

32002R1360

5.8.2002

URADNI LIST EVROPSKIH SKUPNOSTI

L 207/1

UREDBA KOMISIJE (ES) št. 1360/2002**z dne 13. junija 2002****o sedmi prilagoditvi Uredbe Sveta (EGS) št. 3821/85 o tahografu (nadzorni napravi) v cestnem prometu tehničnemu napredku****(Besedilo velja za EGP)**

KOMISIJA EVROPSKIH SKUPNOSTI JE

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti,

ob upoštevanju Uredbe Sveta (EGS) št. 3821/85 z dne 20. decembra 1985 o tahografu (zapisovalni napravi) v cestnem prometu ⁽¹⁾, kakor je bila nazadnje spremenjena z Uredbo (ES) št. 2135/98 ⁽²⁾, ter zlasti členov 17 in 18 uredbe,

ob upoštevanju naslednjega:

- (1) Ker je treba tehnične specifikacije Priloge I(B) k Uredbi (EGS) št. 3821/85 prilagoditi tehničnemu napredku s posebnim poudarkom na skupni varnosti sistema in interoperabilnosti med zapisovalno napravo in voznikovimi karticami.
- (2) Ker prilagoditev naprave terja tudi prilagoditev Priloge II k Uredbi (EGS) št. 3821/85, ki opredeljuje oznake in certifikate o odobritvi.
- (3) Ker odbor, ustanovljen s členom 18 Uredbe (EGS) št. 3821/85, ni dal mnenja o ukrepih, ki jih predvideva predlog, in je zato Komisija predložila Svetu predlog v zvezi s temi ukrepi.
- (4) Po izteku obdobja iz člena 18(5)(b) Uredbe (EGS) št. 3821/85 Svet ni sprejel odločitve, zato mora predlagane ukrepe sprejeti Komisija,

SPREJELA NASLEDNJO UREDBO:

Člen 1

Priloga k Uredbi (ES) št. 2135/98 se nadomesti s Prilogo k tej uredbi.

Člen 2

Priloga II k Uredbi (EGS) št. 3821/85 se spremeni:

1. Prvi odstavek točke 1 poglavja I se spremeni:
 - dogovorjena oznaka Grčije „GR“ se nadomesti s „23“,
 - dogovorjena oznaka Irske „IRL“ se nadomesti s „24“,
 - za Avstrijo se doda dogovorjena oznaka „12“,
 - za Finsko se doda dogovorjena oznaka „17“,
 - za Švedsko se doda dogovorjena oznaka „5“,
2. Drugi odstavek točke 1 poglavja I se spremeni:
 - za besedilom „tahografskega vložka“ se doda besedilo „ali tahografske kartice“.
3. Točka 2 Poglavja I se spremeni:
 - za besedilom „na vsakem tahografskem vložku“ se doda besedilo „in na vsaki tahografski kartici“.
4. V poglavju II se naslovu doda naslednje besedilo „ZA IZDELKE, SKLADNE S PRILOGO I“.

⁽¹⁾ UL L 370, 31.12.1985, str. 8.⁽²⁾ UL L 274, 9.10.1998, str. 1.

5. Doda se naslednje Poglavje III:

„III. CERTIFIKAT O ODOBRTVI ZA IZDELKE, SKLADNE S PRILOGO I B

Država, ki je izdala odobritev, mora vlagatelju izdati certifikat o odobritvi, katerega vzorec je dan spodaj. Pri obveščanju drugih držav članic o izdanih odobritvah ali po potebi o umiku odobritve, mora država članica uporabiti kopije tega certifikata.

CERTIFIKAT O ODOBRTVI ZA IZDELKE, SKLADNE S PRILOGO I B

Ime pristojne uprave

Uradno obvestilo o ⁽³⁾:

- ☐ odobritvi
- ☐ umiku odobritve
- ☐ modelu zapisovalne naprave
- ☐ sestavnem delu zapisovalne naprave ⁽⁴⁾
- ☐ voznikovi kartici
- ☐ delavniški kartici
- ☐ kartici podjetja
- ☐ nadzornikovi kartici.

Odobritev št.

1. Proizvajalčeva ali blagovna znamka:
2. Ime modela
3. Ime proizvajalca
4. Naslov proizvajalca
5. Predloženo v odobritev za
6. Laboratorij(-i)
7. Datum in število preskusov
8. Datum odobritve
9. Datum umika odobritve
10. Model dela(-ov) zapisovalne naprave, s katerim je sestavni del zasnovan za uporabo
11. Kraj
12. Datum
13. Priloženi opisni dokumenti
14. Opombe (vključno z mesti morabitnih pečatov)

(podpis)

⁽³⁾ Označite ustrezna okenca.

⁽⁴⁾ Navedite sestavni del, ki ga obravnava uradno obvestilo.“

Člen 3

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropskih skupnosti*.

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

V Bruslju, 13. junija 2002

Za Komisijo
Loyola DE PALACIO
Podpredsednica

PRILOGA

„PRILOGA I B

ZAHTEVE GLEDE IZDELAVE, PRESKUŠANJA, NAMESTITVE IN KONTROLE

VSEBINA

I.	OPREDELITVE POJMOV	286
II.	SPLOŠNE ZNAČILNOSTI IN FUNKCIJE ZAPISOVALNE NAPRAVE	290
1.	Splošne značilnosti	290
2.	Funkcije	290
3.	Režimi delovanja	291
4.	Varnost	292
III.	ZAHTEVE GLEDE IZDELAVE IN FUNKCIONALNE ZAHTEVE ZA ZAPISOVALNO NAPRAVO	292
1.	Spremljanje vstavljanja in izvlečenja kartic	292
2.	Merjenje hitrosti in razdalj	292
2.1	Merjenje prevožene razdalje	293
2.2	Merjenje hitrosti	293
3.	Merjenje časa	293
4.	Spremljanje vztrajnosti dejavnosti	294
5.	Spremljanje stanja vožnje	294
6.	Voznikovi ročni vnosi	294
6.1	Vnos krajev, v katerih se dnevne delovne izmene začnejo in/ali končajo	294
6.2	Ročni vnos vztrajnosti dejavnosti	294
6.3	Vnos posebnih stanj	296
7.	Upravljanje blokad s strani podjetja	296
8.	Spremljanje nadzornih dejavnosti	296
9.	Zaznavanje dogodkov in/ali napak	296
9.1	Dogodek ‚vstavev neveljavne kartice‘	296
9.2	Dogodek ‚navzkrižje med karticami‘	297
9.3	Dogodek ‚časovno prekrivanje‘	297
9.4	Dogodek ‚vožnja brez ustrezne kartice‘	297
9.5	Dogodek ‚vstavev kartice med vožnjo‘	297
9.6	Dogodek ‚zadnja seja s kartico nepravilno zaključena‘	297
9.7	Dogodek ‚prekoračitev hitrosti‘	297

9.8	Dogodek ‚izpad napajanja‘	298
9.9	Dogodek ‚napaka v podatkih o gibanju‘	298
9.10	Dogodek ‚poskus kršenja varnosti‘	298
9.11	Napaka ‚kartica‘	298
9.12	Napaka ‚zapisovalna naprava‘	298
10.	Vgrajeni preskusi in preskusi lastnega delovanja	298
11.	Branje iz pomnilnika podatkov	298
12.	Zapisovanje in hranjenje podatkov v pomnilniku podatkov	299
12.1	Identifikacijski podatki naprave	299
12.1.1	Identifikacijski podatki enote na vozilu	299
12.1.2	Identifikacijski podatki zaznavala gibanja	299
12.2	Varnostni elementi	300
12.3	Podatki o vstavljanju in izvlačenju voznikove kartice	300
12.4	Podatki o voznikovih dejavnostih	301
12.5	Kraji, v katerih se dnevne delovne izmene začenejo in/ali končajo	301
12.6	Podatki števca prevožene poti	301
12.7	Podrobni podatki o hitrosti	301
12.8	Podatki o dogodkih	301
12.9	Podatki o napakah	303
12.10	Kalibracijski podatki	304
12.11	Podatki o nastavljanju časa	304
12.12	Podatki o nadzornih dejavnostih	304
12.13	Podatki o blokadah s strani podjetja	305
12.14	Podatki o prenosih podatkov v naprave	305
12.15	Podatki o posebnih stanjih	305
13.	Branje s tahografskih kartic	305
14.	Zapisovanje in hranjenje podatkov na tahografskih karticah	305
15.	Prikazovanje	306
15.1	Privzeti prikaz	306
15.2	Opozorilni prikaz	307
15.3	Dostop do menijev	307
15.4	Drugi prikazi	307
16.	Tiskanje	307
17.	Opozorila	308
18.	Prenos podatkov na zunanje medije	309
19.	Iznos podatkov na dodatne zunanje naprave	309
20.	Kalibriranje	310
21.	Nastavljanje časa	310

22.	Delovne karakteristike	310
23.	Gradiva	310
24.	Oznake	311
IV.	ZAHTEVE GLEDE IZDELAVE IN FUNKCIONALNE ZAHTEVE ZA TAHOGRAFSKE KARTICE	311
1.	Vidni podatki	311
2.	Varnost	314
3.	Standardi	314
4.	Okoljske in električne tehnične zahteve	314
5.	Hranjenje podatkov	314
5.1	Identifikacijski podatki kartice in varnostni podatki	315
5.1.1	Identifikacija aplikacije	315
5.1.2	Identifikacija čipa	315
5.1.3	Identifikacija kartice s tiskanim vezjem	315
5.1.4	Varnostni elementi	315
5.2	Voznikova kartica	315
5.2.1	Identifikacija kartice	315
5.2.2	Identifikacija imetnika kartice	316
5.2.3	Podatki o vozniskem dovoljenju	316
5.2.4	Podatki o uporabljenih vozilih	316
5.2.5	Podatki o voznikovih dejavnostih	316
5.2.6	Kraji, v katerih se dnevne delovne izmene začenjajo in/ali končajo	317
5.2.7	Podatki o dogodkih	317
5.2.8	Podatki o napakah	318
5.2.9	Podatki o nadzornih dejavnostih	318
5.2.10	Podatki o sejah s kartico	318
5.2.11	Podatki o posebnih stanjih	318
5.3	Delavniška kartica	319
5.3.1	Varnostni elementi	319
5.3.2	Identifikacija kartice	319
5.3.3	Identifikacija imetnika kartice	319
5.3.4	Podatki o uporabljenih vozilih	319
5.3.5	Podatki o voznikovih dejavnostih	319
5.3.6	Podatki o začetkih in/ali zaključkih dnevnih delovnih izmen	319
5.3.7	Podatki o dogodkih in napakah	319
5.3.8	Podatki o nadzornih dejavnostih	319
5.3.9	Podatki o kalibriranju in nastavljanju časa	320
5.3.10	Podatki o posebnih stanjih	320
5.4	Nadzorna kartica	320

5.4.1	Identifikacija kartice	320
5.4.2	Identifikacija imetnika kartice	320
5.4.3	Podatki o nadzornih dejavnostih	320
5.5	Kartica podjetja	321
5.5.1	Identifikacija kartice	321
5.5.2	Identifikacija imetnika kartice	321
5.5.3	Podatki o dejavnostih podjetja	321
V.	NAMESTITIV ZAPISOVALNE NAPRAVE	321
1.	Namestitev	321
2.	Namestitvena ploščica	322
3.	Plombiranje	322
VI.	PREVERJANJA, KONTROLE IN POPRAVILA	323
1.	Odobritev izvajalcev ali delavnic	323
2.	Preverjanje novih in popravljenih instrumentov	323
3.	Pregled namestitve	323
4.	Redne kontrole	323
5.	Meritve pogreškov	324
6.	Popravlila	324
VII.	IZDAJANJE KARTIC	324
VIII.	ODOBRITEV TIPA ZAPISOVALNE NAPRAVE IN TAHOGRAFSKIH KARTIC	324
1.	Splošno	324
2.	Varnostni certifikat	325
3.	Funkcionalni certifikat	325
4.	Certifikat skupne uporabnosti	325
5.	Certifikat odobritve tipa	326
6.	Izjemni postopek: prvi preskusi skupne uporabnosti	326
Dodatek 1.	Slovar podatkov	
Dodatek 2.	Tehnični podatki tahografskih kartic	
Dodatek 3.	Grafični znaki	
Dodatek 4.	Izpisi	
Dodatek 5.	Prikaz	
Dodatek 6.	Zunanji vmesniki	
Dodatek 7.	Protokol prenosa podatkov v naprave	
Dodatek 8.	Protokol kalibriranja	
Dodatek 9.	ODOBRITEV TIPA — SEZNAM OBVEZNIH PRESKUSOV	
Dodatek 10.	GENERIČNI VARNOSTNI CILJI	
Dodatek 11.	SKUPNI VARNOSTNI MEHANIZMI	

I. OPREDELITVE POJMOV

V tej prilogi

(a) **„aktiviranje“ pomeni:**

fazo, v kateri se vzpostavijo polna delovna sposobnost zapisovalne naprave in vse funkcije, vključno z varnostnimi funkcijami,

Za aktiviranje zapisovalne naprave sta potrebna uporaba delavniške kartice in vpis gesla PIN,

(b) **„avtentifikacija“ pomeni:**

funkcijo, namenjeno ugotavljanju in preverjanju priglašene identitete,

(c) **„avtentičnost“ pomeni:**

lastnost, da informacija prihaja od vira, katerega identiteto je mogoče preveriti,

(d) **„vgrajeni preskus“ (BIT) pomeni:**

preskuse, ki se izvedejo na zahtevo, sproži pa jih operater ali zunanja oprema,

(e) **„koledarski dan“ pomeni:**

dan, ki se začne ob uri 00.00 in traja do ure 24.00. Vsi koledarski dnevi so vezani na čas UTC (usklajeni svetovni čas),

(f) **„kalibriranje“ pomeni:**

posodobitev ali potrditev parametrov vozila, ki se hranijo v pomnilniku podatkov. Parametri vozila obsegajo identifikacijo vozila (VIN, VRM in državo članico, v kateri je vozilo registrirano) in značilnosti vozila (w, k, l, dimenzije avtoplaščev, nastavitve naprave za omejevanje hitrosti (če obstaja), tekoči čas UTC, tekočo vrednost števca prevožene poti),

za kalibriranje zapisovalne naprave je potrebna delavniška kartica,

(g) **„številka kartice“ pomeni:**

niz 16 alfanumeričnih znakov, ki nedvoumno identificira tahografsko kartico v državi članici. Številka kartice obsega zaporedno tekočo številko (če obstaja), tekočo številko zamenjave in tekočo številko obnove,

kartica je zato nedvoumno identificirana s kodo države izdajateljice in številko kartice,

(h) **„zaporedna tekoča številka kartice“ pomeni:**

štirinajsti alfanumerični znak v številki kartice, ki služi za razlikovanje med karticami, izdanimi podjetju, ki je upravičeno do prejema več tahografskih kartic. Podjetje ali organ nedvoumno identificira prvih 13 znakov številke kartice,

(i) **„zaporedna številka obnove kartice“ pomeni:**

šestnajsti alfanumerični znak v številki kartice, ki se poveča za eno ob vsaki obnovi tahografske kartice,

(j) **„zaporedna številka zamenjave kartice“ pomeni:**

petnajsti alfanumerični znak v številki kartice, ki se poveča za eno ob vsaki zamenjavi tahografske kartice,

(k) **„značilni koeficient vozila“ pomeni:**

številsko karakteristiko, ki pomeni vrednost signala, ki ga odda del vozila, s katerim je povezana zapisovalna naprava (izhodna gred menjalnika ali pogonska gred kolesa), med tem ko vozilo prevozi razdaljo enega kilometra pri standardnih preskusnih pogojih (glej poglavje VI(5)). Značilni koeficient je izražen v impulzih na kilometer ($w = \dots \text{imp/km}$),

(l) **„kartica podjetja“ pomeni:**

tahografsko kartico, ki jo organi države članice izdajo lastniku ali imetniku vozil, opremljenih z zapisovalno napravo,

kartica podjetja identificira podjetje in omogoča prikaz, prenos podatkov v napravo in izpis podatkov, shranjenih v zapisovalni napravi, ki jo je blokiralo to podjetje,

(m) **„konstanta zapisovalne naprave“ pomeni:**

številčno značilnost, ki podaja vrednost vhodnega signala, potrebno za prikaz in zapis prevožene razdalje enega kilometra; ta konstanta se izraža v impulzih na kilometer ($k = \dots \text{imp/km}$),

(n) **„čas neprekinjene vožnje“ izračuna zapisovalna naprava kot ⁽¹⁾:**

čas neprekinjene vožnje se izračuna kot dosednji skupni čas vožnje določenega voznika od konca njegovega zadnjega obdobja RAZPOLOŽLJIVOSTI, obdobja ODMORA/POČITKA ali NEZNANEGA ⁽²⁾ obdobja, daljšega od 45 minut (to obdobje je bilo lahko razdeljeno v več obdobjih, dolgih 15 minut ali več). V izračunu se po potrebi upoštevajo pretekle dejavnosti, shranjene v voznikovi kartici. Če voznik ni vstavil svoje kartice, izračun temelji na zapisih v pomnilniku podatkov za sedanje obdobje, ko v ustrezni reži ni vstavljena nobena kartica,

(o) **„nadzorna kartica“ pomeni:**

tahografsko kartico, ki jo organ države članice izda nacionalnemu organu, pristojnemu za nadzor,

nadzorna kartica identificira nadzorni organ in morda nadzornega referenta ter omogoča dostop do podatkov, shranjenih v pomnilniku podatkov ali na voznikovi kartici za branje, izpis in/ali prenos,

(p) **„skupni čas odmorov“ izračuna zapisovalna naprava kot ⁽¹⁾:**

skupni čas odmorov od vožnje določenega voznika se izračuna kot dosednji skupni čas obdobjih RAZPOLOŽLJIVOSTI, obdobjih ODMOROV/POČITKOV ali NEZNANIH ⁽²⁾ obdobjih, dolgih 15 minut ali več, od konca njegovega zadnjega obdobja RAZPOLOŽLJIVOSTI, obdobja ODMORA/POČITKA ali NEZNANEGA ⁽²⁾ obdobja, ki je trajalo 45 minut ali (to obdobje je bilo lahko razdeljeno v več obdobjih, dolgih 15 minut ali več).

V izračunu se po potrebi upoštevajo pretekle dejavnosti, shranjene v voznikovi kartici. Ne upoštevajo se morebitna neznana obdobja negativnega trajanja (čas začetka neznanega obdobja > čas konca neznanega obdobja) zaradi časovnega prekrivanja med dvema različnima zapisovalnima napravama.

Če voznik ni vstavil svoje kartice, izračun temelji na zapisih v pomnilniku podatkov za sedanje obdobje, ko v ustrezni reži ni vstavljena nobena kartica,

(q) **„pomnilnik podatkov“ pomeni:**

elektronsko napravo za hranjenje podatkov, vgrajeno v zapisovalno napravo,

(r) **„digitalni podpis“ pomeni:**

podatke, dodane bloku podatkov, ali kriptografsko transformacijo tega bloka podatkov, ki omogočajo prejemniku dokazati avtentičnost in celovitost bloka podatkov,

(s) **„prenos podatkov v napravo“ pomeni:**

kopiranje, skupaj z digitalnim podpisom, dela ali celote niza podatkov shranjenih v pomnilniku podatkov vozila ali v pomnilniku tahografske kartice,

pri prenosu se noben shranjeni podatek ne sme spremeniti ali zbrisati,

⁽¹⁾ Ta način izračuna časa neprekinjene vožnje in skupnega časa odmorov služi za to, da zapisovalna naprava izračuna podatke za opozorilo o prekoračitvi časa neprekinjene vožnje. Ne služi kot podlaga za pravno razlago teh časov.

⁽²⁾ NEZNANO obdobje pomeni obdobje, v katerem voznikova kartica ni vstavljena v zapisovalno napravo in za katero ni nikakršnega ročnega vnosa voznikove dejavnosti.

(t) **‚voznikova kartica‘ pomeni:**

tahografsko kartico, ki jo organ države članice izda določenemu vozniku,

voznikova kartica identificira voznika in omogoča hranjenje podatkov o voznikovih dejavnostih,

(u) **‚efektivni obseg avtoplaščev‘ pomeni:**

povprečje razdalj, ki jih prevozijo vsa posamezna pogonska kolesa vozila (kolesa, ki premikajo vozilo) med enim polnim obratom. Merjenje teh razdalj se opravlja pri standardnih preskusnih pogojih (poglavje VI(5)), rezultati so izraženi kot „l = ... mm“. Proizvajalec vozila lahko nadomesti merjenje teh razdalj s teoretičnim izračunom, v katerem upošteva porazdelitev mase med osmi pri praznem in na vožnjo pripravljenem vozilu ⁽¹⁾. Metodo takega teoretičnega izračuna odobri pristojni organ države članice,

(v) **‚dogodek‘ pomeni:**

nenormalno delovanje, ki ga zazna zapisovalna naprava, katerega vzrok je lahko poskus zlorabe,

(w) **‚napaka‘ pomeni:**

nenormalno delovanje, ki ga zazna zapisovalna naprava, katerega vzrok je lahko nepravilno delovanje ali odpoved opreme,

(x) **‚namestitev‘ pomeni:**

vgradnjo zapisovalne naprave v vozilo,

(y) **‚zaznavalo gibanja‘ pomeni:**

del zapisovalne naprave, ki daje signal, ustrezajoč hitrosti in/ali prevoženi poti vozila,

(z) **‚neveljavna kartica‘ pomeni:**

kartico, ki je zaznana kot kartica z napako ali pri kateri začetna avtentifikacija ni bila uspešno kočana ali kateri se veljavnost še ni začela ali pa je že potekla,

(aa) **‚zunaj področja veljavnosti‘ pomeni:**

stanje, v katerem po določbah Uredbe Sveta (EGS) št. 3820/85 uporaba zapisovalne naprave ni potrebna,

(bb) **‚prekoračitev hitrosti‘ pomeni:**

prekoračitev odobrene najvišje hitrosti vozila, opredeljeno kot poljubno več kakor 60 sekund dolgo obdobje, v katerem izmerjena hitrost vozila presega omejitve, nastavljeno na napravi za omejevanje hitrosti vozila, ki jo določa Direktiva Sveta 92/6/EGS z dne 10. februarja 1992 o namestitvi in uporabi naprav za omejevanje hitrosti pri nekaterih kategorijah motornih vozil v Skupnosti ⁽²⁾,

(cc) **‚redna kontrola‘ pomeni:**

skupek del, opravljenih za preveritev, ali zapisovalna naprava deluje pravilno in ali njene nastavitve ustrezajo parametrom vozila,

(dd) **‚tiskalnik‘ pomeni:**

del zapisovalne naprave, ki služi za izpisovanje shranjenih podatkov,

(ee) **‚zapisovalna naprava‘ pomeni:**

vso opremo, ki se namesti v vozila za avtomatsko ali polavtomatsko prikazovanje, zapisovanje in hranjenje podatkov o gibanju teh vozil in o določenih delovnih obdobjih njihovih voznikov,

⁽¹⁾ Direktiva 97/27/ES z dne 22. julija 1997 o masah in dimenzijah nekaterih kategorij motornih vozil in njihovih priklopnikov ter o spremembi Direktive 70/156/EGS (UL L 233, 25.8.1997, str. 1).

⁽²⁾ UL L 57, 2.3.1992, str. 27.

(ff) **„obnovitev“ pomeni:**

izdajo nove tahografske kartice, ko obstoječi tahografski kartici poteče veljavnost ali ne deluje pravilno in je vrnjena pristojnemu izdajatelju. Pri obnovitvi kartice je z gotovostjo znano, da ne obstajata hkrati dve veljavni kartici,

(gg) **„popravilo“ pomeni:**

kakršno koli popravilo zaznavala gibanja ali enote v vozilu, pri katerem je potreben odklop napajanja, odklop od drugih delov zapisovalne naprave ali odpiranje,

(hh) **„zamenjava“ pomeni:**

izdaja tahografske kartice za nadomestitev obstoječe kartice, ki je bila prijavljena kot izgubljena, ukradena ali nepravilno delujoča in ni bila vrnjena pristojnemu izdajatelju. Z zamenjavo kartice je vedno povezano tveganje hkratnega obstoja dveh veljavnih kartic,

(ii) **„varnostno certificiranje“ pomeni:**

proces certificiranja, ki ga opravi certifikacijski organ ITSEC ⁽¹⁾, za zagotovitev, da obravnavana zapisovalna naprava (ali njen del) ali tahografska kartica izpolnjuje varnostna merila, opredeljena v dodatku 10, „Generični varnostni cilji“,

(jj) **„samopreskus“ pomeni:**

preskuse, ki jih zapisovalna naprava ciklično in avtomatsko izvaja za ugotavljanje napak,

(kk) **„tahografska kartica“ pomeni:**

pametno kartico, namenjeno za uporabo z zapisovalno napravo. Tahografska kartica omogoča na zapisovalni napravi ugotavljati identiteto (ali identifikacijsko skupino) imetnika kartice in omogoča prenos ter hranjenje podatkov. Tipi tahografskih kartic so:

— voznikova kartica;

— nadzorna kartica;

— delavniška kartica;

— kartica podjetja,

(ll) **„odobritev tipa“ pomeni:**

proces, s katerim država članica potrdi, da obravnavana zapisovalna naprava (ali sestavni del) ali tahografska kartica izpolnjuje zahteve te uredbe,

(mm) **„mere avtoplašča“ pomenijo:**

oznako mer avtoplašča (zunanjih vozniških koles) v skladu z Direktivo 92/23/EGS z dne 31. marca 1992 ⁽²⁾,

(nn) **„identifikacija vozila“ pomeni:**

števila, ki identificirajo vozilo: registrsko številko vozila (VRN) z oznako države, v kateri je vozilo registrirano, in identifikacijsko številko vozila (VIN) ⁽³⁾,

(oo) **„enota v vozilu (VU)“ pomeni:**

zapisovalno napravo, razen zaznavala gibanja in povezovalnih kablov zaznavala gibanja. Enota v vozilu je lahko ena sama enota ali več enot, porazdeljenih po vozilu, če le izpolnjuje varnostne zahteve te uredbe,

⁽¹⁾ Priporočilo Sveta 95/144/ES z dne 7. aprila 1995 o skupnih merilih vrednotenja varnosti informacijske tehnologije (UL L 93, 26.4.1995, str. 27).

⁽²⁾ UL L 129, 14.5.1992, str. 95.

⁽³⁾ Direktiva 76/114/EGS z dne 18. decembra 1975 o približevanju zakonodaje držav članic v zvezi s predpisanimi tablicami in napisi za motorna vozila in njihove priklopneke, njihov položaj in način pritrditve (UL L 24, 30.1.1976, str. 1).

(pp) **v izračunih, ki jih opravlja zapisovalna naprava, 'teden' pomeni:**

obdobje od časa 00.00 UTC v ponedeljek do časa 24.00 UTC v nedeljo,

(qq) **'delavniška kartica' pomeni:**

tahografsko kartico, ki jo organ države članice izda proizvajalcu zapisovalne naprave, proizvajalcu vozil ali delavnic, odobrenim v navedeni državi članici.

Delavniška kartica identificira imetnika in omogoča preskušanje, kalibriranje in/ali prenos podatkov v zapisovalno napravo,

II. SPLOŠNE ZNAČILNOSTI IN FUNKCIJE ZAPISOVALNE NAPRAVE

000 Vsako vozilo, opremljeno z zapisovalno napravo v skladu z določbami te priloge mora biti opremljeno s prikazovalnikom hitrosti in števcem prevožene poti. Ti funkciji sta lahko vključeni v zapisovalno napravo.

1. Splošne značilnosti

Naloge zapisovalne naprave so zapisovanje, hranjenje, prikaz, tiskanje in iznos podatkov povezanih z voznikovimi dejavnostmi.

001 Zapisovalna napravo obsega kable, zaznavalo gibanja in enoto v vozilu.

002 Enota v vozilu obsega procesno enoto, pomnilnik za podatke, uro realnega časa, dve vmesniški napravi za pametne kartice (voznikovo in sovoznikovo), tiskalnik, prikazovalnik, enoto za vizualno opozarjanje, konektor za kalibriranje/prenos podatkov in priprave za uporabnikovo vnašanje podatkov.

Zapisovalna naprava je lahko z dodatnimi konektorji povezana tudi z drugimi napravami.

003 Nobena odobrena ali neodobrena vključitev v zapisovalno napravo ali priključitev nanjo kakršne koli funkcije ali ene naprave ali več ne sme posegati ali odpreti možnosti za poseganje v pravilno in varno delovanje zapisovalne naprave ali kršiti določb te uredbe.

Uporabniki zapisovalne naprave se identificirajo napravi s tahografskimi karticami.

004 Zapisovalna naprava omogoča uporabniku selektiven dostop do podatkov in funkcij glede na tip in/ali identiteto uporabnika. Zapisovalna naprava zapisuje in hrani podatke v svojem pomnilniku podatkov in na tahografske kartice.

To poteka v skladu z Direktivo 95/46/ES z dne 24. oktobra 1995 o zaščiti posameznika pri obdelavi osebnih podatkov in o prostem pretoku teh podatkov ⁽¹⁾.

2. Funkcije

005 Zapisovalna naprava mora zagotavljati naslednje funkcije:

- spremljanje vstavljanja in izvlečenja kartic,
- merjenje hitrosti in razdalj,
- merjenje časa,
- spremljanje voznikovih dejavnosti,
- spremljanje stanja vožnje,
- voznikove ročne vnose:
 - vnos krajev, v katerih se dnevne delovne izmene začnejo in/ali zaključijo,
 - ročni vnos voznikovih dejavnosti,
 - vnos posebnih stanj,

⁽¹⁾ UL L 281, 23.11.1995, str. 31.

- upravljanje blokad s strani podjetja,
- spremljanje nadzornih dejavnosti,
- zaznavanje dogodkov in/ali napak,
- vgrajeni preskusi in preskusi lastnega delovanja,
- branje iz pomnilnika podatkov,
- zapisovanje in hranjenje v pomnilniku podatkov,
- branje s tahografskih kartic,
- zapisovanje in shranjevanje na tahografske kartice,
- prikazovanje,
- tiskanje,
- opozarjanje,
- prenos podatkov na zunanje medije,
- iznos podatkov na dodatne zunanje naprave,
- kalibriranje,
- nastavljanje časa.

3. Režimi delovanja

006 Zapisovalna naprava mora imeti štiri režime delovanja:

- delovni režim,
- nadzorni režim,
- režim kalibriranja,
- režim dela v podjetju.

007 Zapisovalna naprava se mora preklopiti v naslednji režim delovanja glede na veljavni tahografski kartici, vstavljeni v vmesniških napravah za kartice.

Režim delovanja		Voznikova reža				
		Brez kartice	Voznikova kartica	Nadzorna kartica	Delavniška kartica	Kartica podjetja
Sovoznikova reža	Brez kartice	Delovni	Delovni	Nadzorni	Kalibriranje	Dela v podjetju
	Voznikova kartica	Delovni	Delovni	Nadzorni	Kalibriranje	Dela v podjetju
	Nadzorna kartica	Nadzorni	Nadzorni	Kontrolni Nadzorni (*)	Delovni	Delovni
	Delavniška kartica	Kalibriranje	Kalibriranje	Delovni	Kalibriranje (*)	Delovni
	Kartica podjetja	Dela v podjetju	Dela v podjetju	Delovni	Delovni	Dela v podjetju (*)

008 (*) V teh stanjih mora zapisovalna naprava uporabljati le tahografsko kartico v voznikovi reži.

- 009 Zapisovalna naprava mora ignorirati vstavljene neveljavne kartice; mogoče mora biti le prikazovanje, tiskanje ali prenos podatkov, shranjenih na kartici s pretečeno veljavnostjo.
- 010 Vse funkcije, naštetje v točki II.2, morajo delovati v katerem koli režimu delovanja; pri tem veljajo naslednje izjeme:
- funkcija kalibriranja je dosegljiva le v režimu kalibriranja,
 - možnosti funkcije nastavljanja časa so omejene, kadar oprema ni v režimu kalibriranja,
 - funkcije voznikovega ročnega vnosa so dosegljive le v delovnem režimu in režimu kalibriranja,
 - funkcija upravljanja blokad s strani podjetja je dosegljiva le v režimu del v podjetju,
 - funkcija spremljanja nadzornih dejavnosti deluje le v nadzornem režimu,
 - funkcija prenosa podatkov ni dosegljiva v delovnem režimu (razen kakor določa zahteva št. 150).
- 011 Zapisovalna naprava lahko iznaša katere koli podatke na prikazovalnik, tiskalnik ali vmesnike za zunanje naprave; pri tem veljajo naslednje izjeme:
- v delovnem režimu mora biti zbrisan vsak osebni identifikacijski podatek (priimek in ime(-na)), različen od teh podatkov na vstavljeni tahografski kartici, in delno zbrisana (zbrisana vsaka liha številka od leve proti desni) številka kartice, različna od vstavljene tahografske kartice,
 - v režimu del v podjetju je možno iznašanje podatkov povezanih z voznikom (zahteve št. 081, 084 in 087) le za obdobja, ki niso blokirana s strani kakega drugega podjetja (ki se identificira s prvimi 13 števki številke kartice podjetja),
 - kadar v zapisovalno napravo ni vstavljena nobena kartica, je mogoče podatke povezane z voznikom iznašati le za tekoči dan in za zadnjih osem koledarskih dni.

4. Varnost

Cilji varnosti sistema so zaščita pomnilnika podatkov s tem, da preprečuje nepooblaščen dostop do podatkov in nepooblaščen manipuliranje z njimi ter da zaznava poskuse takih posegov, zaščita celovitosti in avtentičnosti podatkov, izmenjanih med zaznavanjem gibanja in enoto v vozilu, zaščita celovitosti in avtentičnosti podatkov, izmenjanih med zapisovalno opremo in tahografskimi karticami, in preverjanje celovitosti in avtentičnosti prenesenih podatkov.

- 012 Za zagotovitev varnosti sistema mora zapisovalna naprava izpolnjevati varnostne zahteve, določene v generičnih varnostnih ciljih za zaznavanje gibanja in enoto v vozilu (dodatek 10).

III. ZAHTEVE GLEDE IZDELAVE IN FUNKCIONALNE ZAHTEVE ZA ZAPISOVALNO NAPRAVO

1. Spremljanje vstavljanja in izvlečenja kartic

- 013 Zapisovalna naprava mora spremljati stanje vmesniških naprav za kartice, da zazna vstavitve in izvleke kartic.
- 014 Po vstavitvi kartice mora zapisovalna naprava ugotoviti, ali je vstavljena kartica veljavna tahografska kartica, in če je, identificirati tip kartice.
- 015 Zapisovalna naprava mora biti projektirana tako, da se po pravilni vstavitvi tahografske kartice v vmesniško napravo za kartice ta zaskoči v vstavljenem položaju.
- 016 Sprostitev tahografskih kartic mora biti mogoča le, ko se vozilo ustavi in so na kartici že shranjeni potrebni podatki. Za sprostitve kartice mora biti potreben aktivni poseg uporabnika.

2. Merjenje hitrosti in razdalj

- 017 Ta funkcija mora neprekinjeno meriti in po potrebi posredovati vrednost števca, ustrezajočo celotni prevoženi poti vozila.
- 018 Ta funkcija mora neprekinjeno meriti in po potrebi posredovati vrednost hitrosti vozila.

- 019 Funkcija merjenja hitrosti mora posredovati tudi podatek, ali se vozilo premika ali pa je ustavljeno. Da se vozilo premika, velja, kakor hitro funkcija prejema od zaznavala gibanja več kakor 1 imp/s najmanj pet sekund zaporedoma; drugače velja, da je vozilo ustavljeno.

Napravi za prikaz hitrosti (merilnik hitrosti) in celotne prevožene poti (števec prevožene poti) vgrajeni v vozilo, opremljeno z zapisovalno napravo v skladu z določbami te uredbe, morata biti v skladu z zahtevami glede največjih dopustnih pogreškov, določenih v tej prilogi (poglavji III(2)(1) in III(2)(2)).

2.1 Merjenje prevožene razdalje

- 020 Prevožena razdalja se lahko meri na enega od naslednjih načinov:
- s seštevanjem vseh premikov vozila naprej in nazaj, ali
 - z upoštevanjem samo premikov vozila naprej.
- 021 Zapisovalna naprava mora meriti razdalje v območju od 0 do 9 999 999,9 km.
- 022 Razdalja mora biti izmerjena v naslednjih dopustnih mejah (razdalje najmanj 1 000 m):
- $\pm 1\%$ pred namestitvijo,
 - $\pm 2\%$ ob namestitvi in ob rednih kontrolah,
 - $\pm 4\%$ med uporabo.

- 023 Razdalja mora biti merjena z ločljivostjo enako ali boljšo od 0,1 km.

2.2 Merjenje hitrosti

- 024 Zapisovalna naprava mora meriti hitrosti v območju od 0 do 220 km/h.
- 025 Za zagotovitev največjega dopustnega pogreška prikazane hitrosti ± 6 km/h med uporabo in ob upoštevanju:
- največjega dopustnega pogreška ± 2 km/h zaradi odstopanj vhodnih podatkov (odstopanja avtoplaščev, ...),
 - največjega dopustnega pogreška merjenj ± 1 km/h med nameščanjem in ob rednih kontrolah,
- mora zapisovalna naprava pri hitrostih med 20 in 180 km/h in pri značilnih koeficientih vozila med 4 000 in 25 000 imp/km meriti hitrost v okviru največjega dopustnega pogreška ± 1 km/h (pri stalni hitrosti).

Opomba: Ločljivost pomnilnika podatkov vnese v podatke o hitrosti, ki jih hrani zapisovalna naprava, še dodatni največji dopustni pogrešek $\pm 0,5$ km/h.

- 025a V 2 sekundah po končani spremembi hitrosti do 2 m/s² mora biti hitrost spet merjena pravilno in v okviru normalnih-največjih dopustnih pogreškov.
- 026 Hitrost mora biti merjena z ločljivostjo enako ali boljšo od 1 km/h.

3. Merjenje časa

- 027 Funkcija merjenja časa mora meriti čas neprekinjeno in posredovati UTC čas in datum v digitalni obliki.
- 028 Pri vseh dejavnostih z zapisovalno napravo, pri katerih nastopa čas (zapisovanju, tiskanju, izmenjavi in prikazu podatkov) se uporabljata UTC čas in datum.
- 029 Za prikaz lokalnega časa mora biti mogoče spreminjati zamik časa za prikaz, v polurnih korakih.
- 030 Pri pogojih odobritve tipa mora biti lezenje časa v mejah ± 2 sekundi na dan.
- 031 Čas mora biti merjen z ločljivostjo enako ali boljšo od 1 sekunde.
- 032 Merjenje časa mora pri pogojih odobritve tipa teči neodvisno od izklopa zunanega napajanja, če je ta izklop krajši od 12 mesecev.

4. Spremljanje voznikovih dejavnosti

- 033 Ta funkcija mora neprekinjeno in ločeno nadzirati dejavnosti enega voznika in enega sovoznika.
- 034 Voznikove dejavnosti so: VOŽNJA, DELO, RAZPOLOŽLJIVOST ali ODMOR/POČITEK.
- 035 Voznik in/ali sovoznik mora imeti možnost ročne izbire dejavnosti DELO, RAZPOLOŽLJIVOST ali ODMOR/POČITEK.
- 036 Kadar se vozilo premika, se mora za voznika avtomatsko izbrati dejavnost VOŽNJA, za sovoznika pa se mora avtomatsko izbrati dejavnost RAZPOLOŽLJIVOST.
- 037 Ko se vozilo ustavi, se mora za voznika avtomatsko izbrati dejavnost DELO.
- 038 Za prvo spremembo dejavnosti v času 120 sekund od avtomatske spremembe v dejavnost DELO zaradi ustavitve vozila, velja, da je nastopila v trenutku, ko se je vozilo ustavilo (kar lahko prekliče prvotno spremembo v dejavnost DELO).
- 039 Ta funkcija mora funkcijam zapisovanja posredovati spremembe dejavnosti z ločljivostjo ene minute.
- 040 Če v določeni koledarski minuti nastopi dejavnost VOŽNJA, ta minuta v celoti šteje kot minuta VOŽNJE.
- 041 Če je v minuti neposredno pred določeno koledarsko minuto in v minuti neposredno za njo nastopila dejavnost VOŽNJA, ta koledarska minuta v celoti šteje kot minuta VOŽNJE.
- 042 Določena koledarska minuta, ki po gornjih zahtevah ne šteje kot minuta VOŽNJE, v celoti velja kot minuta tiste dejavnosti, ki je neprekinjeno trajala najdalj v tej minuti (ali zadnje od enako dolgih najdalj trajajočih dejavnosti).
- 043 Ta funkcija mora tudi neprekinjeno spremljati čas neprekinjene vožnje in kupni čas odmorov voznika.

5. Nadzor stanja vožnje

- 044 Ta funkcija mora neprekinjeno in avtomatsko nadzorovati stanje vožnje.
- 045 Stanje vožnje POSADKA mora biti izbrano, kadar sta v napravi vstavljeni dve veljavni voznikovi kartici, v vseh ostalih primerih pa stanje vožnje POSAMEZNIK.

6. Voznikovi ročni vnosi

6.1 Vnos krajev, v katerih se dnevne delovne izmene začnejo in/ali končajo

- 046 Ta funkcija mora omogočati vnos krajev, v katerih se začnejo in/ali končajo dnevne delovne izmene voznika in/ali sovoznika.
- 047 Kraj je opredeljen kot država, po potebi pa še dodatno kot regija.
- 048 Ob izvleku voznikove (ali delavniške) kartice mora zapisovalna naprava pozvati (so)voznika k vnosu „kraja, v katerem se konča dnevna delovna izmena“.
- 049 Zapisovalna naprava mora dopuščati (so)vozniku, da ta poziv spregleda.
- 050 Mogoči morajo biti tudi vnosi krajev začetkov in/ali koncev dnevnih delovnih izmen brez vstavljenе kartice ali ob drugih časih, ne le pri vstavljanju ali izvleku kartice.

6.2 Ročni vnos voznikovih dejavnosti

- 050a Takoj po vstavitvi voznikove (ali delavniške) kartice, in le tedaj, mora zapisovalna naprava:
- prikazati imetniku kartice datum in čas njegovega zadnjega izvleka kartice, in
 - pozvati imetnika kartice, naj opredeli, ali pomeni sedanja vstavev kartice nadaljevanje tekoče dnevne delovne izmene ali ne.

Zapisovalna naprava mora dopuščati, da imetnik kartice sploh ne odgovori na to vprašanje, ali da odgovori pritrdilno ali nikalno.

- če imetnik kartice ne odgovori na vprašanje, ga mora zapisovalna naprava pozvati, naj vnese ‚kraj začetka dnevne delovne izmene‘. Zapisovalna naprava mora dopuščati imetniku kartice, da ta poziv spregleda. Če vnese kraj, mora ta podatek zapisovalna naprava zapisati v pomnilnik podatkov in na tahografsko kartico skupaj s časom vstavitve kartice,
- ob pritrdilnem ali nikalnem odgovoru mora zapisovalna naprava imetnika kartice pozvati, naj ročno vnese eno izmed dejavnosti DELO, RAZPOLOŽLJIVOST ali ODMOR/POČITEK, skupaj z datumi in časi njihovih začetkov in koncev, izključno v okviru obdobja od zadnjega izvleka do sedanje vstavitve kartice, in ne sme dopuščati, da bi se posamezne dejavnosti med seboj časovno prekrivale. To se izvede v skladu z naslednjimi postopki:
- če imetnik kartice na vprašanje odgovori pritrdilno, ga mora zapisovalna naprava pozvati, naj ročno vnese svoje dejavnosti, v časovnem zaporedju, v obdobju od zadnjega izvleka do sedanje vstavitve kartice. Proces je zaključen, ko se čas zaključka ročno vnešene dejavnosti pokrije s časom vstavitve kartice.
- če imetnik kartice na vprašanje odgovori nikalno, mora zapisovalna naprava:

- pozvati imetnika kartice, naj ročno vnese svoje dejavnosti, v časovnem zaporedju, v obdobju od zadnjega izvleka do konca zadevne dnevne delovne izmene (ali do konca dejavnosti, povezanih z vozilom, če je dnevna delovna izmena po delovnem dnevniku trajala še naprej). Zato mora zapisovalna naprava pred sprejemom imetnikovega ročnega vnosa posamezne dejavnosti imetnika pozvati, naj označi, ali čas zaključka zadnje zapisane dejavnosti pomeni tudi zaključek prejšnje delovne izmene (glej spodnjo opombo),

Opomba: če imetnik ne navede časa zaključka prejšnje delovne izmene, in ročno vnese dejavnost, katere zaključek se pokriva s časom vstavitve kartice, mora zapisovalna naprava:

- predpostaviti, da se je dnevna delovna izmena končala ob začetku prvega obdobja POČITKA (ali preostalega NEZNANEGA obdobja) po izvleku kartice ali ob času izvleka kartice, če ni bilo vnešeno nikakršno obdobje POČITKA (in ni nobeno obdobje ostalo NEZNANO),
- predpostaviti, da je čas začetka (glej spodaj) enak času vstavitve kartice,
- nadaljevati s spodaj opisanimi koraki,
- nato v primeru, če je čas konca obravnavane delovne izmene različen od časa izvleka kartice, ali če ni bil vnešen kraj zaključka dnevne delovne izmene, pozove imetnika kartice, naj ‚potrdi ali vnese kraj zaključka dnevne delovne izmene‘ (zapisovalna naprava mora dopuščati imetniku kartice, da ta poziv spregleda). Če imetnik kartice vnese ta kraj, ga mora zapisovalna naprava zapisati na tahografsko kartico le v primeru, če je različen od kraja, vnešenega ob izvleku kartice (če je bil takrat vnešen) in to skupaj s časom zaključka delovne izmene,
- nato pozove imetnika kartice, naj vnese ‚čas začetka‘ tekoče dnevne delovne izmene (ali začetka dejavnosti, povezanih s tem vozilom, če je imetnik kartice do sedaj uporabljal tahografski vložek) in pozove imetnika kartice k vnosu ‚kraja začetka dnevne delovne izmene‘ (zapisovalna naprava mora dopuščati imetniku kartice, da ta poziv spregleda). Če imetnik kartice vnese ta kraj, ga mora zapisovalna naprava zapisati na tahografsko kartico skupaj s časom začetka delovne izmene. Če je čas začetka delovne izmene enak času vstavitve kartice, se v pomnilnik podatkov zapiše tudi kraj,
- nato v primeru, če je čas začetka različen od časa vstavitve kartice, pozove imetnika kartice k ročnemu vnosu dejavnosti, v časovnem zaporedju, od časa začetka do časa vstavitve kartice. Proces je zaključen, ko se čas zaključka ročno vnešene dejavnosti pokrije s časom vstavitve kartice,
- nato mora zapisovalna naprava omogočiti imetniku kartice še spreminjati podatke ročno vnešenih dejavnosti, do potrditve vnosa s posebnim ukazom; po tej potrditvi pa zapisovalna naprava ne sme dopuščati nobenega spreminjanja več,
- če na začetni poziv imetnik kartice ne vnese nikakršne dejavnosti, mora zapisovalna naprava predpostaviti, da je imetnik kartice poziv spregledal.

Med celotnim procesom mora zapisovalna naprava čakati na imetnikove vnose najdalj naslednje čakalne čase:

- eno minuto, če v tem času ne zazna nobenega posredovanja imetnika kartice (z vizualnim, po možnosti pa tudi zvočnim opozorilom po 30 sekundah), ali
- do trenutka izvleka kartice ali vstavitve kartice drugega voznika (ali delavniške kartice), ali
- do trenutka, ko se vozilo začne premikati,

v tem primeru mora zapisovalna naprava sprejeti kot veljavne vse že vnešene dejavnosti.

6.3 Vnos posebnih stanj

050b Zapisovalna naprava mora vozniku omogočati vnos naslednjih dveh posebnih stanj v realnem času:

- ‚ZUNAJ PODROČJA VELJAVNOSTI‘ (začetek, zaključek)
- ‚PREVOZ S TRAJEKTOM/VLAKOM‘

Stanje ‚PREVOZ S TRAJEKTOM/VLAKOM‘ ni mogoče, kadar velja stanje ‚ZUNAJ PODROČJA VELJAVNOSTI‘.

Odprto stanje ‚ZUNAJ OBMOČJA VELJAVNOSTI‘ mora zapisovalna naprava avtomatsko zaključiti, če voznik svojo kartico vstavi ali izvleče.

7. Upravljanje blokad s strani podjetja

- 051 Ta funkcija mora omogočati upravljanje blokad, ki jih nastavi podjetje za omejitev lastnega dostopa do podatkov v režimu del v podjetju.
- 052 Blokada s strani podjetja sestavlja začetni datum/čas (vklop blokade) in zaključni datum/čas (izklop blokade) povezana z identifikacijo podjetja navedeno v številki kartice podjetja (ob vklopu blokade).
- 053 Blokada je mogoče vklopiti in izklopiti le v realnem času.
- 054 Izklop blokade mora biti mogoč le podjetju, katerega blokada je vključena (podjetju, ki ga določa prvih 13 števk številke kartice podjetja) ali
- 055 blokada mora biti izklopljena avtomatsko, ko svojo blokado nastavi drugo podjetje.
- 055a Če določeno podjetje nastavi svojo blokado, prejšnja blokada pa je bila vklopljena za isto podjetje, se smatra, da prejšnja blokada ni izklopljena, pač pa ostane vklopljena še naprej.

8. Spremljanje nadzornih dejavnosti

- 056 Ta funkcija mora spremljati dejavnosti PRIKAZOVANJA, TISKANJA, VU (enota v vozilu) in PRENOS v nadzornem režimu.
- 057 Ta funkcija mora v nadzornem režimu nadzirati tudi dejavnost NADZOR PREKORAČITVE HITROSTI. Velja, da se je nadzor prekoračitve hitrosti izvedla, kadar se v nadzornem režimu pošlje obvestilo ‚prekoračitev hitrosti‘ na tiskalnik ali na prikazovalnik ali kadar so se iz pomnilnika podatkov VU prenesli podatki o ‚dogodkih in napakah‘.

9. Zaznavanje dogodkov in/ali napak

- 058 Ta funkcija mora zaznavati naslednje dogodke in/ali napake:

9.1 Dogodek ‚vstavitve neveljavne kartice‘

- 059 Ta dogodek se mora sprožiti ob vstavitvi kakršnekoli neveljavne kartice in/ali ob poteku veljavnosti vstavljene veljavne kartice.

9.2 *Dogodek „navzkrižje med karticami“*

060 Ta dogodek se mora sprožiti ob nastopu katerekoli od kombinacij veljavnih kartic označenih z X v naslednji tabeli:

Navzkrižje med karticami		Voznikova reža				
		Brez kartice	Voznikova kartica	Nadzorna kartica	Delavniška kartica	Kartica podjetja
Sovoznikova reža	Brez kartice					
	Voznikova kartica				X	
	Nadzorna kartica			X	X	X
	Delavniška kartica		X	X	X	X
	Kartica podjetja			X	X	X

9.3 *Dogodek „časovno prekrivanje“*

061 Ta dogodek se mora sprožiti, kadar je s kartice prebrani datum/čas zadnjega izvleka voznikove kartice poznejši od tekočega datuma/časa zapisovalne naprave, v katero je kartica vstavljena.

9.4 *Dogodek „vožnja brez ustrezne kartice“*

062 Ta dogodek se mora sprožiti ob katerikoli od kombinacij tahografskih kartic, označenih z X v naslednji tabeli, ko se voznikova dejavnost preklopi v VOŽNJO ali ob kakršnikoli spremembi režima delovanja v času, ko je voznikova dejavnost VOŽNJA.

Vožnja brez ustrezne kartice		Voznikova reža				
		Brez kartice ali neveljavna kartica	Voznikova kartica	Nadzorna kartica	Delavniška kartica	Kartica podjetja
Sovoznikova reža	Brez kartice ali neveljavna kartica	X		X		X
	Voznikova kartica	X		X	X	X
	Nadzorna kartica	X	X	X	X	X
	Delavniška kartica	X	X	X		X
	Kartica podjetja	X	X	X	X	X

9.5 *Dogodek „vstavev kartice med vožnjo“*

063 Ta dogodek se mora sprožiti ob vstavitvi tahografske kartice v katerokoli režo med tem, ko je voznikova dejavnost VOŽNJA.

9.6 *Dogodek „zadnja seja s kartico nepravilno zaključena“*

064 Ta dogodek se mora sprožiti, kadar zapisovalna naprava ob vstavitvi kartice zazna, da prejšnja seja s kartico ni bila zaključena pravilno glede na določbe v točki III(1) (kartica je bila izvlečena pred shranitvijo vseh potrebnih podatkov nanjo). Ta dogodek morajo sprožiti samo voznikove in delavniške kartice.

9.7 *Dogodek „prekoračitev hitrosti“*

065 Ta dogodek se mora sprožiti ob vsaki prekoračitvi hitrosti.

9.8 Dogodek ‚zpad napajanja‘

- 066 Ta dogodek se mora sprožiti, kadar naprava ni v režimu kalibriranja, kadar prekinitve napajanja zaznavala gibanja in/ali enote v vozilu traja dlje kakor 200 milisekund. Prag prekinitve mora opredeliti proizvajalec. Prehodni izpad napajanja ob zagonu motorja vozila ne sme sprožiti tega dogodka.

9.9 Dogodek ‚napaka v podatkih o gibanju‘

- 067 Ta dogodek se mora sprožiti ob prekinitvi normalnega pretoka podatkov med zaznavalom gibanja in enot v vozilu in/ali ob napaki celovitosti ali avtentičnosti podatkov pri prenosu podatkov med zaznavalom gibanja in enoto v vozilu.

9.10 Dogodek ‚poskus kršenja varnosti‘

- 068 Ta dogodek se mora sprožiti, kadar naprava ni v režimu kalibriranja, ob kateremkoli dogodku, ki vpliva na varnost zaznavala gibanja in/ali enote v vozilu predpisano za ti napravi v generičnih varnostnih ciljih.

9.11 Napaka ‚kartica‘

- 069 Ta dogodek se mora sprožiti ob napaki tahografske kartice med delovanjem.

9.12 Napaka ‚zapisovalna naprava‘

- 070 Ta napaka se mora sprožiti, kadar naprava ni v režimu kalibriranja, ob kateri koli od naslednjih odpovedi:

- interna napaka VU,
- napaka na tiskalniku,
- napaka na prikazovalniku,
- napaka pri prenosu podatkov,
- napaka na zaznavalu.

10. Vgrajeni preskusi in preskusi lastnega delovanja

- 071 Zapisovalna naprava mora sama zaznavati napake z izvajanjem vgrajenih preskusov in preskusov lastnega delovanja po naslednji tabeli:

Preskušani podstestav	Preskus lastnega delovanja	Vgrajeni preskus
Programska oprema		Celovitost
Pomnilnik podatkov	Dostop	Dostop, celovitost podatkov
Vmesniške naprave za kartice	Dostop	Dostop
Tipkovnica		Ročno preverjanje
Tiskalnik	(določi proizvajalec)	Izpis
Prikazovalnik		Vizualno preverjanje
Prenos podatkov (izvajanje samo med prenosom podatkov)	Pravilno delovanje	
Zaznavalo	Pravilno delovanje	Pravilno delovanje

11. Branje iz pomnilnika podatkov

- 072 Zapisovalna naprava mora biti zmožna brati vse podatke, shranjene v svojem pomnilniku podatkov.

12. Zapisovanje in hranjenje podatkov v pomnilniku podatkov

V okviru te točke velja naslednje:

- ‚365 dni‘ pomeni 365 koledarskih dni povprečnih voznikovih dejavnosti v vozilu. Povprečna dejavnost na dan na vozilo je opredeljena kot najmanj šest voznikov ali sovoznikov, šest ciklov vstavitve in izvleka kartice ter 256 sprememb dejavnosti. ‚365 dni‘ torej pomeni najmanj 2 190 (so)voznikov, 2 190 ciklov vstavitve in izvleka kartice in 93 440 sprememb dejavnosti,
- časi so zapisani z ločljivostjo ene minute, če ni predpisano drugače,
- vrednosti števca prevožene poti so zapisani z ločljivostjo enega kilometra,
- hitrosti so zapisane z ločljivostjo 1 km/h.

073 Na podatke shranjene v pomnilniku podatkov pri pogojih postopka odobritve tipa ne sme vplivati noben izklop zunanjega napajanja, če je ta izklop krajši od dvanajst mesecev.

074 Zapisovalna naprava mora biti zmožna zapisati in hraniti implicitno ali eksplicitno v svojem pomnilniku podatkov naslednje podatke:

12.1 Identifikacijski podatki naprave

12.1.1 Identifikacijski podatki enote na vozilu

075 Zapisovalna naprava mora biti zmožna hraniti v svojem pomnilniku podatkov naslednje identifikacijske podatke enote v vozilu:

- ime proizvajalca,
- naslov proizvajalca,
- kataloška številka,
- serijska številka,
- številka verzije programske opreme,
- datum namestitve verzije programske opreme,
- leto izdelave opreme,
- številka odobritve.

076 Identifikacijske podatke enote v vozilu zapiše in shrani enkrat za vselej proizvajalec enote v vozilu, razen podatkov povezanih s programsko opremo in številke odobritve, ki se lahko spremenijo ob nadgradnji programske opreme.

12.1.2 Identifikacijski podatki zaznavala gibanja

077 Zaznavalo gibanja mora biti zmožno hraniti v svojem pomnilniku naslednje identifikacijske podatke:

- ime proizvajalca,
- kataloška številka,
- serijska številka,
- številka odobritve,
- identifikator vgrajenega varnostnega dela (npr. številka vgrajenega čipa/procesorja),
- identifikator operacijskega sistema (npr. številka verzije programske opreme).

078 Identifikacijske podatke zaznavala gibanja zapiše in shrani v zaznavalo gibanja enkrat za vselej proizvajalec zaznavala gibanja.

079 Enota v vozilu mora biti zmožna zapisati in hraniti v svojem pomnilniku podatkov naslednje identifikacijske podatke trenutno povezanega zaznavala gibanja:

- serijska številka,
- številka odobritve,
- datum prve povezave.

12.2 **Varnostni elementi**

080 Zapisovalna naprava mora biti zmožna hraniti naslednje varnostne elemente:

- evropski javni ključ,
- certifikat države članice,
- certifikat naprave,
- zasebni ključ naprave.

Varnostne elemente zapisovalne naprave vnese v napravo proizvajalec enote v vozilu.

12.3 **Podatki o vstavljanju in izvlečenju voznikove kartice**

081 Za vsak cikel vstavljanja in izvleka voznikove ali delavniške kartice v napravo mora zapisovalna naprava v svoj pomnilnik podatkov zapisati in shraniti naslednje podatke:

- priimek in ime(na) imetnika kartice, shranjene na kartici,
- številka kartice, država izdajateljica in datum poteka veljavnosti, zapisani na kartici,
- datum in čas vstavitve,
- vrednost števca prevožene poti ob vstavitvi kartice,
- reža, v katero je vstavljena kartica,
- datum in čas izvleka,
- vrednost števca prevožene poti ob izvleku kartice,
- naslednji podatki o vozilu, ki ga je pred tem uporabljal voznik, shranjeni na kartici:
 - registrska številka vozila in država, v kateri je registrirano,
 - datum in čas izvleka kartice,
- zastavica, ki kaže, ali je ob vstavitvi imetnik kartice ročno vnesel svoje dejavnosti ali ne.

082 Pomnilnik podatkov mora biti zmožen hraniti te podatke najmanj 365 dni.

083 Ko se pomnilnik zapolni s podatki, se morajo novi podatki prepisovati čez najstarejše podatke.

12.4 Podatki o vznikačih dejavnostih

084 Zapisovalna naprava mora zapisovati in hraniti v svojem pomnilniku podatkov ob vsaki spremembi vznikač/sovoznika dejavnosti in/ali ob vsaki spremembi stanja vožnje in/ali ob vsaki vstavitvi ali izvleku vznikače ali delavniške kartice naslednje podatke:

- stanje vožnje (POSADKA, POSAMEZNIK),
- reža (VOZNIK, SOVOZNIK),
- stanje kartice v ustrezni reži (VSTAVLJENA, NI VSTAVLJENA) (glej opombo),
- dejavnost (VOŽNJA, RAZPOLOŽLJIVOST, DELO, ODMOR/POČITEK),
- datum in čas spremembe.

Opomba: VSTAVLJENA pomeni, da je v reži vstavljena veljavna vznikača ali delavniška kartica. NI VSTAVLJENA pomeni nasprotno, tj., v reži ni vstavljena veljavna vznikača ali delavniška kartica (npr. vstavljena je kartica podjetja ali pa v reži ni kartice).

Opomba: Podatki o dejavnostih, ki jih ročno vnese voznik, se ne zapišejo v pomnilnik podatkov.

085 Pomnilnik podatkov mora biti zmožen hraniti podatke o dejavnostih voznika najmanj 365 dni.

086 Ko se pomnilnik zapolni s podatki, se morajo novi podatki prepisovati čez najstarejše podatke.

12.5 Kraji, v katerih se dnevne delovne izmene začnajo in/ali končajo

087 Zapisovalna naprava mora zapisati in hraniti v svojem pomnilniku podatkov ob vsakem vznikačem vnosu kraja začetka in/ali zaključka dnevne delovne izmene naslednje podatke:

- če pride v poštev, številka (so)vznikače kartice in država izdajateljica,
- datum in čas vnosa (ali datum/čas povezan z vnosom, kadar je vnos opravljen s postopkom ročnega vnosa),
- vrsta vnosa (začetek ali konec, stanje vnosa),
- vnesena država in regija,
- vrednost števca prevožene poti vozila.

088 Pomnilnik podatkov mora biti zmožen hraniti podatke o začetkih in koncih dnevnih delovnih izmen najmanj 365 dni (ob predpostavki, da en voznik vnese dva zapisa na dan).

089 Ko se pomnilnik zapolni s podatki, se morajo novi podatki prepisovati čez najstarejše podatke.

12.6 Podatki števca prevožene poti

090 Zapisovalna naprava mora zapisati v svoj pomnilnik podatkov vrednost števca prevožene poti in ustrezajoči datum vsak koledarski dan ob polnoči.

091 Pomnilnik podatkov mora biti zmožen hraniti ob polnoči zapisane vrednosti števca prevožene poti najmanj 365 koledarskih dni.

092 Ko se pomnilnik zapolni s podatki, se morajo novi podatki prepisovati čez najstarejše podatke.

12.7 Podrobni podatki o hitrosti

093 Zapisovalna naprava mora zapisati in hraniti v svojem pomnilniku podatkov trenutno hitrost vozila in odgovarjajoči datum in čas vsako sekundo in hraniti te podatke za najmanj zadnjih 24 ur gibanja vozila.

12.8 Podatki o dogodkih

V okviru te točke velja, da se čas zapisuje z ločljivostjo ene sekunde.

094 Zapisovalna naprava mora zapisati in hraniti v svojem pomnilniku podatkov za vsak zaznani dogodek naslednje podatke po naslednjih pravilih shranjevanja:

Dogodek	Pravila shranjevanja	Podatki, ki se zapišejo za vsak dogodek
Navzkrižje med karticami	— 10 najnovejših dogodkov	— datum in čas začetka dogodka, — datum in čas konca dogodka, — tipa, številki in državi izdajateljici obeh kartic, ki sta povzročili navzkrižje.
Vožnja brez ustrezne kartice	— najdaljši dogodek na vsakega od 10 zadnjih dni nastopov dogodkov, — pet najdaljših dogodkov v zadnjih 365 dneh.	— datum in čas začetka dogodka, — datum in čas konca dogodka, — tipi, številke in države izdajateljice kartic, ki so bile vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v tem dnevu.
Vstavev kartice med vožnjo	— zadnji dogodek na vsakih 10 zadnjih dni nastopov dogodkov,	— datum in čas dogodka, — tip, številka in država izdajateljica kartice, — število podobnih dogodkov v tem dnevu.
Zadnja seja s kartico nepravilno zaključena	— 10 najnovejših dogodkov	— datum in čas vstavitve kartice, — tip, številka in država izdajateljica kartice, — podatki zadnje seje, prebrani s kartice: — datum in čas vstavitve kartice, — VRN in država članica, v kateri je vozilo registrirano.
Prekoračitev hitrosti ⁽¹⁾	— najresnejši tak dogodek na vsakih 10 zadnjih dni nastopov dogodkov (tj. dogodek z najvišjo povprečno hitrostjo), — pet najresnejših dogodkov v zadnjih 365 dneh, — prvi dogodek, ki je nastopil po zadnjem kalibriranju.	— datum in čas začetka dogodka, — datum in čas konca dogodka, — najvišja hitrost izmerjena med dogodkom, — aritmetična povprečna hitrost izmerjena med dogodkom, — tip, številka in država izdajateljica vozniške kartice (če pride v poštev), — število podobnih dogodkov v tem dnevu.

Dogodek	Pravila shranjevanja	Podatki, ki se zapišejo za vsak dogodek
Izpad napajanja ⁽²⁾	— najdaljši dogodek na vsakega od 10 zadnjih dni nastopov dogodkov, — pet najdaljših dogodkov v zadnjih 365 dneh.	— datum in čas začetka dogodka, — datum in čas konca dogodka, — tipi, številke in države izdajateljice kartic, ki so bile vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v tem dnevu.
Napaka podatkov o gibanju	— najdaljši dogodek na vsakega od 10 zadnjih dni nastopov dogodkov, — pet najdaljših dogodkov v zadnjih 365 dneh.	— datum in čas začetka dogodka, — datum in čas konca dogodka, — tipi, številke in države izdajateljice kartic, ki so bile vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v tem dnevu.
Poskus kršenja varnosti	— 10 najnovejših dogodkov za vsak tip dogodka.	— datum in čas začetka dogodka, — datum in čas konca dogodka (če je pomemben), — tipi, številke in države izdajateljice kartic, ki so bile vstavljene ob začetku in/ali koncu dogodka, — vrsta dogodka.

095

⁽¹⁾ Zapisovalna naprava mora zapisati in hraniti v svojem pomnilniku podatkov tudi naslednje podatke:

- datum in čas zadnjega NADZORA PREKORAČITVE HITROSTI,
- datum in čas prve prekoračitve hitrosti po tem NADZORU PREKORAČITVE HITROSTI,
- število dogodkov prekoračitve hitrosti od zadnjega NADZORA PREKORAČITVE HITROSTI.

⁽²⁾ Te podatke se lahko zapiše šele po ponovni vzpostavitvi napajanja; časi so lahko točni na minuto.

12.9 Podatki o napakah

V okviru te točke velja, da se čas zapisuje z ločljivostjo ene sekunde.

096

Zapisovalna naprava mora poskusiti zapisati in hraniti v svojem pomnilniku podatkov za vsako zaznano napako naslednje podatke po naslednjih pravilih shranjevanja:

Napaka	Pravila shranjevanja	Podatki, ki se zapišejo za vsako napako
Napaka na kartici	— 10 zadnjih napak na vozni-kovi kartici.	— datum in čas začetka napake, — datum in čas konca napake, — tip, številka in država izdajateljica kartice.
Napaka na zapisovalni napravi	— 10 zadnjih napak za vsako vrsto napake, — prva napaka po zadnjem kalibriranju.	— datum in čas začetka napake, — datum in čas konca napake, — vrsta napake, — tipi, številke in države izdajateljice kartic, ki so bile vstavljene ob začetku in/ali koncu napake.

12.10 Kalibracijski podatki

- 097 Zapisovalna naprava mora zapisati in hraniti v svojem pomnilniku podatke, nanašajoče se na:
- znane kalibracijske parametre ob času aktiviranja,
 - prvo kalibriranje po aktiviranju,
 - prvo kalibriranje v vozilu, v katerem je vgrajena sedaj (ki ga identificira VIN),
 - pet zadnjih kalibriranj (Če se na isti koledarski dan opravi več kalibriranj, se shrani le podatke za zadnje kalibriranje na ta dan).
- 098 Za vsako od teh kalibriranj se zapiše naslednje podatke:
- namen kalibriranja (aktiviranje, prvo nameščanje, nameščanje, rednakontrola),
 - ime in naslov delavnice,
 - številka delavniške kartice, država izdajateljica delavniške kartice in datum poteka veljavnosti delavniške kartice,
 - identifikacija vozila,
 - posodobljeni ali potrjeni parametri: w, k, l, mere avtoplaščev, nastavitve naprave za omejevanje hitrosti (stare in nove vrednosti), datum in čas (stare in nove vrednosti).
- 099 Zaznavalo gibanja mora zapisati in hraniti v svojem pomnilniku naslednje podatke o namestitvi zaznavala gibanja:
- prva povezava z VU (datum, čas, številka odobritve VU, serijska številka VU),
 - zadnja povezava z VU (datum, čas, številka odobritve VU, serijska številka VU).

12.11 Podatki o nastavljanju časa

- 100 Zapisovalna naprava mora zapisati in hraniti v svojem pomnilniku podatke, nanašajoče se na:
- zadnje nastavljanje časa,
 - pet največjih popravkov časa od zadnje kalibracije,
- opravljene v režimu kalibriranja zunaj domene rednega kalibriranja (opredelitev (f)).
- 101 Za vsako od teh nastavljanj časa se zapiše naslednje podatke:
- datum in čas, stara vrednost,
 - datum in čas, nova vrednost,
 - ime in naslov delavnice,
 - številka delavniške kartice, država izdajateljica kartice in datum poteka veljavnosti kartice.

12.12 Podatki o nadzornih dejavnostih

- 102 Zapisovalna naprava mora zapisati in hraniti v svojem pomnilniku naslednje podatke nanašajoče se na 20 zadnjih nadzornih dejavnosti:
- datum in čas nadzora,
 - številka in država izdajateljica nadzorne kartice,
 - vrsta nadzora (prikazovanje in/ali tiskanje in/ali prenos podatkov iz VU in/ali prenos podatkov iz kartice).

- 103 Pri prenosu podatkov se zapiše tudi prvi in zadnji dan obdobja, za katerega so podatki prenešeni.

12.13 Podatki o blokadah s strani podjetja

- 104 Zapisovalna naprava mora zapisati in hraniti v svojem pomnilniku naslednje podatke nanašajoče se na 20 zadnjih dejavnosti blokad s strani podjetja:

- datum in čas vklopa blokade,
- datum in čas izklopa blokade,
- številka in država izdajateljica kartice podjetja,
- ime in naslov podjetja.

12.14 Podatki o prenosih podatkov v naprave

- 105 Zapisovalna naprava mora zapisati in hraniti v svojem pomnilniku podatkov naslednje podatke nanašajoče se na zadnji prenos podatkov na zunanji medij v režimu del v podjetju ali režimu kalibriranja:

- datum in čas prenosa,
- številka in država izdajateljica kartice podjetja,
- ime podjetja ali delavnice.

12.15 Podatki o posebnih stanjih

- 105a Zapisovalna naprava mora zapisati v svoj pomnilnik podatkov naslednje podatke nanašajoče se na posebna stanja:

- datum in čas vnosa,
- vrsta posebnega stanja.

- 105b Pomnilnik podatkov mora biti zmožen hraniti podatke o posebnih stanjih najmanj 365 dni (ob predpostavki, da se povprečno odpre in zapre po eno posebno stanje na dan). Ko se pomnilnik zapolni s podatki, se morajo novi podatki prepisovati čez najstarejše podatke.

13. Branje s tahografskih kartic

- 106 Zapisovalna naprava mora biti po potrebi zmožna brati s tahografskih kartic potrebne podatke za:

- identifikacijo vrste kartice, imetnika kartice, prej uporabljanega vozila, datuma in časa zadnjega izvleka kartice in takrat izbrane dejavnosti,
- preverjanje, ali je bila zadnja seja s kartico pravilno zaključena,
- izračun voznikovega časa neprekinjene vožnje, skupnega časa odmorov in skupnega časa vožnje v preteklem in tekočem tednu,
- tiskanje zahtevanih izpisov nanašajočih se na podatke zapisane na voznikovi kartici,
- prenos podatkov z voznikove kartice na zunanje medije.

- 107 V primeru napake pri branju mora zapisovalna naprava še do trikrat poskusiti izvesti isti ukaz za branje, če vsi ti ponovni poskusi spodletijo, pa proglasiti, da je kartica neveljavna ali da ima napako.

14. Zapisovanje in hranjenje podatkov na tahografskih karticah

- 108 Zapisovalna naprava mora takoj po vstavitvi kartice nastaviti 'podatke o seji s kartico' na voznikovi ali delavniški kartici.

- 109 Zapisovalna naprava mora posodobiti podatke shranjene na veljavni voznikovi, delavniški in/ali nadzorni kartici z vsemi podatki nanašajočimi se na obdobje, v katerem je kartica vstavljena, in ki zadevajo imetnika kartice. Podatki shranjeni na teh karticah so predpisani v poglavju IV.
- 109a Zapisovalna naprava mora posodobiti podatke o voznikovih dejavnostih in krajih (kakor je predpisano v točkah 5.2.5 in 5.2.6 poglavja IV), shranjene na voznikovih in/ali delavniških karticah, s podatki, ki jih imetnik kartice ročno vnese.
- 110 Posodabljanje podatkov na tahografskih karticah mora potekati tako, da se po potrebi in ob upoštevanju dejanske zmogljivosti pomnilnika kartice, najnovejši podatki zapišejo čez najstarejše podatke.
- 111 V primeru napake pri pisanju mora zapisovalna naprava še do trikrat poskusiti izvesti isti ukaz za pisanje, če vsi ti ponovni poskusi spodletijo, pa proglasiti, da je kartica neveljavna ali da ima napako.
- 112 Pred sprostitvijo voznikove kartice in po shranitvi vseh potrebnih podatkov nanjo mora zapisovalna naprava resetirati podatke o seji s kartico.

15. Prikazovanje

- 113 Prikazovalnik mora obsegati najmanj 20 znakov.
- 114 Znak na prikazovalniku mora biti najmanj 5 mm visok in 3,5 mm širok.
- 114a Prikazovalnik mora podpirati nabor znakov Latin 1 in grški nabor znakov, opredeljena v delih 1 in 7 standarda ISO 8859, kakor je predpisano v dodatku 1 poglavja 4, 'Nabori znakov'. Prikazovalnik lahko uporablja poenostavljene glife (npr. lahko so opuščeni znaki za naglase, male črke so lahko prikazane kot velike črke).
- 115 Prikazovalnik mora biti ustrezno osvetljen, vendar ne sme slepiti uporabnika.
- 116 Prikazi morajo biti vidni zunaj zapisovalne naprave.
- 117 Zapisovalna naprava mora biti zmožna prikazovati:
- privzete podatke,
 - podatke povezane z opozorili,
 - podatke povezane z dostopom do menijev,
 - druge podatke po zahtevah uporabnika.
- Zapisovalna naprava lahko prikazuje tudi druge podatke, pod pogojem, da je te dodatne podatke mogoče jasno ločiti od zgoraj predpisanih podatkov.
- 118 Prikazovalnik zapisovalne naprave mora uporabljati grafične znake ali kombinacije grafičnih znakov naštetih v dodatku 3. Prikazovalnik lahko podpira tudi dodatne grafične znake ali kombinacije grafičnih znakov pod pogojem, da jih je mogoče jasno ločiti od zgoraj navedenih grafičnih znakov ali kombinacij grafičnih znakov.
- 119 Med gibanjem vozila mora biti prikazovalnik ves čas vključen.
- 120 Zapisovalna naprava lahko avtomatsko izklopi ali omogoča ročni izklop prikazovalnika, kadar vozilo miruje.
- Oblika prikaza je predpisana v dodatku 5.

15.1 Privzeti prikaz

- 121 Če ni potreben prikaz nobenih posebnih podatkov, mora zapisovalna naprava po privzetem dogovoru prikazovati naslednje informacije:
- lokalni čas (seštevek časa UTC in zamika časa, ki ga je nastavil voznik),
 - režim delovanja,
 - tekočo dejavnost voznika in tekočo dejavnost sovoznika,

- informacije nanašajoče se na voznika:
 - če je njegova tekoča dejavnost VOŽNJA, njegov tekoči čas neprekinjene vožnje in njegov skupni čas odmorov,
 - če njegova tekoča dejavnost ni VOŽNJA, dosedanji čas te dejavnosti (od takrat, ko je to dejavnost izbral) in njegov skupni čas odmorov,
- informacije nanašajoče se na sovoznika:
 - dosedanji čas te dejavnosti (od takrat, ko je to dejavnost izbral).

- 122 Prikaz podatkov o vsakem od njiju (vozniku oz. sovozniku) mora biti jasen, enostaven in nedvoumen. Če ni mogoče istočasno prikazovati informacij o vozniku in sovozniku, mora zapisovalna naprava po privzetem dogovoru prikazovati informacije nanašajoče se na voznika in omogočati uporabniku tudi izbiro prikaza informacij o sovozniku.
- 123 Če širina prikazovalnika ne omogoča trajnega prikaza režima delovanja, mora zapisovalna naprava za kratek čas prikazati novi režim po vsaki spremembi režima.
- 124 Zapisovalna naprava mora po vstavitvi kartice za kratek čas prikazati ime imetnika kartice.
- 124a Kadar je odprto stanje ‚ZUNAJ PODROČJA VELJAVNOSTI‘, mora privzeti prikaz kazati tudi ustrezni grafični znak tega stanja (Sprejemljivo je, da v tem primeru ni mogoče istočasno prikazovati tudi tekoče voznikove dejavnosti).

15.2 Opozorilni prikaz

- 125 Zapisovalna naprava mora prikazovati opozorilne informacije prevsem z grafičnimi znaki predpisanimi v dodatku 3, po potrebi dopolnjenimi z dodatnimi številsko kodiranimi informacijami. Lahko je dodan tudi besedni opis opozorila v voznikovem izbranem jeziku.

15.3 Dostop do menijev

- 126 Zapisovalna naprava mora zagotavljati potrebne ukaze za gibanje skozi sestav menijev.

15.4 Drugi prikazi

- 127 Omogočeni morajo biti naslednji izbirni posebni prikazi:
- datum in čas UTC,
 - režim delovanja (če ni vključen v privzetem prikazu),
 - čas neprekinjene vožnje in skupni čas odmorov voznika,
 - čas neprekinjene vožnje in skupni čas odmorov sovoznika,
 - skupni čas vožnje voznika v prejšnjem in tekočem tednu,
 - skupni čas vožnje sovoznika v prejšnjem in tekočem tednu,
 - vsebina kateregakoli šestih tiskanih izpisov v enaki obliki, kakršno imajo sami izpisi.
- 128 Prikaz vsebine tiskanih izpisov je zaporeden, po vrsticah. Če je širina prikazovalnika manjša od 24 znakov, mora biti uporabniku zagotovljena popolna informacija z ustrezno rešitvijo (prikaz v več vrsticah, drsno premikanje, ...). Vrstice tiskanega izpisa, namenjene ročnemu vpisu podatkov, so lahko na prikazovalniku izpuščene.

16. Tiskanje

- 129 Zapisovalna naprava mora biti zmožna tiskati informacije iz svojega pomnilnika podatkov in/ali tahografskih kartic v naslednjih šestih oblikah izpisov:
- dnevni izpis voznikovih dejavnosti s kartice,
 - dnevni izpis voznikovih dejavnosti iz enote v vozilu,

- izpis dogodkov in napak s kartice,
- izpis dogodkov in napak z enote v vozilu,
- izpis tehničnih podatkov,
- izpis prekoračenj hitrosti.

Oblike in vsebine teh izpisov so podrobno predpisane v dodatku 4. Na koncu izpisov so lahko priključeni še dodatni podatki.

Zapisovalna naprava lahko omogoča še druge izpise, če je le-te mogoče jasno ločiti od zgoraj navedenih šestih izpisov.

- 130 ‚Dnevni izpis voznikovih dejavnosti s kartice‘ in ‚izpis dogodkov in napak s kartice‘ morata biti mogoča le, kadar je v zapisovalno napravo vstavljena voznikova ali delavniška kartica. Pred začetkom tiskanja mora zapisovalna naprava posodobiti podatke shranjene na ustrezni kartici.
- 131 Za izvedbo ‚dnevnega izpisa voznikovih dejavnosti s kartice‘ ali ‚izpisa dogodkov in napak s kartice‘ mora zapisovalna naprava:
- bodisi avtomatsko izbrati voznikovo ali delavniško kartico, če je vstavljena samo ena od teh kartic, ali pa
 - omogočati izbiro izvirne kartice z ustreznim ukazom ali izbrati kartico v voznikovi reži, če sta vstavljeni dve taki kartici.
- 132 Tiskalnik mora omogočati tiskanje do 24 znakov v vrstici.
- 133 Znak mora biti najmanj 2,1 mm visok in 1,5 mm širok.
- 133a Tiskalnik mora podpirati nabor znakov Latin 1 in grški nabor znakov, opredeljena v delih 1 in 7 standarda ISO 8859, kakor je predpisano v dodatku 1 poglavja 4, ‚Nabori znakov‘.
- 134 Tiskalniki morajo imeti zadostno ločljivost, da je mogoče nedvoumno branje izpisov.
- 135 Izpisi morajo pri normalni vlažnosti (10 do 90 %) in temperaturi ohraniti svoje mere in zapis.
- 136 Papir za zapisovalno napravo mora imeti ustrezne oznake odobritve tipa in oznake vrst(-e) zapisovalne naprave, za katero(-e) je namenjen. Izpisi morajo pri normalnih pogojih hranjenja (osvetlitev, vlažnost in temperatura) ostati jasno čitljivi vsaj eno leto.
- 137 Izpisi morajo zagotavljati prostor za ročne dopise, npr. voznikov podpis.
- 138 Zapisovalna naprava mora obvladovati stanja, ko zmanjka papirja: Ko uporabnik vstavi nov papir, mora zapisovalna naprava nadaljevati tiskanje od začetka izpisa ali pa nadaljevati tiskanje od tam, kjer je bilo prekinjeno, vendar nedvoumno označiti, na kateri prej natisnjeni del se nadaljevanje nanaša.

17. Opozorila

- 139 Zapisovalna naprava mora voznika opozoriti, kakor hitro zazna dogodek in/ali napako.
- 140 Opozorilo na izpad napajanja je lahko naknadno, po ponovni vzpostavitvi napajanja.
- 141 Zapisovalna naprava mora voznika opozoriti 15 minut vnaprej in ko je presežen čas neprekinjene vožnje 4 ur in 30 minut.
- 142 Opozorilo mora biti vizualno. Vizualno opozorilo je lahko dopolnjeno tudi z zvočnim opozorilom.

- 143 Vizualna opozorila morajo biti taka, da jih uporabnik jasno zazna, prilagojena voznikovemu vidnemu polju in jasno čitljiva podnevi in ponoči.
- 144 Prikazovalnik vizualnih opozoril je lahko vgrajen v zapisovalni napravi ali nameščen posebej.
- 145 Če je vgrajen posebej, mora biti označen s simbolom „T“ in biti jantarne ali oranžne barve.
- 146 Opozorila morajo trajati najmanj 30 sekund, če jih uporabnik vmes ne potrdi s pritiskom na katero koli tipko na zapisovalni napravi. Ta prva potrditev ne sme zbrisati prikaza vzroka opozorila, navedenega v naslednjem odstavku.
- 147 Na zapisovalni napravi se mora prikazati vzrok opozorila in ostati viden, dokler ga uporabnik ne potrdi z namensko tipko na zapisovalni napravi ali ukazom.
- 148 Dodatna opozorila so dovoljena, če jih voznik ne more zamenjati z zgoraj opredeljenimi opozorili.

18. Prenos podatkov na zunanje medije

- 149 Zapisovalna naprava mora biti zmožna na zahtevo prenašati podatke iz svojega pomnilnika ali z voznikove kartice na zunanji pomnilni medij skozi konektor za kalibriranje/prenos podatkov. Pred začetkom prenosa mora zapisovalna naprava posodobiti podatke shranjene na ustrezni kartici.
- 150 Poleg tega lahko kot opcijsko funkcijo zapisovalna naprava v katerem koli režimu delovanja omogoča prenos podatkov tudi skozi kak drug konektor podjetju, ki se avtentificira na tem kanalu. Za tak prenos veljajo dostopne pravice, ki veljajo v režimu del v podjetju.
- 151 Pri prenosu se noben shranjeni podatek ne sme spremeniti ali zbrisati.

Električni vmesnik konektorja za kalibriranje/prenos podatkov je predpisan v dodatku 6.

Protokoli za prenos podatkov so predpisani v dodatku 7.

19. Iznos podatkov na dodatne zunanje naprave

- 152 Če nima vgrajenih funkcij za prikaz hitrosti in/ali števca prevožene poti, mora zapisovalna naprava zagotavljati izhodni signal (izhodna signala) za prikaz hitrosti na merilniku hitrosti in/ali števcu prevožene poti, vgrajenem (vgrajenih) v vozilu.
- 153 Enota v vozilu mora biti zmožna po ustrezni namenski serijski povezavi, neodvisni od opcijske povezave CAN preko vodila (ISO 11898 Cestna vozila – izmenjava digitalnih informacij – kontrolno območno omrežje (Controller Area Network, CAN) za komunikacije z veliko hitrostjo) iznašati naslednje podatke za obdelavo v drugih elektronskih napravah nameščenih v vozilu:
- tekoči datum in čas UTC,
 - hitrost vozila,
 - celotno prevoženo pot vozila (števce prevožene poti),
 - tekočo izbrano dejavnost voznika in sovoznika,
 - informacijo, ali je v voznikovi reži in v sovoznikovi reži vstavljena kakšna tahografska kartica, in če je, identifikacijske informacije o kartici (številko kartice in državo izdajateljico).

Poleg tega minimalnega seznama lahko zapisovalna naprava iznaša še druge podatke.

Kadar je ključ električnega kontakta vozila vključen, mora te podatke oddajati ves čas. Kadar je ključ električnega kontakta izključen, mora oddajati vsaj ustrezne podatke o vsaki menjavi voznikove ali sovoznikove dejavnosti in o vstavitvi ali izvleku tahografske kartice. Če je zapisovalna naprava katerega od izhodnih podatkov v stanju izključenega električnega kontakta vozila zadržala, jih mora posredovati, ko je električni kontakt spet vključen.

20. Kalibriranje

- 154 Funkcija kalibriranja mora omogočati:
- avtomatično povezavo zaznavala gibanja in VU,
 - digitalno prilagoditev konstante zapisovalne naprave (k) značilnemu koeficientu vozila (w) (vozila z dvema osnima prenosnima razmerjema ali več morajo biti opremljena s stikalno napravo, s katero se ta prenosna razmerja avtomatsko prilagodijo s tistim razmerjem, za katerega je naprava nastavljena na vozilu),
 - nastavitev (neomejeno) tekočega časa,
 - nastavitev tekoče vrednosti števca prevožene poti,
 - posodobitev identifikacijskih podatkov zaznavala gibanja shranjenih v pomnilniku podatkov,
 - posodobitev ali potrditev drugih parametrov, ki so znani zapisovalni naprava, identifikacijo vozila, w, l, mere avtoplaščev in nastavitev naprave za omejevanje hitrosti, če pride v poštev.
- 155 Povezovanje zaznavala gibanja z VU mora obsegati najmanj:
- posodobitev namestitvenih podatkov zaznavala gibanja, ki jih hrani zaznavalo gibanja (po potrebi),
 - kopiranje potrebnih identifikacijskih podatkov zaznavala gibanja iz zaznavala gibanja v pomnilnik podatkov VU.
- 156 Funkcija kalibriranja mora podpirati vnos potrebnih podatkov skozi konektor za kalibriranje/prenos podatkov v skladu s protokolom kalibriranja, opredeljenim v dodatku 8. Funkcija kalibriranja lahko omogoča vnos podatkov tudi skozi druge konektorje.

21. Nastavljanje časa

- 157 Funkcija nastavljanja časa mora omogočati nastavljanje tekočega časa v korakih največ ene minute v časovnih razmakih vsaj sedem dni.
- 158 V režimu kalibriranja pa mora funkcija nastavljanja časa omogočati nastavljanje tekočega časa brez omejitev.

22. Delovne karakteristike

- 159 Zapisovalna naprava mora polno delovati v temperaturnem območju od $-20\text{ }^{\circ}\text{C}$ do $70\text{ }^{\circ}\text{C}$, zaznavalo gibanja pa v temperaturnem območju od $-40\text{ }^{\circ}\text{C}$ do $135\text{ }^{\circ}\text{C}$. Vsebinsa pomnilnika podatkov se mora ohraniti pri temperaturah do $-40\text{ }^{\circ}\text{C}$.
- 160 Zapisovalna naprava mora polno delovati v območju vlažnosti od 10 % do 90 %.
- 161 Zapisovalna naprava mora biti zaščitena pred prenapetostjo, zamenjavo polaritete napajanja in kratkimi stiki.
- 162 Zapisovalna naprava mora biti v skladu z Direktivo Komisije 95/54/ES z dne 31. oktobra 1995 ⁽¹⁾ o prilagoditvi Direktive Sveta 72/245/EGS ⁽²⁾ o elektromagnetni združljivosti tehničnemu napredku in mora biti zaščitena pred elektrostatičnimi razelektritvami in prehodnimi pojavi.

23. Gradiva

- 163 Vsi sestavni deli zapisovalne naprave morajo biti izdelani iz ustrezno obstojnih in mehansko trdnih gradiv s stabilnimi električnimi in magnetnimi lastnostmi.
- 164 Pri normalnih pogojih uporabe morajo biti notranji deli naprave zaščiteni pred vlago in prahom.
- 165 Enota v vozilu mora imeti stopnjo zaščite IP 40 po standardu IEC 529, zaznavalo gibanja pa stopnjo zaščite IP 64.

⁽¹⁾ UL L 266, 8.11.1995, str. 1.

⁽²⁾ UL L 152, 6.7.1972, str. 15.

166 Zapisovalna naprava mora biti v skladu z ustreznimi tehničnimi zahtevami glede ergonomije.

167 Zapisovalna naprava mora biti zaščiten pred nenamernimi poškodbami.

24. Oznake

168 Če zapisovalna naprava prikazuje stanje števca prevožene poti in hitrost vozila, morajo biti na tem prikazu naslednji podatki:

- poleg prikazane vrednosti prevožene poti merska enota prevožene poti, navedena kot kratica ,km‘,
- poleg prikazane vrednosti hitrosti oznaka ,km/h‘.

Zapisovalna naprava lahko omogoča tudi preklap na prikaz hitrosti v miljah na uro; pri takem prikazu mora biti poleg vrednosti hitrosti enota označena s kratico ,mph‘.

169 Na vsako samostojno nameščeno enoto zapisovalne naprave mora biti pritrjena označevalna ploščica z naslednjimi podatki:

- imenom in naslovom proizvajalca naprave,
- proizvajalčevo kataloško številko in letom proizvodnje,
- serijsko številko naprave,
- znakom odobritve naprave.

170 Če prostor fizično ne omogoča prikaza vseh zgoraj omenjenih podatkov, mora označevalna ploščica prikazovati vsaj: proizvajalčevo ime ali logo in kataloško številko dela.

IV. ZAHTEVE GLEDE IZDELAVE IN FUNKCIONALNE ZAHTEVE ZA TAHOGRAFSKE KARTICE

1. Vidni podatki

Prednja stran mora vsebovati:

171 besedi ,voznikova kartica‘ ali ,nadzorna kartica‘ ali ,delavniška kartica‘ ali ,kartica podjetja‘ glede na vrsto kartice, natisnjeni z velikimi črkami v uradnem jeziku države izdajateljice kartice,

172 iste besede v drugih uradnih jezikih Skupnosti, ki so natisnjeni kot grafično ozadje 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 ΟΔΗΓΟΥ	ΚΑΡΤΑ ΕΛΕΓΧΟΥ	ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΗΣ
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTROLEUR	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 CENTRO DE ENSAIO	CARTÃO DE EMPRESA
FI	KULJETTAJA KORTTILLA	VALVONTA KORTILLA	TESTAUSASEMA KORTILLA	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

173 ime države izdajateljice (neobvezno),

- 174 oznako države članice, ki izda kartico, natisnjena v negativu v modrem pravokotniku in obkrožena z 12 rumenimi zvezdami; oznake so naslednje:

B	Belgija
DK	Danska
D	Nemčija
GR	Grčija
E	Španija
F	Francija
IRL	Irska
I	Italija
L	Luksemburg
NL	Nizozemska
A	Avstrija
P	Portugalska
FIN	Finska
S	Švedska
UK	Združeno kraljestvo

- 175 informacije po vrstah kartic, oštevilčene, kakor sledi:

	Voznikova kartica	Nadzorna kartica	Kartica podjetja ali delavniška kartica
1.	Priimek voznika	Ime nadzornegaorgana	Kartica podjetja ali delavniška kartica
2.	Osebnostno ime (imena) voznika	Priimek nadzornika(če pride v poštev)	Priimek imetnika kartice (če pride v poštev)
3.	Rojstni datum voznika	Osebnostno ime (imena) nadzornika(če pride v poštev)	Osebnostno ime (imena) imetnika kartice (če pride v poštev)
4.(a)	Datum začetka veljavnosti kartice		
(b)	Datum poteka veljavnosti (če je določen)		
(c)	Ime pristojnega izdajatelja (je lahko natisnjeno na 2. strani)		
(d)	Številka pod postavko 5 v drugi obliki, za administrativne namene (neobvezno)		
5.(a)	Številka voznškega dovoljenja (na dan izdaje voznikove kartice)		
5.(b)	Številka kartice		
6.	Fotografija voznika	Fotografija kontrolorja (neobvezna)	—
7.	Podpis voznika	Podpis imetnika (neobvezen)	
8.	Naslov stalnega bivališča ali poštni naslov imetnika (neobvezen)	Poštni naslov nadzornega organa	Poštni naslov podjetja ali delavnice

- 176 176 datumi se pišejo v obliki ,dd/mm/llll' ali ,dd.mm.llll' (dan, mesec, leto);

zadnja stran bovsbovala:

- 177 razlago oštevilčenih postavk na prednji strani kartice,

- 178 ob izrecnem pisnem soglasju imetnika se lahko doda tudi informacije, ki niso vezane na administriranje kartic; te informacije pa ne smejo na noben način spremeniti načina uporabe modela kot tahografske kartice.

VZORCI TAHOGRFSKIH KARTIC V SKUPNOSTI

PREDNJA STRAN

ZADNJA STRAN

PREDNJA STRAN VOZNIKOVA KARTICA 1.  2.  3.  4a.  4c.  4d.  5a.  5b.  7.  (8.) 	DRŽAVA ČLANICA TARJETA DEL CONDUCTOR FØRERKORT FAHRERKARTE ΚΑΡΤΑ Ο ΔΗΤΟΥ 4b. DRIVER CARD CARTE DE CONDUCTEUR CÁRTA TIONÁNAÍ CARTA DEL CONDUCENTE BESTUURDESKAART CARTÃO DE CONDUTOR KULJETTAJAKORTTILLA FÖRARKORT
PREDNJA STRAN NADZORNA KARTICA 1.  2.  3.  4a.  4c.  4d.  5b.  7.  8. 	DRŽAVA ČLANICA TARJETA DE CONTROL KONTROLKORT KONTROLLKARTE ΚΑΡΤΑ ΕΛΕΓΧΟΥ 4b. CONTROL CARD CARTE DE CONTROLEUR CÁRTA STIÚRTHA CARTA DI CONTROLLO CONTOLEKAART CARTÃO DE CONTROLO VALVONTAKORTTILLA KONTROLLKORT
PREDNJA STRAN DELAVNIŠKA KARTICA 1.  2.  3.  4a.  4c.  4d.  5b.  7.  8. 	DRŽAVA ČLANICA TARJETA DEL CENTRO DE ENSAYO VÆRKSTEDSKORT WERKSTATTKARTE ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ 4b. WORKSHOP CARD CARTE D'ATELIER CÁRTA CEARDLAINNE CARTA DELL'OFFICINA WERKPLAATSKAART CARTÃO DO CENTRO DE ENSAIO TESTAUSASEMAKORTTILLA VERKSTADSKORT
PREDNJA STRAN KARTICA PODJETJA 1.  2.  3.  4a.  4c.  4d.  5b.  7.  8. 	DRŽAVA ČLANICA TARJETA DE LA EMPRESA VIRKSOMHEDSKORT UNTERNEHMENSKARTE ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΕΩΣ 4b. COMPANY CARD CARTE D'ENTREPRISE CÁRTA COMHLACHTA CARTA DELL'AZIENDA BEDRIJFSKAART CARTÃO DE EMPRESA YRITYSKORTTILLA FÖRETAGSKORT

179 Tahografske kartice morajo biti natisnjene na ozadjih naslednjih prevladujočih barv:

- voznikova kartica: bela,
- nadzorna kartica: modra,
- delavniška kartica: rdeča,
- kartica podjetja: rumena.

180 Telo tahografske kartice mora biti zaščiteno pred ponarejanjem in nepooblaščenimi posegi vsaj z naslednjimi zaščitami:

- varnostni vzorec ozadja s finimi črtnimi vzorci in mavričnim tiskom,
- v območju fotografije se morata varnostni vzorec ozadja in fotografija prekrivati,
- vsaj ena dvobarvna črta v mikrotisku.

- 181 Po posvetu s Komisijo lahko država članica uporabi kake dodatne barve ali oznake, npr. nacionalne simbole in zaščite, brez poseganja v druge določbe te priloge.

2. Varnost

Cilji varnosti sistema so zaščita celovitosti in avtentičnosti podatkov, izmenjanih med karticami in zapisovalno napravo, zaščita celovitosti in avtentičnosti podatkov, prenesenih s kartic, s tem, da se se dovoljuje določene operacije pisanja na kartice samo zapisovalni napravi, kar izključi vsako možnost ponarejanja podatkov, shranjenih na karticah, prepreči nepooblaščen poseg in zazna kakršen koli poskus takega posega.

- 182 Za zagotovitev varnosti sistema morajo tahografske kartice izpolnjevati varnostne zahteve opredeljene v generičnih varnostnih ciljih za tahografske kartice (dodatek 10).

- 183 Tahografske kartice morajo biti berljive z drugo opremo, npr. osebnimi računalniki.

3. Standardi

- 184 Tahografske kartice morajo biti v skladu z naslednjimi standardi:

- ISO/IEC 7810 Identifikacijske kartice – fizične lastnosti,
- ISO/IEC 7816 Identifikacijske kartice – kontaktna integrirana vezja:
 - Del 1: fizične lastnosti,
 - Del 2: mere in položaj kontaktov,
 - Del 3: elektronski signali in protokoli prenosa,
 - Del 4: skupni ukazi za izmenjavo,
 - Del 8: skupni ukazi povezani z varnostjo,
- ISO/IEC 10373 Identifikacijske kartice – metode preskušanja.

4. Okoljske in električne tehnične zahteve

- 185 Tahografske kartice morajo delovati pravilno v vseh podnebnih pogojih, ki jih normalno lahko srečamo na območju Skupnosti, in najmanj v območju temperatur od -25°C do $+70^{\circ}\text{C}$ z občasnimi temperaturnimi konicami do $+85^{\circ}\text{C}$, pri čemer 'občasno' pomeni ne več kakor 4 ure naenkrat in skupaj ne več kakor 100-krat v dobi uporabe kartice.
- 186 Tahografske kartice morajo delovati pravilno v območju vlažnosti od 10 % do 90 %.
- 187 Tahografske kartice morajo ob uporabi v predpisanih okoljskih in električnih pogojih delovati pravilno pet let.
- 188 Med delovanjem morajo tahografske kartice izpolnjevati zahteve Direktive Komisije 95/54/ES z dne 31. oktobra 1995 ⁽¹⁾ o elektromagnetni združljivosti in morajo biti zaščitene pred elektrostatičnimi razelektritvami.

5. Hranjenje podatkov

V okviru te točke velja naslednje:

- časi so zapisani z ločljivostjo ene minute, če ni predpisano drugače,
- vrednosti števca prevožene poti so zapisani z ločljivostjo enega kilometra,
- hitrosti so zapisane z ločljivostjo 1 km/h.

Funkcije, ukazi in logične strukture tahografskih kartic, s katerimi se izpolni zahteve glede hranjenja podatkov, so predpisani v dodatku 2.

⁽¹⁾ UL L 266, 8.11.1995, str. 1.

- 189 Ta člen predpisuje minimalne zmogljivosti hranjenja podatkov za različne aplikativne podatkovne datoteke. Tahografske kartice morajo biti zmožne posredovati zapisovalni napravi podatke o dejanskih zmogljivosti teh podatkovnih datotek.

Morebitni drugi podatki, ki jih hrani tahografska kartica v zvezi s svojimi drugimi aplikacijami, morajo biti hranjeni v skladu z Direktivo 95/46/ES z dne 24. oktobra 1995 o zaščiti posameznika pri obdelavi osebnih podatkov in o prostem pretoku teh podatkov ⁽¹⁾.

5.1 **Identifikacijski podatki kartice in varnostni podatki**

5.1.1 *Identifikacija aplikacije*

- 190 Tahografska kartica mora biti zmožna hraniti naslednje identifikacijske podatke aplikacije:

- identifikacija tahografske aplikacije,
- vrsta identifikacije tahografske kartice.

5.1.2 *Identifikacija čipa*

- 191 Tahografska kartica mora biti zmožna hraniti naslednje identifikacijske podatke integriranega vezja (IC):

- serijska številka IC,
- proizvodni podatki IC.

5.1.3 *Identifikacija kartice s tiskanim vezjem*

- 192 Tahografska kartica mora biti zmožna hraniti naslednje identifikacijske podatke pametne kartice:

- serijska številka kartice (vključno s proizvodnimi podatki),
- številka odobritve tipa kartice,
- identifikacija (ID) personalizatorja kartice,
- identifikacija (ID) vgraditelja čipa,
- identifikator IC.

5.1.4 *Varnostni elementi*

- 193 Tahografska kartica mora biti zmožna hraniti naslednje podatke varnostnih elementov:

- Evropski javni ključ,
- certifikat države članice,
- certifikat kartice,
- zasebni ključ kartice.

5.2 **Voznikova kartica**

5.2.1 *Identifikacija kartice*

- 194 Voznikova kartica mora biti zmožna hraniti naslednje identifikacijske podatke kartice:

- številka kartice,
- država izdajateljica, ime organa izdajatelja, datum izdaje,
- datum začetka veljavnosti kartice, datum poteka veljavnosti kartice.

⁽¹⁾ UL L 281, 23.11.1995, str. 31.

5.2.2 Identifikacija imetnika kartice

195 Voznikova kartica mora biti zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

- priimek imetnika,
- osebno ime (imena) imetnika,
- datum rojstva,
- izbrani jezik.

5.2.3 Podatki o vozniskem dovoljenju

196 Voznikova kartica mora biti zmožna hraniti naslednje podatke o vozniskem dovoljenju:

- država izdajateljica, ime organa izdajatelja
- številka vozniskega dovoljenja (na dan izdaje voznikove kartice).

5.2.4 Podatki o uporabljenih vozilih

197 Voznikova kartica mora biti zmožna hraniti za vsak koledarski dan, na katerega je bila kartica uporabljena, in za vsako obdobje uporabe določenega vozila na ta dan (obdobje uporabe vključuje vse cikle vstavitve/izvleka kartice v vozilu z vidika kartice) naslednje podatke:

- datum in čas prve uporabe vozila (t.j. prve vstavitve kartice v tem obdobju uporabe vozila ali čas 00.00, če v tem času teče uporaba vozila),
- vrednost števca prevožene poti ob tem času,
- datum in čas zadnje uporabe vozila (t.j. zadnjega izvleka kartice v tem obdobju uporabe vozila ali čas 23.59, če v tem času teče uporaba vozila),
- vrednost števca prevožene poti ob tem času,
- registrska številka vozila in država, v kateri je vozilo registrirano.

198 Voznikova kartica mora biti zmožna hraniti najmanj 84 takih zapisov.

5.2.5 Podatki o voznikovih dejavnostih

199 Voznikova kartica mora biti zmožna hraniti, za vsak koledarski dan, na katerega je bila kartica uporabljena, ali za katerega je voznik ročno vnesel dejavnosti, naslednje podatke:

- datum,
- števec dnevov prisotnosti (ki se poveča za eno ob vsakem takem novem koledarskem dnevu),
- celotno dolžino, ki jo je prevozil voznik na ta dan,
- stanje voznika ob 00.00,
- ob vsaki voznikovi spremembi dejavnosti in/ali ob vsaki spremembi stanja vožnje in/ali ob vsaki vstavitvi/izvleku kartice:
 - stanje vožnje (POSADKA, POSAMEZNIK),
 - reža (VOZNIK, SOVOZNIK),
 - stanje kartice (VSTAVLJENA, NI VSTAVLJENA),
 - dejavnost (VOŽNJA, RAZPOLOŽLJIVOST, DELO, ODMOR/POČITEK),
 - čas spremembe.

200 Pomnilnik podatkov na voznikovi kartici mora biti zmožen hraniti podatke o voznikovih dejavnostih najmanj 28 dni (povprečna voznikova dejavnost je opredeljena kot 93 sprememb dejavnosti na dan).

- 201 Podatki, našteti v zahtevah 197 in 199, morajo biti shranjeni tako, da je mogoče poizvedovanje po dejavnostih iz pomnilnika v zaporedju njihovih nastopov, tudi v primerih časovnih prekrivanj.

5.2.6 Kraji, v katerih se dnevne delovne izmene začnajo in/ali končajo

- 202 Voznikova kartica mora biti zmožna hraniti naslednje podatke v zvezi s kraji začetkov in/ali koncev dnevnih delovnih izmen, ki jih vnaša voznik:

- datum in čas vnosa (ali datum/čas povezan z vnosom, kadar je vnos opravljen s postopkom ročnega vnosa),
- vrsta vnosa (začetek ali konec, stanje vnosa),
- vnesena država in regija,
- vrednost števca prevožene poti vozila.

- 203 Voznikova kartica mora biti zmožna hraniti najmanj 42 parov takih zapisov.

5.2.7 Podatki o dogodkih

V okviru te točke velja, da se čas zapisuje z ločljivostjo ene sekunde.

- 204 Voznikova kartica mora biti zmožna hraniti podatke povezane z naslednji dogodki, ki jih zazna zapisovalna naprava v času, ko je kartica vstavljena:

- časovno prekrivanje (kjer je vzrok dogodka ta kartica),
- vstavitve kartice med vožnjo (kjer pri dogodku nastopa ta kartica),
- zadnja seja s kartico nepravilno zaključena (kjer pri dogodku nastopa ta kartica),
- prekinitev napajanja,
- napaka podatkov o gibanju,
- poskusi kršenja varnosti.

- 205 Voznikova kartica mora biti zmožna hraniti naslednje podatke o teh dogodkih:

- koda dogodka,
- datum in čas začetka dogodka (ali vstavitve kartice, če je dogodek ob tem času že tekkel),
- datum in čas konca dogodka (ali izvleka kartice, če je dogodek ob tem času še tekkel),
- registrska številka vozila, v katerem je dogodek nastopil, in država, v kateri je vozilo registrirano.

Opomba: Pri dogodku 'časovno prekrivanje':

- datum in čas začetka dogodka pomeni datum in čas izvleka kartice v prejšnjem vozilu,
- datum in čas konca dogodka pomeni datum in čas izvleka kartice v sedanjem vozilu,
- podatki o vozilu se nanašajo na sedanje vozilo, v katerem je dogodek nastopil.

Opomba: Pri dogodku 'zadnja seja s kartico nepravilno zaključena':

- datum in čas začetka dogodka sta datum in čas vstavitve kartice pri seji, ki ni bila pravilno zaključena,
- datum in čas konca dogodka sta datum in čas vstavitve kartice pri seji, v kateri je bil dogodek zaznan (tj. sedanji seji),
- podatki o vozilu se nanašajo na vozilo, v katerem seja s kartico ni bila pravilno zaključena.

206 Voznikova kartica mora biti zmožna hraniti podatke o šestih najnovejših dogodkih vsake vrste (tj. skupaj 36 dogodkih).

5.2.8 Podatki o napakah

V okviru te točke velja, da se čas zapisuje z ločljivostjo ene sekunde.

207 Voznikova kartica mora biti zmožna hraniti podatke povezane z naslednji napakami, ki jih zazna zapisovalna naprava v času, ko je kartica vstavljena:

- napaka kartice (kjer pri dogodku nastopa ta kartica),
- napaka na zapisovalni napravi.

208 Voznikova kartica mora biti zmožna hraniti naslednje podatke o teh napakah:

- koda napake,
- datum in čas začetka napake (ali vstavitve kartice, če je napaka ob tem času že tekla),
- datum in čas konca napake (ali izvleka kartice, če je napaka ob tem času še tekla),
- registrska številka vozila, v katerem je napaka nastopila, in država, v kateri je vozilo registrirano.

209 Voznikova kartica mora biti zmožna hraniti podatke o dvanajstih najnovejših napakah vsake vrste (tj. skupaj 24 napakah).

5.2.9 Podatki o nadzornih dejavnostih

210 Voznikova kartica mora biti zmožna hraniti naslednje podatke o nadzornih dejavnostih:

- datum in čas nadzora,
- številka in država izdajateljica nadzorne kartice,
- vrsta nadzora (prikazovanje in/ali tiskanje in/ali prenos podatkov iz VU in/ali prenos podatkov iz kartice (glej opombo)),
- v primeru prenosa podatkov obdobje, za katerega so preneseni podatki,
- registrska številka vozila, v katerem je potekal nadzor, in država, v kateri je vozilo registrirano.

Opomba: varnostne zahteve narekujejo, naj se prenos podatkov zabeleži le, če poteka preko zapisovalne naprave.

211 Voznikova kartica mora biti zmožna hraniti en tak zapis.

5.2.10 Podatki o sejah s kartico

212 Voznikova kartica mora biti zmožna hraniti naslednje podatke o vozilu, na katerem je bila odprta tekoča seja s to kartico:

- datum in čas odprtja seje (tj. vstavitve kartice) z ločljivostjo ene sekunde,
- registrska številka vozila in država, v kateri je registrirano.

5.2.11 Podatki o posebnih stanjih

212a Voznikova kartica mora biti zmožna hraniti naslednje podatke povezane s posebnimi stanji vnesenimi v času, ko je bila kartica vstavljena (v katerikoli reži):

- datum in čas vnosa,
- vrsta posebnega stanja.

212b Voznikova kartica mora biti zmožna hraniti 56 takih zapisov.

5.3 **Delavniška kartica**

5.3.1 *Varnostni elementi*

213 Delavniška kartica mora biti zmožna hraniti osebno identifikacijsko številko (PIN).

214 Delavniška kartica mora biti zmožna hraniti kriptografski ključ za povezovanje zaznaval gibanja z enotami v vozilu.

5.3.2 *Identifikacija kartice*

215 Delavniška kartica mora biti zmožna hraniti naslednje identifikacijske podatke kartice:

- številka kartice,
- država izdajateljica, ime organa izdajatelja, datum izdaje,
- datum začetka veljavnosti kartice, datum poteka veljavnosti kartice.

5.3.3 *Identifikacija imetnika kartice*

216 Delavniška kartica mora biti zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

- ime delavnice,
- naslov delavnice,
- priimek imetnika,
- osebno ime (imena) imetnika,
- izbrani jezik.

5.3.4 *Podatki o uporabljenih vozilih*

217 Delavniška kartica mora biti zmožna hraniti zapise podatkov uporabljenih vozil na enak način kakor voznikova kartica.

218 Delavniška kartica mora biti zmožna hraniti najmanj 4 take zapise.

5.3.5 *Podatki o voznikovih dejavnostih*

219 Delavniška kartica mora biti zmožna hraniti podatke o dejavnostih voznika na enak način kakor voznikova kartica.

220 Delavniška kartica mora biti zmožna hraniti podatke o voznikovih dejavnostih za najmanj en dan povprečnih voznikovih dejavnosti.

5.3.6 *Podatki o začetkih in/ali zaključkih dnevnih delovnih izmen*

221 Delavniška kartica mora biti zmožna hraniti zapise podatkov o začetkih in/ali koncih dnevnih delovnih izmen na enak način kakor voznikova kartica.

222 Delavniška kartica mora biti zmožna hraniti najmanj tri pare takih zapisov.

5.3.7 *Podatki o dogodkih in napakah*

223 Delavniška kartica mora biti zmožna hraniti podatke o dogodkih in napakah na enak način kakor voznikova kartica.

224 Delavniška kartica mora biti zmožna hraniti podatke za tri najnovejše dogodke vsake vrste (tj. skupaj 18 dogodkov) in za šest najnovejših napak vsake vrste (tj. 12 napak).

5.3.8 *Podatki o kontrolnih dejavnostih*

225 Delavniška kartica mora biti zmožna hraniti podatke o nadzornih dejavnostih na enak način kakor voznikova kartica.

5.3.9 Podatki o kalibriranju in nastavljanju časa

- 226 Delavniška kartica mora biti zmožna hraniti zapise o kalibriranjih in/ali nastavljanjih časa, opravljenih pri kartici vstavljeni v zapisovalno napravo.
- 227 Vsak zapis o kalibriranju mora obsegati naslednje podatke:
- namen kalibriranja (prvo nameščanje, nameščanje, rednakontrola),
 - identifikacija vozila,
 - posodobljeni ali potrjeni parametri (w, k, l, mere avtoplaščev, nastavitve naprave za omejevanje hitrosti (stare in nove vrednosti), datum in čas (stare in nove vrednosti),
 - identifikacija zapisovalne naprave (kataloška številka VU; serijska številka VU, serijska številka zaznavala gibanja).
- 228 Delavniška kartica mora biti zmožna hraniti najmanj 88 takih zapisov.
- 229 Delavniška kartica mora imeti vgrajen števec, ki kaže, koliko kalibriranj je že bilo opravljenih s to kartico.
- 230 Delavniška kartica mora imeti vgrajen števec, ki kaže, koliko kalibriranj je že bilo opravljenih s to kartico od zadnjega prenosa podatkov z nje.

5.3.10 Podatki o posebnih stanjih

- 230a Delavniška kartica mora biti zmožna hraniti podatke o posebnih stanjih na enak način kakor voznikova kartica. Delavniška kartica mora biti zmožna hraniti dva taka zapisa.

5.4 Nadzorna kartica

5.4.1 Identifikacija kartice

- 231 Nadzorna kartica mora biti zmožna hraniti naslednje identifikacijske podatke kartice:
- številka kartice,
 - država izdajateljica, ime organa izdajatelja, datum izdaje,
 - datum začetka veljavnosti kartice, datum poteka veljavnosti kartice (če je določen).

5.4.2 Identifikacija imetnika kartice

- 232 Nadzorna kartica mora biti zmožna hraniti naslednje identifikacijske podatke imetnika kartice:
- ime nadzornega organa,
 - naslov nadzornega organa,
 - priimek imetnika,
 - osebno ime (imena) imetnika,
 - izbrani jezik.

5.4.3 Podatki o nadzornih dejavnostih

- 233 Nadzorna kartica mora biti zmožna hraniti naslednje podatke o nadzornih dejavnostih:
- datum in čas nadzora,
 - vrsta nadzora (prikazovanje in/ali tiskanje in/ali prenos podatkov iz VU in/ali prenos podatkov iz kartice),

- obdobje, katerega podatki so preneseni (če je bil prenos opravljen),
- registrska številka vozila in država, v kateri je vozilo registrirano,
- številka in država izdajateljica nadzorovane voznikove kartice.

234 Delavniška kartica mora biti zmožna hraniti najmanj 230 takih zapisov.

5.5 **Kartica podjetja**

5.5.1 *Identifikacija kartice*

235 Kartica podjetja mora biti zmožna hraniti naslednje identifikacijske podatke kartice:

- številka kartice,
- država izdajateljica, ime organa izdajatelja, datum izdaje,
- datum začetka veljavnosti kartice, datum poteka veljavnosti kartice (če je določen).

5.5.2 *Identifikacija imetnika kartice*

236 Kartica podjetja mora biti zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

- ime podjetja,
- naslov podjetja.

5.5.3 *Podatki o dejavnostih podjetja*

237 Kartica podjetja mora biti zmožna hraniti naslednje podatke o dejavnostih podjetja:

- datum in čas dejavnosti,
- vrsta dejavnosti (vklop in/ali izklop blokade VU; prenos podatkov z VU in/ali kartice),
- obdobje, katerega podatki so preneseni (če je bil prenos opravljen),
- registrska številka vozila in država, v kateri je vozilo registrirano,
- številka in država izdajateljica kartice (če je bil opravljen prenos podatkov s kartice).

238 Kartica podjetja mora biti zmožna hraniti najmanj 230 takih zapisov.

V. NAMESTITEV ZAPISOVALNE NAPRAVE

1. **Namestitev**

239 Nova zapisovalna naprava se dobavlja izvajalcem namestitve ali proizvajalcem vozil neaktivirana, z vsemi kalibracijskimi parametri naštetimi v točki III(20) nastavljenimi na ustrezne in veljavne privzete vrednosti. Kjer ni ustrezna nobena privzeta vrednost, naj bodo besedilni parametri nastavljeni kot nizi znakov ,?' , številski parametri pa na vrednosti ,0'.

240 Dokler ni aktivirana, naj zapisovalna naprava omogoča dostop do funkcije kalibriranja tudi kadar ni v režimu kalibriranja.

241 Dokler ni aktivirana, naj zapisovalna naprava ne zapisuje niti hrani podatkov, omenjenih v točkah III.12.3 do III.12.9 in III.12.12 do III.12.14.

242 Pri nameščanju morajo proizvajalci vozil nastaviti vse znane parametre.

- 243 Proizvajalci vozil ali izvajalci namestitve morajo, preden vozilo zapusti delavnico, v kateri je bila opravljena namestitev, nameščeno zapisovalno napravo aktivirati.
- 244 Aktiviranje zapisovalne naprave mora avtomatsko sprožiti prva vstavitev delavniške kartice v katerokoli od vmesniških naprav za kartice.
- 245 Pred aktiviranjem ali med njim se morajo avtomatsko opraviti tudi vse potrebne operacije povezave med zaznavalom gibanja in enoto v vozilu.
- 246 Po aktiviranju mora zapisovalna naprava polno opravljati predpisane funkcije in omejevati dostop do podatkov.
- 247 Po prvem aktiviranju mora zapisovalna naprava polno opravljati funkcije zapisovanja in hranjenja podatkov.
- 248 Namestitvi sledi kalibriranje. Prvo kalibriranje vključuje vnos registrske številke vozila in mora biti opravljeno najpozneje v dveh tednih po namestitvi ali po registraciji vozila, kar od tega dvojega je kasnejše.
- 248a Zapisovalna naprava mora biti vgrajena v vozilu tako, da lahko voznik doseže potrebne funkcije s svojega sedeža.

2. Namestitvena ploščica

- 249 Po preverjanju zapisovalne naprave ob namestitvi se nanjo ali ob njej pritrdi jasno vidna in enostavno dostopna namestitvena ploščica. Po vsaki kontroli pri pooblaščenem izvajalcu ali delavnici se namesto prejšnje ploščice pritrdi nova ploščica.
- 250 Na ploščici morajo biti vsaj naslednji podatki:
- ime, naslov ali blagovno ime pooblaščenega izvajalca ali delavnice,
 - značilni koeficient vozila v obliki $w = \dots \text{ imp/km'}$,
 - konstanta zapisovalne naprave v obliki $k = \dots \text{ imp/km'}$,
 - efektivni obseg avtoplaščev v obliki $l = \dots \text{ mm'}$,
 - mere avtoplaščev,
 - datum določitve značilnega koeficienta vozila in merjenja efektivnega obsega avtoplaščev,
 - identifikacijska številka vozila.

3. Plombiranje

- 251 Plombirani morajo biti naslednji deli:
- vsi priključki, ki bi lahko odklopljeni omogočili izvedbo nezaznavnih sprememb ali nezaznavno izgubo podatkov,
 - namestitvena ploščica, če ni pritrjena tako, da je ni mogoče odstraniti brez uničenja oznak na njej.
- 252 Zgoraj omenjene plombe se sme odstraniti:
- v primeru sile,
 - za namestitev, nastavev ali popravilo naprave za omejevanje hitrosti vozila ali kake druge naprave za varno vožnjo, pod pogojem, da zapisovalna naprava tudi po tem deluje zanesljivo in pravilno ter da jo po namestitvi naprave za omejevanje hitrosti vozila ali druge naprave za varno vožnjo pooblaščen izvajalec ali delavnica ponovno plombira takoj (v skladu s poglavjem IV), v drugih primerih pa najpozneje v sedmih dneh.

- 253 Ob vsakem prelomu plomb je treba pripraviti pisno izjavo o razlogih za to dejanje in jo dati na voljo pristojnim organom.

VI. PREVERJANJA, KONTROLE IN POPRAVILA

Zahteve glede okoliščin, ki upravičujejo prelom plomb, omenjene v členu 12.5 Uredbe (EGS) št. 3821/85, nazadnje spremenjene z Uredbo (ES) št. 2135/98, so opredeljene v točki V(3) te priloge.

1. Odobritev izvajalcev ali delavnic

Države članice odobravajo, redno nadzorujejo in certificirajo organe, ki izvajajo:

- nameščanje,
- preverjanja,
- kontrole,
- popravila.

V okviru člena 12(1) te uredbe se delavniške kartice izdajajo le izvajalcem in/ali delavnicam, odobrenim za aktiviranje in/ali kalibriranje zapisovalne naprave v skladu s to prilogo in, če ni ustrezno utemeljeno drugače:

- ki niso upravičeni do kartice podjetja,
- in katerih druge poslovne dejavnosti ne pomenijo potencialnega tveganja za varnost sistema, opredeljeno v dodatku 10.

2. Preverjanje novih in popravljenih instrumentov

- 254 Vsako posamezno napravo, novo ali popravljeno, se preveri glede pravilnosti delovanja in točnosti odčitavanja in zapisovanja v okviru mej predpisanih v točkah III.2.1 in III.2.2 s plombiranjem v skladu s točko V.3 in kalibriranjem.

3. Pregled namestitve

- 255 Ob namestitvi na vozilo mora celotna instalacija (vključno z zapisovalno napravo) izpolnjevati določbe o največjih dovoljenih pogreških iz točk III.2.1 in III.2.2.

4. Redne kontrole

- 256 Redne kontrole v vozilu nameščene opreme se opravljajo po vsakem popravilu opreme ali po vsaki spremembi značilnega koeficienta vozila ali efektivnega obsega avtoplaščev ali po tem, ko napaka UTC časa opreme preseže 20 minut, ali po spremembi registrske številke vozila, ali najpozneje dve leti (24 mesecev) po zadnji kontroli.

- 257 Te kontrole obsegajo naslednja preverjanja:

- ali zapisovalna naprava deluje pravilno, vključno s funkcijo shranjevanja podatkov na tahografske kartice,
- ali je zagotovljena skladnost z določbami točk III.2.1 in III.2.2 o največjih tolerancah celotne instalacije,
- ali ima zapisovalna naprava oznako odobritve tipa,
- ali je pritrjena namestitvena ploščica,
- ali so plombe na napravi in na drugih delih instalacije nedotaknjene,
- preverjanje dejanskega obsega avtoplaščev.

258 Ti pregledi morajo obsegati tudi kalibriranje.

5. Meritve pogreškov

259 Meritve pogreškov ob namestitvi in med uporabo morajo biti opravljene pod naslednjimi pogoji, ki veljajo za standardne preskusne pogoje:

- vozilo neobremenjeno, pripravljeno za vožnjo,
- tlak v avtoplaščih v skladu z navodili proizvajalca,
- obraba avtoplaščev v okviru omejitev, ki jih določajo nacionalni predpisi,
- gibanje vozila:
 - vozilo se premika na lastni motorni pogon v ravni črti na ravni podlagi s hitrostjo 50 ± 5 km/h. Merilna razdalja mora biti vsaj 1 000 m,
- za ta preskus se lahko uporabi tudi kaka druga metoda primerljive točnosti, npr. ustrezna preskusna proga.

6. Popravila

260 Delavnica mora imeti zmogljivosti za prenos podatkov z zapisovalne naprave, tako da lahko te podatke posreduje nazaj prevoznemu podjetju.

261 Če okvara zapisovalna naprave, tudi po popravilu v delavnici, onemogoča prenos zapisanih podatkov, pooblaščen delavnica izda prevoznemu podjetju certifikat, da podatkov ni mogoče prenesti z zapisovalne naprave. Delavnica mora hraniti kopijo vsakega izdanega certifikata najmanj eno leto.

VII. IZDAJANJE KARTIC

Procesi izdajanja kartic, ki jih vzpostavijo posamezne države članice, morajo biti v skladu z naslednjimi določbami:

- 262 Ob prvi izdaji tahografske kartice prosilcu morajo biti zaporedna tekoča številka kartice (če obstaja), zaporedna številka zamenjave in zaporedna številka obnovitve nastavljene na ,0'.
- 263 Številke kartic pri neosebni tahografskih karticah, ki se jih izda enemu nadzornemu organu ali eni delavnici ali enemu prevoznemu podjetju, morajo imeti prvih 13 števil enakih, zaporedne tekoče številke pa morajo biti različne.
- 264 Tahografska kartica, ki se jo izda kot zamenjavo za obstoječo tahografsko kartico, mora imeti enako številko kartice kakor zamenjana kartica, le zaporedna številka zamenjave se poveča za ,1' (v vrstnem redu 0...9, A...Z).
- 265 Tahografska kartica, ki se jo izda kot zamenjavo za obstoječo tahografsko kartico, mora imeti isti datum poteka veljavnosti kakor zamenjana kartica.
- 266 Tahografska kartica, ki se jo izda kot obnovitev obstoječe tahografske kartice, mora imeti enako številko kartice kakor kartica, ki se jo obnavlja, le zaporedna številka zamenjave se vrne na vrednost ,0', zaporedna številka obnovitve pa se poveča za ,1' (v vrstnem redu 0...9, A...Z).
- 267 Zamenjava obstoječe tahografske kartice, potrebna za spremembo administrativnih podatkov, poteka po pravilih za obnovitev kartice, če se izvede v isti državi članici, ali po pravilih za prvo izdajo kartice, če se izvede v drugi državi članici.
- 268 V polje ,priimek imetnika kartice' se pri neosebni delavniški ali nadzorni kartici zapiše ime delavnice ali nadzornega organa.

VIII. ODOBRITEV TIPA ZAPISOVALNE NAPRAVE IN TAHOGRAFSKIH KARTIC

1. Splošno

V okviru tega poglavja izraz ,zapisovalna naprava' pomeni ,zapisovalno napravo ali njene sestavne dele'. Za kabel (kable) za povezavo zaznavala gibanja z enoto v vozilu ni potrebnaodobritev tipa. Papir, ki ga uporablja zapisovalna naprava, šteje kot sestavni del zapisovalne naprave.

- 269 Zapisovalna naprava mora biti predložena v odobritev skupaj z vsemi vgrajenimi dodatnimi napravami.
- 270 Odobritev tipa zapisovalne naprave in tahografskih kartic obsega varnostne preskuse, funkcionalne preskuse in preskuse skupne uporabnosti. Pozitivne rezultate vsakega od teh preskusov se navede v ustreznem certifikatu.
- 271 Organi držav članic, ki so pristojni za odobritev tipa, ne izdajo certifikata o odobritvi tipa v skladu s členom 5 te uredbe, če nimajo:
- varnostnega certifikata,
 - funkcionalnega certifikata,
 - in certifikata skupne uporabnosti
- za zapisovalno napravo ali tahografsko kartico, ki je predmet odobritve tipa.
- 272 O vsaki spremembi programske opreme, strojne opreme ali vrste gradiv, uporabljenih pri njeni izdelavi, je treba pred uporabo obvestiti organ, ki je napravo tipsko odobril. Ta organ lahko proizvajalcu podaljša odobritev tipa, lahko pa zahteva posodobitev ali potrditev ustreznih funkcionalnih, varnostnih certifikatov in/ali certifikatov skupne uporabnosti.
- 273 Postopke za nadgradnjo nameščene zapisovalne naprave mora odobriti organ, ki je zapisovalno napravo tipsko odobril. Nadgradnja programske opreme ne sme spremeniti ali zbrisati nobenih podatkov o vzrokih dejavnosti, shranjenih v zapisovalni napravi. Nadgradnja programske opreme se sme izvesti le na odgovornost proizvajalca opreme.

2. Varnostni certifikat

- 274 Varnostni certifikat se izda v skladu z določbami dodatka 10 te priloge.

3. Funkcionalni certifikat

- 275 Vlagatelj zahtevka za tipsko odobritev mora organu države članice, pristojnemu za odobritev tipa, predložiti vsa gradiva in dokumentacijo, ki jih ta organ smatra za potrebna.
- 276 Funkcionalni certifikat se izda proizvajalcu šele po tem, ko so uspešno opravljeni vsaj vsi funkcionalni preskusi, predpisani v dodatku 9.
- 277 Organ, pristojen za odobritev tipa, izda funkcionalni certifikat. Ta certifikat navaja poleg imena prejemnika in identifikacije modela tudi podroben seznam opravljenih preskusov in doseženih rezultatov.

4. Certifikat skupne uporabnosti

- 278 Preskusi skupne uporabnosti se opravljajo v enem samem laboratoriju, za katerega je pristojna in zanj odgovarja Evropska komisija.
- 279 Laboratorij registrira zahtevke proizvajalcev za preskuse skupne uporabnosti v vrstnem redu njihove predložitve.
- 280 Zahtevek se uradno registrira šele takrat, ko laboratorij razpolaga s:
- vsemi gradivi in dokumentacijo, potrebnimi za te preskuse skupne uporabnosti,
 - ustreznim varnostnim certifikatom,
 - ustreznim funkcionalnim certifikatom.
- O datumu registracije zahtevka se obvesti proizvajalca.
- 281 Laboratorij ne opravi nikakršnih preskusov skupne uporabnosti za zapisovalno napravo ali tahografsko kartico, za katero še nista izdana varnostni certifikat in funkcionalni certifikat.
- 282 Proizvajalec, ki vložil zahtevek za preskuse skupne uporabnosti, se obveže laboratoriju, odgovornemu za te preskuse, prepustiti na razpolago vsa gradiva in dokumentacijo, ki jih je predložil za izvedbo preskusov.

- 283 Preskusi skupne uporabnosti se opravijo v skladu z določbami člena 5 dodatka 9 te priloge, ki zadevajo posamezni tip zapisovalne naprave ali tahografsko kartico:
- za katero tipska odobritev še velja, ali
 - za katero se tipska odobritev opravlja in ki ima veljaven certifikat skupne uporabnosti.
- 284 Laboratorij izda proizvajalcu certifikat skupne uporabnosti šele po uspešno opravljenih vseh zahtevanih preskusih skupne uporabnosti.
- 285 Če pri eni postavki ali več zapisovalne naprave ali tahografskih kartic preskusi skupne uporabnosti niso uspešni, kakor je predpisano v zahtevi 283, laboratorij proizvajalcu ne izda certifikata skupne uporabnosti, dokler ta ne izvede potrebnih sprememb in preskusi skupne uporabnosti niso uspešni. Laboratorij mora ob pomoči proizvajalca, ki ga napaka glede skupne uporabnosti zadeva, navesti vzrok problema in mora poskušati pomagati proizvajalcu pri iskanju tehnične rešitve. V primerih, ko proizvajalec spremeni svoj izdelek, mora na svojo odgovornost pri ustreznih organih ugotoviti, ali varnostni in funkcionalni certifikat za ta izdelek še veljata.
- 286 Certifikat skupne uporabnosti velja šest mesecev. Če proizvajalec v tem času ne pridobi ustreznega certifikata o odobritvi tipa, je preklican. Ta certifikat proizvajalec posreduje organu države članice, pristojnemu za odobritev tipa, pri katerem je bil izdan funkcionalni certifikat.
- 287 Nobenega elementa, ki bi bil lahko vzrok napake glede skupne uporabnosti, ni dopustno uporabiti za doseganje dobička ali prevladujočega položaja.

5. Certifikat o odobritvi tipa

- 288 Organ države članice, pristojen za odobritev tipa, izda certifikat o odobritvi tipa takoj, ko ima vse tri zahtevane certifikate.
- 289 Ko izda certifikat o odobritvi tipa proizvajalcu, pošlje kopijo certifikata tudi laboratoriju, pristojnemu za preskuse skupne uporabnosti.
- 290 Laboratorij, pristojen za preskuse skupne uporabnosti, mora vzdrževati javno spletno stran, na kateri objavlja tekoči seznam modelov zapisovalne naprave ali tahografskih kartic:
- za katere je registriral zahteve za preskuse skupne uporabnosti,
 - za katere je izdal certifikate skupne uporabnosti (tudi začasne),
 - za katere so bili izdani certifikati o odobritvi tipa.

6. Izjemni postopek: prvi certifikati skupne uporabnosti

- 291 Dokler ne bodo pretekli štirje meseci po izdaji certifikatov skupne uporabnosti za prvih nekaj modelov zapisovalne naprave in tahografskih kartic (voznikovih, delavniških, kontrolnih in kartic podjetja), bo vsak izdan certifikat skupne uporabnosti (tudi prvi izdani certifikat) pri zahtevkih registriranih v tem obdobju štel za začasnega.
- 292 Če bodo po izteku tega obdobja vsi obravnavani izdelki med seboj skupno uporabni, bodo vsi ustrezni certifikati skupne uporabnosti postali dokončni.
- 293 Če bodo v tem obdobju ugotovljene napake glede skupne uporabnosti, mora laboratorij, pristojen za preskuse skupne uporabnosti, ob pomoči vseh prizadetih proizvajalcev navesti vzroke problemov in jih mora pozvati k izvedbi potrebnih sprememb.
- 294 Če bodo tudi po koncu tega obdobja ostali nerešeni kakšni problemi v zvezi s skupno uporabnostjo, mora laboratorij, pristojen za preskuse skupne uporabnosti, v sodelovanju s prizadetimi proizvajalci in organi, pristojnimi za odobritev tipa, ki so izdali ustrezne funkcionalne certifikate, ugotoviti vzroke napak glede skupne uporabnosti in ugotoviti, katere spremembe mora izvesti vsak od prizadetih proizvajalcev. Iskanje tehničnih rešitev lahko traja največ dva meseca; če v tem času ne bo najdena skupna rešitev, mora Komisija po posvetovanju z laboratorijem, pristojnim za preskuse skupne uporabnosti, odločiti, katerim modelom naprave in tahografskih kartic bo izdala dokončne certifikate skupne uporabnosti, in svojo odločitev obrazložiti.
- 295 Vsi zahtevki za preskuse skupne uporabnosti, ki jih bo laboratorij registriral v času od konca štirimesečnega obdobja po izdaji prvega začasnega certifikata skupne uporabnosti do dne odločitve Komisije omenjene v zahtevi 294, bodo odloženi do rešitve začetnih problemov glede skupne uporabnosti. Te zahteve se bo nato obdelovalo v enakem vrstnem redu, kakor so bili registrirani.

Dodatek 1

SLOVAR PODATKOV

VSEBINA

1.	Uvod	322
1.1	Pristop pri opredeljevanju podatkovnih tipov	322
1.2	Literatura	322
2.	Opredelitve podatkovnih tipov	333
2.1	ActivityChangeInfo	333
2.2	Address	334
2.3	BCDString	334
2.4	CalibrationPurpose	334
2.5	CardActivityDailyRecord	335
2.6	CardActivityLengthRange	335
2.7	CardApprovalNumber	335
2.8	CardCertificate	335
2.9	CardChipIdentification	335
2.10	CardConsecutiveIndex	336
2.11	CardControlActivityDataRecord	336
2.12	CardCurrentUse	336
2.13	CardDriverActivity	336
2.14	CardDrivingLicenceInformation	337
2.15	CardEventData	337
2.16	CardEventRecord	337
2.17	CardFaultData	338
2.18	CardFaultRecord	338
2.19	CardIccIdentification	338
2.20	CardIdentification	339
2.21	CardNumber	339
2.22	CardPlaceDailyWorkPeriod	339
2.23	CardPrivateKey	340
2.24	CardPublicKey	340
2.25	CardRenewalIndex	340
2.26	CardReplacementIndex	340
2.27	CardSlotNumber	340
2.28	CardSlotsStatus	340
2.29	CardStructureVersion	341

2.30	CardVehicleRecord	341
2.31	CardVehiclesUsed	341
2.32	Certificate	342
2.33	CertificateContent	342
2.34	CertificateHolderAuthorisation	342
2.35	CertificateRequestID	343
2.36	CertificationAuthorityKID	343
2.37	CompanyActivityData	343
2.38	CompanyActivityType	344
2.39	CompanyCardApplicationIdentification	344
2.40	CompanyCardHolderIdentification	344
2.41	ControlCardApplicationIdentification	345
2.42	ControlCardControlActivityData	345
2.43	ControlCardHolderIdentification	345
2.44	ControlType	346
2.45	CurrentDateTime	346
2.46	DailyPresenceCounter	346
2.47	Datef	347
2.48	Distance	347
2.49	DriverCardApplicationIdentification	347
2.50	DriverCardHolderIdentification	347
2.51	EntryTypeDailyWorkPeriod	348
2.52	EquipmentType	348
2.53	EuropeanPublicKey	348
2.54	EventFaultType	348
2.55	EventFaultRecordPurpose	349
2.56	ExtendedSerialNumber	350
2.57	FullCardNumber	350
2.58	HighResOdometer	350
2.59	HighResTripDistance	350
2.60	HolderName	350
2.61	K-ConstantOfRecordingEquipment	351
2.62	KeyIdentifier	351
2.63	L-TyreCircumference	351
2.64	Language	351
2.65	LastCardDownload	351
2.66	ManualInputFlag	351
2.67	ManufacturerCode	352

2.68	MemberStateCertificate	352
2.69	MemberStatePublicKey	353
2.70	Name	353
2.71	NationAlpha	353
2.72	NationNumeric	354
2.73	NoOfCalibrationRecords	355
2.74	NoOfCalibrationSinceDownload	355
2.75	NoOfCardPlaceRecords	355
2.76	NoOfCardVehicleRecords	355
2.77	NoOfCompanyActivityRecords	355
2.78	NoOfControlActivityRecords	356
2.79	NoOfEventsPerType	356
2.80	NoOfFaultsPerType	356
2.81	OdometerValueMidnight	356
2.82	OdometerShort	356
2.83	OverspeedNumber	356
2.84	PlaceRecord	356
2.85	PreviousVehicleInfo	357
2.86	PublicKey	357
2.87	RegionAlpha	357
2.88	RegionNumeric	357
2.89	RSAPublicModulus	358
2.90	RSAPublicExponent	358
2.91	RSAPrivateExponent	358
2.92	SensorApprovalNumber	358
2.93	SensorIdentification	358
2.94	SensorInstallation	359
2.95	SensorInstallationSecData	359
2.96	SensorOSIdentifier	359
2.97	SensorPaired	359
2.98	SensorPairingDate	360
2.99	SensorSerialNumber	360
2.100	SensorSCIdentifier	360
2.101	Signature	360
2.102	SimilarEventsNumber	360
2.103	SpecificConditionType	360
2.104	SpecificConditionRecord	360
2.105	Speed	361

2.106	SpeedAuthorised	361
2.107	SpeedAverage	361
2.108	SpeedMax	361
2.109	TdesSessionKey	361
2.110	TimeReal	361
2.111	TyreSize	361
2.112	VehicleIdentificationNumber	362
2.113	VehicleRegistrationIdentification	362
2.114	VehicleRegistrationNumber	362
2.115	VuActivityDailyData	362
2.116	VuApprovalNumber	362
2.117	VuCalibrationData	362
2.118	VuCalibrationRecord	363
2.119	VuCardIWDData	363
2.120	VuCardIWRRecord	364
2.121	VuCertificate	364
2.122	VuCompanyLocksData	364
2.123	VuCompanyLocksRecord	365
2.124	VuControlActivityData	365
2.125	VuControlActivityRecord	365
2.126	VuDataBlockCounter	365
2.127	VuDetailedSpeedBlock	365
2.128	VuDetailedSpeedData	366
2.129	VuDownloadablePeriod	366
2.130	VuDownloadActivityData	366
2.131	VuEventData	366
2.132	VuEventRecord	367
2.133	VuFaultData	367
2.134	VuFaultRecord	367
2.135	VuIdentification	368
2.136	VuManufacturerAddress	368
2.137	VuManufacturerName	368
2.138	VuManufacturingDate	368
2.139	VuOverSpeedingControlData	369
2.140	VuOverSpeedingEventData	369
2.141	VuOverSpeedingEventRecord	369
2.142	VuPartNumber	369
2.143	VuPlaceDailyWorkPeriodData	370

2.144	VuPlaceDailyWorkPeriodRecord	370
2.145	VuPrivateKey	370
2.146	VuPublicKey	370
2.147	VuSerialNumber	370
2.148	VuSoftInstallationDate	370
2.149	VuSoftwareIdentification	370
2.150	VuSoftwareVersion	371
2.151	VuSpecificConditionData	371
2.152	VuTimeAdjustmentData	371
2.153	VuTimeAdjustmentRecord	371
2.154	W-VehicleCharacteristicConstant	371
2.155	WorkshopCardApplicationIdentification	372
2.156	WorkshopCardCalibrationData	372
2.157	WorkshopCardCalibrationRecord	372
2.158	WorkshopCardHolderIdentification	373
2.159	WorkshopCardPIN	373
3.	Opredelitve območij vrednosti in velikosti	374
3.1	Opredelitve za voznikovo kartico	374
3.2	Opredelitve za delavniško kartico	374
3.3	Opredelitve za kontrolno kartico	374
3.4	Opredelitve za kartico podjetja	374
4.	Nabori znakov	374
5.	Kodiranje	374

1. UVOD

Ta dodatek določa podatkovne formate, podatkovne elemente in podatkovne strukture, ki se uporabljajo pri zapisovalni napravi in tahografskih karticah.

1.1 Pristop pri opredeljevanju podatkovnih tipov

V tem dodatku se za opredeljevanje podatkovnih tipov uporablja abstraktni sintaktični zapis ASN.1. Ta zapis omogoča enostavno in strukturirano opredeljevanje podatkov, hkrati pa ne predpisuje pravil kodiranja, ki so odvisna od aplikacije in izvedbenega okolja.

Konvencije poimenovanja tipov ASN.1 so v skladu s standardom ISO/IEC 8824-1. To pomeni naslednje:

- kjer je mogoče, je podatkovni tip nakazan že z izbranim imenom podatka,
- tudi kjer je podatkovni tip sestavljen iz drugih podatkovnih tipov, je ime podatkovnega tipa enovit niz črkovnih znakov, velike začetnice v okviru tega niza pa posredujejo ustrezní pomen,
- v splošnem so imena podatkovnih tipov povezana z imeni podatkovnih tipov, iz katerih so sestavljena, napravo, v katerih so ti podatki shranjeni, in funkcijami, povezanimi s temi podatki.

Če je določen podatkovni tip po ASN.1 že opredeljen v okviru kakega drugega standarda in če zadeva uporabo pri zapisovalni napravi, je tak tip po ASN.1, opredeljen v tem dodatku.

Da je mogoča uporaba več pravil kodiranja, so določeni tipi po ASN.1 v tem dodatku omejeni z identifikatorji območij vrednosti. Identifikatorji območij vrednosti so opredeljeni v točki 3.

1.2 Literatura

V tem dodatku so uporabljeni naslednji viri:

ISO 639	Pravilnik za predstavljanje imen jezikov. Prva izdaja: 1988
EN 726-3	Sistemi identifikacijskih kartic – Telekomunikacijske kartice in terminali s tiskanimi vezji – Del 3: Zahteve za kartice, neodvisne od aplikacije. December 1994
ISO 3779	Cestna vozila – Identifikacijska številka vozila (VIN) – Vsebina in struktura. 3. izdaja: 1983
ISO/IEC 7816-5	Informacijska tehnologija – Identifikacijske kartice – Kontaktne kartice s tiskanimi vezji – Del 5: Sistemi številčenja in postopek registracije za identifikatorje aplikacij. Prva izdaja: 1994 +Dopolnitev 1: 1996
ISO/IEC 8824-1	Informacijska tehnologija – Abstraktni sintaktični zapis 1 (ASN.1): Specifikacije osnovnega zapisa. 2. izdaja: 1998
ISO/IEC 8825-2	Informacijska tehnologija – pravila kodiranja ASN.1: specifikacije pravil paketnega kodiranja (PER).2. izdaja: 1998
ISO/IEC 8859-1	Informacijska tehnologija – nabori 8-bitnih enobajtnih grafičnih znakov – Del 1: nabor Latin 1. Prva izdaja: 1998
ISO/IEC 8859-7	Informacijska tehnologija – nabori 8-bitnih enobajtnih grafičnih znakov – Del 7: Latinski zapis grških znakov. Prva izdaja: 1987
ISO 16844-3	Cestna vozila – Tahografski sistemi – Vmesnik za zaznavalo gibanja. WD 3-20/05/99.

2. OPREDELITVE PODATKOVNIH TIPOV

Pri vsakem od podatkovnih tipov v nadaljevanju je privzeta vrednost za „neznano“ ali „ne pride v poštev“ podatkovni element zapolnjen z bajti „FF“.

2.1 ActivityChangeInfo

Ta podatkovni tip omogoča kodiranje, v okviru dvobajtne besede, stanja reže ob času 00.00 in/ali stanja voznika ob času 00.00 in/ali spremembe dejavnosti in/ali spremembe stanja vožnje in/ali spremembe stanja kartice za voznika ali sovoznika. Ta podatkovni tip je povezan z zahtevami 084, 109a, 199 in 219.

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

Prirejanje vrednosti – oktetno poravnano: 'scpaatttttttttt'B (16 bitov)

Za zapis v pomnilnik podatkov (ali stanje reže):

's'B	Reža:
	'0'B: DRIVER (VOZNIK),
	'1'B: CO-DRIVER (SOVOZNIK),
'c'B	Stanje vožnje:
	'0'B: SINGLE (POSAMEZNIK),
	'1'B: CREW (EKIPA),
'p'B	Stanje voznikove (ali delavniške) kartice v ustrezni reži:
	'0'B: INSERTED (VSTAVLJENA), kartica je vstavljena,
	'1'B: NOT INSERTED (NI VSTAVLJENA), ni vstavljena nobena kartica (ali: kartica je izvlečena),
'aa'B	Dejavnost:
	'00'B: BREAK/REST (ODMOR/POČITEK),
	'01'B: AVAILABILITY (RAZPOLOŽLJIVOST),
	'10'B: WORK (DELO),
	'11'B: DRIVING (VOŽNJA),
'tttttttttttt'B	Čas spremembe: Število minut po času 00h00 na ta dan.

Za zapis na voznikovo (ali delavniško) kartico (in stanje voznika):

's'B	Reža (ni pomembno, kadar je 'p' = 1, razen kakor je navedeno v spodnji opombi):
	'0'B: DRIVER (VOZNIK),
	'1'B: 2. CO-DRIVER (SOVOZNIK),
'c'B	Stanje vožnje (primer 'p' = 0) ali Naslednje stanje dejavnosti (primer 'p' = 1):
	'0'B: SINGLE (POSAMEZNIK), '0'B: UNKNOWN (NEZNANO)
	'1'B: CREW (EKIPA), '1'B: KNOWN (ZNANO) (= vneseno ročno)
'p'B	Stanje kartice:
	'0'B: INSERTED (VSTAVLJENA), kartica je vstavljena v zapisovalno napravo,
	'1'B: NOT INSERTED (NI VSTAVLJENA), kartica ni vstavljena (ali: kartica je izvlečena),

'aa'B	Dejavnost (ni pomembno, kadar je 'p' = 1 in V = 0, razen kakor je navedeno v spodnji opombi):
'00'B:	BREAK/REST (ODMOR/POČITEK),
'01'B:	AVAILABILITY (RAZPOLOŽLJIVOST),
'10'B:	WORK (DELO),
'11'B:	DRIVING (VOŽNJA),
'tttttttttt'B	Čas spremembe: Število minut po času 00h00 na ta dan.

Opomba v primeru ,izvleka kartice':

Ko se izvleče kartico:

- je spremenljivka V pomembna in pomeni režo, iz katere je kartica izvlečena,
- mora biti 'c' nastavljena na 0,
- mora biti 'p' nastavljena na 1,
- mora 'aa' pomeniti kodo tekoče dejavnosti, izbrane ob tem času,

Zaradi ročnega vnosa se lahko bita 'c' in 'aa' besede (shranjene na kartici) kasneje prepiseta tako, da odražata ta ročni vnos.

2.2 Address

Naslov.

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

codePage predpisuje del ISO/IEC 8859 uporabljen za kodiranje naslova,

address je naslov kodiran v skladu z ISO/IEC 8859-codePage.

2.3 BCDString

BCDString se uporablja za dvojiško kodirano predstavitev desetiških števil (predstavitev BCD). Ta podatkovni tip se uporablja za predstavitev ene desetiške številke v enem pol-oktetu (4 bitih). BCDString temelji na ISO/IEC 8824-1 ,tip znakovni niz'.

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

BCD String uporablja zapis ,hstring'. Skrajna leva šestnajstiška številka je najpomembnejši pol-oktet prvega okteta. Mnogokratnik okteta se tvori tako, da se vstavi pol-oktete z zaključnimi ničlami za mestom levega pol-okteta v prvem oktetu.

Dovoljene številke so: 0, 1, ... 9.

2.4 CalibrationPurpose

Koda, ki razloži, zakaj je bil nabor kalibracijskih parametrov zapisan. Ta podatkovni tip je povezan z zahtevama 097 in 098.

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

Prirrejanje vrednosti:

'00'H rezervirana vrednost,

'01'H aktiviranje: zapis kalibracijskih parametrov, znanih ob času aktiviranja VU,

'02'H prva namestitev: prvo kalibriranje VU po njenem aktiviranju,

'03'H namestitev: prvo kalibriranje VU v vozilu, v katerem je nameščena sedaj,

'04'H redna kontrola.

2.5 CardActivityDailyRecord

Informacija, shranjena na kartici, povezana z voznikovimi dejavnostmi na določen koledarski dan. Ta podatkovni tip je povezan z zahtevama 199 in 219.

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

activityPreviousRecordLength je celotna dolžina prejšnjega dnevnega zapisa, v bajtih. Največja vrednost je podana z dolžino OCTET STRING, ki vsebuje te zapise (glej CardActivityLengthRange v točki 3). Kadar je ta zapis najstarejši dnevni zapis, mora biti vrednost activityPreviousRecordLength nastavljena na 0.

activityRecordLength je celotna dolžina tega zapisa, v bajtih. Največja vrednost je podana z dolžino OCTET STRING, ki vsebuje te zapise.

activityRecordDate je datum zapisa.

activityDailyPresenceCounter je dnevni števec prisotnosti kartice za ta dan.

activityDayDistance je celotna prevožena razdalja na ta dan.

activityChangeInfo je množica podatkov ActivityChangeInfo za voznika za ta dan. Lahko vsebuje do največ 1 440 vrednosti (ena sprememba dejavnosti na minuto). Ta množica obvezno vsebuje tudi kodo activityChangeInfo voznikovega stanja ob času 00.00.

2.6 CardActivityLengthRange

Število bajtov na voznikovi ali delavniški kartici, ki so na voljo za hranjenje zapisov voznikovih dejavnosti.

```
CardActivityLengthRange ::= INTEGER(0..216-1)
```

Prilaganje vrednosti: glej točko 3.

2.7 CardApprovalNumber

Številka odobritve tipa kartice.

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

Prilaganje vrednosti: Ni predpisano.

2.8 CardCertificate

Certifikat javnega ključa kartice.

```
CardCertificate ::= Certificate.
```

2.9 CardChipIdentification

Informacija, shranjena na kartici, povezana z identifikacijo integriranega vezja (IC) kartice (zahteva 191).

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


activityPointerOldestDayRecord je podatek o začetku pomnilniškega prostora (število bajtov od začetka niza) najstarejšega popolnega dnevnega zapisa v nizu activityDailyRecords. Največjo vrednost podaja dolžina niza.

activityPointerNewestRecord je podatek o začetku pomnilniškega prostora (število bajtov od začetka niza) najnovejšega dnevnega zapisa v nizu activityDailyRecords. Največjo vrednost podaja dolžina niza.

activityDailyRecords je prostor, na voljo za hranjenje podatkov o vznikaških dejavnostih (podatkovna struktura: CardActivityDailyRecord) za vsak koledarski dan, na katerega je kartica uporabljena.

Priranje vrednosti: ta oktetni niz se ciklično polni z zapisi CardActivityDailyRecord. Ob prvi uporabi se začne shranjevanje v prvi bajt niza. Vsak novi zapis se pripne za koncem prejšnjega. Ko je niz poln, se shranjevanje nadaljuje v prvi bajt niza ne glede na prekinitev, ki zaradi tega nastane v podatkovnem elementu. Pred vstavitvijo novih podatkov o dejavnostih v niz (podaljšanjem tekočega activityDailyRecord ali vstavitvijo novega activityDailyRecord), ki bodo prepisali starejše podatke o dejavnostih, je treba posodobiti activityPointerOldestDayRecord, tako da ustreza novemu položaju najstarejšega popolnega dnevnega zapisa, activityPreviousRecordLength tega (novega) najstarejšega popolnega dnevnega zapisa pa nastaviti na 0.

2.14 CardDrivingLicenceInformation

Informacija, shranjena na vznikaški kartici, povezana s podatki o imetnikovem vozniškem dovoljenju (zahteva 196).

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

drivingLicenceIssuingAuthority je organ, pristojen za izdajanje voznških dovoljenj.

drivingLicenceIssuingNation je državna pripadnost organa, ki je izdal voznško dovoljenje.

drivingLicenceNumber je številka voznškega dovoljenja.

2.15 CardEventData

Informacija, shranjena na vznikaški ali delavniški kartici, povezana z dogodki v zvezi z imetnikom (zahtevi 204 in 223).

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

CardEventData je zaporedje, urejeno po naraščajoči vrednosti EventFaultType, zapisov cardEventRecords (razen zapisov poskusov kršenja varnosti, ki so zbrani v zadnjem nizu zaporedja).

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

2.16 CardEventRecord

Informacija, shranjena na vznikaški ali delavniški kartici, povezana z dogodkom v zvezi z imetnikom (zahtevi 205 in 223).

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

eventType je vrsta dogodka.

eventBeginTime je datum in čas začetka dogodka.

eventEndTime je datum in čas konca dogodka.

eventVehicleRegistration je registrska številka vozila, v katerem se je zgodil dogodek, in država, v kateri je vozilo registrirano.

2.17 CardFaultData

Informacija, shranjena na voznikovi ali delavniški kartici, povezana z napakami v zvezi z imetnikom (zahtevi 207 in 223).

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

CardFaultData je zaporedje množice zapisov napak v zapisovalni napravi, za njimi pa še množice zapisov napak na kartici.

cardFaultRecords je množica zapisov napak določene kategorije napak (zapisovalna naprava ali kartica).

2.18 CardFaultRecord

Informacija, shranjena na voznikovi ali delavniški kartici, povezana z napako v zvezi z imetnikom (zahtevi 208 in 223).

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

faultType je vrsta napake.

faultBeginTime je datum in čas začetka napake.

faultEndTime je datum in čas konca napake.

faultVehicleRegistration je registrska številka vozila, v katerem se je zgodila napaka, in država, v kateri je vozilo registrirano.

2.19 CardIccIdentification

Informacija, shranjena na kartici, povezana z identifikacijo integriranega vezja (IC) kartice (zahteva 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 opredeljen v EN 726-3.

cardExtendedSerialNumber obsega serijsko številko IC in proizvodne podatke IC, opredeljene v EN 726-3 in kakor jih podrobneje predpisuje podatkovni tip ExtendedSerialNumber.

cardApprovalNumber je številka odobritve tipa kartice.

cardPersonaliserID je ID personalizatorja kartice, opredeljena v EN 726-3.

embedderIcAssemblerId je identifikator vgrajevalca/sestavljalca IC, opredeljen v EN 726-3.

icIdentifier je identifikator IC na kartici in izdelovalca IC, opredeljen v EN 726-3.

2.20 CardIdentification

Informacija, shranjena na kartici, povezana z identifikacijo kartice (zahteve 194, 215, 231, 235).

CardIdentification ::= SEQUENCE

```

    cardIssuingMemberState      NationNumeric,
    cardNumber                   CardNumber,
    cardIssuingAuthorityName     Name,
    cardIssueDate                TimeReal,
    cardValidityBegin            TimeReal,
    cardExpiryDate               TimeReal
}

```

cardIssuingMemberState je koda države članice, ki je izdala kartico.

cardNumber je številka kartice.

cardIssuingAuthorityName je ime organa, ki je izdal kartico.

cardIssueDate je datum izdaje kartice sedanjemu imetniku.

cardValidityBegin je datum začetka veljavnosti kartice.

cardExpiryDate je datum poteka veljavnosti kartice.

2.21 CardNumber

Številka kartice, kakor jo opredeljuje opredelitev 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 nedvoumna identifikacija voznika v državi članici.

ownerIdentification je nedvoumna identifikacija podjetja, delavnice ali nadzornega organa v državi članici.

cardConsecutiveIndex je zaporedna tekoča številka kartice.

cardReplacementIndex je zaporedna številka zamenjave kartice.

cardRenewalIndex je zaporedna številka obnovitve kartice.

Prva oblika zaporedja je primerna za kodiranje številke voznikove kartice, druga oblika zaporedja pa za kodiranje številke delavniških kartic, nadzornih kartic ali kartic podjetja.

2.22 CardPlaceDailyWorkPeriod

Informacija, shranjena na voznikovi ali delavniški kartici, povezana s kraji začetkov in/ali koncev dnevnih delovnih izmen (zahtevi 202 in 221).

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

placePointerNewestRecord je indeks zadnjega posodobljenega zapisa krajev.

Prirjevanje vrednosti: Število, ki ustreza števcu zapisa krajev; začne se z vrednostjo ,0' za prvi zapis krajev v strukturi.

placeRecords je množica zapisov z informacijami vnešenih krajev.

2.23 CardPrivateKey

Zasebni ključ kartice.

CardPrivateKey ::= RSAKeyPrivateExponent.

2.24 CardPublicKey

Javni ključ kartice.

CardPublicKey ::= PublicKey.

2.25 CardRenewalIndex

Zaporedna številka obnove kartice (opredelitev i).

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

Prirjevanje vrednosti: (glej poglavje VII te priloge).

'0' prva izdaja.

Vrstni red povečevanja: '0, ..., 9, A, ..., Z'.

2.26 CardReplacementIndex

Zaporedna številka zamenjave kartice (opredelitev j).

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

Prirjevanje vrednosti: (glej poglavje VII te priloge).

'0' originalna kartica.

Vrstni red povečevanja: '0, ..., 9, A, ..., Z'.

2.27 CardSlotNumber

Koda za razločevanje med režama enote v vozilu.

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

Prirjevanje vrednosti: ni nadalje predpisano.

2.28 CardSlotsStatus

Koda vrst kartic vstavljenih v reži enote v vozilu.

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

Prirejanje vrednosti – oktetno poravnano: 'ccccdddd'B:

'cccc'B Identifikacija vrste kartice vstavljene v sovoznikovi reži,

'dddd'B Identifikacija vrste kartice vstavljene v voznikovi reži,

z naslednjimi identifikacijskimi kodami:

'0000'B ni vstavljena nikakršna kartica,

'0001'B vstavljena je voznikova kartica,

'0010'B vstavljena je delavniška kartica,

'0011'B vstavljena je nadzorna kartica,

'0100'B vstavljena je kartica podjetja.

2.29 CardStructureVersion

Koda, ki kaže verzijo strukture na tahografski kartici.

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

Prيرهانجه vrednosti: 'aabb'H:

'aa'H indeks sprememb strukture,

'bb'H indeks sprememb pri uporabi podatkovnih elementov opredeljenih za strukturo podano z višjim bajtom.

2.30 CardVehicleRecord

Informacija, shranjena na voznikovi ali delavniški kartici, povezana z obdobjem uporabe vozila na določen koledarski dan (zahtevi 197 in 217).

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

vehicleOdometerBegin je vrednost števca prevožene poti ob začetku obdobja uporabe vozila.

vehicleOdometerEnd je vrednost števca prevožene poti ob koncu obdobja uporabe vozila.

vehicleFirstUse je datum in čas začetka obdobja uporabe vozila.

vehicleLastUse je datum in čas konca obdobja uporabe vozila.

vehicleRegistration je VRN in država registracije vozila.

vuDataBlockCounter je vrednost VuDataBlockCounter ob zadnjem izpisu obdobja uporabe vozila.

2.31 CardVehiclesUsed

Informacija, shranjena na voznikovi ali delavniški kartici, povezana z vozili, ki jih je uporabljal imetnik kartice (zahtevi 197 in 217).

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

vehiclePointerNewestRecord je indeks zadnjega posodobljenega zapisa vozil.

Prirjevanje vrednosti: Število, ki ustreza števcu zapisa vozil; začne se z vrednostjo ,0' za prvi zapis vozil v strukturi.

cardVehicleRecords je množica zapisov podatkov o uporabljenih vozilih.

2.32 Certificate

Certifikat javnega ključa, izdan od certifikacijske agencije.

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

Prirjevanje vrednosti: digitalni podpis z delno obnovljeno vsebino certifikata po dodatku 11 „Skupni varnostni mehanizmi”: Podpis (128 bajtov) || Ostanek javnega ključa (58 bajtov) || Oznaka certifikacijske agencije (8 bajtov).

2.33 CertificateContent

(Berljiva) vsebina certifikata javnega ključa po dodatku 11 „Skupni varnostni mehanizmi”.

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

certificateProfileIdentifier je verzija ustreznega certifikata.

Prirjevanje vrednosti: '01h' za to verzijo.

CertificationAuthorityReference identificira certifikacijsko agencijo, ki je izdala ta certifikat. Vsebuje tudi sklic na javni ključ te certifikacijske agencije.

certificateHolderAuthorisation identificira pravice imetnika certifikata.

certificateEndOfValidity je datum administrativnega izteka veljavnosti certifikata.

certificateHolderReference identificira imetnika certifikata. Vsebuje tudi sklic na njegov javni ključ.

publicKey je javni ključ, certificiran s tem certifikatom.

2.34 CertificateHolderAuthorisation

Identifikacija pravic imetnika certifikata.

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

tachographApplicationID je identifikator tahografske aplikacije.

Prirjevanje vrednosti: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Ta identifikator aplikacije (AID) je lastniški neregistrirani identifikator aplikacije v skladu z ISO/IEC 7816-5.

equipmentType je identifikacija vrste naprave, za katero je namenjen certifikat.

Prirjevanje vrednosti: v skladu s podatkovnim tipom EquipmentType. 0, če je imetnik certifikata katera od držav članic.

2.35 CertificateRequestID

Nedvoumna identifikacija zahtevka za certifikat. Če v času tvorbe certifikata ni znana serijska številka enote v vozilu, za katero je ključ namenjen, se lahko uporabi tudi kot identifikator javnega ključa enote v vozilu.

```
CertificateRequestID ::= SEQUENCE {
    requestSerialNumber          INTEGER(0..232-1)
    requestMonthYear             BCDString(SIZE(2))
    crIdentifier                 OCTET STRING(SIZE(1))
    manufacturerCode            ManufacturerCode
}
```

requestSerialNumber je zaporedna številka zahtevka za certifikat, enkratna za proizvajalca in mesec.

requestMonthYear je identifikacija meseca in leta zahtevka za certifikat.

Prirjevanje vrednosti: BCD kodirani mesec (dve števki) in leto (zadnji dve števki).

crIdentifier: je identifikator, s katerim se zahtevek za certifikat loči od podaljšane zaporedne številke.

Prirjevanje vrednosti: 'FFh'.

manufacturerCode: je številski koda proizvajalca, ki zahteva certifikat.

2.36 CertificationAuthorityKID

Identifikator javnega ključa certifikacijske agencije (na nivoju države članice ali na nivoju EU).

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

nationNumeric je številski koda države, pod katero spada certifikacijska agencija.

nationAlpha je alfanumerična koda države, pod katero spada certifikacijska agencija.

keySerialNumber je zaporedna številka, po kateri se v primeru sprememb ključev med seboj ločijo različni ključi certifikacijske agencije.

additionalInfo je dvobajtno polje za dodatne kode (določi certifikacijska agencija).

caIdentifier je identifikator, po katerem se identifikator ključa certifikacijske agencije loči od drugih identifikatorjev ključev.

Prirjevanje vrednosti: '01h'.

2.37 CompanyActivityData

Informacija, shranjena na kartici podjetja, povezana z dejavnostmi opravljenimi s kartico (zahteva 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 zadnjega posodobljenega zapisa **companyActivityRecord**.

Prirrejanje vrednosti: Število, ki ustreza števcu zapisa dejavnosti podjetja; začne se z vrednostjo ,0' za prvi zapis dejavnosti podjetja v strukturi.

companyActivityRecords je množica vseh zapisov dejavnosti podjetja.

companyActivityRecord je zaporedje informacij povezanih z eno dejavnostjo podjetja.

companyActivityType je vrsta dejavnosti podjetja.

companyActivityTime je datum in čas dejavnosti podjetja.

cardNumberInformation je številka kartice in država izdajateljica kartice, s katere je bil opravljen prenos podatkov, če je bil opravljen.

vehicleRegistrationInformation je registrska številka vozila, v katerem je bil opravljen prenos podatkov ali izveden vklop ali izklop blokade.

downloadPeriodBegin in **downloadPeriodEnd** sta začetek in konec obdobja, za katerega so bili prenešeni podatki iz VU, če je bil opravljen prenos.

2.38 CompanyActivityType

Koda dejavnosti, ki jo je opravilo podjetje s svojo kartico podjetja.

```

CompanyActivityType ::= INTEGER {
    prenos podatkov s kartice                (1),
    prenos podatkov z VU                     (2),
    vklop blokade VU                        (3),
    izklop blokade VU                       (4).
}

```

2.39 CompanyCardApplicationIdentification

Informacija, shranjena na kartici, povezana z identifikacijo aplikacije kartice (zahteva 190).

```

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

```

typeOfTachographCardId določa uporabljeno vrsto kartice.

cardStructureVersion določa verzijo strukture na kartici.

noOfCompanyActivityRecords je število zapisov dejavnosti podjetja, ki jih lahko hrani kartica.

2.40 CompanyCardHolderIdentification

Informacija, shranjena na kartici podjetja, povezana z identifikacijo imetnika kartice (zahteva 236).

```

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

```

companyName je ime podjetja, imetnika kartice.

companyAddress je naslov podjetja, imetnika kartice.

cardHolderPreferredLanguage je izbrani jezik imetnika kartice.

2.41 ControlCardApplicationIdentification

Informacija, shranjena na nadzorni kartici, povezana z identifikacijo aplikacije kartice (zahteva 190).

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

typeOfTachographCardId določa uporabljeno vrsto kartice.

cardStructureVersion določa verzijo strukture na kartici.

noOfControlActivityRecords je število zapisov nadzornih dejavnosti, ki jih lahko hrani kartica.

2.42 ControlCardControlActivityData

Informacija, shranjena na nadzorni kartici, povezana z dejavnostmi opravljenimi s kartico (zahteva 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 zadnjega posodobljenega zapisa nadzornih dejavnosti.

Prirejanje vrednosti: Število, ki ustreza števcu zapisa nadzornih dejavnosti; začne se z vrednostjo ,0' za prvi zapis nadzornih dejavnosti v strukturi.

controlActivityRecords je množica vseh zapisov nadzornih dejavnosti.

controlActivityRecord je zaporedje informacij povezanih z eno nadzorno dejavnostjo.

controlType je vrsta nadzora.

controlTime je datum in čas nadzora.

controlledCardNumber je številka kartice in država izdajateljica nadzorovane kartice.

controlledVehicleRegistration je registrska številka vozila, v katerem je potekal nadzor, in država, v kateri je vozilo registrirano.

controlDownloadPeriodBegin in **controlDownloadPeriodEnd** označujeta obdobje, za katerega je bil opravljen prenos podatkov, če je bil opravljen,

2.43 ControlCardHolderIdentification

Informacija, shranjena na nadzorni kartici, povezana z identifikacijo imetnika kartice (zahteva 232).

```

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

```

controlBodyName je ime nadzornega organa, imetnika kartice.

controlBodyAddress je naslov nadzornega organa, imetnika kartice.

cardHolderName je priimek in ime imetnika nadzorne kartice.

cardHolderPreferredLanguage je izbrani jezik imetnika kartice.

2.44 ControlType

Koda, ki označuje dejavnosti, opravljene med nadzorom. Ta podatkovni tip je povezan z zahtevami 102, 210 in 225.

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

Prirjevanje vrednosti – oktetno poravnano: 'cvpdxxxx'B (8 bitov)

```

'c'B      prenos podatkov s kartice:
           '0'B: med to nadzorno dejavnosti podatki s kartice niso bili preneseni,
           '1'B: med to nadzorno dejavnosti so bili podatki s kartice preneseni,
'v'B      prenos podatkov z VU:
           '0'B: med to nadzorno dejavnosti podatki iz VU niso bili preneseni,
           '1'B: med to nadzorno dejavnosti so bili podatki iz VU preneseni,
'p'B      tiskanje:
           '0'B: med to nadzorno dejavnostjo ni bilo opravljeno tiskanje,
           '1'B: med to nadzorno dejavnostjo je bilo opravljeno tiskanje,
'd'B      prikaz:
           '0'B: med to nadzorno dejavnostjo ni bil uporabljen prikaz,
           '1'B: med to nadzorno dejavnostjo je bil uporabljen prikaz,
'xxxx'B   ni uporabljeno.

```

2.45 CurrentDateTime

Tekoči datum in čas zapisovalne naprave.

```
CurrentDateTime ::= TimeReal
```

Prirjevanje vrednosti: ni nadalje predpisano.

2.46 DailyPresenceCounter

Števec, shranjen na voznikovi ali delavniški kartici, ki se poveča za eno na vsak koledarski dan, v katerem je kartica vstavljena v VU. Ta podatkovni tip je povezan z zahtevama 199 in 219.

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

Prirjevanje vrednosti: Zaporedno število z največjo vrednostjo = 9 999; po tem začne spet od 0. Ob prvi izdaji kartice je število nastavljeno na 0.

2.47 Datef

Datum, zapisan v za tiskanje primerni številski obliki.

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

Prirrejanje vrednosti:

```
YYYY      Leto
mm        Mesec
dd        Dan
```

'00000000'H pomeni izrecno: brez datuma.

2.48 Distance

Prevožena razdalja (rezultat izračuna razlike med dvema vrednostima števca prevožene poti, v kilometrih).

```
Distance ::= INTEGER(0..216-1)
```

Prirrejanje vrednosti: binarno število brez preznaka. Vrednost, v km, v območju od 0 do 9 999 km.

2.49 DriverCardApplicationIdentification

Informacija, shranjena na voznikovi kartici, povezana z identifikacijo aplikacije kartice (zahteva 190).

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

typeOfTachographCardId določa uporabljeno vrsto kartice.

cardStructureVersion določa verzijo strukture na kartici.

noOfEventsPerType je število dogodkov posamezne vrste, ki jih lahko zapiše kartica.

noOfFaultsPerType je število napak posamezne vrste, ki jih lahko zapiše kartica.

activityStructureLength označuje število bajtov na razpolago za hranjenje zapisov dejavnosti.

noOfCardVehicleRecords je število zapisov vozila, ki jih lahko vsebuje kartica.

noOfCardPlaceRecords je število krajev, ki jih lahko zapiše kartica.

2.50 DriverCardHolderIdentification

Informacija, shranjena na voznikovi kartici, povezana z identifikacijo imetnika kartice (zahteva 195).

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

cardHolderName je priimek in ime imetnika voznikove kartice.

cardHolderBirthDate je datum rojstva imetnika voznikove kartice.

cardHolderPreferredLanguage je izbrani jezik imetnika kartice.

2.51 EntryTypeDailyWorkPeriod

Koda, po kateri se razlikujejo vnosi kraja in načini vnosa ob začetku in ob koncu dnevne delovne izmene.

EntryTypeDailyWorkPeriod ::= INTEGER

Za\232etek, ustrezni \232as = \232as vstavitve kartice ali vnosa	(0),
Konec, ustrezni \232as = \232as izvleka kartice ali vnosa	(1),
Za\232etek, ustrezni \232as ro\232no vnešen (\232as za\232etka)	(2),
Konec, ustrezni \232as ro\232no vnešen (konec delovne izmene)	(3),
Za\232etek, ustrezni \232as predpostavi VU	(4),
Konec, ustrezni \232as predpostavi VU	(5)

}

Prirjeanje vrednosti: po ISO/IEC8824-1.

2.52 EquipmentType

Koda, po kateri se ločijo vrste naprave za tahografsko aplikacijo.

EquipmentType ::= INTEGER(0..255)

-Rezervirano	(0),
-Voznikova kartica	(1),
-Delavniška kartica	(2),
-Nadzorna kartica	(3),
-Kartica podjetja	(4),
-Kartica proizvajalca	(5),
-Enota v vozilu	(6),
-Zaznavalo gibanja	(7),
-RFU	(8..255)

Prirjeanje vrednosti: po ISO/IEC8824-1.

Vrednost 0 je rezervirana za označevanje države članice ali Evrope v polje CHA certifikatov.

2.53 EuropeanPublicKey

Evropski javni ključ.

EuropeanPublicKey ::= PublicKey.

2.54 EventFaultType

Koda, ki označuje dogodek ali napako.

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

Prirjeanje vrednosti:

'0x'H	Splošni dogodki,
'00'H	Ni dodatnih podrobnosti,
'01'H	Vstavitve neveljavne kartice,
'02'H	Navzkrižje med karticami,
'03'H	Časovno prekrivanje,
'04'H	Vožnja brez ustrezne kartice,
'05'H	Vstavitve kartice med vožnjo,
'06'H	Zadnja seja s kartico nepravilno zaključena,
'07'H	Prekoračitev hitrosti,

'08'H	Prekinitev napajanja,
'09'H	Napaka podatkov o gibanju,
'0A'H do '0F'H	RFU,
'1x'H	Dogodki poskusov kršenja varnosti povezani z enoto v vozilu
'10'H	Ni dodatnih podrobnosti,
'11'H	Neuspela avtentifikacija zaznavala gibanja,
'12'H	Neuspela avtentifikacija tahografske kartice,
'13'H	Nepooblaščen zamenjava zaznavala gibanja,
'14'H	Napaka v celovitosti vhodnih podatkov s kartice,
'15'H	Napaka v celovitosti shranjenih podatkov uporabnika,
'16'H	Napaka pri notranjem prenosu podatkov,
'17'H	Nepooblaščen odprtje ohišja,
'18'H	Sabotaža strojne opreme,
'19'H do '1F'H	RFU,
'2x'H	Dogodki poskusov kršenja varnosti povezani z zaznavalom,
'20'H	Ni dodatnih podrobnosti,
'21'H	Neuspela avtentifikacija,
'22'H	Napaka v celovitosti shranjenih podatkov,
'23'H	Napaka pri notranjem prenosu podatkov,
'24'H	Nepooblaščen odprtje ohišja,
'25'H	Sabotaža strojne opreme,
'26'H do '2F'H	RFU,
'3x'H	Napaka na zapisovalni napravi,
'30'H	Ni dodatnih podrobnosti,
'31'H	Interna napaka VU,
'32'H	Napaka na tiskalniku,
'33'H	Napaka na prikazovalniku,
'34'H	Napaka pri prenosu podatkov,
'35'H	Napaka na zaznavalu,
'36'H do '3F'H	RFU
'4x'H	Napake na kartici,
'40'H	Ni dodatnih podrobnosti,
'41'H do '4F'H	RFU
'50'H do '7F'H	RFU,
'80'H do 'FF'H	Določi proizvajalec.

2.55 EventFaultRecordPurpose

Koda, ki razlaga, zakaj je bil(a) dogodek ali napaka zapišan(a).

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

Prirejanje vrednosti:

'00'H	eden od 10 najnovejših (oz. zadnjih) dogodkov ali napak
'01'H	najdaljši dogodek na enega od 10 zadnjih dni nastopov dogodkov,
'02'H	eden od petih najdaljših dogodkov v zadnjih 365 dneh
'03'H	zadnji dogodek na enega od 10 zadnjih dni nastopov dogodkov,
'04'H	najresnejši dogodek na enega od 10 zadnjih dni nastopov dogodkov,
'05'H	eden od petih najresnejših dogodkov v zadnjih 365 dneh
'06'H	prvi dogodek, ki je nastopil po zadnjem kalibriranju
'07'H	aktivni / tekoči dogodek ali napaka
'08'H do '7F'H	RFU
'80'H do 'FF'H	določi proizvajalec.

2.56 ExtendedSerialNumber

Nedvoumna identifikacija naprave. Lahko se uporabi tudi kot identifikator javnega ključa naprava.

```
ExtendedSerialNumber ::= SEQUENCE {
    serialNumber          INTEGER(0..232-1)
    monthYear             BCDString(SIZE(2))
    type OCTET            STRING(SIZE(1))
    manufacturerCode      ManufacturerCode
}
```

serialNumber je serijska številka naprave, enkratna za proizvajalca, vrsto naprave in mesec.

monthYear je identifikacija meseca in leta izdelave (ali dodelitve serijske številke).

Prirejanje vrednosti: BCD kodirani mesec (dve števki) in leto (zadnji dve števki).

type je identifikator vrste naprave.

Prirejanje vrednosti: določi proizvajalec; vrednost 'FFh' je rezervirana.

manufacturerCode: je številski koda proizvajalca naprave.

2.57 FullCardNumber

Koda, ki popolno identificira tahografsko kartico.

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

cardType je vrsta tahografske kartice.

cardIssuingMemberState je koda države članice, ki je izdala kartico.

cardNumber je številka kartice.

2.58 HighResOdometer

Vrednost števca prevožene poti vozila: Skupna pot, ki jo je vozilo prevozilo do sedaj.

```
HighResOdometer ::= INTEGER(0..232-1)
```

Prirejanje vrednosti: binarno število brez preznaka. Vrednost, v enotah 1/200 km, v območju od 0 do 21 055 406 km.

2.59 HighResTripDistance

Pot, prevožena na določeni vožnji ali etapi vožnje.

```
HighResTripDistance ::= INTEGER(0..232-1)
```

Prirejanje vrednosti: binarno število brez preznaka. Vrednost, v enotah 1/200 km, v območju od 0 do 21 055 406 km.

2.60 HolderName

Priimek in ime(na) imetnika kartice.

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


holderSurname je priimek imetnika. Priimek ne vključuje nazivov.

Prirejanje vrednosti: Če kartica ni osebna kartica, vsebuje holderSurname isto informacijo kakor companyName ali workshopName ali controlBodyName.

holderFirstNames so ime(na) in začetnice imetnika.

2.61 K-ConstantOfRecordingEquipment

Konstanta zapisovalne naprave (opredelitev m)).

`K-ConstantOfRecordingEquipment ::= INTEGER(0..216-1)`

Prirejanje vrednosti: Število pulzov na kilometer poti, v delovnem območju od 0 do 64 255 pulzov/km.

2.62 KeyIdentifier

Nedvoumni identifikator javnega ključa, uporabljan za navajanje in izbiranje ključa. Identificira tudi imetnika ključa.

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

Prva oblika je primerna za navajanje javnega ključa enote v vozilu ali tahografske kartice.

Druga oblika je primerna za navajanje javnega ključa enote v vozilu (v primeru, če ob času tvorbe javnega ključa ni mogoče poznati serijske številke enote v vozilu).

Tretja oblika je primerna za navajanje javnega ključa države članice.

2.63 L-TyreCircumference

Efektivni obseg avtoplaščev (opredelitev u)).

`L-TyreCircumference ::= INTEGER(0..216-1)`

Prirejanje vrednosti: Binarno število brez predznaka, vrednost v enotah 1/8 mm v območju od 0 do 8 031 mm.

2.64 Language

Koda, ki označuje jezik.

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

Prirejanje vrednosti: Dvomestna koda z malimi črkami po ISO 639.

2.65 LastCardDownload

Datum in čas, shranjen na voznikovi kartici, zadnjega prenosa podatkov s kartice (v kak drug namen, ne v okviru nadzora). Ta datum lahko posodablja Vu ali kak drug čitalnik kartic.

`LastCardDownload ::= TimeReal`

Prirejanje vrednosti: ni nadalje predpisano.

2.66 ManualInputFlag

Koda, ki označuje, ali je imetnik kartice ob njeni vstavitvi ročno vnesel voznikove dejavnosti ali ne (zahteva 081).

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

Prirjevanje vrednosti: ni nadalje predpisano.

2.67 ManufacturerCode

Koda, ki označuje proizvajalca.

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

Prirjevanje vrednosti:

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

2.68 MemberStateCertificate

Certifikat javnega ključa države članice, ki ga izda evropska certifikacijska agencija.

```
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 predpisuje del ISO/IEC 8859 uporabljen za kodiranje imena,

name je ime kodirano v skladu z ISO/IEC 8859-codePage.

2.71 NationAlpha

Črkovna oznaka države v skladu z dogovorjenim kodiranjem držav na nalepkah na vozilih in/ali v skladu z mednarodno usklajenim kodiranjem na zavarovalnih policah (zelenih kartah).

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

Prirejanje vrednosti:

' '	Ni na voljo nikakršnih informacij
'A'	Avstrija
'AL'	Albanija
'AND'	Andorra
'ARM'	Armenija
'AZ'	Azerbejdžan
'B'	Belgija
'BG'	Bolgarija
'BIH'	Bosna in Hercegovina
'BY'	Belorusija
'CH'	Švica
'CY'	Ciper
'CZ'	Češka Republika
'D'	Nemčija
'DK'	Danska
'E'	Španija
'EST'	Estonija
'F'	Francija
'FIN'	Finska
'FL'	Liechtenstein
'FR'	Ferski otoki
'UK'	Združeno Kraljestvo, Alderney, Guernsey, Jersey, Isle of Man, Gibraltar
'GE'	Gruzija
'GR'	Grčija
'H'	Madžarska
'HR'	Hrvaška
'I'	Italija
'IRL'	Irska
'IS'	Islandija
'KZ'	Kazahstan
'L'	Luksembourg
'LT'	Litva
'LV'	Latvija
'M'	Malta
'MC'	Monaco

'MD'	Republika Moldavija
'MK'	Makedonija
'N'	Norveška
'NL'	Nizozemska
'P'	Portugalska
'PL'	Poljska
'RO'	Romunija
'RSM'	San Marino
'RUS'	Ruska Federacija
'S'	Švedska
'SK'	Slovaška
'SLO'	Slovenija
'TM'	Turkmenistan
'TR'	Turčija
'UA'	Ukrajina
'V'	Vatikan
'YU'	Jugoslavija
'UNK'	Neznano
'EC'	Evropska skupnost
'EUR'	Drugi deli Evrope
'WLD'	Drugi deli sveta.

2.72 NationNumeric

Številska oznaka države.

NationNumeric ::= INTEGER(0..255)

Prirjevanje vrednosti:

-- Ni na voljo nikakršnih informacij	(00)H,
-- Avstrija	(01)H,
-- Albanija	(02)H,
-- Andorra	(03)H,
-- Armenija	(04)H,
-- Azerbejdžan	(05)H,
-- Belgija	(06)H,
-- Bolgarija	(07)H,
-- Bosna in Hercegovina	(08)H,
-- Belorusija	(09)H,
-- Švica	(0A)H,
-- Ciper	(0B)H,
-- Češka Republika	(0C)H,
-- Nemčija	(0D)H,
-- Danska	(0E)H,
-- Španija	(0F)H,
-- Estonija	(10)H,
-- Francija	(11)H,
-- Finska	(12)H,
-- Liechtenstein	(13)H,
-- Ferski otoki	(14)H,
-- Združeno Kraljestvo	(15)H,
-- Gruzija	(16)H,
-- Grčija	(17)H,
-- Madžarska	(18)H,
-- Hrvaška	(19)H,
-- Italija	(1A)H,
-- Irska	(1B)H,
-- Islandija	(1C)H,

- - Kazahstan	(1D) H,
- - Luksembourg	(1E) H,
- - Litva	(1F) H,
- - Latvija	(20) H,
- - Malta	(21) H,
- - Monaco	(22) H,
- - Republika Moldavija	(23) H,
- - Makedonija	(24) H,
- - Norveška	(25) H,
- - Nizozemska	(26) H,
- - Portugalska	(27) H,
- - Poljska	(28) H,
- - Romunija	(29) H,
- - San Marino	(2A) H,
- - Ruska Federacija	(2B) H,
- - Švedska	(2C) H,
- - Slovaška	(2D) H,
- - Slovenija	(2E) H,
- - Turkmenistan	(2F) H,
- - Turčija	(30) H,
- - Ukrajina	(31) H,
- - Vatikan	(32) H,
- - Jugoslavija	(33) H,
- - RFU	(34 . . FC) H,
- - Evropska skupnost	(FD) H,
- - Drugi deli Evrope	(FE) H,
- - Drugi deli sveta.	(FF) H

2.73 NoOfCalibrationRecords

Število zapisov kalibriranja, ki jih lahko hrani delavniška kartica.

NoOfCalibrationRecords ::= INTEGER(0..255)

Prirejanje vrednosti: glej točko 3.

2.74 NoOfCalibrationsSinceDownload

Števec, ki kaže število kalibriranj, opravljenih z delavniško kartico od zadnjega prenosa podatkov z nje (zahteva 230).

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

Prirejanje vrednosti: ni nadalje predpisano.

2.75 NoOfCardPlaceRecords

Število zapisov krajev, ki jih lahko hrani voznikova ali delavniška kartica.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Prirejanje vrednosti: glej točko 3.

2.76 NoOfCardVehicleRecords

Število zapisov uporabljenih vozil, ki jih lahko hrani voznikova ali delavniška kartica.

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

Prirejanje vrednosti: glej točko 3.

2.77 NoOfCompanyActivityRecords

Število zapisov dejavnosti podjetja, ki jih lahko hrani kartica podjetja.

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

Prirejanje vrednosti: glej točko 3.

2.78 NoOfControlActivityRecords

Število zapisov nadzornih dejavnosti, ki jih lahko hrani nadzorna kartica.

`NoOfControlActivityRecords ::= INTEGER(0..216-1)`

Prirjevanje vrednosti: glej točko 3.

2.79 NoOfEventsPerType

Število dogodkov posamezne vrste, ki jih lahko hrani kartica.

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

Prirjevanje vrednosti: glej točko 3.

2.80 NoOfFaultsPerType

Število napak posamezne vrste, ki jih lahko hrani kartica.

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

Prirjevanje vrednosti: glej točko 3.

2.81 OdometerValueMidnight

Vrednost števca prevožene poti vozila na določen dan ob polnoči (zahteva 090).

`OdometerValueMidnight ::= OdometerShort`

Prirjevanje vrednosti: ni nadalje predpisano.

2.82 OdometerShort

Vrednost števca prevožene poti vozila v kratki obliki.

`OdometerShort ::= INTEGER(0..224-1)`

Prirjevanje vrednosti: binarno število brez preznaka. Vrednost, v km, v območju od 0 do 9 999 999 km.

2.83 OverspeedNumber

Število dogodkov prekoračitve hitrosti od zadnjega nadzora prekoračitev hitrosti.

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

Prirjevanje vrednosti: 0 pomeni, da od zadnjega nadzora prekoračitev hitrosti ni bilo nobene prekoračitve hitrosti; 1 pomeni, da se je od zadnjega nadzora prekoračitve hitrosti zgodil en dogodek prekoračitve hitrosti, ... 255 pomeni, da je bilo od zadnjega nadzora prekoračitve hitrosti že 255 ali več dogodkov prekoračitve hitrosti.

2.84 PlaceRecord

Informacija povezana s krajem začetka ali konca dnevne delovne izmene (zahteve 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {
    entryTime                               TimeReal,
    entryTypeDailyWorkPeriod               EntryTypeDailyWorkPeriod,
    dailyWorkPeriodCountry                  NationNumeric,
    dailyWorkPeriodRegion                   RegionNumeric,
    vehicleOdometerValue                    OdometerShort
}
```

entryTime je datum in čas vnosa.

entryTypeDailyWorkPeriod je vrsta vnosa.

dailyWorkPeriodCountry je vnesena država.

dailyWorkPeriodRegion je vnesena regija.

vehicleOdometerValue je vrednost števca prevožene poti ob času vnosa kraja.

2.85 PreviousVehicleInfo

Informacija povezana z vozilom, ki ga je uporabljal voznik pred vstavitvijo svoje kartice v enoto v vozilu (zahteva 081).

```
PreviousVehicleInfo ::= SEQUENCE {
    vehicleRegistrationIdentification      VehicleRegistrationIdentification,
    cardWithdrawalTime                    TimeReal
}
```

vehicleRegistrationIdentification je VRN in država registracije vozila.

cardWithdrawalTime je datum in čas izvleka kartice.

2.86 PublicKey

Javni ključ RSA.

```
PublicKey ::= SEQUENCE {
    rsaKeyModulus                      RSAKeyModulus,
    rsaKeyPublicExponent               RSAKeyPublicExponent
}
```

rsaKeyModulus je modul para ključev.

rsaKeyPublicExponent je javni eksponent para ključev.

2.87 RegionAlpha

Črkovna oznaka regije v določeni državi.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Prirejanje vrednosti:

' ' Ni na voljo nikakršnih informacij

Španija

'AN' Andaluzija

'AR' Aragonija

'AST' Asturija

'C' Kantabrija

'CAT' Katalonija

'CL' Kastilja-Leon

'CM' Kastilja-Mancha

'CV' Valencija

'EXT' Extremadura

'G' Galicija

'IB' Baleari

'IC' Kanarski otoki

'LR' La Rioja

'M' Madrid

'MU' Murcia

'NA' Navara

'PV' Pais Vasco.

2.88 RegionNumeric

Številska oznaka regije v določeni državi.

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

Prirejanje vrednosti:

'00'H Ni na voljo nikakršnih informacij

Španija

'01'H Andaluzija
 '02'H Aragonija
 '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 otoki
 '0D'H La Rioja
 '0E'H Madrid
 '0F'H Murcia
 '10'H Navara
 '11'H Pais Vasco.

2.89 RSAKeyModulus

Modul para ključev RSA.

`RSAKeyModulus ::= OCTET STRING (SIZE(128))`

Prirejanje vrednosti: Ni predpisano.

2.90 RSAKeyPrivateExponent

Zasebni eksponent para ključev RSA.

`RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))`

Prirejanje vrednosti: Ni predpisano.

2.91 RSAKeyPublicExponent

Javni eksponent para ključev RSA.

`RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))`

Prirejanje vrednosti: Ni predpisano.

2.92 SensorApprovalNumber

Številka odobritve tipa zaznavala.

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

Prirejanje vrednosti: Ni predpisano.

2.93 SensorIdentification

Informacija, shranjena v zaznavalu gibanja, povezana z identifikacijo zaznavala gibanja (zahteva 077).

```
SensorIdentification ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber        SensorApprovalNumber,
    sensorSCIdentifier           SensorSCIdentifier,
    sensorOSIdentifier           SensorOSIdentifier
}
```


sensorSerialNumber je razširjena serijska številka zaznavala gibanja (vključuje kataloško številko in kodo proizvajalca).

sensorApprovalNumber je številka odobritve zaznavala gibanja.

sensorSCIdentifier je identifikator varnostnega dela zaznavala gibanja.

sensorOSIdentifier je identifikator operacijskega sistema zaznavala gibanja.

2.94 SensorInstallation

Informacija, shranjena v zaznavalu gibanja, povezana z namestitvijo zaznavala gibanja (zahteva 099).

```
SensorInstallation ::= SEQUENCE {
    sensorPairingDateFirst          SensorPairingDate,
    firstVuApprovalNumber          VuApprovalNumber,
    firstVuSerialNumber            VuSerialNumber,
    sensorPairingDateCurrent       SensorPairingDate,
    currentVuApprovalNumber        VuApprovalNumber,
    currentVUSerialNumber          VuSerialNumber
}
```

sensorPairingDateFirst je datum prve povezave zaznavala gibanja z enoto v vozilu.

firstVuApprovalNumber je številka odobritve prve enote v vozilu, s katero je bilo povezano zaznavalo gibanja.

firstVuSerialNumber je serijska številka prve enote v vozilu, s katero je bilo povezano zaznavalo gibanja.

sensorPairingDateCurrent je datum sedanje povezave zaznavala gibanja z enoto v vozilu.

currentVuApprovalNumber je številka odobritve enote v vozilu, s katero je povezano zaznavalo gibanja sedaj.

currentVUSerialNumber je serijska številka enote v vozilu, s katero je povezano zaznavalo gibanja sedaj.

2.95 SensorInstallationSecData

Informacija, shranjena na delavniški kartici, povezana z varnostnimi podatki, potrebnimi za povezavo zaznaval gibanja z enotami v vozilu (zahteva 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Prirjevanje vrednosti: v skladu z ISO 16844-3.

2.96 SensorOSIdentifier

Identifikator operacijskega sistema zaznavala gibanja.

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

Prirjevanje vrednosti: določi proizvajalec.

2.97 SensorPaired

Informacija, shranjena v enoti v vozilu, povezana z identifikacijo zaznavala gibanja, povezana z enoto v vozilu (zahteva 079).

```
SensorPaired ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber        SensorApprovalNumber,
    sensorPairingDateFirst      SensorPairingDate
}
```

sensorSerialNumber je serijska številka zaznavala gibanja, s katerim je povezana enota v vozilu sedaj.

sensorApprovalNumber je številka odobritve zaznavala gibanja, s katerim je povezana enota v vozilu sedaj.

sensorPairingDateFirst je datum prve povezave enote v vozilu z zaznavalom gibanja, s katerim je povezana sedaj.

2.98 SensorPairingDate

Datum povezave zaznavala gibanja z enoto v vozilu.

`SensorPairingDate ::= TimeReal`

Prirrejanje vrednosti: Ni predpisano.

2.99 SensorSerialNumber

Serijska številka zaznavala gibanja.

`SensorSerialNumber ::= ExtendedSerialNumber:`

2.100 SensorSCIdentifier

Identifikator varnostnega dela zaznavala gibanja.

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

Prirrejanje vrednosti: določi proizvajalec dela.

2.101 Signature

Digitalni podpis.

`Signature ::= OCTET STRING (SIZE(128))`

Prirrejanje vrednosti: v skladu z dodatkom 11, „Skupni varnostni mehanizmi“.

2.102 SimilarEventsNumber

Število podobnih dogodkov na določen dan (zahteva 094).

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

Prirrejanje vrednosti: 0 se ne uporablja, 1 pomeni, da se je na ta dan zgodil le en dogodek te vrste, 2 pomeni, da sta se na ta dan zgodila dva dogodka te vrste (shranjen pa je le eden), ... 255 pomeni, da se je na ta dan zgodilo 255 ali več dogodkov te vrste.

2.103 SpecificConditionType

Koda, ki označuje posebno stanje (zahteve 050b, 105a, 212a in 230a).

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

Prirrejanje vrednosti:

'00'H	RFU
'01'H	Zunaj področja veljavnosti – začetek
'02'H	Zunaj področja veljavnosti – konec
'03'H	Vožnja s trajektom/vlakom
'04'H .. 'FF'H	RFU

2.104 SpecificConditionRecord

Informacija, shranjena na voznikovi kartici, na delavniški kartici ali v enoti v vozilu, povezana s posebnim stanjem (zahteve 105a, 212a in 230a).

```
SpecificConditionRecord ::= SEQUENCE {
    entryTime                TimeReal,
    specificConditionType    SpecificConditionType
}
```

entryTime je datum in čas vnosa.

specificConditionType je koda, ki označuje posebno stanje.

2.105 Speed

Hitrost vozila (km/h).

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

Prirejanje vrednosti: kilometri na uro v delovnem območju od 0 do 220 km/h.

2.106 SpeedAuthorised

Odobrena največja hitrost vozila (opredelitev bb).

```
SpeedAuthorised ::= Speed.
```

2.107 SpeedAverage

Povprečna hitrost v prej določenem obdobju (km/h).

```
SpeedAverage ::= Speed.
```

2.108 SpeedMax

Največja hitrost izmerjena v prej določenem obdobju.

```
SpeedMax ::= Speed.
```

2.109 TDesSessionKey

Trojni DES ključ seje.

```
TDesSessionKey ::= SEQUENCE {
    tDesKeyA                OCTET STRING (SIZE(8))
    tDesKeyB                OCTET STRING (SIZE(8))
}
```

Prirejanje vrednosti: ni nadalje predpisano.

2.110 TimeReal

Koda sestava datum/čas, v kateri sta datum in čas izražena kot število sekund od časa 00h00m00s po GMT dne 1. januarja 1970.

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

Prirejanje vrednosti – oktetno poravnano: Število sekund od polnoči po GMT 1. januarja 1970.

Najpoznejši možni čas pri tem zapisu leži v letu 2106.

2.111 TyreSize

Oznaka mer avtoplaščev.

```
TyreSize ::= IA5String(SIZE(15))
```

Prirejanje vrednosti: v skladu z Direktivo 92/23 (EGS) 31.3.1992, UL L 129, str. 95.

2.112 VehicleIdentificationNumber

Identifikacijska številka vozila (VIN) nanašajoča se na vozilo kot celoto; navadno serijska številka šasije ali okvira podvozja.

VehicleIdentificationNumber ::= IA5String(SIZE(17))

Prirrejanje vrednosti: kakor opredeljuje ISO 3779.

2.113 VehicleRegistrationIdentification

Identifikacija vozila, nedvoumna za celo Evropo (registrska številka in država registracije).

```
VehicleRegistrationIdentification ::= SEQUENCE {
    vehicleRegistrationNation      NationNumeric,
    vehicleRegistrationNumber      VehicleRegistrationNumber
}
```

vehicleRegistrationNation je država, v kateri je vozilo registrirano.

vehicleRegistrationNumber je registrska številka vozila (VRN).

2.114 VehicleRegistrationNumber

Registrska številka vozila (VRN). Registrsko številko dodeli organ, pristojen za registracijo.

```
VehicleRegistrationNumber ::= SEQUENCE {
    codePage                      INTEGER(0..255),
    vehicleRegNumber              OCTET STRING(SIZE(13))
}
```

codePage predpisuje del ISO/IEC 8859 uporabljen za kodiranje vehicleRegNumber,

vehicleRegNumber je VRN, kodirana v skladu z ISO/IEC 8859-codePage.

Prirrejanje vrednosti: predpiše posamezna država.

2.115 VuActivityDailyData

Informacija, shranjena v enoti v vozilu, povezana s spremembami dejavnosti in/ali spremembami stanja vožnje in/ali spremembami stanja kartice na določen koledarski dan (zahteva 084) in s stanjem rež ob 00.00 na ta dan.

```
VuActivityDailyData ::= SEQUENCE {
    noOfActivityChanges           INTEGER SIZE(0..1440),
    activityChangeInfos           SET SIZE(noOfActivityChanges) OF
    ActivityChangeInfo
}
```

noOfActivityChanges je število besed ActivityChangeInfo v množici activityChangeInfos.

activityChangeInfos je množica besed ActivityChangeInfo shranjena v VU za določen dan. Vedno vključuje dve besedi ActivityChangeInfo o stanju rež ob 00.00 na ta dan.

2.116 VuApprovalNumber

Številka odobritve tipa enote v vozilu.

VuApprovalNumber ::= IA5String(SIZE(8))

Prirrejanje vrednosti: Ni predpisano.

2.117 VuCalibrationData

Informacija, shranjena v enoti v vozilu, povezana s kalibriranjem zapisovalne naprave (zahteva 098).

```
VuCalibrationData ::= SEQUENCE {
    noOfVuCalibrationRecords      INTEGER(0..255),
    vuCalibrationRecords          SET SIZE(noOfVuCalibrationRecords) OF
    VuCalibrationRecord
}
```

noOfVuCalibrationRecords je število zapisov, ki jih vsebuje množica **vuCalibrationRecords**.

vuCalibrationRecords je množica zapisov o kalibriranju.

2.118 VuCalibrationRecord

Informacija, shranjena v enoti v vozilu, povezana s kalibriranjem zapisovalne naprave (zahteva 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 namen kalibriranja.

workshopName, **workshopAddress** sta ime in naslov delavnice.

workshopCardNumber identificira delavniško kartico, uporabljeno pri kalibriranju.

workshopCardExpiryDate je datum izteka veljavnosti kartice.

vehicleIdentificationNumber je VIN.

vehicleRegistrationIdentification vsebuje VRN in državo registracije vozila.

wVehicleCharacteristicConstant je značilni koeficient vozila.

kConstantOfRecordingEquipment je konstanta zapisovalne naprave.

lTyreCircumference je efektivni obseg avtoplaščev.

tyreSize je oznaka mer avtoplaščev na vozilu.

authorisedSpeed je odobrena hitrost vozila.

oldOdometerValue, **newOdometerValue** sta stara in nova vrednost števca prevožene poti.

oldTimeValue, **newTimeValue** sta stara in nova vrednost datuma in časa.

nextCalibrationDate je datum, na katerega naj se opravi naslednje kalibriranje vrste, označene v **CalibrationPurpose**, pri pooblaščenem kontrolnem organu.

2.119 VuCardIWData

Informacija, shranjena v enoti v vozilu, povezana s cikli vstavitve in izvleka voznikovih ali delavniških kartic v enoto v vozilu (zahteva 081).

```
VuCardIWData ::= SEQUENCE {
    noOfIWRecords                INTEGER(0..216-1),
    vuCardIWRecords SET          SIZE(noOfIWRecords) OF
                                VuCardIWRecord
}
```

noOfIWRecords je število zapisov, ki jih vsebuje množica **vuCardIWRecords**.

vuCardIWRecords je množica zapisov, povezanih s cikli vstavitve in izvleka kartice.

2.120 **VuCardIWRecord**

Informacija, shranjena v enoti v vozilu, povezana s ciklom vstavitve in izvleka voznikove ali delavniške kartice v enoti v vozilu (zahteva 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 priimek in ime(na) imetnika voznikove ali delavniške kartice, shranjen na kartici.

fullCardNumber obsega vrsto kartice, državo izdajateljico in številko kartice, shranjeno na kartici.

cardExpiryDate je datum izteka kartice, shranjen na kartici.

cardInsertionTime je datum in čas vstavitve.

vehicleOdometerValueAtInsertion je vrednost števca prevožene poti ob vstavitvi kartice.

cardSlotNumber je reža, v katero je vstavljena kartica.

cardWithdrawalTime je datum in čas izvleka kartice.

vehicleOdometerValueAtWithdrawal je vrednost števca prevožene poti ob izvleku kartice.

previousVehicleInfo vsebuje podatke o vozilu, ki ga je pred tem uporabljal voznik, shranjene na kartici.

manualInputFlag je zastavica, ki kaže, ali je imetnik kartice ob vstavitvi kartice ročno vnesel voznikove dejavnosti.

2.121 **VuCertificate**

Certifikat javnega ključa enote v vozilu.

```
VuCertificate ::= Certificate
```

2.122 **VuCompanyLocksData**

Informacija, shranjena v enoti v vozilu, povezana z blokadami podjetja (zahteva 104).

```
VuCompanyLocksData ::= SEQUENCE {
    noOfLocks                    INTEGER(0..20),
    vuCompanyLocksRecords        SET SIZE(noOfLocks) OF
                                VuCompanyLocksRecord
}
```

noOfLocks je število blokad, navedenih v **vuCompanyLocksRecords**.

vuCompanyLocksRecords je množica zapisov blokad podjetja.

2.123 VuCompanyLocksRecord

Informacija, shranjena v enoti v vozilu, povezana z blokado podjetja (zahteva 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
    lockInTime                TimeReal,
    lockOutTime               TimeReal,
    companyName               Name,
    companyAddress             Address,
    companyCardNumber         FullCardNumber
}
```

lockInTime, lockOutTime sta datum in čas vklopa ali izklopa blokade.

companyName, companyAddress sta ime in naslov podjetja, povezanega z vklopom blokade.

companyCardNumber identificira kartico, uporabljeno ob vklopu blokade.

2.124 VuControlActivityData

Informacija, shranjena v enoti v vozilu, povezanaz nadzori, pri katerih je bila uporabljena ta VU (zahteva 102).

```
VuControlActivityData ::= SEQUENCE {
    noOfControls               INTEGER(0..20),
    vuControlActivityRecords   SET SIZE(noOfControls) OF
                               VuControlActivityRecord
}
```

noOfControls je število nadzorov, navedenih v vuControlActivityRecords.

vuControlActivityRecords je množica zapisov nadzornih dejavnosti.

2.125 VuControlActivityRecord

Informacija, shranjena v enoti v vozilu, povezanaz nadzorom, pri kateri je bila uporabljena ta VU (zahteva 102).

```
VuControlActivityRecord ::= SEQUENCE {
    controlType                ControlType,
    controlTime                TimeReal,
    controlCardNumber          FullCardNumber,
    downloadPeriodBeginTime    TimeReal,
    downloadPeriodEndTime      TimeReal
}
```

controlType je vrsta nadzora.

controlTime je datum in čas nadzora.

ControlCardNumber identificira nadzornokartico, uporabljeno pri nadzoru.

downloadPeriodBeginTime je začetek obdobja, za katerega je bil opravljen prenos podatkov, če je bil tak prenos opravljen.

downloadPeriodEndTime je konec obdobja, za katerega je bil opravljen prenos podatkov, če je bil tak prenos opravljen.

2.126 VuDataBlockCounter

Števec, shranjen na kartici, ki označuje zaporedje ciklov vstavitve in izvleka kartice v različnih enotah v vozilu.

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

Priranje vrednosti: Zaporedno število z največjo vrednostjo 9 999; nato se začne spet od 0.

2.127 VuDetailedSpeedBlock

Informacija, shranjena v enoti v vozilu, povezana s podrobnimi podatki o hitrosti med gibanjem vozila (zahteva 093).

```

VuDetailedSpeedBlock ::= SEQUENCE {
    speedBlockBeginDate          TimeReal,
    speedsPerSecond              SEQUENCE SIZE (60) OF Speed
}

```

speedBlockBeginDate je datum in čas prve vrednosti hitrosti v bloku.

speedsPerSecond je časovno zaporedje vsako sekundo izmerjenih hitrosti od (vključno) minute, navedene v speed-BlockBeginDate.

2.128 VuDetailedSpeedData

Informacija, shranjena v enoti v vozilu, povezana s podrobnimi podatki o hitrosti vozila.

```

VuDetailedSpeedData ::= SEQUENCE
{
    noOfSpeedBlocks              INTEGER (0..216-1),
    vuDetailedSpeedBlocks        SET SIZE (noOfSpeedBlocks) OF
                                VuDetailedSpeedBlock
}

```

noOfSpeedBlocks je število blokov hitrosti v množici vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks je množica blokov podrobnih podatkov o hitrosti.

2.129 VuDownloadablePeriod

Najstarejši in najnovejši datum, za katerega enota v vozilu hrani podatke o vznikaških dejavnostih (zahteve 081, 084 ali 087).

```

VuDownloadablePeriod ::= SEQUENCE {
    minDownloadableTime          TimeReal
    maxDownloadableTime          TimeReal
}

```

minDownloadableTime is the oldest card insertion or activity change or place entry date and time stored in the VU.

maxDownloadableTime.

2.130 VuDownloadActivityData

Informacija, shranjena v enoti v vozilu, povezana z zadnjim prenosom podatkov (zahteva 105).

```

VuDownloadActivityData ::= SEQUENCE {
    downloadingTime              TimeReal,
    fullCardNumber                FullCardNumber,
    companyOrWorkshopName         Name
}

```

downloadingTime je datum in čas, ob katerem je bil opravljen prenos podatkov.

fullCardNumber identificira kartico, uporabljeno za odobritev prenosa podatkov.

companyOrWorkshopName je ime podjetja ali delavnice.

2.131 VuEventData

Informacija, shranjena v enoti v vozilu, povezana z dogodki (zahteva 094, razen z dogodki prekoračitve hitrosti).

```

VuEventData ::= SEQUENCE {
    noOfVuEvents                  INTEGER (0..255),
    vuEventRecords                SET SIZE (noOfVuEvents) OF VuEventRecord
}

```

noOfVuEvents je število dogodkov, navedenih v množici vuEventRecords.

vuEventRecords je množica zapisov dogodkov.

2.132 **VuEventRecord**

Informacija, shranjena v enoti v vozilu, povezana z dogodkom (zahteva 094, razen z dogodkom prekoračitve hitrosti).

```
VuEventRecord ::= SEQUENCE {
    eventType                      EventFaultType,
    eventRecordPurpose             EventFaultRecordPurpose,
    eventBeginTime                 TimeReal,
    eventEndTime                  TimeReal,
    cardNumberDriverSlotBegin     FullCardNumber,
    cardNumberCodriverSlotBegin   FullCardNumber,
    cardNumberDriverSlotEnd       FullCardNumber,
    cardNumberCodriverSlotEnd     FullCardNumber,
    similarEventsNumber           SimilarEventsNumber
}
```

eventType je vrsta dogodka.

eventRecordPurpose je namen, v katerega je bil ta dogodek zapisan.

eventBeginTime je datum in čas začetka dogodka.

eventEndTime je datum in čas konca dogodka.

cardNumberDriverSlotBegin identificira kartico, vstavljeno v voznikovo režo ob začetku dogodka.

cardNumberCodriverSlotBegin identificira kartico, vstavljeno v sovoznikovo režo ob začetku dogodka.

cardNumberDriverSlotEnd identificira kartico, vstavljeno v voznikovo režo ob koncu dogodka.

cardNumberCodriverSlotEnd identificira kartico, vstavljeno v sovoznikovo režo ob koncu dogodka.

similarEventsNumber je število podobnih dogodkov v tem dnevu.

To zaporedje se lahko uporablja za vse dogodke razen dogodkov prekoračitve hitrosti.

2.133 **VuFaultData**

Informacija, shranjena v enoti v vozilu, povezana z napakami (zahteva 096).

```
VuFaultData ::= SEQUENCE {
    noOfVuFaults                  INTEGER(0..255),
    vuFaultRecords SET            SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults je število napak, navedenih v množici vuFaultRecords.

vuFaultRecords je množica zapisov napak.

2.134 **VuFaultRecord**

Informacija, shranjena v enoti v vozilu, povezana z napako (zahteva 096).

```
VuFaultRecord ::= SEQUENCE {
    faultType                      EventFaultType,
    faultRecordPurpose             EventFaultRecordPurpose,
    faultBeginTime                 TimeReal,
    faultEndTime                  TimeReal,
    cardNumberDriverSlotBegin     FullCardNumber,
    cardNumberCodriverSlotBegin   FullCardNumber,
    cardNumberDriverSlotEnd       FullCardNumber,
    cardNumberCodriverSlotEnd     FullCardNumber
}
```

faultType je vrsta napake zapisovalne naprave.

faultRecordPurpose je namen, v katerega je bila ta napaka zapisana.

faultBeginTime je datum in čas začetka napake.

faultEndTime je datum in čas konca napake.

cardNumberDriverSlotBegin identificira kartico, vstavljeno v voznikovo režo ob začetku napake.

cardNumberCodriverSlotBegin identificira kartico, vstavljeno v sovoznikovo režo ob začetku napake.

cardNumberDriverSlotEnd identificira kartico, vstavljeno v voznikovo režo ob koncu napake.

cardNumberCodriverSlotEnd identificira kartico, vstavljeno v sovoznikovo režo ob koncu napake.

2.135 VuIdentification

Informacija, shranjena v enoti v vozilu, povezana z identifikacijo enote v vozilu (zahteva 075).

```
VuIdentification ::= SEQUENCE {
    vuManufacturerName          VuManufacturerName,
    vuManufacturerAddress       VuManufacturerAddress,
    vuPartNumber                VuPartNumber,
    vuSerialNumber              VuSerialNumber,
    vuSoftwareIdentification     VuSoftwareIdentification,
    vuManufacturingDate         VuManufacturingDate,
    vuApprovalNumber            VuApprovalNumber
}
```

vuManufacturerName je ime proizvajalca enote v vozilu.

vuManufacturerAddress je naslov proizvajalca enote v vozilu.

vuPartNumber je kataloška številka enote v vozilu.

vuSerialNumber je serijska številka enote v vozilu.

vuSoftwareIdentification identificira programsko opremo, nameščeno v enoti v vozilu.

vuManufacturingDate je datum izdelave enote v vozilu.

vuApprovalNumber je številka odobritve tipa enote v vozilu.

2.136 VuManufacturerAddress

Naslov proizvajalca enote v vozilu.

```
VuManufacturerAddress ::= Address
```

Prirejanje vrednosti: Ni predpisano.

2.137 VuManufacturerName

Ime proizvajalca enote v vozilu.

```
VuManufacturerName ::= Name
```

Prirejanje vrednosti: Ni predpisano.

2.138 VuManufacturingDate

Datum izdelave enote v vozilu.

```
VuManufacturingDate ::= TimeReal
```

Prirejanje vrednosti: Ni predpisano.

2.139 VuOverSpeedingControlData

Informacija, shranjena v enoti v vozilu, povezana z dogodki prekoračitve hitrosti od zadnjega nadzora prekoračitev hitrosti (zahteva 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
    lastOverspeedControlTime      TimeReal,
    firstOverspeedSince           TimeReal,
    numberOfOverspeedSince        OverspeedNumber
}
```

lastOverspeedControlTime je datum in čas zadnjega nadzora prekoračitev hitrosti.

firstOverspeedSince je datum in čas prve prekoračitve hitrosti po tem nadzoru prekoračitev hitrosti.

numberOfOverspeedSince je število dogodkov prekoračitve hitrosti od zadnjega nadzora prekoračitev hitrosti.

2.140 VuOverSpeedingEventData

Informacija, shranjena v enoti v vozilu, povezana s prekoračitvami hitrosti (zahteva 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
    noOfVuOverSpeedingEvents      INTEGER(0..255),
    vuOverSpeedingEventRecords    SET SIZE(noOfVuOverSpeedingEvents) OF
                                   VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents je število dogodkov, navedenih v množici vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords je množica zapisov dogodkov prekoračitve hitrosti.

2.141 VuOverSpeedingEventRecord

Informacija, shranjena v enoti v vozilu, povezana s prekoračitvami hitrosti (zahteva 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    eventType                     EventFaultType,
    eventRecordPurpose            EventFaultRecordPurpose,
    eventBeginTime                TimeReal,
    eventEndTime                  TimeReal,
    maxSpeedValue                 SpeedMax,
    averageSpeedValue             SpeedAverage,
    cardNumberDriverSlotBegin     FullCardNumber,
    similarEventsNumber           SimilarEventsNumber
}
```

eventType je vrsta dogodka.

eventRecordPurpose je namen, v katerega je bil ta dogodek zapisan.

eventBeginTime je datum in čas začetka dogodka.

eventEndTime je datum in čas konca dogodka.

maxSpeedValue je najvišja hitrost, izmerjena med dogodkom.

averageSpeedValue je aritmetična srednja vrednost hitrosti, izmerjenih med dogodkom.

cardNumberDriverSlotBegin identificira kartico, vstavljeno v voznikovo režo ob začetku dogodka.

similarEventsNumber je število podobnih dogodkov v tem dnevu.

2.142 VuPartNumber

Kataloška številka enote v vozilu.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Prirjevanje vrednosti: določi proizvajalec VU.

2.143 VuPlaceDailyWorkPeriodData

Informacija, shranjena v enoti v vozilu, povezana s kraji začetkov in koncev dnevnih delovnih izmen voznikov (zahteva 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
    noOfPlaceRecords                INTEGER(0..255),
    vuPlaceDailyWorkPeriodRecords    SET SIZE(noOfPlaceRecords) OF
                                     VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords je število zapisov, ki jih vsebuje množica vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords je množica zapisov krajev.

2.144 VuPlaceDailyWorkPeriodRecord

Informacija, shranjena v enoti v vozilu, povezana s krajem začetka ali konca dnevna delovne izmene voznika (zahteva 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
    fullCardNumber                  FullCardNumber,
    placeRecord                     PlaceRecord
}
```

fullCardNumber obsega vrsto voznikove kartice, državo izdajateljico in številko kartice.

placeRecord vsebuje informacije, povezane z vnesenim krajem.

2.145 VuPrivateKey

Zasebni ključ enote v vozilu.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146 VuPublicKey

Javni ključ enote v vozilu.

```
VuPublicKey ::= PublicKey
```

2.147 VuSerialNumber

Serijska številka enote v vozilu (zahteva 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148 VuSoftInstallationDate

Datum namestitve verzije programske opreme enote v vozilu.

```
VuSoftInstallationDate ::= TimeReal
```

Prirjevanje vrednosti: Ni predpisano.

2.149 VuSoftwareIdentification

Informacija, shranjena v enoti v vozilu, povezana z nameščeno programsko opremo.

```
VuSoftwareIdentification ::= SEQUENCE {
    vuSoftwareVersion                VuSoftwareVersion,
    vuSoftInstallationDate            VuSoftInstallationDate
}
```

vuSoftwareVersion je verzija programske opreme enote v vozilu.

vuSoftInstallationDate je datum namestitve programske opreme.

2.150 VuSoftwareVersion

Številka verzije programske opreme enote v vozilu.

VuSoftwareVersion ::= IA5String(SIZE(4))

Prirrejanje vrednosti: Ni predpisano.

2.151 VuSpecificConditionData

Informacija, shranjena v enoti v vozilu, povezana s posebnimi stanji.

```
VuSpecificConditionData ::= SEQUENCE {
    noOfSpecificConditionRecords          INTEGER(0..216-1)
    specificConditionRecords              SET SIZE (noOfSpecificConditionRecords) OF
                                          SpecificConditionRecord
}
```

noOfSpecificConditionRecords je število zapisov, ki jih vsebuje množica specificConditionRecords.

specificConditionRecords je množica zapisov o posebnih stanjih.

2.152 VuTimeAdjustmentData

Informacija, shranjena v enoti v vozilu, povezana z nastavitvami časa, opravljenimi izven okvira rednih kalibriranj (zahteva 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
    noOfVuTimeAdjRecords                INTEGER(0..6),
    vuTimeAdjustmentRecords              SET SIZE (noOfVuTimeAdjRecords) OF
                                          VuTimeAdjustmentRecords
}
```

noOfVuTimeAdjRecords je število zapisov v množici vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords je množica zapisov nastavljanja časa.

2.153 VuTimeAdjustmentRecord

Informacija, shranjena v enoti v vozilu, povezana z nastavitvijo časa, opravljeno izven okvira rednih kalibriranj (zahteva 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
    oldTimeValue                        TimeReal,
    oldTimeValue                        TimeReal,
    newTimeValue                        TimeReal,
    workshopName                        Name,
    workshopAddress                     Address,
    workshopCardNumber                  FullCardNumber
}
```

oldTimeValue, newTimeValue sta stara in nova vrednost datuma in časa.

workshopName, workshopAddress sta ime in naslov delavnice.

workshopCardNumber identificira delavniško kartico, uporabljeno pri nastavljanju časa.

2.154 W-VehicleCharacteristicConstant

Značilni koeficient vozila (opredelitev k).

W-VehicleCharacteristicConstant ::= INTEGER(0..2¹⁶-1)

Prirrejanje vrednosti: Število pulzov na kilometer poti, v delovnem območju od 0 do 64 255 pulzov/km.

2.155 WorkshopCardApplicationIdentification

Informacija, shranjena na delavniški kartici, povezana z identifikacijo aplikacije kartice (zahteva 190).

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

typeOfTachographCardId določa uporabljeno vrsto kartice.

cardStructureVersion določa verzijo strukture na kartici.

noOfEventsPerType je število dogodkov posamezne vrste, ki jih lahko zapiše kartica.

noOfFaultsPerType je število napak posamezne vrste, ki jih lahko zapiše kartica.

activityStructureLength označuje število bajtov na razpolago za hranjenje zapisov dejavnosti.

noOfCardVehicleRecords je število zapisov vozila, ki jih lahko vsebuje kartica.

noOfCardPlaceRecords je število krajev, ki jih lahko zapiše kartica.

noOfCalibrationRecords je število zapisov kalibriranja, ki jih lahko hrani kartica.

2.156 WorkshopCardCalibrationData

Informacija, shranjena na delavniški kartici, povezana z delavniškimi dejavnostmi opravljenimi s kartico (zahtevi 227 in 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
    calibrationTotalNumber      INTEGER(0..216-1),
    calibrationPointerNewestRecord  INTEGER(0..NoOfCalibrationRecords-1),
    calibrationRecords           SET SIZE (NoOfCalibrationRecords) OF
                                WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber je skupno število kalibriranj, opravljenih s kartico.

calibrationPointerNewestRecord je indeks zadnjega posodobljenega zapisa kalibriranja.

Prirjevanje vrednosti: Število, ki ustreza števcu zapisa kalibriranja; začne se z vrednostjo ,0' za prvi zapis kalibriranja v strukturi.

calibrationRecords je množica zapisov informacij o kalibriranju in/ali nastavljanju časa.

2.157 WorkshopCardCalibrationRecord

Informacija, shranjena na delavniški kartici, povezana s kalibriranjem opravljenim s kartico (zahteva 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 namen kalibriranja.

vehicleIdentificationNumber je VIN.

vehicleRegistration vsebuje VRN in državo registracije vozila.

wVehicleCharacteristicConstant je značilni koeficient vozila.

kConstantOfRecordingEquipment je konstanta zapisovalne naprave.

lTyreCircumference je efektivni obseg avtoplaščev.

tyreSize je oznaka mer avtoplaščev na vozilu.

authorisedSpeed je odobrena hitrost vozila.

oldOdometerValue, **newOdometerValue** sta stara in nova vrednost števca prevožene poti.

oldTimeValue, **newTimeValue** sta stara in nova vrednost datuma in časa.

nextCalibrationDate je datum, na katerega naj se opravi naslednje kalibriranje vrste, označene v **CalibrationPurpose**, pri pooblaščenem kontrolnem organu.

vuPartNumber, **vuSerialNumber** in **sensorSerialNumber** so podatkovni elementi za identifikacijo zapisovalne naprave.

2.158 WorkshopCardHolderIdentification

Informacija, shranjena na delavniški kartici, povezana z identifikacijo imetnika kartice (zahteva 216).

```

WorkshopCardHolderIdentification ::= SEQUENCE {
    workshopName                Name,
    workshopAddress              Address,
    cardHolderName               HolderName,
    cardHolderPreferredLanguage  Language
}

```

workshopName je ime delavnice imetnika kartice.

workshopAddress je naslov delavnice imetnika kartice.

cardHolderName je priimek in ime imetnika kartice (tj. ime mehanika).

cardHolderPreferredLanguage je izbrani jezik imetnika kartice.

2.159 WorkshopCardPIN

Osebnostna identifikacijska številka (PIN) delavniške kartice (requirement 213).

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

Prirejanje vrednosti: Koda PIN, poznana imetniku, desno do 8 bajtov napolnjena z vrednostmi 'FF'.

3. OPREDELITVE OBMOČIJ VREDNOSTI IN VELIKOSTI

Opredelitev vrednosti spremenljivk uporabljenih pri opredelitvah v točki 2.

TimeRealRange ::= 2³²-1

3.1 Opredelitve za voznikovo kartico:

Ime vrednosti spremenljivke	Minimum	Maksimum
CardActivityLengthRange	5 544 bajtov (28 dni po 93 sprememb dejavnosti na dan)	13 776 bajtov (28 dni po 240 sprememb dejavnosti na dan)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2 Opredelitve za delavniško kartico:

Ime vrednosti spremenljivke	Minimum	Maksimum
CardActivityLengthRange	198 bajtov (1 dan s 93 spremembami dejavnosti)	492 bajtov (1 dan s 240 spremembami dejavnosti)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3 Opredelitve za nadzorno kartico:

Ime vrednosti spremenljivke	Minimum	Maksimum
NoOfControlActivityRecords	230	520

3.4 Opredelitve za kartico podjetja:

Ime vrednosti spremenljivke	Minimum	Maksimum
NoOfCompanyActivityRecords	230	520

4. NABORI ZNAKOV

IA5Strings uporabljajo znake ASCII, opredeljene v ISO/IEC 8824-1. Za čitljivost in lažje navajanje so po rastočih vrednostih navedeni spodaj. V primerih neskladnosti ima ISO/IEC 8824-1 prednost pred spodnjim informativnim zapisom.

```
! " # $ % & ' ( ) * + , - . / 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 nizi znakov (Address, Name, VehicleRegistrationNumber) uporabljajo tudi znake, opredeljene s kodami 192 do 255 v ISO/IEC 8859-1 (nabor znakov Latin1) ali v ISO/IEC 8859-7 (grški nabor znakov).

5. KODIRANJE

Pri kodiranju po pravilih zapisa ASN.1 morajo biti vsi opredeljeni podatkovni tipi kodirani v skladu z ISO/IEC 8825-2 (poravnana varianta).

Dodatek 2

SPECIFIKACIJE TAHOGRAFSKIH KARTIC

Vsebina

1.	Uvod	377
1.1	Kratice	377
1.2	Literatura	378
2.	Električne in fizične lastnosti	378
2.1	Napajalna napetost in poraba toka	378
2.2	Napetost programiranja V_{pp}	379
2.3	Tvorba urnega signala in frekvenca	379
2.4	V/I kontakt	379
2.5	Stanja kartice	379
3.	Strojna oprema in komunikacije	379
3.1	Uvod	379
3.2	Protokol prenosa	379
3.2.1	Protokoli	379
3.2.2	ATR	380
3.2.3	PTS	381
3.3	Pogoji dostopa (AC)	381
3.4	Šifriranje podatkov	382
3.5	Pregled ukazov in kod napak	382
3.6	Opis ukazov	383
3.6.1	Izbira datoteke	383
3.6.1.1	Izbira po imenu (AID)	383
3.6.1.2	Izbira elementarne datoteke z uporabo njenega identifikatorja datoteke	384
3.6.2	Binarno branje	384
3.6.2.1	Ukazi brez varne obdelave sporočil	385
3.6.2.2	Ukazi z varno obdelavo sporočil	385
3.6.3	Binarno posodabljanje	387
3.6.3.1	Ukazi brez varne obdelave sporočil	387
3.6.3.2	Ukazi z varno obdelavo sporočil	388
3.6.4	Pridobitev poziva	389
3.6.5	Preverjanje	389
3.6.6	Pridobitev odziva	390
3.6.7	PSO: preverjanje certifikata	390
3.6.8	Notranja avtentifikacija	391

3.6.9	Zunanja avtentifikacija	392
3.6.10	Upravljanje varnega okolja	393
3.6.11	PSO: razpršitev	394
3.6.12	Razpršitev datoteke	394
3.6.13	PSO: izračun digitalnega podpisa	395
3.6.14	PSO: preverjanje digitalnega podpisa	396
4.	Struktura tahografskih kartic	396
4.1	Struktura voznikove kartice	397
4.2	Struktura delavniške kartice	399
4.3	Struktura nadzorne kartice	401
4.4	Struktura kartice podjetja	403

1. UVOD

1.1 Kratice

V okviru tega dodatka se uporabljajo naslednje kratice:

AC	pogoji dostopa
AID	identifikator aplikacije
ALW	vedno
APDU	podatkovna enota aplikacijskega protokola (struktura ukaza)
ATR	odziv na ponastavitev
AUT	avtentificiran
C6, C7	kontakta kartice št. 6 in 7, opisana v ISO/IEC 7816-2
cc	urni cikli
CHV	informacija preverjanja imetnika kartice
CLA	bajt razreda v ukazu APDU
DF	namenska datoteka. DF lahko vsebuje druge datoteke (EF ali DF)
EF	elementarna datoteka
ENC	šifrirano: dostop je možen le s kodiranjem podatkov
etu	elementarna enota časa
IC	integrirano vezje
ICC	kartica z integriranim vezjem
ID	identifikator
IFD	vmesniška naprava
IPS	velikost polja informacije
IFSC	velikost polja informacije za kartico
IFSD	velikost polja informacije za napravo (za terminal)
INS	bajt instrukcije v ukazu APDU
Lc	dolžina vhodnih podatkov za ukaz APDU
Le	dolžina pričakovanih podatkov (izhodni podatki za ukaz)
MF	glavna datoteka (korenska DF)
P1-P2	bajta parametrov
NAD	vozliščni naslov pri protokolu T=1
NEV	nikoli
PIN	osebna identifikacijska številka
PRO SM	zaščiteno z varno obdelavo sporočil
PTS	izbira protokola prenosa
RFU	rezervirano za prihodnjo rabo

RST	ponastavitev (kartice)
SM	varna obdelava sporočil
SW1-SW2	statusna bajta
TS	začetni znak ATR
VPP	napetost programiranja
XXh	vrednost XX v šestnajstiškem zapisu
	simbol spetja 03 04=0304.

1.2 Literatura

V tem dodatku so uporabljeni naslednji viri:

EN 726-3	Sistemi identifikacijskih kartic – Telekomunikacijske kartice in terminali s tiskanimi vezji – Del 3: Zahteve za kartice, neodvisne od aplikacije. December 1994
ISO/IEC 7816-2	Informacijska tehnologija – identifikacijske kartice — kontaktne kartice s tiskanimi vezji – Del 2: mere in položaj kontaktov. Prva izdaja: 1999.
ISO/IEC 7816-3	Informacijska tehnologija – identifikacijske kartice – kontaktne kartice s tiskanimi vezji – Del 3: elektronski signali in protokoli prenosa. 2. izdaja: 1997.
ISO/IEC 7816-4	Informacijska tehnologija – identifikacijske kartice — kontaktne kartice s tiskanimi vezji – Del 4: Panožni ukazi za izmenjavo. Prva izdaja: 1995 +Dopolnitev 1: 1997.
ISO/IEC 7816-6	Informacijska tehnologija – identifikacijske kartice – kontaktne kartice s tiskanimi vezji – Del 6: Panožni podatkovni elementi. Prva izdaja: 1996 + popr. 1: 1998.
ISO/IEC 7816-8	Informacijska tehnologija – identifikacijske kartice – kontaktne kartice s tiskanimi vezji – Del 8: Panožni ukazi povezani z varnostjo. Prva izdaja: 1999.
ISO/IEC 9797	Informacijska tehnologija – Varnostne tehnike – Mehanizem celovitosti podatkov z uporabo funkcije kriptografskega preverjanja z algoritmom šifre bloka. 2. izdaja: 1994.

2. ELEKTRIČNE IN FIZIČNE LASTNOSTI

TCS_200 Če ni predpisano drugače, morajo biti vsi elektronski signali v skladu z ISO/IEC 7816-3.

TCS_201 Položaji in mere kontaktov kartice morajo biti v skladu z ISO/IEC 7816-2.

2.1 Napajalna napetost in poraba toka

TCS_202 Kartica mora delovati v okviru predpisanih omejitev porabe v ISO/IEC 7816-3.

TCS_203 Kartica mora delovati z $V_{cc} = 3 \text{ V } (+/- 0,3 \text{ V})$ ali $V_{cc} = 5 \text{ V } (+/- 0,5 \text{ V})$.

Napetost se izbere po ISO/IEC 7816-3.

2.2 Napetost programiranja V_{pp}

- TCS_204 Kartica ne sme zahtevati napetosti programiranja na C6. Pričakuje se, da nožica C6 v IFD ni priključena. Kontakt C6 je lahko na kartici priključen na V_{cc} , ne sme pa biti priključen na ozemljitev. Te napetosti se ne sme prevajati v nobenem primeru.

2.3 Tvorba urnega signala in frekvenca

- TCS_205 Kartica mora delovati v območju frekvenc od 1 do 50 MHz. V eni seji s kartico se lahko urna frekvenca spreminja v območju $\pm 2\%$. Urno frekvenco tvori enota v vozilu, ne pa sama kartica. Obratovalni cikel se lahko spreminja v območju od 40 do 60 %.
- TCS_206 Pod pogoji, ki jih določa datoteka EF_{ICC} na kartici, se lahko zunanjo uro ustavi. V prvem bajtu vsebine datoteke EF_{ICC} so kodirani pogoji za režim Clockstop (glede podrobnosti glej EN 726-3).

Nizek	Visok		
Bit 3	Bit 2	Bit 1	
0	0	1	Ustavitev ure (Clockstop) dovoljena, ni prednostnega nivoja.
0	1	1	Ustavitev ure (Clockstop) dovoljena, prednostni nivo visok.
1	0	1	Ustavitev ure (Clockstop) dovoljena, prednostni nivo nizek.
0	0	0	Ustavitev ure (Clockstop) ni dovoljena.
0	1	0	Ustavitev ure (Clockstop) dovoljena le pri visokem nivoju.
1	0	0	Ustavitev ure (Clockstop) dovoljena le pri nizkem nivoju.

Biti 4 do 8 niso uporabljeni.

2.4 V/I kontakt

- TCS_207 V/I kontakt C7 se uporablja za sprejem podatkov iz IFD in oddajanje podatkov v IFD. Med delovanjem sme biti v oddajnem režimu bodisi samo kartica bodisi samo IFD. Tudi če sta obe enoti v režimu oddajanja, to ne sme poškodovati kartice. Kadar ne oddaja, se mora kartica prekloniti v režim sprejema.

2.5 Stanja kartice

- TCS_208 Kadar je priključena napajalna napetost, je kartica lahko v dveh stanjih:

- stanje delovanja, kadar izvršuje ukaze ali sodeluje z digitalno enoto,
- stanje mirovanja ves preostali čas; v tem stanju mora kartica ohranjati vse podatke.

3. STROJNA OPREMA IN KOMUNIKACIJE

3.1 Uvod

Ta točka opisuje minimalne funkcionalne zahteve za tahografske kartice in enote v vozilu, ki zagotavljajo pravilno delovanje in skupno uporabnost.

Tahografske kartice so kolikor le mogoče v skladu z ustreznimi veljavnimi standardi ISO/IEC (zlasti z ISO/IEC 7816). Vendar so ukazi in protokoli opisani v celoti, da so opredeljene morebitne omejitve rabe in razlike. Kadar ni označeno drugače, so določeni ukazi v celoti v skladu z navedenimi standardi.

3.2 Protokol prenosa

- TCS_300 Protokol prenosa je v skladu z ISO/IEC 7816-3. Še zlasti mora VU razpoznati podaljške čakalnih časov, ki ji jih sporoči kartica.

3.2.1 Protokoli

- TCS_301 Kartica mora podpirati oba protokola: T=0 in T=1.

TCS_302 Privzeti protokol je protokol T=0; za preklop na protokol T=1 je torej potreben ukaz PTS.

TCS_303 Naprave morajo podpirati neposredno konvencijo pri obeh protokolih. Torej je neposredna konvencija za kartico obvezna.

TCS_304 Ob ATR mora biti kartični bajt ‚velikost polja informacije‘ prisoten v znaku TA3. Ta vrednost mora biti najmanj ‚F0h‘ (= 240 bajtov).

Za protokola veljajo naslednje omejitve:

TCS_305 T=0

- Vmesniška naprava mora podpirati odgovor na V/I od 400 cc po dviznem robu signala na RST.
- Vmesniška naprava mora biti zmožna brati znake ločene z 12 etu.
- Vmesniška naprava mora prebrati napačen znak in njegovo ponovitev, če sta ločena s 13 etu. Če je zaznan napačen znak, lahko signal napake na V/I nastopi med 1 etu in 2 etu. Naprava mora podpirati zakasnitev 1 etu.
- Vmesniška naprava mora sprejemati 32-bajtni ATR (TS+32)
- Če je v ATR prisoten TC1, mora biti za znake, poslane iz vmesniške naprave, podan tudi dodatni varovalni čas (Extra Guard Time), znaki, poslani s kartice, pa so še vedno lahko ločeni z 12 etu. To velja tudi za znak ACK, ki ga pošlje kartica po znaku P3, oddanem iz vmesniške naprave.
- Vmesniška naprava mora upoštevati znak NUL, ki ga pošlje kartica.
- Vmesniška naprava mora sprejemati tudi komplementarni način ACK.
- Ukaza pridobitev odziva se ne sme uporabljati v verižnem režimu za pridobitev podatkov, katerih dolžina lahko presega 255 bajtov.

TCS_306 T=1

- Bajt NAD: se ne uporablja (NAD mora biti nastavljen na ‚00‘).
- ABORT S-bloka: se ne uporablja.
- Napaka stanja VPP S-bloka: se ne uporablja.
- Skupna dolžina veriženja podatkovnega polja ne presega 255 bajtov (kar naj zagotovi IFD).
- IFD mora podati velikost polja informacije za napravo (IFSD) takoj po ATR: IFD mora po ATR poslati zahtevek za IFS S-bloka, kartica pa mora poslati nazaj IFS S-bloka. Priporočena vrednost IFSD je 254 bajtov.
- Kartica ne bo zahtevala ponovne nastavitve IFS.

3.2.2 ATR

TCS_307 Naprava preverja bajte ATR po ISO/IEC 7816-3. Zgodovinskih znakov ATR se ne preverja.

Primer osnovnega bi-protokola ATR po ISO/IEC 7816-3

Znak	Vrednost	Opombe
TS	‚3Bh‘	Označuje neposredno konvencijo
T0	‚85h‘	TD1 prisoten; prisotnih je 5 zgodovinskih bajtov
TD1	‚80h‘	TD2 prisoten; uporablja se T=0
TD2	‚11h‘	TA3 prisoten; uporablja se T=1
TA3	‚XXh‘ (mind. ‚F0h‘)	Velikost polja informacij za kartico (IFSC)
TH1 do TH5	‚XXh‘	Zgodovinski znaki
TCK	‚XXh‘	Znaki za preverjanje (EX-OR)

TCS_308 Po odgovoru na ponastavitev (ATR) se samoumevno izbere glavna datoteka (MF) in ta postane tekoči imenik.

3.2.3 PTS

TCS_309 Privzeti protokol je T=0. Za nastavitev protokola T=1 mora naprava poslati kartici PTS (znan tudi kot PPS).

TCS_310 Ker sta za kartico obvezna oba protokola, T=0 in T=1, je za kartico obvezen tudi osnovni PTS za preklp protokolov.

PTS se lahko uporablja, kakor je prikazano v ISO/IEC 7816-3, za preklp na baudne hitrosti, višje od privzete baudne hitrosti, ki jo morebiti predlaga kartica v ATR (bajt TA(1)).

Za kartico so višje baudne hitrosti neobvezne.

TCS_311 Če ni podprta nobena baudna hitrost razen privzete (ali če ni podprta izbrana baudna hitrost), mora kartica na PTS odgovoriti pravilno po ISO/IEC 7816-3 z izpustitvijo bajta PPS1.

Primeri osnovnih PTS za izbiro protokola so naslednji:

Znak	Vrednost	Opombe
PPSS	'FFh'	Znak za začetek
PPS0	'00h' ali '01h'	PPS1 do PPS3 niso prisotni; z '00h' se izbere T0, z '01h' pa T1.
PK	'XXh'	Znak za preverjanje: 'XXh' = 'FFh' če PPS0 = '00h' 'XXh' = 'FEh' če PPS0 = '01h'

3.3 Pogoji dostopa (AC)

Pogoji dostopa (AC) za ukaza UPDATE_BINARY in READ_BINARY so opredeljeni za vsako elementarno datoteko posebej.

TCS_312 Pred dostopom do trenutne datoteke s tema ukazoma morajo biti izpolnjeni AC za to datoteko.

Opredelitve razpoložljivih pogojev dostopa so naslednje:

- ALW: Akcija je vedno mogoča in se lahko izvede brez vseh omejitev.
- NEV: Akcija ni mogoča nikoli.
- AUT: Pravico je treba zagotoviti z ustrezno zunanjo avtentifikacijo (ki se izvede z ukazom EXTERNAL_AUTHENTICATE).
- PRO SM: Ukaz je treba poslati skupaj s kriptografsko preskusno vsoto in s postopkom varnega sporočanja (glej dodatek 11).
- AUT in PRO-SM (združena).

Za ukaza za obdelavo (UPDATE_BINARY in READ_BINARY) je mogoče na kartici nastaviti naslednje pogoje dostopa:

	UPDATE_BINARY	READ_BINARY
ALW	da	da
NEV	da	da
AUT	da	da
PRO SM	da	ne
AUT in PRO SM	da	ne

Za ukaz READ_BINARY pogoja dostopa PRO SM ni mogoče nastaviti. To pomeni, da prisotnost kriptografske preskusne vsote za ukaz READ ni nikoli obvezna. Z uporabo vrednost '0C' za razred pa je mogoče uporabljati ukaz READ_BINARY tudi z varnim sporočanjem, kakor je opisano v točki 3.6.2.

3.4 Šifriranje podatkov

Kadar je treba varovati zaupnost podatkov branih iz datoteke, je ta datoteka označena kot ‚šifrirana‘. Šifriranje se izvaja s postopki varnega sporočanja (glej dodatek 11).

3.5 Pregled ukazov in kod napak

Ukazi in organizacija datotek so izpeljani iz ISO/IEC 7816-4 in so v skladu s tem standardom.

TCS_313 Ta točka opisuje naslednje pare ukazov-odgovorov APDU:

Ukaz	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 V vsako sporočilo odgovora sta vključeni statusni besedi SW1 SW2, ki označujeta stanje obdelave ukaza.

SW1	SW2	Pomen
90	00	Normalna obdelava
61	XX	Normalna obdelava. XX = število razpoložljivih bajtov odgovora
62	81	Opozorilo glede obdelave. Del vrnjenih podatkov je lahko pokvarjenih.
63	CX	Napačen CHV (PIN). Števec preostalih poskusov je podan v 'X'.
64	00	Napaka pri izvedbi — stanje trajnega pomnilnika nespremenjeno. Napaka celovitosti.
65	00	Napaka pri izvedbi — stanje trajnega pomnilnika spremenjeno.
65	81	Napaka pri izvedbi — stanje trajnega pomnilnika spremenjeno — Napaka pomnilnika.
66	88	Varnostna napaka: napačna kriptografska preskusna vsota (pri varnem sporočanju) ali napačen certifikat (pri preverjanju certifikata) ali napačen kriptogram (pri zunanji avtentifikaciji) ali napačen podpis (pri preverjanju podpisa).
67	00	Napačna dolžina (napačen Lc ali Le)
69	00	Prepovedan ukaz (pri T=0 ni na voljo nikakršnega odgovora)
69	82	Varnostni status nezadovoljiv
69	83	Metoda avtentifikacije blokirana
69	85	Pogoji uporabe niso izpolnjeni
69	86	Ukaz ni dovoljen (ni tekoče EF)
69	87	Manjkajo pričakovani podatkovni objekti varnega sporočanja
69	88	Nepravilni podatkovni objekti varnega sporočanja
6A	82	Datoteka ni najdena
6A	86	Napačna parametra P1-P2
6A	88	Podatki, na katere se sklicuje ukaz, niso najdeni
6B	00	Napačni parametri (zamik zunaj EF)

SW1	SW2	Pomen
6C	XX	Napačna dolžina, SW2 podaja točno dolžino. Ni vrnjeno nobeno podatkovno polje.
6D	00	Ukazna koda ni podprta ali ni veljavna.
6E	00	Razred ni podprt
6F	00	Druge napake pri preverjanju

3.6 Opis ukazov

V tej točki so opisani obvezni ukazi tahografske kartice.

Druge pomembne podrobnosti, povezane z uporabljanimi kriptografskimi postopki, so podane v dodatku 11, Skupni varnostni mehanizmi.

Opisi ukazov so podani neodvisno od uporabljenega protokola (T=0 ali T=1). Pri vsakem so navedeni bajti APDU CLA, INS, P1, P2, Lc in Le. Če pri določenem ukazu Lc ali Le ni potreben, so postavke dolžine, vrednosti in opisa prazne.

TCS_315 Če sta zahtevana oba bajta dolžine (Lc in Le), mora biti opisani ukaz razdeljen v dva dela, kadar IFD uporablja protokol T=0. IFD najprej pošlje opisani ukaz s P3=Lc + podatki, nato pa pošlje ukaz GET_RESPONSE (glej točko 3.6.6) s P3=Le.

TCS_316 Če sta zahtevana oba bajta dolžine in je Le=0 (varno sporočanje):

- Pri protokolu T=1 mora kartica odgovoriti na Le=0 tako, da pošlje vse razpoložljive izhodne podatke.
- Pri protokolu T=0 mora IFD poslati prvi ukaz s P3=Lc + podatki; kartica mora odgovoriti (na ta implicitni Le=0) tako, da pošlje statusna bajta '61La', pri čemer je La razpoložljivih bajtov za odgovor. IFD mora nato za branje podatkov tvoriti ukaz GET RESPONSE s P3=La.

3.6.1 Izbira datoteke

Ta ukaz je v skladu z ISO/IEC 7816-4, ima pa v primerjavi z opredelitvijo v tem standardu precej omejeno uporabo.

Ukaz SELECT FILE se uporablja:

- za izbiro aplikativne DF (obvezna izbira po imenu),
- za izbiro elementarne datoteke, ki ustreza podanemu ID datoteke.

3.6.1.1 Izbira po imenu (AID)

Ta ukaz omogoča izbiro aplikativne DF na kartici.

TCS_317 Ta ukaz se lahko izvede od koderkoli v datotečni strukturi (po ATR ali ob kateremkoli drugem času).

TCS_318 Izbira aplikacije ponastavi tekoče varnostno okolje. Po izbiri aplikacije ne ostane izbran noben javni ključ, prav tako za varno sporočanje ni več na voljo prejšnji ključ seje. Izgubljen je tudi pogoj dostopa AUT.

TCS_319 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Izbira po imenu (AID)
P2	1	'0Ch'	Ni pričakovan nikakršen odgovor
Lc	1	'NNh'	Število bajtov poslanih kartici (dolžina AID): '06h' za tahografsko aplikacijo
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' za tahografsko aplikacijo

Na ukaz SELECT FILE ni potreben nikakršen odgovor (Pri T=0 je Le odsoten, pri T=1 pa ni zahtevan nikakršen odgovor).

TCS_320 Sporočilo odgovora (ni zahtevan nikakršen odgovor)

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če aplikacija, ustrežajoča AID, ni najdena, je vrnjeno stanje obdelave '6A82',
- pri T=1 je pri prisotnem Le vrnjeno stanje '6700',
- pri T=0 je v primeru, če je po ukazu SELECT FILE zahtevan odgovor, vrnjeno stanje obdelave '6900',
- če velja izbrana aplikacija za pokvarjeno (ugotovljena napaka celovitosti v atributih datoteke), je vrnjeno stanje obdelave '6400' ali '6581'.

3.6.1.2 Izbira elementarne datoteke z uporabo njenega identifikatorja datoteke

TCS_321 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Izbira EF v okviru tekoče DF
P2	1	'0Ch'	Ni pričakovan nikakršen odgovor
Lc	1	'02h'	Število bajtov poslanih kartici
#6-#7	2	'XXXXh'	Identifikator datoteke

Na ukaz SELECT FILE ni potreben nikakršen odgovor (Pri T=0 je Le odsoten, pri T=1 pa ni zahtevan nikakršen odgovor).

TCS_322 Sporočilo odgovora (ni zahtevan nikakršen odgovor)

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če datoteka, ustrežajoča identifikatorju, ni najdena, je vrnjeno stanje obdelave '6A82',
- pri T=1 je pri prisotnem Le vrnjeno stanje '6700',
- pri T=0 je v primeru, če je po ukazu SELECT FILE zahtevan odgovor, vrnjeno stanje obdelave '6900',
- če velja izbrana datoteka za pokvarjeno (ugotovljena napaka celovitosti v atributih datoteke), je vrnjeno stanje obdelave '6400' ali '6581'.

3.6.2 **Binarno branje**

Ta ukaz je v skladu z ISO/IEC 7816-4, ima pa v primerjavi z opredelitvijo v tem standardu precej omejeno uporabo.

Ukaz READ BINARY se uporablja za branje podatkov iz transparentne datoteke.

Odgovor kartice obsega vrnjene prebrane podatke, neobvezno enkapsulirane v strukturo varnega sporočanja.

TCS_323 Ukaz se lahko izvede le, če varnostni status ustreza varnostnim atributom, opredeljenim za EF za funkcijo READ:

3.6.2.1 Ukaz brez varne obdelave sporočil

Ta ukaz omogoča IFD brati podatke iz trenutno izbrane EF brez postopkov varnega sporočanja.

TCS_324 Ta ukaz ne sme omogočati branja podatkov iz datoteke z oznako ‚šifrirana‘.

TCS_325 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	Ni zahtevano varno sporočanje
INS	1	'B0h'	
P1	1	'XXh'	Zamik, v bajtih, od začetka datoteke: bajt z največjo težo
P2	1	'XXh'	Zamik, v bajtih, od začetka datoteke: bajt z najmanjšo težo
Le	1	'XXh'	Pričakovana dolžina podatkov, število bajtov, ki naj se preberejo

:Opomba: bit 8 v P1 mora biti nastavljen na 0.

TCS_326 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
#1-#X	X	'XX..XXh'	Prebrani podatki
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če ni izbrana nobena EF, je vrnjeno stanje obdelave '6986',
- če niso izpolnjeni pogoji dostopa za izbrano datoteko, se ukaz prekine z '6982',
- če zamik ni v skladu z velikostjo EF (zamik > velikost EF), je vrnjeno stanje obdelave '6B00',
- če velikost polja podatkov, ki jih jer treba prebrati, ni v skladu z velikostjo EF (zamik + Le > velikost EF), je vrnjeno stanje '6700' ali '6Cxx', pri čemer je 'xx' točna dolžina,
- če je zaznana napaka celovitosti v atributih datoteke, mora kartica šteti datoteko za pokvarjeno in nepopravljivo ter vrniti stanje obdelave '6400' ali '6581',
- če je zaznana napaka celovitosti v shranjenih podatkih, mora kartica vrniti zahtevane podatke in stanje obdelave '6281'.

3.6.2.2 Ukaz z varno obdelavo sporočil

Ta ukaz omogoča IFD brati podatke iz trenutno izbrane EF s postopki varnega sporočanja s preverjanjem celovitosti sprejetih podatkov in z zaščito zaupnosti podatkov, kadar je datoteka označena kot ‚šifrirana‘.

TCS_327 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'0Ch'	Zahtevano varno sporočanje
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (zamik, v bajtih, od začetka datoteke): bajt z največjo težo
P2	1	'XXh'	P2 (zamik, v bajtih, od začetka datoteke): bajt z najmanjšo težo
Lc	1	'09h'	Dolžina vhodnih podatkov za varno sporočanje
#6	1	'97h'	T _{LE} : značka predpisa pričakovane dolžine
#7	1	'01h'	L _{LE} : dolžina pričakovane dolžine
#8	1	'NNh'	Predpis pričakovane dolžine (originalni Le): število bajtov, ki naj se preberejo

Bajt	Dolžina	Vrednost	Opis
#9	1	'8Eh'	T _{CC} : značka za kriptografsko preskusno vsoto
#10	1	'04h'	L _{CC} : dolžina kriptografske preskusne vsote v nadaljevanju
#11-#14	4	'XX..XXh'	Kriptografska preskusna vsota (4 bajti z največjo težo)
Le	1	'00h'	Kakor predpisuje ISO/IEC 7816-4

TCS_328 Sporočilo odziva, če EF ni označena kot 'šifrirana' in če je vhodni format varnega sporočanja nepravilen:

Bajt	Dolžina	Vrednost	Opis
#1	1	'81h'	T _{py} : značka za nešifrirane podatke
#2	L	'NNh' ali '81	L _{py} : dolžina vrnjenih podatkov (=originalni Le) L je 2 bajta, če je L _{py} > 127 bajtov
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	nešifrirana vrednost podatkov
#(2+L+NN)	1	'8Eh'	T _{CC} : značka za kriptografsko preskusno vsoto
#(3+L+NN)	1	'04h'	L _{CC} : dolžina kriptografske preskusne vsote v nadaljevanju
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Kriptografska preskusna vsota (4 bajti z največjo težo)
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

TCS_329 Sporočilo odziva, če je EF označena kot 'šifrirana' in če je vhodni format varnega sporočanja pravilen:

Bajt	Dolžina	Vrednost	Opis
#1	1	'87h'	T _{PI CG} : značka za šifrirane podatke (kriptogram)
#2	L	'MMh' ali '81 MMh'	L _{H CG} : dolžina vrnjenih šifriranih podatkov (različna od originalne vrednosti Le iz ukaza zaradi šifriranja) L je 2 bajta, če je L _{PI CG} > 127 bajtov
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Šifrirani podatki: oznaka šifriranja in kriptogram
#(2+L+MM)	1	'8Eh'	T _{CC} : značka za kriptografsko preskusno vsoto
#(3+L+MM)	1	'04h'	L _{CC} : dolžina kriptografske preskusne vsote v nadaljevanju
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Kriptografska preskusna vsota (4 bajti z največjo težo)
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

V prvem bajtu vrnjenih šifriranih podatkov je označen način šifriranja. Pri tahografski aplikaciji ima oznaka šifriranja vedno vrednost '01h', kar pomeni, da je uporabljen način šifriranja tak, kakršnega predpisuje ISO/IEC 7816-4 (en bajt z vrednostjo '80h', sledi pa mu nekaj ničelnih bajtov: metoda 2 po ISO/IEC 9797).

Vrnjena so lahko 'pravilna' stanja obdelave, opisana pri ukazu READ BINARY brez varnega sporočanja (v točki 3.6.2.1), z uporabljenimi zgoraj opisanimi strukturami sporočil odgovora, z značko '99h' (kakor je opisano v TCS_335).

Lahko pa pride tudi do nekaterih napak, povezanih posebej z varnim sporočanjem. V teh primerih se enostavno vrne stanje obdelave brez vključitve struktur varnega sporočanja.

TCS_330 Sporočilo odgovora pri nepravilnem vhodnem formatu varnega sporočanja

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

— Če ni na voljo nobenega ključa tekoče seje, je vrnjeno stanje obdelave '6A88'. To se zgodi lahko v primeru, če ključ seje še ni bil tvorjen ali če je veljavnost ključa seje iztekla (v tem primeru mora IFD ponovno izvesti proces medsebojne avtentifikacije, ki tvori nov ključ seje).

— Če nekateri pričakovani podatkovni objekti (predpisani zgoraj) manjkajo v formatu varnega sporočanja, je vrnjeno stanje obdelave '6987': ta napaka nastopi, če manjka pričakovana značka ali če telo ukaza ni pravilno sestavljeno.

- Če so napačni nekateri podatkovni objekti, se vrne stanje obdelave '6988': ta napaka nastopi, če so prisotne vse zahtevane značke, pač pa so nekatere dolžine drugačne od pričakovanih.
- Če ne uspe preverjanje kriptografske preskusne vsote, se vrne stanje obdelave '6688'.

3.6.3 *Binarno posodabljanje*

Ta ukaz je v skladu z ISO/IEC 7816-4, ima pa v primerjavi z opredelitvijo v tem standardu precej omejeno uporabo.

Sporočilo ukaza UPDATE BINARY sproži posodobitev (brisanje + pisanje) bitov, ki so v EF že prisotni v binarni obliki, z biti, podanim v ukazu APDU.

TCS_331 Ukaz je mogoče izvesti le, če varnostni status ustreza varnostnim atributom, opredeljenim za EF za funkcijo UPDATE (Če pogoji dostopa funkcije UPDATE vključujejo pogoj PRO SM, mora biti v ukaz vključeno varno sporočanje).

3.6.3.1 *Ukaz brez varne obdelave sporočil*

Ta ukaz omogoča IFD vpisati podatke v trenutno izbrano EF, ne da bi kartica preverjala celovitost prejetih podatkov. Ta navadni način je dovoljen le, če zadevna datoteka ni označena kot 'šifrirana'.

TCS_332 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	Ni zahtevano varno sporočanje
INS	1	'D6h'	Zamik, v bajtih, od začetka datoteke: bajt z največjo težo
P1	1	'XXh'	
P2	1	'XXh'	Zamik, v bajtih, od začetka datoteke: bajt z najmanjšo težo
Lc	1	'NNh'	Lc: dolžina podatkov, ki naj se posodobijo. Število bajtov, ki naj se zapišejo.
#6-#(5+NN)	NN	'XX..XXh'	Podatki, ki naj se zapišejo.

:Opomba: bit 8 v P1 mora biti nastavljen na 0.

TCS_333 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če ni izbrana nobena EF, je vrnjeno stanje obdelave '6986',
- če niso izpolnjeni pogoji dostopa za izbrano datoteko, se ukaz prekine z '6982',
- če zamik ni v skladu z velikostjo EF (zamik > velikost EF), je vrnjeno stanje obdelave '6B00',
- če velikost polja podatkov, ki jih je treba zapisati, ni v skladu z velikostjo EF (zamik + Le > velikost EF), je vrnjeno stanje '6700',
- če je zaznana napaka celovitosti v atributih datoteke, mora kartica šteti datoteko za pokvarjeno in nepopravljivo ter vrniti stanje obdelave '6400' ali '6500',
- če vpis ni uspešen, je vrnjeno stanje obdelave '6581'.

3.6.3.2 Ukaz z varno obdelavo sporočil

Ta ukaz omogoča IFD vpisati podatke v trenutno izbrano EF, pri tem pa kartica preveri celovitost prejetih podatkov. Ker ni zahtevana zaupnost, podatki niso šifrirani.

TCS_334 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'0Ch'	Zahtevana varna obdelava sporočil.
INS	1	'D6h'	INS
P1	1	'XXh'	Zamik, v bajtih, od začetka datoteke: bajt z največjo težo
P2	1	'XXh'	Zamik, v bajtih, od začetka datoteke: bajt z najmanjšo težo
Lc	1	'XXh'	Dolžina polja zaščitene podatkov
#6	1	'81h'	T _{PV} : značka za nešifrirane podatke
#7	L	'NNh' ali '81 NNh'	L _{PV} : dolžina poslanih podatkov L je 2 bajta, če je L _{PV} > 127 bajtov
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Vrednost nešifriranih podatkov (ki naj se zapišejo)
#(7+L+NN)	1	'8Eh'	T _{CC} : značka za kriptografsko preskusno vsoto
#(8+L+NN)	1	'04h'	L _{CC} : dolžina kriptografske preskusne vsote v nadaljevanju
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Kriptografska preskusna vsota (4 bajti z največjo težo)
Le	1	'00h'	Kakor predpisuje ISO/IEC 7816-4

TCS_335 Sporočilo odgovora pri pravilnem vhodnem formatu varnega sporočanja

Bajt	Dolžina	Vrednost	Opis
#1	1	'99h'	T _{SW} : značka za statusne besede (ki naj se jih zaščiti s CC)
#2	1	'02h'	L _{SW} : dolžina vrnjenih statusnih besed
#3-#4	2	'XXXXh'	Statusni besedi (SW1, SW2)
#5	1	'8Eh'	T _{CC} : značka za kriptografsko preskusno vsoto
#6	1	'04h'	L _{CC} : dolžina kriptografske preskusne vsote v nadaljevanju
#7-#10	4	'XX..XXh'	Kriptografska preskusna vsota (4 bajti z največjo težo)
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

Vrnjena so lahko 'pravilna' stanja obdelave, opisana pri ukazu UPDATE BINARY brez varnega sporočanja (v točki 3.6.3.1), z uporabljenimi zgoraj opisanimi strukturami sporočil odgovora.

Lahko pa pride tudi do nekaterih napak, povezanih posebej z varnim sporočanjem. V teh primerih se enostavno vrne stanje obdelave brez vključitve struktur varnega sporočanja.

TCS_336 Sporočilo odgovora ob napaki pri varnem sporočanju

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če ni na voljo nobenega ključa tekoče seje, je vrnjeno stanje obdelave '6A88',
- če nekateri pričakovani podatkovni objekti (predpisani zgoraj) manjkajo v formatu varnega sporočanja, je vrnjeno stanje obdelave '6987': ta napaka nastopi, če manjka pričakovana značka ali če telo ukaza ni pravilno sestavljeno,
- če so napačni nekateri podatkovni objekti, se vrne stanje obdelave '6988': ta napaka nastopi, če so prisotne vse zahtevane značke, pač pa so nekatere dolžine drugačne od pričakovanih,
- če ne uspe preverjanje kriptografske preskusne vsote, se vrne stanje obdelave '6688'.

3.6.4 **Pridobitev poziva**

Ta ukaz je v skladu z ISO/IEC 7816-4, ima pa v primerjavi z opredelitvijo v tem standardu precej omejeno uporabo.

Ukaz GET CHALLENGE zahteva od kartice, naj pošlje poziv, ki bo uporabljen pri določenem varnostnem postopku, s katerim se kartici pošlje kriptogram ali šifrirane podatke.

TCS_337 Poziv, ki ga izda kartica, velja le za naslednji ukaz, ki uporablja od kartice izdani poziv.

TCS_338 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (dolžina pričakovanega poziva)

TCS_339 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
#1-#8	8	'XX..XXh'	Poziv
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če je Le različen od '08h', je stanje obdelave '6700',
- če nista pravilna parametra P1-P2, je stanje obdelave '6A86'.

3.6.5 **Preverjanje**

Ta ukaz je v skladu z ISO/IEC 7816-4, ima pa v primerjavi z opredelitvijo v tem standardu precej omejeno uporabo.

Ukaz VERIFY sproži na kartici primerjavo podatkov CHV (PIN), poslanega z ukazom, z referenčnim CHV, shranjenim na kartici.

Opomba: PIN, ki ga vnese uporabnik, mora IFD na desni dopolniti z bajti 'FFh' do skupne dolžine 8 bajtov.

TCS_340 Če je ukaz uspešen, se odobrijo pravice, ki ustrezajo predloženemu CHV, števec preostalih poskusov vnosa CHV pa se nastavi nazaj na začetno vrednost.

TCS_341 Neuspešna primerjava se zapiše na kartico, tako da se omeji število nadaljnjih poskusov uporabe referenčnega CHV.

TCS_342 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (preverjani CHV je implicitno poznan)
Lc	1	'08h'	Dolžina kode CHV, ki se pošilja
#6-#13	8	'XX..XXh'	CHV

TCS_343 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če referenčni CHV ni najden, je vrnjeno stanje obdelave '6A88',
- če je CHV blokiran (števec preostalih poskusov za CHV je nič), je vrnjeno stanje obdelave '6983'. Ko določen CHV enkrat pride v to stanje, ga ni nikoli več mogoče uspešno predložiti,
- če je primerjava neuspešna, se števec preostalih poskusov zmanjša in je vrnjeno stanje obdelave '63CX' ($X > 0$, pri čemer je X vrednost števca preostalih poskusov. X = 'F' pomeni, da je števec preostalih poskusov večji od 'F'),
- če referenčni CHV velja za pokvarjenega, je vrnjeno stanje obdelave '6400' ali '6581'.

3.6.6 Pridobitev odziva

Ta ukaz je v skladu z ISO/IEC 7816-4.

Ta ukaz (potrben in na voljo le pri protokolu T=0) se uporablja za prenos pripravljenih podatkov s kartice v vmesniško napravo (primer, ko ukaz vključuje tako Lc kot Le).

Ukaz GET_RESPONSE mora biti izdan neposredno po ukazu za pripravo podatkov, drugače so podatki izgubljeni. Po izvedbi ukaza GET_RESPONSE prej pripravljeni podatki niso več na voljo (razen ob napaki '61xx' ali '6Cxx' — glej spodaj).

TCS_344 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Število pričakovanih bajtov

TCS_345 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
#1-#X	X	'XX..XXh'	Podatki
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000'.
- Če kartica ni pripravila nobenih podatkov, vrne stanje obdelave '6900' ali '6F00'.
- Če Le presega število razpoložljivih bajtov ali če je Le nič, se vrne stanje obdelave '6Cxx', pri čemer 'xx' pomeni dejansko število razpoložljivih bajtov. V tem primeru ostanejo pripravljeni podatki na voljo za naslednji ukaz GET_RESPONSE.
- Če Le ni nič in je manjši od števila razpoložljivih bajtov, kartica normalno pošlje zahtevano število bajtov in vrne stanje obdelave '61xx', pri čemer 'xx' pomeni število dodatnih bajtov, ki so še na voljo za naslednji ukaz GET_RESPONSE.
- Če ukaz ni podprt (protokol T=1), kartica vrne stanje obdelave '6D00'.

3.6.7 PSO: preverjanje certifikata

Ta ukaz je v skladu z ISO/IEC 7816-8, ima pa v primerjavi z opredelitvijo v tem standardu precej omejeno uporabo.

Ukaz VERIFY CERTIFICATE uporablja kartica za to, da pridobi od zunaj javni ključ in preveri njegovo veljavnost.

TCS_346 Če je ukaz VERIFY CERTIFICATE uspešen, se javni ključ shrani za nadaljnjo uporabo v varnem okolju. Ta ključ mora ob uporabi svojega identifikatorja ključa izrecno nastaviti ukaz MSE (glej točko 3.6.10) za uporabo pri ukazih, povezanih z varnostjo (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE ali VERIFY CERTIFICATE).

TCS_347 V vsakem primeru ukaz VERIFY CERTIFICATE uporablja za odpiranje certifikata javni ključ, ki ga je pred tem izbral ukaz MSE. Ta javni ključ mora biti javni ključ države članice ali evropski javni ključ.

TCS_348 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Izvedba varnostne operacije
P1	1	'00h'	P1
P2	1	'AEh'	P2: podatki, ne kodirani z BER-TLV (združevanje podatkovnih elementov)
Lc	1	'CEh'	Lc: dolžina certifikata, 194 bajtov
#6-#199	194	'XX.XXh'	Certifikat: združevanje podatkovnih elementov (opisano v dodatku 11)

TCS_349 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če ne uspe preverjanje certifikata, se vrne stanje obdelave '6688'. Proces razvitja in preverjanja certifikata je opisan v dodatku 11,
- če v varnem okolju ni prisoten noben javni ključ, se vrne stanje '6A88',
- če velja izbrani javni ključ (uporabljen za razvitje certifikata) za pokvarjenega, se vrne stanje obdelave '6400' ali '6581',
- če ima izbrani javni ključ (uporabljen za razvitje certifikata) CHA.LSB (CertificateHolderAuthorisation.equipmentType) različen od '00' (tj., ni javni ključ države članice ali evropski javni ključ), se vrne stanje obdelave '6985'.

3.6.8 Notranja avtentifikacija

Ta ukaz je v skladu z ISO/IEC 7816-4.

Z ukazom INTERNAL AUTHENTICATE lahko IFD avtentificira kartico.

Proces avtentifikacije je opisan v dodatku 11. Obsega naslednje stavke:

TCS_350 Ukaz INTERNAL AUTHENTICATE uporablja zasebni ključ kartice (izbran implicitno) za označitev avtentifikacijskih podatkov, vključno s K1 (prvi element za dogovor o ključu seje) in RND1, ter uporablja trenutno izbrani javni ključ (izbran z ukazom MSE) za šifriranje podpisa in oblikovanje avtentifikacijskega žetona (podrobnejši opis v dodatku 11).

TCS_351 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Dolžina podatkov poslanih kartici
#6-#13	8	'XX..XXh'	Poziv, uporabljen za avtentifikacijo kartice
#14-#21	8	'XX..XXh'	VU.CHR (glej dodatek 11)
Le	1	'80h'	Dolžina podatkov, pričakovana od kartice

TCS_352 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
#1-#128	128	'XX..XXh'	Žeton avtentifikacije kartice (glej dodatek 11)
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če v varnem okolju ni prisoten noben javni ključ, se vrne stanje '6A88',
- če v varnem okolju ni prisoten noben zasebni ključ, se vrne stanje '6A88',
- če se VU.CHR ne ujema z identifikatorjem trenutnega javnega ključa, se vrne stanje '6A88',
- če izbrani zasebni ključ velja za pokvarjenega, je vrnjeno stanje obdelave '6400' ali '6581'.

TCS_353 Če je ukaz INTERNAL_AUTHENTICATE uspešen, se trenutni ključ seje (če obstaja) zbriše in ni več na voljo. Pogoji za razpoložljivost novega ključa seje je uspešna izvedba ukaza EXTERNAL_AUTHENTICATE.

3.6.9 Zunanja avtentifikacija

Ta ukaz je v skladu z ISO/IEC 7816-4.

Z ukazom EXTERNAL_AUTHENTICATE lahko kartica avtentificira IFD.

Proces avtentifikacije je opisan v dodatku 11. Obsega naslednje stavke:

TCS_354 Neposredno pred ukazom EXTERNAL_AUTHENTICATE mora biti izveden ukaz GET_CHALLENGE. Kartica pošlje poziv v okolje (RND3).

TCS_355 Preverjanje kriptograma uporablja RND3 (poziv, ki ga pošlje kartica), zasebni ključ kartice (implicitno izbran) in javni ključ, pred tem izbran z ukazom MSE.

TCS_356 Kartica preveri kriptogram; če je pravilen, odobri pogoj dostopa AUT.

TCS_357 Vhodni kriptogram nosi drugi element za dogovor o ključu seje K2.

TCS_358 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (javni ključ, ki naj se uporabi, je implicitno znan in ga je pred tem nastavil ukaz MSE)
Lc	1	'80h'	Lc (dolžina podatkov poslanih kartici)
#6-#133	128	'XX..XXh'	Kriptogram (glej dodatek 11)

TCS_359 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če v varnem okolju ni prisoten noben javni ključ, se vrne stanje '6A88',
- če CHA trenutno nastavljenega javnega ključa ni podaljšek AID tahografske aplikacije in tipa opreme VU, se vrne stanje obdelave '6F00' (glej dodatek 11),
- če v varnem okolju ni prisoten noben zasebni ključ, se vrne stanje '6A88',
- če ne uspe preverjanje kriptograma, se vrne stanje obdelave '6688',
- če neposredno pred tem ukazom ni bil poslan ukaz GET CHALLENGE, se vrne stanje obdelave '6985',
- če izbrani zasebni ključ velja za pokvarjenega, je vrnjeno stanje obdelave '6400' ali '6581'.

TCS_360 Če je ukaz EXTERNAL AUTHENTICATE uspešen, in če je na podlagi uspešnega ukaza INTERNAL AUTHENTICATE na voljo prvi del ključa seje, se za nadaljnjo uporabo pri ukazih varnega sporočanja nastavi ključ seje.

TCS_361 Če iz prej izvedenega ukaza INTERNAL AUTHENTICATE ni na voljo prvega dela ključa seje, kartica ne shrani drugega dela ključa seje, ki ji ga pošlje IFD. Ta mehanizem zagotavlja, da se proces medsebojne avtentifikacije izvaja v zaporedju, predpisanem v dodatku 11.

3.6.10 Upravljanje varnega okolja (MSE)

Ta ukaz se uporablja za nastavitev javnega ključa za avtentifikacijo.

Ta ukaz je v skladu s standardom ISO/IEC 7816-8. Uporaba ukaza pa je v primerjavi s tem standardom omejena.

TCS_362 Ključ, naveden v podatkovnem polju MSE, velja za vse datoteke tahografske DF.

TCS_363 Ključ, naveden v podatkovnem polju MSE, ostane trenutno izbrani javni ključ do naslednjega ukaza MSE.

TCS_364 Če navedeni javni ključ (še) ni prisoten na kartici, ostane varno okolje nespremenjeno.

TCS_365 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: navedeni ključ veljaven za vse kriptografske postopke
P2	1	'B6h'	P2 (navedeni podatki nanašajoči se na digitalni podpis)
Lc	1	'0Ah'	Lc: dolžina podatkovnega polja v nadaljevanju
#6	1	'83h'	Značka za navajanje javnega ključa v asimetričnih primerih
#7	1	'08h'	Dolžina navedbe ključa (identifikatorja ključa)
#8-#15	08h	'XX..XXh'	Identifikator ključa, predpisan v dodatku 11

TCS_366 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- če je ukaz uspešen, kartica vrne '9000',
- če v varnem okolju ni prisoten navedeni ključ, se vrne stanje obdelave '6A88',
- če nekateri pričakovani podatkovni objekti manjkajo v formatu varnega sporočanja, je vrnjeno stanje obdelave '6987'. To se lahko zgodi, če manjka značka '83h',
- če so napačni nekateri podatkovni objekti, se vrne stanje obdelave '6988'. To se lahko zgodi, če dolžina identifikatorja ključa ni '08h',
- če izbrani ključ velja za pokvarjenega, je vrnjeno stanje obdelave '6400' ali '6581'.

3.6.11 **PSO: HASH**

Ta ukaz se uporablja za prenos rezultatov izračunov razpršitve določenih podatkov na kartico. Ukaz se uporablja za preverjanje digitalnih podpisov. Vrednost razpršitve se shrani v EEPROM za naslednji ukaz preverjanja digitalnega podpisa.

Ta ukaz je v skladu s standardom ISO/IEC 7816-8. Uporaba ukaza pa je v primerjavi s tem standardom omejena.

TCS_367 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Izvedba varnostne operacije
P1	1	'90h'	Vrnitev kode razpršitve
P2	1	'A0h'	Značka: podatkovno polje vsebuje DO, pomembne za razpršitev
Lc	1	'16h'	Dolžina Lc polja podatkov v nadaljevanju
#6	1	'90h'	Značka kode razpršitve
#7	1	'14h'	Dolžina kode razpršitve
#8-#27	20	'XX..XXh'	Koda razpršitve

TCS_368 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če nekateri pričakovani podatkovni objekti (predpisani zgoraj) manjkajo, je vrnjeno stanje obdelave '6987'. To se lahko zgodi, če manjka značka '90h',
- če so napačni nekateri podatkovni objekti, se vrne stanje obdelave '6988'. Ta napaka se zgodi, če je zahtevana značka prisotna, njena dolžina pa je različna od '14h'.

3.6.12 **Razpršitev datoteke fik**

Ta ukaz ni v skladu z ISO/IEC 7816-8. Tako bajt CLA tega ukaza kaže, da gre za lastno uporabo ukaza PERFORM SECURITY OPERATION/HASH.

TCS_369 Ukaz razpršitve datoteke se uporablja za razpršitev podatkovnega območja trenutno izbrane transparentne EF.

TCS_370 Rezultat postopka razpršitve se shrani na kartici. Nato se lahko uporablja za pridobitev digitalnega podpisa iz datoteke z ukazom PSO-COMPUTE_DIGITAL_SIGNATURE. Ta rezultat ostane na voljo za ukaz COMPUTE DIGITAL SIGNATURE do naslednjega uspešno izvedenega ukaza PERFORM HASH ali FILE.

TCS_371 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'80h'	CLA
INS	1	'2Ah'	Izvedba varnostne operacije
P1	1	'90h'	Značka: razpršitev
P2	1	'00h'	P2: razpršitev podatkov trenutno izbrane transparentne datoteke

TCS_372 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če ni izbrana nobena aplikacija, je vrnjeno stanje obdelave '6985',
- če velja izbrana EF za pokvarjeno (ugotovljena napaka celovitosti v atributih datoteke ali shranjenih podatkih), je vrnjeno stanje obdelave '6400' ali '6581',
- če izbrana datoteka ni transparentna, se vrne stanje obdelave '6986'.

3.6.13 PSO: izračun digitalnega podpisa

Ta ukaz se uporablja za izračun digitalnega podpisa iz prej izračunane kode razpršitve (glej točko 3.6.12, PERFORM HASH of FILE).

Ta ukaz je v skladu s standardom ISO/IEC 7816-8. Uporaba ukaza pa je v primerjavi s tem standardom omejena.

TCS_373 Za izračun digitalnega podpisa se uporablja zasebni ključ kartice, ki ga kartica implicitno pozna.

TCS_374 Kartica izdela digitalni podpis z metodo šifriranja, v skladu s PKCS1 (podrobnosti so opisane v dodatku 11).

TCS_375 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Izvedba varnostne operacije
P1	1	'9Eh'	Digitalni podpis, ki ga je treba vrniti
P2	1	'9Ah'	Značka: podatkovno polje vsebuje podatke, ki jih je treba podpisati. Ker ni vključeno nikakršno podatkovno polje, se predpostavlja, da so podatki že na kartici (razpršitev datoteke).
Le	1	'80h'	Dolžina pričakovanega podpisa

TCS_376 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
#1-#128	128	'XX..XXh'	Podpis prej izračunane razpršitve
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če implicitno izbrani zasebni ključ velja za pokvarjenega, je vrnjeno stanje obdelave '6400' ali '6581'.

3.6.14 PSO: preverjanje digitalnega podpisa

Ta ukaz služi za preverjanje digitalnega podpisa, ki je podan v vhodnih podatkih, v skladu s PKCS1 sporočila, katerega razpršitev kartica pozna. Kartica implicitno pozna algoritem podpisa.

Ta ukaz je v skladu s standardom ISO/IEC 7816-8. Uporaba ukaza pa je v primerjavi s tem standardom omejena.

TCS_377 Ukaz VERIFY DIGITAL SIGNATURE vedno uporablja javni ključ, ki je bil prej izbran z ukazom MSE, in prej izračunano kodo razpršitve, ki jo poda ukaz PSO: HASH.

TCS_378 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Izvedba varnostne operacije
P1	1	'00h'	Značka: podatkovno polje vsebuje DO, pomembne za preverjanje
P2	1	'A8h'	
Lc	1	'83h'	Dolžina Lc polja podatkov v nadaljevanju
#28	1	'9Eh'	Značka za digitalni podpis
#29-#30	2	'8180h'	Dolžina digitalnega podpisa (128 bajtov, kodiranih po ISO/IEC 7816-6)
#31-#158	128	'XX.XXh'	Vsebina digitalnega podpisa

TCS_379 Sporočilo odgovora

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Statusni besedi (SW1, SW2)

- Če je ukaz uspešen, kartica vrne '9000',
- če preverjanje podpisa ne uspe, se vrne stanje obdelave '6688'. Proces preverjanja je opisan v dodatku 11,
- če ni izbran noben javni ključ, je vrnjeno stanje obdelave '6A88',
- če nekateri pričakovani podatkovni objekti (predpisani zgoraj) manjkajo, je vrnjeno stanje obdelave '6987'. To se lahko zgodi, če manjka katera od zahtevanih značk,
- če za obdelavo ukaza ni na voljo nobene kode razpršitve (rezultata prej izvedenega ukaza PSO: HASH), se vrne stanje obdelave '6985',
- če so napačni nekateri podatkovni objekti, se vrne stanje obdelave '6988'. To se lahko zgodi, če je nepravilna katera od dolžin zahtevanih podatkovnih objektov,
- če izbrani javni ključ velja za pokvarjenega, je vrnjeno stanje obdelave '6400' ali '6581'.

4. STRUKTURA TAHOGRAFSKIH KARTIC

Ta točka predpisuje strukture datotek tahografskih kartic za shranjevanje dosegljivih podatkov.

Ne predpisuje notranjih struktur, ki jih določajo proizvajalci, npr. glav datotek, niti shranjevanja in ravnanja s podatkovnimi elementi potrebnimi samo za interno rabo, npr. `EuropeanPublicKey`, `CardPrivateKey`, `TDesSessionKey` ali `WorkshopCardPin`.

Uporabna zmogljivost pomnilnika tahografske kartice mora biti najmanj 11 kilobajtov. Uporabljajo se lahko tudi kartice z večjimi pomnilniki. V takih primerih ostane struktura kartice enaka, večja pa so števila zapisov določenih elementov strukture. Ta točka predpisuje najmanjše in največje vrednosti števil teh zapisov.

4.1 Struktura voznikove kartice

TCS_400 Po personalizaciji mora imeti voznikova kartica naslednjo strukturo trajnih datotek in naslednje pogoje dostopa do datotek:

File	File ID	Access conditions		
		Read	Update	Encrypted
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	ALW	NEV	No
EF Card_Download	050E	ALW	ALW	No
EF Driving_Licence_Info	0521	ALW	NEV	No
EF Events_Data	0502	ALW	PRO SM / AUT	No
EF Faults_Data	0503	ALW	PRO SM / AUT	No
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
EF Places	0506	ALW	PRO SM / AUT	No
EF Current_Usage	0507	ALW	PRO SM / AUT	No
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_401 Vse strukture EF morajo biti transparentne.

TCS_402 Pri vseh datotekah v okviru tahografske DF mora biti možno branje z varnim sporočanjem.

TCS_403 Voznikova kartica mora imeti naslednji podatkovno strukturo:

File/Data element	No of Records	Size (bytes)		Default Values
		Min	Max	
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 V naslednji tabeli so podane najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura voznikove kartice; te vrednosti so uporabljene za izračun velikosti v gornji tabeli:

		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	5 544 bajtov (28 dni * 93 sprememb dejavnosti)	13 776 bajtov (28 dan * 240 spre- memb dejavnosti)

4.2 Struktura delavniške kartice

TCS_405 Po personalizaciji mora imeti delavniška kartica naslednjo strukturo trajnih datotek in naslednje pogoje dostopa do datotek:

File	File ID	Access conditions		
		Read	Update	Encrypted
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	ALW	NEV	No
EF Card_Download	0509	ALW	ALW	No
EF Calibration	050A	ALW	PRO SM / AUT	No
EF Sensor_Installation_Data	050B	ALW	NEV	Yes
EF Events_Data	0502	ALW	PRO SM / AUT	No
EF Faults_Data	0503	ALW	PRO SM / AUT	No
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
EF Places	0506	ALW	PRO SM / AUT	No
EF Current_Usage	0507	ALW	PRO SM / AUT	No
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_406 Vse strukture EF morajo biti transparentne.

TCS_407 Pri vseh datotekah v okviru tahografske DF mora biti možno branje z varnim sporočanjem.

TCS_408 Delavniška kartica mora imeti naslednji podatkovno strukturo:

File/Data element	No of Records	Size (Bytes)		Default Values
		Min	Max	
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
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 V naslednji tabeli so podane najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura delavniške kartice; te vrednosti so uporabljene za izračun velikosti v gornji tabeli:

		Min	Max
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 bajtov (1 dan * 93 sprememb dejavnosti)	492 bajtov (1 dan * 240 sprememb dejavnosti)

4.3 Struktura kontrolne kartice

TCS_410 Po personalizaciji mora imeti kontrolna kartica naslednjo strukturo trajnih datotek in naslednje pogoje dostopa do datotek:

File	File ID	Access conditions		
		Read	Update	Encrypted
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	AUT	NEV	No
EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	No

TCS_411 Vse strukture EF morajo biti transparentne.

TCS_412 Pri vseh datotekah v okviru tahografske DF mora biti možno branje z varnim sporočanjem.

TCS_413 Nadzorna kartica mora imeti naslednji podatkovno strukturo:

Archivo/Elemento de datos	No of Records	Size (Bytes)		Default Values
		Min	Max	
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 V naslednji tabeli so podane najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura nadzorne kartice; te vrednosti so uporabljene za izračun velikosti v gornji tabeli:

		Min	Maks.
n ₇	NoOfControlActivityRecords	230	520

4.4 A vállalkozás adatkártyájának Struktúra kartice podjetja

TCS_415 Po personalizaciji mora imeti kartica podjetja naslednjo strukturo trajnih datotek in naslednje pogoje dostopa do datotek:

File	File ID	Access conditions		
		Read	Update	Encrypted
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	AUT	NEV	No
EF Company_Activity_Data	050D	ALW	PRO SM / AUT	No

TCS_416 Vse strukture EF morajo biti transparentne.

TCS_417 Pri vseh datotekah v okviru tahografske DF mora biti možno branje z varnim sporočanjem.

TCS_418 Kartica podjetja mora imeti naslednji podatkovno strukturo:

File/Data element	No of Records	Size (bytes)		Default Values
		Min	Max	
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 V naslednji tabeli so podane najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura kartice podjetja; te vrednosti so uporabljene za izračun velikosti v gornji tabeli:

		Min	Maks.
n8	NoOfCompanyActivityRecords	230	520

*Dodatek 3***PIKTOGRAMI**

PIC_001 Zapisovalna naprava lahko uporablja naslednje piktogramе in kombinacije piktogramov:

1. OSNOVNI PIKTOGRAMI

	Ljudje	Dejanja	Režimi delovanja
	Podjetje		Režim dela v podjetju
	Nadzornik	Nadzor	Nadzorni režim
	Voznik	Voznik	Delovni režim
	Delavnica/preizkusna postaja	Pregled/kalibriranje	Režim kalibriranja
	Gyártó		

	Dejavnosti	Trajanje
	Razpoložljivost	Tekoče obdobje razpoložljivosti
	Vožnja	Čas neprekinjene vožnje
	Počitek	Tekoče obdobje počitka
	Delo	Tekoče obdobje dela
	Odmor	Skupni čas odmorov
	Neznana	

	Oprema	Funkcije
	Voznikova reža	
	Sovoznikova reža	
	Kartica	
	Ura	
	Prikaz	Prikazovanje
	Zunanji pomnilnik	Prenos podatkov
	Napajalnik	
	Tiskalnik/izpis	Tiskanje
	Zaznavalo	
	Velikost avtoplaščev	
	Vozilo/enota v vozilu	

	Posebna stanja
	Zunaj področja veljavnosti
	VOŽNJA S TRAJEKTOM/VLAKOM

	Razno		
	Dogodki		Napake
	Začetek dnevne delovne izmene		Konec dnevne delovne izmene
	Kraj		Ročni vnos voznikovih dejavnosti
	Varnost		Hitrost
	Čas		Skupaj/vsota

	Kvalifikatorji
	Dnevno
	Tedensko
	Dva tedna
	Od ali do

2. KOMBINACIJE PIKTOGRAMOV

	Razno		
	Kraj nadzora		Kraj konca dnevne delovne izmene
	Kraj začetka dnevne delovne izmene		Do časa
	Od časa		
	Od vozila		
	Začetek stanja zunaj območja veljavnosti		Konec stanja zunaj območja veljavnosti

Kartice

	Voznikova kartica
	Kartica podjetja
	Nadzorna kartica
	Delavniška kartica
	Ni kartice

Vožnja

	Vožnja s posadko
	Čas vožnje v enem tednu
	Čas vožnje v dveh tednih

Izpisi

24h	Dnevni izpis vozniških dejavnosti s kartice
24h	Dnevni izpis vozniških dejavnosti iz VU
	Izpis dogodkov in napak s kartice
	Izpis dogodkov in napak iz VU
	Izpis tehničnih podatkov
	Izpis prekoračitev hitrosti

Dogodki

	Vstavev neveljavne kartice
	Navzkrižje med karticama
	Časovno prekrivanje
	Vožnja brez ustrezne kartice
	Vstavev kartice med vožnjo
	Zadnja seja s kartico nepravilno zaključena
	Prekoračitev hitrosti
	Prekinitev napajanja
	Napaka v podatkih gibanja
	Kršitev varnosti
	Nastavitev časa (v delavnici)
	Nadzor prekoračitev hitrosti

Napake

	Napaka kartice (voznikova reža)
	Napaka kartice (sovoznikova reža)
	Napaka na prikazu
	Napaka pri prenosu podatkov
	Napaka na tiskalniku
	Napaka na zaznavalu
	Interna napaka VU

Postopek ročnega vnosa

	Še vedno ista dnevna delovna izmena?
	Konec prejšnje delovne izmene?
	Potrdite ali vnesite kraj konca delovne izmene
	Vnesite čas začetka
	Vnesite kraj začetka delovne izmene

Opomba: Dodatne kombinacije piktogramov za oblikovanje blokov izpisa ali identifikatorjev zapisov so opredeljene v dodatku 4.]

Dodatek 4

IZPISI

VSEBINA

1.	Splošno	409
2.	Predpisi blokov podatkov	409
3.	Predpisi izpisov	415
3.1	Dnevni izpis voznikovih dejavnosti s kartice	416
3.2	Dnevni izpis voznikovih dejavnosti iz VU	416
3.3	Izpis dogodkov in napak s kartice	417
3.4	Izpis dogodkov in napak iz VU	417
3.5	Izpis tehničnih podatkov	418
3.6	Izpis prekoračenj hitrosti	418

📅 dd/mm/yyyy hh:mm (UTC)

2. **Vrsta izpisa**

Identifikator bloka
Kombinacija piktogramov izpisa (glej dodatek 3), nastavitve naprave za omejevanje hitrosti (samo pri izpisu prekoračitev hitrosti).

Picto xxx km/h

3. **Identifikacija imetnika kartice**

Identifikator bloka P = piktogram 'Ljudje'
Priimek imetnika kartice
Ime(na) imetnika kartice (če so shranjena)
Identifikacija kartice
Datum poteka veljavnosti (če je določen)
Če kartica ni izdana osebi, ali če priimek imetnika ni zapisan, se namesto priimka natisne ime delavnice ali nadzornega organa.

-----P-----
P Last_Name _____
First_Name _____
Card_Identification _____
dd/mm/yyyy

4. **Identifikacija vozila**

Identifikator bloka
(VIN)
Registrska številka vozila in država, v kateri je registrirano

-----A-----
A VIN _____
Nat/VRN _____

5. **Identifikacija VU**

Identifikator bloka
Ime proizvajalca VU
Kataloška številka VU.

-----B-----
B VU_Manufacturer _____
VU_Part_Number _____

6. **Zadnje kalibriranje zapisovalne naprave**

Identifikator bloka
Ime delavnice
Identifikacija delavniške kartice
Datum kalibriranja

-----T-----
T Last_Name _____
Card_Identification _____
T dd/mm/yyyy

7. **Zadnji nadzor (s strani nadzornega referenta)**

Identifikator bloka
Identifikacija nadzornikove kartice
Datum, čas in tip nadzora
###Tip kontrole: Do štirje piktogrami. Tip kontrole je lahko (kombinacija) naslednji(h):
■: Q: prenos podatkov s kartice, T: ^: prenos podatkov z VU, P: ELψ: TMizpis, □: fi: prikaz.

-----B-----
Card_Identification _____
B dd/mm/yyyy hh:mm pppp

8. **Voznikove dejavnosti, shranjene na kartici, v vrstnem redu, v kakršnem so potekale**

Identifikator bloka
Datum, za katerega je zahtevan izpis (koledarski dan) + dnevni števec prisotnosti kartice

-----B-----
dd/mm/yyyy xxx

8.1 *Obdobje, v katerem kartica ni bila vstavljena*

8.1a Identifikator bloka (začetek obdobja)

8.1b Neznano obdobje. Čas začetka in konca, trajanje

8.1c Ročno vnesena dejavnost

Piktogram dejavnosti, čas začetka in konca (vključno), trajanje, obdobja počitka dolžine vsaj ene ure so označena z zvezdico.

? hh:mm hh:mm hh:mm
A hh:mm hh:mm hh:mm *

- 8.2 *Vstavitev kartice v režo S*
 Identifikator bloka, S = piktogram reže
 VRN in država registracije vozila
 Stanje števca prevožene poti ob vstavitvi kartice.
- 8.3 *A Dejavnost (pri vstavljeni kartici)*
 Piktogram dejavnosti, čas začetka in konca (vključno), trajanje, stanje posadke (piktogram posadke, če je stanje POSADKA, prazno, če je stanje POSAMEZNIK), obdobja počitka dolžine vsaj ene ure so označena z zvezdico.
- 8.3a *Posebno stanje*
 Čas vnosa, piktogram posebnega stanja (ali kombinacija piktogramov).
- 8.4 *Izvek kartice*
 Stanje števca prevožene poti in razdalja, prevožena od zadnje vstavitve, za katero je znano stanje števca prevožene poti.
9. **Voznikove aktivnosti iz VU po režah v časovnem vrstnem redu**
 Identifikator bloka
 Datum, za katerega je zahtevan izpis (koledarski dan)
 Stanje števca prevožene poti ob 00:00 in 24:00.
10. **Dejavnosti pri kartici v reži S**
 Identifikator bloka
- 10.1 *Obdobje, v katerem v reži S ni bila vstavljena nobena kartica*
 Identifikator zapisa
 Ni vstavljena nobena kartica
 Stanje števca prevožene poti ob začetku obdobja.
- 10.2 *Vstavitev kartice*
 Identifikator zapisa vstavitve kartice
 Priimek voznika
 Ime voznika
 Identifikacija voznikove kartice
 Datum izteka veljavnosti voznikove kartice
 VRN in država registracije prej uporabljanega vozila
 Datum in čas izvleka kartice iz prej uporabljanega vozila
 Prazna vrstica
 Stanje števca ob vstavitvi kartice, značka ročnega vnosa voznikovih dejavnosti (M: da, prazno: ne).
- 10.3 *Dejavnost*
 Piktogram dejavnosti, čas začetka in konca (vključno), trajanje, stanje posadke (piktogram posadke, če je stanje POSADKA, prazno, če je stanje POSAMEZNIK), obdobja počitka dolžine vsaj ene ure so označena z zvezdico.

-----S-----
 A Nat/VRN _____
 x xxx xxx km

A hh:mm hh:mm hh:mm *
 * *

hh:mm ----- pppp -----

x xxx xxx km; x xxx km

 dd/mm/yyyy
 x xxx xxx - x xxx xxx km

----- S -----

 * * ---
 x xxx xxx km

 Last_Name _____
 First_Name _____
 Card_Identification _____
 dd/mm/yyyy
 A + Nat/VRN _____
 dd/mm/yyyy hh:mm
 x xxx xxx km M

A hh:mm hh:mm hh:mm *
 * *

10.3a	<i>Posebno stanje</i> Čas vnosa, piktogram posebnega stanja (ali kombinacija piktogramov).	hh:mm ----- pppp -----
10.4	<i>Izvlek kartice ali konec stanja ,brez kartice'</i> Stanje števca prevožene poti ob izvleku kartice ali koncu obdobja ,brez kartice' in razdalja, prevožena od vstavitve ali od začetka obdobja ,brez kartice'.	x xxx xxx km; x xxx km
11.	Dnevni povzetek Identifikator bloka	----- Σ -----
11.1	<i>Povzetek obdobj brez kartice v voznikovi reži iz VU</i> Identifikator bloka	100 ---
11.2	<i>Povzetek obdobj brez kartice v sovoznikovi reži iz VU</i> Identifikator bloka	200 ---
11.3	<i>Dnevni povzetek za voznika iz VU</i> Identifikator zapisa Priimek voznika Ime voznika Identifikacija voznikove kartice	----- Ⓜ Last_Name _____ First_Name _____ Card_Identification _____
11.4	<i>Vnos kraja, v katerem se dnevna delovna izmena začne in/ali konča</i> pi = piktogram kraja začetka/konca, čas, država, regija, stanje števca prevožene poti	pihh:mm Cou Reg x xxx xxx km
11.5	<i>Skupne vrednosti po dejavnostih (s kartice)</i> Skupni čas vožnje, prevožena razdalja Skupno trajanje dela in razpoložljivosti Skupno trajanje počitka in neznanih dejavnosti Skupno trajanje dejavnosti posadke.	Ⓜ hhhmm x xxx km ✱ hhhmm Ⓜ hhhmm ┌ hhhmm ? hhhmm ⓂⓂ hhhmm
11.6	<i>Skupne vrednosti po dejavnostih (obdobja brez kartice v voznikovi reži)</i> Skupni čas vožnje, prevožena razdalja Skupno trajanje dela in razpoložljivosti Skupno trajanje počitka.	Ⓜ hhhmm x xxx km ✱ hhhmm Ⓜ hhhmm ┌ hhhmm
11.7	<i>Skupne vrednosti po dejavnostih (obdobja brez kartice v sovoznikovi reži)</i> Skupno trajanje dela in razpoložljivosti Skupno trajanje počitka.	✱ hhhmm Ⓜ hhhmm ┌ hhhmm

- 11.8 *Skupne vrednosti po dejavnostih (za vznika, upoštevani obe reži)*
 Skupni čas vožnje, prevožena razdalja
 Skupni čas vožnje, prevožena razdalja
 Skupno trajanje počitka
 Skupno trajanje dejavnosti posadke
 Če je zahtevan izpis za tekoči dan, se dnevni povzetek izračuna iz podatkov, ki so na voljo ob času izpisa.

⊗ hh:mm x xxx km
 ✕ hh:mm ⊗ hh:mm
 ⌂ hh:mm
 ⊗⊗ hh:mm

12. Dogodki in/ali napake, shranjeni na kartici

- 12.1 Identifikator bloka 5 zadnjih ‚dogodkov in napak‘ s kartice

----- ! ✕ ⊗ -----

- 12.2 Identifikator bloka vseh zapisanih ‚dogodkov‘ na kartici

----- ! ⊗ -----

- 12.3 Identifikator bloka vseh zapisanih ‚napak‘ na kartici

----- ✕ ⊗ -----

- 12.4 *Zapis dogodka in/ali napake*
 Identifikator zapisa
 Piktogram dogodka/napake, namen zapisa, datum in čas začetka
 Koda dodatnega dogodka/napake (če obstaja), trajanje
 Država registracije in VRN vozila, na katerem se je dogodek ali napaka zgodil(a).

 Pic dd/mm/yyyy hh:mm
 ! xxx hh:mm
 ⌂ Nat/VRN _____

13. Dogodki in/ali napake, shranjeni na VU ali tekoči

- 13.1 Identifikator bloka 5 zadnjih ‚dogodkov in napak‘ iz VU

----- ! ✕ ⌂ -----

- 13.2 Identifikator bloka vseh zapisanih ali tekočih ‚dogodkov‘ v VU

----- ! ⌂ -----

- 13.3 Identifikator bloka vseh zapisanih ali tekočih ‚napak‘ v VU

----- ✕ ⌂ -----

- 13.4 *Zapis dogodka in/ali napake*
 Identifikator zapisa
 Piktogram dogodka/napake, namen zapisa, datum in čas začetka
 Koda dodatnega dogodka/napake (če obstaja), število podobnih dogodkov na ta dan, trajanje
 Identifikacija kartic, vstavljenih ob začetku ali ob koncu dogodka ali napake (do 4 vrstice, brez ponavljanja istih števil kartic)
 Primer, ko ni bila vstavljena nobena kartica
 Namen zapisa (p) je številska koda, ki pojasnjuje, čemu je bil dogodek ali napaka zapisan(a); kodiranje je v skladu z opredelitvijo podatkovnega elementa *EventFaultRecordPurpose*.

 Pic (p) dd/mm/yyyy hh:mm
 ! xxx (xxx) hh:mm
 Card_Identification _____
 Card_Identification _____
 Card_Identification _____
 Card_Identification _____
 ⊗ ---

14. **Identifikacija VU**

Identifikator bloka
 Ime proizvajalca VU
 Naslov proizvajalca VU
 Kataloška številka VU
 Številka odobritve VU
 Serijska številka VU
 Leto izdelave VU
 Verzija in datum namestitve programske opreme VU.

-----B-----
 B Name _____
 Address _____
 PartNumber _____
 Apprv _____
 S/N _____
 yyyy
 V xx.xx.xx dd/mm/yyyy

15. **Identifikacija zaznavala**

Identifikator bloka
 Serijska številka zaznavala
 Številka odobritve zaznavala
 Datum prve namestitve zaznavala.

-----L-----
 L S/N _____
 Apprv _____
 dd/mm/yyyy

16. **Kalibracijski podatki**

Identifikator bloka

-----T-----

16.1 *Zapis kalibriranja*

Identifikator zapisa
 Delavnica, ki je opravila kalibriranje
 Naslov delavnice
 Identifikacija delavniške kartice
 Datum izteka veljavnosti delavniške kartice
 Prazna vrstica
 Datum kalibriranja + namen kalibriranja
 VIN
 Registrska številka vozila in država, v kateri je registrirano
 Značilni koeficient vozila
 Konstanta zapisovalne naprave
 Efektivni obseg avtoplaščev
 Velikost nameščenih avtoplaščev
 Nastavitev naprave za omejevanje hitrosti
 Staro in novo stanje števca prevožene poti
 Namen kalibriranja (p) je številski koda, ki pojasnjuje, čemu so bili ti kalibracijski parametri zapisani; kodiranje je v skladu z opredelitvijo podatkovnega elementa CalibrationPurpose.

 T Workshop_name _____
 Workshop_address _____
 Card-Identification _____
 dd/mm/yyyy
 T dd/mm/yyyy (p)
 A VIN _____
 Nat/VRN _____
 w xx xxx Imp/km
 k xx xxx Imp/km
 l xx xxx mm
 o TyreSize _____
 > xxx km/h
 x xxx xxx - x xxx xxx km

17. **Nastavljanje časa**

Identifikator bloka

-----C-----

17.1 *Zapis nastavljanja časa*

Identifikator zapisa
 Stari datum in čas
 Novi datum in čas
 Delavnica, ki je opravila nastavljanje časa
 Naslov delavnice
 Identifikacija delavniške kartice
 Datum izteka veljavnosti delavniške kartice.

 ! C dd/mm/yyyy hh:mm
 C dd/mm/yyyy hh:mm
 T Workshop_name _____
 Workshop_address _____
 Card_Identification _____
 dd/mm/yyyy

18. **Najnovejši dogodek in napaka, zapisana v VU**

Identifikator bloka

Datum in čas najnovejšega dogodka

Datum in čas najnovejše napake.

```

----- ! x A -----
!  jj/mm/aaaa  hh:mm
x  jj/mm/aaaa  hh:mm

```

19. **Informacije o nadzoru prekoračitev hitrosti**

Identifikator bloka

Datum in čas zadnjega NADZORA PREKORAČITVE HITROSTI

Datum/čas prve prekoračitve hitrosti in število dogodkov prekoračitve hitrosti od takrat.

```

----- >> -----
> d dd/mm/yyyy  hh:mm
>> dd/mm/yyyy  hh:mm (nnn)

```

20. **Zapis prekoračitve hitrosti**

20.1 Identifikator bloka ,prva prekoračitev hitrosti po zadnjem kalibriranju'

```

----- >> T -----

```

20.2 Identifikator bloka ,5 najresnejših dogodkov v zadnjih 365 dneh'

```

----- >> (365) -----

```

20.3 Identifikator bloka ,najresnejši dogodek na enega od 10 zadnjih dni nastopov dogodkov'

```

----- >> (10) -----

```

20.4 Identifikator zapisa

Datum, čas in trajanje

Največja in povprečna hitrost, število podobnih dogodkov na ta dan

Priimek voznika

Ime voznika

Identifikacija voznikove kartice

```

-----
>> dd/mm/yyyy hh:mm hh:mm
xxx km/h xxx km/h (xxx)
@ Last_Name _____
First_Name _____
Card_Identification _____

```

20.5 Če v bloku ni nobenega zapisa prekoračitve hitrosti.

```

>> - - -

```

21. **Ročno vpisani podatki**

Identifikator bloka

21.1 Kraj nadzora

21.2 Podpis nadzornika

21.3 Od časa

21.4 Do časa

21.5 Podpis voznika

```

-----
@ + .....
@ .....
@ + .....
+ @ .....
@ .....

```

,Ročno vpisani podatki'. V izpisu mora biti dovolj praznega prostora, da je zahtevane podatke ali podpis mogoče vpisati.

3. **PREDPISI IZPISOV**

V tem poglavju se uporabljajo naslednji dogovori o zapisovanju:

N
N
X/Y

Številka izpisa ali zapisa N

Številka izpisa ali zapisa N, ponovljena, kolikorkrat je potrebno

Izpis ustreznega bloka ali zapisa X in/ali Y, ponovljen, kolikorkrat je potrebno

3.1 Dnevni izpis voznikovih dejavnosti s kartice

PRT_007 Dnevni izpis voznikovih dejavnosti s kartice mora biti v skladu z naslednjo obliko:

1	Datum in čas tiskanja dokumenta
2	Vrsta izpisa
3	Identifikacija nadzornika (če je v VU vstavljena nadzorna kartica)
3	Identifikacija voznika (iz kartice, iz katere teče izpis)
4	Identifikacija vozila (vozilo, na katerem teče izpis)
5	Identifikacija VU (VU, na kateri teče izpis)
6	Zadnje kalibriranje te VU
7	Zadnji nadzorvoznika, ki ga nadzorujemo
8	Ločilo voznikovih dejavnosti
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Voznikove dejavnosti v vrstnem redu, v kakršnem so potekale
11	Ločilo dnevnega povzetka
11.4	Vneseni kraji v časovnem zaporedju
11.5	Skupne vrednosti dejavnosti
12.1	Ločilo dogodkov ali napak s kartice
12.4	Zapisi dogodkov/napak (zadnjih 5 dogodkov ali napak, shranjenih na kartici)
13.1	Ločilo dogodkov ali napak iz VU
13.4	Zapisi dogodkov/napak (zadnjih 5 dogodkov ali napak, shranjenih ali tekočih v VU)
21.1	Kraj nadzora
21.2	Podpis nadzornika
21.5	Podpis voznika

3.2 Dnevni izpis voznikovih dejavnosti iz VU

PRT_008 Dnevni izpis voznikovih dejavnosti iz VU mora biti v skladu z naslednjo obliko:

1	Datum in čas tiskanja dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice vstavljene v VU)
4	Identifikacija vozila (vozilo, na katerem teče izpis)
5	Identifikacija VU (VU, na kateri teče izpis)
6	Zadnje kalibriranje te VU
7	Zadnji nadzor na tej zapisovalni napravi
9	Ločilo voznikovih dejavnosti
10	Ločilo voznikove reže (reže 1)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Dejavnosti v časovnem zaporedju (voznikova reža)
10	Ločilo sovoznikove reže (reže 2)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Dejavnosti v časovnem zaporedju (sovoznikova reža)
11	Ločilo dnevnega povzetka
11.1	Povzetek obdobja brez kartice v voznikovi reži
11.4	Vneseni kraji v časovnem zaporedju
11.6	Skupne vrednosti dejavnosti

11.2	Povzetek obdobj brez kartice v voznikovi reži	
11.4	Vneseni kraji v časovnem zaporedju	
11.7	Skupne vrednosti dejavnosti	
11.3	Skupne vrednosti po dejavnostih (za voznika, upoštevani obe reži)	
11.4	Kraji, ki jih je vnesel ta voznik, v časovnem zaporedju	
11.7	Skupne vrednosti po dejavnostih za tega voznika	
13.1	Ločilo dogodkov in napak	
13.4	Zapisi dogodkov/napak (zadnjih 5 dogodkov ali napak, shranjenih ali tekočih v VU)	
21.1	Kraj nadzora	
21.2	###Podpis nadzornika	
21.3	Od časa	Prostor, na katerem lahko voznik brez kartice označi, katera obdobja se nanašajo nanj
21.4	Do časa	
21.5	Podpis voznika	

3.3 Izpis dogodkov in napak s kartice

PRT_009 Dnevni izpis dogodkov in napak s kartice mora biti v skladu z naslednjo obliko:

1	Datum in čas tiskanja dokumenta
2	Vrsta izpisa
3	Identifikacija nadzornika (če je v VU vstavljena nadzorna kartica)
3	Identifikacija voznika (iz kartice, iz katere teče izpis)
4	Identifikacija vozila (vozilo, na katerem teče izpis)
12.2	Ločilo dogodkov
12.4	Zapisi dogodkov (vsi dogodki, shranjeni na kartici)
12.3	Ločilo napak
12.4	Zapisi napak (vse napake, shranjene na kartici)
21.1	Kraj nadzora
21.2	Podpis nadzornika
21.5	Podpis voznika

3.4 Izpis dogodkov in napak iz VU

PRT_010 Dnevni izpis dogodkov in napak iz VU mora biti v skladu z naslednjo obliko:

1	Datum in čas tiskanja dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice vstavljene v VU)
4	Identifikacija vozila (vozilo, na katerem teče izpis)
13.2	Ločilo dogodkov
13.4	Zapisi dogodkov (vsi dogodki, shranjeni ali tekoči v VU)
13.3	Ločilo napak
13.4	Zapisi napak (vse napake, shranjene ali tekoče v VU)
21.1	Kraj nadzora
21.2	Podpis nadzornika
21.5	Podpis voznika

3.5 Izpis tehničnih podatkov

PRT_011 Izpis tehničnih podatkov mora biti v skladu z naslednjo obliko:

1	Datum in čas tiskanja dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice vstavljene v VU)
4	Identifikacija vozila (vozilo, na katerem teče izpis)
14	Identifikacija VU
15	Identifikacija zaznavala
16	Ločilo kalibracijskih podatkov
16.1	Zapisi kalibriranja (vsi razpoložljivi zapisi v časovnem zaporedju)
17	Ločilo nastavljanj časa
17.1	Zapisi nastavljanj časa (vsi razpoložljivi zapisi iz dejavnosti nastavljanja časa in dejavnosti kalibriranja)
18	Najnovejši dogodek in napaka, zapisana v VU

3.6 Izpis prekoračenj hitrosti

PRT_012 Izpis prekoračenj hitrosti mora biti v skladu z naslednjo obliko:

1	Datum in čas tiskanja dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice vstavljene v VU)
4	Identifikacija vozila (vozilo, na katerem teče izpis)
19	Informacije o nadzoru prekoračitev hitrosti
20.1	Identifikator podatkov prekoračitev hitrosti
20.4 / 20.5	Prva prekoračitev hitrosti po zadnjem kalibriranju
20.2	Identifikator podatkov prekoračitev hitrosti
20.4 / 20.5	5 najresnejših dogodkov prekoračitve hitrosti v zadnjih 365 dneh
20.3	Identifikator podatkov prekoračitev hitrosti
20.4 / 20.5	Najresnejši dogodek na vsakega od 10 zadnjih dni nastopov dogodkov
21.1	Kraj nadzora
21.2	Podpis nadzornika
21.5	Podpis voznika

Dodatek 5

PRIKAZI

V tem poglavju se uporabljajo naslednji dogovori o zapisovanju formatov:

- znaki natisnjeni krepko označujejo besedilo, ki se prikazuje tako, kakršno je (prikaz z normalnimi znaki),
- znaki v normalni pisavi označujejo spremenljivke (piktogrami ali podatke), ki se jih pri prikazu nadomesti z njihovimi vrednostmi:

dd mm yyyy: dan, mesec, leto,

hh: ure,

mm: minute,

D: piktogram trajanja

EF: kombinacija piktogramov dogodkov ali napak,

O: piktogram režima delovanja.

DIS_001 Zapisovalna naprava mora prikazovati podatke v naslednjih oblikah:

Podatki	Oblika
Privzeti prikaz	
Lokalni čas	hh:mm
Režim delovanja	O
Informacije nanašajoče se na voznika	1 Dhhmm hhmm
Informacije nanašajoče se na sovoznika	2 Dhhmm
Zunaj področja veljavnosti — začetek	OUT
Opozorilni prikaz	
Presežen čas neprekinjene vožnje	1 0hhmm hhmm
Dogodek ali napaka	EF
Drugi prikazi	
Datum in čas UTC	UTC 9 dd/mm/111 ali UTC 9 dd.mm.1111 hh:mm
Voznikov čas neprekinjene vožnje in skupni čas odmorov	1 0hhmm hhmm
Sovoznikov čas neprekinjene vožnje in skupni čas odmorov	2 0hhmm hhmm
Skupni čas vožnje voznika v prejšnjem in tekočem tednu	1 0 hhmm
Skupni čas vožnje sovoznika v prejšnjem in tekočem tednu	2 0 hhmm

*Dodatek 6***ZUNANJI VMESNIKI**

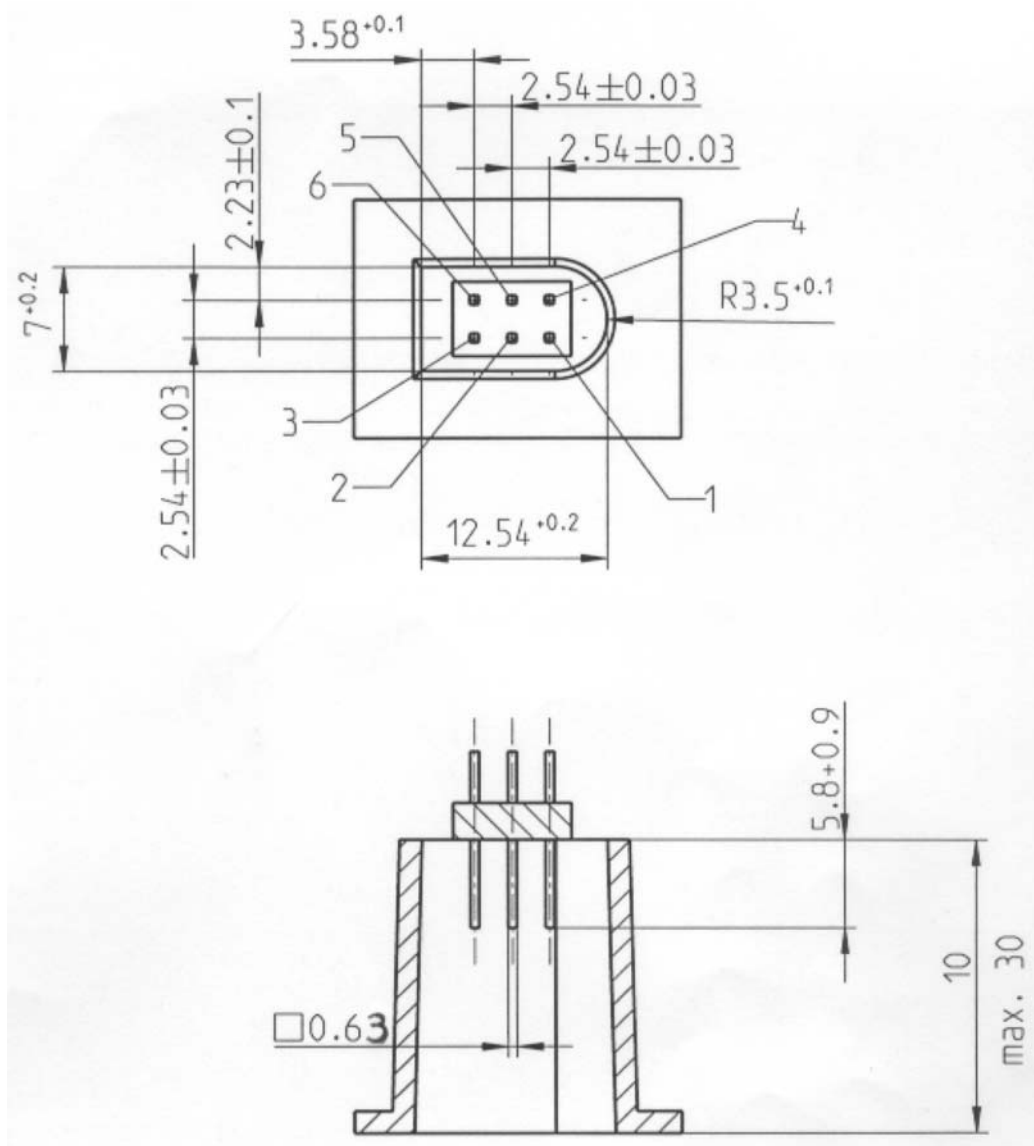
VSEBINA

1.	Strojna oprema	422
1.1	Konektor	422
1.2	Razporeditev kontaktov	424
1.3	Bločna shema	424
2.	Vmesnik za prenos podatkov	424
3.	Vmesnik za kalibriranje	425

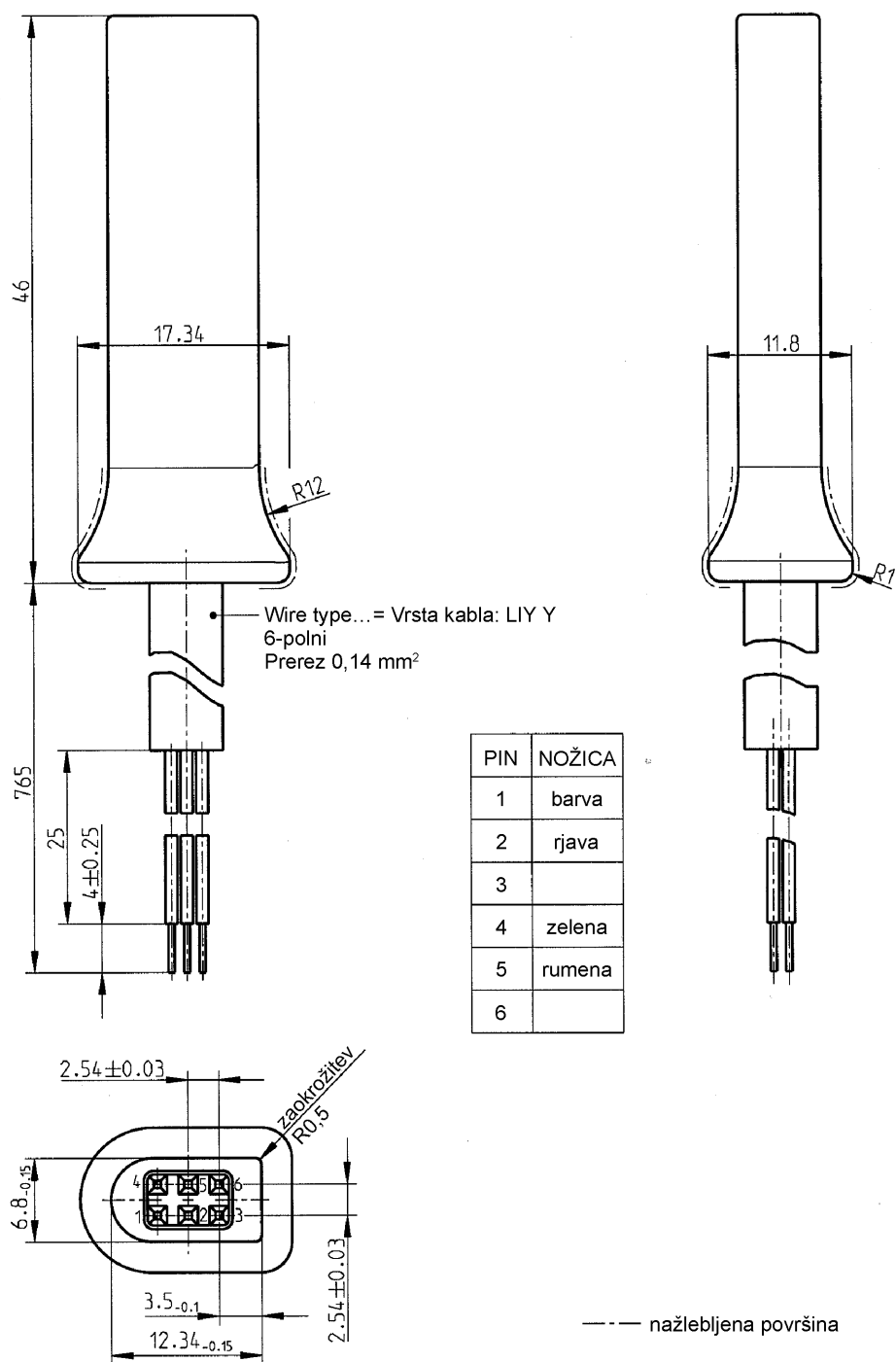
1. STROJNA OPREMA

1.1 Konektor

INT_001 Konektor za prenos podatkov/kalibriranje mora biti konektor s šestimi nožicami, dosegljiv na čelni plošči brez odklapanja katerega koli dela zapisovalne naprave, skladen z naslednjo risbo (vse mere podane v mm):



Naslednja shema kaže tipični ustrezni 6-polni vtikač:



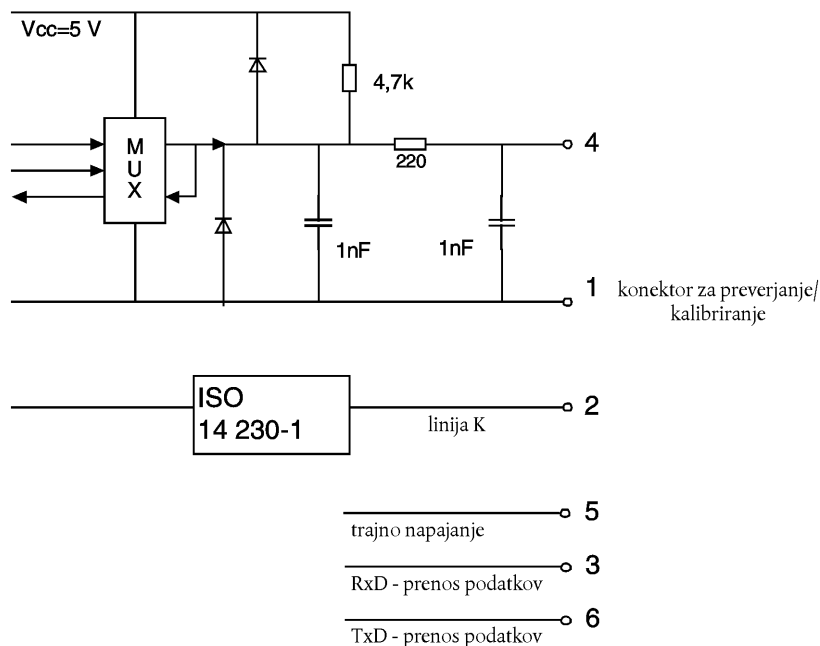
1.2 Razporeditev kontaktov

INT_002 Kontakti so razporejeni v skladu z naslednjo tabelo:

Nožica	Opis	Opomba
1	Akumulator — minus	Priključeno na negativni pol akumulatorja vozila
2	Podatkovna komunikacija	Linija K (po ISO 14 230-1)
3	RxD — prenos podatkov	Vhod podatkov v zapisovalno napravo
4	Vhodni/izhodni signal	Kalibriranje
5	Trajni napajalni izhod	Predpisano območje napetosti je napetost napeljave v vozilu, znižano za 3 V zaradi padca napetosti na zaščitnih vezjih Izhod 40 mA
6	TxD — prenos podatkov	Izhod podatkov iz zapisovalne naprave

1.3 Bločna shema

INT_003 Bločna shema mora biti v skladu z naslednjo:



2. VMESNIK ZA PRENOS PODATKOV

INT_004 Vmesnik za prenos podatkov mora ustrezati specifikacijam RS232.

INT_005 Vmesnik za prenos podatkov mora uporabljati en bit za začetek, 8 podatkovnih bitov, pri čemer je prvi bit z najmanjšo težo (LSB), in en končni bit.



Organizacija podatkovnih bajtov

Začetni bit: en bit na logičnem nivoju 0

Podatkovni biti: prenašani tako, da je LSB prvi

Parnostni bit: soda parnost

Končni bit: en bit na logičnem nivoju 1]

Pri prenosu številskih podatkov, ki jih sestavlja več bajtov, se najprej prenese bajt z največjo težo, nazadnje pa bajt z najmanjšo težo.

INT_006 Baudna hitrost prenosa mora biti nastavljiva v območju od 9 600 bps do 115 200 bps. Prenos mora potekati z najvišjo možno hitrostjo prenosa; ob začetku komunikacije se baudna hitrost nastavi na začetno vrednost 9600 bps.

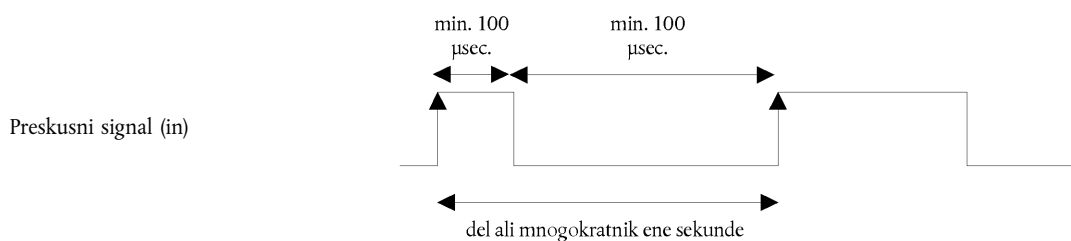
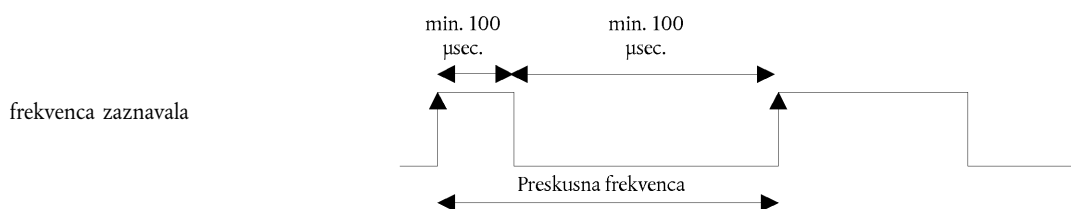
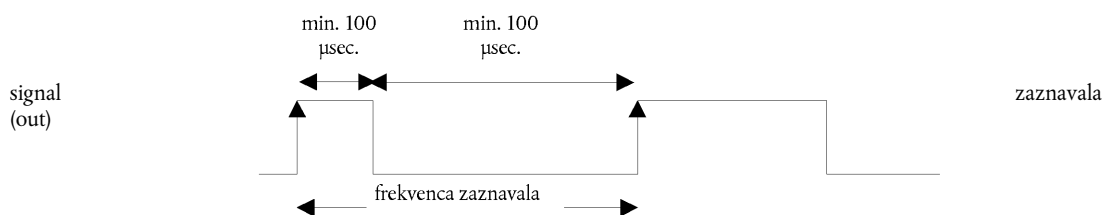
3. VMESNIK ZA KALIBRIRANJE

INT_007 Podatkovna komunikacija mora biti skladna z ISO 14 230-1 Cestna vozila — diagnostični sistemi — protokol s ključnimi besedami 2000 — del 1: fizična raven, prva izdaja: 1999.

INT_008 Vhodno/izhodni signal mora biti skladen z naslednjimi električnimi specifikacijami:

Parameter	Minimalno	Tipično	Maksimalno	Opomba
U_{low} (in)			1,0 V	$I = 750 \mu\text{A}$
U_{high} (in)	4 V			$I = 200 \mu\text{A}$
Frekvenca			4 kHz	
U_{low} (in)			1,0 V	$I = 1 \text{ mA}$
U_{high} (out)	4 V			$I = 1 \text{ mA}$

INT_009 Vhodno/izhodni signal mora biti skladen z naslednjimi časovnimi diagrami:



Dodatek 7

PROTOKOLI PRENOSA PODATKOV

VSEBINA

1.	Uvod	428
1.1	Veljavnost	428
1.2	Akronimi in notacije	428
2.	Prenos podatkov z VU	429
2.1	Postopek prenosa	429
2.2	Protokol prenosa podatkov	429
2.2.1	Sestava sporočila	429
2.2.2	Vrste sporočil	430
2.2.2.1	Zahtevek za začetek komunikacije (SID 81)	434
2.2.2.2	Pozitivni odgovor na zahtevek za začetek komunikacije (SID C1)	434
2.2.2.3	Zahtevek za začetek diagnostične seje (SID 10)	434
2.2.2.4	Pozitivni odgovor na zahtevek za začetek diagnostične seje (SID 50)	434
2.2.2.5	Storitev upravljanja povezave (SID 87)	434
2.2.2.6	Pozitivni odgovor na zahtevek za storitev upravljanja povezave (SID C7)	434
2.2.2.7	Zahtevek za začetek prenosa podatkov iz VU (SID 35)	434
2.2.2.8	Pozitivni odgovor na zahtevek za začetek prenosa podatkov iz VU (SID 75)	434
2.2.2.9	Zahtevek za prenos podatkov (SID 36)	434
2.2.2.10	Pozitivni odgovor na zahtevek za prenos podatkov (SID 76)	433
2.2.2.11	Zahtevek za izhod iz prenosa podatkov (SID 37)	433
2.2.2.12	Pozitivni odgovor na zahtevek za izhod iz prenosa podatkov (SID 77)	433
2.2.2.13	Zahtevek za konec komunikacije (SID 82)	433
2.2.2.14	Pozitivni odgovor na zahtevek za konec komunikacije (SID C2)	433
2.2.2.15	Potrditev delnega sporočila (SID 83)	433
2.2.2.16	Negativni odgovor (SID 7F)	433
2.2.3	Tok sporočil	434
2.2.4	Časovni diagrami	435
2.2.5	Obravnavna napak	435
2.2.5.1	Faza začetka komunikacije	435
2.2.5.2	Faza komunikacije	435
2.2.6	Vsebina sporočila odgovora	438
2.2.6.1	Pozitivni odgovor na zahtevek za prenos pregledov	438
2.2.6.2	Pozitivni odgovor na zahtevek za prenos podatkov o dejavnostih	439
2.2.6.3	Pozitivni odgovor na zahtevek za prenos podatkov o dogodkih in napakah	440

2.2.6.4	Pozitivni odgovor na zahtevek za prenos podrobnih podatkov o hitrostih	441
2.2.6.5	Pozitivni odgovor na zahtevek za prenos tehničnih podatkov	441
2.3	Hranjenje datoteke ESM	442
3.	Protokol prenosa podatkov s tahografske kartice	442
3.1	Veljavnost	442
3.2	Opredelitve	442
3.3	Prenos podatkov s kartice	442
3.3.1	Inicializacijsko zaporedje	443
3.3.2	Zaporedje za nepodpisane podatkovne datoteke	443
3.3.3	Zaporedje za podpisane podatkovne datoteke	443
3.3.4	zaporedje za ponastavitev števca kalibriranj	444
3.4	Format hranjenja podatkov	444
3.4.1	Uvod	444
3.4.2	Format datoteke	444
4.	Prenos podatkov s tahografske kartice preko enote v vozilu	445

1. UVOD

Ta dodatek predpisuje postopke, ki se jih uporablja pri različnih vrstah prenosov podatkov na zunanje pomnilne medije, in protokole, ki jih je treba uporabljati za zagotovitev pravilnega prenosa podatkov in polne združljivosti formatov prenesenih podatkov, tako da jih lahko pregleduje vsak nadzornik in lahko pred analiziranjem preveri njihovo avtentičnost in celovitost.

1.1 Veljavnost

Podatke se lahko prenaša v ESM:

- iz enote v vozilu, z inteligentno namensko opremo (IDE), povezano v VU,
- s tahografske kartice z IDE opremljeno z vmesniško napravo za kartico (IFD),
- s kartice preko enote v vozilu, z IDE, povezano v VU.

Da je mogoče preveriti avtentičnost in celovitost prenesenih podatkov, shranjenih v ESM, se podatke prenaša s pripetim podpisom, v skladu z določbami dodatka 11, Skupni varnostni mehanizmi. Prenese se tudi identifikacijo in varnostne certifikate (države članice in opreme) izvirne opreme (VU ali kartice). Oseba, ki želi preveriti podatke, mora neodvisno imeti lasten varnostni evropski javni ključ.

DDP_001 Podatki, preneseni v eni seji prenosa, morajo biti shranjeni v ESM v eni datoteki.

1.2 Akronimi in notacije

V tem dodatku so uporabljeni naslednji akronimi:

AID	identifikator aplikacije
ATR	odziv na ponastavitev
CS	bajt preskusne vsote
DF	namenska datoteka
DS_	diagnostična seja
EF	elementarna datoteka
ESM	zunanjí pomnilniški medij
FID	identifikator datoteke (ID datoteke)
FMT	formatni bajt (prvi bajt glave sporočila)
ICC	kartica z integriranim vezjem
IDE	inteligentna namenska oprema: Oprema, ki se uporablja za prenos podatkov na ESM (npr. osebni računalnik)
IFD	vmesniška naprava
KWP	protokol s ključnimi besedami 2000
LEN	bajt dolžine (zadnji bajt glave sporočila)
PPS	izbira parametrov protokola
PSO	izvedba varnostne operacije
SID	identifikator storitve
SRC	izvirni bajt
TGT	ciljni bajt
TLV	vrednost dolžine značke
TREP	parameter odgovora pri prenosu
TRTP	parameter zahtevka za prenos
VU	enota v vozilu.

2. PRENOS PODATKOV IZ VU

2.1 Postopek prenosa

Za prenos podatkov iz VU mora operater izvesti naslednje operacije:

- vstaviti svojo tahografsko kartico v rezo v VU ⁽¹⁾,
- priključiti IDE na konektor za prenos podatkov na VU,
- vzpostaviti povezavo med IDE in VU,
- na IDE izbrati podatke, ki jih želi prenesti, in poslati zahtevek VU,
- zaključiti sejo prenosa podatkov.

2.2 Protokol prenosa podatkov

Protokol je strukturiran kot sodelovanje nadrejenega in podrejenega udeleženca, pri čemer je IDE nadrejeni, VU pa podrejeni udeleženec.

Struktura, vrste in tok sporočil temeljijo v glavnem na protokolu ključnih besed 2000 (KWP) (ISO 14230-2 Cestna vozila – diagnostični sistemi – protokol ključnih besed 2000 – del 2: raven podatkovnih povezav).

Aplikativna raven v glavnem temelji na sedanjem osnutku ISO 14229-1 (Cestna vozila – diagnostični sistemi – del 1: diagnostične storitve, verzija 6 z dne 22. februarja 2001).

2.2.1 Sestava sporočila

DDP_002 Vsa sporočila, ki si jih izmenjujeta IDE in VU, so formatirana tako, da jih sestavljajo po trije deli:

- glava, ki jo sestavljajo formatni bajt (FMT), ciljni bajt (TGT), izvorni bajt (SRC) in lahko še bajt dolžine (LEN),
- podatkovno polje, ki ga sestavljajo bajt identifikatorja storitve (SID) in spremenljivo število podatkovnih bajtov, ki lahko vključujejo neobvezni bajt diagnostične seje (DS_) ali neobvezni bajt parametrov prenosa (TRTP ali TREP).
- preskusna vsota, ki jo sestavlja bajt preskusne vsote (CS).

Glava				Podatkovno polje					Preskusna vsota
FMT	TGT	SRC	LEN	SID	Podatki	...	...	...	CS
4 bajti				največ 225 bajtov					1 bajt

Bajta TGT in SRC predstavljata fizična naslova prejemnika in tvorca sporočila. Vrednosti sta F0h za IDE in EEh za VU.

Bajt LEN je dolžina podatkovnega dela sporočila.

Bajt preskusne vsote je 8-bitni rezultat ostanka vsote po modulu 256 vseh bajtov sporočila razen bajta CS samega.

Bajti FMT, SID, DS_, TRTP in TREP so opredeljeni kasneje v tem besedilu.

⁽¹⁾ Vstavljena kartica bo sprožila ustrezne pravice dostopa do funkcij prenosa in do podatkov.

DDP_003 Če mora sporočilo prenesti več podatkov kot je na voljo prostora v podatkovnem delu, se sporočilo dejansko prenese kot več delnih sporočil. Vsako delno sporočilo ima glavo, isti SID in TREP ter 2-bajtni števec delnih sporočil, ki kaže zaporedno številko delnega sporočila v celotnem sporočilu. Da je mogoče preverjati napake in prekiniti prenos, IDE potrdi vsako delno sporočilo. IDE lahko delno sporočilo sprejme, zahteva njegov ponovni prenos, zahteva od VU, naj začne prenos znova, ali prekine prenos.

DDP_004 Če zadnje delno sporočilo v svojem podatkovnem polju vsebuje natanko 255 bajtov, mora biti poslano še končno delno sporočilo s praznim podatkovnim poljem (razen bajtov SID, TREP in števca delnih sporočil), ki označi konec celotnega sporočila.

Primer:

Glava	SID	TREP	Sporočilo	CS
4 bajti	Daljše od 255 bajtov			

To sporočilo bo preneseno v naslednji obliki:

Glava	SID	TREP	00	01	Delno sporočilo 1	CS
4 bajti	255 bajtov					

Glava	SID	TREP	00	01	Delno sporočilo 2	CS
4 bajti	255 bajtov					

...

Glava	SID	TREP	xx	yy	Delno sporočilo n	CS
4 bajti	Manj kot 255 bajtov					

ali v naslednji:

Glava	SID	TREP	00	01	Delno sporočilo 1	CS
4 bajti	255 bajtov					

Glava	SID	TREP	00	02	Delno sporočilo 2	CS
4 bajti	255 bajtov					

...

Glava	SID	TREP	xx	yy	Delno sporočilo n	CS
4 bajti	255 bajtov					

Glava	SID	TREP	xx	yy+1	CS
4 bajti	4 bajti				

2.2.2 Vrste sporočil

Komunikacijski protokol za prenos podatkov med VU in IDE zahteva izmenjavo sporočil osmih različnih vrst.

Ta sporočila povzema naslednja tabela.

Sestava sporočila	Glava - največ 4 bajti				Podatki – največ 255 bajtov			Preskusna vsota – 1 bajt
IDE ->	<- VU				SID	DS/TRTP	DATA	CS
Zahtevek za začetek komunikacije	81	EE	F0		81			E0
Pozitivni odgovor na zahtevek za začetek komunikacije	80	F0	EE	03	C1		8F,EA	9B
Zahtevek za začetek diagnostične seje	80	EE	F0	02	10	81		F1
Pozitivni odgovor na zahtevek za začetek diagnostične seje	80	F0	EE	02	50	81		31
Storitev upravljanja povezave								
Preverjanje baudne hitrosti (faza 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	ED
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Pozitivni odgovor na zahtevek za preverjanje baudne hitrosti	80	F0	EE	02	C7		01	28
Prehodna baudna hitrost (faza 2)	80	EE	F0	03	87		02,03	ED
Zahtevek za prenos iz VU	80	EE	F0	0A	35		00,00,00,00,00,FF,FF,FF,FF	99
Pozitivni odgovor na zahtevek za začetek prenosa podatkov iz VU	80	F0	EE	03	75		00,FF	D5
Zahtevek za prenos podatkov								
Pregled	80	EE	F0	02	36	01		97
Dejavnosti	80	EE	F0	06	36	02	Date	CS
Dogodki in napake	80	EE	F0	02	36	03		99
Podrobni podatki o hitrosti	80	EE	F0	02	36	04		9A
Tehnični podatki	80	EE	F0	02	36	05		9B
Prenos podatkov s kartice	80	EE	F0	02	36	06		9C
Pozitivni odgovor na zahtevek za prenos podatkov	80	F0	EE	Len	76	TREP	Data	CS
Zahtevek za izhod iz prenosa podatkov	80	EE	F0	01	37			96
Pozitivni odgovor na zahtevek za izhod iz prenosa podatkov	80	F0	EE	01	77			D6
Zahtevek za konec komunikacije	80	EE	F0	01	82			E1
Pozitivni odgovor na zahtevek za konec komunikacije	80	F0	EE	01	C2			21
Potrditev delnega sporočila	80	EE	F0	Len	83		Data	CS
Negativni odgovori								
Splošna zavrnitev	80	F0	EE	03	7F	Sid Req	10	CS
Storitev ni podprta	80	F0	EE	03	7F	Sid Req	11	CS
Podfunkcija ni podprta	80	F0	EE	03	7F	Sid Req	12	CS
Nepravilna dolžina sporočila	80	F0	EE	03	7F	Sid Req	13	CS
Nepravilni pogoji ali napaka v zaporedju zahtevkov	80	F0	EE	03	7F	Sid Req	22	CS
Zahtevek izven območja	80	F0	EE	03	7F	Sid Req	31	CS
Prenos ni sprejet	80	F0	EE	03	7F	Sid Req	50	CS
Čakanje na odgovor	80	F0	EE	03	7F	Sid Req	78	CS
Podatki niso na voljo	80	F0	EE	03	7F	Sid Req	FA	CS

Opombe:

- Sid Req = Sid zadevnega zahtevka.
- TREP = TRTP zadevnega zahtevka.
- Osenčene celice pomenijo, da se ne prenese nič podatkov.
- Morebitni 2-bajtni števec delnih sporočil v tej tabeli niso prikazani.

2.2.2.1 Zahtevek za začetek komunikacije (SID 81)

DDP_005 To sporočilo pošlje IDE za vzpostavitev komunikacijske povezave z VU. Začetna komunikacija vedno poteka s hitrostjo 9600 baud (dokler baudne hitrosti ne spremeni ustreznega storitev upravljanja povezave).

2.2.2.2 Pozitivni odgovor na zahtevek za začetek komunikacije (SID C1)

DDP_006 To sporočilo pošlje VU kot pozitivni odgovor na zahtevek za vzpostavitev komunikacijske povezave. Sporočilo vsebuje dva ključna bajta '8F ??', ki kazeta, da enota podpira protokol, pri katerem glava vsebuje podatke o izvoru, cilju in dolžini.

2.2.2.3 Zahtevek za začetek diagnostične seje (SID 10)

DDP_007 zahtevek za začetek diagnostične seje pošlje IDE; z njim zahteva novo diagnostično sejo z VU. Podfunkcija 'privzeta seja' (81h) pomeni, naj se začne standardna diagnostična seja.

2.2.2.4 Pozitivni odgovor na zahtevek za začetek diagnostične seje (SID 50)

DDP_008 To sporočilo pošlje VU kot pozitivni odgovor na zahtevek za začetek diagnostične seje.

2.2.2.5 Storitve upravljanja povezave (SID 87)

DDP_052 Sporočilo storitve upravljanja povezave pošlje IDE kot zahtevek za spremembo baudne hitrosti. Ta sprememba se izvede v dveh korakih. V prvem koraku IDE predlaga spremembo baudne hitrosti in predlaga novo baudno hitrost. Po prejemu pozitivnega odgovora od VU pošlje IDE v VU potrditev spremembe baudne hitrosti (drugi korak). Nato IDE spremeni baudno hitrost na novo vrednost. Po prejemu potrditve VU spremeni baudno hitrost na novo vrednost.

2.2.2.6 Pozitivni odgovor na zahtevek za storitev upravljanja povezave (SID C7)

DDP_053 To sporočilo pošlje VU kot pozitivni odgovor na zahtevek za storitev upravljanja povezave (prvi korak). Na zahtevek za potrditev (drugi korak) VU ne da nikakršnega odgovora.

2.2.2.7 Zahtevek za začetek prenosa podatkov iz VU (SID 35)

DDP_009 Zahtevek za začetek prenosa podatkov iz VU pošlje IDE; z njim sporoči VU, da zahteva operacijo prenosa podatkov iz VU v IDE. Za izpolnitev zahtev ISO 14229, so vključeni podatki o naslovu, velikosti in podrobnostih formata zahtevanih podatkov. Ker teh podatkov IDE pred začetkom prenosa podatkov ne pozna, je pomnilniški naslov nastavljen na 0, format na nešifrirani in nekomprimirani format, pomnilniška velikost pa na največjo.

2.2.2.8 Pozitivni odgovor na zahtevek za začetek prenosa podatkov iz VU (SID 75)

DDP_010 Pozitivni odgovor na zahtevek za začetek prenosa podatkov iz VU pošlje VU; z njim sporoči IDE, da je pripravljena na operacijo prenosa podatkov. Za izpolnitev zahtev ISO 14229 so v ta pozitivni odgovor vključeni podatki, ki IDE povedo, da bodo naslednja sporočila prenosa podatkov vsebovala največ FFh bajtov.

2.2.2.9 Zahtevek za prenos podatkov (SID 36)

DDP_011 Zahtevek za začetek prenosa podatkov iz VU pošlje IDE; z njim sporoči VU, katere podatke na prenes. Enobajtni parameter zahtevka za prenos (TRTP) označuje vrsto prenosa.

Obstaja šest vrst prenosa podatkov:

- pregled (TRTP 01),
- dejavnosti na določen dan (TRTP 02),
- dogodki in napake (TRTP 03),
- podrobni podatki o hitrosti (TRTP 04),
- tehnični podatki (TRTP 05),
- prenos podatkov s kartice (TRTP 06).

DDP_054 IDE mora med sejo prenosa podatkov obvezno zahtevati prenos preglednih podatkov (TRTP 01), saj se lahko le na ta način v datoteko prenesenih podatkov zapišejo tudi certifikati VU (in je tako mogoče preveriti digitalni podpis).

V drugem primeru (TRTP 02) sporočilo zahtevka za prenos podatkov vsebuje podatek o koledarskem dnevu (v formatu `TimeReal`), za katerega naj se prenesejo podatki.

2.2.2.10 Pozitivni odgovor na zahtevek za prenos podatkov (SID 76)

DDP_012 Pozitivni odgovor na zahtevek za prenos podatkov pošlje VU kot odgovor na zahtevek za prenos podatkov. Sporočilo vsebuje zahtevane podatke, parameter odgovora pri prenosu (TREP) pa ustreza TRTP iz zahtevka.

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

- varnostni certifikati,
- identifikacija vozila,
- tekoči datum in čas VU,
- najstarejši in najnovejši datum, za katerega je mogoče prenesti podatke (po podatkih v VU),
- znak, kateri kartici sta vstavljeni v VU,
- predhodni prenosi podatkov za potrebe podjetja,
- blokade s strani podjetja,
- predhodni nadzori.

2.2.2.11 Zahtevek za izhod iz prenosa podatkov (SID 37)

DDP_013 Zahtevek za izhod iz prenosa podatkov pošlje IDE; z njim sporoči VU, da je seja prenosa podatkov iz VU zaključena.

2.2.2.12 Pozitivni odgovor na zahtevek za izhod iz prenosa podatkov (SID 77)

DDP_014 Pozitivni odgovor na zahtevek za izhod iz prenosa podatkov pošlje VU kot potrditev zahtevka za izhod iz prenosa podatkov.

2.2.2.13 Zahtevek za konec komunikacije (SID 82)

DDP_015 Sporočilo zahtevka za konec komunikacije pošlje IDE za prekinitev komunikacijske povezave z VU.

2.2.2.14 Pozitivni odgovor na zahtevek za konec komunikacije (SID C2)

DDP_016 Pozitivni odgovor na zahtevek za konec komunikacije pošlje VU kot potrditev zahtevka za konec komunikacije.

2.2.2.15 Potrditev delnega sporočila (SID 83)

DDP_017 Sporočilo potrditve delnega sporočila pošlje IDE kot potrditev sprejema vsakega dela sporočila, ki se prenaša v več delnih sporočilih. Podatkovno polje vsebuje SID, sprejet od VU, in naslednjo 2-bajtno kodo:

- `MsgC + 1` potrjuje pravilni sprejem delnega sporočila štev. `MsgC`.
Zahtevek IDE, naj VU pošlje naslednje delno sporočilo,
- `MsgC` kaže, da je med sprejemanjem delnega sporočila štev. `MsgC` prišlo do določenega problema.
Zahtevek IDE, naj VU pošlje isto delno sporočilo še enkrat,
- `FFFF` zahteva prekinitev pošiljanja sporočila.

To sporočilo lahko pošlje IDE v VU kot zahtevek, naj konča prenašanje sporočila, iz kateregakoli razloga.

Zadnje delno sporočilo (bajt `LEN < 255`) lahko IDE potrdi s katerokoli od teh kod ali pa sprejema sploh ne potrdi.

Odgovori VU, ki bodo obsegali več delnih sporočil, so:

- pozitivni odgovor na zahtevek za prenos podatkov (SID 76).

2.2.2.16 Negativni odgovor (SID 7F)

DDP_018 Sporočilo negativnega odgovora pošlje VU kot odgovor na zgornja sporočila zahtevkov, kadar VU zahtevka ne more izpolniti. Podatkovno polje sporočila vsebuje SID odgovora (7F), SID zahtevka in kodo, ki označuje vzrok za negativni odgovor. Možne so naslednje kode:

- 10 splošna zavrnitev
Akcije ni mogoče izvesti iz razloga, ki ga ne opisujejo kode v nadaljevanju
- 11 storitev ni podprta
VU ne razume SID zahtevka
- 12 podfunkcija ni podprta
VU ne razume DS_ ali TRTP zahtevka, ali pa ni več sporočil, ki bi jih lahko VU poslala
- 13 nepravilna dolžina sporočila
Dolžina sprejetega sporočila ni pravilna
- 22 nepravilni pogoji ali napaka v zaporedju zahtevkov
Zahtevana storitev ni aktivna ali pa ni pravilno zaporedje sporočil zahtevkov
- 31 zahtevek izven območja
Parameter zapisa (podatkovno polje) v zahtevku ni veljaven
- 50 prenos ni sprejet
Zahtevka ni mogoče izpolniti (VU ni v ustreznem režimu delovanja ali pa ima VU interno napako)
- 78 čakanje na odgovor
Zahtevane akcije ni mogoče zaključiti pravočasno, zato VU ne more sprejeti drugega zahtevka
- FA podatki niso na voljo
Podatkovni objekt iz zahtevka za prenos podatkov ni na voljo VU (npr. kartica ni vstavljena, ...)

2.2.3 Tok sporočil

Tipični tok podatkov med normalnim postopkom prenosa podatkov je naslednji:

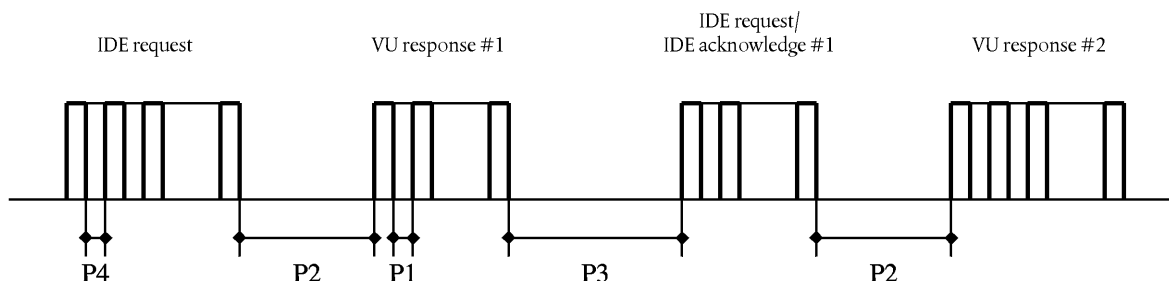
IDE		FE
Zahtevek za začetek komunikacije	⇨ ⇧	Pozitivni odgovor
Zahtevek za začetek diagnostične seje	⇨ ⇧	Pozitivni odgovor
Zahtevek za prenos iz VU	⇨ ⇧	Pozitivni odgovor
Zahtevek za prenos preglednih podatkov	⇨ ⇧	Pozitivni odgovor — prenos
Zahtevek za podatke #2	⇨	Pozitivni odgovor #1 Pozitivni odgovor #2 Pozitivni odgovor #m Pozitivni odgovor (podatkovno polje < 255 bajtov)
Potrditev delnega sporočila #1	⇧	
Potrditev delnega sporočila #2	⇨	
Potrditev delnega sporočila #m	⇧	
Potrditev delnega sporočila #m	⇨	
Potrditev delnega sporočila (neobvezna)	⇧	
	⇨	
...		
Zahtevek za prenos podatkov #n	⇨ ⇧	Pozitivni odgovor
Zahtevek za izhod iz prenosa podatkov	⇨ ⇧	Pozitivni odgovor
Zahtevek za konec komunikacije	⇨ ⇧	Pozitivni odgovor

2.2.4 Časovni diagrami

DDP_019 Med normalnim delovanjem so pomembni časovni parametri, prikazani na naslednjem diagramu:

Slika 1

Tok sporočil, časovni diagram



Pri čemer so:

P1 = čas med bajti odgovora VU

P2 = čas med koncem zahtevka iz IDE in začetkom odgovora VU ali med potrditvijo iz IDE in začetkom naslednjega odgovora VU

P3 = čas med koncem odgovora VU in novim zahtevkom IDE, ali med koncem odgovora VU in začetkom potrditve iz IDE, ali med koncem zahtevka iz IDE in začetkom novega zahtevka iz IDE; če VU ne odgovori

P4 = čas med bajti zahtevka IDE

P5 = podaljšana vrednost P3 pri prenosu podatkov iz kartice

Dopustne vrednosti časovnih parametrov so podane v naslednji tabeli (razširjeni nabor časovnih parametrov KWP, uporabljen pri fizičnem naslavljanju za hitrejšo komunikacijo).

Časovni parameter	Spodnja mejna vrednost (ms)	Zgornja mejna vrednost (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minut

(*) Če VU pošlje negativen odgovor s kodo, ki pomeni 'zahtevek v redu sprejet, čakanje na odgovor', se ta vrednost podaljša na vrednost, enako gornji mejni vrednosti parametra P3.

2.2.5 Obravnava napak

Če pri izmenjavi sporočil pride do napake, se tok sporočil spremeni glede na to, kateri del opreme je zaznal napako in glede na sporočilo, ki je povzročilo napako.

Sliki 2 in 3 prikazujeta postopke obravnave napak v VU in v IDE.

2.2.5.1 Faza začetka komunikacije

DDP_020 Če IDE zazna napako v fazi začetka komunikacije, bodisi časovne ali v toku bitov, počaka čas P3min, nato pa ponovno pošlje zahtevek.

DDP_021 Če VU zazna napako v sekvenci, ki jo prejema iz IDE; ne pošlje nikakršnega odgovora in počaka naslednji zahtevek za začetek komunikacije, ki ga mora prejeti najkasneje v obdobju P3.

2.2.5.2 Faza komunikacije

Opredelimo lahko dve območji obravnave napak:

1. VU zazna napako prenosa iz IDE.

DDP_022 Pri vsakem sprejetem sporočilu VU preverja napake časovnega poteka, napake v formatih bajtov (npr. kršitve pravil glede začetnih ali končnih bitov) in napake v okviru (prejeto napačno število bajtov, napaka v bajtu preskusne vsote).

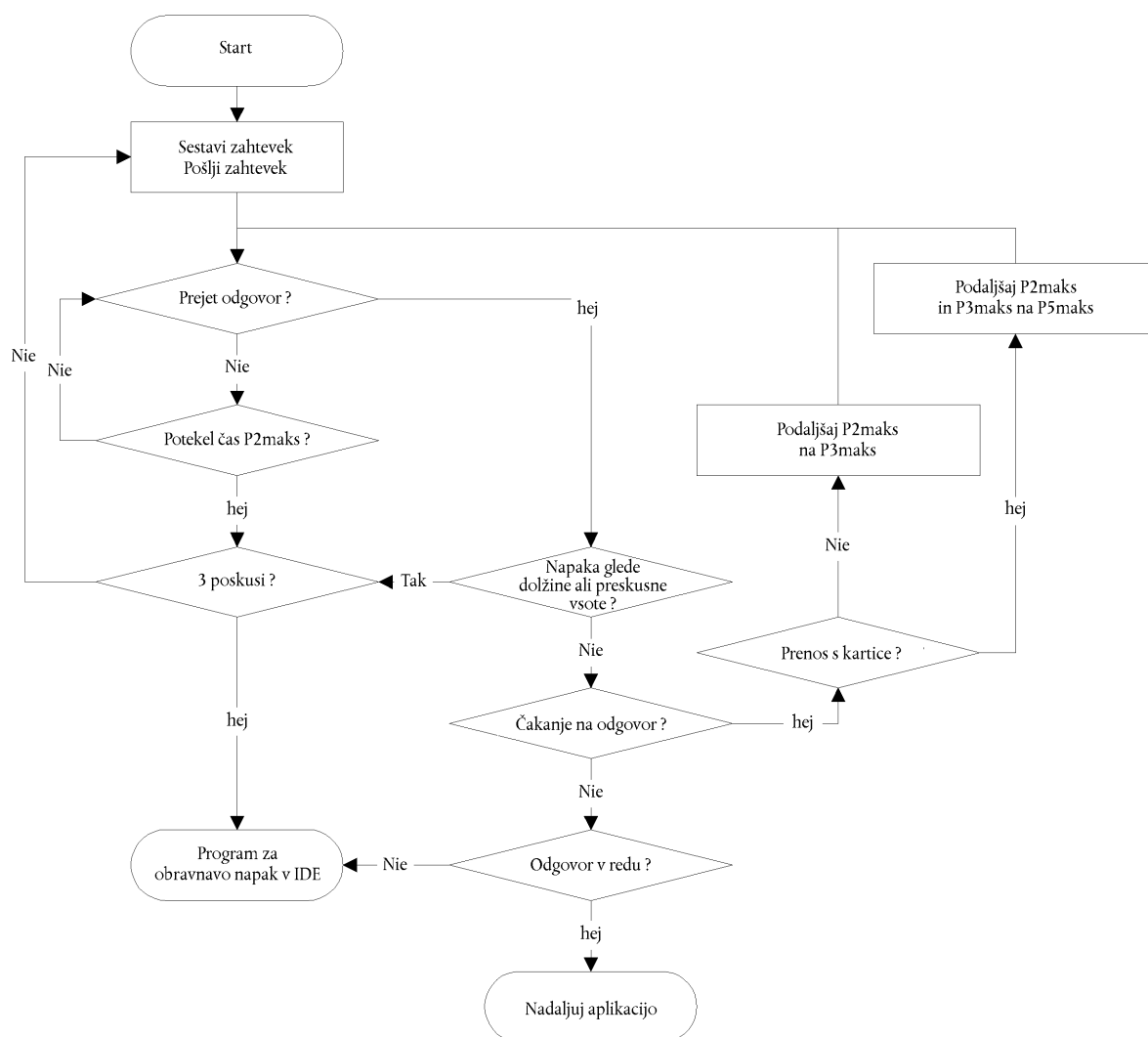
DDP_023 Če VU zazna katero od gornjih napak, ne pošlje nikakršnega odgovora in zanemari prejeto sporočilo.

2. IDE zazna napako prenosa iz VU.

- DDP_025 Pri vsakem sprejetem sporočilu IDE preverja napake časovnega poteka, napake v formatih bajtov (npr. kršitve pravil glede začetnih ali končnih bitov) in napake v okviru (prejeto napačno število bajtov, napaka v bajtu preskusne vsote).
- DDP_026 IDE mora preverjati tudi napake v zaporedju sporočil, npr. nepravilno povečevanje števca delnih sporočil, v zaporedoma prejetih sporočilih.
- DDP_027 Če IDE zazna napako ali če ne prejme odgovora iz VU v času P2maks, pošlje sporočilo z zahtevkom še enkrat — največ trikrat. V okviru obravnave te napake velja sporočilo potrditve delnega sporočila za zahtevek poslan v VU.
- DDP_028 Pred začetkom vsakega pošiljanja mora IDE počakati čas najmanj P3min; obdobje čakanja se meri od zadnjega izračunane nastopa zaključnega bita po tem, ko je bila napaka zaznana.

Slika 3

Obravnava napak v IDE



2.2.6 Vsebina sporočila odgovora

Ta točka predpisuje vsebino podatkovnih polj posameznih sporočil pozitivnih odgovorov.

Podatkovni elementi so opredeljeni v slovarju podatkov v dodatku 1.

2.2.6.1 Pozitivni odgovor na zahtevek za prenos pregledov

DDP_029 Podatkovno polje ‚pozitivnega odgovora na zahtevek za prenos pregledov‘ mora vsebovati spodaj naštetе podatke v predpisanem vrstnem redu; SID mora biti 76h, TREP 01; sporočilo mora biti ustrezno razdeljeno in delna sporočila označena z zaporednimi številkami:

Data Element	Length (Bytes)	Comment
MemberStateCertificate	194	Varnostni certifikati VU
VUCertificate	194	
VehicleIdentificationNumber	17	Identifikacija vozila
VehicleRegistrationIdentification	1	
vehicleRegistrationNation	14	
vehicleRegistrationNumber	14	
CurrentDateTime	4	Tekoči datum in čas VU
VuDownloadablePeriod	4	Obdobje, za katerega je mogoče prenesti podatke
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Vrsti kartic vstavljenih v VU
VuDownloadActivityData	4	Prejšnji prenos podatkov iz VU
downloadingTime	18	
fullCardNumber	36	
companyOrWorkshopName	36	
VuCompanyLocksData	1	Vse shranjene blokade podjetja. Če je ta del prazen, se pošlje le podatek noOfLocks = 0
noOfLocks	(98)	
...		
Vu Company Locks Record	4	
lockInTime	4	
lockOutTime	36	
companyName	36	
companyAddress	36	
companyCardNumber	18	
...		
VuControlActivityData	1	Vsi zapisi nadzorov, shranjeni v VU. Če je ta del prazen, se pošlje le podatek noOfControls = 0
noOfControls	(31)	
...		
Vu Control Activity Record	1	
controlType	4	
controlTime	18	
controlCardNumber	4	
downloadPeriodBeginTime	4	
downloadPeriodEndTime	4	
...		
Signature	128	RSA podpis vseh podatkov (razen certifikatov), od VehicleIdentificationNumber do zadnjega bajta zapisa VuControlActivityRecord.

2.2.6.2 Pozitivni odgovor na zahtevek za prenos podatkov o dejavnostih

DDP_030 Podatkovno polje 'pozitivnega odgovora na zahtevek za prenos podatkov o dejavnostih' mora vsebovati spodaj naštetе podatke v predpisanem vrstnem redu; SID mora biti 76h, TREP 02; sporočilo mora biti ustrezno razdeljeno in delna sporočila označena z zaporednimi številkami:

Data Element	Length (Bytes)	Comment
TimeReal	4	Datum dneva, katerega podatki se prenašajo
OdometerValueMidnight	3	Števec prevožene poti na koncu dne, katerega podatki se prenašajo
VuCardIWData noOfVuCardIWRecords	2	Podatki o ciklih vstavitve in izvleka kartic — Če v tem delu ni na voljo nobenih podatkov, se pošlje le podatek noOfVUCardIWRecord = 0
...	(129)	
VuCardIWRecord cardHolderName holderSurname holderFirstNames fullCardNumber cardExpiryDate cardInsertionTime vehicleOdometerValueAtInsertion cardSlotNumber cardWithdrawalTime vehicleOdometerValueAtWithdrawal previousVehicleInfo vehicleRegistrationIdentification vehicleRegistrationNation vehicleRegistrationNumber cardWithdrawalTime manualInputFlag	36 36 18 4 4 3 1 4 3 1 14 4 1	— Če sega določen VUCardIWRecord čez čas 00:00 (kartica je bila vstavljena prejšnji dan) ali čez 24:00 (kartica izvlečena naslednji dan), se ta zapis prenese cel, s štetima obema dnevoma
...		
VuActivityDailyData noOfActivityChanges	2	Stanje rež ob 00:00 in zapisane spremembe dejavnosti na dan, za katerega se prenaša podatke
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData noOfPlaceRecords	1	Podatki o krajih, zapisani na dan, za katerega se prenaša podatke.
...	(28)	Če je ta del prazen, se pošlje le podatek noOfPlacesRecords = 0.
VuPlaceDailyWorkPeriodRecord fullCardNumber placeRecord entryTime entryTypeDailyWorkPeriod dailyWorkPeriodCountry dailyWorkPeriodRegion vehicleOdometerValue	18 4 1 1 1 1 3	
...		
VuSpecificConditionData noOfSpecificConditionRecords	2	Podatki o posebnih stanjih, zapisani na dan, za katerega se prenaša podatke.
...	(5)	Če je ta del prazen, se pošlje le podatek noOfSpecificConditionRecords = 0.
SpecificConditionRecord EntryTime specificConditionType	4 1	
...		
Signature	128	RSA podpis vseh podatkov (razen certifikatov), od TimeReal do zadnjega bajta zapisa posebnih stanj.

2.2.6.3 Pozitivni odgovor na zahtevek za prenos podatkov o dogodkih in napakah

DDP_031 Podatkovno polje 'pozitivnega odgovora na zahtevek za prenos podatkov o dogodkih in napakah' mora vsebovati spodaj našete podatke v predpisanem vrstnem redu; SID mora biti 76h, TREP 03; sporočilo mora biti ustrezno razdeljeno in delna sporočila označena z zaporednimi števkami:

Data Element	Length (Bytes)	Comment
VuFaultData		
NoOfVuFaults	1	Vse napake, shranjene ali tekoče v VU. Če je ta del prazen, se pošlje le podatek noOfVUFaults = 0
...	(82)	
VuFaultRecord		
FaultType	1	
FaultRecordPurpose	1	
FaultBeginTime	4	
FaultEndTime	4	
CardNumberDriverSlotBegin	18	
cardNumberCodriverSlotBegin	18	
CardNumberDriverSlotEnd	18	
CardNumberCodriverSlotEnd	18	
...		
VuEventData		
NoOfVuEvents	1	Vsi dogodki (razen prekoračitev hitrosti), shranjeni ali tekoči v VU. Če je ta del prazen, se pošlje le podatek noOfVUEvents = 0
...	(83)	
VuEventRecord		
EventType	1	
EventRecordPurpose	1	
EventBeginTime	4	
EventEndTime	4	
CardNumberDriverSlotBegin	18	
cardNumberCodriverSlotBegin	18	
CardNumberDriverSlotEnd	18	
CardNumberCodriverSlotEnd	18	
SimilarEventsNumber	1	
...		
VuOverSpeedingControlData		
LastOverspeedControlTime	4	Podatki o zadnjem nadzoru prekoračitev hitrosti (če ni podatkov - privzeta vrednost)
FirstOverspeedSince	4	
NumberOfOverspeedSince	1	
VuOverSpeedingEventData		
NoOfVuOverSpeedingEvents	1	Vsi dogodki prekoračitve hitrosti, shranjeni v VU. Če je ta del prazen, se pošlje le podatek noOfVUOverSpeedingEvents = 0
...	(31)	
VuOverSpeedingEventRecord		
EventType	1	
EventRecordPurpose	1	
EventBeginTime	4	
EventEndTime	4	
MaxSpeedValue	1	
AverageSpeedValue	1	
CardNumberDriverSlotBegin	18	
SimilarEventsNumber	1	
...		
VuTimeAdjustmentData		
NoOfVuTimeAdjRecords	1	Vsi dogodki nastavljanja časa, shranjeni v VU (razen nastavljanj časa pri polnem kalibriranju). Če je ta del prazen, se pošlje le podatek noOfVUTimeAdjRecords = 0
...	(98)	
VuTimeAdjustmentRecord		
OldTimeValue	4	
NewTimeValue	4	
WorkshopName	36	
WorkshopAddress	36	
WorkshopCardNumber	18	
...		
Signature	128	

2.2.6.4 Pozitivni odgovor na zahtevek za prenos podrobnih podatkov o hitrostih

DDP_032 Podatkovno polje ‚pozitivnega odgovora na zahtevek za prenos podrobnih podatkov o hitrostih‘ mora vsebovati spodaj našteje podatke v predpisanem vrstnem redu; SID mora biti 76h, TREP 04; sporočilo mora biti ustrezno razdeljeno in delna sporočila označena z zaporednimi številkami:

Data element	Length (Bytes)	Comment
VuDetailedSpeedData		
NoOfSpeedBlocks	2	Vsi dogodki nastavljanja časa, shranjeni v VU (razen nastavljanj časa pri polnem kalibriranju). Če je ta del prazen, se pošlje le podatek noOfVUTimeAdjRecords = 0
...		
VuDetailedSpeedBlock	4	
SpeedBlockBeginDate	60	
speedsPerSecond		
...		
Signature	128	RSA podpis vseh podatkov (razen certifikatov), od noOfVUFaults do zadnjega bajta zapisa nastavljanja časa.

2.2.6.5 Pozitivni odgovor na zahtevek za prenos tehničnih podatkov

DDP_033 Podatkovno polje ‚pozitivnega odgovora na zahtevek za prenos tehničnih podatkov‘ mora vsebovati spodaj našteje podatke v predpisanem vrstnem redu; SID mora biti 76h, TREP 05; sporočilo mora biti ustrezno razdeljeno in delna sporočila označena z zaporednimi številkami:

Data element	Length (Bytes)	Comment
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		
noOfVuCalibrationRecords	1	Vsi zapisi kalibriranj, shranjeni v VU
...	(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 podpis vseh podatkov (razen certifikatov), od vuManufacturerName do zadnjega bajta zapisa VuCalibrationRecord.

2.3 Hranjenje datoteke ESM

DDP_034 Če je bil med sejo prenosa podatkov opravljen tudi prenos podatkov iz VU, mora IDE shraniti v eno samo fizično datoteko vse podatke, prejete iz VU v tej seji, ki so bili sprejeti v okviru sporočil pozitivnih odgovorov na zahteve za prenos podatkov. Ne shrani se naslednjih podatkov: glav sporočil, števecv delnih sporočil, praznih delnih sporočil in prekusnih vsot, shrani pa se oznake SID in TREP (če sporočilo sestavlja več delnih sporočil, samo za prvo delno sporočilo).

3. PROTOKOL PRENOSA PODATKOV S TAHOGRAFSKE KARTICE

3.1 Veljavnost

Ta točka opisuje neposredni prenos podatkov s tahografske kartice v IDE. IDE ni del varnega okolja, zato se med IDE in kartico ne opravi nikakršna avtentifikacija.

3.2 Opredelitve

Seja prenosa podatkov: Vsak dogodek prenosa podatkov s kartice vrste ICC: Seja obsega celotni postopek od ponastavitve ICC z IFD do deaktiviranja ICC (izvlek kartice ali naslednja ponastavitev).

Podpisana podatkovna datoteka: Datoteka iz ICC. Datoteka se prenese v IDE kot čitljivo besedilo. Datoteko ICC razprši in podpiše, podpis pa prenese v IDE:

3.3 Prenos podatkov s kartice

DDP_035 Prenos podatkov s tahografske kartice obsega naslednje korake:

- prenos skupnih podatkov kartice iz EF ICC in IC. Ti podatki niso obvezni in niso zavarovani z digitalnim podpisom,
- prenos EF Card_Certificate in CA_Certificate. Ti podatki niso zavarovani z digitalnim podpisom,

Te podatke se obvezno prenese v vsaki seji prenosa podatkov.

- prenos drugih aplikativnih EF (v tahografski DF) razen Card_Download. Ti podatki so zavarovani z digitalnim podpisom,
 - med vsako sejo prenosa podatkov je obvezno treba prenesti vsaj EF Application_Identification in ID vsake seje prenosa podatkov,
 - pri prenosu podatkov z voznikove kartice je obvezen tudi prenos naslednjih EF:
 - Events_Data,
 - Faults_Data,
 - Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - Control_Activity_Data,
 - Specific_Conditions.
- Pri prenosu podatkov z voznikove kartice se posodobi datum LastCardDownload v EF Card_Download,
- Pri prenosu podatkov z delavniške kartice se ponastavi števec kalibriranj v EF Card_Download.

3.3.1 Inicializacijsko zaporedje

DDP_036 IDE inicializira zaporedje na naslednji način:

Kartica	Smer	IDE/IFD	Pomen/opombe
	↩	Ponastavitev strojne opreme	
ATR	⇒		

Dovoljena (neobvezna) je uporaba PPS za zvišanje baudne hitrosti, če ICC podpira to storitev.

3.3.2 Zaporedje za nepodpisane podatkovne datoteke

DDP_037 Zaporedje prenosa ICC, IC, Card_Certificate in CA_Certificate je naslednje:

Kartica	Smer	IDE/IFD	Pomen/opombe
	↩	Izbira datoteke	Izbira datoteke: z identifikatorji datotek
OK	⇒		
	↩	Binarno branje	Če datoteka vsebuje več podatkov, kot je zmogljivost vmesnega pomnilnika čitalnika ali kartice, je treba ukaz ponoviti tolikokrat, da se prebere cela datoteka.
Podatki datoteke OK	⇒	Shranitev podatkov v ESM	v skladu s točko 3.4 (Format hranjenja podatkov)

Opomba: Pred izbiro EF Card_Certificate je treba izbrati tahografsko aplikacijo (izbira z AID).

3.3.3 Zaporedje za podpisane podatkovne datoteke

DDP_038 Za vsako od naslednjih datotek je obvezno uporabiti opisano zaporedje; datoteke je treba prenašati skupaj z njihovimi podpisi.

Kartica	Irány	IDE/IFD	Pomen/opombe
	↩	Izbira datoteke	
OK	⇒		
	↩	Razpršitev datoteke	Izračun vrednosti razpršitve vsebine izbrane datoteke po predpisanem razpršitvenem algoritmu v skladu z dodatkom 11. Ta ukaz ni ISO ukaz.
Izračun razpršitve datoteke in začasna shranitev vrednosti razpršitve			
OK	⇒		
	↩	Binarno branje	Če datoteka vsebuje več podatkov, kot je zmogljivost vmesnega pomnilnika čitalnika ali kartice, je treba ukaz ponoviti tolikokrat, da se prebere cela datoteka.
Podatki datoteke OK	⇒	Shranitev sprejetih podatkov v ESM	v skladu s točko 3.4 (Format hranjenja podatkov)
	↩	PSO: Izračun digitalnega podpisa	
Izvedba varnostne operacije 'izračun digitalnega podpisa' z začasno shranjeno vrednostjo razpršitve			
Podpis OK	⇒	Dopis podatkov na konec prej shranjenih podatkov v ESM	v skladu s točko 3.4 (Format hranjenja podatkov)

3.3.4 Zaporedje za ponastavitev števca kalibriranj

DDP_039 Zaporedje ponastavitve števca NoOfCalibrationsSinceDownload v EF Card_Download na delavniški kartici je naslednje:

Kartica	Smer	IDE/IFD	Pomen/opombe
OK	↩	Izbira datoteke EFCard_Download	Izbira z identifikatorji datotek
	⇒		
	↩	Binarno posodabljanje NoOfCalibrationsSinceDownload = '00 00'	
Ponastavitev števila prenosov podatkov s kartice			
OK	⇒		

3.4 Format hranjenja podatkov

3.4.1 Uvod

DDP_040 Prenesene podatke se shrani na naslednji način:

- podatke se shrani transparentno. To pomeni, da se med shranjevanjem ohrani zaporedje bajtov in zaporedje bitov v vsakem bajtu tako, v kakršnem so podatki preneseni s kartice,
- vse datoteke, prenesene v okviru ene seje prenosa podatkov, se shrani v eni datoteki ESM.

3.4.2 Format datoteke

DDP_041 Datoteko sestavlja zaporedje (zlepek) več objektov TLV.

DDP_042 Značko EF sestavljata FID in dodatek ,00'.

DDP_043 Značko podpisa EF sestavljata FID datoteke in dodatek ,01'.

DDP_044 Dolžina je dvobajtna vrednost. Vrednost opredeljuje število bajtov v polju vrednosti. Vrednost ,FF FF' v polju dolžine je rezervirana za prihodnjo rabo.

DDP_045 Če datoteka ni prenesena, se ne shrani noben podatek v zvezi s to datoteko (niti značka niti ničelna dolžina).

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

Opredelitev	Pomen	Dolžina
FID (2 bajta) ,00'	Značka EF (FID)	3 bajti
FID (2 bajta) ,01'	Značka podpis EF (FID)	3 bajti
xx xx	Dolžina polja vrednosti	2 bajta

Primer podatkov v preneseni datoteki na ESM:

Značka:	Dolžina	Vrednost
00 02 00	00 11	Podatki EF ICC
C1 00 00	00 C2	Podatki EF Card_Certificate
		...
05 05 00	0A 2E	Podatki EF Vehicles_Used
05 05 01	00 80	Podpis EF Vehicles_Used

4. PRENOS PODATKOV S TAHOGRAFSKE KARTICE PREKO ENOTE V VOZILU

- DDP_047 VU mora omogočati prenos vsebine vstavljene voznikove kartice v priključeno IDE.
- DDP_048 IDE za vstop v ta režim pošlje sporočilo ‚zahtevke za prenos podatkov s kartice‘ v VU (glej točko 2.2.2.9).
- DDP_049 VU nato prenese vsebino celotne kartice, po datotekah, v skladu s protokolom prenosa podatkov opredeljenim v točki 3, in posreduje od kartice prejete podatke v IDE v ustreznem formatu datotek TLV (glej točko 3.4.2), v okviru sporočil pozitivnih odgovorov na zahtevke za prenos podatkov.
- DDP_050 IDE očisti podatke iz sprejetih sporočil (tako da odstrani glave, značke SID in TREP, števce delnih sporočil in preskusne vsote) in jih shrani v eni fizični datoteki, kakor je opisano v točki 2.3.
- DDP_051 Nato VU po potrebi posodobi datoteko `Control_Activity_Data` ali `Card_Download` na voznikovi kartici.
-

Dodatek 8

KALIBRACIJSKI PROTOKOL

VSEBINA

1.	Uvod	448
2.	Izrazi, opredelitve in literatura	448
3.	Pregled storitev	448
3.1	Možne storitve	448
3.2	Kode odgovorov	449
4.	Komunikacijske storitve	449
4.1	Storitev StartCommunication	449
4.2	Storitev StopCommunication	451
4.2.1	Opis sporočil	451
4.2.2	Format sporočil	452
4.2.3	Opredelitev parametrov	453
4.3	Storitev TesterPresent	453
4.3.1	Opis sporočil	453
4.3.2	Format sporočil	453
5.	Storitve upravljanja	454
5.1	Storitev StartDiagnosticSession	454
5.1.1	Opis sporočil	454
5.1.2	Format sporočil	455
5.1.3	Opredelitev parametrov	456
5.2	Storitev SecurityAccess	456
5.2.1	Opis sporočil	456
5.2.2	Format sporočil – SecurityAccess – requestSeed	457
5.2.3	Format sporočil – SecurityAccess – sendKey	458
6.	Storitve prenosa podatkov	459
6.1	Storitev DataByIdentifier	459
6.1.1	Opis sporočil	459
6.1.2	Format sporočil	459
6.1.3	Opredelitev parametrov	460
6.2	Storitev WriteDataByIdentifier	461
6.2.1	Opis sporočil	461
6.2.2	Format sporočil	461
6.2.3	Opredelitev parametrov	462
7.	Upravljanje preskusnih pulzov – funkcionalna enota za upravljanje vhodov/izhodov	462
7.1	Storitev InputOutputControlByIdentifier	462

7.1.1	Opis sporočil	462
7.1.2	Format sporočil	463
7.1.3	Opredelitev parametrov	464
8.	Formati dataRecords	465
8.1	Območja prenesenih parametrov	465
8.2	Formati dataRecords	466

1. UVOD

Ta dodatek opisuje, kako se izmenjujejo podatki med enoto v vozilu in preskusno enoto po liniji K, ki je del kalibracijskega vmesnika, opisanega v dodatku 6. Opisano je tudi upravljanje linije vhodno/izhodnih signalov na kalibracijskem konektorju.

Vzpostavitev komunikacij po liniji K je opisano v točki 4 ‚Komunikacijske storitve‘.

V tem dodatku je pri določanju obsega upravljanja linije K v različnih pogojih uporabljen koncept diagnostičnih ‚sej‘. Privzeta vrsta seje je ‚StandardDiagnosticSession‘, pri kateri je mogoče iz enote v vozilu brati vse podatke, v enoto v vozilu pa ni mogoče vpisovati podatkov.

Izbira diagnostične seje je opisana v točki 5 ‚Storitve upravljanja‘.

CPR_001 Vnos podatkov v enoto v vozilu omogoča seja ‚ECUProgrammingSession‘. Za vnos kalibracijskih podatkov (zahtevi 097 in 098) mora biti poleg tega biti enota v vozilu v režimu CALIBRATION.

Prenos podatkov po liniji K je opisan v točki 6 ‚Storitve prenosa podatkov‘. Formati prenašanih podatkov so podrobno opisani v točki 8 ‚Formati dataRecords‘.

CPR_002 Seja ‚ECUAdjustmentSession‘ omogoča izbiro V/I režima kalibracijske V/I linije preko vmesnika linije K. Upravljanje kalibracijske V/I linije je opisano v točki 7 ‚Upravljanje preskusnih pulzov – funkcionalna enota za upravljanje vhodov/izhodov‘.

CPR_003 V tem gradivu je naslov preskuševalnika vedno označen kot ‚tt‘. Lahko se sicer uporablja prednostne naslove preskuševalnika, vendar mora VU pravilno odgovoriti na vsak naslov preskuševalnika. Tipičen naslov VU je 0xEE.

2. IZRAZI, OPREDELITVE IN LITERATURA

Protokoli, sporočila in kode napak v glavnem temeljijo na sedanjem osnutku ISO 14229-1 (Cestna vozila – diagnostični sistemi – del 1: diagnostične storitve, verzija 6 z dne 22. februarja 2001).

Pri identifikatorjih storitev, zahtevkih za storitve in odgovorih ter pri standardnih parametrih se uporablja kodiranje bajtov in šestnajstiške vrednosti.

Izraz ‚preskuševalnik‘ se nanaša na opremo za vnos programskih/kalibracijskih vrednosti v VU.

Izraza ‚odjemalec‘ in ‚strežnik‘ se nanašata na preskuševalnik in VU.

Izraz ECU pomeni ‚elektronsko enoto za upravljanje‘ in se nanaša na VU.

Literatura:

ISO 14230-2: Cestna vozila – diagnostični sistemi – protokol s ključnimi besedami 2000 – del 2: raven podatkovnih povezav. Prva izdaja: 1999. vozila – diagnostični sistemi.

3. PREGLED STORITEV

3.1 Možne storitve

Naslednja tabela podaja pregled storitev, ki jih omogoča zapisovalna naprava in ki so opredeljene v tem gradivu.

CPR_004 Tabela prikazuje storitve, ki so možne v omogočeni diagnostični seji.

— V prvem stolpcu so našteje možne storitve,

— v drugem stolpcu so podane številke točk v tem dodatku, v katerih so storitve podrobneje opredeljene,

- tretji stolpec predpisuje vrednosti identifikatorja storitve za sporočila zahtevkov,
- četrti stolpec predpisuje, katere storitve mora vsaka VU podpirati v seji „StandardDiagnosticSession“(SD),
- peti stolpec predpisuje storitve v seji „ECUAdjustmentSession“ (ECUAS), ki morajo biti vgrajene za upravljanje vhodno/izhodne signalne linije preko kalibracijskega konektorja na čelni plošči VU,
- šesti stolpec predpisuje storitve v seji „ECUProgrammingSession“ (ECUPS), ki morajo biti vgrajene za programiranje parametrov VU.

Tabela 1

Pregledna tabela vrednosti identifikatorjev storitev

Ime diagnostične storitve	Točka	Vrednost reg. SID	Diagnostične seje		
			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		■	

■ Ta simbol pomeni, da je storitev v tej diagnostični seji obvezna.
 Če simbola ni, ta storitev v tej diagnostični seji ni dovoljena.

3.2 Kode odgovorov

Za vsako storitev so opredeljene kode odgovorov.

4. KOMUNIKACIJSKE STORITVE

Vzpostavitev in vzdrževanje komunikacije zahtevata določene storitve. Te storitve ne nastopajo na ravni aplikacije. Možne storitve so opisane v naslednji tabeli:

Tabela 2

Komunikacijske storitve

Ime storitve	Opis
StartCommunication	Odjemalec zahteva začetek komunikacijske seje s strežnikom (strežniki)
StopCommunication	Odjemalec zahteva konec komunikacijske seje
TesterPresent	Odjemalec sporoči, da je preskuševalnik še vedno prisoten

CPR_005 S storitvijo StartCommunication Service se začne komunikacija. Za izvedbo kakršnekoli storitve mora biti komunikacija inicializirana in komunikacijski parametri morajo ustrezati želenemu režimu.

4.1 Storitve StartCommunication

CPR_006 Po sprejemu primitiva StartCommunication mora VU preveriti, ali je zahtevano komunikacijsko povezavo v sedanjem stanju mogoče inicializirati. Veljavni pogoji za inicializacijo komunikacijske povezave so opisani v dokumentu ISO 14230-2.

CPR_007 Nato VU opravi vse potrebno za inicializacijo komunikacijske povezave in pošlje primitiv odgovora StartCommunication s pozitivnimi parametri odgovora.

CPR_008 Če je VU ob sprejemu novega zahtevka StartCommunication (npr. ob odpravi napake v preskuševalniku) že inicializirana (in je že vstopila v kakšno diagnostično sejo), mora zahtevek sprejeti in se ponovno inicializirati.

CPR_009 Če komunikacijske povezave iz kakršnegakoli vzroka ni mogoče inicializirati, mora VU nadaljevati delovanje, v katerem je bila tik pred poskusom inicializacije komunikacijske povezave.

CPR_010 Sporočilo zahtevka StartCommunication mora biti fizično naslovljeno.

CPR_011 Inicializacija VU za storitve se opravi po postopku „hitre inicializacije“.

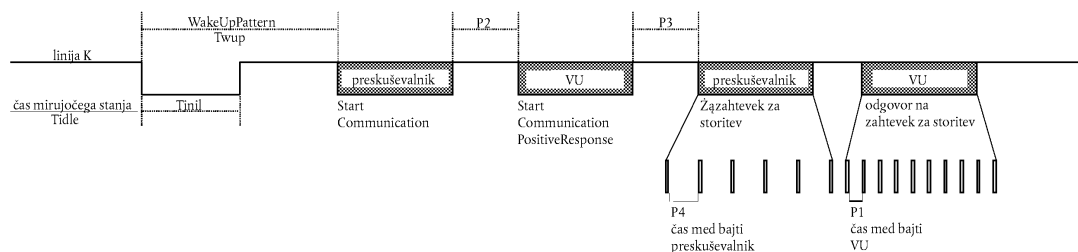
- pred kakršnimkoli dejanjem se pusti določen čas, v katerem je vodilo v mirovnem stanju,
- nato preskuševalnik pošlje inicializacijski vzorec,
- odgovor VU vsebuje vse podatke, potrebne za vzpostavitev komunikacije.

CPR_012 Po zaključku inicializacije:

- so vsi komunikacijski parametri nastavljeni na vrednosti v tabeli 4 glede na ključne bajte,
- VU čaka na prvi zahtevek iz preskuševalnika,
- je VU v privzetem diagnostičnem režimu, tj. v seji StandardDiagnosticSession,
- je kalibracijska V/I signalna linija v privzetem stanju, tj. v onemogočenem stanju.

CPR_014 Hitrost prenosa podatkov po liniji K je 10 400 Baud.

CPR_016 Preskuševalnik sproži inicializacijo tako, da pošlje budilni vzorec (Wup) po liniji K. Vzorec se začne po preteku časa mirujočega stanja linije K, s časom nizkega stanja Tinil. Preskuševalnik pošlje prvi bit zahtevka za storitev StartCommunication po času Twup po prvem upadnem robu.



CPR_017 Časovne nastavitve za hitro inicializacijo in komunikacijo na splošno so prikazane v tabelah v nadaljevanju. Čas mirujočega stanja ima lahko različne vrednosti:

- pri prvem prenosu po vklopu napajanja: $T_{idle} = 300 \text{ ms}$
- po zaključku storitve StopCommunication Service: $T_{idle} = P3 \text{ min}$
- po koncu komunikacije zaradi izteka časovne kontrole P3 maks: $T_{idle} = 0$.

Tabela 3

Časovne nastavitve za hitro inicializacijo

Parameter		najmanjša vrednost	največja vrednost
Tinil	$25 \pm 1 \text{ ms}$	24 ms	26 ms
Twup	$50 \pm 1 \text{ ms}$	49 ms	51 ms

Tabela 4

Časovne nastavitve med komunikacijo

Časovni parameter	Opis parametra	Spodnja mejna vrednost (ms)	Zgornja mejna vrednost (ms)
		najmanj	največ
P1	Čas med bajti odgovora VU	0	20
P2	Čas med zahtevkom preskuševalnika in odgovorom VU ali med dvema odgovoroma VU	25	250
P3	Čas med koncem odgovorov VU in začetkom novega zahtevka preskuševalnika	55	5 000
P4	Čas med bajti zahtevka preskuševalnika	5	20

CPR_018 Format sporočil pri hitri inicializaciji je prikazan v naslednjih tabelah:

Tabela 5

Sporočilo zahtevka StartCommunication

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	81	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvirnega naslova	tt	SRC
#4	Zahtevak za storitev StartCommunication	81	SCR
#5	Preskusna vsota	00-FF	CS

Tabela 6

Pozitivni odgovor na zahtevak StartCommunication

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	ID pozitivnega odgovora storitve StartCommunication	C1	SCRPR
#6	Ključni bajt 1	EA	KB1
#7	Ključni bajt 2	8F	KB2
#8	Preskusna vsota	00-FF	CS

CPR_019 Na sporočilo zahtevka StartCommunication Request ni negativnega odgovora; če ne more poslati pozitivnega odgovora, se VU ne inicializira, ne sporoči ničesar in ostane v svojem normalnem delovanju.

4.2 Storitve StopCommunication

4.2.1 Opis sporočil

Namen te storitve na komunikacijski ravni je končati komunikacijsko sejo.

CPR_020 Po sprejemu primitiva StopCommunication mora VU preveriti, ali je zahtevano komunikacijsko povezavo v sedanjem stanju mogoče končati. V tem primeru VU opravi vse za končanje te komunikacije.

CPR_021 Če je komunikacijo mogoče končati, VU pred koncem komunikacije pošlje primitiv odgovora StopCommunication s pozitivnimi parametri odgovora.

CPR_022 Če komunikacije iz kateregakoli razloga ni mogoče končati, VU pošlje primitiv odgovora StopCommunication z negativnimi parametri odgovora.

CPR_023 Če VU zazna iztek časovne kontrole P3 maks, konča komunikacijo, ne da bi poslala kakršenkoli primitiv odgovora.

4.2.2 **Format sporočil**

CPR_024 Format sporočil pri primitivih StopCommunication je prikazan v naslednjih tabelah:

Tabela 7

Sporočilo zahtevka StopCommunication

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvirnega naslova	tt	SRC
#4	Dodatni bajt dolžine	01	LEN
#5	ID zahtevka za storitev StopCommunication	82	SPR
#6	Preskusna vsota	00-FF	CS

Tabela 8

Pozitivni odgovor na zahtevek StopCommunication

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	01	LEN
#5	ID pozitivnega odgovora storitve StopCommunication	C2	SPRPR
#6	Preskusna vsota	00-FF	CS

Tabela 9

Negativni odgovor na zahtevek StopCommunication

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	ID negativnega odgovora storitve	7F	NR
#6	ID zahtevka za storitev StopCommunication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Preskusna vsota	00-FF	CS

4.2.3 *Opredelitev parametrov*

Ta storitev ne zahteva nobene opredelitve parametrov.

4.3 **Storitev TesterPresent**

4.3.1 *Opis sporočil*

Storitev TesterPresent sproži preskuševalnik. Z njo sporoči strežniku, da je še vedno prisoten, in tako prepreči, da bi se strežnik samodejno vrnil v svoje normalno delovanje in morebiti končal komunikacijo. Ta storitev, ki se jo pošilja redno, vzdržuje diagnostično sejo, saj vsak sprejem zahtevka te storitve ponastavi časovnik P3.

4.3.2 *Format sporočil*

CPR_079 Format sporočil pri primitivih TesterPresent je prikazan v naslednjih tabelah:

Tabela 10

Sporočilo zahtevka TesterPresent

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	02	LEN
#5	ID zahtevka za storitev TesterPresent	3E	TP
#6	Podfunkcija = responseRequired = [da ne]	01 02	RESPREQ_Y RESPREQ_NO
#7	Preskusna vsota	00-FF	CS

CPR_080 Če je parameter responseRequired nastavljen na ‚da‘, mora strežnik odgovoriti z naslednjim sporočilom pozitivnega odgovora. Če je nastavljen na ‚ne‘, strežnik ne pošlje nikakršnega odgovora.

Tabela 11

Pozitivni odgovor na zahtevek TesterPresent

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	01	LEN
#5	ID pozitivnega odgovora storitve TesterPresent	7E	TPPR
#6	Preskusna vsota	00-FF	CS

CPR_081 Storitev mora podpirati naslednje kode negativnih odgovorov:

Tabela 12

Negativni odgovor na zahtevek TesterPresent

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	ID negativnega odgovora storitve	7F	NR
#6	ID zahtevka za storitev TesterPresent	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat incorrectMessageLength]	12	RC_SFNS_IF
		13	RC_IML
#8	Preskusna vsota	00-FF	CS

5. STORITVE UPRAVLJANJA

Možne storitve so opisane v naslednji tabeli:

Tabela 13

Storitve upravljanja

Ime storitve	Opis
StartDiagnosticSession	Odjemalec zahteva začetek diagnostične seje z VU
SecurityAccess	Odjemalec zahteva varni dostop do funkcije, katere uporaba je omejena na pooblaščen uporabnike

5.1 Storitev StartDiagnosticSession

5.1.1 Opis sporočil

CPR_025 Storitev StartDiagnosticSession služi za to, da se v strežniku omogoči različne diagnostične seje. Diagnostična seja omogoči določen nabor storitev po tabeli 17. Seja lahko omogoči tudi posebne storitve, ki jih določi proizvajalec; take storitve v tem dokumentu niso opisane. Pravila izvedbe morajo izpolnjevati naslednje zahteve:

- v VU mora biti ves čas aktivna natanko ena diagnostična seja,
- ob vklopu napajanja mora VU vedno začeti sejo StandardDiagnosticSession. Če ni sprožena nobena druga diagnostična seja, mora seja StandardDiagnosticSession teči, dokler je vključeno napajanje VU,
- če preskuševalnik zahteva začetek določene diagnostične seje, ki pa že teče, mora VU poslati sporočilo pozitivnega odgovora,
- kadarkoli preskuševalnik zahteva novo diagnostično sejo, pred aktiviranjem te nove seje v VU ta vedno pošlje sporočilo pozitivnega odgovora StartDiagnosticSession. Če VU ne more začeti zahtevane nove diagnostične seje, mora poslati sporočilo negativnega odgovora StartDiagnosticSession in nadaljevati tekočo sejo.

CPR_026 Diagnostična seja se sme začeti le, če je med odjemalcem in VU že vzpostavljena komunikacija.

CPR_027 Po uspešni storitvi StartDiagnosticSession morajo biti aktivne v tabeli 4 prikazane časovne nastavitve, parameter diagnosticSession pa nastavljen na „StandardDiagnosticSession“ iz sporočila zahtevka, če je bila prej aktivna kakšna druga diagnostična seja.

5.1.2 **Format sporočil**

CPR_028 Formati sporočil pri primitivih StartDiagnosticSession so prikazani v naslednjih tabelah:

Tabela 14

Sporočilo zahtevka StartDiagnosticSession

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvirnega naslova	tt	SRC
#4	Dodatni bajt dolžine	02	LEN
#5	ID zahtevka za storitev StartDiagnosticSession	10	STDS
#6	diagnosticSession = (ena od vrednosti iz tabele 17)	xx	DS_...
#7	Preskusna vsota	00-FF	CS

Tabela 15

Pozitivni odgovor na zahtevek StartDiagnosticSession

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	02	LEN
#5	ID pozitivnega odgovora storitve StartDiagnosticSession	50	STDSPR
#6	DiagnosticSession = (ista vrednost kot v bajtu #6 v tabeli 14)	xx	DS_...
#7	Preskusna vsota	00-FF	CS

Tabela 16

Negativni odgovor na zahtevek StartDiagnosticSession

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	ID negativnega odgovora storitve	7F	NR
#6	ID zahtevka za storitev StartDiagnosticSession	10	STDS
#7	ResponseCode = (subFunctionNotSupported ^(a))	12	RC_SFNS
	incorrectMessageLength ^(b)	13	RC_IML
	conditionsNotCorrect ^(c)	22	RC_CNC
#8	Preskusna vsota	00-FF	CS

^(a) Vrednost v bajtu #6 sporočila zahtevka ni podprta, tj. ni je v tabeli 17.

^(b) Dolžina sporočila ni pravilna.

^(c) Kriteriji za zahtevek niso izpolnjeni..

5.1.3 Opredelitev parametrov

CPR_029 Storitev StartDiagnosticSession uporablja parameter *diagnosticSession* (DS_) za izbiro posebnega obnašanja strežnika (strežnikov). V tem dokumentu so predpisane naslednje diagnostične seje:

Tabela 17

Opredelitev vrednosti *diagnosticSession*

Šestnaj-stiško	Opis	Mnemonik
81	StandardDiagnosticSession Ta diagnostična seja omogoča vse storitve, predpisane v stolpcu 4, 'SD', tabele 1. Te storitve omogočajo branje podatkov iz strežnika (VU). Ta diagnostična seja je aktivna po uspešni inicializaciji odjemaca (preskuševalnika) in strežnika (VU). To diagnostično sejo lahko nadomestijo druge diagnostične seje, predpisane v tej točki.	SD
85	ECUProgrammingSession Ta diagnostična seja omogoča vse storitve, predpisane v stolpcu 6, 'ECUPS', tabele 1. Te storitve podpirajo programiranje strežnika (VU). To diagnostično sejo lahko nadomestijo druge diagnostične seje, predpisane v tej točki.	ECUPS
87	ECUAdjustmentSession Ta diagnostična seja omogoča vse storitve, predpisane v stolpcu 5, 'ECUAS', tabele 1. Te storitve omogočajo upravljanje vhodov/izhodov strežnika (VU). To diagnostično sejo lahko nadomestijo druge diagnostične seje, predpisane v tej točki.	ECUAS

5.2 Storitve SecurityAccess

Če VU ni v režimu CALIBRATION, ni mogoče vpisovanje kalibracijskih parametrov ali dostopanje do kalibracijske vhodno/izhodne linije. Pred odobritvijo vstopa v režim CALIBRATION je treba poleg vstavitve veljavne delavniške kartice v VU tudi vnesti ustrezen PIN v VU.

Storitev SecurityAccess omogoča uporabniku vnesti PIN, preskuševalniku pa ugotoviti, ali je VU v režimu CALIBRATION ali ne.

Dopustno je tudi omogočiti vnos PIN na kak drug način.

5.2.1 Opis sporočil

Storitev SecurityAccess obsega sporočilo SecurityAccess 'requestSeed', ki mu nato sledi sporočilo SecurityAccess 'sendKey'. Storitve SecurityAccess je treba izvesti po storitvi StartDiagnosticSession.

CPR_033 Preskuševalnik uporabi sporočilo SecurityAccess 'requestSeed' za to, da preveri, ali je enota v vozilu pripravljena na sprejem PIN.

CPR_034 Če je enota v vozilu že v režimu CALIBRATION, odgovori na zahtevek tako, da pošlje 'seme' 0x0000 s storitvijo pozitivnega odgovora na zahtevek SecurityAccess.

CPR_035 Če je enota v vozilu pripravljena na sprejem PIN za preveritev delavniške kartice, odgovori na zahtevek tako, da pošlje 'seme' večje od 0x0000 s storitvijo pozitivnega odgovora na zahtevek SecurityAccess.

CPR_036 Če enota v vozilu ni pripravljena na sprejem PIN od preskuševalnika, bodisi zato, ker vstavljena delavniška kartica ni veljavna ali ker delavniška kartica ni vstavljena, ali ker enota v vozilu pričakuje vnos PIN na kak drug način, odgovori na zahtevek z negativnim odgovorom s kodo odgovora nastavljeno na conditionsNotCorrectOrRequestSequenceError.

CPR_037 Preskuševalnik nato morebiti uporabi sporočilo SecurityAccess 'sendKey' za to, da posreduje PIN enoti v vozilu. Da zagotovi zadosten čas za izvedbo procesa avtentifikacije kartice, mora VU podaljšati čas za odgovor z negativnim odgovorom s kodo requestCorrectlyReceived-ResponsePending. Največji čas do odgovora pa ne sme preseči 5 minut. Takoj po izvršitvi zahtevane storitve VU pošlje sporočilo pozitivnega odgovora ali sporočilo negativnega odgovora z drugačno kodo. VU lahko ponavlja negativne odgovore s kodo requestCorrectlyReceived-ResponsePending, dokler ne izvrši zahtevane storitve, nato pa pošlje končno sporočilo odgovora.

CPR_038 Enota v vozilu odgovori na ta zahtevek s pozitivnim odgovorom na zahtevek SecurityAccess le, kadar je v režimu CALIBRATION.

CPR_039 V naslednjih primerih enota v vozilu odgovori na ta zahtevek z negativnim odgovorom, koda odgovora pa je nastavljena na naslednje vrednosti:

- subFunctionNot supported: nepravilen format parametra podfunkcije (accessType),
- conditionsNotCorrectOrRequestSequenceError: enota v vozilu ni pripravljena na vnos PIN,
- invalidKey: PIN ni veljaven in število dovoljenih poskusov vnosa PIN še ni preseženo,
- exceededNumberOfAttempts: PIN ni veljaven in število dovoljenih poskusov vnosa PIN je preseženo,
- generalReject: PIN pravilen, ni pa uspela medsebojna avtentifikacija z delavniško kartico.

5.2.2 Format sporočil – SecurityAccess – requestSeed

CPR_040 Format sporočil pri primitivih SecurityAccess ,requestSeed' je prikazan v naslednjih tabelah:

Tabela 18

Sporočilo zahtevka SecurityAccess – requestSeed

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvirnega naslova	tt	SRC
#4	Dodatni bajt dolžine	02	LEN
#5	ID zahtevka za storitev SecurityAccess	27	SA
#6	accessType – requestSeed	7D	AT_RSD
#7	Preskusna vsota	00-FF	CS

Tabela 19

Pozitivni odgovor na zahtevek SecurityAccess – requestSeed

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	04	LEN
#5	ID pozitivnega odgovora na zahtevek SecurityAccess	67	SAPR
#6	accessType – requestSeed	7D	AT_RSD
#7	SeedHigh	00-FF	SEEDH
#8	SeedLow	00-FF	SEEDL
#9	Preskusna vsota	00-FF	CS

Tabela 20

Negativni odgovor na zahtevek SecurityAccess

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	ID negativnega odgovora	7F	NR
#6	ID zahtevka za storitev SecurityAccess	27	SA
#7	responseCode = (conditionsNotCorrectOrRequestSequenceError incorrectMessageLength)	22	RC_CNC
		13	RC_IML
#8	Preskusna vsota	00-FF	CS

5.2.3 Format sporočil – SecurityAccess – sendKey

CPR_041 Format sporočil pri primitivih SecurityAccess 'sendKey' je prikazan v naslednjih tabelah:

Tabela 21

Sporočilo zahtevka SecurityAccess – sendKey

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvirnega naslova	tt	SRC
#4	Dodatni bajt dolžine	m+2	LEN
#5	ID zahtevka za storitev SecurityAccess	27	SA
#6	accessType – sendKey	7E	AT_SK
#7-(#m+6)	Key#1 (višji del vrednosti)	xx	KEY
	...	...	
	Key #m (nižji del vrednosti; 'm' mora biti najmanj 4 in največ 8)	xx	
#m+7	Preskusna vsota	00-FF	CS

Tabela 22

Pozitivni odgovor SecurityAccess – sendKey

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	02	LEN
#5	ID pozitivnega odgovora na zahtevek SecurityAccess	67	SAPR
#6	accessType – sendKey	7E	AT_SK
#7	Preskusna vsota	00-FF	CS

Tabela 23

Negativni odgovor na zahtevek SecurityAccess

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	ID negativnega odgovora	7F	NR
#6	ID zahtevka za storitev SecurityAccess	27	SA
#7	ResponseCode = (generalReject subFunctionNotSupported incorrectMessageLength conditionsNotCorrectOrRequestSequenceError invalidKey exceededNumberOfAttempts requestCorrectlyReceived-ResponsePending)	10 12 13 22 35 36 78	RC_GR RC_SFNS RC_IML RC_CNC RC_IK RC_ENA RC_RCR_RP
#8	Preskusna vsota	00-FF	CS

6. STORITVE PRENOSA PODATKOV

Možne storitve so opisane v naslednji tabeli:

Tabela 24

Storitve prenosa podatkov

Ime storitve	Opis
ReadDataByIdentifier	Odjemalec zahteva prenos sedanje vrednosti zapisa, katerega dostop določa recordDataIdentifier
WriteDataByIdentifier	Odjemalec zahteva vpis zapisa, katerega dostop določa recordDataIdentifier

6.1 Storitev ReadDataByIdentifier**6.1.1 Opis sporočil**

CPR_050 Storitev ReadDataByIdentifier uporablja odjemalec za to, da od strežnika zahteva vrednosti podatkovnih zapisov. Podatke določa recordDataIdentifier. Proizvajalec VU odgovarja za to, da so med izvajanjem te storitve izpolnjeni pogoji na strežniku.

6.1.2 Format sporočil

CPR_051 Format sporočil pri primitivih ReadDataByIdentifier je prikazan v naslednjih tabelah:

Tabela 25

Sporočilo zahtevka ReadDataByIdentifier

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	ID zahtevka za storitev ReadDataByIdentifier	22	RDBI
#6 in #7	recordDataIdentifier = (ena od vrednosti iz tabele 28)	xxxx	RDI_...
#8	Preskusna vsota	00-FF	CS

Tabela 26

Pozitivni odgovor na zahtevek ReadDataByIdentifier

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	m+3	LEN
#5	ID pozitivnega odgovora storitve ReadDataByIdentifier	62	RDBIPR
#6 in #7	recordDataIdentifier = (ista vrednost kot v bajtih #6 in #7 v tabeli 25)	xxxx	RDI_...
#8 do #m+7	dataRecord() = (data#1 : data#m)	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Preskusna vsota	00-FF	CS

Tabela 27

Negativni odgovor na zahtevek ReadDataByIdentifier

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	ID negativnega odgovora	7F	NR
#6	ID zahtevka za storitev ReadDataByIdentifier	22	RDBI
#7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Preskusna vsota	00-FF	CS

6.1.3 Opredelitev parametrov

CPR_052 Parameter recordDataIdentifier (RDI_) v sporočilu zahtevka ReadDataByIdentifier določa podatkovni zapis.

CPR_053 Vrednosti parametra recordDataIdentifier, opredeljene v tem dokumentu, so prikazane v spodnji tabeli.

Tabela parametrov recordDataIdentifier obsega štiri stolpce in več vrstic.

- V prvem stolpcu (Šestnajstiško) so podane šestnajstiške vrednosti, dodeljene parametrom recordDataIdentifier predpisanim v tretjem stolpcu.
- Drugi stolpec (Podatkovni element) prikazuje podatkovne elemente iz dodatka 1, na katerih temelji parameter recordDataIdentifier (v nekaterih primerih je potrebno prekodiranje).
- Tretji stolpec (Opis) prikazuje ime parametra recordDataIdentifier.
- Četrty stolpec (Mnemonik) prikazuje mnemonik tega parametra recordDataIdentifier.

Tabela 28

Opredelitev vrednosti recordDataIdentifier

Šest-naj-stiško	Podatkovni element	ime recordDataIdentifier (format opisan v 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 Parameter dataRecord (DREC_) se pošlje s sporočilom pozitivnega odgovora ReadDataByIdentifier in podaja odjemalcu (preskuševalniku) vrednost podatkovnega zapisa, ki ga določa parameter recordDataIdentifier. Formati podatkov so predpisani v točki 8. Lahko so podprti tudi drugi neobvezni parametri dataRecords, npr. vhodni, notranji in izhodni podatki, specifični za posamezno VU, vendar v tem dokumentu niso opredeljeni.

6.2 Storitev StartDiagnosticSession**6.2.1 Opis sporočil**

CPR_056 Storitev WriteDataByIdentifier uporablja odjemalec za to, da v strežnik zapiše vrednosti podatkovnih zapisov. Podatke določa recordDataIdentifier. Proizvajalec VU odgovarja za to, da so med izvajanjem te storitve izpolnjeni pogoji na strežniku. Za posodobitev parametrov v tabeli 28 mora biti VU v režimu CALIBRATION.

6.2.2 Format sporočil

CPR_057 Format sporočil pri primitivih WriteDataByIdentifier je prikazan v naslednjih tabelah:

Tabela 29

Sporočilo zahtevka WriteDataByIdentifier

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	m+3	LEN
#5	ID zahtevka za storitev WriteDataByIdentifier	2E	WDBI
#6 in #7	recordDataIdentifier = (ena od vrednosti iz tabele 28)	xxxx	RDI_...
#8 do #m+7	dataRecord() = (data#1 : data#m)	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Preskusna vsota	00-FF	CS

Tabela 30

Pozitivni odgovor na zahtevek WriteDataByIdentifier

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	ID pozitivnega odgovora na zahtevek WriteDataByIdentifier	6E	WDBIPR
#6 in #7	recordDataIdentifier = (ista vrednost kot v bajtih #6 in #7 v tabeli 29)	xxxx	RDI_...
#8	Preskusna vsota	00-FF	CS

Tabela 31

Negativni odgovor na zahtevek WriteDataByIdentifier

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	ID negativnega odgovora	7F	NR
#6	ID zahtevka za storitev WriteDataByIdentifier	2E	WDBI
#7	ResponseCode = (requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect)	22	RC_CNC
#8	Preskusna vsota	00-FF	CS

6.2.3 Opredelitev parametrov

Parameter recordDataIdentifier (RDI_) je opredeljen v tabeli 28.

Parameter dataRecord (DREC_) se pošlje s sporočilom zahtevka WriteDataByIdentifier in podaja strežniku (VU) vrednosti podatkovnih zapisov, ki jih določa parameter recordDataIdentifier. Formati podatkov so predpisani v točki 8.

7. UPRAVLJANJE PRESKUSNIH PULZOV – FUNKCIONALNA ENOTA ZA UPRAVLJANJE VHODOV/IZHODOV

Možne storitve so opisane v naslednji tabeli:

Tabela 32

Funkcionalna enota za upravljanje vhodov/izhodov

Ime storitve	Opis
InputOutputControlByIdentifier	Odjemalec zahteva upravljanje določenega vhoda/izhoda strežnika

7.1 Opis sporočil**7.1.1 Opis sporočil**

Po zvezi preko konektorja na čelni plošči je mogoče z ustreznim preskuševalnikom upravljati ali nadzirati preskusne pulze.

CPR_058 To kalibracijsko V/I linijo se lahko konfigurira z ukazom za linijo K s storitvijo InputOutputControlByIdentifier; s tem se izbere želeno vhodno ali izhodno funkcijo linije. Možna stanja linije so:

- onemogočena,
- speedSignalInput, pri čemer se kalibracijska V/I signalna linija uporablja za vnos signala hitrosti (preskusnega signala), ki nadomešča signal zaznavala gibanja,
- speedSignalInput, pri čemer se kalibracijska V/I signalna linija uporablja za iznos signala hitrosti zaznavala gibanja,
- RTCOutput, pri čemer se kalibracijska V/I signalna linija uporablja za iznos urnega signala UTC.

CPR_059 Enota v vozilu mora biti za konfiguriranje stanja linije v seji nastavljanja in v režimu CALIBRATION. Ob izstopu iz seje nastavljanja ali iz režima CALIBRATION mora enota v vozilu zagotoviti vrnitev kalibracijske V/I linije v ,onemogočeno'(privzeto) stanje.

CPR_060 Če VU prejme hitrostne pulze po normalni vhodni signalni liniji pri tem, ko je kalibracijska V/I linija nastavljena na stanje vhoda, mora kalibracijsko V/I linijo nastaviti v stanje izhoda ali vrniti v onemogočeno stanje.

CPR_061 Zaporedje je naslednje:

- vzpostavitev komunikacij s storitvijo StartCommunication
- vstop v sejo nastavljanja s storitvijo StartDiagnosticSession in vstop v režim delovanja CALIBRATION (zaporedje teh dveh vstopov ni pomembno).
- sprememba stanja v stanje izhoda s storitvijo InputOutputControlByIdentifier.

7.1.2 Format sporočil

CPR_062 Format sporočil pri primitivih InputOutputControlByIdentifier je prikazan v naslednjih tabelah:

Tabela 33

Sporočilo zahtevka InputOutputControlByIdentifier

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	xx	LEN
#5	SID zahtevka InputOutputControlByIdentifier	2F	IOCBI
#6 in #7	InputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 ali #8 do #9	ControlOptionRecord = (inputOutputControlParameter – ena od vrednosti iz tabele 36 controlState – ena od vrednosti iz tabele 38 (glej opombe spodaj))	xx	COR_... IOCP_...
		xx	CS_...
#9 ali #10	Preskusna vsota	00-FF	CS

Opomba: Parameter controlState je prisoten le v nekaterih primerih (glej točko 7.1.3).

Tabela 34

Pozitivni odgovor na zahtevek InputOutputControlByIdentifier

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	xx	LEN
#5	SID pozitivnega odgovora na zahtevek InputOutputControlByIdentifier	6F	IOCBIPR
#6 in #7	inputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 ali #8 do #9	controlStatusRecord = (inputOutputControlParameter (ista vrednost kot vrednost bajta #8 v tabeli 33)	xx	CSR_ IOCP_...
	controlState (ista vrednost kot vrednost bajta #9 v tabeli 33)) (če pride v poštev)	xx	CS_...
#9 ali #10	Preskusna vsota	00-FF	CS

Tabela 35

Negativni odgovor na zahtevek InputOutputControlByIdentifier

Bajt #	Ime parametra	Šestnajstiška vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvirnega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	SID negativnega odgovora	7F	NR
#6	SID zahtevka InputOutputControlByIdentifier	2F	IOCB I
#7	responseCode = (incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded)	7A	RC_DCLE
#8	Preskusna vsota	00-FF	CS

7.1.3 Opredelitev parametrov

CPR_064 Parameter inputOutputControlParameter (IOCP_) je opredeljen v naslednji tabeli:

Tabela 36

Opredelitev vrednosti parametra inputOutputControlParameter

Šestnajstiško	Opis	Mnemonik
00	ReturnControlToECU Ta vrednost kaže strežniku (VU), da preskuševalnik ne upravlja več kalibracijske V/I signalne linije.	RCTECU
01	ResetToDefault Ta vrednost sporoča strežniku (VU), naj ponastavi kalibracijsko V/I signalno linijo v njeno privzeto stanje.	RTD
03	ShortTermAdjustment Ta vrednost sporoča strežniku (VU), naj nastavi kalibracijsko V/I signalno linijo na vrednost, ki jo vsebuje parameter controlState.	STA

CPR_065 Parameter controlState je prisoten le, kadar je parameter inputOutputControlParameter nastavljen na ShortTermAdjustment, opredeljen pa je v naslednji tabeli:

Tabela 37

Opredelitev vrednosti controlState

Režim	Šestnajstiška vrednost	Opis
Onemogočeno	00	V/I linija je onemogočena (privzeto stanje)
Omogočeno	01	Omogočenje kalibracijske V/I linije kot linije za speedSignalInput
Omogočeno	02	Omogočenje kalibracijske V/I linije kot linije za ealTimeSpeedSignalOutputSensor
Omogočeno	03	Omogočenje kalibracijske V/I linije kot linije za RTCOutput

8. FORMATI DATARECORDS

Ta točka opisuje:

- splošna pravila glede območij parametrov, ki jih enota v vozilu pošilja v preskuševalnik,
- formate, ki jih je treba uporabljati za podatke, ki se prenašajo s storitvami prenosa podatkov opisanimi v točki 6.

CPR_067 VU mora podpirati vse našteje parametre.

CPR_068 Podatki, ki jih VU pošlje v preskuševalnik z odgovorom na sporočilo zahtevka, morajo biti merjeni podatki (tj. tekoča vrednost zahtevanega parametra, kakršno meri ali zaznava VU).

8.1 Območja prenesenih parametrov

CPR_069 Tabela 38 opredeljuje območja, ki se jih uporablja za ugotavljanje veljavnosti prenesenih parametrov.

CPR_070 Vrednosti v območju „znak napake“ služijo VU za takojšnje sporočanje, da trenutno zaradi kake napake na zapisovalni napravi nima na voljo veljavnih vrednosti parametrov.

CPR_071 Vrednosti v območju „ni na voljo“ služijo VU za pošiljanje sporočila, ki vsebuje parameter, ki ga nima na voljo ali v trenutnem režimu ni podprt. Vrednosti v območju „ni zahtevano“ služijo napravi za pošiljanje komandnega sporočila in določitev tistih parametrov, za katere od sprejemne naprave ne pričakuje odgovora.

CPR_072 Če napaka določenega sestavnega dela onemogoča prenos veljavne vrednosti kakega parametra, se namesto podatkov tega parametra uporabi znak napake, opisan v tabeli 38. Če pa meritev ali izračun da vrednost, ki je veljavna, vendar leži zunaj opredeljenega območja parametra, se znaka napake ne uporablja. Tak podatek se prenese z uporabo ustrezne najmanjše ali največje vrednosti parametra.

Tabela 38

Območja dataRecords

Ime območja	1 bajt (šestnajstiška vrednost)	2 bajta (šestnajstiška vrednost)	4 bajtai (šestnajstiška vrednost)	ASCII
Veljaven signal	00 do FA	0000 do FAFF	00000000 do FAFFFFFF	1 do 254
Specifični znak parametra	FB	FB00 do FBFF	FB000000 do FBFFFFFF	noben
Rezervirano območje za prihodnje označevalne bite	FC do FD	FC00 do FDFF	FC000000 do FDFFFFFF	noben
Znak napake	FE	FE00 do FEFF	FE000000 do FEFFFFFF	0
Ni na voljo ali ni zahtevan	FF	FF00 do FFFF	FF000000 do FFFFFFFF	FF

CPR_073 Pri ASCII kodiranih parametrih je ASCII znak *,* rezerviran za ločilo.

8.2 Formati dataRecords

Spodnje tabele 40 do 44 prikazujejo formate, ki se jih uporablja pri storitvah ReadDataByIdentifier in WriteDataByIdentifier.

CPR_074 Tabela 40 podaja dolžino, ločljivost in delovno območje vseh parametrov, ki jih določajo identifikatorji recordDataIdentifier:

Tabela 39

Format dataRecords

Ime parametra	Dolžina podatkov (bajtov)	Ločljivost	Delovno območje
TimeDate	8	(podrobnosti v tabeli 40)	
HighResolutionTotalVehicleDistance	4	ojačitev 5 m/bit, zamik 0 m	0 do + 21 055 406 km
Kfactor	2	ojačitev 0,001 pulzov/m/bit, zamik 0	0 do 64.255 pulzov/m
LfactorTyreCircumference	2	ojačitev 0,125 10 ⁻³ /bit, zamik 0	0 do 8 031 m
WvehicleCharacteristicFactor	2	ojačitev 0,001 pulzov/m/bit, zamik 0	0 do 64.255 pulzov/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	(podrobnosti v tabeli 41)	
SpeedAuthorised	2	ojačitev 1/256 km/h/bit, zamik 0	0 do 250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	(podrobnosti v tabeli 44)	
VIN	17	ASCII	ASCII

CPR_075 Tabela 40 opisuje formate različnih bajtov parametra TimeDate:

Tabela 40

Podrobni format parametra TimeDate (vrednost recordDataIdentifier # F00B)

Bajt	Opredelitev parametra	Ločljivost	Delovno območje
1	Sekunde	ojačitev 0,25 s/bit, zamik 0 s	0 do 59,75 s
2	Minute	ojačitev 1 min/bit, zamik 0 min	0 do 59 min
3	Ure	ojačitev 1 h/bit, zamik 0 h	0 do 23 h
4	Mesec	ojačitev 1 mesec/bit, zamik 0 mesecev	mesec 1 do 12
5	Dan	ojačitev 0,25 dneva/bit, zamik 0 dni (glej opombo pod tabelo 41)	0,25 do 31,75 dni
6	Leto	ojačitev 1 leto/bit, zamik +1985 let (glej opombo pod tabelo 41)	leto 1985 do 2235
7	Lokalni zamik minut	ojačitev 1 min/bit, zamik –125 min	–59 do 59 min
8	Lokalni zamik ur	ojačitev 1 h/bit, zamik –125 h	–23 do +23 h

CPR_076 Tabela 41 opisuje formate različnih bajtov parametra NextCalibrationDate:

Tabela 41

Podrobni format parametra NextCalibrationDate (vrednost recordDataIdentifier # F022)

Bajt	Opredelitev parametra	Ločljivost	Delovno območje
1	Mesec	ojačitev 1 mesec/bit, zamik 0 mesecev	mesec 1 do 12
2	Dan	ojačitev 0,25 dneva/bit, zamik 0 dni (glej spodnjo opombo)	0,25 do 31,75 dni
3	Leto	ojačitev 1 leto/bit, zamik +1985 let (glej spodnjo opombo)	leto 1985 do 2235

Opomba glede uporabe parametra „Dan“:

1. Vrednost datuma 0 je prazna vrednost. Vrednosti 1, 2, 3 in 4 pomenijo prvi dan v mesecu, vrednosti 5, 6, 7, in 8 pomenijo drugi dan v mesecu itd.
2. Ta parameter ne vpliva na parameter ur in ga ne spreminja.

Opomba glede uporabe parametra „Leto“:

Vrednost parametra „Leto“ 0 pomeni leto 1985; vrednost 1 pomeni leto 1986 itd.

CPR_078 Tabela 42 opisuje formate različnih bajtov parametra VehicleRegistrationNumber:

Tabela 42

Podrobni format parametra VehicleRegistrationNumber (vrednost recordDataIdentifier # F07E)

Bajt	Opredelitev parametra	Ločljivost	Delovno območje
1	Kodna stran (opredeljena v dodatku 1)	ASCII	01 do 0A
2 do 14	Registrska številka vozila (opredeljena v dodatku 1)	ASCII	ASCII

Dodatek 9

ODOBTITEV TIP A – SEZNAM OBVEZNIH PRESKUSOV

VSEBINA

1.	Uvod	469
1.1	Odobritev tipa	469
1.2	Literatura	469
2.	Funkcionalni preskusi enote v vozilu	470
3.	Funkcionalni preskusi zaznavala gibanja	473
4.	Funkcionalni preskusi tahografske kartice	475
5.	Preskusi skupne uporabnosti	476

1. UVOD

1.1 Odobritev tipa

EGS-dobritev tipa zapisovalne naprave (ali njenega sestavnega dela) ali tahografske kartice temelji na:

- varnostnem certificiranju, s katerim organ ITSEC ugotovi, ali so varnostni cilji izpolnjeni popolnoma v skladu s dodatkom 10 te priloge,
- funkcionalnem certificiranju, s katerim organ države članice potrdi, da preskušana oprema izpolnjuje zahteve te priloge glede izvajanja funkcij, točnosti meritev in okoljskih lastnosti,
- certificiranju skupne uporabnosti, s katerim pristojni organ potrdi, da je zapisovalna naprava (ali tahografska kartica) v celoti skupno uporabna z zahtevanimi modeli tahografskih kartic (ali zapisovalne naprave) (glej poglavje VIII te priloge).

Ta dodatek predpisuje, katere preskuse mora (najmanj) opraviti organ države članice v okviru funkcionalnega preskušanja, in katere preskuse mora (najmanj) opraviti pristojni organ v okviru preskušanja skupne uporabnosti. Postopki izvedbe preskusov in vrste preskusov niso podrobneje predpisani.

Ta dodatek ne obravnava vidikov varnostnega certificiranja. Če so bili določeni preskusi, predpisani za odobritev tipa, opravljeni že v procesu varnostne presoje in varnostnega certificiranja, teh preskusov ni potrebno opraviti še enkrat. V takem primeru se lahko pregleda zgolj rezultate teh preskusov. V informacijo so zahteve, katerih preskušanje se pričakuje (ali so tesno povezane s preskusi, katerih izvedba se pričakuje), v tem dodatku označene z *,*.

Ta dodatek ločeno obravnava odobritev tipa zaznavala gibanja in odobritev tipa enote v vozilu kot sestavnih delov zapisovalne naprave. Ni zahtevana skupna uporabnost vsakega modela zaznavala gibanja in vsakega modela enote v vozilu, zato se lahko odobritev tipa zaznavala gibanja izda le skupaj s odobritvijo tipa enote v vozilu in obratno.

1.2 Literatura

V tem dodatku so uporabljeni naslednji viri:

- | | |
|---------------|--|
| IEC 68-2-1 | Okoljsko preskušanje – Del 2: Preskusi – Preskusi A: Hladni. 1990 +Dopolnitev 2: 1994. |
| IEC 68-2-2 | Okoljsko preskušanje – Del 2: Preskusi – Preskusi B: Suha vročina. 1974 +Dopolnitev 2: 1994. |
| IEC 68-2-6 | Osnovni postopki okoljskega preskušanja – Preskusne metode – Preskus Fc in smernice: Tresljaji (sinusni). 6. izdaja: 1985. |
| IEC 68-2-14 | Osnovni postopki okoljskega preskušanja – Preskusne metode – Preskus N: Sprememba temperature. Sprememba 1: 1986. |
| IEC 68-2-27 | Osnovni postopki okoljskega preskušanja – Preskusne metode – Preskus Ea in smernice: Udarci. 3. izdaja: 1987. |
| IEC 68-2-30 | Osnovni postopki okoljskega preskušanja – Preskusne metode – Preskus Db in smernice: Vlažna vročina, ciklična (cikel 12 + 12 ur). Sprememba 1: 1985. |
| IEC 68-2-35 | Osnovni postopki okoljskega preskušanja – Preskusne metode – Preskus Fda: Naključni širokopasovni tresljaji – ponovljivost visoka. Sprememba 1: 1983. |
| IEC 529 | Stopnje zaščite ohišij (pravilnik IP). 2. izdaja: 1989. |
| IEC 61000-4-2 | Elektromagnetna združljivost (EMC) – Tehnike preskušanja in merjenja – Preskus odpornosti proti elektrostatskim razelektritvam: 1995 / Dopolnitev 1: 1998. |
| ISO 7637-1 | Cestna vozila – Električne motnje zaradi prevodnosti in stikov – Del 1: Osebna vozila in lahka gospodarska vozila z nazivno napajalno napetostjo 12 V – Prehodnao električna prevodnost samo po napajalnih vodih. 2. izdaja: 1990. |

- ISO 7637-2 Cestna vozila – Električne motnje zaradi prevodnosti in stikov – Del 1: Osebna vozila in lahka gospodarska vozila z nazivno napajalno napetostjo 12 V – Prehodna električna prevodnost samo po napajalnih vodih. 2. izdaja: 1990.
- ISO 7637-3 Cestna vozila – Električne motnje zaradi prevodnosti in stikov – Del 3: Vozila z napajalno napetostjo 12 V ali 24 V – Prehodni električni prenos s kapacitivnimi in induktivnimi stiki po drugih vodih (ne napajalnih). Prva izdaja: 1995 + popr. 1: 1995.
- ISO/IEC 7816-1 Identifikacijske kartice – kontaktne kartice s tiskanimi vezji – Del 1: Fizične lastnosti. Prva izdaja: 1998.
- ISO/IEC 7816-2 Informacijska tehnologija – Identifikacijske kartice – Kontaktne kartice s tiskanimi vezji – Del 2: Mere in položaj kontaktov. Prva izdaja: 1999.
- ISO/IEC 7816-3 Informacijska tehnologija – Identifikacijske kartice – Kontaktne kartice s tiskanimi vezji – Del 3: Elektronski signali in protokoli prenosa. 2. izdaja: 1997.
- ISO/IEC 10373 Identifikacijske kartice – Metode preskušanja. Prva izdaja: 1993.

2. FUNKCIONALNI PRESKUSI ENOTE V VOZILU

Št.	Preskus	Opis	Povezane zahteve
1.	Administrativni pregled		
1.1	Dokumentacija	Pravilnost dokumentacije	
1.2	Rezultati proizvajalčevih preskusov	Rezultati proizvajalčevih preskusov med sestavljanjem. Papirna dokazila	070, 071, 073
2.	Vizualni pregled		
2.1	Skladnost z dokumentacijo		
2.2	Identifikacija/oznake		168, 169
2.3	Gradiva		163 do 167
2.4	Plombiranje		251
2.5	Zunanji vmesniki		
3.	Funkcionalni preskusi		
3.1	Zagotovljene funkcije		002, 004, 244
3.2	Režimi delovanja		006*, 007*, 008*, 009*, 106, 107
3.3	Pravice dostopa do funkcij in podatkov		010*, 011*, 240, 246, 247
3.4	Spremljanje vstavljanja in izvlečenja kartic		013, 014, 015*, 016*, 106
3.5	Merjenje hitrosti in razdalj		017 do 026
3.6	Merjenje časa (preskus se opravlja pri 20 °C)		027 do 032
3.7	Spremljanje vznikovih dejavnosti		033 do 043, 106
3.8	Spremljanje stanja vožnje		044, 045, 106
3.9	Ročni vnosi		046 do 050b
3.10	Upravljanje blokad s strani podjetja		051 do 055
3.11	Spremljanje nadzornih dejavnosti		056, 057
3.12	Zaznavanje dogodkov in/ali napak		059 do 069, 106

Št.	Preskus	Opis	Povezane zahteve
3.13	Identifikacijski podatki naprave		075*, 076*, 079
3.14	Podatki o vstavljanju in izvlačenju voznikove kartice		081* do 083*
3.15	Podatki o voznikovih dejavnostih		084* do 086*
3.16	Podatki o krajih		087* do 089*
3.17	Podatki števca prevožene poti		090* do 092*
3.18	Podrobni podatki o hitrosti		093*
3.19	Podatki o dogodkih		094*, 095
3.20	Podatki o napakah		096*
3.21	Kalibracijski podatki		097*, 098*
3.22	Podatki o nastavljanju časa		100*, 101*
3.23	Podatki o nadzornih dejavnostih		102*, 103*
3.24	Podatki o blokadah s strani podjetja		104*
3.25	Podatki o prenosih podatkov iz naprav		105*
3.26	Podatki o posebnih stanjih		105a*, 105b*
3.27	Zapisovanje in hranjenje podatkov na tahografskih karticah		108, 109*, 109a*, 110*, 111, 112
3.28	Prikazovanje		072, 106, 113 do 128, PIC 001, DIS_001
3.29	Tiskanje		072, 106, 129 do 138, PIC 001, PRT_001 do PRT_012
3.30	Opozorila		106, 139 do 148, PIC_001
3.31	Prenos podatkov na zunanje medije		072, 106, 149 do 151
3.32	Iznos podatkov na dodatne zunanje naprave		152, 153
3.33	Kalibriranje		154*, 155*, 156*, 245
3.34	Nastavljanje časa		157*, 158*
3.35	Varnost pred posegi s strani dodatnih funkcij		003, 269

Št.	Preskus	Opis	Povezane zahteve
4.	Okoljski preskusi		
4.1	Temperatura	Preverjanje funkcionalnosti s preskusi: — IEC 68-2-1, preskus Ad, trajanje preskusa 72 ur pri nizki temperaturi (–20 °C), 1 h deluje, 1 h ne deluje, — IEC 68-2-2, preskus Bd, trajanje preskusa 72 ur pri visoki temperaturi (+ 70 °C), 1 h deluje, 1 h ne deluje, Temperaturni cikli: preverjanje ali lahko enota v vozilu prenese hitre spremembe temperature okolice, s preskusom Na po IEC 68-2-14, 20 ciklov, pri vsaki spremembi temperature od nizke (– 20 °C) do visoke (+ 70 °C) oz. obratno, nato držanje po 2 uri pri nizki oz. pri visoki temperaturi Skrčeni nabor preskusov (izbranih med preskusi, predpisanimi v točki 3 te tabele) se lahko opravi pri nizki temperaturi, pri visoki temperaturi ali med temperaturnimi cikli.	159
4.2	Vlaga	Preverjanje, ali lahko enota v vozilu prenese cikle vlage (preskus v vročem) s preskusom Db po IEC 68-2-30, šest 24-urnih ciklov, pri vsaki spreminjanje temperature od + 25 °C do + 55 °C, relativna vlažnost 97 % pri + 25 °C in 93 % pri + 55 °C	160
4.3	Tresljaji	1. Sinusni tresljaji: preverjanje, ali lahko enota v vozilu prenese sinusne tresljaje naslednjih lastnosti: konstantni premiki s 5 in 11 Hz: konica 10 mm konstantni pospeški od 11 do 300 Hz: 5 g To zahtevo se preverja s preskusom Fc po IEC 68-2-6, z najmanjšim trajanjem preskusa 3 x 12 ur (12 ur na vsako os) 2. Naključni tresljaji: preverjanje, ali lahko enota v vozilu prenese naključne tresljaje naslednjih lastnosti: frekvenca 5–150 Hz, raven 0,02 g²/Hz To zahtevo se preverja s preskusom Ffda po IEC 68-2-35, z najmanjšim trajanjem preskusa 3 x 12 ur (12 ur na vsako os); 1 uro deluje, 1 uro ne deluje Zgoraj opisana preskusa se opravita na dveh različnih primerkih preskušane opreme	163
4.4	Zaščita pred vodo in tujki	Preverjanje, ali je razred zaščite enote v vozilu vsaj insured person 40 po IEC 529, pri enoti vgrajeni na vozilu in pri delovnih pogojih	164, 165
4.5	Prenapetostna zaščita	Preverjanje, ali enota v vozilu prenese naslednje napajanje:	161
		24V izvedbe: 34 V pri + 40 °C 1 uro;	
		12V izvedbe: 17 V pri + 40 °C 1 uro	
4.6	Zaščita pred zamenjavo polaritete	Preverjanje, ali enota v vozilu prenese zamenjavo polaritete svoje napajalne napetosti.	161

Št.	Preskus	Opis	Povezane zahteve
4.7	Kratkostična zaščita	Preverjanje, ali so izhodni signali zaščiteni pred kratkimi stiki z napajalno napetostjo in ozemljitvijo	161
5.	Preskusi elektromagnetne združljivosti (EMC)		
5.1	Lastna sevanja in občutljivost na zunanja sevanja	Skladnost z Direktivo 95/54/EGS	162
5.2	Elektrostatične razelektritve	Skladnost z IEC 61000-4-2, ± 2 kV (raven 1)	162
5.3	Prehodni pojavi prevodnosti	Pri 24V izvedbah: skladnost z ISO 7637-2 občutljivost na napajanje pulz 1a: $V_s = -100$ V, $R_i = 10$ ohmov pulz 2: $V_s = +100$ V, $R_i = 10$ ohmov pulz 3a: $V_s = -100$ V, $R_i = 50$ ohmov pulz 3b: $V_s = +100$ V, $R_i = 50$ ohmov pulz 4: $V_s = -16$ V, $V_a = -12$ V, $t_6 = 100$ ms pulz 5: $V_s = +120$ V, $R_i = 2,2$ ohmov, $t_d = 250$ ms Pri 12V izvedbah: skladnost z ISO 7637-1: pulz 1: $V_s = -100$ V, $R_i = 10$ ohmov pulz 2: $V_s = +100$ V, $R_i = 10$ ohmov pulz 3a: $V_s = -100$ V, $R_i = 50$ ohmov pulz 3b: $V_s = +100$ V, $R_i = 50$ ohmov pulz 4: $V_s = -6$ V, $V_a = -5$ V, $t_6 = 15$ ms pulz 5: $V_s = +65$ V, $R_i = 3$ Ohm, $t_d = 100$ ms S pulzom 5 se preskuša le enote v vozilu, namenjene za vgradnjo v vozila brez vgrajene zunanje skupne zaščite pred razbremenitvami	162

3. FUNKCIONALNI PRESKUSI ZAZNAVALA GIBANJA

Št.	Preskus	Opis	Povezane zahteve
1.	Administrativni pregled		
1.1	Dokumentacija	Pravilnost dokumentacije	
2.	Vizualni pregled		
2.1	Skladnost z dokumentacijo		
2.2	Identifikacija/oznake		169, 170
2.3	Gradiva		163 do 167
2.4	Plombiranje		251
3.	Funkcionalni preskusi		
3.1	Identifikacijski podatki zaznavala		077*
3.2	Povezava zaznavala gibanja in enote v vozilu		099*, 155
3.3	Zaznavanje gibanja		
	Točnost merjenja gibanja		022 do 026

Št.	Preskus	Opis	Povezane zahteve
4.	Okoljski preskusi		
4.1	Delovna temperatura	Preverjanje funkcionalnosti (opredeljene pri preskusu št. 3.3) v temperaturnem območju [– 40 °C; + 135 °C] s preskusi: — IEC 68-2-1, preskus Ad, trajanje preskusa 96 ur pri najnižji temperaturi Tomin — IEC 68-2-2, preskus Bd, trajanje preskusa 96 ur pri najvišji temperaturi Tomax	159
4.2	Temperaturni cikli:	Preverjanje funkcionalnosti (opredeljene pri preskusu št. 3.3), s preskusom Na po IEC 68-2-14, 20 ciklov, pri vsakem sprememba temperature od nizke (–40 °C) do visoke (+135 °C) oz. obratno, nato držanje po 2 uri pri nizki oz. pri visoki temperaturi Skrčeni nabor preskusov (izbranih med preskusi, predpisanimi pri preskusu št. 3.3) se lahko opravi pri nizki temperaturi, pri visoki temperaturi ali med temperaturnimi cikli.	159
4.3	Cikli vlažnosti	Preverjanje funkcionalnosti (opredeljene pri preskusu št. 3.3) s preskusom Db po IEC 68-2-30, šest 24-unrih ciklov, pri vsakem spreminjanje temperature od + 25 °C do + 55 °C, relativna vlažnost 97 % pri + 25 °C in 93 % pri + 55 °C	160
4.4	Tresljaji	Preverjanje funkcionalnosti (opredeljene pri preskusu št. 3.3) s preskusom Fc po IEC 68-2-6, trajanje preskusa 100 ciklov frekvence: konstantni premiki med 10 in 57 Hz: konica 1,5 mm; konstantni pospeški od 57 do 500 Hz: 20 g	163
4.5	Mehanski udarci	Preverjanje funkcionalnosti (opredeljene pri preskusu št. 3.3) s preskusom Ea po IEC 68-2-27, udarci v obeh smereh v vseh treh pravokotnih oseh	163
4.6	Zaščita pred vodo in tuji	Preverjanje, ali je razred zaščite zaznavala gibanja vsaj IP 64 po IEC 529, pri zaznavalu vgrajenem na vozilu in pri delovnih pogojih	165
4.7	Zaščita pred zamenjavo polaritete	Preverjanje, ali zaznavalo gibanja prenese zamenjavo polaritete svoje napajalne napetosti.	161
4.8	Kratkostična zaščita	Preverjanje, ali so izhodni signali zaščiteni pred kratkimi stiki z napajalno napetostjo in ozemljitvijo	161
5.	EMC		
5.1	Lastna sevanja in občutljivost	Preverjanje skladnosti z Direktivo 95/54/EGS	162
5.2	Elektrostatične razelektritve	Skladnost z IEC 61000-4-2, ± 2 kV (raven 1)	162
5.3	Občutljivost podatkovnih linij na prehodne pojave zaradi prevodnosti	Skladnost z ISO 7637-3 (raven III)	162

4. FUNKCIONALNI PRESKUSI TAHOGRAFSKIH KARTIC

Št.	Preskus	Opis	Povezane zahteve
1.	Administrativni pregled		
1.1	Dokumentacija	Pravilnost dokumentacije	
2.	Vizualni pregled		
2.1		Preverjanje, ali so vse varnostne značilnosti in vidni podatki natisnjeni na kartici pravilno in v skladu z zahtevami	171 do 181
3.	Fizični preskusi		
3.1		Preverjanje mer kartice in položaja kontaktov	184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	Preskusi protokolov		
4.1	ATR	Preverjanje skladnosti ATR	ISO/IEC 7816-3 TCS 304, 307, 308
4.2	T=0	Preverjanje skladnosti protokola T=0	ISO/IEC 7816-3 TCS 302, 303, 305
4.3	PTS	Preverjanje skladnosti ukaza PTS, s preklpom s T=0 na T=1	ISO/IEC 7816-3 TCS 309 do 311
4.4	T=1	Preverjanje skladnosti protokola T=1	ISO/IEC 7816-3 TCS 303, / 306
5.	Struktura kartice		
5.1		Preskus skladnosti datotečne strukture kartice, s preverjanjem prisotnosti obveznih datotek na kartici in pogojev za dostop do njih	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	Funkcionalni preskusi		
6.1	Normalna obdelava	Vsaj en preskus vsake dovoljene uporabe vsakega ukaza (npr: preverjanje ukaza UPDATE BINARY s CLA = '00', CLA = OC' ter z različnimi parametri PI, P2 in Lc) Preverjanje, ali so se operacije na kartici dejansko izvedle (npr.: z branjem datoteke, na kateri je bila operacija izvedena)	TCS 313 do TCS 379
6.2	Sporočila napak	Vsaj en preskus vsakega sporočila napak (kakor so opredeljena v dodatku 2) pri vsakem ukazu Vsaj en preskus vsake generične napake (razen napak celovitosti '6400', ki se jih preverja v okviru varnostnega certificiranja)	
7.	Okoljski preskusi		
7.1		Preverjanje, ali kartica deluje v območju mejnih pogojev opredeljenih po ISO/IEC 10373.	185 do 188 ISO/IEC 7816-1

5. PRESKUSI SKUPNE UPORABNOSTI

Št.	Preskus	Opis
1.	Medsebojna avtentifikacija	Preverjanje normalnega poteka medsebojne avtentifikacije enote v vozilu in tahografske kartice
2.	Preskusi pisanje/branja	Izvedba značilnega scenarija uporabe enote v vozilu. Scenarij mora biti prilagojen vrsti preskušane kartice in mora obsegati vpise v kar največ elementarnih datotek na kartici. Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov s kartice Preverjanje, ali je mogoče vse zapise pravilno prebrati, s tiskanjem dnevnih dejavnosti s kartice

Dodatek 10

GENERIČNI VARNOSTNI CILJI

Ta dodatek predpisuje obvezno vsebino varnostnih ciljev zaznavala gibanja, enote v vozilu in tahografske kartice.

Pri oblikovanju varnostnih ciljev, s katerimi bodo utemeljevali svoje zahteve po varnostnem certificiranju, morajo proizvajalci po potrebi dopolniti in izpopolniti dokumente, pri tem pa ne smejo spremeniti ali opustiti predpisanih groženj, ciljev, postopkov ali predpisov funkcij za zagotavljanje varnosti.

VSEBINA

Generični varnostni cilj zaznavala gibanja

1.	Uvod	482
2.	Kratice, opredelitve in literatura	482
2.1	Kratice	482
2.2	Opredelitve	482
2.3	Literatura	482
3.	Obrazložitev izdelka	483
3.1	Opis zaznavala gibanja in načina uporabe	483
3.2	Življenjski cikel zaznavala gibanja	484
3.3	Grožnje	484
3.3.1	Grožnje politiki upravljanja dostopa	484
3.3.2	Grožnje, povezane s projektiranjem	485
3.3.3	Grožnje, povezane z delovanjem	485
3.4	Varnostni cilji	485
3.5	Informacijski varnostni cilji	485
3.6	Načini zagotavljanja varnosti s fizičnega vidika, vidika osebja in vidika postopkov	486
3.6.1	Projektiranje opreme	486
3.6.2	Dobava opreme	486
3.6.3	Tvorba in dobava varnostnih podatkov	486
3.6.4	Namestitev, kalibriranje in kontrola zapisovalne naprave	486
3.6.5	Upravljanje uveljavljanja predpisov	486
3.6.6	Nadgradnje programske opreme	486
4.	Funkcije zagotavljanja varnosti	486
4.1	Identifikacija in avtentifikacija	486
4.2	Upravljanje dostopa	487
4.2.1	Politika upravljanja dostopa	487
4.2.2	Pravice dostopa do podatkov	487
4.2.3	Datotečna struktura in pogoji dostopa	487
4.3	Odgovornost	487

4.4	Revizija	488
4.5	Točnost	488
4.5.1	Politika upravljanja toka informacij	488
4.5.2	Notranji prenosi podatkov	488
4.5.3	Celovitost shranjenih podatkov	488
4.6	Zanesljivost storitev	488
4.6.1	Preskusi	488
4.6.2	Programska oprema	489
4.6.3	Fizična zaščita	489
4.6.4	Prekinitev napajanja	489
4.6.5	Stanje ponastavitve	489
4.6.6	Razpoložljivost podatkov	489
4.6.7	Več aplikacij	489
4.7	Izmenjava podatkov	489
4.8	Kriptografska podpora	489
5.	Opredelitev varnostnih mehanizmov	490
6.	Minimalna trdnost varnostnih mehanizmov	490
7.	Raven zagotavljanja varnosti	490
8.	Obrazložitev	490

Generični varnostni cilj enote v vozilu

1.	Uvod	492
2.	Kratice, opredelitve in literatura	492
2.1	Kratice	492
2.2	Opredelitve	492
2.3	Literatura	492
3.	Obrazložitev izdelka	492
3.1	Opis enote v vozilu in načina uporabe	492
3.2	Življenjski cikel enote v vozilu	494
3.3	Grožnje	494
3.3.1	Grožnje politiki identifikacije in upravljanja dostopa	494
3.3.2	Grožnje, povezane s projektiranjem	495
3.3.3	Grožnje, povezane z delovanjem	495
3.4	Varnostni cilji	495
3.5	Informacijski varnostni cilji	496
3.6	Načini zagotavljanja varnosti s fizičnega vidika, vidika osebja in vidika postopkov	496
3.6.1	Projektiranje opreme	496
3.6.2	Dobava in aktiviranje opreme	496

3.6.3	Tvorba in dobava varnostnih podatkov	496
3.6.4	Dobava kartic	497
3.6.5	Namestitvev, kalibriranje in kontrola zapisovalne naprave	497
3.6.6	Delovanje opreme	497
3.6.7	Upravljanje uveljavljanja predpisov	497
3.6.8	Nadgradnje programske opreme	497
4.	Funkcije zagotavljanja varnosti	497
4.1	Identifikacija in avtentifikacija	497
4.1.1	Identifikacija in avtentifikacija zaznavala gibanja	497
4.1.2	Identifikacija in avtentifikacija uporabnika	498
4.1.3	Identifikacija in avtentifikacija podjetja na daljavo	499
4.1.4	Identifikacija in avtentifikacija naprave za upravljanje	499
4.2	Upravljanje dostopa	499
4.2.1	Politika upravljanja dostopa	499
4.2.2	Pravice dostopa do funkcij	499
4.2.3	Pravice dostopa do podatkov	499
4.2.4	Datotečna struktura in pogoji dostopa	500
4.3	Odgovornost	500
4.4	Revizija	500
4.5	Ponovna uporaba objektov	501
4.6	Točnost	501
4.6.1	Politika upravljanja toka informacij	501
4.6.2	Notranji prenosi podatkov	501
4.6.3	Celovitost shranjenih podatkov	501
4.7	Zanesljivost storitev	501
4.7.1	Preskusi	501
4.7.2	Programska oprema	502
4.7.3	Fizična zaščita	502
4.7.4	Prekinitve napajanja	502
4.7.5	Stanje ponastavitve	502
4.7.6	Razpoložljivost podatkov	502
4.7.7	Več aplikacij	502
4.8	Izmenjava podatkov	502
4.8.1	Izmenjava podatkov z zaznavalom gibanja	502
4.8.2	Izmenjava podatkov s tahografsko kartico	503
4.8.3	Izmenjava podatkov z zunanje pomnilne medije (prenos podatkov na zunanje pomnilne medije)	503
4.9	Kriptografska podpora	503

5.	Opredelitev varnostnih mehanizmov	503
6.	Minimalna trdnost varnostnih mehanizmov	503
7.	Raven zagotavljanja varnosti	503
8.	Obrazložitev	504

Generični varnostni cilj tahografske kartice

1.	Uvod	508
2.	Kratice, opredelitve in literatura	508
2.1	Kratice	508
2.2	Opredelitve	508
2.3	Literatura	509
3.	Obrazložitev izdelka	509
3.1	Opis tahografske kartice in načina uporabe	509
3.2	Življenjski cikel tahografske kartice	509
3.3	Grožnje	510
3.3.1	Končni cilji	510
3.3.2	Poti napadov	510
3.4	Varnostni cilji	510
3.5	Informacijski varnostni cilji	510
3.6	Načini zagotavljanja varnosti s fizičnega vidika, vidika osebja in vidika postopkov	510
4.	Funkcije zagotavljanja varnosti	511
4.1	Skladnost s profili zaščite	511
4.2	Identifikacija in avtentifikacija uporabnika	511
4.2.1	Identifikacija uporabnika	511
4.2.2	Avtentifikacija uporabnika	511
4.2.3	Neuspela avtentifikacija	511
4.3	Upravljanje dostopa	512
4.3.1	Politika upravljanja dostopa	512
4.3.2	Funkcije upravljanja dostopa	512
4.4	Odgovornost	512
4.5	Revizija	512
4.6	Točnost	512
4.6.1	Celovitost shranjenih podatkov	512
4.6.2	Osnovna avtentifikacija podatkov	512
4.7	Zanesljivost storitev	513
4.7.1	Preskusi	513
4.7.2	Programska oprema	513
4.7.3	Napajanje	513

4.7.4	Stanje ponastavitve	513
4.8	Izmenjava podatkov	513
4.8.1	Izmenjava podatkov z enoto v vozilu	513
4.8.2	Izvoz podatkov v enote zunaj vozila (funkcija prenosa podatkov)	513
4.9	Kriptografska podpora	513
5.	Opredelitev varnostnih mehanizmov	513
6.	Zahtevana minimalna trdnost varnostnih mehanizmov	514
7.	Raven zagotavljanja varnosti	514
8.	Obrazložitev	514

GENERIČNI VARNOSTNI CILJI ZAZNAVALA GIBANJA

1. Uvod

Ta dokument vsebuje opise zaznavala gibanja, groženj, ki jih mora obvladovati in varnostnih ciljev, ki jih mora dosegati. Dokument predpisuje funkcije zagotavljanja varnosti. Navaja najmanjšo obvezno trdnost varnostnih mehanizmov in zahtevano raven zagotavljanja varnosti, ki jih je treba upoštevati pri razvoju in ocenjevanju.

V tem dokumentu omenjene zahteve so zahteve, podane v osnovnem besedilu priloge I B. Da bi bila predstavitev čim jasnejša, se zahteve v besedilu priloge I B in zahteve varnostnih ciljev ponekod podvajajo. Pri morebitnih razlikah med omembami besedila v prilogi I B v teh zahtevah glede varnostnih ciljev in osnovnim besedilom priloge I B se upošteva osnovno besedilo priloge I B.

Zahteve v osnovnem besedilu priloge I B, ki jih varnostni cilji ne omenjajo, niso predmet funkcij zagotavljanja varnosti.

Grožnje, cilji, postopki in specifikacije SEF so označeni z enoznačnimi naslovi, tako da je mogoča njihova sledljivost v projektni in ocenjevalni dokumentaciji.

2. Kratice, opredelitve in literatura**2.1 Kratice**

ROM	bralni pomnilnik
SEF	funkcija zagotavljanja varnosti
TBD	bo še opredeljeno
TOE	cilj pri vrednotenju
VU	enota v vozilu.

2.2 Opredelitve

Digitalni tahograf	zapisovalna naprava
Osebek	naprava, priključena na zaznavalo gibanja
Podatki o gibanju	podatki, ki se jih izmenjuje z VU in ki kažejo hitrost in prevoženo pot
Fizično ločeni deli	fizični sestavni deli zaznavala gibanja, ki so razporejeni po vozilu, v nasprotju s fizičnimi sestavnimi deli v ohišju zaznavala gibanja
Varnostni podatki	posebni podatki, potrebni za podporo funkcij zagotavljanja varnosti (npr. kriptografski ključi)
Sistem	oprema, osebje ali organizacije, ki kakor koli delujejo v zvezi z zapisovalno napravo
Uporabnik	človek-uporabnik zaznavala gibanja (razen v izrazu „uporabniški podatki“)
Uporabniški podatki	kakršnikoli podatki, razen varnostnih podatkov zaznavala gibanja, ki jih zapisuje ali shranjuje zaznavalo gibanja

2.3 Literatura

ITSEC Merila vrednotenja informacijske varnosti ITSEC 1991.

3. Obrazložitev izdelka

3.1 Opis zaznavala gibanja in načina uporabe

Zaznavalo gibanja je namenjeno za namestitev v cestna transportna vozila. Njegov namen je zagotavljati enoti v vozilu varne podatke o gibanju vozila, ki kažejo hitrost in prevoženo pot vozila.

Zaznavalo gibanja je mehansko povezano s premikajočim se delom vozila, katerega premikanje lahko predstavlja hitrost in prevoženo pot vozila. Lahko je nameščeno na menjalniku vozila ali na kakem drugem delu vozila.

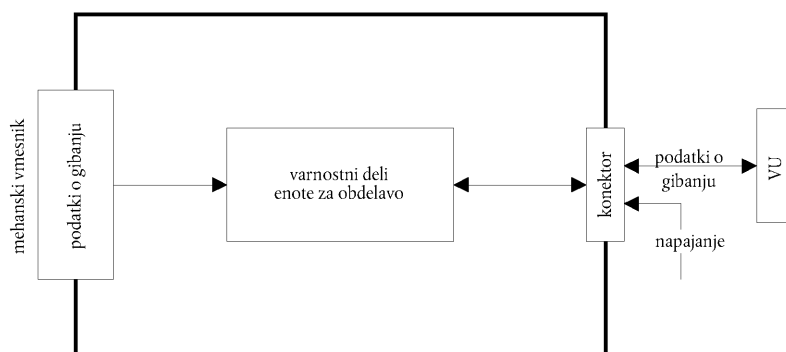
Med delovanjem je zaznavalo gibanja povezano z VU.

Lahko je povezano s posebno opremo, ki služi upravljanju (kar opredeli proizvajalec).

Značilno zaznavalo gibanja prikazuje naslednja slika:

Slika 1

Značilno zaznavalo gibanja

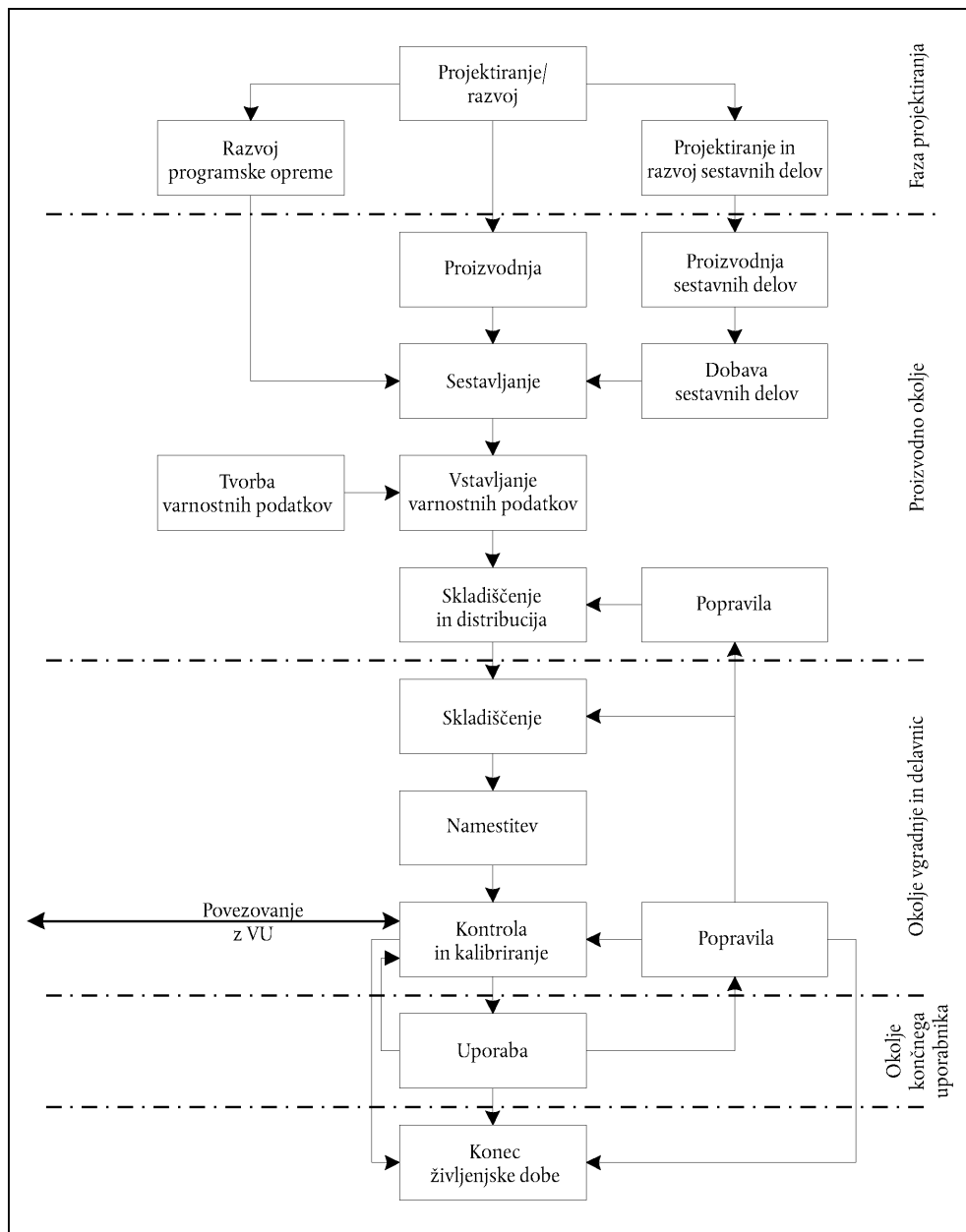


3.2 Življenjski cikel zaznavala gibanja

Značilni življenjski cikel zaznavala gibanja opisuje naslednja slika:

Slika 2

Značilni življenjski cikel zaznavala gibanja



3.3 Grožnje

Ta točka opisuje grožnje, ki jim je lahko izpostavljeno zaznavalo gibanja.

3.3.1 Grožnje politiki upravljanja dostopa

T.Access

Uporabniki lahko zahtevajo dostop do funkcij, do katerih niso upravičeni.

3.3.2 Grožnje, povezane s projektiranjem

T.Faults	Napake v strojni opremi, programski opremi ali komunikacijskih postopkih lahko privedejo zaznavalo gibanja v nepredvideno stanje, ki ogroža varnost njegovega delovanja.
T.Tests	Uporaba nepreverjenih preskusov ali „stranskih vrat“ lahko ogrozi varnost delovanja zaznavala gibanja
T.Design	Uporabniki lahko poskušajo pridobiti neupravičene informacije o projektnih lastnostih, bodisi iz proizvajalčevih gradiv (s krajo, podkupninami,...) ali z obratnim inženirstvom.

3.3.3 Grožnje, povezane z delovanjem

T.Environment	Uporabniki lahko ogrozijo varnost zaznavala gibanja z okoljskimi napadi (toplotnimi, elektromagnetnimi, optičnimi, kemičnimi, mehanskimi, ...)
T.Hardware	Uporabniki lahko poskusijo predelati strojno opremo zaznavala gibanja
T.Mechanical_Origin	Uporabniki lahko poskusijo vplivati na vhod zaznavala gibanja (npr. odviti ga z menjalnika, ...)
T.Motion_Data	Uporabniki lahko poskusijo spremeniti podatke o gibanju vozila (dodati, spremeniti, zbrisati, ponovno predvajati signal)
T.Power_Supply	Uporabniki lahko poskusijo ogroziti varnostne cilje zaznavala s predelavo (odklopom, znižanjem, zvišanjem) njegovega napajanja
T.Security_Data	Uporabniki lahko poskusijo pridobiti neupravičen dostop do varnostnih podatkov med tvorbo varnostnih podatkov, njihovim prenosom ali shranjevanjem v opremi
T.Software	Uporabniki lahko poskusijo predelati programsko opremo zaznavala gibanja
T.Stored_Data	Uporabniki lahko poskusijo predelati shranjene podatke (varnostne ali uporabniške podatke).

3.4 Varnostni cilji

Glavni varnostni cilj digitalnega tahografskega sistema je naslednji:

O.Main	Podatki, ki jih preverjajo nadzorni organi, morajo biti na voljo in morajo v celoti in točno odražati dejavnosti nadzorovanih voznikov in vozil, kar se tiče obdobja vožnje, dela, razpoložljivosti in odmorov in kar se tiče hitrosti vozila.
--------	--

Zato je varnostni cilj zaznavala gibanja v okviru splošnega varnostnega cilja:

O.Sensor_Main	Podatki, ki jih posreduje zaznavalo gibanja, morajo biti na voljo VU tako, da lahko VU v celoti in točno ugotavlja gibanje vozila, kar se tiče hitrosti in prevožene poti.
---------------	--

3.5 Informacijski varnostni cilji

Posebni informacijski varnostni cilji zaznavala gibanja v okviru splošnega varnostnega cilja so naslednji:

O.Access	Zaznavalo gibanja mora nadzorovati dostop priključenih osebkov do funkcij in podatkov
O.Audit	Zaznavalo gibanja mora pregledovati poskuse spodkopavanja njegove varnosti in mora slediti take poskuse do ustreznih osebkov
O.Authentication	Zaznavalo gibanja mora avtentificirati povezane osebkove

O.Processing	Zaznavalo gibanja mora zagotoviti točno obdelavo vhodov za pridobitev podatkov o gibanju
O.Reliability	Zaznavalo gibanja mora zagotavljati zanesljive storitve
O.Secured_Data_Exchange	Zaznavalo gibanja mora varovati izmenjavo podatkov z VU.

3.6 Načini zagotavljanja varnosti s fizičnega vidika, vidika osebja in vidika postopkov

Ta točka opisuje zahteve glede varovanja s fizičnega vidika, vidika osebja in vidika postopkov, ki prispevajo k varnosti zaznavala gibanja.

3.6.1 Projektiranje opreme

M.Development	Razvijalci zaznavala gibanja morajo poskrbeti, da odgovornosti pri razvoju zagotavljajo informacijsko varnost
M.Manufacturing	Proizvajalci zaznavala gibanja morajo zagotoviti, da odgovornosti med proizvodnjo zagotavljajo informacijsko varnost in da je med proizvodnjo zaznavalo gibanja zaščiteno pred fizičnimi napadi, ki bi lahko ogrozili njegovo informacijsko varnost.

3.6.2 Dobava opreme

M.Delivery	Proizvajalci zaznavala gibanja, proizvajalci vozil ter delavnice morajo zagotoviti tak način dela z zaznavalom gibanja, ki zagotavlja njegovo informacijsko varnost.
------------	--

3.6.3 Tvorba in dobava varnostnih podatkov

M.Sec_Data_Generation	Algoritmi tvorbe varnostnih podatkov morajo biti dostopni samo pooblaščenim in zaupnim osebam
M.Sec_Data_Transport	Varnostni podatki morajo biti tvorjeni, prenašani in vneseni v zaznavalo gibanja tako, da se ustrezno ohrani njihova zaupnost in celovitost.

3.6.4 Namestitve, kalibriranje in kontrola zapisovalne naprave

M.Approved_Workshops	Nameščanje, kalibriranje in popravila zapisovalne naprave morajo opravljati zaupni in pooblaščeni izvajalci ali delavnice.
M.Mechanical_Interface	Predvideni morajo biti načini za ugotavljanje poskusov posegov v mehansko povezavo (npr. plombe)
M.Regular_Inspections	Zapisovalno napravo je treba redno kontrolirati in kalibrirati.

3.6.5 Upravljanje uveljavljanja predpisov

M.Controls	Redno in naključno je treba izvajati funkcije uveljavljanja predpisov, te funkcije morajo obsegati tudi revizije varnosti.
------------	--

3.6.6 Nadgradnje programske opreme

M.Software_Upgrade	Pred vgradnjo v zaznavalo gibanj morajo biti nadgradnje programske opreme varnostno certificirane.
--------------------	--

4. Funkcije zagotavljanja varnosti

4.1 Identifikacija in avtentifikacija

UIA_101 Zaznavalo gibanja mora biti zmožno pri vsaki interakciji ugotoviti identiteto osebk, s katerim je povezano.

UIA_102 Identifikacijo povezanega osebkca morajo sestavljati:

- skupina, v katero spada osebek:
 - VU,
 - naprava za upravljanje,
 - drugo
- ID osebkca (samo pri VU).

UIA_103 ID osebkca pri povezani VU sestavljata številka odobritve VU in serijska številka VU.

UIA_104 Zaznavalo gibanja mora biti zmožno avtentificirati vsako VU ali napravo za upravljanje, s katero je povezano:

- ob povezavi z osebkom,
- ob obnovitvi napajanja.

UIA_105 Zaznavalo gibanja mora biti zmožno občasno ponovno avtentificirati VU, s katero je povezano.

UIA_106 Zaznavalo gibanja mora zaznati in preprečiti uporabo kopiranih in ponovno predvajanih podatkov za avtentifikacijo.

UIA_107 Po (številu naj določi proizvajalec, vendar ne sme presegati 20) zaznanih zaporednih neuspešnih poskusih avtentifikacije mora SEF:

- oblikovati revizijski zapis dogodka.
- opozoriti osebek,
- naprej izvažati podatke v nezavarovanem režimu.

4.2 **Upravljanje dostopa**

Upravljanje dostopa zagotavlja, da podatke iz TOE berejo, vanj zapisujejo ali v njem spreminjajo le osebkci, ki so za to pooblašeni.

4.2.1 *Politika upravljanja dostopa*

ACC_101 Zaznavalo gibanja mora nadzorovati pravic dostopa do funkcij in podatkov.

4.2.2 *Pravice dostopa do podatkov*

ACC_102 Zaznavalo gibanja mora zagotavljati, da je mogoče identifikacijske podatke zaznavala gibanja zapisati le enkrat (zahteva 078).

ACC_103 Zaznavalo gibanja mora sprejemati in/ali shranjevati uporabniške podatke le od avtentificiranih osebkov.

ACC_104 Zaznavalo gibanja mora uveljavljati ustrezne pravice branja in pisanja varnostnih podatkov.

4.2.3 *Datotečna struktura in pogoji dostopa*

ACC_105 Struktura aplikativnih in podatkovnih datotek in pogoji dostopa morajo biti oblikovani v proizvodnem procesu, nato pa blokirani pred kakršnokoli naknadno spremembo ali brisanjem.

4.3 **Odgovornost**

ACT_101 Zaznavalo gibanja mora v svojem pomnilniku hraniti identifikacijske podatke zaznavala gibanja (zahteva 077).

ACT_102 Zaznavalo gibanja mora v svojem pomnilniku hraniti podatke o namestitvi (zahteva 099).

ACT_103 Zaznavalo gibanja mora biti zmožno iznesti podatke o odgovornosti avtentificiranim osebkom, če ti osebkci tak iznos zahtevajo.

4.4 **Revizija**

AUD_101 Zaznavalo gibanja mora pri dogodkih, ki ogrožajo njegovo varnost, oblikovati zapis takih dogodkov.

AUD_102 Dogodki, ki vplivajo na varnost zaznavala gibanja, so:

- poskusi kršenja varnosti,
 - neuspela avtentifikacija,
 - napaka v celovitosti shranjenih podatkov,
 - napaka pri notranjem prenosu podatkov,
 - nepooblaščen odprtje ohišja,
 - sabotaza strojne opreme.
- napaka na zaznavalu.

AUD_103 Revizijski zapisi morajo vsebovati naslednje podatke:

- datum in čas dogodka,
- vrsta dogodka.
- identiteta povezanega osebk.

Če zahtevani podatki niso na voljo, mora biti podan ustrezni privzeti identifikator (ki ga opredeli proizvajalec).

AUD_104 Zaznavalo gibanja mora vsak revizijski zapis poslati VU, takoj ko ga oblikuje, lahko pa ga tudi shrani v svojem pomnilniku.

AUD_105 Če zaznavalo gibanja revizijske zapise shranjuje, mora njegov pomnilni prostor zagotavljati hranjenje 20 revizijskih zapisov in mora biti zmožno na zahtevo iznesti shranjene revizijske zapise avtentificiranim osebkom.

4.5 **Točnost**

4.5.1 *Politika upravljanja toka informacij*

ACR_101 Zaznavalo gibanja mora zagotavljati, da je mogoče obdelovati in izpeljevati le podatke o gibanju, ki izvirajo iz mehankega vhoda zaznavala.

4.5.2 *Notranji prenos podatkov*

Zahteve te točke veljajo le, kadar zaznavalo gibanja uporablja fizično ločene dele.

ACR_102 Če se podatki prenašajo med fizično ločenimi deli zaznavala gibanja, morajo biti zaščiteni pred spreminjanjem.

ACR_103 Če je med notranjim prenosom podatkov zaznana napaka pri prenosu podatkov, mora biti prenos podatkov ponovljen in SEF mora oblikovati zapis dogodka.

4.5.3 *Celovitost shranjenih podatkov*

ACR_104 Zaznavalo gibanja mora preverjati napake celovitosti podatkov, shranjenih v svojem pomnilniku.

ACR_105 Če ugotovi napako celovitosti shranjenih podatkov, mora SEF oblikovati revizijski zapis.

4.6 **Zanesljivost storitev**

4.6.1 *Preskusi*

RLB_101 Pred zaključkom proizvodne faze morajo biti onemogočeni ali odstranjeni vsi ukazi, dejavnosti ali preskusne točke, namenjene za prekušanje posebej v fazi proizvodnje. Ne sme biti mogoča njihova obnova za kasnejšo rabo.

RLB_102 Zaznavalo gibanja mora med začetnim zagonom in med normalnim delovanjem opravljati preskuse lastnega delovanja, s katerimi preverja pravilno delovanje. Preskusi lastnega delovanja zaznavala gibanja morajo obsegati preverjanje celovitosti varnostnih podatkov in preverjanje celovitosti shranjenega izvršljivega programa (če ni shranjen v ROM).

RLB_103 Če med preskusom lastnega delovanja ugotovi interno napako, mora SEF oblikovati revizijski zapis (napaka zaznavala).

4.6.2 Programska oprema

RLB_104 Programske opreme zaznavala gibanja na terenu ne sme biti mogoče analizirati ali odpravljati napak v njej.

RLB_105 Zaznavalo gibanja ne sme sprejemati vhodov iz zunanjih virov kot izvršnih programov.

4.6.3 Fizična zaščita

RLB_106 Če je projektirano tako, da ga je mogoče odpreti, mora zaznavalo gibanja zaznati vsako odpiranje ohišja, vsaj 6 mesecev tudi ob izklopljenem napajanju. Ob odprtju ohišja mora SEF oblikovati revizijsko poročilo o dogodku. (Dopustno je, da se poročilo oblikuje in odda šele po ponovni vzpostavitvi napajanja).

Če je zaznavalo gibanja projektirano tako, da ga ni mogoče odpreti, mora biti projektirano tako, da je zlahka mogoče zaznati poskuse fizičnih posegov vanj (npr. z vizualnim pregledom).

RLB_107 Zaznavalo gibanja mora zaznati določene (določi proizvajalec) sabotaže strojne opreme.

RLB_108 V zgoraj opisanih primerih mora SEF oblikovati revizijski zapis in zaznavalo gibanja mora: (določi proizvajalec).

4.6.4 Az Prekinitve napajanja

RLB_109 Zaznavalo gibanja mora med izpadom ali nihanji napajanja ostati v varnem stanju.

4.6.5 Stanje ponastavitve

RLB_110 Ob izpadu napajanja ali ob prekinitvi transakcije pred njenim zaključkom ali v drugih stanjih ponastavitve se mora zaznavalo gibanja ponastaviti na čist način.

4.6.6 Razpoložljivost podatkov

RLB_111 Zaznavalo gibanja mora zagotavljati dostop do virov, kadar je potreben, in preprečevati nepotrebne zahteve po virih ali njihovo zadrževanje.

4.6.7 Več aplikacij

RLB_112 Če zaznavalo gibanja služi poleg tahografski tudi drugim aplikacijam, morajo biti vse aplikacije med seboj fizično in/ali logično ločene. Aplikacije ne smejo souporabljati varnostnih podatkov. Naenkrat sme biti aktivno le eno samo opravilo.

4.7 Izmenjava podatkov

DEX_101 zaznavalo gibanja mora iznašati podatke o gibanju v VU skupaj z ustreznimi varnostnimi atributi, tako da lahko VU preverja njihovo celovitost in avtentičnost.

4.8 Kriptografska podpora

Zahteve iz te točke veljajo le po potrebi, glede na uporabljene varnostne mehanizme in proizvajalčeve rešitve.

CSP_101 Vse kriptografske operacije zaznavala gibanja morajo biti opravljene po predpisanem algoritmu in s predpisano velikostjo ključa.

CSP_102 Kadar zaznavalo gibanja tvori kriptografske ključke, mora to izvajati po predpisanih algoritmihi za tvorbo kriptografskih ključev in s predpisano velikostjo kriptografskih ključev.

CSP_103 Kadar zaznavalo gibanja distribuira kriptografske ključke, mora to izvajati po predpisanih postopkih distribucije ključev.

CSP_104 Kadar zaznavalo gibanja dostopa do kriptografskih ključev, mora dostopati do njih po predpisanih postopkih dostopa do ključev.

CSP_105 Kadar zaznavalo gibanja dostopa do kriptografskih ključev, mora dostopati do njih po predpisanih postopkih dostopa do ključev.

5. Opredelitev varnostnih mehanizmov

Varnostne mehanizme za izpolnitev funkcij uveljavljanja varnosti zaznavala varnosti opredelijo proizvajalci zaznaval gibanja.

6. Minimalna trdnost varnostnih mehanizmov

Minimalna trdnost varnostnih mehanizmov zaznavala gibanja je po opredelitvi (ITSEC) ‚visoka‘.

7. Raven zagotavljanja varnosti

Ciljna raven zagotavljanja varnosti zaznavala gibanja je po opredelitvi v (ITSEC) raven ITSEC E3.

8. Obrazložitev

Naslednje matrike razlagajo SEF s prikazom naslednjih postavk:

- katere SEF ali načini delujejo proti katerim grožnjam,
- katere SEF izpolnjujejo katere informacijske varnostne cilje.

	Grožnje												Informacijski cilji					
	Dostop	Napake	Preskusi	Projekriranje	Okolje	Strojna oprema	Mechanical_Origin	Motion_Data	Power_Supply	Security_Data	Programska oprema	Stored_Data	Dostop	Revizija	Avtentifikacija	Obdelava	Zanesljivost	Secured_Data_Exchange
Načini zagotavljanja varnosti s fizičnega vidika, vidika osebja in vidika postopkov																		
Razvoj		x	x	x														
Proizvodnja			x	x														
Dobava						x					x	x						
Tvorba varnostnih podatkov										x								
Prenos varnostnih podatkov										x								
Odobrene delavnice							x											
Mehanski vmesnik							x											
Redne kontrole						x	x		x		x							
Upravljanje uveljavljanja predpisov					x	x	x		x	x	x							
Nadgradnje programske opreme											x							
Funkcije zagotavljanja varnosti																		
Identifikacija in avtentifikacija																		
UIA_101 Identifikacija osebkov	x							x					x		x			x
UIA_102 Identiteta osebkov	x												x		x			
UIA_103 Identiteta VU														x				
UIA_104 Avtentifikacija osebkov	x							x					x		x			x
UIA_105 Ponovna avtentifikacija	x							x					x		x			x
UIA_106 Nepozabna avtentifikacija	x							x					x		x			
UIA_107 Neuspela avtentifikacija								x						x			x	
Upravljanje dostopa																		
ACC_101 Politika upravljanja dostopa	x									x		x	x					
ACC_102 ID zaznavala gibanja												x	x					

[illegible]

GENERIČNI VARNOSTNI CILJ ENOTE V VOZILU

1. Uvod

Ta dokument vsebuje opise enote v vozilu, groženj, ki jih mora obvladovati in varnostnih ciljev, ki jih mora dosegati. Dokument predpisuje funkcije zagotavljanja varnosti. Navaja najmanjšo obvezno trdnost varnostnih mehanizmov in zahtevano raven zagotavljanja varnosti, ki jih je treba upoštevati pri razvoju in ocenjevanju.

V tem dokumentu omenjene zahteve so zahteve, podane v osnovnem besedilu priloge I B. Da bi bila predstavitev čim jasnejša, se zahteve v besedilu priloge I B in zahteve varnostnih ciljev ponekod podvajajo. Pri morebitnih razlikah med omembami besedila v prilogi I B v teh zahtevah glede varnostnih ciljev in osnovnim besedilom priloge I B se upošteva osnovno besedilo priloge I B.

Zahteve v osnovnem besedilu priloge I B, ki jih varnostni cilji ne omenjajo, niso predmet funkcij zagotavljanja varnosti.

Grožnje, cilji, postopki in specifikacije SEF so označeni z enoznačnimi naslovi, tako da je mogoča njihova sledljivost v projektni in ocenjevalni dokumentaciji.

2. Kratice, opredelitve in literatura

2.1 Kratice

PIN	osebna identifikacijska številka
ROM	bralni pomnilnik
SEF	funkcija zagotavljanja varnosti
TBD	bo še opredeljeno
TOE	cilj pri vrednotenju
VU	enota v vozilu.

2.2 Opredelitve

Digitalni tahograf	zapisovalna naprava
Podatki o gibanju	podatki, ki se jih izmenjuje z zaznavalom gibanja in ki kažejo hitrost in prevoženo pot
Fizično ločeni deli	fizični sestavni deli VU, ki so razporejeni po vozilu, v nasprotju s fizičnimi sestavnimi deli v ohišju VU
Varnostni podatki	posebni podatki, potrebni za podporo funkcij zagotavljanja varnosti (npr. kriptografski ključi)
Sistem	oprema, osebje ali organizacije, ki kakorkoli delujejo v zvezi z zapisovalno napravo
Uporabnik	Uporabniki pomenijo ljudi-uporabnike opreme. Normalni uporabniki VU so vozniki, kontrolorji, delavnice in podjetja.
Uporabniški podatki	kakršnikoli podatki, razen varnostnih podatkov VU, ki jih zapisuje ali shranjuje VU po zahtevah točke III. 12.

2.3 Literatura

ITSEC Merila vrednotenja informacijske varnosti ITSEC 1991.

3. Obrazložitev izdelka

3.1 Opis enote v vozilu in načina uporabe

VU je namenjena za namestitve v cestna transportna vozila. Njene naloge so zapisovanje, hranjenje, prikaz, tiskanje in iznos podatkov povezanih z voznikovimi dejavnostmi.

Povezana je z zaznavalom gibanja in si z njim izmenjuje podatke o gibanju vozila. Uporabniki se identificirajo enoti v vozilu s tahografskimi karticami.

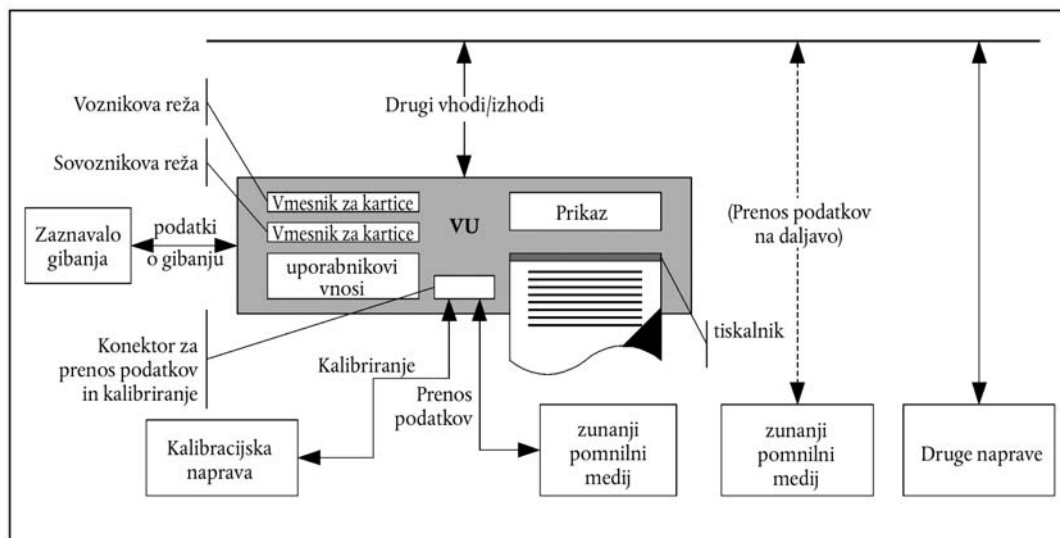
VU zapisuje in hrani podatke o dejavnostih uporabnikov v svojem pomnilniku podatkov in zapisuje podatke o dejavnostih uporabnikov na tahografske kartice.

VU iznaša podatke na prikaz, tiskalnik in zunanje naprave.

Delovno okolje enote v vozilu, nameščene v vozilu, prikazuje naslednja slika:

Slika 1

Delovno okolje VU



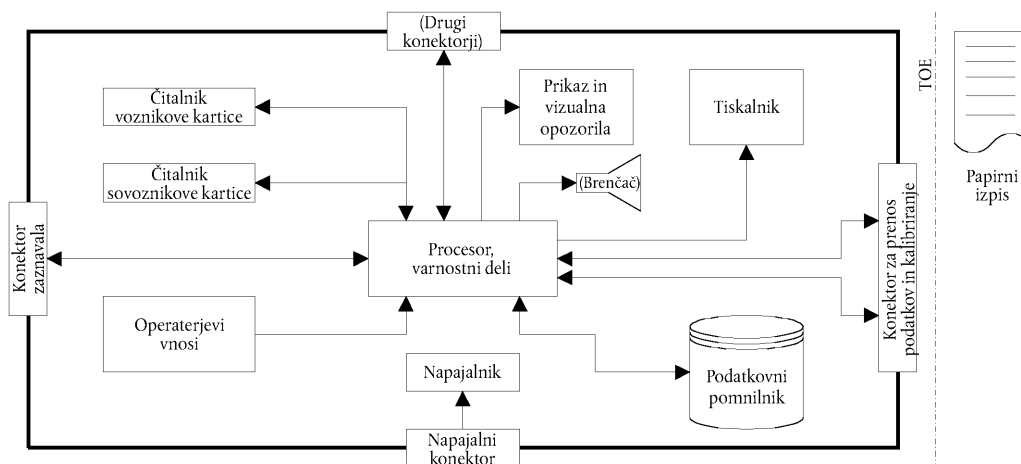
Splošne lastnosti, funkcije in režimi delovanja VU so opisani v poglavju II v ptilogi I B.

Funkcionalne zahteve VU so predpisane v poglavju III priloge I B.

Značilno VU prikazuje naslednja slika:

Slika 2

Značilna VU (...) neobvezno.



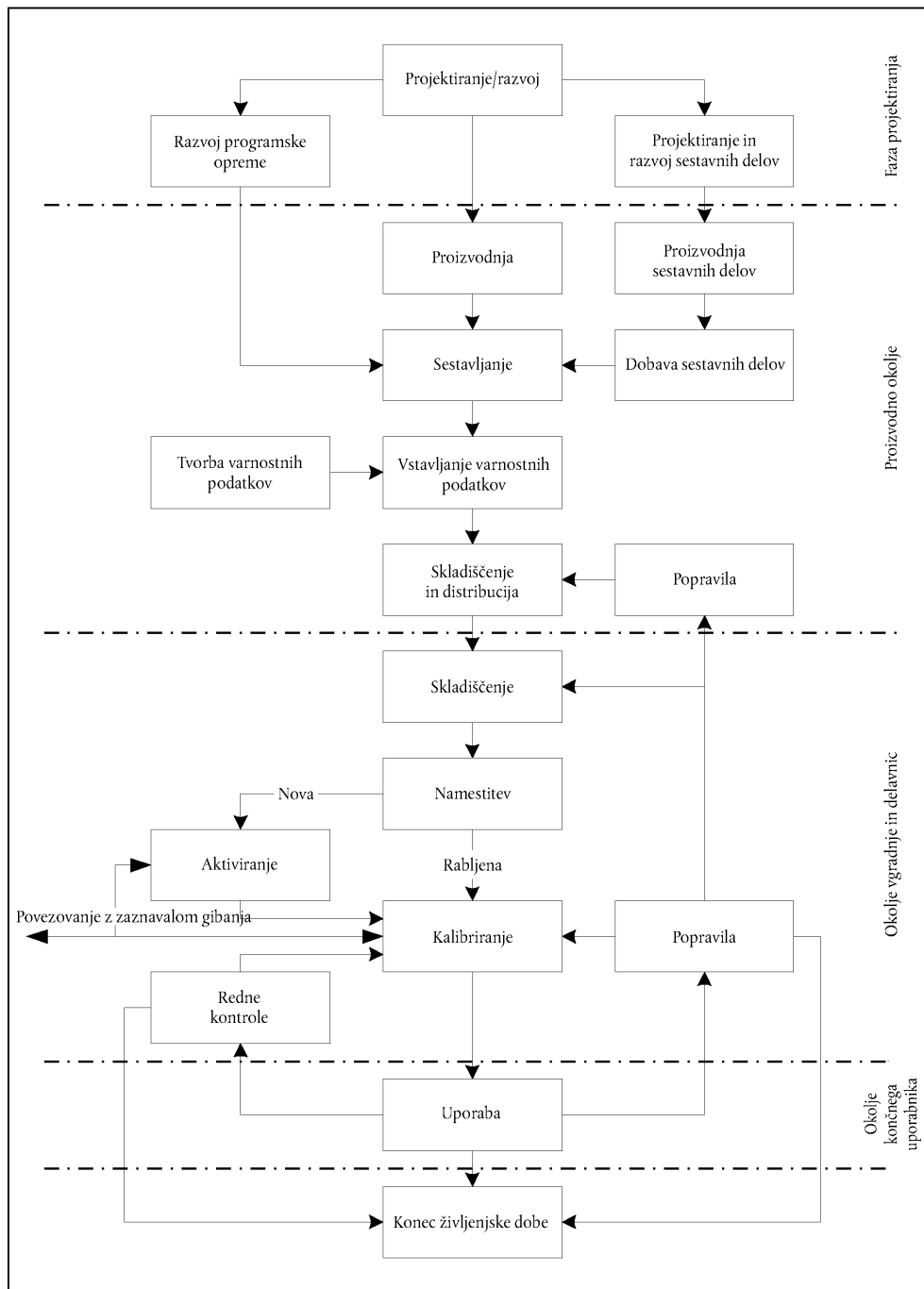
Upoštevati je treba naslednje: mehanizem tiskalnika je del TOE, papirni dokument pa po tem, ko je natisnjen, ne več.

3.2 Življenjski cikel enote v vozilu

Značilni življenjski cikel VU opisuje naslednja slika:

Slika 3

Značilni življenjski cikel VU



3.3 Grožnje

Ta točka opisuje grožnje, ki jim je lahko izpostavljena VU.

3.3.1 Grožnje politiki identifikacije in upravljanja dostopa

T.Access

Uporabniki lahko zahtevajo dostop do funkcij, do katerih niso upravičeni (npr. voznikov poskus dostopa do funkcij kalibriranja).

T.Identification

Uporabniki lahko poskusijo uporabljati več identifikacij ali delati brez identifikacije.

3.3.2 Grožnje, povezane s projektiranjem

T.Faults	Napake v strojni opremi, programski opremi ali komunikacijskih postopkih lahko privedejo VU v nepredvideno stanje, ki ogroža njeno varnost.
T.Tests	Uporaba nepreverjenih preskusov ali „stranskih vrat“ lahko ogrozi varnost delovanja VU
T.Design	Uporabniki lahko poskušajo pridobiti neupravičene informacije o projektnih lastnostih, bodisi iz proizvajalčevih gradiv (s krajo, podkupninami,...) ali z obratnim inženirstvom.

3.3.3 Grožnje, povezane z delovanjem

T.Calibration_Parameters	Uporabniki lahko poskušajo razkalibrirati opremo (s spreminjanjem kalibracijskih podatkov ali z zlorabo organizacijskih slabosti)
T.Card_Data_Exchange	Uporabniki lahko poskusijo spremeniti podatke med njihovo izmenjavo med VU in tahografskimi karticami (dodati, spremeniti, zbrisati, ponovno predvajati signal)
T.Clock	Uporabniki lahko poskusijo spremeniti notranjo uro
T.Environment	Uporabniki lahko ogrozijo varnost VU z okoljskimi napadi (toplotnimi, elektromagnetnimi, optičnimi, kemičnimi, mehanskimi, ...)
T.Fake_Devices	Uporabniki lahko poskušajo priključiti ponarejene naprave (zaznavalo gibanja, pametne kartice) na VU
T.Hardware	Uporabniki lahko poskusijo spremeniti strojno opremo VU
T.Motion_Data	Uporabniki lahko poskusijo spremeniti podatke o gibanju vozila (dodati, spremeniti, zbrisati, ponovno predvajati signal)
T.Non_Activated	Uporabniki lahko uporabljajo neaktivirano opremo
T.Output_Data	Uporabniki lahko poskusijo predelati podatkovne izhode (prikaz, tiskanje ali prenos).
T.Power_Supply	Uporabniki lahko poskusijo ogroziti varnostne cilje VU s predelavo (odklopom, znižanjem, zvišanjem) njegovega napajanja
T.Security_Data	Uporabniki lahko poskusijo pridobiti neupravičen dostop do varnostnih podatkov med tvorbo varnostnih podatkov, njihovim prenosom ali shranjevanjem v opremi
T.Software	Uporabniki lahko poskusijo spremeniti programsko opremo VU
T.Stored_Data	Uporabniki lahko poskusijo predelati shranjene podatke (varnostne ali uporabniške podatke).

3.4 Varnostni cilji

Glavni varnostni cilj digitalnega tahografskega sistema je naslednji:

O.Main	Podatki, ki jih preverjajo nadzorni organi, morajo biti na voljo in morajo v celoti in točno odražati dejavnosti nadzorovanih voznikov in vozil, kar se tiče obdobja vožnje, dela, razpoložljivosti in odmorov in kar se tiče hitrosti vozila.
--------	--

Zato so varnostni cilji VU v okviru splošnega varnostnega cilja naslednji:

O.VU_Main	Podatki, ki se merijo in zapisujejo, nato pa jih preverjajo nadzorni organi, morajo biti na voljo in morajo točno odražati dejavnosti nadzorovanih voznikov in vozil, kar se tiče obdobja vožnje, dela, razpoložljivosti in odmorov in kar se tiče hitrosti vozila.
O.VU_Export	VU mora biti zmožna izvažati podatke na zunanje pomnilne medije tako, da je mogoče preverjati njihovo celovitost in avtentičnost.

3.5 Informacijski varnostni cilji

Posebni informacijski varnostni cilji VU v okviru splošnega varnostnega cilja so naslednji:

O.Access	VU mora nadzorovati dostop uporabnikov do funkcij in podatkov
O.Accountability	VU mora zbirati točne podatke glede odgovornosti
O.Audit	VU mora pregledovati poskuse spodbijanja njene varnosti in mora slediti take poskuse do ustreznih uporabnikov
O.Authentication	VU mora avtentificirati uporabnike in priključene osebe (kadar je potrebna vzpostavitev zaupne poti med osebkami)
O.Integrity	VU mora vzdrževati celovitost shranjenih podatkov
O.Output	VU mora zagotavljati, da izhodni podatki točno odražajo merjene ali shranjene podatke
O.Processing	VU mora zagotoviti točnost obdelave vhodov za pridobitev uporabniških podatkov
O.Reliability	VU mora zagotavljati zanesljive storitve
O.Secured_Data_Exchange	VU mora varovati izmenjavo podatkov z zaznavalom gibanja in tahografskimi karticami.

3.6 Načini zagotavljanja varnosti s fizičnega vidika, vidika osebja in vidika postopkov

Ta točka opisuje zahteve glede varovanja s fizičnega vidika, vidika osebja in vidika postopkov, ki prispevajo k varnosti VU.

3.6.1 Projektiranje opreme

M.Development	Razvijalci VU morajo poskrbeti, da odgovornosti pri razvoju zagotavljajo informacijsko varnost
M.Manufacturing	Proizvajalci VU morajo zagotoviti, da odgovornosti med proizvodnjo zagotavljajo informacijsko varnost in da je med proizvodnjo VU zaščitena pred fizičnimi napadi, ki bi lahko ogrozili njeno informacijsko varnost.

3.6.2 Dobava in aktiviranje opreme

M.Delivery	Proizvajalci VU, proizvajalci vozil ter delavnice morajo zagotoviti tak način dela z VU, ki zagotavlja njeno informacijsko varnost.
M.Activation	Proizvajalci vozil ali izvajalci namestitve ali delavnice morajo, preden vozilo zapusti delavnico, v kateri je bila opravljena namestitve, nameščeno VU aktivirati.

3.6.3 Tvorba in dobava varnostnih podatkov

M.Sec_Data_Generation	Algoritmi tvorbe varnostnih podatkov morajo biti dostopni samo pooblaščenim in zaupnim osebam
M.Sec_Data_Transport	Varnostni podatki morajo biti tvorjeni, prenašani in vneseni v VU tako, da se ustrezno ohrani njihova zaupnost in celovitost.

3.6.4 Dobava kartic

M.Card_Availability	Tahografske kartice se sme dajati na voljo in dobavljati samo pooblaščenim osebam
M.Driver_Card_Uniqueness	Voznik sme hkrati imeti zgolj eno veljavno voznikovo kartico
M.Card_Traceability	Dobava kartic mora biti sledljiva (beli seznam, črni seznam), med varnostnimi revizijami je obvezna uporaba črnih seznamov.

3.6.5 Namestitve, kalibriranje in kontrola zapisovalne naprave

M.Approved_Workshops	Nameščanje, kalibriranje in popravila zapisovalne naprave morajo opravljati zaupni in pooblaščeni izvajalci ali delavnice.
M.Regular_Inspections	Zapisovalno napravo je treba redno kontrolirati in kalibrirati
M.Faithful_Calibration	Odobreni izvajalci namestitve in delavnice morajo med kalibriranjem v zapisovalno napravo vnesti pravilne parametre vozila.

3.6.6 Delovanje opreme

M.Faithful_Drivers	Vozniki morajo ravnati po pravilih in odgovorno (npr. pravilno uporabljati svoje kartice, pravilno izbirati dejavnosti pri ročnem vnosu, ...)
--------------------	---

3.6.7 Upravljanje uveljavljanja predpisov

M.Controls	Redno in naključno je treba izvajati funkcije uveljavljanja predpisov, te funkcije morajo obsegati tudi revizije varnosti.
------------	--

3.6.8 Nadgradnje programske opreme

M.Software_Upgrade	Pred vgradnjo v VU morajo biti nadgradnje programske opreme varnostno certificirane.
--------------------	--

4. Funkcije zagotavljanja varnosti

4.1 Identifikacija in avtentifikacija

4.1.1 Identifikacija in avtentifikacija zaznavala gibanja

UIA_201 VU mora biti zmožno pri vsaki interakciji ugotoviti identiteto zaznavala gibanja, s katerim je povezano.

UIA_202 Identiteto zaznavala gibanja sestavlja številka odobritve zaznavala gibanja in serijska številka zaznavala gibanja.

UIA_203 VU mora avtentificirati zaznavalo gibanja, s katerim je povezana:

- ob priključitvi zaznavala gibanja,
- ob vsakem kalibriranju zapisovalne naprave,
- ob obnovitvi napajanja.

Avtentifikacija mora biti medsebojna in jo sproži VU.

UIA_204 VU mora občasno (obdobje opredeli proizvajalec, mora pa biti krajše od ene ure) ponovno identificirati in ponovno avtentificirati priključeno zaznavalo gibanja in preverjati, ali je zaznavalo gibanja še vedno tisto, ki ga je VU identificirala ob zadnjem kalibriranju zapisovalne naprave.

UIA_205 VU mora zaznati in preprečiti uporabo kopiranih in ponovno predvajanih podatkov za avtentifikacijo.

UIA_206 Po (število naj določi proizvajalec, vendar ne sme presegati 20) zaznanih zaporednih neuspešnih poskusih avtentifikacije in/ali če zazna nepooblaščen spremembo identitete zaznavala gibanja (npr. ne med kalibriranjem zapisovalne naprave) mora SEF:

- oblikovati revizijski zapis dogodka,
- opozoriti uporabnika,
- naprej sprejemati in uporabljati ne-varne podatke od zaznavala gibanja.

4.1.2 Identifikacija in avtentifikacija uporabnika

UIA_207 VU mora stalno in selektivno slediti identiteto obeh uporabnikov, s spremljanjem vstavljenih tahografskih kartic v voznikovi ali sovoznikovi reži VU.

UIA_208 Identiteto uporabnika sestavljata:

- skupina, v katero spada uporabnik:
 - VOZNIK (voznikova kartica),
 - KONTROLOR (nadzorna kartica),
 - DELAVNICA (delavniška kartica),
 - PODJETJE (kartica podjetja),
 - NEZNAN (ni vstavljena nikakršna kartica),
- ID uporabnika, ki jo sestavljajo:
 - država izdajateljica kartice in številka kartice,
 - NEZNANA, če uporabnik spada v skupino NEZNAN

Identiteta NEZNANEGA uporabnika je lahko implicitno ali eksplicitno poznana.

UIA_209 VU mora avtentificirati svoje uporabnike ob vstavitvi kartic.

UIA_210 VU mora ponovno avtentificirati svoje uporabnike:

- ob obnovitvi napajanja,
- občasno ali po določenih dogodkih (kar opredeli proizvajalec, pogostost pa mora biti večja kot enkrat na dan)

UIA_211 Avtentifikacijo se opravi tako, da se dokaže, da je vstavljena tahografska kartica veljavna kartica, ki vsebuje varnostne podatke, ki jih je lahko distribuiral samo sistem. Avtentifikacija mora biti medsebojna in jo sproži VU.

UIA_212 Poleg gornjega mora biti za delavnico obvezna tudi uspešna avtentifikacija s preverjanjem PIN. Dolžina PIN mora biti vsaj 4 znake.
Opomba: Če se PIN prenaša v VU iz zunanje opreme, nameščene v bližini VU, je treba med prenosom varovati zaupnost PIN.

UIA_213 VU mora zaznati in preprečiti uporabo kopiranih in ponovno predvajanih podatkov za avtentifikacijo.

UIA_214 Po petih zaznanih zaporednih neuspešnih poskusih avtentifikacije mora SEF:

- oblikovati revizijski zapis dogodka,
- opozoriti uporabnika,
- predpostaviti, da je uporabnik NEZNAN in da kartica ni veljavna (po opredelitvi z in po zahtevi 007).

4.1.3 Identifikacija in avtentifikacija podjetja na daljavo

Zmožnost priključitve podjetja na daljavo ni obvezna. Ta točka torej velja le, kadar je ta zmožnost vgrajena.

- UIA_215 Pri vsaki interakciji s podjetjem, priključenim na daljavo, mora biti VU zmožna ugotoviti identiteto tega podjetja.
- UIA_216 Identiteto na daljavo priključenega podjetja sestavljajo država izdajateljica kartice podjetja in številka kartice podjetja.
- UIA_217 Preden dovoli izvoz podatkov na daljavo priključenemu podjetju, mora VU uspešno avtentificirati to podjetje.
- UIA_218 Avtentifikacijo se opravi tako, da se dokaže, da je podjetje imetnik veljavne kartice podjetja, ki vsebuje varnostne podatke, ki jih je lahko distribuiral samo sistem.
- UIA_219 VU mora zaznati in preprečiti uporabo kopiranih in ponovno predvajanih podatkov za avtentifikacijo.
- UIA_220 Po petih zaznanih zaporednih neuspešnih poskusih avtentifikacije mora VU:

— opozoriti na daljavo priključeno podjetje.

4.1.4 Identifikacija in avtentifikacija naprave za upravljanje

Proizvajalci VU lahko predvidijo namenske naprave za dodatne funkcije upravljanja VU (npr. za nadgrajevanje programske opreme, ponovno nalaganje varnostnih podatkov, ...). Ta točka torej velja le, kadar je ta zmožnost vgrajena.

- UIA_221 Pri vsaki interakciji z napravo za upravljanje mora biti VU zmožna ugotoviti identiteto te naprave.
- UIA_222 Preden dovoli nadaljnje interakcije, mora VU uspešno avtentificirati napravo za upravljanje.
- UIA_223 VU mora zaznati in preprečiti uporabo kopiranih in ponovno predvajanih podatkov za avtentifikacijo.

4.2 Upravljanje dostopa

Upravljanje dostopa zagotavlja, da podatke iz TOE berejo, vanj zapisujejo ali v njem spreminjajo le osebk, ki so za to pooblašeni.

Upoštevati je treba, da podatki, zapisani v VU, četudi so zaupne narave ali poslovno občutljivi, niso podatki zaupne narave. Zato funkcionalne zahteve glede pravic dostopa do podatkov (zahteva 011) niso predmet funkcij zagotavljanja varnosti.

4.2.1 Politika upravljanja dostopa

- ACC_201 VU mora upravljati in preverjati pravice dostopa do funkcij in podatkov.

4.2.2 Pravice dostopa do funkcij

- ACC_202 VU mora izvajati pravila izbire režimov delovanja (zahteve 006 do 009).
- ACC_203 VU mora uporabljati režim delovanja pri zagotavljanju upoštevanja pravil upravljanja dostopa do funkcij (zahteva 010).

4.2.3 Pravice dostopa do podatkov

- ACC_204 VU mora zagotavljati upoštevanje pravil o pravicah dostopa do identifikacijskih podatkov VU (zahteva 076).
- ACC_205 VU mora zagotavljati upoštevanje pravil o pravicah dostopa do identifikacijskih podatkov povezanega zaznavala gibanja (zahtevi 079 in 155).
- ACC_206 Po aktiviranju VU mora VU zagotavljati, da je mogoč vnos kalibracijskih podatkov v VU in njihovo shranjevanje v njenem pomnilniku le v kalibracijskem režimu (zahtevi 154 in 156).
- ACC_207 Po svojem aktiviranju mora VU zagotavljati upoštevanje pravil o pravicah pisanja in brisanja kalibracijskih podatkov (zahteva 097).

ACC_208 Po svojem aktiviranju mora VU zagotavljati, da je mogoč vnos podatkov za nastavljanje časa v VU in njihovo shranjevanje v njenem pomnilniku le v kalibracijskem režimu (Ta zahteva ne velja za manjša nastavljanja časa, ki jih dopuščata zahtevi 157 in 158).

ACC_209 Po svojem aktiviranju mora VU zagotavljati upoštevanje pravil o pravicah pisanja in brisanja podatkov za nastavljanje časa (zahteva 100).

ACC_210 VU mora uveljavljati ustrezne pravice branja in pisanja varnostnih podatkov (zahteva 080).

4.2.4 Datotečna struktura in pogoji dostopa

ACC_211 Struktura aplikativnih in podatkovnih datotek in pogoji dostopa morajo biti oblikovani v proizvodnem procesu, nato pa blokirani pred kakršnokoli naknadno spremembo ali brisanjem.

4.3 Odgovornost

ACT_201 VU mora zagotavljati, da vozniki nosijo odgovornost za svoje dejavnosti (zahteve 081, 084, 087, 105a, 105b, 109 in 109a).

ACT_202 VU mora hraniti trajne identifikacijske podatke (zahteva 075).

ACT_203 VU mora zagotavljati, da delavnice nosijo odgovornost za svoje dejavnosti (zahteve 098, 101 in 109).

ACT_204 VU mora zagotavljati, da nadzorniki nosijo odgovornost za svoje dejavnosti (zahteve 102, 103 in 109).

ACT_205 VU mora zapisovati podatke števca prevožene poti (zahteva 090) in podrobne podatke o hitrosti (zahteva 093).

ACT_206 VU mora zagotavljati, da uporabniških podatkov povezanih z zahtevami 081 do 093 in 102 do vključno 105b po njihovem zapisu ni več mogoče spreminjati, razen takrat, ko so kot najstarejši shranjeni podatki prepisani z novimi podatki.

ACT_207 VU mora zagotavljati, da ne spreminja že shranjenih podatkov na tahografski kartici (zahtevi 109 in 109a), razen takrat, ko prepisuje najstarejše podatke z novimi podatki (zahteva 110) ali v primeru, opisanem v opombi v točki 2.1 dodatka 1.

4.4 Revizija

Zmožnost revizij je zahtevana le za dogodke, ki lahko kažejo na poskuse manipuliranja ali ogrožanja varnosti. Ni zahtevana za normalno uveljavljanje pravic, četudi je to pomembno za varnost.

AUD_201 VU mora dogodke, ki ogrožajo varnost VU, zapisati skupaj z zadevnimi podatki (zahteve 094, 096 in 109).

AUD_202 Dogodki, ki vplivajo na varnost VU, so:

- poskusi kršenja varnosti,
- neuspela avtentifikacija zaznavala gibanja,
- neuspela avtentifikacija tahografske kartice,
- nepooblaščen zamenjava zaznavala gibanja,
- napaka v celovitosti vhodnih podatkov s kartice,
- napaka v celovitosti shranjenih podatkov uporabnika,
- napaka pri notranjem prenosu podatkov,
- nepooblaščen odprtje ohišja,
- sabotaza strojne opreme,

- zadnja seja s kartico nepravilno zaključena,
- dogodek „napaka v podatkih o gibanju“,
- dogodek „izpad napajanja“,
- interna napaka VU.

AUD_203 VU mora zagotavljati izvajanje pravil hranjenja revizijskih zapisov (zahtevi 094 in 096).

AUD_204 VU mora v svojem pomnilniku hraniti revizijske zapise, ki jih tvori zaznavalo gibanja.

AUD_205 Revizijske zapise mora biti mogoče tiskati, prikazovati in prenašati na zunanje pomnilne medije.

4.5 **Ponovna uporaba objektov**

REU_201 VU mora zagotavljati, da je mogoče začasno shranjene objekte ponovno uporabiti, ne da bi pri tem prišlo do nedopustnih tokov informacij.

4.6 **Točnost**

4.6.1 *Politika upravljanja toka informacij*

ACR_201 VU mora zagotavljati, da je pri uporabniških podatkih, povezanih z zahtevami 081, 084, 087, 090, 093, 102, 104, 105, 105a in 109, mogoča le obdelava vrednosti iz pravih vhodnih virov:

- podatki o gibanju,
- ura realnega časa v VU,
- kalibracijski parametri zapisovalne naprave,
- tahografske kartice,
- uporabnikovi vnosi.

ACR_201a VU mora zagotavljati, da je mogoče uporabniške podatke, povezane z zahtevo 109a, vnesti le za obdobje od zadnjega izvleka kartice do tekoče vstavitve kartice (zahteva 050a).

4.6.2 *Notranji prenos podatkov*

Zahteve te točke veljajo le, kadar VU uporablja fizično ločene dele.

ACR_202 Če se podatki prenašajo med fizično ločenimi deli VU, morajo biti zaščiteni pred spreminjanjem.

ACR_203 Če je med notranjim prenosom zaznana napaka pri prenosu podatkov, mora biti prenos podatkov ponovljen in SEF mora oblikovati zapis dogodka.

4.6.3 *Celovitost shranjenih podatkov*

ACR_204 VU mora preverjati napake celovitosti uporabniških podatkov, shranjenih v svojem pomnilniku.

ACR_205 Če ugotovi napako celovitosti shranjenih uporabniških podatkov, mora SEF oblikovati revizijski zapis.

4.7 **Zanesljivost storitev**

4.7.1 *Preskusi*

RLB_201 Pred aktiviranjem VU morajo biti onemogočeni ali odstranjeni vsi ukazi, dejavnosti ali preskusne točke, namenjene za preskušanje posebej v fazi proizvodnje. Ne sme biti mogoča njihova obnova za kasnejšo rabo.

RLB_202 VU mora med začetnim zagonom in med normalnim delovanjem opravljati preskuse lastnega delovanja, s katerimi preverja pravilno delovanje. Preskusi lastnega delovanja VU morajo obsegati preverjanje celovitosti varnostnih podatkov in preverjanje celovitosti shranjenega izvršljivega programa (če ni shranjen v ROM).

RLB_203 Če med preskusom lastnega delovanja ugotovi interno napako, mora SEF:

- oblikovati revizijski zapis (razen v režimu kalibriranja) (interna napaka VU),
- ohraniti celovitost shranjenih podatkov.

4.7.2 Programska oprema

RLB_204 Programske opreme VU na terenu po aktiviranju VU ne sme biti mogoče analizirati ali odpravljati napak v njej.

RLB_205 VU ne sme sprejemati vhodov iz zunanjih virov kot izvršnih programov.

4.7.3 Fizična zaščita

RLB_206 Če je projektirana tako, da jo je mogoče odpreti, mora VU zaznati vsako odpiranje ohišja razen v režimu kalibriranja, vsaj 6 mesecev tudi ob izklopljenem napajanju. V takem primeru mora SEF oblikovati revizijsko poročilo. (Dopustno je, da se poročilo oblikuje in shrani šele po ponovni vzpostavitvi napajanja).

Če je VU projektirana tako, da je ni mogoče odpreti, mora biti projektirana tako, da je zlahka mogoče zaznati poskuse fizičnih posegov vanjo (npr. z vizualnim pregledom).

RLB_207 Po aktiviranju mora VU zaznati določene (določi proizvajalec) sabotaže strojne opreme.

RLB_208 V zgoraj opisanih primerih mora SEF oblikovati revizijski zapis in VU mora: (določi proizvajalec).

4.7.4 Prekinitev napajanja

RLB_209 VU mora zaznati odstopanja od predpisanih vrednosti napajanja, tudi prekinitve napajanja.

RLB_210 V zgoraj opisanem primeru mora SEF:

- oblikovati revizijski zapis (razen v režimu kalibriranja),
- ohraniti varno stanje VU,
- vzdrževati varnostne funkcije povezane s še delujočimi sestavnimi deli ali procesi,
- ohraniti celovitost shranjenih podatkov.

4.7.5 Stanje ponastavitve

RLB_211 Ob prekinitvi napajanja ali ob prekinitvi transakcije pred njenim zaključkom ali v drugih stanjih ponastavitve se mora VU ponastaviti na čist način.

4.7.6 Razpoložljivost podatkov

RLB_212 VU mora zagotavljati dostop do virov, kadar je potreben, in preprečevati nepotrebne zahteve po virih ali njihovo zadrževanje.

RLB_213 VU mora zagotavljati, da kartic ni mogoče izvleči, preden se nanje shranijo ustrezni podatki (zahtevi 015 in 016).

RLB_214 V zgoraj opisanih primerih mora SEF oblikovati revizijski zapis dogodka.

4.7.7 Več aplikacij

RLB_215 Če VU služi poleg tahografski tudi drugim aplikacijam, morajo biti vse aplikacije med seboj fizično in/ali logično ločene. Aplikacije ne smejo souporabljati varnostnih podatkov. Naenkrat sme biti aktivno le eno samo opravilo.

4.8 Izmenjava podatkov

Ta točka se nanaša na izmenjavo podatkov med VU in priključenimi napravami.

4.8.1 Izmenjava podatkov z zaznavalom gibanja

DEX_201 VU mora preverjati celovitost in avtentičnost podatkov o gibanju, uvoženih iz zaznavala gibanja.

DEX_202 Če zazna napako celovitosti ali avtentičnosti podatkov o gibanju, mora SEF:

- oblikovati revizijski zapis,
- uvožene podatke uporabljati naprej.

4.8.2 *Izmenjava podatkov s tahografsko kartico*

DEX_203 VU mora preverjati celovitost in avtentičnost podatkov, uvoženih iz tahografskih kartic.

DEX_204 Če zazna napako celovitosti ali avtentičnosti podatkov iz kartic, mora VU:

- oblikovati revizijski zapis,
- ne uporabljati podatkov.

DEX_205 VU mora iznašati podatke na kartico skupaj z ustreznimi varnostnimi atributi, tako da lahko kartica preverja njihovo celovitost in avtentičnost.

4.8.3 *Izmenjava podatkov z zunanje pomnilne medije (prenos podatkov na zunanje pomnilne medije)*

DEX_206 VU mora tvoriti evidenco izvorov podatkov, ki jih prenaša na zunanje pomnilne medije.

DEX_207 VU mora prejemniku omogočati preverjanje evidence izvorov prenesenih podatkov.

DEX_208 VU mora prenašati podatke na zunanje pomnilne medije skupaj z ustreznimi varnostnimi atributi, tako da je mogoče preverjati celovitost in avtentičnost prenesenih podatkov.

4.9 **Kriptografska podpora**

Zahteve iz te točke veljajo le po potrebi, glede na uporabljene varnostne mehanizme in proizvajalčeve rešitve.

CSP_201 Vse kriptografske operacije VU morajo biti opravljene po predpisanem algoritmu in s predpisano velikostjo ključa.

CSP_202 Kadar VU tvori kriptografske ključke, mora to izvajati po predpisanih algoritmihi za tvorbo kriptografskih ključev in s predpisano velikostjo kriptografskih ključev.

CSP_203 Kadar VU distribuira kriptografske ključke, mora to izvajati po predpisanih postopkih distribucije ključev.

CSP_204 Kadar VU dostopa do kriptografskih ključev, mora dostopati do njih po predpisanih postopkih dostopa do ključev.

CSP_205 Kadar VU uničuje kriptografske ključke, jih mora uničevati po predpisanih postopkih uničevanja kriptografskih ključev.

5. **Opredelitev varnostnih mehanizmov**

Zahtevani varnostni mehanizmi so predpisani v dodatku 11.

Vse druge varnostne mehanizme predpišejo proizvajalci.

6. **Minimalna trdnost varnostnih mehanizmov**

Minimalna trdnost varnostnih mehanizmov enote v vozilu je po opredelitvi (ITSEC) visoka.

7. **Raven zagotavljanja varnosti**

Ciljna raven zagotavljanja varnosti enote v vozilu je po opredelitvi v (ITSEC) raven ITSEC E3.

	Grožnje																Informacijski cilji										
	Dostop Identifikacija	Napake	Preskusi	Projekiranje	Calibration Parameters	Card Data Exchange	Ura	Okolje	Fake Devices	Strojna oprema	Podatki o gibanju	Neaktivirana	Izhodni podatki	Napajanje	Security Data	Programska oprema	Stored Data	Dostop	Odgovornost	Revizija	Avtentifikacija	Celovitost	Izhod	Obdelava	Zanesljivost	Secured Data Exchange	
UIA_214 Neuspela avtentifikacija	x	x							x										x								
UIA_215 Identifikacija uporabnika na daljavo	x	x																x		x						x	
UIA_216 Identiteta uporabnika na daljavo	x	x																x		x							
UIA_217 Avtentifikacija uporabnika na daljavo	x	x																x		x						x	
UIA_218 Načini avtentifikacije	x	x																x		x							
UIA_219 Nepozabna avtentifikacija	x	x																x		x							
UIA_220 Neuspela avtentifikacija	x	x																									
UIA_221 Identifikacija naprave za upravljanje	x	x																x		x							
UIA_222 Avtentifikacija naprave za upravljanje	x	x																x		x							
UIA_223 Nepozabna avtentifikacija	x	x																x		x							
Upravljanje dostopa																											
ACC_201 Politika upravljanja dostopa	x				x	x									x	x	x										
ACC_202 Pravice dostopa do funkcij	x				x	x												x									
ACC_203 Pravice dostopa do funkcij	x				x	x												x									
ACC_204 VU ID																		x	x								
ACC_205 ID priključenega zaznavala gibanja									x									x	x								
ACC_206 Kalibracijski podatki	x				x													x	x								
ACC_207 Kalibracijski podatki					x													x	x								
ACC_208 Podatki za nastavljanje časa						x												x	x								
ACC_209 Podatki za nastavljanje časa						x												x	x								
ACC_210 Varnostni podatki																x	x	x									
ACC_211 Datotečna struktura in pogoji dostopa	x				x										x	x	x										
Odgovornost																											
ACT_201 Voznikova odgovornost																			x								
ACT_202 ID podatki VU																			x	x							
ACT_203 Odgovornost delavnice																			x								
ACT_204 Odgovornost kontrolorja																			x								
ACT_205 Odgovornost glede gibanja vozila:																			x								
ACT_206 Odgovornost za spremembe podatkov																		x				x			x		
ACT_207 Odgovornost za spremembe podatkov																		x				x			x		

[illegible]

GENERIČNI VARNOSTNI CILJ TAHOGRAFSKIH KARTIC

1. Uvod

Ta dokument vsebuje opise tahografske kartice, groženj, ki jih mora obvladovati in varnostnih ciljev, ki jih mora dosegati. Dokument predpisuje funkcije zagotavljanja varnosti. Navaja najmanjšo obvezno trdnost varnostnih mehanizmov in zahtevano raven zagotavljanja varnosti, ki jih je treba upoštevati pri razvoju in ocenjevanju.

V tem dokumentu omenjene zahteve so zahteve, podane v osnovnem besedilu priloge I B. Da bi bila predstavitev čim jasnejša, se zahteve v besedilu priloge I B in zahteve varnostnih ciljev ponekod podvajajo. Pri morebitnih razlikah med omembami besedila v prilogi I B v teh zahtevah glede varnostnih ciljev in osnovnim besedilom priloge I B se upošteva osnovno besedilo priloge I B.

Zahteve v osnovnem besedilu priloge I B, ki jih varnostni cilji ne omenjajo, niso predmet funkcij zagotavljanja varnosti.

Tahografska kartica je standardna pametna kartica, ki vsebuje namensko tahografsko aplikacijo in mora izpolnjevati naj-novejše funkcionalne in varnostne zahteve za pametne kartice. Ta varnostni cilj zato obravnava le posebne varnostne zahteve za tahografsko aplikacijo.

Grožnje, cilji, postopki in specifikacije SEF so označeni z enoznačnimi naslovi, tako da je mogoča njihova sledljivost v projektni in ocenjevalni dokumentaciji.

2. Kratice, opredelitve in literatura**2.1 Kratice**

IC	IC integrirano vezje (elektronsko vezje, namenjeno za obdelavo in hranjenje podatkov)
OS	operacijski sistem
PIN	osebna identifikacijska številka
ROM	bralni pomnilnik
SFP	Politika varnostnih funkcij
TBD	bo še opredeljeno
TOE	cilj pri vrednotenju
TSF	varnostna funkcija cilja vrednotenja
VU	enota v vozilu.

2.2 Opredelitve

Digitalni tahograf	zapisovalna naprava
Občutljivi podatki	Podatki, shranjeni na tahografski kartici, ki jih je treba varovati glede celovitosti, nepooblaščenih sprememb in zaupnosti (kjer pride v poštev za varnostne podatke). Občutljivi podatki obsegajo varnostne podatke in uporabniške podatke.
Varnostni podatki	posebni podatki, potrebni za podporo funkcij zagotavljanja varnosti (npr. kriptografski ključi)
Sistem	oprema, osebje ali organizacije, ki kakorkoli delujejo v zvezi z zapisovalno napravo
Uporabnik	katerikoli osebek (človek-uporabnik ali zunanji informacijski uporabnik) zunaj TOE, ki sodeluje s TOE (razen v izrazu „uporabniški podatki“)

Uporabniški podatki	občutljivi podatki, shranjeni na tahografski kartici, razen varnostnih podatkov. Uporabniški podatki vključujejo identifikacijske podatke in podatke o dejavnostih.
Identifikacijski podatki	identifikacijski podatki vključujejo identifikacijske podatke kartice in identifikacijske podatke imetnika kartice
Identifikacijski podatki	kartice uporabniški podatki, povezani z identifikacijo kartice, opredeljeni v zahtevah 190, 191, 192, 194, 215, 231 in 235.
Identifikacijski podatki imetnika kartice	uporabniški podatki, povezani z identifikacijo imetnika kartice, opredeljeni v zahtevah 195, 196, 216, 232 in 236.
Podatki o dejavnostih	Podatki o dejavnostih vključujejo podatke o dejavnostih imetnika kartice, dogodkih in napakah ter podatke o nadzornih dejavnostih.
Podatki o dejavnostih	imetnika kartice uporabniški podatki, povezani z dejavnostmi imetnika kartice, opredeljeni v zahtevah 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 in 237.
Podatki o dogodkih in napakah	uporabniški podatki, povezani z dogodki in napakami, opredeljeni v zahtevah 204, 205, 207, 208 in 223.
Podatki o nadzornih dejavnostih	uporabniški podatki, povezani z dejavnostmi uveljavljanja predpisov, opredeljeni v zahtevah 210 in 225.

2.3 Literatura

ITSEC	Merila vrednotenja informacijske varnosti ITSEC 1991
IC PP	Zaščitni profil integriranih vezij pametnih kartic — verzija 2.0 — izdaja septembra 1998. Registriran pri francoskem certifikacijskem organu pod številko PP/9806.
ES PP	Zaščitni profil integriranih vezij pametnih kartic z vgrajeno programsko opremo — verzija 2.0 — izdaja junija 99. Registriran pri francoskem certifikacijskem organu pod številko PP/9911.

3. Obrazložitev izdelka

3.1 Opis tahografske kartice in načina uporabe

Tahografska kartica je pametna kartica, opisana v (IC PP) in (ES PP), ki vsebuje aplikacijo za uporabo z zapisovalno napravo.

Osnovne funkcije tahografske kartice so:

- hraniti identifikacijske podatke kartice in identifikacijske podatke imetnika kartice. Te podatke uporablja enota v vozilu za identifikacijo imetnika kartice in temu ustrezno zagotavljanje pravic dostopa do funkcij in podatkov ter za zagotavljanje odgovornosti imetnika kartice za svoje dejavnosti,
- hranjenje podatkov o dejavnostih imetnika kartice, podatkov o dogodkih in napakah ter podatkov o nadzornih dejavnostih, povezanih z imetnikom kartice.

Tahografska kartica je torej namenjena za uporabo v vmesniški napravi za kartice enote v vozilu. Lahko jo uporablja tudi katerikoli drug čitalnik kartic (npr. na osebem računalniku), ki mora imeti polno pravico branja vseh uporabniških podatkov.

V fazi končne uporabe v življenjskem ciklu tahografske kartice (7. faza življenjskega cikla po (ES PP)) sme na kartico zapisovati podatke samo enota v vozilu.

Funkcionalne zahteve za tahografsko kartico so predpisane v osnovnem besedilu priloge I B in v dodatku 2.

3.2 Življenjski cikel tahografske kartice

Življenjski cikel tahografske kartice je v skladu z življenjskim ciklom pametne kartice, opisanim v (ES PP).

3.3 Grožnje

Poleg splošnim grožnjam tahografskim karticam, naštetim v (ES PP) in (IC PP), je lahko tahografska kartica izpostavljena še naslednjim grožnjam:

3.3.1 Končni cilji

Končni cilj napadalcem bo spremeniti uporabniške podatke shranjene v TOE.

T.Ident_Data	Uspešna sprememba identifikacijskih podatkov shranjenih v TOE (npr. vrste kartice, datuma izteka veljavnosti kartice, identifikacijskih podatkov imetnika kartice) bi lahko omogočila goljufivo uporabo TOE in bi pomenila veliko grožnjo skupnemu varnostnemu cilju sistema.
T.Activity_Data	Uspešna sprememba podatkov o dejavnostih shranjenih v TOE bi ogrozila varnost TOE.
T.Data_Exchange	Uspešna sprememba podatkov o dejavnostih (dodajanje, brisanje, spreminjanje) med uvozom ali izvozom podatkov bi ogrozila varnost TOE.

3.3.2 Poti napadov

Možni načini napada na TOE so:

- poskus pridobitve neupravičenih podatkov o strojni in programski zasnovi TOE, še zlasti o njenih varnostnih funkcijah ali varnostnih podatkih. Neupravičene podatke se lahko pridobi z napadi na projektantova ali proizvajalčeva gradiva (kraja, podkupovanje, ...) ali z neposrednim preučevanjem TOE (fizično sondiranje, interferenčna analiza, ...)
- izkoriščanje slabosti projekta ali izvedbe TOE (izkoriščanje napak na strojni opremi, napak v programski opremi, napak pri prenosu, napak, ki jih na TOE povzročijo okoljske obremenitve, izkoriščanje slabosti varnostnih funkcij, npr. avtentifikacijskih postopkov, upravljanja dostopa do podatkov, kriptografskih operacij, ...),
- spreminjanje TOE ali njenih varnostnih funkcij s fizičnimi, električnimi ali logičnimi posegi ali njihovimi kombinacijami.

3.4 Varnostni cilji

Glavni varnostni cilj celotnega digitalnega tahografskega sistema je naslednji:

O.Main	Podatki, ki jih preverjajo nadzorni organi, morajo biti na voljo in morajo v celoti in točno odražati dejavnosti nadzorovanih voznikov in vozil, kar se tiče obdobja vožnje, dela, razpoložljivosti in odmorov in kar se tiče hitrosti vozila.
--------	--

Zato so varnostni cilji TOE v okviru splošnega varnostnega cilja naslednji:

O.Card_Identification_Data	TOE mora ohranяти identifikacijske podatke katrice in identifikacijske podatke imetnika kartice, ki se nanjo shranijo med presonalizacijo.
O.Card_Activity_Storage	TOE mora ohranяти uporabniške podatke, ki jih nanjo shranijo enote v vozilu.

3.5 Informacijski varnostni cilji

Poleg splošnih varnostnih ciljev pametnih kartic, naštetih v (ES PP) in (IC PP), so posebni informacijski varnostni cilji TOE v okviru glavnega varnostnega cilja v fazi končne uporabe v življenjskem ciklu naslednji:

O.Data_Access	TOE mora omejevati pravico pisanja uporabniških podatkov na avtentificirane enote v vozilu,
O.Secure_Communications	TOE mora podpirati protokole in postopke varnega komuniciranja med kartico in vmesniško napravo za kartice na enoti v vozilu, ki jih zahteva aplikacija.

3.6 Načini zagotavljanja varnosti s fizičnega vidika, vidika osebja in vidika postopkov

Načini zagotavljanja varnosti TOE s fizičnega vidika, vidika osebja in vidika postopkov so našteti v (ES PP) in (IC PP) (poglavja o okoljskih varnostnih ciljih).

4. Funkcije zagotavljanja varnosti

Ta točka podrobneje obravnava nekatere dovoljene operacije, npr. prirejanje ali izbiro (ES PP) in podaja dodatne funkcionalne zahteve za SEF.

4.1 Skladnost s profili zaščite

CPP_301 TOE mora biti v skladu z (IC PP).

CPP_302 TOE mora biti v skladu z (ES PP), kakor je podrobneje opisano v nadaljevanju.

4.2 Identifikacija in avtentifikacija uporabnika

Kartica mora identificirati osebek, v katerem je vstavljena, in mora vedeti, ali je ta osebek avtentificirana enota v vozilu ali ne. Kartica lahko vsakemu povezanemu osebkcu izvaža katerekoli uporabniške podatke, razen nadzorne kartice, ki sme izvažati identifikacijske podatke imetnika kartice samo avtentificiranim enotam v vozilu (tako da lahko nadzornik ugotovi pristnost enote v vozilu po tem, da je na prikazu ali izpisu njegovo ime).

4.2.1 Identifikacija uporabnika

Prireditve (FIA_UID.1.1) *Seznam akcij TSF*: nobena.

Prireditve (FIA_ATD.1.1) *Seznam varnostnih atributov*:

USER_GROUP VEHICLE_UNIT, NON_VEHICLE_UNIT,

USER_ID registrska številka vozila (VRN) in koda države registracije (USER_ID je znano samo za USER_GROUP = VEHICLE_UNIT).

4.2.2 Avtentifikacija uporabnika

Prireditve (FIA_UAU.1.1) *Seznam akcij TSF*:

- voznikove in delavniške kartice: izvoz uporabniških podatkov z varnostnimi atributi (funkcija prenosa podatkov s kartice),
- nadzorna kartica: izvoz uporabniških podatkov brez varnostnih atributov, razen pri identifikacijskih podatkih imetnika kartice.

UIA_301 Avtentifikacijo enote v vozilu se opravi tako, da se dokaže, da razpolaga z varnostnimi podatki, ki jih je lahko distribuiral samo sistem.

Izbira (FIA_UAU.3.1 in FIA_UAU.3.2): preprečiti.

Prireditve (FIA_UAU.4.1) *Identificirani avtentifikacijski mehanizem(mehanizmi)*: katerikoli avtentifikacijski mehanizem

UIA_302 Delavniška kartica mora zagotavljati še dodatni avtentifikacijski mehanizem, preverjanje kode PIN (Ta mehanizem služi enoti v vozilu za to, da preveri identiteto imetnika kartice, ne pa za zaščito vsebine delavniške kartice).

4.2.3 Neuspela avtentifikacija

Naslednje prireditve opisujejo reakcije kartice na vsako posamezno neuspešno avtentifikacijo uporabnika.

Prireditve (FIA_AFL.1.1) *Število: 1, seznam dogodkov pri avtentifikaciji*: avtentifikacija vmesniške naprave za kartice.

Prireditve (FIA_AFL.1.2) *Seznam akcij*:

- opozoriti povezani osebek,
- prepostaviti, da je uporabnik NON_VEHICLE_UNIT.

Naslednje prireditve opisujejo reakcijo kartice ob neuspelem dodatnem avtentifikacijskem mehanizmu po zahtevi UIA_302.

Prireditve (FIA_AFL.1.1) *Število: 5, seznam dogodkov pri avtentifikaciji*: preverjanja PIN (delavniška kartica).

Prireditev (FIA_AFL.1.2) *Seznam akcij:*

- opozoriti povezani osebek,
- blokirati postopek preverjanja PIN tako, da bodo vsi naslednji poskusi preverjanja PIN neuspešni,
- znati prikazati naslednjim uporabnikom razlog blokiranja.

4.3 Upravljanje dostopa**4.3.1 Politika upravljanja dostopa**

V fazi končne uporabe velja za tahografsko kartico ena sama politika varnostnih funkcij upravljanja dostopa (SFP), imenovana AC_SFP.

Prireditev (FDP_ACC.2.1) *SFP upravljanja dostopa: AC_SFP.***4.3.2 Funkcije upravljanja dostopa****Prireditev** (FDP_ACF.1.1) *SFP upravljanja dostopa: AC_SFP.***Prireditev** (FDP_ACF.1.1) *Imenovana skupina varnostnih atributov: USER_GROUP.*

Prireditev (FDP_ACF.1.2) *Pravila uravnavanja dostopa med nadzorovanimi osebkami in nadzorovanimi predmeti, ki uporabljajo nadzorovane operacije na nadzorovanih predmetih:*

GENERAL_READ:	Uporabniške podatke lahko bere s TOE katerikoli uporabnik, razen identifikacijskih podatkov imetnika kartice, ki jih lahko z nadzornih kartic bere samo VEHICLE_UNIT.
IDENTIF_WRITE:	Identifikacijski podatki smejo biti zapisani samo enkrat in to pred koncem 6. faze življenjskega cikla kartice. Noben uporabnik ne sme vpisovati ali spreminjati identifikacijskih podatkov v fazi končne uporabe v življenjskem ciklu kartice.
ACTIVITY_WRITE:	Podatke o dejavnostih sme zapisovati na TOE samo VEHICLE_UNIT.
SOFT_UPGRADE:	Noben uporabnik ne sme nadgrajevati programske opreme TOE.
FILE_STRUCTURE:	Datotečna struktura in pogoji dostopa morajo biti tvorjeni pred koncem 6. faze življenjskega cikla TOE, nato pa morajo biti zavarovani pred kakršnim koli spreminjanjem ali brisanjem s strani kateregakoli uporabnika.

4.4 Odgovornost

ACT_301 TOE mora hraniti trajne identifikacijske podatke.

ACT_302 Datum in čas personalizacije TOE morata biti označena. Ta oznaka mora biti taka, da se je ne da spreminjati.

4.5 Revizija

TOE mora spremljati dogodke, ki kažejo na morebitno kršenje njene varnosti.

Prireditev (FAU_SAA.1.2) *Podmnožica opredeljenih revizijskih dogodkov:*

- neuspela avtentifikacija imetnika kartice (5 zaporednih neuspešnih preverjanj PIN),
- napaka med preskusom lastnega delovanja,
- napaka v celovitosti shranjenih podatkov,
- napaka v celovitosti vnesenih podatkov o dejavnostih.

4.6 Točnost**4.6.1 Celovitost shranjenih podatkov****Prireditev** (FDP_SDI.2.2) *Ukrepi, ki jih je treba izvesti: opozoriti povezani osebek,***4.6.2 Osnovna avtentifikacija podatkov****Prireditev** (FDP_DAU.1.1) *Seznam objektov ali informacijskih tipov: podatki o dejavnostih.***Prireditev** (FDP_DAU.1.2) *Seznam subjektov: katerikoli.*

4.7 Zanesljivost storitev

4.7.1 Preskusi

Izbira (FPT TST.1.1): med začetnim zagonom, občasno med normalnim delovanjem.

Opombamed začetnim zagonom pomeni pred izvajanjem programa (ne pa nujno med postopkom odgovora na ponastavitev).

RLB_301 Preskusi lastnega delovanja TOE morajo vključevati preverjanje celovitosti programov, ki niso shranjeni v ROM.

RLB_302 Ob zaznani napaki med preskušanjem lastnega delovanja mora TSF opozoriti povezani osebek.

RLB_303 Po zaključenem preskusu OS je treba vse ukaze in akcije, namenjene posebej preskušanju, onesposobiti ali odstraniti. Ne sme biti mogoča kasnejša preglasitev teh ukrepov in obnova ukazov in akcij za uporabo. Ukazi, povezani izključno z enim stanjem v življenjskem ciklu, ne smejo biti dosegljivi v nobenem drugem stanju.

4.7.2 Programska oprema

RLB_304 Programske opreme TOE na terenu ne sme biti mogoče analizirati, odpravljati napak v njej ali spreminjati.

RLB_305 TOE ne sme sprejemati vhodov iz zunanjih virov kot izvršnih programov.

4.7.3 Napajanje

RLB_306 TOE mora med izpadom ali nihanji napajanja ostati v varnem stanju.

4.7.4 Stanje ponastavitve

RLB_307 Ob prekinitvi napajanja (ali nihanji napajanja) TOE ali ob prekinitvi transakcije pred njenim zaključkom ali v drugih stanih ponastavitve se mora TOE ponastaviti na čist način.

4.8 Izmenjava podatkov

4.8.1 Izmenjava podatkov z enoto v vozilu

DEX_301 TOE mora preverjati celovitost in avtentičnost podatkov, uvoženih iz enote v vozilu.

DEX_302 Če zazna napako celovitosti uvoženih podatkov, mora TOE:

— opozoriti osebek, ki pošilja podatke,

— ne uporabljati podatkov.

DEX_303 TOE mora izvažati podatke enoti v vozilu skupaj z ustreznimi varnostnimi atributi, tako da lahko enota v vozilu preverja njihovo celovitost in avtentičnost.

4.8.2 Izvoz podatkov v enote zunaj vozila (funkcija prenosa podatkov)

DEX_304 TOE mora biti zmožna tvoriti evidenco izvorov podatkov, ki jih prenaša na zunanje pomnilne medije.

DEX_305 TOE mora prejemniku omogočati preverjanje evidence izvorov prenesenih podatkov.

DEX_306 TOE mora biti zmožna prenašati podatke na zunanje pomnilne medije skupaj z ustreznimi varnostnimi atributi, tako da je mogoče preverjati celovitost in avtentičnost prenesenih podatkov.

4.9 Kriptografska podpora

CSP_301 Kadar TOE tvori kriptografske ključe, mora to izvajati po predpisanih algoritmihi za tvorbo kriptografskih ključev in s predpisano velikostjo kriptografskih ključev. Tvorjeni kriptografski ključi se morajo imeti omejeno število (ki ga opredeli proizvajalec, vendar ne sme presežati 240) dovoljenih uporab.

CSP_302 Kadar TOE distribuira kriptografske ključe, mora to izvajati po predpisanih postopkih distribucije kriptografskih ključev.

5. Opredelitev varnostnih mehanizmov

Zahtevani varnostni mehanizmi so predpisani v dodatku 11.

Vse druge varnostne mehanizme predpišejo proizvajalci TOE.

6. Zahtevana minimalna trdnost varnostnih mehanizmov

Minimalna trdnost varnostnih mehanizmov tahografske kartice je po opredelitvi (ITSEC) visoka.

7. Raven zagotavljanja varnosti

Ciljna raven zagotavljanja varnosti tahografske kartice je po opredelitvi v (ITSEC) raven ITSEC E3.

8. Obrazložitev

Naslednje matrike razlagajo dodatne SEF s prikazom naslednjih postavk:

- katere SEF delujejo proti katerim grožnjam,
- katere SEF izpolnjujejo katere informacijske varnostne cilje.

	Grožnje											Informacijski cilji									
	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.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Data_Access	Secured_Communications	
UIA_301 Načini avtentifikacije																			x		
UIA_302 Preverjanje PIN																			x		
ACT_301 Identifikacijski podatki																					
ACT_302 Datum personalizacije																					
RLB_301 Celovitost programske opreme												x		x							
RLB_302 Preskusi lastnega delovanja												x		x							
RLB_303 Preskusi med proizvodnjo					x	x						x		x							
RLB_304 Analiza programske opreme					x		x	x				x		x							
RLB_305 Vnos programske opreme					x	x		x				x		x							
RLB_306 Napajanje									x	x		x		x							
RLB_307 Ponastavljanje												x		x							
DEX_301 Zavarovan uvoz podatkov											x									x	
DEX_302 Zavarovan uvoz podatkov											x									x	
DEX_303 Zavarovan izvoz podatkov v VU											x									x	
DEX_304 Evidenca izvorov											x									x	
DEX_305 Evidenca izvorov											x									x	
DEX_306 Zavarovan prenos podatkov na zunanje medije											x									x	
CSP_301 Tvorba ključev												x								x	
CSP_302 Distribucija ključev												x								x	

Dodatek 11

SKUPNI VARNOSTNI MEHANIZMI

VSEBINA

1.	Splošno	516
1.1	Literatura	516
1.2	Notacija in kratice	517
2.	Kriptografski sistemi in algoritmi	518
2.1	Kriptografski sistemi	518
2.2	Kriptografski algoritmi	518
2.2.1	Algoritem RSA	518
2.2.2	Algoritem razpršitve	518
2.2.3	Algoritem šifriranja podatkov	518
3.	Ključni in certifikati	518
3.1	Tvorba in distribucija ključev	518
3.1.1	Tvorba in distribucija ključev RSA	518
3.1.2	Preskusni ključni RSA	520
3.1.3	Ključni zaznavala gibanja	520
3.1.4	Tvorba in distribucija ključev sej T-DES	520
3.2	Ključni	520
3.3	Certifikati	520
3.3.1	Vsebina certifikatov	521
3.3.2	Izdani certifikati	522
3.3.3	Preverjanje in razvijanje certifikatov	523
4.	Mehanizem medsebojne avtentifikacije	523
5.	Mehanizem zaupnosti, celovitosti in avtentifikacije prenosa podatkov med VU in kartico	526
5.1	Varno sporočanje	526
5.2	Obravnava napak pri varnem sporočanju	527
5.3	Algoritmi izračuna kriptografskih preskusnih vsot	528
5.4	Algoritmi izračuna kriptogramov za DO povezane z zaupnostjo	528
6.	Mehanizmi digitalnega podpisa za prenos podatkov	529
6.1	Tvorba podpisa	529
6.2	Preverjanje podpisa	529

1. SPLOŠNO

Ta dodatek predpisuje varnostne mehanizme za zagotavljanje:

- medsebojne avtentifikacije med VU in tahografskimi karticami, vključno z dogovori o ključih sej,
- zaupnosti, celovitosti in avtentifikacije podatkov, ki se prenašajo med VU in tahografskimi karticami,
- celovitosti in avtentifikacije podatkov, ki se prenašajo z VU na zunanje pomnilne medije,
- celovitosti in avtentifikacije podatkov, ki se prenašajo s tahografske kartice na zunanje pomnilne medije.

1.1 Literatura

V tem dodatku so uporabljeni naslednji viri:

SHA-1	Nacionalni institut za standarde in tehnologijo (NIST): Publikacija FIPS 180-1: Standard varnostnega razprševanja. April 1995
PKCS1	Laboratoriji RSA. PKCS # 1: Standard šifriranja RSA. Verzija 2.0. Oktober 1998
TDES	Nacionalni institut za standarde in tehnologijo (NIST): Publikacija FIPS 46-3: Standard šifriranja podatkov. Osnutek 1999
TDES-OP	ANSI X9.52, Načini delovanja algoritma trojnega šifriranja podatkov. 1998
ISO/IEC 7816-4	Informacijska tehnologija – Identifikacijske kartice – Kontaktne kartice s tiskanimi vezji – Del 4: Panožni ukazi za izmenjavo. Prva izdaja: 1995 +dopolnitev 1: 1997
ISO/IEC 7816-6	Informacijska tehnologija – Identifikacijske kartice – Kontaktne kartice s tiskanimi vezji – Del 6: Panožni podatkovni elementi. Prva izdaja: 1996 + popr. 1: 1998
ISO/IEC 7816-8	Informacijska tehnologija – Identifikacijske kartice – Kontaktne kartice s tiskanimi vezji – Del 8: Panožni ukazi povezani z varnostjo. Prva izdaja: 1999
ISO/IEC 9796-2	Informacijska tehnologija – Varnostne tehnike – Sheme digitalnih ključev za obnovo sporočil – Del 2: Mehanizmi, ki uporabljajo funkcijo razpršitve. Prva izdaja: 1997
ISO/IEC 9798-3	Informacijska tehnologija – Varnostne tehnike – Sheme digitalnih ključev za obnovo sporočil – Del 3: Avtentifikacija osebkov z algoritmom javnega ključa. Druga izdaja: 1998
ISO 16844-3	Cestna vozila – Tahografski sistemi – Del 3: Vmesnik za zaznavalo gibanja.

1.2 Notacija in kratice

V tem dodatku so uporabljene notacije in kratice:

(K_a, K_b, K_c)	šop ključev za algoritem trojnega šifriranja podatkov
CA	certifikacijska agencija
CAR	referenca certifikacijske agencije
CC	kriptografska preskusna vsota
CG	kriptogram
CH	glava ukaza
CHA	pooblastilo imentika certifikata
CHR	referenca imentika certifikata
$D()$	dešifriranje z DES
DE	podatkovni element
DO	podatkovni objekt
d	zasebni ključ RSA, zasebni eksponent
e	javni ključ RSA, javni eksponent
$E()$	šifriranje z DES
EQT	oprema
$Hash()$	vrednost razpršitve, izhod funkcije razpršitve
$Hash$	funkcija razpršitve
KID	identifikator ključa
K_m	ključ TDES. Glavni ključ po opredelitvi v ISO 16844-3
$K_{m_{vu}}$	ključ TDES vstavljen v enote v vozilih
$K_{m_{wc}}$	ključ TDES vstavljen v delavniške kartice
m	predstavnik sporočila, cela vrednost med 0 in $n-1$
n	ključi RSA, modul
PB	bajti omota
PI	označevalni bajt omota (za kriptograme DO, povezanih z zaupnostjo)
PV	nešifrirana vrednost
s	predstavnik podpisa, cela vrednost med 0 in $n-1$
SSC	števec sekvence pošiljanja
SM	varno sporočanje
TCBC	režim delovanja z veriženjem šifrirnih blokov TDEA
TDEA	Algoritem trojnega šifriranja podatkov
TLV	vrednost dolžine značke
VU	enota v vozilu.
X.C	certifikat uporabnika X, izdan od certifikacijske agencije
X.CA	certifikatsko pooblastilo uporabnika X
$X.CA.PK_oX.C$	operacija razvitja certifikata za ekstrakcijo javnega ključa. To je vmesni operator, katerega levi operand je javni ključ certifikacijske agencije, desni operand pa certifikat, izdan od te certifikacijske agencije. Rezultat je javni ključ uporabnika X, katerega certifikat je desni operand,

X.PK	javni ključ uporabnika X
X.PK[I]	informacija I, šifrirana po RSA ob uporabi javnega ključa uporabnika X
X.SK	zasebni ključ RSA uporabnika X
X.SK[I]	informacija I, šifrirana po RSA ob uporabi zasebnega ključa uporabnika X
'xx'	šestnajstiška vrednost
	operator združevanja.

2. KRIPTOGRAFSKI SISTEMI IN ALGORITMI

2.1 Kriptografski sistemi

CSM_001 Enote v vozilu in tahografske kartice morajo uporabljati klasični kriptografski sistem RSA z javnim ključem za zagotavljanje naslednjih varnostnih mehanizmov:

- avtentifikacija med enotami v vozilu in karticami,
- prenos ključev sej 3-DES med enotami v vozilu in tahografskimi karticami,
- digitalno podpisovanje podatkov, ki se prenašajo iz enot v vozilu ali tahografskih kartic na zunanje pomnilne medije.

CSM_002 Enote v vozilu in tahografske kartice morajo uporabljati simetrični kriptografski sistem 3-DES za zagotavljanje mehanizma celovitosti podatkov pri izmenjavi uporabniških podatkov med enotami v vozilu in tahografskimi karticami ter za po potrebi zagotavljanje zaupnosti izmenjave podatkov med enotami v vozilu in tahografskimi karticami.

2.2 Kriptografski algoritmi

2.2.1 Algoritem RSA

CSM_003 Algoritem RSA v celoti opredeljujeta naslednji relaciji:

$$\begin{aligned} \text{X.SK}[m] &= s = m^d \bmod n \\ \text{X.PK}[s] &= m = s^e \bmod n \end{aligned}$$

Popolnejši opis funkcije RSA je podan v viru (PKCS1). Javni eksponent e za izračune RSA bo različen od 2 pri vseh tvorjenih ključih RSA.

2.2.2 Algoritem razpršitve

CSM_004 Mehanizmi digitalnega podpisa morajo uporabljati algoritem razpršitve SHA-1, opredeljen v viru (SHA-1).

2.2.3 Algoritem šifriranja podatkov

CSM_005 V režimu veriženja šifrirnih blokov se uporabljajo algoritmi na podlagi DES.

3. KLJUČI IN CERTIFIKATI

3.1 Tvorba in distribucija ključev

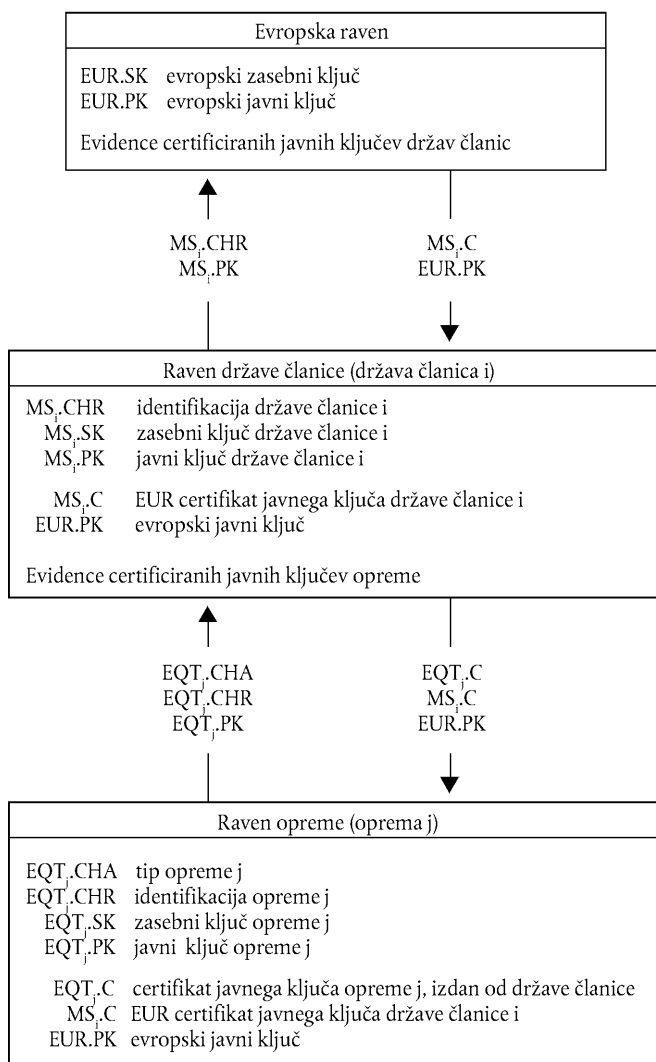
3.1.1 Tvorba in distribucija ključev RSA

CSM_006 Ključi RSA se tvorijo na treh funkcionalnih hierarhičnih ravneh:

- evropski ravni,
- ravni države članice,
- ravni opreme.

- CSM_007 Na evropski ravni se tvori en sam evropski par ključev (EUR.SK in EUR.PK). Evropski zasebni ključ se uporablja za certificiranje javnih ključev držav članic. Vodi se evidenca vseh certificiranih ključev. Te naloge opravlja evropska certifikacijska agencija v pristojnosti in odgovornosti Evropske komisije.
- CSM_008 Na ravni držav članic se tvori par ključev države članice (MS.SK in MS.PK). Javne ključe držav članic certificira evropska certifikacijska agencija. Zasebni ključ države članice se uporablja za certificiranje javnih ključev, ki se vstavljajo v opremo (enote v vozilu in tahografske kartice). Vodi se evidenca certificiranih javnih ključev z identifikacijo opreme, za katero so namenjeni. Te naloge opravljajo certifikacijske agencije držav članic. Država članica mora redno spreminjati svoj par ključev.
- CSM_009 Na ravni opreme se tvori en sam ključev (EQT.SK in EQT.PK) in se vstavi v vsak primerek opreme. Javne ključe opreme certificira certifikacijska agencija države članice. Te naloge lahko opravljajo proizvajalci opreme, izvajalci personalizacije opreme ali organi držav članic. Ti pari ključev služijo za storitve avtentifikacije, digitalnega podpisovanja in šifriranja.
- CSM_010 Med tvorbo, prenosom (če pride do njega) in hranjenjem je treba vzdrževati zaupnost zasebnih ključev. Naslednja slika povzema tok podatkov v tem procesu:

Evropska raven



3.1.2 Preskusni ključi RSA

- CSM_011 Za preskušanje opreme (vključno s preskušanjem skupne uporabnosti) evropska certifikacijska agencija tvori drugačen enojen evropski par preskusnih ključev in vsaj preskusna para ključev za dve državi članici; javna ključa v teh parih se certificira z zasebnim evropskim preskusnim ključem. Proizvajalci morajo v opremo, ki jo predložijo v preskušanje odobritve tipa, vložiti preskusne ključe, certificirane z enim od teh preskusnih ključev držav članic.

3.1.3 Ključi zaznavala gibanja

Med tvorbo, prenosom (če pride do njega) in hranjenjem je treba vzdrževati zaupnost treh spodaj opisanih ključev TDES.

Za zagotavljanje skladnosti opreme z ISO 16844 morajo evropska certifikacijska agencija in certifikacijske agencije držav članic zagotoviti dodatno še naslednje:

- CSM_036 Evropska certifikacijska agencija mora tvoriti Km_{VU} in Km_{WC} , dva neodvisna in enkratna ključa 3-DES, ter tvoriti Km kot:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

Evropska certifikacijska agencija mora te ključe na zahtevo posredovati certifikacijskim agencijam držav članic z ustrezno zavarovanimi postopki.

- CSM_037 Certifikacijske agencije držav članic morajo:

- uporabljati Km za šifriranje podatkov zaznaval gibanja za potrebe proizvajalcev zaznaval gibanja (podatki, ki se šifrirajo s Km , so opredeljeni v ISO 16844-3),
- z ustrezno zavarovanimi postopki posredovati Km_{VU} proizvajalcem enot v vozilu za vstavitev v enote v vozilu,
- zagotoviti, da se Km_{WC} vstavi v vse delavniške kartice (*SensorInstallationSecData* v elementarni datoteki *Sensor_Installation_Data*) med personalizacijo kartic.

3.1.4 Tvorba in distribucija ključev sej T-DES

- CSM_012 Enote v vozilu in tahografske kartice morajo v okviru procesa medsebojne avtentifikacije tvoriti in si izmenjati podatke, potrebne za izdelavo skupnega ključa seje 3-DES. Zaupnost te izmenjave podatkov mora biti zaščitena z mehanizmom šifriranja RSA.
- CSM_013 Ta ključ se uporablja za vse naslednje kriptografske operacije, ki uporabljajo varno sporočanje. Veljavnost ključa mora izteči ob koncu seje (izvlek kartice ali ponastavitev kartice) in/ali po 240 uporabah (ena uporaba ključa = en ukaz, ki uporablja varno sporočanje, poslan kartici, in odgovor na ta ukaz).

3.2 Ključi

- CSM_014 Ključi RSA morajo (na vseh ravneh) imeti naslednje dolžine: modulo n 1024 bitov, javni eksponent e največ 64 bitov, zasebni eksponent d 1024 bitov.
- CSM_015 Ključi 3-DES morajo imeti obliko (K_a, K_b, K_a) , pri čemer sta K_a in K_b neodvisna ključa dolžine 64 bitov. Nastavljen ne sme biti noben bit za ugotavljanje parnostnih napak.

3.3 Certifikati

- CSM_016 Certifikati javnih ključev RSA morajo biti 'ne-samoopisni' ,s kartico preverljivi' certifikati (vir: ISO/IEC 7816-8)

3.3.1 Vsebina certifikatov

CSM_017 Certifikate javnih ključev RSA se gradi iz naslednjih podatkov v naslednjem vrstnem redu:

Podatki	Oblika	Bajtov	Opis
CPI	CELO ŠTEVILO	1	Identifikator profila certifikata (v tej verziji ,01')
CAR	OKTETNI NIZ	8	Referenca certifikacijske agencije
CHA	OKTETNI NIZ	7	Pooblastilo imentika certifikata
EOV	TimeReal	4	Konec veljavnosti certifikata. Neobvezen; če ni uporabljen, se polje napolni s ,FF'
CHR	OKTETNI NIZ	8	Referenca imentika certifikata
<i>n</i>	OKTETNI NIZ	128	Javni ključ (modul)
<i>e</i>	OKTETNI NIZ	8	Javni ključ (javni eksponent)
		164	

Opombe:

1. Identifikator profila certifikata (CPI) določa natančno strukturo avtentifikacijskega certifikata. Lahko se uporablja v opremi kot interni identifikator ustreznega seznama, ki opisuje združevanje podatkovnih elementov v certifikatu.

Seznam, povezan s to vsebino certifikata, je naslednji:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Značka razširjenega seznama	Dolžina seznama	Značka CPI	Dolžina CPI	Značka CAR	Dolžina CAR	Značka CHA	Dolžina CHA	Značka EOv	Dolžina EOv	Značka CHR	Dolžina CHR	Značka javnega ključa (zgrajena)	Dolžina naslednjih DO	Značka modula	Dolžina modula	Značka javnega eksponenta	Dolžina javnega eksponenta

2. Referenca certifikacijske agencije (CAR) služi za identifikacijo CA izdajateljice certifikata, tako, da se podatkovni element lahko hkrati uporabi tudi kot identifikator ključa agencije za referenciranje javnega ključa certifikacijske agencije (za kodiranje – glej točko Identifikator ključa v nadaljevanju).
3. Pooblastilo imetnika certifikata (CHA) se uporablja za identifikacijo pravic imetnika certifikata. Sestavlja ga ID tahografske aplikacije in vrsta opreme, za katero je certifikat namenjen (v skladu s podatkovnim elementom EquipmentType, '00' za državo članico).
4. Referenca imetnika certifikata (CHR) služi za nedvoumno identifikacijo imetnika certifikata, tako, da se podatkovni element lahko hkrati uporabi tudi kot identifikator ključa subjekta za referenciranje javnega ključa imetnika certifikata.
5. Identifikatorji ključev nedvoumno identificirajo imetnika certifikata ali certifikacijsko agencijo. Kodirani so na naslednji način:

5.1. Oprema (VU ali kartica):

Podatki	Serijska številka opreme	Datum	Tip	Proizvajalec
Dolžina	4 bajti	2 bajta	1 bajt	1 bajt
Vrednost	celo število	BCD kodirana mm ll	Določi proizvajalec	Koda proizvajalca

Pri VU lahko proizvajalec takrat, ko zahteva certifikate, pozna ali pa ne pozna identifikacije opreme, v katero bo vstavil ključ.

Če jo pozna, pošlje identifikacijo opreme skupaj z javnim ključem certifikacijski agenciji države članice. Certifikat bo v tem primeru vseboval identifikacijo opreme, proizvajalec pa mora zagotoviti, da bodo ključ in certifikat vstavljeni v opremo, za katero so namenjeni. Identifikator ključa ima obliko, prikazano zgoraj.

Če proizvajalec identifikacije opreme ne pozna, mora nedvoumno identificirati vsak zahtevek za certifikat in poslati to identifikacijo skupaj z javnim ključem certifikacijski agenciji države članice. Certifikat bo vseboval identifikacijo zahtevka. Proizvajalec mora certifikacijsko agencijo države članice obvestiti o dodelitvi ključa opremi (t.j. sporočiti identifikacijo zahtevka in identifikacijo opreme) po namestitvi ključa v opremo. Identifikator ključa ima naslednjo obliko:

Podatki	Serijska številka zahtevka za certifikat	Datum	Tip	Proizvajalec
Dolžina	4 bajti	2 bajta	1 bajt	1 bajt
Vrednost	BCD koda	BCD kodirana mm ll	'FF'	Koda proizvajalca

5.2. Certifikacijska agencija

Podatki	Identifikacija agencije	Serijska številka ključa	Dodatne informacije	Identifikator
Dolžina	4 bajte	1 bajt	2 bajta	1 bajt
Vrednost	1-bajtna številka koda države 3-bajtna alfanumerična koda države	celo število	dodatne kode (določi CA) 'FF FF', če ni uporabljeno	'01'

Serijska številka ključa se uporablja za ločevanje med različnimi ključi države članice v primeru sprememb teh ključev.

- Osebk, ki preverjajo certifikat, morajo implicitno vedeti, da je certificirani javni ključ RSA ključ za avtentifikacijo, preverjanje digitalnega podpisa in šifriranje pri zaupnih storitvah (certifikat ne vsebuje nikakršnega identifikatorja objekta, ki bi to sporočal).

3.3.2 Izdani certifikati

CSM_018 Izdani certifikat je digitalni podpis z delno obnovitvijo vsebine certifikata v skladu z ISO/IEC 9796-2, s prilepljeno referenco certifikacijske agencije.

$$X.C = X.CA.SK[6A' || C_r || Hash(Cc) || 'BC'] || C_n || X.CAR$$

Az alábbi bizonyítványtartalommal: $= Cc =$ C_r $||$ C_n
106 bajtov 58 bajtov

Opombe:

- Ta certifikat ima dolžino 194 bajtov.
- CAR, skrit s podpisom, je prav tako prilepljen podpisu, tako da je mogoče pri preverjanju certifikata izbrati javni ključ certifikacijske agencije.
- Osebek, ki preverja certifikat, mora implicitno poznati algoritem, ki ga je uporabila certifikacijska agencija za podpis certifikata.

4. Seznam, povezan s to vsebino izdanega certifikata, je naslednji:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Značka certifikata CV (zgrajena)	Dolžina naslednjih DO	Značka podpisa	Dolžina podpisa	Značka ostanka	Dolžina ostanka	Značka CAR	Dolžina CAR

3.3.3 Preverjanje in razvijanje certifikatov

Preverjanje in razvijanje certifikata obsega preverjanje podpisa po ISO/IEC 9796-2 ter pridobitev vsebine certifikata in javnega ključa iz njega: $X.PK = X.CA.PK_o X.C$, in preverjanje veljavnosti certifikata.

CSM_019 To obsega naslednje korake:

preverjanje podpisa in pridobitev vsebine:

- pridobitev $Sign, C_n'$ in CAR' iz $X.C$:
$$X.C = \begin{array}{c} Sign \\ 128 \text{ bajtov} \end{array} \parallel \begin{array}{c} C_n' \\ 58 \text{ bajtov} \end{array} \parallel \begin{array}{c} CAR' \\ 8 \text{ bajtov} \end{array}$$
- izbira ustreznega javnega ključa certifikacijske agencije iz CAR' (če ni to že storjeno na kak drug način)
- odpiranje $Sign$ z javnim ključem CA : $Sr' = X.CA.PK [Sign]$,
- preverjanje, ali se Sr' začne s '6A' in konča z 'BC'
- izračun Cr' in H' iz:
$$Sr' = \begin{array}{c} '6A' \\ 106 \text{ bajtov} \end{array} \parallel \begin{array}{c} Cr' \\ 106 \text{ bajtov} \end{array} \parallel \begin{array}{c} H' \\ 20 \text{ bajtov} \end{array} \parallel \begin{array}{c} 'BC' \end{array}$$
- Obnovitev vsebine certifikata $C' = C \parallel C_n'$,
- preverjanje, ali je $Hash(C') = H'$

Če so preverjanja uspešna, je certifikat pravi in njegova vsebina je C' .

Preverjanje veljavnosti. Iz C' :

- po potrebi preverjanje datuma izteka veljavnosti,

Pridobitev in shranitev javnega ključa, identifikatorja ključa, pooblastila imetnika certifikata in konca veljavnosti iz C' :

- $X.PK = n \parallel e$,
- $X.KID = CHR$
- $X.CHA = CHA$,
- $X.EOV = EOV$.

4. MEHANIZEM MEDSEBOJNE AVTENTIFIKACIJE

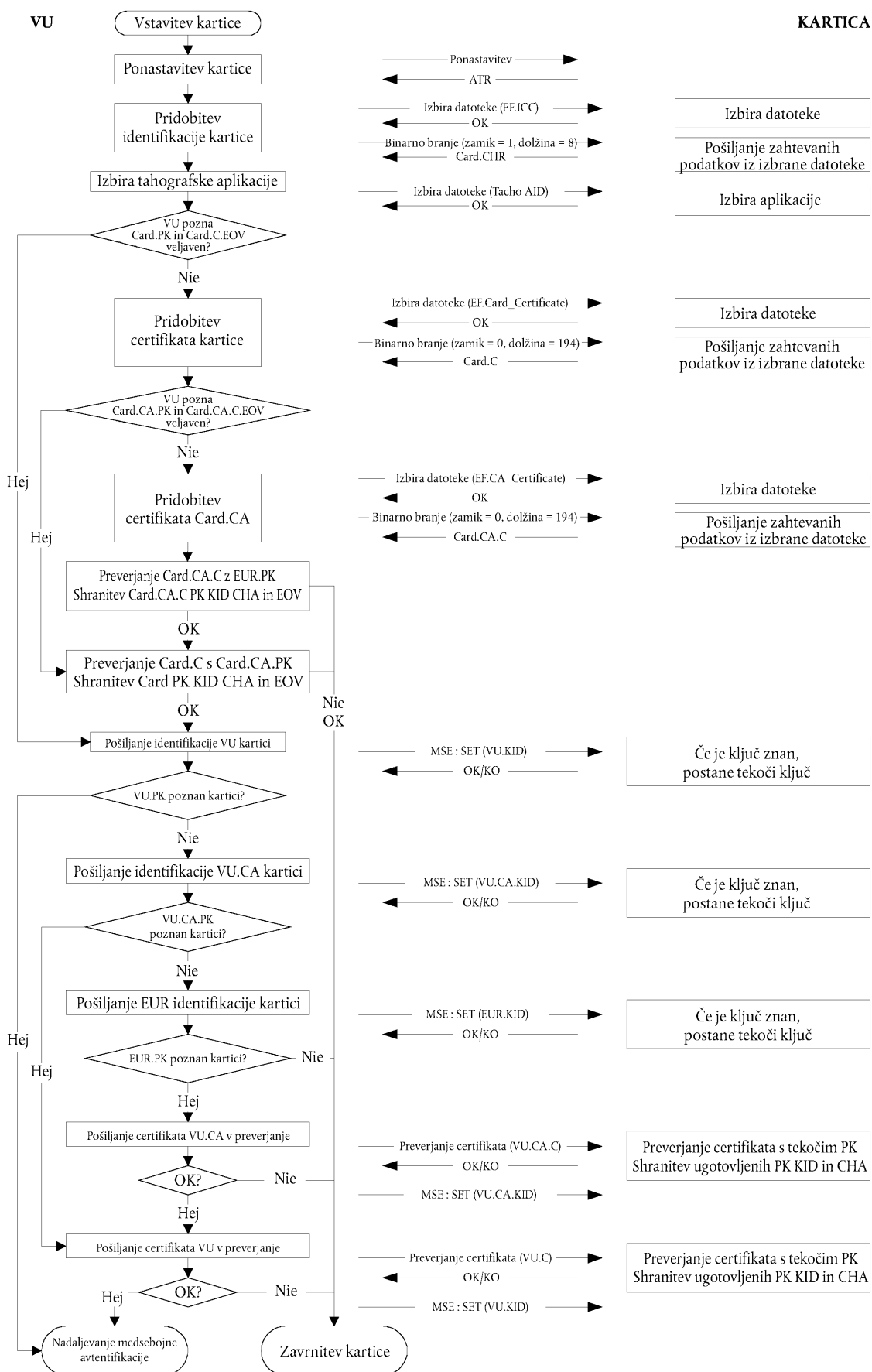
Medsebojna avtentifikacija med karticami in VU temelji na naslednjem načelu:

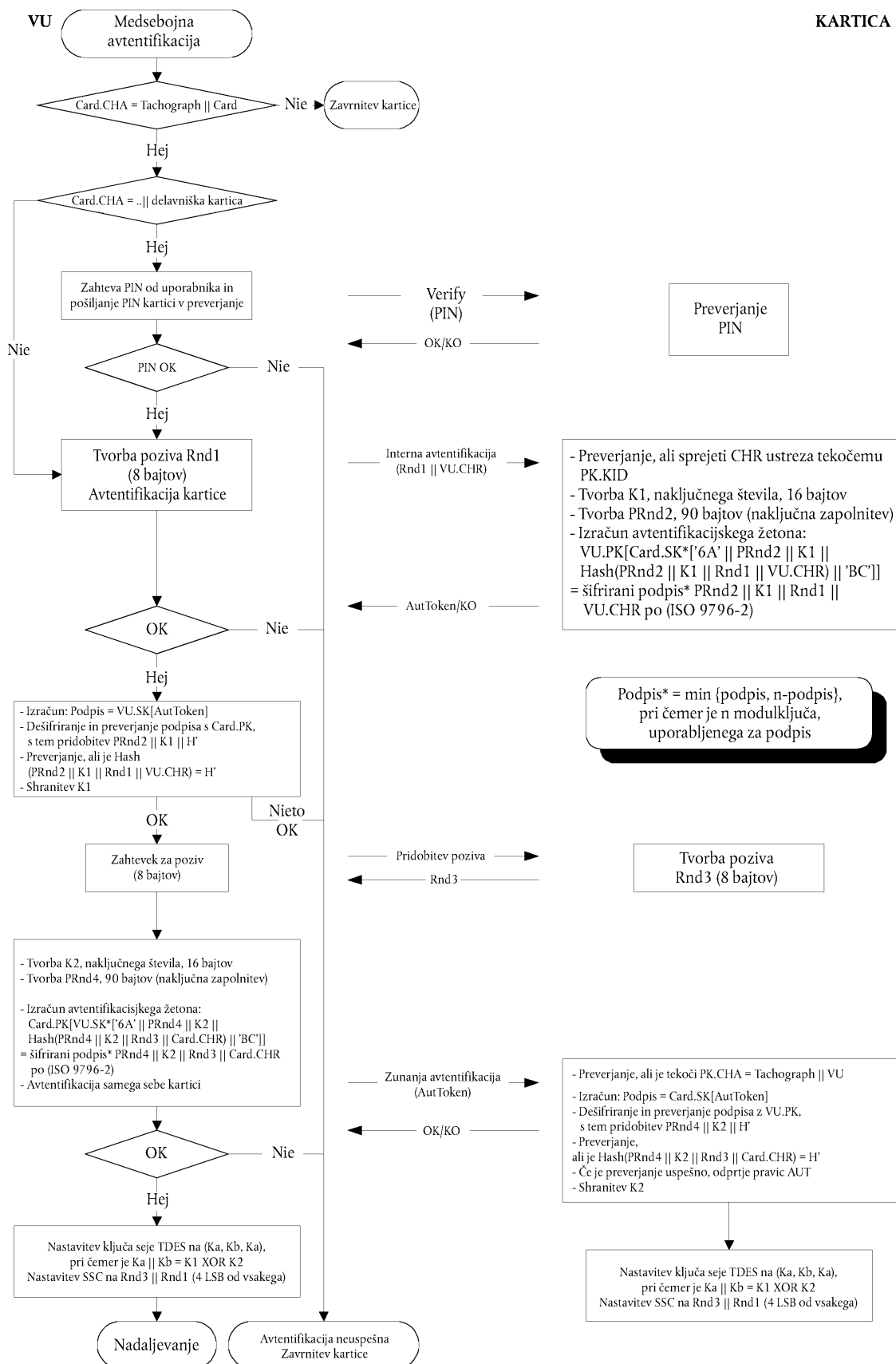
Vsaka stran mora drugi dokazati, da ima veljaven par ključev, v katerem je javni ključ certificirala certifikacijska agencija države članice, ki jo je certificirala evropska certifikacijska agencija.

Dokazovanje je opravljeno tako, da se z zasebnim ključem podpiše naključno število, ki ga je poslala druga stran; ta pa mora za preverjanje tega podpisa spet obnoviti to naključno število.

Mehanizem sproži VU ob vstavitvi kartice. Začne se z izmenjavo certifikatov in razvitjem javnih ključev, konča pa z določitvijo ključa seje.

CSM_020 Uporablja se naslednji protokol (puščice označujejo izmenjavo ukazov in podatkov (glej dodatek 2)):





5. MEHANIZMI ZAUPNOSTI, CELOVITOSTI IN AVTENTIFIKACIJE PRENOSA PODATKOV MED VU IN KARTICO

5.1 Varo sporočanje

- CSM_021 Celovitost prenosov podatkov med VU in kartico mora biti zaščitena z varnim sporočanjem v skladu z viroma (ISO/IEC 7816-4) in (ISO/IEC 7816-8).
- CSM_022 Kadar je treba podatke med prenosom zaščititi, se podatkom, poslanim v okviru ukaza ali odgovora, prilepi podatkovni objekt kriptografske preskusne vsote. Prejemnik mora preveriti kriptografsko preskusno vsoto.
- CSM_023 Kriptografska preskusna vsota v okviru ukaza poslanih podatkov mora združevati glavo ukaza in vse poslane podatkovne objekte ($\text{CLA} = 0C'$, vsi podatkovni objekti pa morajo biti opremljeni z značkami z $b1 = 1$).
- CSM_024 Kadar odgovor ne vsebuje nobenega podatkovnega polja, morajo biti s kriptografsko preskusno vsoto zaščiteni bajti stanja odgovora.
- CSM_025 Kriptografska preskusna vsota mora imeti dolžino 4 bajte.

Pri uporabi varnega sporočanja je torej struktura ukazov in odgovorov naslednja:

Uporabljeni DO so podmnožica DO varnega sporočanja, opisanih v ISO/IEC 7816-4:

Značka:	Mnemonik	Pomen
'81'	T_{PV}	Nešifrirana vrednost ne BER-TLV kodiranih podatkov (ki naj jih ščiti CC)
'97'	T_{LE}	Vrednost Le nezaščenega ukaza (ki naj ga zaščiti CC)
'99'	T_{SW}	Statusne informacije (ki naj jih zaščiti CC)
'8E'	T_{CC}	Kriptografska preskusna vsota
'87'	$T_{PI\ CG}$	Bajt znaka zapolnitve kriptogram (nešifrirana vrednost, nekodirana v BER-TLV)

Ob podanem nezaščitenem paru ukaz-odgovor:

Glava ukaza	Telo ukaza
CLA INS P1 P2	(L_c -field) (Data field) (L_e -field)
4 bajti	Bajti L , označeni kot B_1 to B_L

Telo odgovora	Rep odgovora
(Podatkovno polje)	SW1 SW2
L_r podatkovnih bajtov	dva bajta

Ustrezni zaščiteni par ukaz-odgovor je:

Zaščiteni ukaz:

Glava ukaza (CH)				Telo ukaza										
CLA	INS	P1	P2	(Novo polje L _c)	(Novo podatkovno polje)							(Novo polje L _e)		
'OC'				Dolžina novega podatkovnega 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	

Podatki, ki se jih združi v preskusno vsoto = CH || PB || T_{PV} || LPV || PV || T_{IE} || L_{IE} || Le || PB

PB = bajti za zapolnitev (80 .. 00) v skladu z ISO-IEC 7816-4 in metodo 1 po ISO 9797.

Podatkovna objekta PV in LE nastopata le, kadar je v nezaščitenem ukazu kaj podatkov.

Zaščiteni odgovor:

1. Če podatkovno polje odgovora ni prazno in ni treba zaščititi njegove zaupnosti:

Telo odgovora						Rep odgovora
(Novo podatkovno polje)						nova SW1-SW2
T _{PV}	L _{PV}	PV	T _{CC}	L _{CC}	CC	
'81'	L _r	Podatkovno polje	'8E'	'04'	CC	

Podatki, ki se jih združi v preskusno vsoto = T_{PV} || L_{PV} || PV || PB

2. Če podatkovno polje odgovora ni prazno in je treba zaščititi njegovo zaupnost:

Telo odgovora						Rep 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	

Podatki, ki jih prenaša CG: podatki, ne kodirani z BER-TLV, in bajti zapolnitve.

Podatki, ki se jih združi v preskusno vsoto = T_{PI CG} || L_{PI CG} || PI CG || PB

3. Če je podatkovno polje odgovora prazno:

Telo odgovora						Rep 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	

Podatki, ki se jih združi v preskusno vsoto = T_{sw} || L_{sw} || SW || PB

5.2 Obravnava napak pri varnem sporočanju

CSM_026 Če tahografska kartica pri interpretiranju ukaza ugotovi napako SM, mora vrniti statusna bajta brez uporabe varnega sporočanja. Po ISO/IEC 7816-4 so za označevanje napak SM opredeljeni naslednji statusni bajti:

- '66 88' neuspešno preverjanje kriptografske preskusne vsote,
- '69 87' manjkajo pričakovani podatkovni objekti varnega sporočanja,
- '69 88' nepravilni podatkovni objekti varnega sporočanja.

CSM_027 Ko tahografska kartica vrne statusna bajta brez varnega sporočanja DO ali z napako pri varnem sporočanju DO, mora VU prekiniti sejo.

5.3 Algoritmi izračuna kriptografskih preskusnih vsot

CSM_028 Kriptografske preskusne vsote se tvori z DES s podrobnimi MAC po ANSI X9.19:

- začetna faza: začetni preskusni blok y_0 je $E(K_a, SSC)$.
- naslednje zaporedne faze: preskusni bloki y_1, y_n se računajo s K_a .
- končna faza: kriptografska preskusna vsota se izračuna iz zadnjega preskusnega bloka y_n kot sledi: $E(K_a, D(K_b, y_n))$.

pri čemer pomeni $E()$ šifriranje z DES, $D()$ pa pomeni dešifriranje z DES.

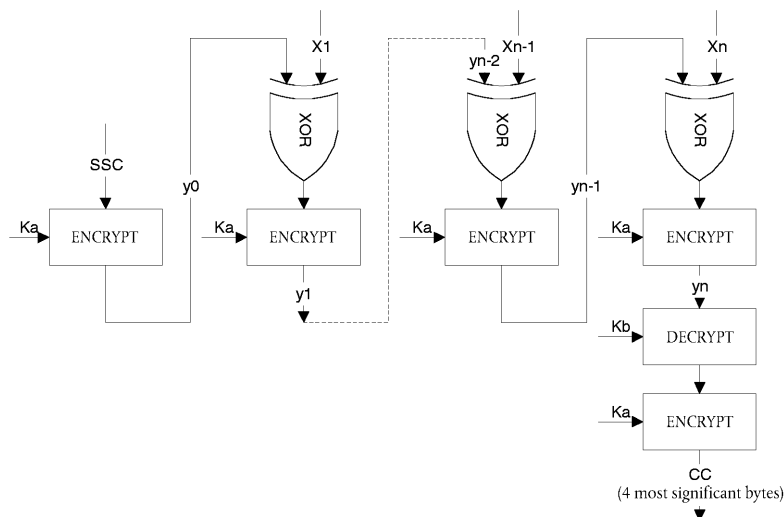
Prenaša se štiri najpomembnejše bajte kriptografske preskusne vsote.

CSM_029 Med postopkom dogovarjanja o ključu se števec zaporedja pošiljanja (SCC) nastavi na: začetni SCC:

Rnd3 (4 bajti z najmanjšo težo) || Rnd1 (4 bajti z najmanjšo težo).

CSM_030 Števec zaporedja pošiljanja se poveča za 1 pred vsakim izračunom MAC (SCC za prvi ukaz je začetni SCC + 1, SCC za prvi odgovor je začetni SCC + 2).

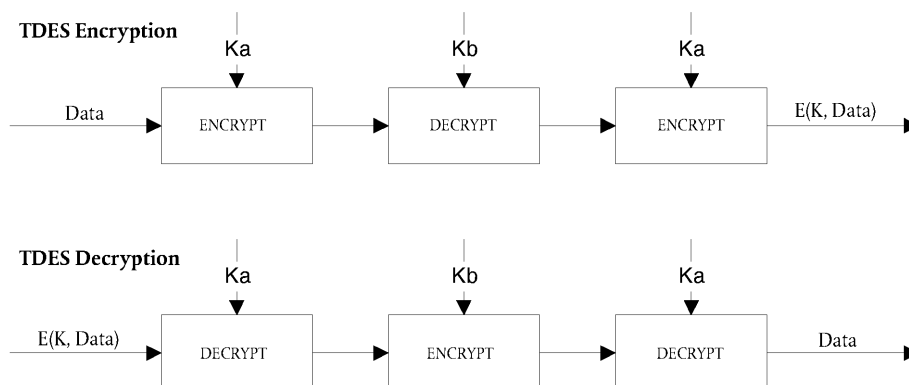
Naslednja slika prikazuje izračun podrobnega MAC:



5.4 Algoritmi izračuna kriptogramov za DO povezane z zaupnostjo

CSM_031 Kriptograme se računa s TDEA v režimu TCBC v skladu z viroma (TDES) in (TDES-OP) in s praznim vektorjem kot blokom začetne vrednosti.

Naslednja slika prikazuje uporabo ključev v TDES:



6. MEHANIZMI DIGITALNEGA PODPISA ZA PRENOS PODATKOV

CSM_032 Inteligentna namenska oprema (IDE) shrani podatke, prejete iz opreme (VU ali kartice) v eni seji prenosa podatkov v eni fizični podatkovni datoteki. Ta datoteka mora vsebovati certifikata $MS_{i,C}$ in EQT.C. Datoteka vsebuje digitalne podpise podatkovnih blokov, kakor je predpisano v dodatku 7, Protokoli prenosa podatkov.

CSM_033 Digitalni podpisi prenesenih podatkov morajo biti izdelani po shemi digitalnega podpisovanja s takim dodatkom, da je mogoče prenesene podatke po želji brati tudi brez kakršnegakoli dešifriranja.

6.1 Tvorba podpisa

CSM_034 Oprema mora tvoriti podpis podatkov po shemi podpisovanja z dodatkom, opredeljenim v viru (PKCS1) s funkcijo razpršitve SHA-1.

$$\text{Podpis} = \text{EQT.SK}[\text{'00' || '01' || PS || '00' || DER(SHA-1(podatki))}]$$

PS oktetni niz za zapolnitev z vrednostjo 'FF' do dolžine 128.

DER(SHA-1(M)) pomeni šifriranje ID algoritma funkcije razpršitve in vrednosti razpršitve v vrednost ASN.1 tipa Digestinfo (znana pravila kodiranja).

'30' || '21' || '30' || '09' || '06' || '05' || '2B' || '0E' || '03' || '02' || '1A' || '05' || '00' || '04' || '14' || rednost razpršitve.

6.2 Preverjanje podpisa

CSM_035 Preverjanje podpisa prenesenih podatkov poteka po shemi podpisovanja z dodatkom, opredeljenim v viru (PKCS1) s funkcijo razpršitve SHA-1.

Osebek, ki opravlja preverjanje, mora neodvisno poznati evropski javni ključ EUR.PK (in mu mora biti ključ zaupan).

Naslednja tabela prikazuje protokol, ki ga lahko uporablja IDE s kontrolno kartico za preverjanje celovitosti podatkov, prenesenih in shranjenih na ESM (zunanji pomnilni medij). Za dešifriranje digitalnih podpisov se uporablja kontrolna kartica. V takem primeru ta funkcija lahko ni vgrajena v IDE.

Oprema, s katere so bili preneseni podatki in je podpisala analizirane podatke, je označena kot EQT.

