIPTOGRAFSKI SUSTAVI I ALGORITMI

2.1. **Kriptografski sustavi**

CSM_001 Jedinice u vozilu i kartice tahografa moraju koristiti klasičan kriptografski sustav javnog ključa RSA koji osigurava sljedeće sigurnosne mehanizme:

— autentifikaciju između jedinica u vozilu i kartica,

— prijenos ključeva trostruke-DES faze između jedinica u vozilu i kartica tahografa,

— digitalni potpis podataka preuzetih sa jedinica u vozilima ili kartica tahografa na vanjske medije.

CSM_002 Jedinice u vozilu i kartice tahografa moraju koristiti trostruki simetričan kriptografski sustav DES za osiguranje mehanizma cjelovitosti podataka tijekom razmjene korisničkih podataka između jedinica u vozilu i kartica tahografa i za osiguranje, ako je primjereno, pouzdanosti razmjene podataka između jedinica u vozilu i kartica tahografa.

2.2. **Kriptografski algoritmi**

2.2.1. ***Algoritam RSA***

CSM_003 Algoritam RSA je u potpunosti definiran sljedećim odnosima:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Potpuniji opis funkcije RSA se može naći u izvoru (PKCS1).

Javni eksponent, e, za izračun RSA će biti različit od 2 u svim generiranim ključevima RSA.

2.2.2. ***Algoritam kompresije***

CSM_004 Mehanizmi digitalnog potpisa moraju koristiti algoritam kompresije SHA-1 definiran u izvoru (SHA-1).

2.2.3. ***Algoritam šifriranja podataka***

CSM_005 Algoritmi utemeljeni na DES se moraju koristiti u načinu ulančavanja šifriranih blokova.

3. KLJUČEVI I CERTIFIKATI

3.1. Generiranje i raspodjela ključeva

3.1.1. ***Generiranje i raspodjela ključeva RSA***

CSM_006 Ključevi RSA se moraju generirati preko tri funkcionalne hijerarhijske razine:

— europska razina,

— razina države članice,

— razina opreme.

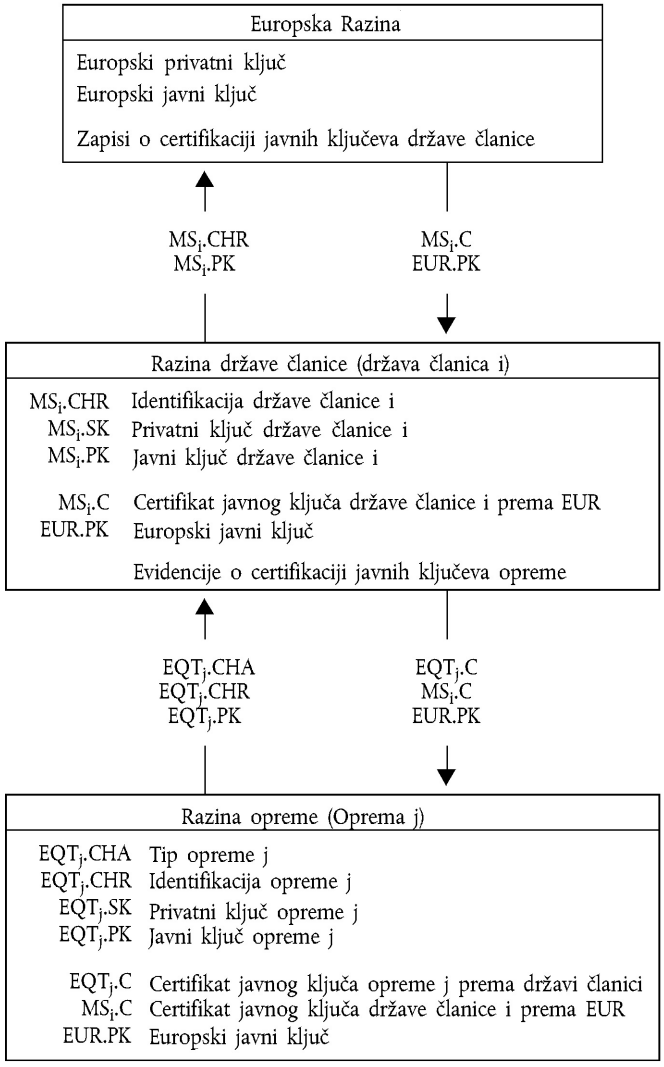
CSM_007 Na europskoj razini se mora generirati jedinstveni europski par ključeva (EUR.SK i EUR.PK). Europski privatni ključ se mora koristiti za certifikaciju javnih ključeva država članica. Moraju se voditi zapisi o svim potvrđenim ključevima. Ove poslove mora voditi Europsko certifikacijsko tijelo, pod nadležnošću i odgovornosti Europske komisije.

CSM_008 Na razini države članice se mora generirati par ključeva države članice (MS.SK i MS.PK). Javni ključevi država članica moraju biti certificirani od strane Europskog certifikacijskog tijela. Privatni ključ države članice mora se koristiti za certificiranje javnih ključeva koji se unose u opremu (jedinica u vozilu ili kartica tahografa). Zapisi svih potvrđenih javnih ključeva moraju se čuvati s identifikacijom opreme za koju su namijenjeni. Ove poslove mora voditi certifikacijsko tijelo države članice. Država članica može redovito mijenjati svoj par ključeva.

CSM_009 Na razini opreme, generira se i umeće u svaku napravu jedan jedini par ključeva (EQT.SK i EQT.PK). Javne ključeve opreme mora certificirati certifikacijsko tijelo države članice. Ove poslove mogu voditi proizvođači opreme, izvođači personalizacije opreme ili vlasti države članice. Ovaj par ključeva se koristi za službe autentifikacije, digitalnog potpisa i šifriranje

CSM_010 Povjerljivost privatnih ključeva mora se održavati tijekom generiranja, prijenosa (ako postoji) i čuvanja.

Sljedeća slika sažima protok podataka u ovom postupku:



3.1.2. ***Ispitni ključevi RSA***

CSM_011 U svrhu ispitivanja opreme (uključujući ispitivanje interoperabilnosti) Europsko certifikacijsko tijelo izrađuje različit jedinstveni europski par ispitnih ključeva i najmanje dva para ispitnih ključeva države članice, čiji se javni ključevi certificiraju europskim privatnim ispitnim ključem. U opremu koja podliježe tipnom odobrenju proizvođači moraju unijeti ispitne ključeve certificirane jednim od ovih ispitnih ključeva države članice.

3.1.3. ***Ključevi senzora kretanja***

Povjerljivost tri ključa TDES koji su opisani u nastavku se mora odgovarajuće održavati tijekom generiranja, prijenosa (ako postoji) i čuvanja.

Za podršku tahografa koji zadovoljava ISO 16844, Europsko certifikacijsko tijelo i certifikacijska tijela države članice moraju, pored toga, osigurati sljedeće:

CSM_036 Europsko certifikacijsko tijelo mora generirati Km_{VU} i Km_{WC}, dva neovisna i jedinstvena trojna ključa DES, te generirati Km kao:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

Europsko certifikacijsko tijelo dostavlja navedene ključeve certifikacijskim tijelu država članica u odgovarajuće osiguranim postupcima, na njihov zahtjev.

CSM_037 Certifikacijska tijela država članica moraju:

— koristiti Km za šifriranje podataka osjetila kretanja koje traže proizvođači senzora kretanja (podaci koji se šifriraju s Km su određeni u ISO 16844-3),

— dostaviti Km_{VU} proizvođačima jedinica u vozilu, u odgovarajuće osiguranim postupcima, za unošenje u jedinice u vozilu,

— osigurati da Km_{WC} bude umetnut u sve kartice radionica (`SensorInstallationSecData` u elementarnoj datoteci`Sensor_Installation_Data`) tijekom personalizacije kartice.

3.1.4. ***Generiranje i raspodjela ključeva postupka T-DES***

CSM_012 Jedinice u vozilu i kartice tahografa moraju, kao dio postupka uzajamne autentifikacije, generirati i razmjenjivati podatke potrebne za izradu zajedničkog kripto ključa trojnog procesa DES. Povjerljivost ove razmjene podataka mora biti zaštićena putem kripto mehanizma šifriranja RSA.

CSM_013 Ovaj ključ se mora koristiti za sve naredne kriptografske radnje koje koriste sigurne poruke. Njegova valjanost mora isteći na kraju postupka (povlačenje kartice ili vraćanje kartice u početno stanje) i/ili nakon 240 upotreba (jedna upotreba ključa = jedna naredba koja koristi sigurne poruke upućene kartici i odgovarajući odgovor).

3.2. **Ključevi**

CSM_014 Ključevi RSA moraju imati (bez obzira na razinu) sljedeće duljine: modul n 1024 bitova, javni eksponent e najviše 64 bitova, privatni eksponent d 1024 bitova.

CSM_015 Trojni ključevi DES moraju imati oblik (K_a, K_b, K_a), pri čemu su K_a i K_b neovisni ključevi dužine 64 bita. Ne smiju biti namješteni bitovi koji ustanovljuju paritetnu grešku.

3.3. **Certifikati**

CSM_016 Certifikati javnih ključeva moraju biti ‚nesamoopisni' ‚karticom provjerljivi' certifikati (izvor: ISO/IEC 7816-8)

3.3.1. ***Sadržaj certifikata***

CSM_017 Certifikati javnih ključeva RSA su ugrađeni u sljedeće podatke sljedećim redom:

Podaci	Oblik	Bajtova	Opis
CPI	CIJELI BROJ	1	Identifikator profila certifikata (u ovoj verziji ‚01')
CAR	OKTETNI NIZ	8	Upućivanje na certifikacijsku vlast
CHA	OKTETNI NIZ	7	Ovlaštenje nositelja certifikata
EOV	TimeReal	4	Kraj valjanosti certifikata. Nije obvezno, dopunjen sa ‚FF' ako se ne koristi
CHR	OKTETNI NIZ	8	Upućivanje na nositelja certifikata
n	OKTETNI NIZ	128	Javni ključ (modul)
e	OKTETNI NIZ	8	Javni ključ (javni eksponent)
		164	

Napomene:

1. ‚Identifikator profila certifikata' (CPI) označuje točnu strukturu autentifikacijskog certifikata. Može se koristiti kao unutarnji identifikator opreme iz zaglavlja odgovarajućeg popisa koji opisuje ulančavanje podatkovnih elemenata unutar certifikata.

   Zaglavlje popisa pridružen sadržaju ovog certifikata je sljedeći:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Oznaka proširenog zaglavlja popisa	Duljina popisa iz zaglavlja	Oznaka CPI	Duljina CPI	Oznaka CAR	Duljina CAR	Oznaka CHA	Duljina CHA	Oznaka EOV	Duljina EO	Oznaka CHR	Duljina CHR	Oznaka javnog ključa (konstruirana)	Duljina narednih DO	Oznaka modula	Duljina modula	Oznaka javnog eksponenta	Duljina javnog eksponenta

2. ‚Upućivanje na certifikacijsko tijelo' (CAR) ima za svrhu identificiranje CA koji izdaje certifikat tako da se podatkovni element može istodobno koristiti kao identifikator ključa vlasti za upućivanje na javni ključ certikacijske vlasti (za šifriranje, vidjeti identifikator ključa u nastavku).

3. ‚Ovlaštenje nositelja certifikata' (CHA) se koristi za identifikaciju prava nositelja certifikata. Ono se sastoji od ID primjene tahografa i vrste opreme za koju je certifikat namijenjen (prema podatkovnom elementu EquipmentType, ‚00' za državu članicu).

4. ‚Upućivanje na nositelja certifikata' (CHR) ima za cilj jedinstvenu identifikaciju nositelja certifikata tako da se podatkovni element može istodobno koristiti kao identifikator ključa predmeta za upućivanje na javni ključ nositelja certifikata.

5. Identifikatori ključa na jedinstven način identificiraju nositelja certifikata ili certifikacijske vlasti. Oni su šifrirani kako slijedi:

   5.1. Oprema (VU ili kartica):

Podaci	Serijski broj opreme	Datum	Tip	Proizvođač
Duljina	4 bajta	2 bajta	1 bajt	1 bajt
Vrijednost	Cijeli broj	BCD šifriranje mm gg	Svojstveno proizvođaču	Šifra proizvođača

Kod VU, proizvođač, prilikom traženja certifikata, može ili ne mora znati identifikaciju opreme u koju se unose ključevi.

U prvom slučaju, proizvođač će poslati na certifikaciju identifikaciju opreme s javnim ključem tijelu svoje države članice. Certifikat će potom sadržati identifikaciju opreme, a proizvođač mora osigurati da se ključevi i certifikat unesu u opremu za koju su namijenjeni. Identifikator ključa ima gore prikazan oblik.

U potonjem slučaju, proizvođač mora na jedinstven način identificirati svaki zahtjev za certifikat i poslati takvu identifikaciju s javnim ključem tijelu svoje države članice na certifikaciju. Certifikat će sadržavati identifikaciju zahtjeva. Proizvođač mora povratno obavijestiti tijelo svoje države članice o dodjeli ključa opremi (tj. identifikaciji zahtjeva za certifikat, identifikaciji opreme) nakon ugradnje ključa u opremu. Identifikator ključa ima sljedeći oblik:

Podaci	Serijski broj zahtjeva za certifikat	Datum	Tip	Proizvođač
Duljina	4 bajta	2 bajta	1 bajt	1 bajt
Vrijednost	BCD šifriranje	BCD šifriranje mm gg	‚FF'	Šifra proizvođača

5.2. Certifikacijska vlast:

Podaci	Identifikacija vlast	Serijski broj ključa	Dodatne informacije	Identifikator
Duljina	4 bajta	1 bajt	2 bajta	1 bajt
Vrijednost	1-bajtna numerička šifra države 3-bajtna alfanumerička šifra države	cijeli broj	dodatno šifriranje (svojstveno CA) ‚FF FF', ako nije iskorišteno	‚01'

Serijski broj ključa se koristi za raspoznavanje različitih ključeva države članice, u slučaju da se ključ promijeni.

6. Osobe koje vrše provjeru certifikata implicitno znaju da je certificirani javni ključ RSA ključ koji se odnosi na autentifikaciju, provjeru digitalnog potpisa i šifriranje za službe povjerljivosti (certifikat ne sadrži identifikator objekta koji bi to navodio).

3.3.2. ***Izdani certifikati***

CSM_018 Izdani certifikat je digitalni potpis s djelomičnim obnavljanjem sadržaja certifikata u skladu s ISO/IEC 9796-2, s priloženim upućivanjem na certifikacijsku vlast.

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

sa sadržajem certifikata

$$= Cc = \underset{106\ \text{Bytes}}{C_r} \,||\, \underset{58\ \text{Bytes}}{C_n}$$

Napomene:

1. Duljina ovog certifikata je 194 bajta.

2. CAR, koji se skriven potpisom, je također priložen potpisu tako da može biti odabran javni ključ certifikacijskog tijela za provjeru certifikata.

3. Osoba koja provjerava certifikat mora implicitno poznavati kod kojeg koristi certifikacijska vlast za potpisivanje certifikata.

4. Zaglavlje pridruženo navedenom izdanom certifikatu je sljedeće:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Oznaka certifikata CV (konstruirana)	Duljina narednih DO	Oznaka potpisa	Duljina potpisa	Oznaka ostatka	Duljina ostatka	Oznaka CAR	Duljina CAR

3.3.3. ***Provjera i otvaranje certifikata***

Provjera i otvaranje certifikata se sastoji od provjere potpisa prema ISO/IEC 9796-2, pronalaženja sadržaja certifikata i sadržanog javnog ključa: X.PK = X.CA.PK$_0$X.C, te provjere valjanosti certifikata.

CSM_019 Obuhvaća sljedeće korake:

provjeriti potpis i pronaći sadržaj:

— u X.C pronaći Sign, C_n' i CAR':

$$X.C = \underset{128\ Bytes}{Sign} \;||\; \underset{58\ Bytes}{C_n'} \;||\; \underset{8\ Bytes}{CAR'}$$

— odabrati iz CAR' odgovarajući javni ključ certifikacijske vlasti (ako to nije učinjeno ranije drugim putem)

— otvoriti Sign s javnim ključem CA: Sr' = X.CA.PK [Znak],

— provjeriti da Sr' započinje sa ‚6A' i završava s ‚BC'

— izračunati Cr' i H' iz:

$$Sr' = \text{'6A'} \;||\; \underset{106\ Bytes}{C_r'} \;||\; \underset{20\ Bytes}{H'} \;||\; \text{'BC'}$$

— ponovno učitati sadržaj certifikata C' = C_r' || Cn',

— provjeriti kompresiju poruke (C') = H'

Ako su provjere u redu, certifikat je autentičan, njegov sadržaj je C'.

Provjeriti valjanost. Iz C':

— prema potrebi, provjeriti datum isteka valjanosti,

Pronaći i spremiti javni ključ, identifikator ključa, autorizaciju nositelja certifikata i istek valjanosti certifikata iz C':

— X.PK = n||e

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV.

4. MEHANIZAM UZAJAMNE AUTENTIFIKACIJE

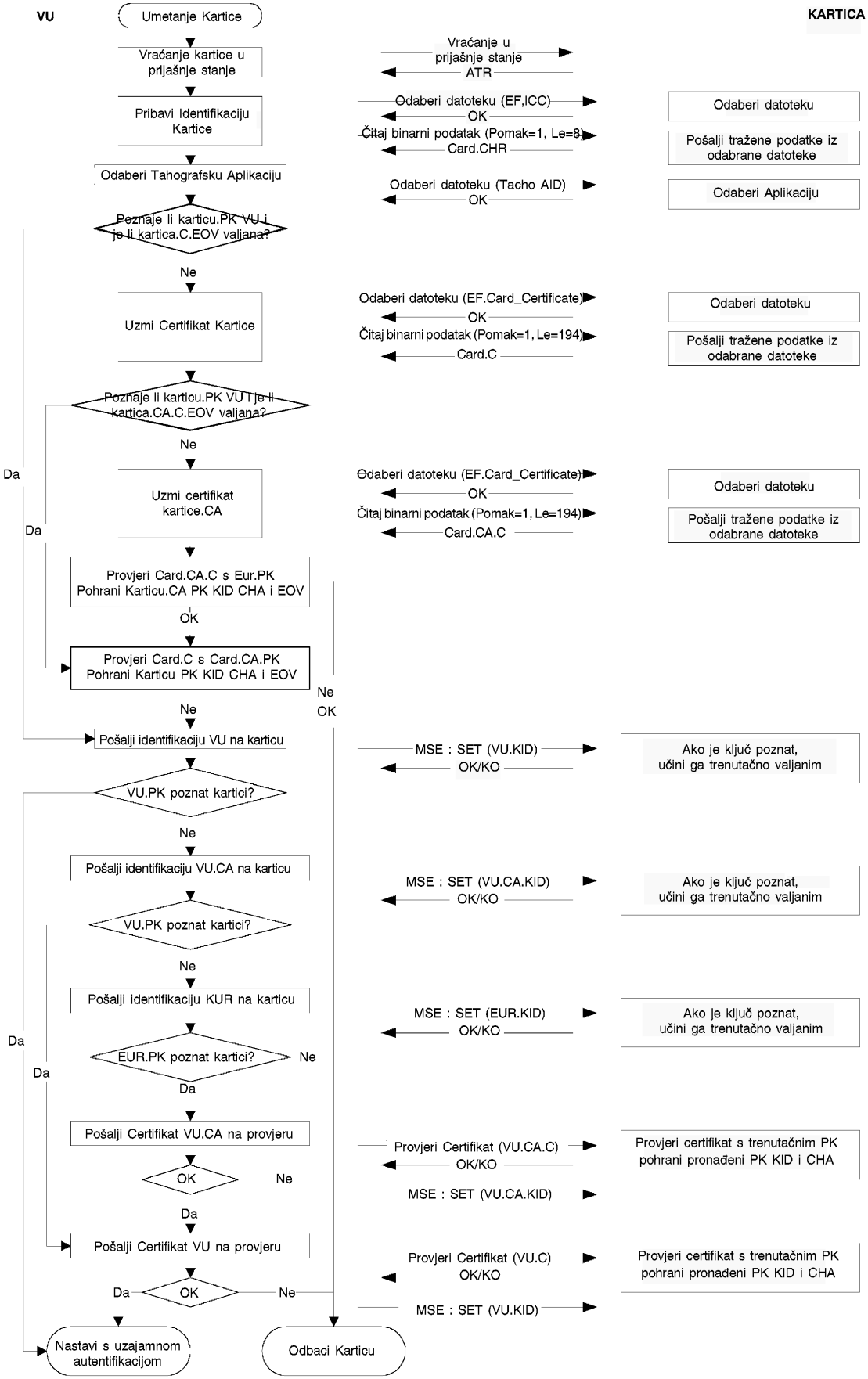
Uzajamna autentifikacija među karticama i VU se temelji na sljedećim načelu:

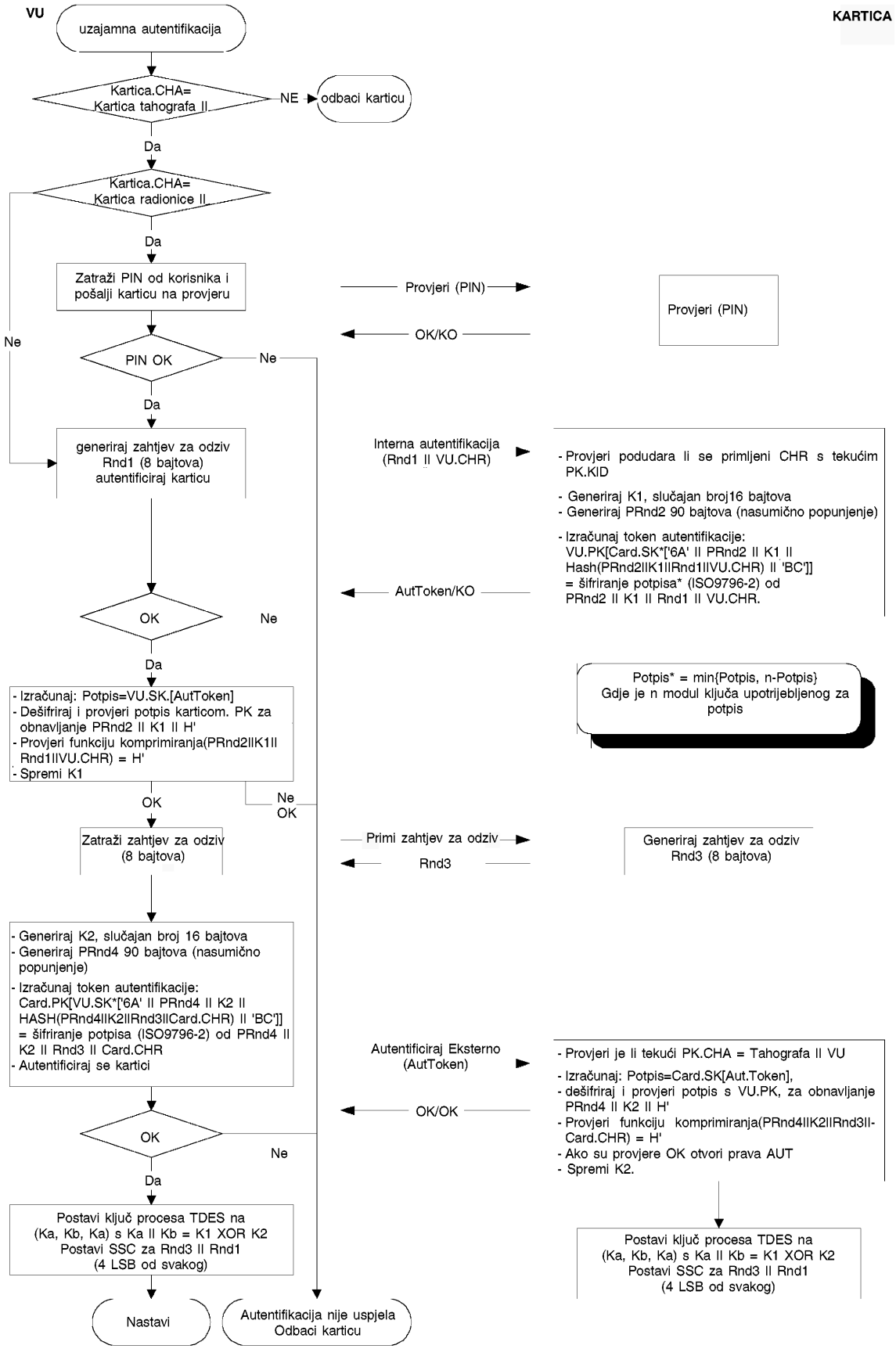
Svaka strana mora dokazati drugoj da posjeduje valjan par ključeva, javni ključ kojih je certificiran od strane certifikacijske vlasti države članice koja je i sama certificirana od strane Europskog certifikacijskog tijela.

Dokazivanje se obavlja potpisivanjem privatnim ključem slučajnog broja kojega je poslala druga strana koja mora obnoviti slučajan broj upućen prilikom provjere potpisa.

Mehanizam aktivira jedinica u vozilu prilikom umetanja kartice. On započinje razmjenom certifikata i razvijanjem javnih ključeva, te završava postavljanjem ključa razmjene podataka.

CSM_020 Mora se koristiti sljedeći protokol (strelice prikazuju naredbe i razmijenjene podatke (vidjeti Dodatak 2.))




VU
KARTICA
uzajamna autentifikacija
Kartica.CHA= Kartica tahografa II
NE
odbaci karticu
Da
Kartica.CHA= Kartica radionice II
Da
Zatraži PIN od korisnika i pošalji karticu na provjeru
Provjeri (PIN)
Provjeri (PIN)
OK/KO
Ne
PIN OK
Ne
Da
generiraj zahtjev za odziv Rnd1 (8 bajtova) autentificiraj karticu
Interna autentifikacija (Rnd1 II VU.CHR)
- Provjeri podudara li se primljeni CHR s tekućim PK.KID
- Generiraj K1, slučajan broj16 bajtova
- Generiraj PRnd2 90 bajtova (nasumično popunjenje)
- Izračunaj token autentifikacije: VU.PK[Card.SK*['6A' II PRnd2 II K1 II Hash(PRnd2IIK1IIRnd1IIVU.CHR) II 'BC']] = šifriranje potpisa* (ISO9796-2) od PRnd2 II K1 II Rnd1 II VU.CHR.
AutToken/KO
OK
Ne
Da
Potpis* = min{Potpis, n-Potpis}
Gdje je n modul ključa upotrijebljenog za potpis
- Izračunaj: Potpis=VU.SK.[AutToken]
- Dešifriraj i provjeri potpis karticom. PK za obnavljanje PRnd2 II K1 II H'
- Provjeri funkciju komprimiranja(PRnd2IIK1II Rnd1IIVU.CHR) = H'
- Spremi K1
Ne OK
OK
Zatraži zahtjev za odziv (8 bajtova)
Primi zahtjev za odziv
Rnd3
Generiraj zahtjev za odziv Rnd3 (8 bajtova)
- Generiraj K2, slučajan broj 16 bajtova
- Generiraj PRnd4 90 bajtova (nasumično popunjenje)
- Izračunaj token autentifikacije: Card.PK[VU.SK*['6A' II PRnd4 II K2 II HASH(PRnd4IIK2IIRnd3IICard.CHR) II 'BC']] = šifriranje potpisa (ISO9796-2) od PRnd4 II K2 II Rnd3 II Card.CHR
- Autentificiraj se kartici
Autentificiraj Eksterno (AutToken)
- Provjeri je li tekući PK.CHA = Tahografa II VU
- Izračunaj: Potpis=Card.SK[Aut.Token],
- dešifriraj i provjeri potpis s VU.PK, za obnavljanje PRnd4 II K2 II H'
- Provjeri funkciju komprimiranja(PRnd4IIK2IIRnd3II-Card.CHR) = H'
- Ako su provjere OK otvori prava AUT
- Spremi K2.
OK/OK
OK
Ne
Da
Postavi ključ procesa TDES na (Ka, Kb, Ka) s Ka II Kb = K1 XOR K2
Postavi SSC za Rnd3 II Rnd1
(4 LSB od svakog)
Postavi ključ procesa TDES na (Ka, Kb, Ka) s Ka II Kb = K1 XOR K2
Postavi SSC za Rnd3 II Rnd1
(4 LSB od svakog)
Nastavi
Autentifikacija nije uspjela
Odbaci karticu

5. MEHANIZAM POVJERLJIVOSTI PRIJENOSA, CJELOVITOSTI I AUTENTIFIKACIJE PRIJENOSA PODATAKA IZMEĐU KARTICA I JEDINICE U VOZILU

5.1. **Sigurne poruke**

CSM_021 Cjelovitost prijenosa podataka između jedinice u vozilu i kartice se mora zaštititi putem sigurnih poruka sukladno izvorima (ISO/IEC 7816-4) i (ISO/IEC 7816-8).

CSM_022 Kada podaci moraju biti zaštićeni tijekom prijenosa, podatkovni objekt kriptografskog kontrolnog zbroja se pridodaje podatkovnim objektima koji se šalju u okviru naredbe ili odgovora. Kriptografski kontrolni zbroj mora provjeriti primatelj.

CSM_023 Kriptografski kontrolni zbroj podataka koji se šalju naredbom moraju objediniti zaglavljem naredbe, a svi poslani podatkovni objekti (= > CLA = ‚0C', i svi podatkovni objekti moraju biti sažeti s oznakama u kojima je b1 = 1).

CSM_024 Status odziva-bajti informacije moraju biti zaštićeni kriptografskim ispitnim zbrojem kada odgovor ne sadrži podatkovno polje.

CSM_025 Kriptografski kontrolni zbroj mora imati duljinu od četiri bajta.

Struktura naredbi i odgovora prilikom korištenja sigurnih poruka je stoga sljedeća:

Korišteni DO su parcijalni skup DO za sigurne poruke opisan u ISO/IEC 7816-4:

Oznaka	Mnemonik	Značenje
‚81'	T_{pv}	Obična vrijednost ne BER-TLV šifrirani podaci (koju mora štititi CC)
‚97'	T_{LE}	Vrijednost Le u nezaštićenoj naredbi (koju mora štititi CC)
‚99'	T_{sw}	Statusne informacije (koje mora štititi CC)
‚8E'	T_{cc}	Kriptografski kontrolni zbroj
‚87'	$T_{PI\ CG}$	Bajt koji označuje popunjenje || kriptogram (obična vrijednost koja nije šifrirana u BER-TLV)

Pod pretpostavkom nezaštićenog para odziva naredbe:

Zaglavlje naredbe	Sadržaj naredbe
CLA INS P1 P2	(L_c-field) (Data field) (L_e-field)
4 bajta	Bajtovi L, označeni kao B_1 do B_L

Sadržaj odziva	Nastavak odgovora
(Podatkovno polje)	SW1 SW2
L_r podatkovnih bajtova	dva bajta

Odgovarajući par zaštićenog odziva naredbe je:

Zaštićena naredba:

Zaglavlje naredbe (CH)	Sadržaj naredbe										
CLA INS P1 P2	(Novo polje L_c)	(Novo podatkovno polje)									(Novo polje L_e)
‚0C'	Duljina novog podatkovnog polja	T_{PV}	L_{pv}	PV	T_{le}	L_{le}	L_e	T_{cc}	L_{cc}	CC	‚00'
		‚81'	L_c	Podatkovno polje	‚97'	‚01'	L_e	‚8E'	‚04'	CC	

Podaci koje treba integrirati u kontrolni zbroj = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = bajti za popunjenje (80..00) u skladu s ISO-IEC 7816-4 i metodom 2 po ISO 9797.

DO PV i LE su prisutni samo kada postoje neki odgovarajući podaci u nezaštićenoj naredbi.

Zaštićeni odgovor:

1. Slučaj kada podatkovno polje odziva nije prazno i ne treba ga zaštititi u pogledu povjerljivosti:

Sadržaj odgovora						Nastavak odgovora
(Novo podatkovno polje)						novi SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{cc}	CC	
‚81'	L_r	Podatkovno polje	‚8E'	‚04'	CC	

Podaci koje treba objediniti u kontrolni zbroj = T_{PV} || L_{PV} || PV || PB

2. Slučaj kada podatkovno polje odziva nije prazno i treba ga zaštititi u smislu povjerljivosti:

Sadržaj odgovora						Nastavak odgovora
(Novo podatkovno polje)						nova SW1 SW2
$T_{pi\ cg}$	$L_{pi\ cg}$	PI CG	T_{CC}	L_{cc}	CC	
‚87'		PI || CG	‚8E'	‚04'	CC	

Podaci koje prenosi CG: podaci koji nisu šifrirani prema BER-TLV i bajtovi popunjenja.

Podaci koje treba objediniti u kontrolni zbroj = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Slučaj kada je podatkovno polje odziva prazno:

Sadržaj odgovora						Nastavak odgovora
(Novo podatkovno polje)						nova SW1 SW2
T_{sw}	L_{sw}	SW	T_{CC}	L_{cc}	CC	
‚99'	‚02'	Nova SW1-SW2	‚8E'	‚04'	CC	

Podaci koje treba objediniti u kontrolni zbroj = T_{sw} || L_{sw} || SW || PB

5.2. **Postupanje s pogreškama kod sigurnog upućivanja poruka**

CSM_026 Kada kartica tahografa prepozna pogrešku SM prilikom tumačenja naredbe, tada se statusni bajtovi moraju vratiti bez SM. U skladu s ISO/IEC 7816-4, definirani su sljedeći statusni bajtovi za označivanje pogrešaka SM:

‚66 88' neuspješna provjera kriptografskog kontrolnog zbroja,

‚69 87' nedostaju očekivani podatkovni objekti SM,

‚69 88' neispravni podatkovni objekti SM.

CSM_027 Kada kartica tahografa vrati statusne bajte bez SM DO ili s pogrešnim SM DO, jedinica vozila mora prekinuti proces.

5.3. **Algoritmi izračuna kriptografskih kontrolnih zbrojeva**

CSM_028 Kriptografski kontrolni zbrojevi su sačinjeni korištenjem podrobnih MAC prema ANSI X9.19 s DES:

— početni stadij: početni ispitni blok y0 je E(Ka, SSC).

— naredni stadij: ispitni blokovi y1, …, yn se računaju pomoću Ka.

— konačni stadij: kriptografski kontrolni zbroj se računa od posljednjeg ispitnog bloka yn kako slijedi: E(Ka, D(Kb, yn)).

pri čemu E() označuje šifriranje pomoću DES, a D() označuje dešifriranje pomoću DES.

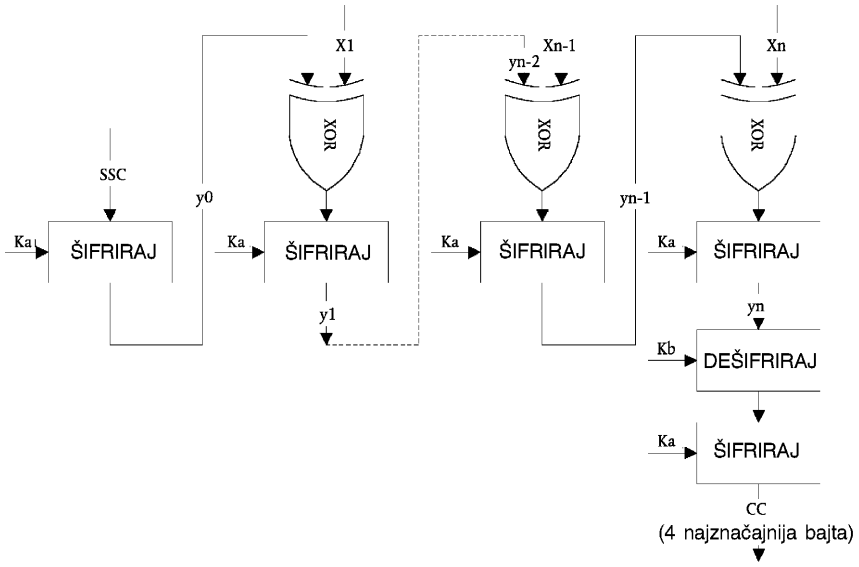
Četiri najznačajnija bajta kriptografskog kontrolnog zbroja se prenose.

CSM_029 Brojač toka slanja (SSC) se aktivira u postupku dogovaranja ključa na:

Početni SCC: Rnd3 (4 najmanje značajna bajta) || Rnd1 (4 najmanje značajna bajta).

CSM_030 Brojač toka slanja se povećava za 1 svaki put prije izračuna MAC (tj. SSC za prvu naredbu je početni SCC + 1, SCC za prvi odgovor je početni SCC + 2).

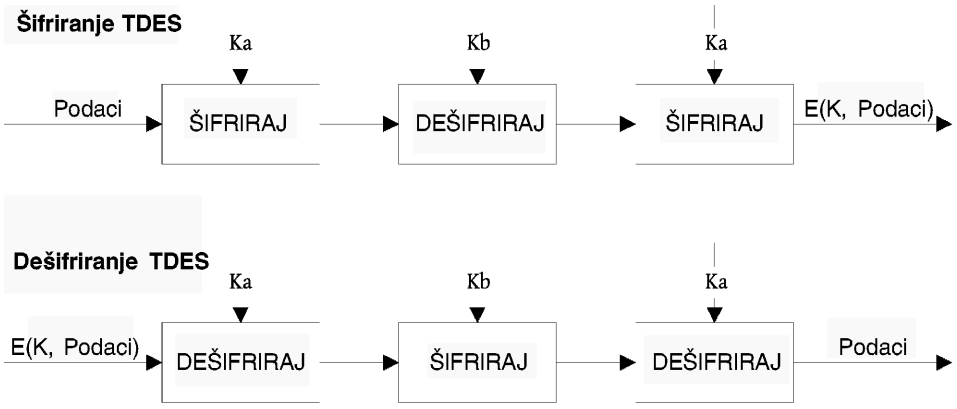
Sljedeća slika prikazuje izračun podrobnog MAC:



5.4. **Algoritam izračuna kriptograma za pouzdanost DO**

CSM_031 Kriptogrami se izračunavaju korištenjem TDEA u načinu rada TCBC u skladu s izvorima (TDES) i (TDES-OP) i s nultim vektorom kao blokom početne vrijednosti.

Sljedeća slika prikazuje korištenje ključeva u TDES:



6. MEHANIZMI DIGITALNOG POTPISA KOD PREUZIMANJA PODATAKA

CSM_032 Inteligentna namjenska oprema (IDE) pohranjuje podatke primljene s opreme (VU ili kartica) tijekom jednog procesa preuzimanja unutar jedne fizičke podatkovne datoteke. Ova datoteka mora sadržavati certifikate MS_i.C i EQT.C. Datoteka sadrži digitalne potpise podatkovnih blokova opisanih u Dodatku 7. ‚Protokoli preuzimanja podataka'.

CSM_033 Digitalni potpisi preuzetih podataka moraju koristiti shemu digitalnog potpisa s takvim dodatkom da se preuzeti podaci mogu čitati bez dešifriranja, ako se to želi.

6.1. **Generiranje potpisa**

CSM_034 Generiranje podatkovnog potpisa od strane opreme mora slijediti shemu potpisa s prilogom koji je definiran u izvoru (PKCS1) s funkcijom komprimiranja SHA-1.

Potpis = EQT.SK[‚00' || ‚01' || PS || ‚00' || DER(SHA-l(Podaci))]

PS Niz okteta za popunjenje s takvom vrijednosti ‚FF' da duljina bude 128.

DER(SHA-1(M)) je šifriranje algoritma ID za funkciju komprimiranja i vrijednost komprimiranja u vrijednosti ASN.1 tipa Digestinfo (poznata pravila šifriranja).

‚30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||03'||'02'||'lA'||'05'||'00'||'04'||'14'||vrijednost komprimiranja.

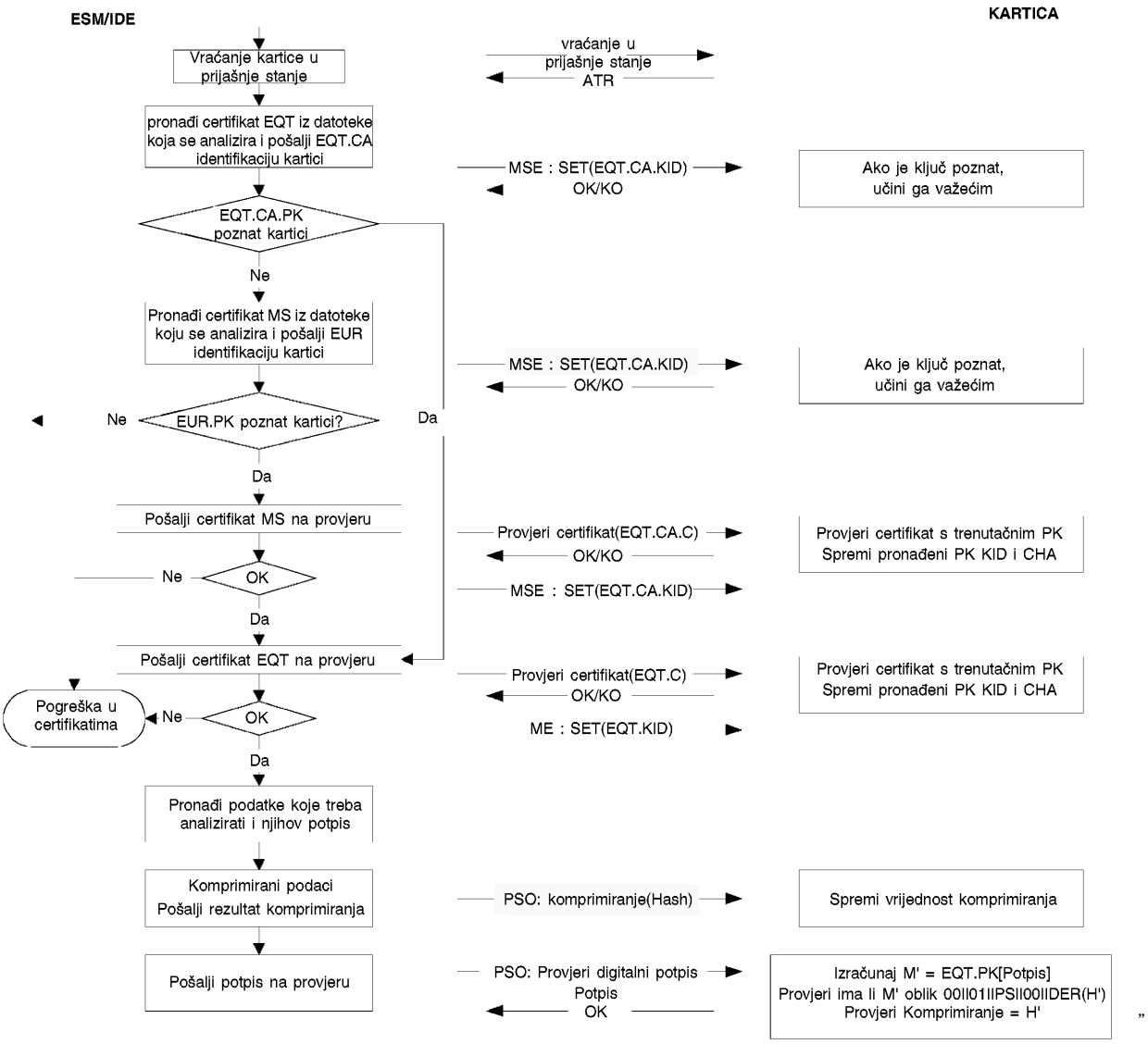
6.2. **Provjera potpisa**

CSM_035 Provjera potpisa na preuzetim podacima mora slijediti shemu potpisa s dodatkom koji je opisan u izvoru (PKCS1) s funkcijom komprimiranja SHA-1.

Verifikator mora neovisno poznavati europski javni ključ EUR.PK (i u njega imati povjerenja).

Sljedeća tablica prikazuje protokol kojega IDE koji nosi nadzornu karticu može slijediti za provjeru cjelovitosti podataka preuzetih i pohranjenih na ESM (vanjski medij za spremanje). Nadzorna kartica se koristi za dešifriranje digitalnih potpisa. U ovom slučaju takva funkcija možebitno nije ugrađena u IDE.

Oprema koja je preuzela i potpisala podatke koji se analiziraju je označena s EQT.


ESM/IDE
KARTICA
Vraćanje kartice u prijašnje stanje
vraćanje u prijašnje stanje
ATR
pronađi certifikat EQT iz datoteke koja se analizira i pošalji EQT.CA identifikaciju kartici
MSE : SET(EQT.CA.KID)
OK/KO
Ako je ključ poznat, učini ga važećim
EQT.CA.PK poznat kartici
Ne
Pronađi certifikat MS iz datoteke koju se analizira i pošalji EUR identifikaciju kartici
MSE : SET(EQT.CA.KID)
OK/KO
Ako je ključ poznat, učini ga važećim
Ne
EUR.PK poznat kartici?
Da
Da
Pošalji certifikat MS na provjeru
Provjeri certifikat(EQT.CA.C)
OK/KO
Provjeri certifikat s trenutačnim PK
Spremi pronađeni PK KID i CHA
Ne
OK
MSE : SET(EQT.CA.KID)
Da
Pošalji certifikat EQT na provjeru
Provjeri certifikat(EQT.C)
OK/KO
Provjeri certifikat s trenutačnim PK
Spremi pronađeni PK KID i CHA
Pogreška u certifikatima
Ne
OK
ME : SET(EQT.KID)
Da
Pronađi podatke koje treba analizirati i njihov potpis
Komprimirani podaci
Pošalji rezultat komprimiranja
PSO: komprimiranje(Hash)
Spremi vrijednost komprimiranja
Pošalji potpis na provjeru
PSO: Provjeri digitalni potpis
Potpis
OK
Izračunaj M' = EQT.PK[Potpis]
Provjeri ima li M' oblik 00||01||PS||00||DER(H')
Provjeri Komprimiranje = H'

„