

32002R1360

5.8.2002

EUROOPA ÜHENDUSTE TEATAJA

L 207/1

KOMISJONI MÄÄRUS (EÜ) nr 1360/2002,**13. juuni 2002,****millega kohandatakse seitsmendat korda tehnika arenguga nõukogu määrust (EMÜ) nr 3821/85 autovedudel kasutatavate sõidumeerikute kohta****(EMPs kohaldatav tekst)**

EUROOPA ÜHENDUSTE KOMISJON,

võttes arvesse Euroopa Ühenduse asutamislepingut,

võttes arvesse nõukogu 20. detsembri 1985. aasta määrust (EMÜ) nr 3821/85 autovedudel kasutatavate sõidumeerikute kohta ⁽¹⁾, viimati muudetud määrusega (EÜ) nr 2135/98 ⁽²⁾, ning eriti selle artikleid 17 ja 18,

ning arvestades järgmist:

- (1) Määruse (EMÜ) nr 3821/85 I B lisa tehnospetsifikaadid tuleks kohandada tehnika arenguga, pööra-tes erilist tähelepanu süsteemi üldisele turvalisusele ning sõidumeeriku ja juhikaartide koostalitlus-võimele.
- (2) Seoses meeriku kohandamisega on tarvis kohandada ka määruse (EMÜ) nr 3821/85 II lisa, milles määratletakse märgid ja tüübikinnitustunnistused.
- (3) Määruse (EMÜ) nr 3821/85 artikli 18 alusel loodud komitee ei esitanud oma arvamust ettepanekus sisalduvate meetmete kohta ning seetõttu esitas komisjon nõukogule nende meetmetega seoses ette-paneku.
- (4) Määruse (EMÜ) nr 3821/85 artikli 18 lõike 5 punktis b sätestatud aja jooksul ei ole nõukogu tegut-senud ning seega peab komisjon need meetmed vastu võtma,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Määruse (EÜ) nr 2135/98 lisa asendatakse käesoleva määruse lisaga.

Artikkel 2

Määruse (EMÜ) nr 3821/85 II lisa muudetakse järgmiselt.

1. I peatüki punkti 1 esimest lõiku muudetakse järgmiselt:
 - Kreeka kokkuleppeline tähis "GR" asendatakse tähisega "23",
 - Iirimaa kokkuleppeline tähis "IRL" asendatakse tähisega "24",
 - Austria tarvis lisatakse kokkuleppeline tähis "12",
 - Soome tarvis lisatakse kokkuleppeline tähis "17",
 - Rootsi tarvis lisatakse kokkuleppeline tähis "5".
2. I peatüki punkti 1 teist lõiku muudetakse järgmiselt:
 - sõna "salvestusleht" järele lisatakse sõnad "või sõidumeerikukaart".
3. I peatüki punkti 2 muudetakse järgmiselt:
 - sõna "salvestusleht" järele lisatakse sõnad "ja igal sõidumeerikukaardil".
4. II peatüki pealkirjale lisatakse sõnastus "I LISALE VASTAVATE TOODETE".

⁽¹⁾ EÜT L 370, 31.12.1985, lk 8.⁽²⁾ EÜT L 274, 9.10.1998, lk 1.

5. Lisatakse järgmine III peatükk:

"III. I B LISALE VASTAVATE TOODETE TÜÜBIKINNITUSTUNNISTUS

Tüübiakinnituse andnud riik annab taotluse esitajale tüübiakinnitustunnistuse, mille näidis on esitatud allpool. Kui liikmesriik teatab teistele liikmesriikidele väljaantud või vajaduse korral tühistatud tüübiakinnitustest, kasutab ta selle tunnistuse koopiaid.

I B LISALE VASTAVATE TOODETE TÜÜBIKINNITUSTUNNISTUS

Pädeva ametiasutuse nimi

Teatamine puudutab ⁽³⁾:

- tüübiakinnitust
- tüübiakinnituse kehtetuks tunnistamist
- sõidumeeriku mudelit
- sõidumeeriku osa ⁽⁴⁾
- juhikaarti
- töökojakaarti
- ettevõttekaarti
- kontrollikaarti

Tüübiakinnitusnumber

1. Tootja mark või kaubamärk
 2. Mudeli nimetus
 3. Tootja nimi
 4. Tootja aadress
 5. Tüübiakinnituseks esitamise kuupäev
 6. Labor(id)
 7. Katse(te) kuupäev ja number
 8. Tüübiakinnituse kuupäev
 9. Tüübiakinnituse tühistamise kuupäev
 10. Sõidumeeriku osa(de) mudel, milles osa on mõeldud kasutada
 11. Koht
 12. Kuupäev
 13. Lisatud kirjeldavad dokumendid
14. Märkused (sealhulgas plommide asukoht, kui need on olemas)

.....
(allkiri)

⁽³⁾ Märgistada vastavad lahtrid ristiga.

⁽⁴⁾ Määratleda teatises käsitletav osa."

Artikkel 3

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Ühenduste Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 13. juuni 2002

Komisjoni nimel
asepresident
Loyola DE PALACIO

LISA

"I B LISA

EHITUS-, KATSETUS-, PAIGALDUS- JA KONTROLLINÕUDED

SISUKORD

I.	MÕISTED	286
II.	SÕIDUMEERIKU ÜLDOMADUSED JA FUNKTSIOONID	290
1.	Üldomadused	290
2.	Funktsioonid	290
3.	Toimimismoodused	291
4.	Turvalisus	292
III.	SÕIDUMEERIKU KONSTRUKTSIOONI- JA FUNKTSIONAALSED NÕUDED	292
1.	Kaartide sisestamise ja väljavõtmise seire	292
2.	Kiiruse ja vahemaa mõõtmine	292
2.1.	Läbitud teepikkuse mõõtmine	293
2.2.	Kiiruse mõõtmine	293
3.	Aja mõõtmine	293
4.	Juhi tegevuste seire	294
5.	Juhtimisstaatuse seire	294
6.	Juhtide käsitsi tehtavad sissekanded	294
6.1.	Sissekanne tööpäeva algus- ja/või lõpukoha kohta	294
6.2.	Käsitsi tehtavad sissekanded juhi tegevuste kohta	294
6.3.	Eritingimuste sissekanne	296
7.	Ettevõtetelukkude haldamine	296
8.	Kontrollitegevuste seire	296
9.	Sündmuste ja/või rikete seire	296
9.1.	"Kehtetu kaardi sisestamise" sündmus	296
9.2.	"Kaardikonflikti" sündmus	297
9.3.	"Aja kattumise" sündmus	297
9.4.	"Vajaliku kaardita juhtimise" sündmus	297
9.5.	"Kaardi sisestamine juhtimise ajal" sündmus	297
9.6.	"Viimane kaardiseanss nõuetekohaselt sulgemata"-sündmus	297
9.7.	"Kiiruse ületamise" sündmus	297

9.8.	“Toiteallika katkestuse” sündmus	298
9.9.	“Liikumisandmete vea” sündmus	298
9.10.	“Turbemurdekatse” sündmus	298
9.11.	“Kaardi” rike	298
9.12.	“Sõidumeeriku” rike	298
10.	Sisseehitatud ja enesekontrollitised	298
11.	Andmemälust lugemine	298
12.	Andmete registreerimine ja salvestamine andmemällu	299
12.1.	Seadme identimisandmed	299
12.1.1.	Sõidukiüksuse identimisandmed	299
12.1.2.	Liikumisanduri identimisandmed	299
12.2.	Turvaelemendid	300
12.3.	Juhikaardi sisestamise ja väljavõtmise andmed	300
12.4.	Andmed juhi tegevuse kohta	301
12.5.	Tööpäeva algus- ja/või lõpukoht	301
12.6.	Läbisõidumõõdiku andmed	301
12.7.	Üksikasjalikud andmed kiiruse kohta	301
12.8.	Andmed sündmuste kohta	301
12.9.	Andmed rikete kohta	303
12.10.	Kalibreerimisandmed	304
12.11.	Andmed aja korrigeerimise kohta	304
12.12.	Andmed kontrollitegevuse kohta	304
12.13.	Andmed ettevõtetelukkude kohta	305
12.14.	Andmed allalaadimise kohta	305
12.15.	Andmed eritingimuste kohta	305
13.	Sõidumeerikukaartidelt lugemine	305
14.	Registreerimine ja salvestamine sõidumeerikukaartidele	305
15.	Kuvamine	306
15.1.	Vaikekuva	306
15.2.	Hoiatuskuva	307
15.3.	Menüüpääs	307
15.4.	Muud kuvad	307
16.	Trükkimine	307
17.	Hoiatused	308
18.	Andmete allalaadimine välisandmekandjale	309
19.	Andmete väljastamine lisavälisseadmetele	309
20.	Kalibreerimine	310
21.	Aja korrigeerimine	310

22.	Toimeomadused	310
23.	Materjalid	310
24.	Märgised	311
IV.	SÕIDUMEERIKUKAARTIDE KONSTRUKTSIOONI- JA FUNKTSIONAALSED NÕUDED	311
1.	Nähtavad andmed	311
2.	Turvalisus	314
3.	Standardid	314
4.	Keskkonnaalased ja elektrilised nõuded	314
5.	Andmete salvestamine	314
5.1.	Kaardi identimis- ja turbeandmed	315
5.1.1.	Rakenduse identifitseerimine	315
5.1.2.	Kiibi identifitseerimine	315
5.1.3.	Kiipkaardi identifitseerimine	315
5.1.4.	Turvaelemendid	315
5.2.	Juhikaart	315
5.2.1.	Kaardi identifitseerimine	315
5.2.2.	Kaardi omaniku identifitseerimine	316
5.2.3.	Teave juhiloa kohta	316
5.2.4.	Andmed kasutatud sõidukite kohta	316
5.2.5.	Andmed juhi tegevuse kohta	316
5.2.6.	Tööpäeva algus- ja/või lõpukoht	317
5.2.7.	Andmed sündmuste kohta	317
5.2.8.	Andmed rikete kohta	318
5.2.9.	Andmed kontrollitegevuse kohta	318
5.2.10.	Andmed kaardiseansi kohta	318
5.2.11.	Andmed eritingimuste kohta	318
5.3.	Töökojakaart	319
5.3.1.	Turvaelemendid	319
5.3.2.	Kaardi identifitseerimine	319
5.3.3.	Kaardi omaniku identifitseerimine	319
5.3.4.	Andmed kasutatud sõidukite kohta	319
5.3.5.	Andmed juhi tegevuse kohta	319
5.3.6.	Andmed tööpäeva alguse ja/või lõpu kohta	319
5.3.7.	Andmed sündmuste ja rikete kohta	319
5.3.8.	Andmed kontrollitegevuse kohta	319
5.3.9.	Andmed kalibreerimise ja aja korrigeerimise kohta	320
5.3.10.	Andmed eritingimuste kohta	320
5.4.	Kontrollikaart	320

5.4.1.	Kaardi identifitseerimine	320
5.4.2.	Kaardi omaniku identifitseerimine	320
5.4.3.	Andmed kontrollitegevuse kohta	320
5.5.	Ettevõttekaart	321
5.5.1.	Kaardi identifitseerimine	321
5.5.2.	Kaardi omaniku identifitseerimine	321
5.5.3.	Andmed ettevõtte tegevuse kohta	321
V.	SÕIDUMEERIKU PAIGALDAMINE	321
1.	Paigaldamine	321
2.	Paigaldustahvel	322
3.	Plommid	322
VI.	KONTROLL, ÜLEVAATUS JA REMONT	323
1.	Paigaldajate ja töökodade kinnitamine	323
2.	Uute või parandatud seadmete kontroll	323
3.	Paigaldamise kontroll	323
4.	Korrapärane ülevaatus	323
5.	Vigade mõõtmine	324
6.	Remont	324
VII.	KAARDI VÄLJAANDMINE	324
VIII.	SÕIDUMEERIKU JA SÕIDUMEERIKUKAARTIDE TÜÜBIKINNITUS	324
1.	Üldpunktid	324
2.	Turbesertifikaat	325
3.	Funktsionaalne sertifikaat	325
4.	Koostalitlusvõime sertifikaat	325
5.	Tüüvikinnitustunnistus	326
6.	Erandkord: esimese koostalitlusvõime katsed	326
1. liide	Andmesõnastik	
2. liide	Sõidumeerikukaartide spetsifikaat	
3. liide	Piktogramm	
4. liide	Väljatrükid	
5. liide	Kuvamine	
6. liide	Välisliidesed	
7. liide	Andmete allalaadimisprotokoll	
8. liide	Kalibreerimisprotokoll	
9. liide	TÜÜBIKINNITUS — MINIMAALSELT NÕUTAVATE KATSETE NIMEKIRI	
10. liide	ÜLDISED TURBE-EESMÄRGID	
11. liide	KÖZÖS BIZTONSÍGI MECHANIZMUSOK	

I. MÕISTED

Käesolevas lisas kasutatakse järgmisi mõisteid:

a) **“aktiveerimine”:**

etapp, mil sõidumeerik hakkab täielikult tööle ja täidab kõiki funktsioone, sealhulgas turbefunktsioone;

sõidumeeriku aktiveerimiseks on vaja kasutada töökojakaarti ja sisestada selle PIN-kood;

b) **“autentimine”:**

funktsioon, mille eesmärk on väidetud isikusamasus kindlaks teha ja tõestada;

c) **“autentsus”:**

omadus, mille puhul teave pärineb allikast, mille isikusamasust saab tõestada;

d) **“sisseehitatud katse”:**

vajaduse korral tehtav katse, mille käivitab operaator või välisseade;

e) **“kalendripäev”:**

päev vahemikus kell 00.00 kuni 24.00. Kõik kalendripäevad on seotud GMTga (universaalaeg);

f) **“kalibreerimine”:**

andmemälus sisalduvate sõiduki parameetrite ajakohastamine või kinnitamine. Sõiduki parameetrid on sõidukit tõendavad andmed (valmistajatehase tähis, sõiduki registreerimisnumber ja registreerinud liikmesriik) ning sõiduki karakteristikud (sõidukit iseloomustav koefitsient, sõidumeeriku konstant, rattarehvide efektiivüumbermoot, rehvi suurus, kiiruspiiriku seadistus (kui see on olemas), tegelik GMT aeg, läbisõidumõõdiku tegelik väärtus);

sõidumeeriku kalibreerimiseks on vaja kasutada töökojakaarti;

g) **“kaardi number”:**

16kohaline tähtnumbriline number, mis idendib üheselt sõidumeerikukaardi liikmesriigis. Kaardi number sisaldab järjestikust indeksit (kui see on olemas), asendus- ja uuendusindeksit;

seega saab kaarti üheselt identida väljaandnud liikmesriigi koodi ja kaardi numbril abil;

h) **“kaardi järjestikune indeks”:**

kaardi numbril 14. tähtnumbriline märk, mida kasutatakse sellele ettevõttele või asutusele, kellele võib välja anda mitu sõidumeerikukaarti, väljaantud erinevate kaartide eristamiseks. Kaardi numbril esimese 13 märgi abil saab ettevõtte või asutuse üheselt identida;

i) **“kaardi uuendusindeks”:**

kaardi numbril 16. tähtnumbriline märk, mis sõidumeerikukaardi igal uuendamisel suureneb;

j) **“kaardi asendusindeks”:**

kaardi numbril 15. tähtnumbriline märk, mis sõidumeerikukaardi igal asendamisel suureneb;

k) **“sõidukit iseloomustav koefitsient”:**

numbriline parameeter, mis kirjeldab sõidukit sõidumeerikuga ühendava osa (käigukasti väljundvõll või -telg) tekitatud väljundsignaali, kui sõiduk läbib standardsetes katsetingimustes ühe kilomeetri pikkuse vahemaa (vt VI peatüki punkt 5). Iseloomustavat koefitsienti väljendatakse impulssides kilomeetri kohta ($w = \dots \text{imp/km}$);

l) **“ettevõttelekaart”:**

liikmesriigi asutuse poolt sõidumeerikuga varustatud sõiduki omanikule või valdajale väljaantud sõidumeerikukaart;

ettevõttelekaardiga määratakse kindlaks ettevõtte ning selle abil saab ettevõtte lukustatud sõidumeerikusse salvestatud andmeid kuvada, alla laadida ja välja trükkida;

m) **“sõidumeeriku konstant”:**

numbriline parameeter, mis vastab ühe kilomeetri jooksul läbitud vahemaa näitamiseks ja registreerimiseks vajaliku sisendsignaali väärtusele; konstanti väljendatakse impulssides kilomeetri kohta ($k = \dots \text{imp/km}$);

n) **“sõidumeerikus arvatud pidev sõiduaeg”⁽¹⁾:**

pidev sõiduaeg arvutatakse konkreetse juhi jooksva kumulatiivse sõiduajana alates viimasest 45minutilise või pikemast VALMISOLEKU või VAHEAJA/PUHKUSE või TEADMATA⁽²⁾ ajast (see aeg võib olla jagatud mitmeks 15minutiliseks või pikemaks ajaks). Arvutuste puhul võetakse vajaduse korral arvesse juhikaardile salvestatud eelnevaid tegevusi. Kui juht ei ole oma kaarti sisestanud, tehakse arvutused mälus olevate andmete põhjal, mis on seotud jooksva ajaga, mil kaart ei olnud sisestatud ega asjaomasesse avasse pistetud;

o) **“kontrollikaart”:**

liikmesriigi asutuste poolt siseriiklikule pädevale kontrolliasutusele väljaantud sõidumeerikukaart;

kontrollikaardiga määratakse kindlaks kontrolliasutus ja võimaluse korral kontrolliametnik ning sellega saab andmemällu või juhikaardile salvestatud andmeid lugeda, trükkida ja/või alla laadida;

p) **“sõidumeerikus arvatud kumuleeritud vaheaeg”⁽¹⁾:**

juhtimise kumuleeritud vaheaeg arvutatakse konkreetse juhi jooksva kumuleeritud 15minutit või kauem kestvatest VALMISOLEKU või VAHEAJA/PUHKUSE või TEADMATA⁽²⁾ aegadest alates viimasest 45minutilise või pikemast VALMISOLEKU või VAHEAJA/PUHKUSE või TEADMATA⁽²⁾ ajast (see aeg võib olla jagatud mitmeks 15minutiliseks või pikemaks ajaks).

Arvutuste puhul võetakse vajaduse korral arvesse juhikaardile salvestatud eelnevaid tegevusi. Negatiivse pikkusega teadmata aegu (teadmata aja algus > teadmata aja lõpp), mis on seotud kahe erineva sõidumeeriku kattuvate aegade, ei võeta arvutamisel arvesse.

Kui juht ei ole oma kaarti sisestanud, tehakse arvutused mälus olevate andmete põhjal, mis on seotud jooksva ajaga, mil kaart ei olnud sisestatud ega asjaomasesse avasse pistetud;

q) **“andmemälu”:**

sõidumeerikusse ehitatud elektrooniline mäluseade;

r) **“digitaalallkiri”:**

andmekogule lisatud andmed või nende krüptograafiline muundamine, mis võimaldab andmekogu saajal tõendada andmekogu autentsust ja terviklikkust;

s) **“allalaadimine”:**

sõiduki mäluseadmesse või sõidumeeriku mälukaardile salvestatud andmete osaline või täielik kopeerimine koos digitaalallkirjaga;

allalaadimine ei tohi salvestatud andmeid muuta ega kustutada;

⁽¹⁾ Juhil pideva sõiduaega ja kumulatiivse vaheaja sellise arvutamise eesmärk on, et sõidumeerik saaks arvutada kumulatiivse juhtimisaja hoiatuse. See ei piira nende aegade juriidilist tõlgendamist.

⁽²⁾ TEADMATA ajad vastavad aegadele, mil juhikaart ei olnud sõidumeerikusse sisestatud ja mille kohta puuduvad käsitsi tehtud sisestatud juhi tegevuse kohta.

- t) **“juhikaart”**:
liikmesriigi asutuste poolt konkreetsele juhile väljaantud sõidumeerikukaart;
juhikaart idendib juhi ning sellega on võimalik salvestada juhi tegevustega seotud andmeid;
- u) **“rattarehvide efektiivüumbermõõt”**:
iga sõidukit vedava ratta (veoratta) keskmine läbitud teepikkus täieliku pöörlemise korral. Teepikkusi tuleb mõõta standardsetes katsetingimustes (VI peatüki punkt 5) ning seda väljendatakse “l = ... mm”. Sõidukitootjad võivad asendada teepikkuste mõõtmise teoreetiliste arvutustega, mille puhul võetakse arvesse normaalses sõidukorras koormata sõiduki massi jaotumist telgede vahel ⁽¹⁾. Teoreetiliste arvutuste meetodid kinnitab liikmesriigi pädev asutus;
- v) **“sündmus”**:
sõidumeeriku tuvastatud väärtoiming, mille põhjuseks võib olla pettuskatse;
- w) **“riike”**:
sõidumeeriku tuvastatud väärtoiming, mille põhjuseks võib olla seadme riike või tõrge;
- x) **“paigaldamine”**:
sõidumeeriku paigaldamine sõidukisse;
- y) **“liikumisandur”**:
sõidumeeriku osa, mis annab sõiduki kiirust ja/või läbitud teepikkust kujutava signaali;
- z) **“kehtetu kaart”**:
kaart, millel on avastatud rikked või mille esialgne autentimine oli vale või mille kehtivusaeg ei ole veel alanud või on juba lõppenud;
- aa) **“sõidumeerik mittevajalik”**:
sõidumeeriku kasutamist ei nõuta vastavalt nõukogu määruse (EMÜ) nr 3820/85 sätetele;
- bb) **“kiiruse ületamine”**:
sõiduki suurima lubatud kiiruse ületamine, mis on määratletud kui mis tahes 60 sekundit ületav aeg, mille jooksul sõiduki mõõdetud kiirus ületab nõukogu 10. veebruari 1992. aasta direktiivis 92/6/EMÜ (teatava kategooria mootorsõidukitele kiiruspiirikute paigaldamise ja nende kasutamise kohta ühenduses) ⁽²⁾ sätestatud kiiruspiiriku ülemmäära;
- cc) **“korrapärane ülevaatus”**:
toimingute kogum, mille eesmärk on kontrollida, kas sõidumeerik töötab nõuetekohaselt ning kas selle seaded vastavad sõiduki parameetritele;
- dd) **“printer”**:
sõidumeeriku osa, mis trüüb välja salvestatud andmed;
- ee) **“sõidumeerik”**:
maanteesõidukitele paigaldamiseks mõeldud täielik seade, mis näitab, registreerib ja salvestab automaatselt või poolautomaatselt nende sõidukite liikumise ja juhtide teatavad tööajad;

⁽¹⁾ 22. juuli 1997. aasta direktiiv 97/27/EÜ, mis käsitleb teatavate mootorsõidukikategooriate ja nende haagiste massi ja mõõtmeid ning millega muudetakse direktiivi 70/156/EMÜ (EÜT L 233, 25.8.1997, lk 1).

⁽²⁾ EÜT L 57, 2.3.1992, lk 27.

ff) **“uuendamine”**:

uue sõidumeerikukaardi väljaandmine, kui olemasoleva kaardi kehtivusaeg hakkab lõppema või kui kaart ei ole töökorras ja on tagastatud kaarte väljaandvale asutusele. Uuendamise puhul tuleb alati olla kindel, et üheaegselt ei ole kahte kehtivat kaarti;

gg) **“remont”**:

liikumisanduri või sõiduki osa mis tahes remont, mille käigus tuleb see toiteallikast või muudest sõidumeeriku osadest lahti ühendada või avada;

hh) **“asendamine”**:

uue sõidumeerikukaardi väljaandmine, asendamaks olemasolevat kaarti, mille kohta on teatatud, et see on kadunud, varastatud või ei ole töökorras ning mida ei ole kaarte väljaandvale asutusele tagastatud. Asendamisega kaasneb alati risk, et üheaegselt eksisteerib kaks kehtivat kaarti;

ii) **“turvalisuse sertifitseerimine”**:

protsess, mille käigus ITSECI⁽¹⁾ sertifitseerimisasutus tõendab, et uurimiselune sõidumeerik (või osa) või sõidumeerikukaart vastab 10. liite “Üldised turbe-eesmärgid” turvanõuetele;

jj) **“enesekontrollitest”**:

sõidumeeriku tehtavad regulaarsed ja automaatsed katsed rikete avastamiseks;

kk) **“sõidumeerikukaart”**:

sõidumeerikus kasutamiseks mõeldud kiipkaart. Sõidumeerikukaardid võimaldavad sõidumeerikul identifitseerida kaardi omaniku isikusamasuse (või isikusamasuse rühma) ning edastada ja salvestada andmeid. Sõidumeerikukaart võib olla järgmist tüüpi:

- juhikaart,
- kontrollikaart,
- töökojakaart,
- ettevõttele;

ll) **“tüübikinnitus”**:

protsess, mille käigus liikmesriik tõendab, et uurimiselune sõidumeerik (või osa) või sõidumeeriku kaart vastab käesoleva määruse nõuetele;

mm) **“rehvi suurus”**:

rehvide (väliste veorataste) mõõtmete määramine vastavalt 31. märtsi 1992. aasta direktiivile 92/23/EMÜ⁽²⁾;

nn) **“sõiduki identimine”**:

sõidukit identifitseerivad numbrid: sõiduki registreerimisnumber (VRN) koos viitega registreerinud liikmesriigile ja valmistajatehase tähis (VIN)⁽³⁾;

oo) **“sõidukiüksus”**:

sõidumeerik, välja arvatud liikumisandur ja liikumisandurit ühendavad juhtmed. Sõidukiüksus võib koosneda ühest või mitmest sõiduki erinevates kohtades asuvast üksusest, kui see vastab käesoleva määruse turvanõuetele;

⁽¹⁾ Komisjoni 7. aprilli 1995. aasta soovitus 95/144/EÜ infotehnoloogia turvalisuse hindamise ühiste kriteeriumide kohta (EÜT L 93, 26.4.1995, lk 27).

⁽²⁾ EÜT L 129, 14.5.1992, lk 95.

⁽³⁾ 18. detsembri 1975. aasta direktiiv 76/114/EMÜ mootorsõidukite ja nende haagiste andmesilte ning kirjeid, nende asukohta ja kinnitust viisi käsitlevate liikmesriikide õigusaktide ühtlustamise kohta (EÜT L 24, 30.1.1976, lk 1).

pp) "sõidumeeriku nädal andmetöötluse seisukohast":

ajavahemik alates kella 00.00 universaalaja järgi esmaspäeval ja lõpetades kell 24.00 universaalaja järgi pühapäeval;

qq) "töökojakaart":

liikmesriigi ametiasutuse poolt selle liikmesriigi kinnitatud sõidumeeriku tootjale, paigaldajale, sõidukitootjale või töökojale väljaantud sõidumeerikukaart.

Töökojakaardi abil identitakse kaardi omanik ning sellega saab sõidumeerikut testida, kalibreerida ja/või sõidumeeriku andmeid alla laadida.

II. SÕIDUMEERIKU ÜLDOMADUSED JA FUNKTSIOONID

000 Käesoleva lisa sätetele vastava sõidumeerikuga varustatud sõidukil peavad olema kiirusekuvar ja läbisõidumõõdik. Need funktsioonid võivad olla integreeritud sõidumeerikusse.

1. Üldomadused

Sõidumeeriku eesmärk on juhi tegevustega seotud andmete registreerimine, salvestamine, kuvamine, trükkimine ja väljastamine.

001 Sõidumeerik koosneb juhtmetest, liikumisandurist ja sõidukiüksusest.

002 Sõidukiüksus koosneb keskseadmest, andmemälust, reaalaega näitavast kellast, kahest kiipkaardiliidesest (juht ja kaasjuht), printerist, kuvarist, visuaalsest hoiatussüsteemist, kalibreerimise/allalaadimise pistikust ning kasutajasisenditest.

Sõidumeerik võib olla lisapistikute abil ühendatud muude seadmete külge.

003 Sõidumeerikule muu funktsiooni, seadme või seadmete lisamine või külge ühendamine, olenemata sellest, kas neil on tüübikinnitus või mitte, ei tohi segada ega olla võimeline segama sõidumeeriku nõuetekohast ja turvalist tööd ega olla vastuolus käesoleva määruse sätetega.

Sõidumeeriku kasutajad idendivad oma isiku seadme jaoks sõidumeerikukaardi abil.

004 Sõidumeerik annab vastavalt kasutaja tüübile ja/või isikusamasusele valikulised pääsuõigused andmetele ja funktsioonidele.

Sõidumeerik registreerib ja salvestab andmed andmemällu ja sõidumeerikukaartidele.

Seda tehakse vastavalt 24. oktoobri 1995. aasta direktiivile 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta ⁽¹⁾.

2. Funktsioonid

005 Sõidumeerikuga tagatakse järgmised funktsioonid:

- kaartide sisestamise ja väljavõtmise seire,
- kiiruse ja teepikkuse mõõtmine,
- aja mõõtmine,
- juhi tegevuste seire,
- juhtimisstaatuse seire,
- juhtide käsitsi tehtud sissekanded:
 - sissekanne tööpäeva algus- ja/või lõpukoha kohta,
 - käsitsi tehtud sissekanne juhi tegevuste kohta,
 - eritingimuste sissekanne,

⁽¹⁾ EÜT L 281, 23.11.1995, lk 31.

- ettevõtetelukkude haldamine,
- kontrollitegevuste seire,
- sündmuste ja/või rikete tuvastamine,
- sisseehitatud ja enesekontrollitised,
- andmemälust lugemine,
- andmete registreerimine ja säilitamine mälus,
- sõidumeerikukaartidelt lugemine,
- registreerimine ja säilitamine sõidumeerikukaartidele,
- kuvamine,
- trükkimine,
- hoiatamine,
- andmete allalaadimine välisandmekandjatele,
- andmete väljastamine välistele lisaseadmetele,
- kalibreerimine,
- aja korrigeerimine.

3. Toimimismoodused

006 Sõidumeerikul on neli toimimismoodust:

- tavamoodus,
- kontrollimoodus,
- kalibreerimismoodus,
- ettevõtetemoodus.

007 Vastavalt kaardiliidesesse sisestatud kehtivale sõidumeerikukaardile peab sõidumeerik lülituma järgmisse toimimismoodusse:

Toimimismoodus		Juhikaardi ava				
		Kaart puudub	Juhikaart	Kontrollikaart	Töökojakaart	Ettevõttekaart
Kaasjuhi kaardi ava	Kaart puudub	Tavaline	Tavaline	Kontroll	Kalibreerimine	Ettevõte
	Juhikaart	Tavaline	Tavaline	Kontroll	Kalibreerimine	Ettevõte
	Kontrollikaart	Kontroll	Kontroll	Kontroll (*)	Tavaline	Tavaline
	Töökojakaart	Kalibreerimine	Kalibreerimine	Tavaline	Kalibreerimine (*)	Tavaline
	Ettevõttekaart	Ettevõte	Ettevõte	Tavaline	Tavaline	Ettevõte (*)

008 (*) Sellisel juhul kasutab sõidumeerik vaid juhikaardi avasse sisestatud sõidumeerikukaarti.

- 009 Sõidumeerik eirab sisestatud kehtetuid kaarte, ent kehtivusaja ületanud kaartidel olevate andmete kuvamine, trükkimine või allalaadimine on võimalik.
- 010 Kõik punktis II.2 loetletud funktsioonid toimivad igas toimimismooduses, välja arvatud järgmised erandid:
- kalibreerimisfunktsioon on võimalik ainult kalibreerimismooduses,
 - aja korrigeerimise funktsioon on piiratud, kui ei olda kalibreerimismooduses,
 - juhi käsitsi tehtavate sissekannete funktsioon on võimalik ainult tava- või kalibreerimismooduses,
 - ettevõtetelukkude haldamisfunktsioon on võimalik ainult ettevõtetemooduses,
 - kontrollitegevuste seire funktsioon toimib ainult kontrollimooduses,
 - allalaadimisfunktsioon ei ole võimalik tavamooduses (välja arvatud nõudes 150 sätestatud juhtudel).
- 011 Sõidumeerik võib väljastada kuvarile, printerisse või välisliidestesse mis tahes andmeid, välja arvatud järgmised erandid:
- tavamooduses sisestatud sõidumeerikukaardile mittevastav isikusamasus (perekonnanimi ja eesnimi või eesnimed) jäetakse esitamata ja sisestatud sõidumeerikukaardile mittevastava kaardi number jäetakse osaliselt esitamata (esitamata jäetakse iga teine tähemärk vasakult paremale),
 - ettevõtetemooduses saab juhiga seotud andmeid (nõuded 081, 084 ja 087) esitada ainult aegade kohta, mida ei ole lukustanud teine ettevõtte (see on idenditud ettevõttekaardi numbriga esimese 13 kohaga),
 - kui sõidumeerikus kaarti ei ole, saab juhiga seotud andmeid esitada ainult jooksva ning eelmise kaheksa kalendripäeva kohta.

4. Turvalisus

Süsteemi turbe-eesmärk on kaitsta andmemälu, vältimaks lubamatut juurdepääsu andmetele ja nendega manipuleerimist ning avastamiseks igasugused katsed seda teha, kaitsta liikumisanduri ja sõidukiüksuse vahel vahetatud andmete terviklikkust ja autentsust, kaitsta sõidumeeriku ja sõidumeerikukaartide vahel vahetatud andmete terviklikkust ja autentsust ning tõendada allalaaditud andmete terviklikkust ja autentsust.

- 012 Süsteemi turvalisuse saavutamiseks peab sõidumeerik vastama turvanõuetele, mis on määratletud liikumisanduri ja sõidukiüksuse üldistes turbe-eesmärkides (10. liide).

III. SÕIDUMEERIKU KONSTRUKTSIOONI- JA FUNKTSIONAALSED NÕUDED

1. Kaartide sisestamise ja väljavõtmise seire

- 013 Sõidumeerik seirab kaardiliideseid, et avastada kaartide sisestamist ja väljavõtmist.
- 014 Kaardi sisestamisel kontrollib sõidumeerik, kas sisestatud kaart on kehtiv sõidumeerikukaart ning kui on, idendib kaardi tüübi.
- 015 Sõidumeerik konstrueeritakse nii, et kui sõidumeerikukaart sisestatakse nõuetekohaselt kaardiliidestesse, lukustatakse see kindlasse asendisse.
- 016 Sõidumeerikukaardi saab välja võtta ainult siis, kui sõiduk on peatunud ja asjaomased andmed on kaardile salvestatud. Kaardi väljavõtmiseks on vaja kasutajapoolset konkreetset tegevust.

2. Kiiruse ja teepikkuse mõõtmine

- 017 Funktsioon mõõdab pidevalt teepikkust ning peab suutma esitada läbisõidumõõdiku näidu, mis vastab sõiduki läbitud kogu teepikkusele.
- 018 See funktsioon mõõdab pidevalt kiirust ning peab suutma esitada sõiduki kiiruse.

019 Kiiruse mõõtmise funktsioon annab teavet ka selle kohta, kas sõiduk liigub või seisab. Sõiduk loetakse liikuvaks kohe, kui funktsioon tuvastab liikumisandurilt rohkem kui ühe impulsi sekundis vähemalt viie sekundi jooksul, muudel juhtudel loetakse sõiduk seisvaks.

Käesoleva määru sätetele vastava sõidumeerikuga varustatud sõidukitesse paigaldatud kiiruse (kiirusmõõdik) ja kogu läbitud teepikkuse (läbisõidumõõdik) kuvamisseadmed peavad vastama käesolevas lisas (III peatüki punktis 2.1 ja 2.2) sätestatud suurima lubatud hälbe nõuetele.

2.1. *Läbitud teepikkuse mõõtmine*

020 Läbitud teepikkust võib mõõta kas:

- nii edaspidi kui tagurpidi sõitmise summana või
- ainult edaspidi sõitmisena.

021 Sõidumeerik mõõdab teepikkust vahemikus 0 kuni 9 999 999,9 km.

022 Teepikkust mõõdetakse järgmise hälbe piires (teepikkus vähemalt 1 000 m):

- $\pm 1\%$ enne paigaldamist,
- $\pm 2\%$ paigaldamisel ja korrapärase ülevaatuse ajal,
- $\pm 4\%$ kasutamisel.

023 Mõõdetud teepikkuse eristusvõime on vähemalt 0,1 km.

2.2. *Kiiruse mõõtmine*

024 Sõidumeerik mõõdab kiirust vahemikus 0 kuni 220 km/h.

025 Tagamaks tavakasutamisel osutatud suurima lubatud hälbe ± 6 km/h ning võttes arvesse

- sisendi erinevustest (rehvi erinevused, ...) tingitud hälvet ± 2 km/h,
- paigaldamisel või korrapärastel ülevaatusel tehtud mõõtmiste hälvet ± 1 km/h,

mõõdab sõidumeerik (püsival kiirusel) kiirust hälbega ± 1 km/h kiiruse juures 20 kuni 180 km/h ja sõidukit iseloomustava koefitsiendi juures 4 000 kuni 25 000 imp/km.

Märkus: andmesalvestuse eristusvõime annab sõidumeeriku salvestatud kiirusele lisahälbe $\pm 0,5$ km/h.

025a Kiirust mõõdetakse korrektselt tavahälbe raames kahe sekundi jooksul alates kiiruse muudatuse lõpust, kui kiirus on muutunud kuni 2 m/s^2 .

026 Kiiruse mõõtmise eristusvõime on vähemalt 1 km/h.

3. *Aja mõõtmine*

027 Aja mõõtmise funktsioon mõõdab aega pidevalt ning esitab kuupäeva ja kellaaja digitaalselt universaalajas.

028 Kuupäeva ja kellaaja universaalajas kasutatakse kõikjal sõidumeerikus dateerimiseks (salvestused, väljatrükid, andmevahetus, kuvamine, ...).

029 Kohaliku aja näitamiseks peab saama kuvatava aja nihet muuta poole tunni kaupa.

030 Tüübikinnitustingimustes on ajanihe ± 2 sekundit päevas.

031 Mõõdetud aja eristusvõime peab olema vähemalt 1 sekund.

032 Tüübikinnitustingimustes ei tohi aja mõõtmist mõjutada alla 12 kuu pikkune välise vooluallika katkestus.

4. Juhhi tegevuse seire

- 033 Funktsioon seirab pidevalt ja eraldi ühe juhi ja ühe kaasjuhi tegevust.
- 034 Juhhi tegevus on JUHTIMINE, TÖÖ, VALMISOLEK ja VAHEAEG/PUHKUS.
- 035 Juht ja/või kaasjuht peavad saama käsitsi valida TÖÖ, VALMISOLEKU ja VAHEAJA/PUHKUSE.
- 036 Kui sõiduk liigub, valitakse juhi tarvis automaatselt JUHTIMINE ja kaasjuhi tarvis valitakse automaatselt VALMISOLEK.
- 037 Kui sõiduk peatub, valitakse juhi tarvis automaatselt TÖÖ.
- 038 Kui sõiduk peatus ja toimus automaatne üleminek TÖÖLE, loetakse sellele järgneva 120 sekundi jooksul toimuvat tegevuse esimest muudatust sõiduki seiskumise ajal toimunuks (sellega võib kaasneda TÖÖLE ülemineku tühistamine).
- 039 See funktsioon väljastab salvestusfunktsioonidele tegevuse muudatusi ühe minuti täpsusega.
- 040 Kui mis tahes JUHTIMISE tegevus on toimunud kalendriminuti jooksul, läheb terve minut JUHTIMISE alla.
- 041 Kui mis tahes JUHTIMISE tegevus on toimunud nii kalendriminutile vahetult eelneva kui järgneva minuti jooksul, läheb terve minut JUHTIMISE alla.
- 042 Kui kalendriminutit ei saa eelnevate nõuete alusel lugeda JUHTIMISE minutiks, läheb kogu minut selles minutis toimunud pikima kestva tegevuse alla (võrdse pikkusega tegevuste puhul arvestatakse viimast tegevust).
- 043 Funktsioon jälgib püsivalt ka pidevat juhtimisaega ja juhi kumulatiivset vaheaega.

5. Juhtimisstaatus seire

- 044 Funktsioon seirab püsivalt ja automaatselt juhtimisstaatus.
- 045 Kui meerikusse sisestatakse kaks kehtivat juhikaarti, valitakse automaatselt juhtimisstaatus MEESKOND, igal muul juhul valitakse juhtimisstaatus ÜKSI.

6. Juhtide käsitsi tehtavad sissekanded

6.1. Sissekanne tööpäeva algus- ja/või lõpukoha kohta

- 046 Funktsioon võimaldab sisestada juhi ja/või kaasjuhi tööpäeva algus- ja/või lõpukohad.
- 047 Kohad on määratletud riikidena ja vajaduse korral ka piirkondadena.
- 048 Juhikaardi (või töökojakaardi) väljavõtmisel soovitab sõidumeerik (kaas)juhil sisestada "tööpäeva lõpukoht".
- 049 Sõidumeerik võimaldab selle soovitusel tähelepanuta jätta.
- 050 Tööpäeva algus- ja/või lõpukohti peab saama sisestada ilma kaardita ja muul ajal kui kaarti sisestades või välja võttes.

6.2. Käsitsi tehtavad sissekanded juhi tegevuste kohta

- 050a Juhikaardi (või töökojakaardi) sisestamisel ja ainult sel ajal sõidumeerik:
- meenutab kaardi omanikule, mis kuupäeval ja ajal ta viimati oma kaardi välja võttis, ja
 - palub kaardi omanikul identifitseerida, kas antud kaardi sisestamine tähendab jooksva tööpäeva jätkumist.

Sõidumeerik võimaldab kaardi omanikul küsimus tähelepanuta jätta, vastata sellele positiivselt või negatiivselt:

- juhul kui kaardi omanik jätab küsimuse tähelepanuta, soovib sõidumeerik kaardi omanikul sisestada “tööpäeva alguskoht”. Sõidumeerik võimaldab selle soovitus tähelepanuta jätta. Kui koht sisestatakse, salvestatakse see andmemälus ja sõidumeerikukaardil ning seotakse kaardi sisestusajaga,
- negatiivse või positiivse vastuse korral soovib sõidumeerik kaardi omanikul sisestada käsitsi tegevused, koos alguse ja lõpu kuupäeva ja ajaga, valides tegevused üksnes TÖÖ, VALMISOLEKU või VAHEAJA/PUHKUSE seast ning üksnes sellest ajavahemikust, mis jääb kaardi viimase väljavõtmise ja praeguse sisestamise vahele, ning need tegevused ei tohi omavahel kattuda. Seda tehakse vastavalt järgmisele korrale:
- kui kaardi omanik vastab positiivselt, soovib sõidumeerik kaardi omanikul sisestada käsitsi kronoloogilises järjestuses toimunud tegevused, mis on tehtud ajavahemikul, mis jääb kaardi viimase väljavõtmise ja praeguse sisestamise vahele. Protsess lõpeb, kui käsitsi sisestatud tegevuse lõpu-aeg võrdub kaardi sisestusajaga.
- kui kaardi omanik vastab küsimusele eitavalt:
 - soovib sõidumeerik kaardi omanikul sisestada käsitsi kronoloogilises järjestuses toimunud tegevused, mis on tehtud ajavahemikul, mis jääb kaardi väljavõtmise ja seotud tööpäeva (või sõidukiga seotud tegevuste, kui tööpäev jätkub salvestuslehel) lõpu vahele. Seetõttu soovib sõidumeerik enne seda, kui võimaldab kaardi omanikul iga tegevust käsitsi sisestada, täpsustada, kas viimase salvestatud tegevuse lõpu-aeg on ühtlasi ka eelmise töötaja lõpu-aeg (vt allpool olev märkus),

Märkused: juhul kui kaardi omanik ei määra eelmise töötaja lõppu ja sisestab käsitsi tegevuse, mille lõpu-aeg võrdub kaardi sisestusajaga, sõidumeerik:

- eeldab, et tööpäev lõppes pärast kaardi väljavõtmist esimese PUHKUSE (või ülejäänud TEADMATA) algusajal, kui ühtegi puhke-aega ei ole sisestatud (ja kui ükski aeg ei ole TEADMATA),
- eeldab, et algusaeg (vt allpool) võrdub kaardi sisestusajaga,
- jätkab, nagu on kirjeldatud allpool;
- seejärel, kui seotud töötaja lõpu-aeg erineb kaardi väljavõtmisajast või kui sel ajal ei ole sisestatud ühtki tööpäeva lõpukohta, soovib kaardi omanikul “kinnitada või sisestada tööpäeva lõpukoht” (sõidumeerik võimaldab selle küsimuse tähelepanuta jätta). Kui koht sisestatakse, salvestatakse see ainult sõidumeerikukaardil ja ainult siis, kui see erineb kaardi väljavõtmisel sisestatud kohast (kui see sisestati), ning seotakse töötaja lõpuajaga,
- soovib seejärel kaardi omanikul sisestada jooksva tööpäeva (või praeguse sõidukiga seotud tegevuste, kui kaardi omanik kasutas varem selle aja jooksul salvestuslehte) “algusaeg”, ning soovib kaardi omanikul sisestada “tööpäeva alguskoht” (sõidumeerik võimaldab selle küsimuse tähelepanuta jätta). Kui koht sisestatakse, salvestatakse see sõidumeerikukaardil ning seotakse selle algusajaga. Kui algusaeg võrdub kaardi sisestusajaga, salvestatakse koht ka andmemällu,
- seejärel, kui see algusaeg erineb kaardi sisestusajast, soovitakse kaardi omanikul sisestada käsitsi kronoloogilises järjestuses tegevused sellest algusajast kuni kaardi sisestusajani. Protsess lõpeb, kui käsitsi sisestatud tegevuse lõpu-aeg võrdub kaardi sisestusajaga,
- seejärel võimaldab sõidumeerik kaardi omanikul muuta iga käsitsi sisestatud tegevust kuni erikäsu abil valitu kinnitamiseni, seejärel on igasugune muutmine keelatud,
- kui esialgsele küsimusele ei järgne tegevuste sisestamist, tõlgendab sõidumeerik seda kui küsimuse tähelepanuta jätmist kaardi omaniku poolt.

Kogu protsessi jooksul ei oota sõidumeerik sisestusi kauem:

- kui seadme ja kasutaja viimasest interaktsioonist on möödunud üks minut (nähtav ja võimaluse korral kuuldav hoiatus 30 sekundi pärast) või
- kui kaart võetakse välja ja sisestatakse teine juhikaart (või töökojakaart) või
- kui sõiduk hakkab liikuma,

sel juhul kinnitab sõidumeerik juba tehtud sissekanded.

6.3. Eritingimuste sisestamine

050b Sõidumeerik võimaldab juhil sisestada reaajas kaks järgmist eritingimust:

- “SÕIDUMEERIK MITTEVAJALIK” (algus, lõpp)
- “PRAAMI-/RONGISÕIT”

Kui tingimus “SÕIDUMEERIK MITTEVAJALIK” on avatud, ei saa esineda tingimust “PRAAMI-/RONGISÕIT”.

Sõidumeerik peab avatud tingimuse “SÕIDUMEERIK MITTEVAJALIK” automaatselt sulgema, kui juhikaart sisestatakse või võetakse välja.

7. Ettevõtetelukkude haldamine

- 051 Funktsioon võimaldab ettevõtte paigaldatud lukke hallata, et piirata ettevõttemooduses pääsu andmetele ainult sellele ettevõttele.
- 052 Ettevõtetelukk koosneb alguse kuupäevast/ajast (lukustamine) ja lõpu kuupäevast/ajast (luku avamine), mis on seotud ettevõtte identimisega ettevõttekaardi numbri alusel (lukustamisel).
- 053 Lukustada ja lukku avada saab ainult reaajas.
- 054 Lukku saab avada ainult see ettevõtte, kelle lukk on peal (idenditud ettevõttekaardi numbri esimese 13 koha alusel), või
- 055 on luku avamine automaatne, kui teine ettevõtte paneb oma luku peale.
- 055a Juhul kui ettevõtte paneb luku peale ja kui eelmine lukk oli sama ettevõtte oma, eeldatakse, et eelmine lukk ei ole avatud ja on ikka veel peal.

8. Kontrollitegevuste seire

- 056 Funktsioon seirab kontrollimooduses tehtud KUVAMISE, TRÜKKIMISE, SÕIDUKIÜKSUSE ja ALLALAADIMISE tegevust.
- 057 Funktsioon seirab kontrollimooduses ka KIIRUSE ÜLETAMISE KONTROLI tegevusi. Kiiruse ületamise kontroll loetakse toimunuks, kui kontrollimooduses on printerile või kuvarile saadetud väljatrükk “kiiruse ületamine” või kui “sündmuste ja rikete” andmed on sõidukiüksuse andmemälust alla laaditud.

9. Sündmuste ja/või rikete tuvastamine

058 Funktsiooniga tuvastatakse järgmised sündmused ja/või rikked:

9.1. “Kehtetu kaardi sisestamise” sündmus

059 Sündmus käivitub mis tahes kehtetu kaardi sisestamisel ja/või sisestatud kehtiva kaardi kehtivusaja lõppemisel.

9.2. "Kaardikonflikti" sündmus

060 Sündmus käivitub siis, kui tekib mis tahes kehtivate kaartide kombinatsioon, mida järgmises tabelis tähistab X:

Kaardikonflikt		Juhikaardi ava				
		Kaart puudub	Juhikaart	Kontrollikaart	Töökojakaart	Ettevõttekaart
Kasjuhi kaardi ava	Kaart puudub					
	Juhikaart				X	
	Kontrollikaart			X	X	X
	Töökojakaart		X	X	X	X
	Ettevõttekaart			X	X	X

9.3. "Aja kattumise" sündmus

061 Sündmus käivitub siis, kui kaardilt loetav juhikaardi viimase väljavõtmise kuupäev/aeg on hilisem kui jooksev kuupäev/aeg sõidumeerikus, millesse kaart sisestatakse.

9.4. "Vajaliku kaardita juhtimise" sündmus

062 Sündmus käivitub järgmises tabelis X-ga tähistatud mis tahes sõidumeerikukaartide kombinatsiooni puhul, kui juhi tegevus muutub JUHTIMISEKS või kui muudetakse toimimismoodust sel ajal, kui juhi tegevus on JUHTIMINE:

Vajaliku kaardita juhtimine		Juhikaardi ava				
		Kaart puudub (või kehtetu kaart)	Juhikaart	Kontrollikaart	Töökojakaart	Ettevõttekaart
Kasjuhi kaardi ava	Kaart puudub (või kehtetu kaart)	X		X		X
	Juhikaart	X		X	X	X
	Kontrollikaart	X	X	X	X	X
	Töökojakaart	X	X	X		X
	Ettevõttekaart	X	X	X	X	X

9.5. "Kaardi sisestamine juhtimise ajal" sündmus

063 Sündmus käivitub sõidumeerikukaardi sisestamisel mis tahes avasse, kui juhi tegevus on JUHTIMINE.

9.6. "Viimane kaardiseanss nõuetekohaselt sulgemata"-sündmus

064 Sündmus käivitub siis, kui kaardi sisestamisel tuvastab sõidumeerik, et vaatamata III lõike punkti 1 sätetele ei ole eelmine kaardiseanss nõuetekohaselt suletud (kaart on välja võetud enne, kui kogu asjaomane teave on kaardile salvestatud). Sündmus käivitub ainult juhi- ja töökojakaartidega.

9.7. "Kiiruse ületamise" sündmus

065 Sündmus käivitub iga lubatava kiiruse ületamise korral.

9.8. "Toiteallika katkestuse" sündmus

- 066 Sündmus käivitub liikumisanduri ja/või sõidukiüksuse toiteallika iga katkestuse korral, mis kestab kauem kui 200 millisekundit, välja arvatud kalibreerimismooduses. Katkestusläve määratleb tootja. Sündmust ei käivita pingelangus toiteallikas seoses sõiduki mootori käivitamisega.

9.9. "Liikumisanndmete vea" sündmus

- 067 Sündmus käivitub normaalse andmevahetuse katkemisel liikumisanduri ja sõidukiüksuse vahel ja/või liikumisanduri ja sõidukiüksuse vahelise andmevahetuse ajal tekkiva andmete terviklikkuse või andmete autentsuse vea puhul.

9.10. "Turbemurdekatse" sündmus

- 068 Sündmus käivitub mis tahes muu sündmuse korral, mis mõjutab liikumisanduri ja/või sõidukiüksuse turvalisust, mis on määratletud nende osade üldistes turbe-eesmärkides, välja arvatud kalibreerimismooduses.

9.11. "Kaardi" rike

- 069 Rike käivitub siis, kui sõidumeerikukaardil esineb töötamise ajal rikkeid.

9.12. "Sõidumeeriku" rike

- 070 Rike käivitub iga järgneva rikke puhul, välja arvatud kalibreerimismooduses:

- sõidukiüksuse siserike,
- printeri rike,
- kuvari rike,
- allalaadimise rike,
- anduri rike.

10. Testid sisseehitatud seadme abil ja enesekontrollitised

- 071 Sõidumeerik tuvastab ise vigu enesekontrollitised ja sisseehitatud seadmega tehtavate testide abil järgmise tabeli kohaselt:

Testitav alakoost	Enesekontrollitised	Test sisseehitatud seadme abil
Tarkvara		Terviklikkus
Andmemälu	Juurdepääs	Juurdepääs, andmeterviklikkus
Kaardiliidese seadmed	Juurdepääsääs	Juurdepääs
Klaviatuur		Käsitsi kontroll
Printer	(tootja otsustada)	Väljatrükk
Kuvar		Visuaalne kontroll
Allalaadimine (toimub ainult allalaadimise ajal)	Nõuetekohane toimimine	
Andur	Nõuetekohane toimimine	Nõuetekohane toimimine

11. Andmemälust lugemine

- 072 Sõidumeerik suudab lugeda kõiki andmeid, mis on tema andmemällu salvestatud.

12. Andmete registreerimine ja salvestamine andmemällu

Käesolevas lõikes:

- tähendab 365 päeva keskmist juhi tegevust sõidukis 365 kalendripäeva jooksul. Keskmine tegevus päeva kohta sõidukis on määratletud vähemalt kuue juhi või kaasjuhi, kuue kaardi sisestamis- ja väljavõtmistsükli ja 256 tegevusmuudatusega. Seetõttu hõlmab 365 päeva vähemalt 2 190 (kaas)juhti, 2 190 kaardi sisestamis- ja väljavõtmistsükli ja 93 440 tegevusmuudatust,
- ajad on salvestatud minutilise täpsusega, kui see ei ole määratletud teisiti,
- läbisõidumõõdiku väärtused on salvestatud täpsusega üks kilomeeter,
- kiirused on salvestatud täpsusega 1 km/h.

073 Tüübikinnitustingimustes ei tohi andmemällu salvestatud andmeid mõjutada alla 12 kuu pikkune välise toiteallika katkestus.

074 Sõidumeerik suudab registreerida ja salvestada oma andmemällu otseselt või kaudselt järgmisi andmeid:

12.1. Seadme identimisandmed

12.1.1. Sõidukiüksuse identimisandmed

075 Sõidumeerik suudab salvestada oma andmemällu järgmisi sõidukiüksuse identimisandmed:

- tootja nimi,
- tootja aadress,
- osa number,
- seerianumber,
- tarkvaraversiooni number,
- tarkvaraversiooni installeerimise kuupäev,
- seadme tootmisaasta,
- tüübikinnitusnumber.

076 Sõidukiüksuse tootja registreerib ja salvestab sõidukiüksuse identimisandmed üks kord ja alatiseks, välja arvatud tarkvaraga seotud andmed ja tüübikinnitusnumber, mida võib tarkvara ajakohastamisel muuta.

12.1.2. Liikumisanduri identimisandmed

077 Liikumisandur suudab salvestada oma mällu järgmisi identimisandmed:

- tootja nimi,
- osa number,
- seerianumber,
- tüübikinnitusnumber,
- sisseehitatud turvakomponendi identifikaator (nt sisekiibi/protssessori osa number)
- operatsioonisüsteemi identifikaator (nt tarkvaraversiooni number).

- 078 Liikumisanduri tootja registreerib ja salvestab liikumisanduri identimisandmed üks kord ja alatiseks liikumisandurisse.
- 079 Sõidukiüksus suudab registreerida ja salvestada oma andemällu järgmisi sellega hetkel ühendatud liikumisanduri identimisandmeid:
- seerianumber,
 - tüübikinnitusnumber,
 - esimese kokkuühendamise kuupäev.

12.2. *Turvaelemendid*

- 080 Sõidumeerik suudab salvestada järgmisi turvaelemente:

- Euroopa avalik võti,
- liikmesriigi sertifikaat,
- seadme sertifikaat,
- meeriku isiklik võti.

Sõidumeeriku turvaelemendid salvestab seadmesse sõidukiüksuse tootja.

12.3. *Juhikaartide sisestamise ja väljavõtmise andmed*

- 081 Juhi- või töökojakaardi iga sisestamis- ja väljavõtmistsükli kohta registreerib ja salvestab sõidumeerik oma andmemällu:

- kaardi omaniku perekonnanime ja eesnime(d), nagu need on kaardile salvestatud,
- kaardi numbril, kaardi väljaandnud liikmesriigi ja kaardi kehtivusaja lõpu, nagu need on kaardile salvestatud,
- sisestamise kuupäeva ja aja,
- sõiduki läbisõidumeeriku näidu kaardi sisestamise ajal,
- ava, millesse kaart sisestati,
- väljavõtmise kuupäeva ja aja,
- sõiduki läbisõidumeeriku näidu kaardi väljavõtmise ajal,
- järgmise teabe juhi poolt enne seda kasutatud sõiduki kohta, nagu see on kaardile salvestatud:
 - sõiduki registreerimisnumber ja registreerinud liikmesriik,
 - kaardi väljavõtmise kuupäev ja kellaaeg,
- tunnuse, mis näitab, kas juht on tegevusi käsitsi sisestanud või mitte.

- 082 Need andmed peavad andmemällus säilima vähemalt 365 päeva.

- 083 Kui salvestusmaht on ammendatud, asendatakse vanimad andmed uute andmetega.

12.4. *Andmed juhi tegevuse kohta*

084 Sõidumeerik registreerib ja salvestab oma andmemällu iga muudatuse korral juhi ja/või kaasjuhi tegevuses ja/või juhtimisstaatuses ja/või iga juhi- või töökojakaardi sisestamisel või väljavõtmisel:

- juhtimisstaatus (MEESKOND, ÜKSI),
- kaardi ava (JUHT, KAASJUHT),
- kaardi staatuse asjaomases avas (SISESTATUD, SISESTAMATA) (vt märkus),
- tegevuse (JUHTIMINE, VALMISOLEK, TÖÖ, VAHEAEG/PUHKUS),
- muudatuse kuupäeva ja aja.

Märkus: SISESTATUD tähendab, et avasse on sisestatud kehtiv juhi- või töökojakaart. SISESTAMATA tähendab vastupidist, st et avasse ei ole sisestatud kehtivat juhi- või töökojakaarti (nt on sisestatud ettevõttekaart või pole ühtegi kaarti sisestatud).

Märkus: juhi käsitsi sisestatud andmeid tegevuse kohta andmemälus ei salvestata.

085 Andmemälus peavad andmed juhi tegevuse kohta säilima vähemalt 365 päeva.

086 Kui salvestusmaht on ammendatud, asendatakse vanimad andmed uute andmetega.

12.5. *Tööpäeva algus- ja/või lõpukoht*

087 Sõidumeerik registreerib ja salvestab alati oma andmemällu, kui (kaas)juht sisestab tööpäeva algus- ja/või lõpukoha:

- (kaas)juhi kaardi numbriga ja vajaduse korral kaardi väljaandnud liikmesriigi,
- sisestamise kuupäeva ja aja (või sisestamisega seotud kuupäeva/aja, kui sisestamine tehakse käsitsi sisestamise käigus),
- sisestuse tüübi (algus või lõpp, sisestustingimus),
- sisestatud riigi või piirkonna,
- sõiduki läbisõidumõõdiku näidu.

088 Andmemälu suudab säilitada vähemalt 365 päeva tööpäeva algus- ja lõpuandmeid (eeldusel et üks juht sisestab andmeid kaks korda päevas).

089 Kui salvestusmaht on ammendatud, asendatakse vanimad andmed uute andmetega.

12.6. *Läbisõidumõõdiku andmed*

090 Sõidumeerik registreerib oma andmemällu sõiduki läbisõidumõõdiku näidu ja vastava kuupäeva iga kalendripäeva keskööl.

091 Andmemälus peavad läbisõidumõõdiku keskõised väärtused säilima vähemalt 365 kalendripäeva kohta.

092 Kui salvestusmaht on ammendatud, asendatakse vanimad andmed uute andmetega.

12.7. *Üksikasjalikud andmed kiiruse kohta*

093 Sõidumeerik registreerib ja salvestab oma andmemällu sõiduki hetkekiiruse ning vastava kuupäeva ja aja kord sekundis vähemalt viimase 24 tunni jooksul, mil see sõiduk on liikunud.

12.8. *Andmed süüdistuste kohta*

Käesoleva lõigu tähenduses salvestatakse aeg sekundilise täpsusega.

094 Sõidumeerik registreerib ja salvestab oma andmemällu iga tuvastatud sündmuse kohta järgmised andmed järgmiste salvestusreeglite kohaselt:

Sündmus	Salvestusreegel	Sündmuse kohta registreeritavad andmed
Kaardikonflikt	— 10 viimast sündmust	— sündmuse alguse kuupäev ja kellaeg, — sündmuse lõpu kuupäev ja kellaeg, — kummagi konflikti tekitanud kaardi tüüp, number ja kaardi väljaandnud liikmesriik.
Kohase kaardita juhtimine	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viimase 365 päeva 5 pikimat sündmust.	— sündmuse alguse kuupäev ja kellaeg, — sündmuse lõpu kuupäev ja kellaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number ja kaardi väljaandnud liikmesriik, — samasuguste sündmuste arv sellel päeval.
Kaardi sisestamine juhtimise ajal	— viimane sündmus iga kümne viimase päeva kohta, mil sündmus toimus.	— sündmuse kuupäev ja kellaeg, — kaardi tüüp, number ja kaardi väljaandnud liikmesriik, — samasuguste sündmuste arv sellel päeval.
Viimane kaardiseanss nõuetekohaselt sulgemata	— 10 viimast sündmust.	— sündmuse kuupäev ja kellaeg, — kaardi tüüp, number ja kaardi väljaandnud liikmesriik, — kaardilt loetud andmed viimase seansi kohta: — kaardi sisestamise kuupäev ja kellaeg, — sõiduki registreerimisnumber ja registreerinud liikmesriik.
Kiiruse ületamine ⁽¹⁾	— kõige tõsisem sündmus (st suurima keskmise kiirusega sündmus) iga kümne viimase päeva kohta, mil sündmusi toimus, — viis kõige tõsisemat sündmust viimase 365 päeva jooksul, — esimene sündmus pärast viimast kalibreerimist.	— sündmuse alguse kuupäev ja kellaeg, — sündmuse lõpu kuupäev ja kellaeg, — sündmuse ajal mõõdetud suurim kiirus, — sündmuse ajal mõõdetud kiiruste aritmeetiline keskmine, — juhikaardi tüüp, number ja vajaduse korral kaardi väljaandnud liikmesriik, — samasuguste sündmuste arv sellel päeval.

Sündmus	Salvestusreegel	Sündmuse kohta registreeritavad andmed
Toiteallika katkestus ⁽²⁾	<ul style="list-style-type: none"> — pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul. 	<ul style="list-style-type: none"> — sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number ja kaardi väljaandnud liikmesriik, — samasuguste sündmuste arv sellel päeval.
Liikumisandmete viga	<ul style="list-style-type: none"> — pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul. 	<ul style="list-style-type: none"> — sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number ja kaardi väljaandnud liikmesriik, — samasuguste sündmuste arv sellel päeval.
Turbemurdekats	<ul style="list-style-type: none"> — 10 viimast sündmust iga sündmuse tüübi kohta. 	<ul style="list-style-type: none"> — sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg vajaduse korral, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number ja kaardi väljaandnud liikmesriik, — sündmuse tüüp.

095

⁽¹⁾ Sõidumeerik registreerib ja salvestab oma andmemällu ka:

- viimase KIIRUSE ÜLETAMISE KONTROLLI kuupäeva ja aja,
- sellele KIIRUSE ÜLETAMISE KONTROLLILE järgneva esimese kiiruse ületamise kuupäeva ja aja,
- pärast viimast KIIRUSE ÜLETAMISE KONTROLLI toimunud kiiruse ületamise sündmuste arvu.

⁽²⁾ Neid andmeid võib registreerida alles toiteallika taasühendamisel, kusjuures aega saab teada minutilise täpsusega.

12.9. Andmed rikete kohta

Käesoleva lõigu tähenduses salvestatakse aeg sekundilise täpsusega.

096

Sõidumeerik püüab registreerida ja salvestada oma andmemällu iga tuvastatud rikke kohta järgmised andmed järgmiste salvestusreeglite kohaselt:

Rike	Salvestusreegel	Rikke kohta registreeritavad andmed
Kaardi rike	<ul style="list-style-type: none"> — 10 viimast juhikaardi riket. 	<ul style="list-style-type: none"> — rikke alguse kuupäev ja kellaaeg, — rikke lõpu kuupäev ja kellaaeg, — kaardi tüüp, number ja kaardi väljaandnud liikmesriik.
Sõidumeeriku rikked	<ul style="list-style-type: none"> — 10 viimast riket iga veatüübi kohta, — esimene rike pärast viimast kalibreerimist. 	<ul style="list-style-type: none"> — rikke alguse kuupäev ja kellaaeg, — rikke lõpu kuupäev ja kellaaeg, — rikke tüüp, — rikke alguses ja/või lõpus sisestatud kaardi tüüp, number ja kaardi väljaandnud liikmesriik.

12.10. Kalibreerimisandmed

- 097 Sõidumeerik registreerib ja salvestab oma andmemällu andmed, mis on seotud:
- teadaolevate kalibreerimisparameetritega aktiveerimise ajal,
 - esimese kalibreerimisega pärast aktiveerimist,
 - esimese kalibreerimisega selles sõidukis (määratakse kindlaks valmistajatehase tähise alusel),
 - viie viimase kalibreerimisega (kui ühel kalendripäeval tehakse mitu kalibreerimist, salvestatakse mällu ainult selle päeva viimane kalibreerimine).
- 098 Iga kalibreerimise kohta registreeritakse järgmised andmed:
- kalibreerimise eesmärk (aktiveerimine, esimene paigaldamine, korrapärane ülevaatus),
 - töökoja nimi ja aadress,
 - töökojakaardi number, kaardi väljaandnud liikmesriik ja kaardi aegumise kuupäev,
 - sõiduki identifikatsioon,
 - ajakohastatud või kinnitatud parameetrid: sõidukit iseloomustav koefitsient, sõidumeeriku konstant, rattarehvide efektiivümberrõõd, rehvi suurus, kiiruspiiriku seadistus, läbisõidumõõdik (vana ja uus näit), kuupäev ja kellaeg (vana ja uus näit).
- 099 Liikumisandur registreerib ja salvestab oma mällu järgmised andmed liikumisanduri paigaldamise kohta:
- esimene sõidukiüksusega kokkuühendamine (kuupäev, aeg, sõidukiüksuse tüübikinnitusnumber, sõidukiüksuse seerianumber),
 - viimane sõidukiüksusega kokkuühendamine (kuupäev, aeg, sõidukiüksuse tüübikinnitusnumber, sõidukiüksuse seerianumber).

12.11. Andmed aja korrigeerimise kohta

- 100 Sõidumeerik registreerib ja salvestab oma andmemällu andmed, mis on seotud:
- viimase aja korrigeerimisega,
 - viie suurima aja korrigeerimisega pärast viimast kalibreerimist,
- mis on tehtud kalibreerimismooduses korrapärase kalibreerimise väliselt (mõiste f).
- 101 Aja iga korrigeerimise kohta registreeritakse järgmised andmed:
- kuupäev ja kellaeg, vana näit,
 - kuupäev ja kellaeg, uus näit,
 - töökoja nimi ja aadress,
 - töökojakaardi number, kaardi väljaandnud liikmesriik ja kaardi aegumise kuupäev.

12.12. Andmed kontrollitegevuse kohta

- 102 Sõidumeerik registreerib ja salvestab oma andmemällu andmed, mis on seotud viimase 20 kontrollitegevusega:
- kontrolli kuupäev ja kellaeg,
 - kontrollikaardi number ja kaardi väljaandnud liikmesriik,
 - kontrolli tüüp (kuvamine ja/või trükkimine ja/või sõidukiüksuse andmete allalaadimine ja/või kaardi andmete allalaadimine).

103 Allalaadimise puhul registreeritakse ka esimese ja viimase allalaadimise kuupäev.

12.13. Andmed ettevõtetelukkude kohta

104 Sõidumeerik registreerib ja salvestab oma andmemällu andmed, mis on seotud viimase 20 ettevõteteluku:

- lukustamise kuupäeva ja ajaga,
- luku avamise kuupäeva ja ajaga,
- ettevõttekaardi numbri ja kaardi väljaandnud liikmesriigiga,
- ettevõtte nime ja aadressiga.

12.14. Andmed allalaadimise kohta

105 Sõidumeerik registreerib ja salvestab oma andmemällu järgmised andmed, mis on seotud viimase andmemälu allalaadimisega väliskandjale ettevõtte- või kalibreerimismooduses:

- allalaadimise kuupäev ja kellaeg,
- ettevõtte- või töökojakaardi number ja kaardi väljaandnud liikmesriik,
- ettevõtte või töökoja nimi.

12.15. Andmed eritingimuste kohta

105a Sõidumeerik registreerib oma andmemällu järgmised andmed, mis on seotud eritingimustega:

- sisestamise kuupäev ja kellaeg,
- eritingimuse tüüp.

105b Andmemälu suudab säilitada eritingimuste andmeid vähemalt 365 päeva (eeldusel et päevas avatakse ja suletakse üks tingimus). Kui salvestusmaht on ammendatud, asendatakse vanimad andmed uute andmetega.

13. Sõidumeerikukaartidelt lugemine

106 Sõidumeerik suudab lugeda sõidumeerikukaartidelt vajaduse korral vajalikke andmeid:

- kaardi tüübi, kaardi omaniku, varem kasutatud sõiduki, kaardi viimase väljavõtmise kuupäeva ja aja ning sel ajal valitud tegevuse identimiseks,
- kontrollimaks, kas viimane kaardiseanss on nõuetekohaselt suletud,
- arvutamaks juhi pidevat sõiduaega, kumulatiivset vaheaega ning eelmise ja jooksva nädala kumulatiivset juhtimisaega,
- trükkimaks vajalikud väljatrükiid, mis on seotud juhikaardile salvestatud andmetega,
- laadimaks alla juhikaardi andmed välisandmekandjatele.

107 Lugemisvea korral üritab sõidumeerik maksimaalselt kolm korda kasutada sama lugemiskäsku, kui see ikkagi ei õnnestu, tunnistatakse kaart vigaseks ja kehtetuks.

14. Registreerimine ja salvestamine sõidumeerikukaartidele

108 Sõidumeerik käivitab "kaardiseansi andmed" juhi- või töökojakaardil kohe pärast kaardi sisestamist.

- 109 Sõidumeerik ajakohastab kehtival juhi-, töökoja- ja/või ettevõttele salvestatud andmed kõigi vajalike andmetega, mis on seotud ajaga, mil kaart on sisestatud, ja kaardi omanikuga. Neile kaartidele salvestatud andmed on määratletud IV peatükis.
- 109a Sõidumeerik ajakohastab andmed juhi tegevuse ja asukoha kohta (IV peatüki lõigete 5.2.5 ja 5.2.6 kohaselt), mis on salvestatud juhi- ja/või töökojakaartidele, kaardi omaniku käsitsi sisestatud andmetega tegevuse ja asukoha kohta.
- 110 Sõidumeerikukaartide ajakohastamine toimub nii, et vajaduse korral ja võttes arvesse kaardi tegelikku salvestusmahtu asendatakse vanimad andmed uusimate andmetega.
- 111 Kirjutamisvea korral üritab sõidumeerik maksimaalselt kolm korda kasutada sama kirjutamiskäsku, kui see ikkagi ei õnnestu, tunnistatakse kaart vigaseks ja kehtetuks.
- 112 Enne juhikaardi vabastamist ja pärast kõigi asjakohaste andmete salvestamist kaardile lähtestab sõidumeerik kaardiseansi andmed.

15. Kuvamine

- 113 Kuvaril on vähemalt 20 tähemärki.
- 114 Tähemärk on vähemalt 5 mm kõrge ja 3,5 mm lai.
- 114a Kuvar toetab ISO 8859 1. ja 7. osas määratletud ladina-1 ja kreeka märgistikku, nagu see on kirjeldatud 1. liite 4. peatükis "Märgistikud". Kuvar võib kasutada lihtsustatud glüüfe (nt rõhumärkidega tähemärke võib kuvada rõhumärkideta või väiketähti võib näidata suurtähtedena).
- 115 Kuvar on varustatud piisava mittepimestava valgustusega.
- 116 Suuruste näidud on nähtavad väljastpoolt sõidumeerikut.
- 117 Sõidumeerik suudab kuvada:
- vaikeandmeid,
 - hoiatustega seotud andmeid,
 - menüüpääsuga seotud andmeid,
 - muid andmeid, mida kasutaja soovib.
- Sõidumeerik võib kuvada lisateavet, eeldusel et see on selgesti eristatav eespool esitatud nõutavast teabest.
- 118 Sõidumeeriku kuvaril kasutatakse 3. liites loetletud piktogramme või piktogrammikombinatsioone. Kuvaril võib olla ka lisapiktogramme või piktogrammikombinatsioone, kui need on selgesti eristatavad eespool nimetatud piktogrammidest ja piktogrammikombinatsioonidest.

- 119 Kuvar on alati lülitatud SISSE, kui sõiduk liigub.
- 120 Sõidumeerikul võib olla ka manuaalne või automaatne funktsioon kuvari lülitamiseks VÄLJA, kui sõiduk ei liigu.
- Kuvamisvorming on määratletud 5. liites.

15.1. Vaikekuva

- 121 Kui muud teavet ei ole tarvis kuvada, näitab kuvar vaikimisi järgmisi andmeid:
- kohalik aeg (universaalaeg + juhivoolne reguleerimine),
 - toimimismoodus,
 - juhi hetketegevus ja kaasjuhi hetketegevus,

- juhiga seotud teave:
 - kui juhi hetketegevus on JUHTIMINE, siis jooksev pidev juhtimisaeg ja jooksev kumulatiivne vaheaeg,
 - kui juhi hetketegevus ei ole JUHTIMINE, siis tegevuse jooksev kestus (alates selle valimisajast) ja jooksev kumulatiivne vaheaeg,
- kaasjuhiga seotud teave:
 - tema tegevuse jooksev kestus (alates selle valimisajast).

- 122 Iga juhiga seotud andmete kuva on selge, lihtne ja üheselt mõistetav. Juhul kui juhi ja kaasjuhiga seotud teavet ei saa kuvada üheaegselt, kuvab sõidumeerik vaikumisi juhiga seotud teavet ja võimaldab kasutajal kuvada kaasjuhiga seotud teavet.
- 123 Juhul kui kuvari laius ei võimalda vaikumisi kuvada toimimismoodust, kuvab sõidumeerik lühidalt uue toimimismooduse, kui see valitakse.
- 124 Kaardi sisestamisel kuvab sõidumeerik hetkeks kaardi omaniku nime.
- 124a Kui avatakse tingimus "SÕIDUMEERIK MITTEVAJALIK", peab kuvar vaikumisi näitama, et see tingimus on avatud, kasutades asjaomast piktogrammi (on lubatud, et juhi hetketegevust sel ajal ei näidata).

15.2. Hoiatuskuva

- 125 Sõidumeerik kuvab hoiatusteavet, kasutades peamiselt 3. liite piktogramme, millele on vajaduse korral lisatud numbriliselt kodeeritud teave. Võib lisada hoiatuse selgesõnalise kirjelduse juhi valitud keeles.

15.3. Menüüpääs

- 126 Sõidumeerikul on kohases menüüstruktuuris vajalikud käsud.

15.4. Muud kuvad

- 127 Soovi korral peab valikuliselt saama kuvada:
- kuupäeva ja kellaaega universaalajas,
 - toimimismoodust (kui seda ei esitata vaikumisi),
 - juhi pidevat juhtimisaega ja kumulatiivset vaheaega,
 - kaasjuhi pidevat juhtimisaega ja kumulatiivset vaheaega,
 - juhi kumulatiivset juhtimisaega eelmisel ja jooksva nädalal,
 - kaasjuhi kumulatiivset juhtimisaega eelmisel ja jooksva nädalal,
 - kuue väljatrüki sisu samas vormingus kui väljatrükk ise.
- 128 Väljatrüki sisu kuva on järjestikune ja rea kaupa. Kui kuvari laius on alla 24 tähemärgi, esitatakse kasutajale kogu teave kohase vahendi (mitu rida, kerimine, ...) abil. Käsitsi kirjutatud teabe tarvis jäetud väljatrüki read võib kuvamisel välja jätta.

16. Trükkimine

- 129 Sõidumeerik suudab trükkida andmeid oma andmemälust ja/või sõidumeerikukaartidelt vastavalt kuuele järgmisele väljatrükile:
- juhi ühe päeva tegevuste väljatrükk kaardilt,
 - juhi ühe päeva tegevuste väljatrükk sõidukiüksusest,

- sündmuste ja rikete väljatrükk kaardilt,
- sündmuste ja rikete väljatrükk sõidukiüksusest,
- tehniliste andmete väljatrükk,
- kiiruse ületamise väljatrükk.

Nende väljatrükkide üksikasjalik vorming ja sisu on määratletud 4. liites.

Sõidumeerik võib esitada ka lisaväljatrükke, kui need on selgesti eristatavad eespool nimetatud kuuest väljatrükist.

- 130 "Juhi ühe päeva tegevuste väljatrükk kaardilt" ja "juhi ühe päeva tegevuste väljatrükk sõidukiüksusest" on võimalikud ainult siis, kui sõidumeerikusse on sisestatud juhi- või töökojakaart. Enne trükkimise alustamist ajakohastab sõidumeerik asjaomasele kaardile salvestatud andmed.
- 131 Selleks et teha "juhi ühe päeva tegevuste väljatrükk kaardilt" või "sündmuste ja rikete väljatrükk kaardilt", sõidumeerik:
- valib automaatselt juhi- või töökojakaardi, kui ainult üks neist kaartidest on sisestatud, või
 - annab käsu valida allikkaart või valida kaart juhikaardi avas, kui sõidumeerikusse on korraga sisestatud kaks kaarti.
- 132 Printer suudab trükkida ühes reas 24 tähemärki.
- 133 Tähemärk on vähemalt 2,1 mm kõrge ja 1,5 mm lai.
- 133a Printer toetab ISO 8859 osades 1 ja 7 määratletud ladina-1 ja kreeka märgistikku, nagu see on kirjeldatud 1. liite 4. peatükis "Märgistikud".
- 134 Printerid on konstrueeritud nii, et väljatrükkide kujutustäpsus välistab lugemisel igasugused arusaamatused.
- 135 Väljatrükkid säilitavad normaalsetes niiskuses- (10 kuni 90 %) ja temperatuuritingimustes oma mõõtmed ja kirjed.
- 136 Sõidumeerikus kasutataval paberil on asjaomane tüübikinnitusmärk ja viide, millist tüüpi sõidumeerikus (sõidumeerikutes) seda võib kasutada. Tavalistes säilitustingimustes, pidades silmas valguse intensiivsust, niiskust ja temperatuuri, jäävad väljatrükkid selgelt loetavaks ja idenditavaks vähemalt ühe aasta jooksul.
- 137 Neile dokumentidele on võimalik lisada ka käsitsi kirjutatud märkusi, näiteks juhi allkiri.
- 138 "Paberi lõppemise" sündmuse korral alustab sõidumeerik paberi lisamisel väljatrükki uuesti algusest või jätkab trükkimist, esitades üheselt mõistetava viite eelnevalt trükitud osale.

17. Hoiatused

- 139 Sõidumeerik annab juhile hoiatuse, kui see tuvastab mis tahes sündmuse ja/või rikke.
- 140 Hoiatuse toiteallika katkestuse sündmuse kohta võib lükata edasi ajani, mil toiteallikas taas külge ühendatakse.
- 141 Sõidumeerik hoiatab juhti 15 minutit enne 4 tunni ja 30 minuti pideva juhtimisaja täitumist ja selle aja täitumisel.
- 142 Hoiatused on visuaalsed. Lisaks nähtavatele hoiatustele võib esitada ka kuuldavaid hoiatusi.

- 143 Visuaalsed hoiatused on kasutajale selgelt äratuntavad, need asuvad juhi vaateväljas ning on selgesti loetavad nii päeval kui öösel.
- 144 Visuaalsed hoiatused võivad olla sõidumeeriku sees ja/või olla sellest väljaspool.
- 145 Viimasel juhul on hoiatusel sümbol "T" ning see on merevaigukollane või oranž.
- 146 Hoiatus kestab vähemalt 30 sekundit, kui kasutaja ei ole sellele sõidumeeriku mis tahes klahvile vajutades reageerinud. Esimene reageerimine ei kustuta hoiatuse põhjuse kuva, millele on viidatud järgmises lõikes.
- 147 Hoiatuse põhjus kuvatakse sõidumeerikul ja see jääb nähtavaks, kuni kasutaja on sellele reageerinud, kasutades sõidumeeriku eriklahvi või -käsku.
- 148 Võib anda lisahoiatusi, kui need ei aja juhti segadusse seoses eelnevalt määratletud hoiatustega.

18. Andmete allalaadimine välisandmekandjatele

- 149 Vajaduse korral suudab sõidumeerik alla laadida oma andmemälust või juhikaardilt andmeid välisandmekandjale kalibreerimise/allalaadimise pistiku kaudu. Enne allalaadimise alustamist ajakohastab sõidumeerik asjaomasele kaardile salvestatud andmed.
- 150 Lisaks sellele ja vabatahtliku funktsioonina võib sõidumeerik mis tahes toimimismooduses alla laadida teise pistiku kaudu andmeid ettevõttele, mis on autenditud selle kanali kaudu. Sellisel juhul kohaldatakse allalaadimise suhtes ettevõtetemooduse andmepääsu õigusi.
- 151 Allalaadimine ei tohi salvestatud andmeid muuta ega kustutada.

Kalibreerimise/allalaadimise pistiku elektriline liides on määratletud 6. liites.

Allalaadimisprotokollid on määratletud 7. liites.

19. Andmete väljastamine välistele lisaseadmetele

- 152 Kui sõidumeerikul ei ole kiiruse ja/või läbisõidumõõdiku kuvamisfunktsioone, annab sõidumeerik väljundsignaali (väljundsignaalid), mille abil on võimalik kuvada sõiduki kiirust (spidomeeter) ja/või sõiduki läbitud kogu teepikkust (läbisõidumõõdik).
- 153 Sõidukiüksus suudab väljastada järgmisi andmeid, kasutades valikulisest CAN-siiniühendusest sõltumatut kohast jadaühendust (ISO 11898 Maanteeõidukid — Digitaalne andmevahetus — Kiirsid ehk Controller Area Network (CAN)), mis võimaldab andmete töötlemist sõidukisse paigaldatud teistes elektroonilistes üksustes:

- käesolev kuupäev ja kellaeg universaalajas,
- sõiduki kiirus,
- sõiduki läbitud kogu teepikkus (läbisõidumõõdik),
- hetkel valitud juhi ja kaasjuhi tegevus,
- teave selle kohta, kas mõni sõidumeerikukaart on hetkel sisestatud juhikaardi avasse ja kaasjuhi kaardi avasse ning vajaduse korral teave vastavate kaartide identifikatsiooni kohta (kaardi number ja kaardi väljaandnud liikmesriik).

Lisaks sellele miinimumnimekirjale võib väljastada ka muid andmeid.

Kui sõiduki süüde on lülitatud SISSE, edastatakse neid andmeid pidevalt. Kui sõiduki süüde on lülitatud VÄLJA, tekitavad vastava andmeväljastuse vähemalt juhi ja/või kaasjuhi tegevuse mis tahes muutus ja/või sõidumeerikukaardi mis tahes sisestamine või väljavõtmine. Juhul kui andmeväljastus on peatunud, kui sõiduki süüde on VÄLJAS, on need andmed taas kättesaadavad, kui sõiduki süüde on uuesti lülitatud SISSE.

20. Kalibreerimine

- 154 Kalibreerimisfunktsioon võimaldab:
- ühendada liikumisandur automaatselt sõidukiüksusega,
 - digitaalselt kohandada sõidumeeriku konstanti (k) sõidukit iseloomustava konstandiga (w) (kahe või enama veosilla ülekandearvuga sõidukitele tuleb paigaldada lülitusseade, mille abil need erinevad ülekandearvud saab automaatselt viia vastavusse ülekandearvuga, millele sõiduki sõidumeerik on kohandatud),
 - korrigeerida (piiranguteta) hetkeagea,
 - korrigeerida läbisõidumõõdiku hetkeväärtust,
 - ajakohastada andmemällu salvestatud liikumisanduri identimisandmeid,
 - ajakohastada või kinnitada muid sõidumeerikule tuntud parameetreid: sõiduki identifitseerimine, sõidukit iseloomustav koefitsient, rattarehvide efektiivümberrõõm, rehvi suurus ja kiiruspiiriku seaded vajaduse korral.
- 155 Liikumisanduri ühendamine sõidukiüksusega hõlmab vähemalt:
- liikumisanduris olevate liikumisanduri paigaldusandmete ajakohastamist (vajaduse korral),
 - vajalike liikumisanduri identimisandmete kopeerimist liikumisandurist sõidukiüksuse andmemällu.
- 156 Kalibreerimisfunktsioon peab suutma sisestada vajalikke andmeid kalibreerimise/allalaadimise pistiku kaudu vastavalt 8. liites määratletud kalibreerimisprotokollile. Kalibreerimisfunktsioon võib sisestada vajalikke andmeid ka muude pistikute kaudu.

21. Aja korrigeerimine

- 157 Aja korrigeerimise funktsioon võimaldab korrigeerida hetkeagea maksimaalselt ühe minuti võrra vähemalt seitsme päeva möödumisel.
- 158 Aja korrigeerimise funktsioon võimaldab hetkeagea piiramata korrigeerida kalibreerimismooduses.

22. Toimeomadused

- 159 Sõidukiüksus toimib täielikult temperatuurivahemikus -20 °C kuni 70 °C , liikumisandur temperatuurivahemikus -40 °C kuni 135 °C . Andmemällu sisu säilib temperatuuril kuni -40 °C .
- 160 Sõidumeerik toimib täielikult niiskuse puhul 10 % kuni 90 %.
- 161 Sõidumeerikut kaitstakse ülepinge, toiteallika polaarsuse vahetuse ja lühiste eest.
- 162 Sõidumeerik vastab komisjoni 31. oktoobri 1995. aasta direktiivile 95/94/EÜ⁽¹⁾, millega kohandatakse nõukogu direktiivi 72/245/EMÜ⁽²⁾ (mis käsitleb elektromagnetilist ühilduvust) tehnika arenguga, ning seda kaitstakse elektrostaatiliste lahenduste ja siirete eest.

23. Materjalid

- 163 Sõidumeeriku kõik koostisosad on tehtud piisavalt stabiilsetest ja piisava mehaanilise tugevusega materjalidest, millel on stabiilsed elektrilised ja magnetilised omadused.
- 164 Normaalseste kasutustingimuste tagamiseks tuleb seadme kõiki sisemisi osi kaitsta niiskuse ja tolmu eest.
- 165 Sõidukiüksus vastab standardi IEC 529 kaitseklassile IP 40 ja liikumisandur kaitseklassile IP 64.

⁽¹⁾ EÜT L 266, 8.11.1995, lk 1.

⁽²⁾ EÜT L 152, 6.7.1972, lk 15.

- 166 Sõidumeerik peab ergonoomilise väliskujunduse poolest vastama kohaldatavatele tehnospetsifikaatidele.
- 167 Sõidumeerikut kaitstakse juhusliku rikkumise eest.

24. Märkised

- 168 Kui sõidumeerik kuvab sõiduki läbisõidumõõdiku väärtust ja kiirust, ilmuvad selle kuvarile järgmised andmed:
- teepikkuse mõõtühik, mida tähistab lühend km teepikkuse näidu lähedal,
 - kiiruse näidu lähedal lühend km/h.
- Sõidumeeriku võib lülitada kuvama kiirust miilides tunnis, sellisel juhul näidatakse kiiruse mõõtühikut lühendi mph abil.
- 169 Sõidumeeriku igale eraldi osale kinnitatakse kirjeldav tahvel, millel on järgmised üksikasjad:
- seadme tootja nimi ja aadress,
 - tootja osa number ja seadme valmistusaasta,
 - seadme seerianumber,
 - seadme tüübikinnitusmärk.
- 170 Kui kõigi eespool nimetatud üksikasjade esitamiseks ei ole ruumi, on kirjeldaval tahvil vähemalt tootja nimi või logo ja seadme osa number.

IV. SÕIDUMEERIKUKAARTIDE KONSTRUKTSIOONI- JA FUNKTSIONAALSED NÕUDED

1. Nähtavad andmed

Esipoolel on:

- 171 vastavalt kaardi tüübile suurelt trükitult sõna "juhikaart" või "kontrollikaart" või "töökojakaart" või "ettevõttele kaardi väljaandnud liikmesriigi ametlikus keeles või ametlikes keeltes";
- 172 sama sõna trükitult ühenduse teistes ametlikes keeltes, mis moodustab kaardi tausta:

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	CĀRTA TIOMĀNAĀ	CĀRTA STIĀRTHA	CĀRTA CEARDLAINNE	CĀRTA 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 KORTTILLA	TESTAUSASEMA KORTTILLA	YRITYSKORTTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

- 173 kaardi väljaandnud liikmesriigi nimi (ei ole kohustuslik);

174 kaardi väljaandnud liikmesriigi rahvusvaheline tähis negatiivina sinises ristkülikus, mida ümbritseb kaksteist kollast tähte. Tähistes on järgmised:

B	Belgia
DK	Taani
D	Saksamaa
GR	Kreeka
E	Hispaania
F	Prantsusmaa
IRL	Iirimaa
I	Itaalia
L	Luksemburg
NL	Madalmaad
A	Austria
P	Portugal
FIN	Soome
S	Rootsi
UK	Ühendkuningriik;

175 teave väljaantud kaardi kohta järgmiste nummerdatud andmetega:

	Juhikaart	Kontrollikaart	Ettevõtte- või töökojakaart
1.	Juhi perekonnanimi	Kontrolliasutuse nimi	Ettevõtte või töökoja nimi
2.	Juhi eesnimi (eesnimed)	Kontrollija perekonnanimi (vajaduse korral)	Kaardi omaniku perekonnanimi (vajaduse korral)
3.	Juhi sünniaeg	Kontrollija eesnimi (eesnimed) (vajaduse korral)	Kaardi omaniku eesnimi (eesnimed) (vajaduse korral)
4.(a)	Kaardi kehtivusaja algus		
(b)	Kaardi kehtivusaja lõpp		
(c)	Kaardi väljaandnud asutuse nimi (võib trükkida kaardi pöördele)		
(d)	Punkti 5 all olevast numbrist erinev haldusnumber (ei ole kohustuslik)		
5.(a)	Juhiloa number (juhikaardi väljaandmise päeval)		
5.(b)	Kaardi number		
6.	Juhi foto	Kontrollija foto (ei ole kohustuslik)	—
7.	Juhi allkiri	Omaniku allkiri (ei ole kohustuslik)	
8.	Omaniku alaline elukoht või postiaadress (ei ole kohustuslik)	Kontrolliasutuse postiaadress	Ettevõtte või töökoja postiaadress





176 kuupäev kirjutatakse vormingus "pp/kk/aaaa" või "pp.kk.aaaa" (päev, kuu, aasta);"

tagumisel küljel on:

177 selgitus kaardi esiküljel olevate nummerdatud punktide kohta;

178 kirjaliku erikokkuleppe alusel omanikuga võib kaardile lisada teavet, mis ei ole seotud kaardi haldamisega, lisamine ei muuda mingil moel selle kasutamist sõidumeerikukaardina.

ÜHENDUSE SÕIDUMEERIKUKAARTIDE NÄIDISED

ESIKÜLG		TAGAKÜLG	
JUHIKAART	LIIKMESRIIK		
1. 	TARJETA DEL CONDUCTOR	1. Perekonnanimi 2. Eesnimi 3. Sünniaeg	
2.	FØRERKORT	4a. Kaardi kehtivusaja algus	
3.	FAHREKARTE	4b. Kaardi halduskehtivuse lõpp	
4a.	ΚΑΡΤΑ Ο ΔΗΤΟΥ	4c. Väljaandnud asutus	
4c.	DRIVER CARD	(4d.) Siseriiklik haldusnumber	
(4d.)	CARTE DE CONDUCTEUR	5a. Juhiloa number	5b. Kaardi number
5a.	CÁRTA TROMÁNAI	6. Foto	
5b.	CARTA DEL CONDUCENTE	7. Allkiri (8.) Address	
7.	BESTUURDERSKAART	<i>Palun tagastada:</i>	
(8.)	CARTÃO DE CONDUTOR	ASUTUSE NIMI JA ADDRESS	
	KULJETTAJAKORTTILLA		
	FØRARKORT		
KONTROLLIKAART	LIIKMESRIIK		
1. 	TARJETA DE CONTROL	1. Kontrolli- 2. Perekonnanimi 3. Eesnimi	
(2.)	KONTROLKORT	asutus (eesnimed)	
(3.)	KONTROLLKARTE	4a. Kaardi kehtivusaja algus	
4a.	ΚΑΡΤΑ ΕΛΕΓΧΟΥ	4b. Kaardi halduskehtivuse lõpp	
4c.	CONTROL CARD	4c. Väljaandnud asutus	
(4d.)	CARTE DE CONTROLEUR	(4d.) Siseriiklik haldusnumber	
5b.	CÁRTA STIURTHA	5b. Kaardi number	
(7.)	CARTA DI CONTROLLO	6.) Foto	
8.	CONTROLEKAART	7.) Allkiri 8. Address	
	CARTÃO DE CONTROLO	<i>Palun tagastada:</i>	
	VALVONTAKORTTILLA	ASUTUSE NIMI JA ADDRESS	
	KONTROLLKORT		
TÖÖKOJA- KAART	LIIKMESRIIK		
1. 	TARJETA DEL CENTRO DE ENSAYO	1. Töökoja 2. Perekonnanimi 3. Eesnimi	
(2.)	VÆRKSTEDSKORT	nimi (eesnimed)	
(3.)	WERKSTATTKARTE	4a. Kaardi kehtivusaja algus	
4a.	ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	4b. Kaardi halduskehtivuse lõpp	
4c.	(4b.) WORKSHOP CARD	4c. Väljaandnud asutus	
(4d.)	CARTE D'ATELIER	(4d.) Siseriiklik haldusnumber	
5b.	CÁRTA CEARDLAINNE	5b. Kaardi number	
(7.)	CARTA DELL'OFFICINA	7.) Allkiri 8. Address	
8.	WERKPLAATSKAART	<i>Palun tagastada:</i>	
	CARTÃO DO CENTRO DE ENSAIO	ASUTUSE NIMI JA ADDRESS	
	TESTAUSAASEMAKORTTILLA		
	VERKSTADSKORT		
ETTEVÕTTE- KAART	LIIKMESRIIK		
1. 	TARJETA DE LA EMPRESA	1. Ettevõtte 2. Perekonnanimi 3. Eesnimi	
(2.)	VIRKSOMHEDSKORT	nimi (eesnimed)	
(3.)	UNTERNEHMENSKARTE	4a. Kaardi kehtivusaja algus	
4a.	ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΕΩΣ	4b. Kaardi halduskehtivuse lõpp	
4c.	(4b.) COMPANY CARD	4c. Väljaandnud asutus	
(4d.)	CARTE D'ENTREPRISE	(4d.) Siseriiklik haldusnumber	
5b.	CÁRTA COMHLACHTA	5b. Kaardi number	
(7.)	CARTA DELL'AZIENDA	7.) Allkiri 8. Address	
8.	BEDRUFSSKAART	<i>Palun tagastada:</i>	
	CARTÃO DE EMPRESA	ASUTUSE NIMI JA ADDRESS	
	YRITYSKORTTILLA		
	FØRETAGSKORT		

179 Sõidumeerikukaartidele trükitakse järgmine taustavärv:

- juhikaart: valge,
- kontrollikaart: sinine,
- töökojakaart: punane,
- ettevõttekaart: kollane.

180 Sõidumeerikukaartidel on vähemalt järgmised omadused, kaitsmaks neid võltsimise ja rikkumise eest:

- peente giljošmustrite ja vikerkaatretrükiga taustaturvamärk,
- foto piirkonnas kattuvad taustaturvamärk ja foto,
- vähemalt üks kahevärviline mikrokirjas rida.

- 181 Liikmesriigid võivad pärast komisjoniga konsulteerimist lisada värve või märgistusi, näiteks riiklikke sümboleid ja turvaelemente, ilma et see piiraks käesoleva lisa muude sätete kohaldamist.

2. Turvalisus

Süsteemi turvalisuse eesmärk on kaitsta kaartide ja sõidumeeriku vahel vahetatud andmete terviklikkust ja autentsust, kaitstes kaartidelt allalaaditud andmete terviklikkust ja autentsust, lubades teatavaid kirjutamisoperatsioone teha kaartidele ainult sõidumeerikul, välistades kaartidele salvestatud andmete igasuguse võltsimise, takistades petmist ning tuvastades igasuguse katse seda teha.

- 182 Süsteemi turvalisuse saavutamiseks peavad sõidumeerikukaardid vastama turvanõuetele, mis on määratletud sõidumeerikukaartide üldistes turbe-eesmärkides (10. liide).

- 183 Sõidumeerikukaarte on võimalik lugeda muude seadmetega, näiteks personaalarvutid.

3. Standardid

- 184 Sõidumeerikukaardid vastavad järgmistele standarditele:

- ISO/IEC 7810 Identification cards — Physical characteristics (Identimiskaardid — Tehnilised karakteristikud),
- ISO/IEC 7816 Identification cards — Integrated circuits with contacts (Identimiskaardid — Kontaktidega kiipkaardid):
 - Osa 1: tehnilised karakteristikud,
 - Osa 2: mõõtmed ja kontaktide asukoht,
 - Osa 3: elektroonilised signaalid ja edastusprotokollid,
 - Osa 4: valdkondadevahelised andmevahetuskäsud,
 - Osa 8: turvalisusega seotud valdkondadevahelised käsud,
- ISO/IEC 10373 Identification cards — Test methods (identimiskaardid — katsemeetodid).

4. Keskkonnavalased ja elektrilised spetsifikaadid

- 185 Sõidumeerikukaardid suudavad nõuetekohaselt toimida kõigis ühenduse territooriumil tavaliselt esinevates kliimatingimustes ning vähemalt temperatuurivahemikus -25 °C kuni $+70\text{ °C}$ juhusliku maksimumtemperatuuriga kuni $+85\text{ °C}$, kusjuures "juhuslik" tähendab kuni 4 tundi korraga ja kuni sada korda kaardi kasutusea jooksul.
- 186 Sõidumeerikukaardid toimivad nõuetekohaselt niiskuse puhul 10 % kuni 90 %.
- 187 Sõidumeerikukaardid toimivad nõuetekohaselt viis aastat, kui neid kasutatakse vastavalt keskkonnavalastele ja elektrilistele spetsifikaatidele.
- 188 Toimimise ajal vastavad sõidumeerikukaardid komisjoni 31. oktoobri 1995. aasta direktiivile 95/54/EÜ, mis käsitleb elektromagnetilist ühilduvust ⁽¹⁾, ning neid kaitstakse elektrostaatiliste lahenduste eest.

5. Andmete salvestamine

Käesolevas lõikes:

- on ajad salvestatud täpsusega üks minut, kui see ei ole määratletud teisiti,
- läbisõidumõõdiku väärtused on salvestatud täpsusega üks kilomeeter,
- kiirused on salvestatud täpsusega 1 km/h.

Andmesalvestusnõuetele vastavad sõidumeerikukaartide funktsioonid, käsud ja loogilised struktuurid on määratletud 2. liites.

⁽¹⁾ EÜT L 266, 8.11.1995, lk 1.

189 Käesolevas lõikes määratletakse erineva kasutusotstarbega andmefailide minimaalne salvestusmaht. Sõidumeerikukaardid suudavad näidata sõidumeerikule nende andmefailide tegelikku salvestusmahtu.

Kõiki sõidumeerikukaartidele salvestatavaid lisaandmeid, mis on seotud muude rakendustega ja mille jaoks kaart on samuti ette nähtud, salvestatakse vastavalt 24. oktoobri 1995. aasta direktiivile 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta ⁽¹⁾.

5.1. **Kaardi identimis- ja turbeandmed**

5.1.1. *Rakenduse identifitseerimine*

190 Sõidumeerikukaardid suudavad salvestada järgmisi andmeid rakenduse identifitseerimise kohta:

- sõidumeeriku rakenduse identifitseerimine,
- sõidumeerikukaardi tüübi identifitseerimine.

5.1.2. *Kiibi identifitseerimine*

191 Sõidumeerikukaardid suudavad salvestada järgmisi andmeid kiibi identifitseerimise kohta:

- kiibi seerianumber,
- kiibi tootmisandmed.

5.1.3. *Kiipkaardi identifitseerimine*

192 Sõidumeerikukaardid suudavad salvestada järgmisi andmeid kiipkaardi identifitseerimise kohta:

- kaardi seerianumber (sealhulgas tootmisandmed),
- kaardi tüübikinnitusnumber,
- kaardi tunnus (ID),
- paigaldaja tunnus,
- kiibi identifikaator.

5.1.4. *Turvaelemendid*

193 Sõidumeerikukaardid suudavad salvestada järgmisi andmeid turvaelementide kohta:

- Euroopa avalik võti,
- liikmesriigi sertifikaat,
- kaardi sertifikaat,
- kaardi isiklik võti.

5.2. **Juhikaart**

5.2.1. *Kaardi identifitseerimine*

194 Juhikaart suudab salvestada järgmisi andmeid kaardi identimisandmeid:

- kaardi number,
- väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,
- kaardi kehtivusaja algus, kaardi kehtivusaja lõpp.

⁽¹⁾ EÜT L 281, 23.11.1995, lk 31.

5.2.2. Kaardi omaniku identifitseerimine

195 Juhikaart suudab salvestada järgmisi kaardi omaniku identifitseerimisandmeid:

- omaniku perekonnanimi,
- omaniku eesnimi (eesnimed),
- sünniaeg,
- eelistatav keel.

5.2.3. Teave juhiloa kohta

196 Juhikaart suudab salvestada järgmisi andmeid juhiloa kohta:

- väljaandnud liikmesriik, väljaandnud asutuse nimi,
- juhiloa number (kaardi väljaandmise päeval).

5.2.4. Andmed kasutatud sõidukite kohta

197 Juhikaart suudab salvestada iga kalendripäeva kohta, mil kaarti on kasutatud, ja sel päeval konkreetse sõiduki kasutaja kohta (kaardi seisukohalt hõlmab kasutusaeg kogu järjestikust sisestamise/väljavõtmise kaarditsükli sõidukis) järgmisi andmeid:

- sõiduki esimese kasutamise kuupäev ja kellaeg (st sõiduki selle kasutaja kaardi esimene sisestamine või 00.00, kui kasutusaeg sel ajal jätkub),
- sõiduki läbisõidumeeriku näit sel ajal,
- sõiduki viimase kasutamise kuupäev ja kellaeg (st sõiduki selle kasutaja kaardi viimane väljavõtmine või 23.59, kui kasutamisaeg sel ajal jätkub),
- sõiduki läbisõidumeeriku näit sel ajal,
- sõiduki registreerimisnumber ja sõiduki registreerinud liikmesriik.

198 Juhikaart suudab salvestada vähemalt 84 sellist kirjet.

5.2.5. Andmed juhi tegevuse kohta

199 Juhikaart suudab salvestada iga päeva kohta, mil kaarti on kasutatud või mille kohta juht on tegevused käitsi sisestanud, järgmised andmed:

- kuupäev,
- tööpäevade loendur (mida suurendatakse igal kalendripäeval ühe võrra),
- juhi poolt läbitud kogu teepikkus sellel päeval,
- juhi staatus kell 00.00,
- kõik korrad, mil juht on muutnud tegevust ja/või juhtimisstaatus ja/või on oma kaardi sisestanud või välja võtnud:
 - juhtimisstaatus (MEESKOND, ÜKSI),
 - ava (JUHT, KAASJUHT),
 - kaardi staatus (SISESTATUD, SISESTAMATA),
 - tegevus (JUHTIMINE, VALMISOLEK, TÖÖ, VAHEAEG/PUHKUS),
 - muudatuse kellaeg.

200 Juhikaardi mälu suudab säilitada vähemalt 28 päeva andmed juhi tegevuse kohta (keskmine juhi tegevus on määratletud 93 tegevusmuudatusega päevas).

201 Nõuetes 197 ja 199 loetletud andmed salvestatakse nii, et tegevuseotsinguid saab teha toimumise järjestuses isegi ajalise kattumise korral.

5.2.6. *Tööpäeva algus- ja/või lõpukoht*

202 Juhikaart suudab salvestada järgmised andmed, mis on seotud juhi sisestatud tööpäeva algus- ja/või lõpukohaga:

- sisestamise kuupäev ja kellaeg (või sisestamisega seotud kuupäev/aeg, kui sisestamine toimub käsitsi),
- sisestuse tüüp (algus või lõpp, sisestustingimus),
- sisestatud riik või piirkond,
- sõiduki läbisõidumõõdiku näit.

203 Juhikaardi mällu mahub vähemalt 42 paari selliseid kirjeid.

5.2.7. *Andmed sündmuste kohta*

Käesoleva lõigu tähenduses salvestatakse kellaeg sekundilise täpsusega.

204 Juhikaart suudab salvestada järgmised andmed, mis on seotud kaardi sisestamisel sõidumeeriku tuvastatud järgmiste sündmustega:

- aja kattumine (kui see kaart on sündmuse põhjustaja),
- kaardi sisestamine juhtimise ajal (kui see kaart on sündmuse põhjustaja),
- viimane kaardiseanss nõuetekohaselt sulgemata (kui see kaart on sündmuse põhjustaja),
- toiteallika katkestus,
- liikumisandmete viga,
- turbemurdekatsed.

205 Juhikaart suudab salvestada järgmisi andmeid nende sündmuste kohta:

- sündmuse kood,
- sündmuse kuupäev ja algusaeg (või kaardi sisestamise kuupäev ja algusaeg, kui sündmus sel ajal kestis),
- sündmuse kuupäev ja lõpuaeg (või kaardi väljavõtmise kuupäev ja algusaeg, kui sündmus sel ajal kestis),
- sõiduki, milles sündmus toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.

Märkus: "aja kattumise" sündmuse korral:

- sündmuse kuupäev ja algusaeg peavad vastama kaardi eelmisest sõidukist väljavõtmise kuupäevale ja kellaajale,
- sündmuse kuupäev ja lõpuaeg peavad vastama kaardi praegusesse sõidukisse sisestamise kuupäevale ja kellaajale,
- sõiduki andmed peavad vastama sellele sõidukile, mis sündmuse põhjustas.

Märkus: "viimane kaardiseanss nõuetekohaselt sulgemata"-sündmuse kohta:

- sündmuse kuupäev ja algusaeg peavad vastama nõuetekohaselt sulgemata kaardiseansi kaardi sisestamise kuupäevale ja ajale,
- sündmuse kuupäev ja lõpuaeg peavad vastama kaardiseansi, mille ajal sündmus tuvastati (praegune seanss), kaardi sisestamise kuupäevale ja ajale,
- sõiduki andmed peavad vastama sõidukile, milles seansi ei suletud nõuetekohaselt.

- 206 Juhikaart suudab salvestada andmeid iga sündmusetüübi viimase kuue sündmuse kohta (st 36 sündmust).
- 5.2.8. *Andmed rikete kohta*
- Käesoleva lõigu tähenduses registreeritakse aeg sekundilise täpsusega.
- 207 Juhikaart suudab salvestada järgmised andmed, mis on seotud kaardi sisestamisel sõidumeeriku tuvastatud järgmiste riketega:
- kaardi rike (kui see kaart on sündmuse põhjustaja),
 - sõidumeeriku rike.
- 208 Juhikaart suudab salvestada järgmisi andmeid nende rikete kohta:
- rikke kood,
 - rikke kuupäev ja algusaeg (või kaardi sisestamise kuupäev ja algusaeg, kui rike sel ajal kestis),
 - rikke kuupäev ja lõpuaeg (või kaardi väljavõtmise kuupäev ja algusaeg, kui rike sel ajal kestis),
 - sõiduki, milles rike toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.
- 209 Juhikaart suudab salvestada andmeid iga rikketüübi viimase kaheteistkümne rikke kohta (st 24 riket).
- 5.2.9. *Andmed kontrollitegevuse kohta*
- 210 Juhikaart suudab salvestada järgmisi kontrollitegevustega seotud andmeid:
- kontrolli kuupäev ja kellaeg,
 - kontrollikaardi number ja kaardi väljaandnud liikmesriik,
 - kontrolli tüüp (kuvamine ja/või trükkimine ja/või sõidukiüksuse andmete allalaadimine ja/või kaardi andmete allalaadimine (vt märkus)),
 - allalaadimise korral allalaaditud ajavahemik,
 - sõiduki, milles kontroll toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.
- Märkus: turbenõuetega pärast registreeritakse kaardilt allalaadimine ainult siis, kui see on toimunud sõidumeeriku kaudu.
- 211 Juhikaart mahutab ühe sellise kirje.
- 5.2.10. *Andmed kaardiseansi kohta*
- 212 Juhikaart suudab salvestada sõidukiga seotud andmeid, kus avati praegune seanss:
- seansi avamise (st kaardi sisestamise) kuupäev ja kellaeg sekundilise täpsusega,
 - sõiduki registreerimisnumber ja registreerinud liikmesriik.
- 5.2.11. *Andmed eritingimuste kohta*
- 212a Juhikaart suudab salvestada järgmised andmed, mis on seotud kaardi sisestamisel (mis tahes avasse) sisestatud eritingimustega:
- sisestamise kuupäev ja kellaeg,
 - eritingimuse tüüp.

212b Juhikaart mahutab 56 sellist kirjet.

5.3. Töökojakaart

5.3.1. Turvaelemendid

213 Töökojakaart suudab salvestada isiku tunnusnumbrit (PIN-kood).

214 Töökojakaart suudab salvestada kodeerimisvõtmeid, mis on vajalikud liikumisandurite kokkuühendamiseks sõidukiüksustega.

5.3.2. Kaardi identifitseerimine

215 Töökojakaart suudab salvestada järgmisi kaardi identifitseerimisandmeid:

- kaardi number,
- väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,
- kaardi kehtivusaja algus, kaardi kehtivusaja lõpp.

5.3.3. Kaardi omaniku identifitseerimine

216 Töökojakaart suudab salvestada järgmisi kaardi omaniku identifitseerimisandmeid:

- töökoja nimi,
- töökoja aadress,
- omaniku perekonnanimi,
- omaniku eesnimi (eesnimed),
- eelistatav keel.

5.3.4. Andmed kasutatud sõidukite kohta

217 Töökojakaart suudab salvestada andmeid kasutatud sõidukite kohta samal viisil nagu juhikaart.

218 Töökojakaart suudab salvestada vähemalt 4 sellist kirjet.

5.3.5. Andmed juhi tegevuse kohta

219 Töökojakaart suudab salvestada andmeid juhi tegevuse kohta samal viisil nagu juhikaart.

220 Töökojakaart sisaldab andmeid vähemalt juhi keskmise tegevuse kohta päevas.

5.3.6. Andmed tööpäeva alguse ja/või lõpu kohta

221 Töökojakaart suudab salvestada andmeid tööpäeva alguse ja/või lõpu kohta samal viisil nagu juhikaart.

222 Töökojakaardi mälu mahub vähemalt kolm paari selliseid kirjeid.

5.3.7. Andmed sündmuste ja rikete kohta

223 Töökojakaart suudab salvestada andmeid sündmuste ja rikete kohta samal viisil nagu juhikaart.

224 Töökojakaart suudab salvestada andmeid iga sündmusetüübi viimase kolme sündmuse kohta (st 18 sündmust) ja iga riketüübi viimase kuue rikke kohta (st 12 riket).

5.3.8. Andmed kontrollitegevuse kohta

225 Töökojakaart suudab salvestada kontrollitegevuse andmeid samal viisil nagu juhikaart.

5.3.9. Andmed kalibreerimise ja aja korrigeerimise kohta

- 226 Töökojakaardile mahuvad andmed kalibreerimiste ja/või aja korrigeerimiste kohta, mis on tehtud siis, kui kaart oli sissestatud sõidumeerikusse.
- 227 Iga kalibreerimiskirje peab sisaldama järgmisi andmeid:
- kalibreerimise eesmärk (esimene paigaldamine, paigaldamine, korrapärase ülevaatus),
 - sõiduki identifitseerimine,
 - ajakohastatud või kinnitatud parameetrid (sõiduki iseloomustav koefitsient, sõidumeeriku konstant, rattarehvide efektiivümbermõõt, rehvi suurus, kiiruspiiriku seadistus, läbisõidumõõdik (vana ja uus näit), kuupäev ja kellaeg (vana ja uus näit),
 - sõidumeeriku identifitseerimine (sõidukiüksuse osa number, sõidukiüksuse seerianumber, liikumisanduri seerianumber).
- 228 Töökojakaart suudab salvestada vähemalt 88 sellist kirjet.
- 229 Töökojakaardil on loendur, mis näitab kaardiga tehtud kõigi kalibreerimiste arvu.
- 230 Töökojakaardil on loendur, mis näitab kaardiga tehtud viimase allalaadimise järgset kalibreerimiste arvu.

5.3.10. Andmed eritingimuste kohta

- 230a Töökojakaart suudab salvestada eritingimustega seotud andmeid samal viisil nagu juhikaart. Töökojakaart suudab salvestada kaks sellist kirjet.

5.4. Kontrollikaart

5.4.1. Kaardi identifitseerimine

- 231 Kontrollikaart suudab salvestada järgmisi kaardi identifitseerimisandmeid:
- kaardi number,
 - väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,
 - kaardi kehtivusaja algus, kaardi kehtivusaja lõpp (kui see on olemas).

5.4.2. Kaardi omaniku identifitseerimine

- 232 Kontrollikaart suudab salvestada järgmisi kaardi omaniku identifitseerimisandmeid:
- kontrolliasutuse nimi,
 - kontrolliasutuse aadress,
 - omaniku perekonnanimi,
 - omaniku eesnimi (eesnimed),
 - eelistatav keel.

5.4.3. Andmed kontrollitegevuse kohta

- 233 Kontrollikaart suudab salvestada järgmisi andmeid kontrollitegevuse kohta:
- kontrolli kuupäev ja kellaeg,
 - kontrolli tüüp (kuvamine ja/või trükkimine ja/või sõidukiüksuse andmete allalaadimine ja/või kaardi andmete allalaadimine),

- allalaaditud ajavahemik (kui see on olemas),
- kontrollitud sõiduki registreerimisnumber ja sõiduki registreerinud liikmesriik,
- kontrollitud juhikaardi number ja kaardi väljaandnud liikmesriik.

234 Kontrollikaart suudab salvestada vähemalt 230 sellist kirjet.

5.5. Ettevõttekaart

5.5.1. Kaardi identifitseerimine

235 Ettevõttekaart suudab salvestada järgmisi kaardi identifitseerimisandmeid:

- kaardi number,
- väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,
- kaardi kehtivusaja algus, kaardi kehtivusaja lõpp (kui see on olemas).

5.5.2. Kaardi omaniku identifitseerimine

236 Ettevõttekaart suudab salvestada järgmisi kaardi omaniku identifitseerimisandmeid:

- ettevõtte nimi,
- ettevõtte aadress.

5.5.3. Andmed ettevõtte tegevuse kohta

237 Ettevõttekaart suudab salvestada järgmisi andmeid ettevõtte tegevuse kohta:

- tegevuse kuupäev ja kellaeg,
- tegevuse tüüp (sõidukiüksuse lukustamine ja/või luku avamine ja/või sõidukiüksuse andmete allalaadimine ja/või kaardi andmete allalaadimine),
- allalaaditud ajavahemik (kui see on olemas),
- sõiduki registreerimisnumber ja sõiduki registreerinud liikmesriigi ametiasutus,
- kaardi number ja kaardi väljaandnud liikmesriik (kaardi andmete allalaadimise korral).

238 Ettevõttekaart suudab salvestada vähemalt 230 sellist kirjet.

V. SÕIDUMEERIKU PAIGALDAMINE

1. Paigaldamine

239 Uued sõidumeerikud tarnitakse paigaldajatele või sõidukitootjatele aktiveerimata kujul, kusjuures kõik kalibreerimisparameetrid, nagu need on loetletud III peatüki punktis 20, on häälestatud kohastele ja kehtivatele vaikimisi väärtustele. Kui ükski konkreetne väärtus ei ole kohane, häälestatakse kirjatähelised parameetrid stringile “?” ja numbrilised parameetrid arvule “0”.

240 Enne aktiveerimist võimaldab sõidumeerik kasutada kalibreerimisfunktsiooni isegi siis, kui see ei ole kalibreerimismooduses.

241 Enne aktiveerimist ei registreeri ega salvesta sõidumeerik punktides III.12.3 kuni III.12.9 ja III.12.12 kuni III.12.14 osutatud andmeid.

242 Sõidukitootjad algsätivad paigaldamise ajal kõik teadaolevad parameetrid.

- 243 Sõidukitootjad või paigaldajad aktiveerivad paigaldatud sõidumeeriku enne seda, kui sõiduk viiakse ära tööruumidest, kus paigaldamine toimus.
- 244 Sõidumeeriku aktiveerimine käivitub automaatselt, kui töökojakaart sisestatakse esimest korda ühte kaardiliidestest.
- 245 Konkreetsed kokkuühendamisoperatsioonid, mis on vajalikud liikumisanduri ja sõidukiüksuse vahel, kui need on olemas, toimuvad automaatselt enne aktiveerimist või selle ajal.
- 246 Pärast aktiveerimist on sõidumeeriku funktsioonid ja andmepääsuõigused täielikult kasutatavad.
- 247 Pärast aktiveerimist toimivad täielikult sõidumeeriku registreerimis- ja salvestusfunktsioonid.
- 248 Paigaldamisele järgneb kalibreerimine. Esimene kalibreerimine hõlmab sõiduki registreerimisnumbri sisestamist ja see toimub kahe nädala jooksul kas pärast paigaldamist või sõidukile registreerimisnumbri andmist, olenevalt sellest, kumb toimub hiljem.
- 248a Sõidumeerik peab asuma sõidukis sellises kohas, et juhul oleks oma kohalt juurdepääs vajalikele funktsioonidele.

2. Paigaldustahvel

- 249 Pärast seda, kui sõidumeerikut on paigaldamise ajal kontrollitud, kinnitatakse selle peale, sisse või kõrvale paigaldustahvel, mis on selgelt nähtav ja millele on kerge juurde pääseda. Pärast iga kinnitatud paigaldaja või töökoja läbiviitud kontrollimist tuleb kinnitada eelmise tahvli asemele uus tahvel.
- 250 Tahvlil on vähemalt järgmised üksikasjad:
- kinnitatud paigaldaja või töökoja nimi, aadress või kaubanimi,
 - sõidukit iseloomustav koefitsient kujul "w =... imp/km",
 - sõidumeeriku konstant kujul "k =... imp/km",
 - rattarehvide efektiivüumbermõõt kujul "1 = ... mm",
 - rehvi suurus,
 - kuupäev, millal määrati sõidukit iseloomustav koefitsient ja mõõdeti rattarehvide efektiivüumbermõõtu,
 - sõiduki valmistajatehase tähis.

3. Plommid

- 251 Plommitakse järgmine osa:
- mis tahes ühendus, mis lahtiühendamise korral põhjustaks tuvastamatuid muudatusi või tuvastamatut andmekadu,
 - paigaldustahvel, kui see ei ole kinnitatud nii, et seda ei saa eemaldada sellel olevaid tähiseid kahjustamata.
- 252 Eespool nimetatud plomme võib eemaldada:
- eriolukorras,
 - kiiruspiiriku või mis tahes muu liiklusohutusseadme paigaldamiseks, reguleerimiseks või remontimiseks, eeldusel et sõidumeerik toimib edasi usaldusväärselt ja täpselt ning kui kinnitatud paigaldaja või töökoda (kooskõlas VI peatükiga) paneb pärast kiiruspiiriku või mis tahes muu liiklusohutusseadme paigaldamist uue plommi kohe või muudel juhtudel seitsme päeva jooksul.

- 253 Plommide eemaldamise korral koostatakse alati pädevale asutusele esitamiseks kirjalik avaldus, kus tuuakse ära eemaldamise põhjus.

VI. KONTROLL, ÜLEVAATUS JA REMONT

Nõuded asjaolude kohta, millal plomme võib eemaldada, nagu sellele on viidatud määruse (EMÜ) nr 3821/85 artiklis 12.5, viimati muudetud määrusega (EÜ) nr 2135/98, on määratletud käesoleva lisa V peatüki punktis 3.

1. Paigaldajate ja töökodade kinnitamine

Liikmesriigid kinnitavad, kontrollivad korrapäraselt ja sertifitseerivad asutusi, kes:

- paigaldavad,
- kontrollivad,
- teevad ülevaatusi,
- teevad remonti.

Käesoleva määruse artikli 12 lõike 1 raames antakse töökojakaarte nõuetekohaselt põhjendatud vastuväidete puudumise korral välja ainult neile paigaldajatele ja/või töökodadele, kes on saanud kooskõlas käesoleva lisaga kinnituse sõidumeerikute aktiveerimiseks ja/või kalibreerimiseks ja:

- kes ei ole kõlblikud saama ettevõttele,
- ja kelle muu ametialane tegevus ei ohusta süsteemi üldturvalisust 10. liite kohaselt.

2. Uute või parandatud seadmete kontroll

- 254 Iga uut või parandatud seadet tuleb kontrollida selle nõuetekohase töötamise ning näitude ja salvestuste täpsuse osas III peatüki punktides 2.1 ja 2.2 sätestatud piires ning panna sellele plomm vastavalt V peatüki punktile 3 ja seade kalibreerida.

3. Paigaldamise kontroll

- 255 Sõidukile paigaldamisel peab kogu seadeldis (sealhulgas sõidumeerik) vastama III peatüki punktides 2.1 ja 2.2 sätestatud lubatud hälbe nõuetele.

4. Korrapärane ülevaatus

- 256 Sõidukile paigaldatud meeriku korrapärane ülevaatus toimub pärast seadme iga remonti või pärast sõidukit iseloomustava koefitsiendi või rehvide efektiivümberrõõdu iga muudatust või kui universaalaeg erineb õigest ajast enam kui 20 minutit või kui muutub sõiduki registreerimisnumber ja kord kahe aasta jooksul (24 kuud) pärast viimast ülevaatusi.

- 257 Ülevaatusete käigus tuleb eelkõige kontrollida:

- et sõidumeerik töötab nõuetekohaselt, sealhulgas andmete salvestamine sõidumeerikukaardi funktsioonis,
- et paigaldamisel on tagatud vastavus III peatüki punktides 2.1 ja 2.2 sätestatud lubatud hälbe nõuetele,
- et sõidumeerikul on tüübikinnitusmärk,
- et paigaldustahvel on kinnitatud,
- et plommid seadmel ja muudel seadeldise osadel on terved,
- rehvi suurust ja rehvide tegelikku ümberrõõdu.

258 Ülevaatuse käigus toimub kalibreerimine.

5. Vigade mõõtmine

259 Vigade mõõtmine paigaldamisel ja kasutamise ajal viiakse läbi järgmistel tingimustel, mida tuleb pidada katsetamise standardtingimusteks:

- normaalses sõidukorras koormata sõiduk,
- rehvirõhk vastavalt tootja juhistele,
- rehvi kulumine siseriikliku seadusega lubatud piires,
- sõiduki liikumine:
 - sõiduk liigub oma mootori jõul otse ja tasasel pinnal kiirusega 50 ± 5 km/h. Mõõdetav teepikkus on vähemalt 1 000 m,
- katsetamiseks võib kasutada alternatiivseid meetodeid, näiteks sobivat katsestendi, eeldusel et selle täpsus on võrreldav.

6. Remont

- 260 Töökojad saavad sõidumeerikust andmeid alla laadida, et anda need tagasi kohasele veoettevõttele.
- 261 Kinnitatud töökoda annab veoettevõttele tõendi selle kohta, et andmeid pole võimalik alla laadida, kui sõidumeeriku rike ei lase eelnevalt registreeritud andmeid isegi pärast töökoja tehtud remonti alla laadida. Töökoda hoiab iga väljaantud tõendi koopiat alles vähemalt ühe aasta.

VII. KAARDI VÄLJAANDMINE

Liikmesriikide kehtestatud kaardi väljaandmisprotsess vastab järgmistele nõuetele.

- 262 Taotluse esitanule esmakordselt väljaantud sõidumeerikukaardi numbris on järjestikune indeks (vajaduse korral), asendusindeks ja uuendusindeks, mis on "0".
- 263 Ühele kontrolliasutusele või ühele töökojale või ühele veoettevõttele väljaantud kõigi mittenimeliste sõidumeerikukaartide numbrites on esimesed 13 kohta ühesugused ning kõigil on erinev järjestikune indeks.
- 264 Olemasoleva sõidumeerikukaardi asendamiseks väljaantud sõidumeerikukaardil on asendatud kaardiga sama number, välja arvatud asendusindeks, mis suureneb ühe võrra (järjekorras 0, ..., 9, A, ..., Z).
- 265 Olemasoleva sõidumeerikukaardi asendamiseks väljaantud sõidumeerikukaardi kehtivusaaja lõpp on sama kui asendatud kaardil.
- 266 Olemasoleva sõidumeerikukaardi uuendamiseks väljaantud sõidumeerikukaardil on uuendatud kaardiga sama number, välja arvatud asendusindeks, mis on nullitud, ja uuendusindeks, mis suureneb ühe võrra (järjekorras 0, ..., 9, A, ..., Z).
- 267 Haldusandmete muutmiseks vahetatud sõidumeerikukaardi puhul kohaldatakse uuenduseeskirju, kui see toimub samas liikmesriigis, või esmakordse väljaandmise eeskirju, kui see toimub teises liikmesriigis.
- 268 Mittenimelisel töökoja- või kontrollikaardil märgitakse "kaardi omaniku perekonnanime" kohale töökoja või kontrolliasutuse nimi.

VIII. SÕIDUMEERIKU JA SÕIDUMEERIKUKAARTIDE TÜÜBIKINNITUS

1. Üldosa

Käesolevas peatükis tähendab "sõidumeerik" "sõidumeerikut või selle osi". Liikumisandurit sõidukiüksusega ühendava juhtme (ühendavate juhtmete) puhul tüübi kinnitust ei nõuta. Sõidumeerikus kasutatavat paberit käsitatakse sõidumeeriku osana.

- 269 Sõidumeerik esitatakse tüübikinnituseks koos kõigi integreeritud lisaseadmetega.
- 270 Sõidumeeriku ja sõidumeerikukaartide tüübikinnitus hõlmab turvalisusega seotud katseid, funktsionaalseid katseid ja koostalitlusvõime katseid. Iga katse positiivsed tulemused kinnitatakse kohase tunnistusega.
- 271 Liikmesriikide tüübikinnitusasutused ei anna tüübikinnitustunnistust vastavalt käesoleva määruse artiklile 5, kui neil ei ole:
- turbesertifikaati,
 - funktsionaalsertifikaati,
 - koostalitlusvõime sertifikaati
- sõidumeeriku või sõidumeerikukaardi kohta, mille tüübikinnitust taotletakse.
- 272 Igast muudatusest seadme tark- või riistvaras või nende valmistamiseks kasutatavates materjalides tuleb enne kasutamist teatada asutusele, kes andis seadme tüübikinnituse. Asutus kinnitab tootjale tüübikinnituse laiendamise või võib nõuda asjaomase funktsionaal-, turva- ja/või koostalitlusvõime sertifikaadi ajakohastamist või kinnitust.
- 273 Sõidumeeriku tarkvara kohapealse värskenduse kinnitab asutus, kes andis sõidumeerikule tüübikinnituse. Tarkvara värskendus ei tohi muuta ega kustutada sõidumeeriku mällu salvestatud andmeid juhi tegevuse kohta. Tarkvara tohib värskendada ainult seadme tootja vastutusel.

2. Turbesertifikaat

- 274 Turbesertifikaat antakse käesoleva lisa 10. liite nõuete kohaselt.

3. Funktsionaalsertifikaat

- 275 Iga tüübikinnituse taotleja esitab liikmesriigi tüübikinnitusasutusele kõik materjalid ja dokumendid, mida see asutus peab vajalikuks.
- 276 Tootjale antakse funktsionaalsertifikaat ainult pärast seda, kui vähemalt 9. liites määratletud kõik funktsionaalsed katsed on edukalt läbitud.
- 277 Funktsionaalsertifikaadi annab tüübikinnitusasutus. Sertifikaadil esitatakse lisaks selle saaja nimele ja mudeli identimiseandmetele üksikasjalik nimekiri sooritatud katsetest ja saadud tulemustest.

4. Koostalitlusvõime sertifikaat

- 278 Koostalitlusvõime katseid teeb üks labor Euroopa Komisjoni järelevalve all ja vastutusel.
- 279 Labor registreerib tootjate esitatud koostalitlusvõime katsete taotlused nende saabumise järjekorras.
- 280 Taotlused registreeritakse ametlikult ainult siis, kui laboril on:
- kõik koostalitlusvõime katseteks vajalikud materjalid ja dokumendid,
 - vastav turbesertifikaat,
 - vastav funktsionaalsertifikaat.
- Tootjale teatatakse taotluse registreerimiskuupäev.
- 281 Sõidumeeriku või sõidumeerikukaardi, millele ei ole antud turbesertifikaati ja funktsionaalsertifikaati, koostalitlusvõime katseid labor ei tee.
- 282 Iga tootja, kes taotleb koostalitlusvõime katsete tegemist, on kohustatud jätma katsete eest vastutavale laborile kõik tema poolt katsete tegemiseks esitatud materjalid ja dokumendid.

Koostalitlusvõime katsed tehakse vastavalt käesoleva lisa 9. liite lõikele 5 kõigi sõidumeeriku või sõidumeerikukaartide tüüpidega:

- mille tüübikinnitus on veel kehtiv või
- mille tüüp on kinnitamisel ja millel on kehtiv koostalitlusvõime sertifikaat.

- 284 Labor annab koostalitlusvõime sertifikaadi tootjale ainult pärast seda, kui kõik koostalitlusvõime katsed on edukalt sooritatud.
- 285 Kui koostalitlusvõime katsed ei ole ühe või mitme sõidumeeriku või sõidumeerikukaardi (sõidumeerikukaartide) puhul edukad, nagu seda nõutakse nõudes 283, siis koostalitlusvõime sertifikaati ei anta, kuni taotluse esitanud tootja on teinud vajalikud muudatused ja koostalitlusvõime katsed on edukalt läbitud. Labor teeb probleemi põhjuse kindlaks koostalitlusvõime rikkega seotud tootja abil ning püüab aidata taotluse esitanud tootjal leida tehniline lahendus. Kui tootja on oma toodet muutnud, on tootja ülesanne saada asjaomastelt asutustelt kinnitus, et turbesertifikaat ja funktsionaalsertifikaat veel kehtivad.
- 286 Koostalitlusvõime sertifikaat kehtib kuus kuud. Selle aja möödumisel see tühistatakse, kui tootja ei ole saanud vastavat tüübikinnitustunnistust. Tootja edastab selle liikmesriigi tüübikinnitusasutusele, kes on andnud funktsionaalsertifikaadi.
- 287 Mis tahes osa, mis võiks olla koostalitlusvõime rikke põhjuseks, ei kasutata kasumi teenimiseks ega turgu valitseva seisundi saamiseks.

5. Tüübikinnitustunnistus

- 288 Liikmesriigi tüübikinnitusasutus võib anda tüübikinnitustunnistuse kohe, kui ta on saanud kolm nõutavat sertifikaati.
- 289 Tüübikinnitusasutus saadab tüübikinnitustunnistuse koopia koostalitlusvõime katsete eest vastutavale laborile samal ajal, kui ta annab selle tootjale.
- 290 Koostalitlusvõime katsete tegemise pädeval laboril on avalik veebilehekülg, millel on ajakohastatud nimekiri sõidumeerikutest ja sõidumeerikukaartidest:
- mille kohta on registreeritud taotlus koostalitlusvõime katsete tegemiseks,
 - millele on antud koostalitlusvõime sertifikaat (ka esialgne),
 - millele on antud tüübikinnitustunnistus.

6. Erandkord: esimese koostalitlusvõime sertifikaadi andmine

- 291 Kuni nelja kuu jooksul pärast esimeste sõidumeerikute ja sõidumeerikukaartide (juhi-, töökoja-, kontrolli- ja ettevõttele kaardid) tunnistamist koostalitlusvõimelisteks loetakse sellel ajavahemikul registreeritud taotlustele antud koostalitlusvõime sertifikaati ajutiseks (kaasa arvatud kõige esimene).
- 292 Kui selle aja lõpuks on kõik asjaomased tooted tunnistatud omavahel koostalitlusvõimelisteks, muutuvad vastavad koostalitlusvõime sertifikaadid lõplikeks.
- 293 Kui selle aja jooksul leitakse koostalitlusvõime rikkeid, teeb koostalitlusvõime katsete eest vastutav labor kindlaks probleemide põhjused kõigi seotud tootjate abil ning soovib neil teha vajalikud muudatused.
- 294 Kui selle aja lõpuks esineb veel koostalitlusvõime probleeme, teeb koostalitlusvõime katsete eest vastutav labor koostöös kõigi seotud tootjate ja vastavad funktsionaalsertifikaadid andnud tüübikinnitusasutustega kindlaks koostalitlusvõime rikete põhjused ning määrab, milliseid muudatusi peaks iga asjaomane tootja tegema. Tehniliste lahenduse otsimine võib kesta maksimaalselt kaks kuud, kui pärast seda ei ole ühist lahendust leitud, otsustab komisjon, olles konsulteerinud koostalitlusvõime katsete eest vastutava laboriga, milline seade (millised seadmed) ja kaardid saavad lõpliku koostalitlusvõime sertifikaadi, ja esitab oma põhjendused.
- 295 Kõik koostalitlusvõime katsete taotlused, mis labor on registreerinud esimese ajutise koostalitlusvõime sertifikaadi andmise järgse nelja kuu möödumise ja nõudes 294 osutatud komisjoni otsuse tegemise kuupäeva vahelisel ajal, lükatakse edasi esialgsete koostalitlusvõimeprobleemide lahendamiseni. Seejärel töödeldakse neid taotlusi nende registreerimise järjekorras.

1. liide

ANDMESÖNASTIK

SISUKORD

1.	Sissejuhatus	332
1.1.	Andmetüüpide määratlusviis	332
1.2.	Viited	332
2.	Andmetüüpide määratlused	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.	VuCardIWRecord	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.	Väärtus- ja suurusulatus määratlused	374
3.1.	Juhikaardi määratlused	374
3.2.	Töökojakaardi määratlused	374
3.3.	Kontrollikaardi määratlused	374
3.4.	Ettevõttekaardi määratlused	374
4.	Märgistikud	374
5.	Kodeerimine	374

1. SISSEJUHATUS

Käesolevas liites määratletakse sõidumeerikus ja sõidumeerikukaartides kasutatavad andmevormingud, andmeelemendid ja andmestruktuurid.

1.1. Andmetüüpide määratlusviis

Käesolevas liites kasutatakse andmetüüpide määratlemiseks abstraktset süntaksi esitust 1 (ASN.1). See võimaldab määratleda liht- ja struktureeritud andmeid, kasutamata mis tahes spetsiifilist edastussüntaksi (kodeerimiseeskirjad), mis oleks sõltuv rakendusest ja keskkonnast.

ASN.1 tüübinimetused on tehtud vastavalt standardile ISO/IEC 8824-1. See tähendab, et:

- võimaluse korral viitab andmetüübile valitud nimi selle tähendusele,
- kui andmetüüp koosneb teistest andmetüüpidest, on andmetüübi nimi siiski suurtähega algav alfabeetilisest tähemärkidest koosnev ühtne jada, olenemata sellest, kuidas kasutatakse nimes suurtähti vastava tähenduse edasiandmiseks,
- üldiselt on andmetüüpide nimed seotud andmetüüpide nimedega, millest need on moodustatud, seadmetega, kuhu andmed on salvestatud, ja andmetega seotud funktsioonidega.

Kui ASN.1 tüüp on juba määratletud teise standardi osana ja kui see on asjakohane sõidumeerikus kasutamiseks, määratletakse see ASN.1 tüüp käesolevas liites.

Võimaldamaks erinevat tüüpi kodeerimiseeskirjade kasutamist, on mõned ASN.1 tüübid käesolevas liites piiratud väärtusulatusse identifikaatoritega. Väärtusulatusse identifikaatorid on määratletud lõikes 3.

1.2. Viited

Käesolevas liites kasutatakse järgmisi viiteid:

- | | |
|----------------|---|
| ISO 639 | Code for the representation of names of languages. First Edition: 1988. (Keelenimede kood, esimene väljaanne, 1988.) |
| EN 726-3 | Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994. (Identimiskaartide süsteemid — Telekommunikatsiooni kiipkaardid ja terminalid — 3. osa: Rakendusest sõltumatud kaardinõuded, detsember 1994.) |
| ISO 3779 | Road vehicles — Vehicle identification number (VIN) — Content and structure. Edition 3: 1983. (Maanteeesõidukid — Valmistajatehase tähis (VIN) — Sisu ja struktuur, 3. väljaanne, 1983.) |
| ISO/IEC 7816-5 | Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers. First edition: 1994 + Amendment 1: 1996. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 5. osa: Rakendusidentifikaatorite numereerimissüsteem ja registreerimiskord, esimene väljaanne, 1994 + 1. muudatus, 1996.) |
| ISO/IEC 8824-1 | Information technology — Abstract Syntax Notation 1 (ASN.1): Specification of basic notation. Edition 2: 1998. (Infotehnoloogia — Abstraktne süntaksi esitus 1 (ASN.1): Baasesituse spetsifikaat, 2. väljaanne, 1998.) |
| ISO/IEC 8825-2 | Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). Edition 2: 1998. (Infotehnoloogia — ASN.1 kodeerimisreeglid: Pakitud kodeerimisreeglite (PER) spetsifikaat, 2. väljaanne, 1998.) |
| ISO/IEC 8859-1 | Information technology — 8 bit single-byte coded graphic character sets — Part 1: Latin alphabet No 1. First edition: 1998. (Infotehnoloogia — 8bitilised ühebaidilised kodeeritud graafilised märgistikud — 1. osa: Ladina tähestik nr 1, esimene väljaanne, 1998.) |
| ISO/IEC 8859-7 | Information technology — 8 bit single-byte coded graphic character sets — Part 7: Latin/Greek alphabet. First edition: 1987. (Infotehnoloogia — 8bitilised ühebaidilised kodeeritud graafilised märgistikud — 7. osa: Ladina/kreeka tähestik, esimene väljaanne, 1987.) |
| ISO 16844-3 | Road vehicles — Tachograph systems — Motion Sensor Interface. WD 3-20/05/99. (Maanteeesõidukid — Sõidumeerikusüsteemid — Liikumisanduri liides.) |

'aa'B Tegevus (ei ole asjakohane, kui $p = 1$ ja $c = 0$, välja arvatud allpool oleva märkuse korral):

'00'B: VAHEAEG/PUHKUS,

'01'B: VALMISOLEK,

'10'B: TÖÖ,

'11'B: JUHTIMINE,

'tttttttttt'B Muutuse aeg: minutite arv alates kell 00.00 sellel päeval.

Märkus "kaardi väljavõtmise" korral:

Kui kaart võetakse välja:

- 's' on asjakohane ja näitab ava, millest kaart välja võeti,
- 'c' peab olema 0,
- 'p' peab olema 1,
- 'aa' peab vastama sel ajal valitud hetketegevusele.

Käsitsi tehtud sissekande tulemusel võib (kaardile salvestatud) bitid 'c' ja 'aa' sissekande kajastamiseks hiljem üle kirjutada.

2.2. Address

Aadress.

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

codePage määratleb ISO/IEC 8859 osa, mida on aadressi kodeerimiseks kasutatud,

address on ISO/IEC 8859-codePage koodilehekülje kohaselt kodeeritud aadress.

2.3. BCDString

Andmetüüpi BCDString kasutatakse kahendkodeeritud kümnendesituses (BCD). Seda andmetüüpi kasutatakse ühe kümnendkoha esitamiseks ühes pooloktetis (4 bitti). BCDString aluseks on ISO/IEC 8824-1 "CharacterStringType".

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

BCDString kasutab "hstring"-esitust. Vasakpoolseim kuueteistkümnendesituse number on esimese okteti kõige tähtsam pooloktet. Täiskordsete oktettide saamiseks sisestatakse vajaduse korral alates esimese okteti kõige vasakpoolsema poolokteti asukohast 0-väärtusega sabapooloktetid.

Lubatud numbrid on: 0, 1, ... 9.

2.4. CalibrationPurpose

Kood, mis seletab, miks registreeriti kalibreerimisparameetrite kogum. See andmetüüp on seotud nõuetega 097 ja 098.

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

Väärtuse omistus:

'00'H reserveeritud väärtus,

'01'H aktiveerimine: sõidukiüksuse aktiveerimishetkel teadaolevate kalibreerimisparameetrite registreerimine,

'02'H esimene paigaldus: sõidukiüksuse esimene kalibreerimine pärast selle aktiveerimist,

'03'H paigaldus: sõidukiüksuse esimene kalibreerimine praeguses sõidukis,

'04'H korrapärane ülevaatus.

2.5. CardActivityDailyRecord

Kaardile salvestatud teave, mis on seotud juhi tegevustega konkreetsel kalendripäeval. See andmetüüp on seotud nõuetega 199 ja 219.

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

activityPreviousRecordLength on eelmise päeva andmete kogupikkus baitides. Maksimumväärtuse määrab neid andmeid sisaldava OCTET STRING'i pikkus (vt CardActivityLengthRange lõikes 3). Kui see kirje on vanim kirje päeva kohta, peab activityPreviousRecordLength'i väärtus olema null.

activityRecordLength on selle kirje kogupikkus baitides. Maksimumväärtuse määrab ära neid andmeid sisaldava OCTET STRING'i pikkus.

activityRecordDate on kirje kuupäev.

activityDailyPresenceCounter on kaardi kasutuskordade lugeja sellel päeval.

activityDayDistance on kogu läbitud teepikkus sellel päeval.

activityChangeInfo on juhi ActivityChangeInfo andmete kogum sellel päeval. See võib sisaldada maksimaalselt 1 440 väärtust (üks tegevusmuutus minutis). Selles kogumis on alati activityChangeInfo väärtus, mis näitab juhtimisstaatust kell 00.00.

2.6. CardActivityLengthRange

Juhi- või töökojakaardil olevate baitide arv, mida saab kasutada kirjete salvestamiseks juhi tegevuse kohta.

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

Väärtuse omistus: vt lõige 3.

2.7. CardApprovalNumber

Kaardi tüübikinnituse number:

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

Väärtuse omistus: määratlemata.

2.8. CardCertificate

Kaardi avaliku võtme sertifikaat.

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

2.9. CardChipIdentification

Kaardile salvestatud teave, mis on seotud kaardi kiibi identimisega (nõue 191).

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


activityPointerOldestDayRecord on stringi activityDailyRecords vanima tervikliku päeva andmete salvestuse alguskoha spetsifikaat (baitide arv stringi algusest). Maksimumväärtus antakse stringi pikkusena.

activityPointerNewestRecord on stringi activityDailyRecords viimase päeva andmete salvestuse alguskoha spetsifikaat (baitide arv stringi algusest). Maksimumväärtus antakse stringi pikkusena.

activityDailyRecords on juhi tegevuse kohta andmete säilitamiseks olemasolev ruum (andmestruktuur: CardActivity-DailyRecord) iga kalendripäeva tarvis, mil kaarti on kasutatud.

Väärtuse omistus: see oktetistring täidetakse tsükliliselt CardActivityDailyRecord'i kirjetega. Esimesel kasutamisel alustatakse salvestamist stringi esimesse baiti. Kõik uued kirjed liidetakse eelmise lõppu. Kui string saab täis, jätkub salvestamine stringi esimesse baiti sõltumaltult andmeelemendis olevast katkestusest. Enne uue tegevuse andmete sisestamist stringi (laiendades olemasolevat activityDailyRecord'i või võttes uue activityDailyRecord'i), mis asendab andmed vanemate tegevuste kohta, tuleb activityPointerOldestDayRecord ajakohastada, et see kajastaks vanima täieliku päeva kirje uut asukohta, ning selle (uue) vanima täieliku päeva kirje activityPreviousRecordLength näit tuleb nullida.

2.14. CardDrivingLicenceInformation

Juhikaardile salvestatud teave, mis on seotud andmetega kaardi omaniku juhiloa kohta (nõue 196).

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

drivingLicenceIssuingAuthority on juhiloa väljaandmise eest vastutav asutus.

drivingLicenceIssuingNation on juhiloa väljandnud asutuse riikkondsus.

drivingLicenceNumber on juhiloa number.

2.15. CardEventData

Juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omanikuga seotud sündmustega (nõuded 204 ja 223).

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

CardEventData on cardEventRecords'i jada EventFaultType'i väärtuse kasvavas järjestuses (välja arvatud kirjed, mis on seotud turbemurdekatssetega, mis kogutakse kokku jada viimasesse kogumisse).

cardEventRecords on konkreetse sündmuse tüübi (või sündmuse kategooria, mis on seotud turbemurdekatssetega) sündmusekirjete kogum.

2.16. CardEventRecord

Juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omanikuga seotud sündmusega (nõuded 205 ja 223).

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

eventType on sündmuse tüüp.

eventBeginTime on sündmuse alguse kuupäev ja kellaeg.

eventEndTime on sündmuse lõpu kuupäev ja kellaeg.

eventVehicleRegistration on sõiduki, milles sündmus toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.

2.17. CardFaultData

Juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omanikuga seotud riketega (nõuded 207 ja 223).

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

CardFaultData on jada sõidumeeriku rikkekirjete kogumist, millele järgneb kaardi rikkekirjete kogum.

cardFaultRecords on rikkekategooria (sõidumeerik või kaart) rikkekirjete kogum.

2.18. CardFaultRecord

Juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omanikuga seotud rikkega (nõuded 208 ja 223).

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

faultType on rikketüüp.

faultBeginTime on rikke alguse kuupäev ja kellaeg.

faultEndTime on rikke lõpu kuupäev ja kellaeg.

faultVehicleRegistration on sõiduki, milles rike toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.

2.19. CardIccIdentification

Kaardile salvestatud teave, mis on seotud kiipkaardi identimisega (nõue 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 on moodus clockStop vastavalt standardile EN 726-3.

cardExtendedSerialNumber on kiipkaardi seerianumber ja kiipkaardi tootjaviide vastavalt standardile EN 726-3, need on kindlaks määratud andmetüübiga ExtendedSerialNumber.

cardApprovalNumber on kaardi tüübikinnituse number.

cardPersonaliserID on kaardi tuvastusandmed vastavalt standardile EN 726-3.

embedderIcAssemblerId on paigaldaja/kiibi koostaja identifikaator vastavalt standardile EN 726-3.

icIdentifier on kaardil oleva kiibi ja kiibi tootja identifikaator vastavalt standardile EN 726-3.

2.20. CardIdentification

Kaardile salvestatud teave, mis on seotud kaardi identimisega (nõuded 194, 215, 231, 235).

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

cardIssuingMemberState on kaardi väljaandnud liikmesriigi kood.

cardNumber on kaardi kaardinumber.

cardIssuingAuthorityName on kaardi väljaandnud asutuse nimi.

cardIssueDate on kaardi praegusele omanikule väljaandmise kuupäev.

cardValidityBegin on kaardi kehtivuse esimene kuupäev.

cardExpiryDate on kaardi kehtivuse viimane kuupäev.

2.21. CardNumber

Kaardi number on määratletud mõistes g.

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

driverIdentification on juhi unikaalne identifitseerimine liikmesriigis.

ownerIdentification on ettevõtte või töökoja või kontrolliasutuse unikaalne identifitseerimine liikmesriigis.

cardConsecutiveIndex on kaardi järjestikune indeks.

cardReplacementIndex on kaardi asendusindeks.

cardRenewalIndex on kaardi uuendusindeks.

Valiku esimene jada sobib juhikaardi numbri kodeerimiseks, valiku teine jada sobib töökoja-, kontroll- ja ettevõttekaardi numbrite kodeerimiseks.

2.22. CardPlaceDailyWorkPeriod

Juhi- või töökojakaardile salvestatud teave, mis on seotud tööpäeva algus- ja/või lõpukohtadega (nõuded 202 ja 221).

```

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

```

placePointerNewestRecord on viimase ajakohastatud kohakirje indeks.

Väärtuse omistus: number, mis vastab kohakirjete lugejale, alates nullist kohakirje esimesel esinemisel struktuuris.

placeRecords on kirjete kogum, mis sisaldab teavet sisestatud kohtade kohta.

2.23. CardPrivateKey

Kaardi isiklik võti.

```
CardPrivateKey ::= RSAKeyPrivateExponent.
```

2.24. CardPublicKey

Kaardi avalik võti.

```
CardPublicKey ::= PublicKey.
```

2.25. CardRenewalIndex

Kaardi uuendusindeks (mõiste i).

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

Väärtuse omistus: (vt käesoleva lisa VII peatükk).

'0' Esimene väljaanne.

Kasvamise järjekord: '0, ..., 9, A, ..., Z'.

2.26. CardReplacementIndex

Kaardi asendusindeks (mõiste j).

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

Väärtuse omistus: (vt käesoleva lisa VII peatükk).

'0' Originaalkaart.

Kasvamise järjekord: '0, ..., 9, A, ..., Z'.

2.27. CardSlotNumber

Sõidukiüksuse kahe ava eristuskood.

```

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

```

Väärtuse omistus: täpsustamata.

2.28. CardSlotsStatus

Kood, mis näitab sõidukiüksuse kahte avasse sisestatud kaartide tüüpi.

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

Väärtuse omistus — okteti joondus: 'ccccddd'B:

'cccc'B Kaasjuhi kaardi avasse sisestatud kaarditiübi identifitseerimine,

'ddd'B Juhikaardi avasse sisestatud kaarditiübi identifitseerimine

järgmiste identifitseerimiskoodidega:

'0000'B kaarti ei ole sisestatud,

'0001'B sisestatud on juhikaart,

'0010'B sisestatud on töökojakaart,

'0011'B sisestatud on kontrollikaart,

'0100'B sisestatud on ettevõttelekaart.

2.29. CardStructureVersion

Kood, mis näitab sõidumeerikukaardi rakendusstruktuuri versiooni.

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

Väärtuse omistus: 'aabb'H:

'aa'H Struktuurimuutuste indeks,

'bb'H Muutuste indeks seoses andmeelementide kasutamisega, mis on antud struktuuri tarvis määratletud kõige tähtsama baidiga.

2.30. CardVehicleRecord

Juhi- või töökojakaardile salvestatud teave, mis on seotud sõiduki kasutusajaga kalendripäevas (nõuded 197 ja 217).

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

vehicleOdometerBegin on sõiduki läbisõidumõõdiku näit sõiduki kasutusaja alguses.

vehicleOdometerEnd on sõiduki läbisõidumõõdiku näit sõiduki kasutusaja lõpus.

vehicleFirstUse on sõiduki kasutusaja alguse kuupäev ja kellaaeg.

vehicleLastUse on sõiduki kasutusaja lõpu kuupäev ja kellaaeg.

vehicleRegistration on sõiduki registreerimisnumber ja sõiduki registreerinud liikmesriik.

vuDataBlockCounter on lugeja vuDataBlockCounter'i väärtus sõiduki kasutusaja viimasel väljavõttel.

2.31. CardVehiclesUsed

Juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omaniku kasutatud sõidukitega (nõuded 197 ja 217).

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

vehiclePointerNewestRecord on viimase ajakohastatud sõidukikirje indeks.

Väärtuse omistus: number, mis vastab sõidukikirjete lugejale, alates nullist sõidukikirje esimesel esinemisel struktuuris.

cardVehicleRecords on kirjete kogum, mis sisaldab teavet kasutatud sõidukite kohta.

2.32. Certificate

Sertifikaat on sertifitseerimisasutuse väljaantud avalik võti.

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

Väärtuse omistus: digitaalalkiri koos andmete CertificateContent osalise taaskasutamisega vastavalt 11. liitele "Ühised turbemehhanismid": allkiri (128 baiti) || avaliku võtme jääk (58 baiti) || sertifitseerimisasutuse viide (8 baiti).

2.33. CertificateContent

Avaliku võtme sertifikaadi (avateksti) sisu vastavalt 11. liitele "Ühised turbemehhanismid".

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

certificateProfileIdentifier on vastava sertifikaadi versioon.

Väärtuse omistus: '01h' selle versiooni puhul.

CertificationAuthorityReference idendib sertifikaadi väljaandnud asutuse. See viitab ka selle sertifitseerimisasutuse avalikule võtmele.

certificateHolderAuthorisation idendib sertifikaadi omaniku õigused.

certificateEndOfValidity on kuupäev, mil sertifikaadi halduskehtivus lõpeb.

certificateHolderReference idendib kaardi omaniku. Viitab ka ta avalikule võtmele.

publicKey on selle sertifikaadiga tõendatud avalik võti.

2.34. CertificateHolderAuthorisation

Sertifikaadi omaniku õiguste identimine.

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

tachographApplicationID on sõidumeerikurakenduse rakendusidentifikaator.

Väärtuse omistus: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. See rakendusidentifikaator (AID) on valmistajaspetsiifiline registreerimata rakendusidentifikaator vastavalt standardile ISO/IEC 7816-5.

equipmentType on seadmetüübi identifikatsioon, mille jaoks sertifikaat on mõeldud.

Väärtuse omistus: vastavalt andmetüübile EquipmentType. 0, kui tegemist on liikmesriigi sertifikaadiga.

2.35. CertificateRequestID

Sertifitseerimistaotluse unikaalne identifikaatsioon. Seda saab kasutada ka sõidukiüksuse avaliku võtme identifikaatorina, kui sõidukiüksuse, mille jaoks võti on mõeldud, seerianumber ei ole sertifikaadi loomise ajal teada.

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

requestSerialNumber on sertifitseerimistaotluse seerianumber, mis on kordumatu allpool esitatud tootja ja kuu tarvis.

requestMonthYear on sertifitseerimistaotluse kuu ja aasta identifikaatsioon.

Väärtuse omistus: binaarkodeeritud kümnendesituses kuu (kaks arvu) ja aasta (kaks viimast arvu).

crIdentifier: laiendatud seerianumbrilt pärineva sertifitseerimistaotluse eristamisidentifikaator.

Väärtuse omistus: 'FFh'.

manufacturerCode: sertifikaati taotleva tootja numbrikood.

2.36. CertificationAuthorityKID

Sertifitseerimisasutuse (liikmesriigi või Euroopa sertifitseerimisasutuse) avaliku võtme identifikaator.

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

nationNumeric on sertifitseerimisasutuse numbrikood.

nationAlpha on sertifitseerimisasutuse tähtnumbriline kood.

keySerialNumber on sertifitseerimisasutuse erinevate võtmete tarvis järjekorranumber, juhul kui võtmeid muudetakse.

additionalInfo on kahebaidiline väli lisakoodi tarvis (puudutab sertifitseerimisasutust).

caIdentifier on identifikaator, eristamaks sertifitseerimisasutuse võtme identifikaatorit muudest võtmeidentifikaatoritest.

Väärtuse omistus: '01h'.

2.37. CompanyActivityData

Ettevõttele salvestatud teave, mis on seotud kaardiga tehtud tegevustega (nõue 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 on viimase ajakohastatud kirje `companyActivityRecord` indeks.

Väärtuse omistus: number, mis vastab ettevõtte tegevuskirjete lugejale, alates nullist ettevõtte tegevuskirje esimesel esinemisel struktuuris.

companyActivityRecords on kõigi ettevõtte tegevuskirjete kogum.

companyActivityRecord on ühe ettevõtte tegevusega seotud teabe jada.

companyActivityType on ettevõtte tegevustüüp.

companyActivityTime on ettevõtte tegevuse kuupäev ja kellaaeg.

cardNumberInformation on vajaduse korral allalaaditud kaardi number ja kaardi väljaandnud liikmesriik.

vehicleRegistrationInformation on sõiduki, milles toimus andmete allalaadimine või lukustamine või luku avamine, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.

downloadPeriodBegin ja **downloadPeriodEnd** on vajaduse korral sõidukiüksusest andmete allalaadimise ajavahemik.

2.38. CompanyActivityType

Kood, mis näitab ettevõtte tegevust ettevõttekaardi kasutamisel.

```

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

```

2.39. CompanyCardApplicationIdentification

Ettevõttekaardile salvestatud teave, mis on seotud kaardirakenduse identifitseerimisega (nõue 190).

```

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

```

typeOfTachographCardId määratleb rakendatud kaardi tüübi.

cardStructureVersion määratleb kaardi rakendusstruktuuri versiooni.

noOfCompanyActivityRecords on arv, mitu ettevõtte tegevuskirjet on võimalik kaardile salvestada.

2.40. CompanyCardHolderIdentification

Ettevõttekaardile salvestatud teave, mis on seotud kaardi omaniku identifitseerimisega (nõue 236).

```

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

```

companyName on kaarti omava ettevõtte nimi.

companyAddress on kaarti omava ettevõtte aadress.

cardHolderPreferredLanguage on kaardi omaniku eelistatud keel.

2.41. ControlCardApplicationIdentification

Kontrollikaardile salvestatud teave, mis on seotud kaardirakenduse identifitseerimisega (nõue 190).

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

typeOfTachographCardId määratleb rakendatud kaardi tüübi.

cardStructureVersion määratleb kaardi rakendusstruktuuri versiooni.

noOfControlActivityRecords on arv, mitu kontrollitegevuse kirjet on võimalik kaardile salvestada.

2.42. ControlCardControlActivityData

Kontrollikaardile salvestatud teave, mis on seotud kaardiga tehtud kontrollitegevustega (nõue 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 on viimase ajakohastatud kontrollikirje indeks.

Väärtuse omistus: number, mis vastab kontrollitegevuse kirjade lugejale, alates nullist kontrollitegevuse kirje esimesel esinemisel struktuuris.

controlActivityRecords on kõigi kontrollitegevuse kirjade kogum.

controlActivityRecord on ühe kontrolliga seotud teabe jada.

controlType on kontrollitüüp.

controlTime on kontrolli kuupäev ja kellaaeg.

controlledCardNumber on kontrollitud kaardi number ja kaardi väljaandnud liikmesriik.

controlledVehicleRegistration on sõiduki, milles kontroll toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.

controlDownloadPeriodBegin ja **controlDownloadPeriodEnd** on tegelikult allalaaditud ajavahemik.

2.43. ControlCardHolderIdentification

Kontrollikaardile salvestatud teave, mis on seotud kaardi omaniku identifitseerimisega (nõue 232).

```

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

```

controlBodyName on kontrolliasutuse nimi, kuhu kaardi omanik kuulub.

controlBodyAddress on kontrolliasutuse aadress, kuhu kaardi omanik kuulub.

cardHolderName on kontrollikaardi omaniku perekonnanimi ja eesnimi (eesnimed).

cardHolderPreferredLanguage on kaardi omaniku eelistatud keel.

2.44. ControlType

Kontrolli käigus läbiviidud tegevuste kood. See andmetüüp on seotud nõuetega 102, 210 ja 225.

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

Väärtuse omistus — okteti joondus: 'c'v'p'd'xxxx'B(8 bitti)

'c'B kaardilt allalaadimine:
 '0'B: selle kontrollitegevuse käigus ei ole kaardilt alla laaditud,
 '1'B: selle kontrollitegevuse käigus on kaardilt alla laaditud

'v'B sõidukiüksusest allalaadimine:
 '0'B: selle kontrollitegevuse käigus ei ole sõidukiüksusest alla laaditud,
 '1'B: selle kontrollitegevuse käigus on sõidukiüksusest alla laaditud

'p'B trükkimine:
 '0'B: selle kontrollitegevuse käigus ei ole trükitud,
 '1'B: selle kontrollitegevuse käigus on trükitud

'd'B kuvar:
 '0'B: selle kontrollitegevuse käigus ei ole kuvarit kasutatud,
 '1'B: selle kontrollitegevuse käigus on kuvarit kasutatud

'xxxx'B Ei ole kasutatud.

2.45. CurrentDateTime

Sõidumeeriku käesolev kuupäev ja kellaeg.

```
CurrentDateTime ::= TimeReal
```

Väärtuse omistus: täpsustamata.

2.46. DailyPresenceCounter

Juhi- või töökojakaardile salvestatud loendur, mis suureneb ühe võrra igal kalendripäeval, millal kaart on sõidukiüksusse sisestatud. See andmetüüp on seotud nõuetega 199 ja 219.

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

Väärtuse omistus: järjestikune number suurima väärtusega 9 999, algab uuesti nullist. Kaardi esmakordse väljaandmise ajal määratakse number nullina.

2.47. Datef

Kergesti trükitav numbriformaadis väljendatud kuupäev.

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

Väärtuse omistus:

```
YYYY      Aasta
mm        Kuu
dd        Päev
```

'00000000'H väljendab üheselt kuupäeva puudumist.

2.48. Distance

Läbitud teepikkus (sõiduki läbisõidumõõdiku kahe näidu vahe kilomeetrites)

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

Väärtuse omistus: kindlaks määramata kahendarv. Väärtus kilomeetrites toimeulatuses 0 kuni 9 999 km.

2.49. DriverCardApplicationIdentification

Juhikaardile salvestatud teave, mis on seotud kaardirakenduse identifikatsiooniga (nõue 190).

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

typeOfTachographCardId määratleb rakendatud kaardi tüübi.

cardStructureVersion määratleb kaardi rakendusstruktuuri versiooni.

noOfEventsPerType on sündmusetüübi kaupa sündmuste arv, mida on võimalik kaardile salvestada.

noOfFaultsPerType on rikketüübi kaupa rikete arv, mida on võimalik kaardile salvestada.

activityStructureLength näitab baitide arvu, mida on võimalik tegevuskirjete salvestamiseks kasutada.

noOfCardVehicleRecords on arv, mitu sõidukikirjet kaart mahutab.

noOfCardPlaceRecords on arv, mitu kohakirjet suudab kaart registreerida.

2.50. DriverCardHolderIdentification

Juhikaardile salvestatud teave, mis on seotud kaardi omaniku identifikatsiooniga (nõue 195).

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

cardHolderName on juhikaardi omaniku perekonnanimi ja eesnimi (eesnimed).

cardHolderBirthDate on juhikaardi omaniku sünniaeg.

cardHolderPreferredLanguage on kaardi omaniku eelistatud keel.

2.51. EntryTypeDailyWorkPeriod

Kood tööpäeva kohakirje alguse ja lõpu eristamiseks ja kirjetingimus.

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

}

Väärtuse omistus: vastavalt standardile ISO/IEC8824-1.

2.52. EquipmentType

Kood sõidumeerikurakenduse erinevate sõidumeerikutüüpide eristamiseks.

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

Väärtuse omistus: vastavalt standardile ISO/IEC 8824-1.

Väärtus 0 on jäetud selleks, et määrata sertifikaadi CHA-väljal liikmesriik või Euroopa.

2.53. EuropeanPublicKey

Euroopa avalik võti.

```
EuropeanPublicKey ::= PublicKey.
```

2.54. EventFaultType

Sündmust või riket täpsustav kood.

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

Väärtuse omistus:

'0x'H	Üldsündmused,
'00'H	Üksikasjad puuduvad
'01'H	Kehtetu kaardi sisestamine,
'02'H	Kaardikonflikt,
'03'H	Aja kattumine,
'04'H	Vajaliku kaardita juhtimine,
'05'H	Kaardi sisestamine juhtimise ajal,
'06'H	Viimane kaardiseanss nõuetekohaselt sulgemata,
'07'H	Kiiruse ületamine,

'08'H	Toiteallika katkestus,
'09'H	Liikumisandmete viga,
'0A'H kuni '0F'H	RFU (reserveeritud kasutuseks tulevikus),
'1x'H	Sõidukiüksusega seotud turbemurdekate sündmused,
'10'H	Üksikasjad puuduvad,
'11'H	Liikumisanduri autentimisriike,
'12'H	Sõidumeerikukaardi autentimisriike,
'13'H	Liikumisanduri lubamatu muutus,
'14'H	Kaardi andmesisestuse terviklikkusriike,
'15'H	Salvestatud kasutajaandmete terviklikkusriike,
'16'H	Sisemine andmeedastusriike,
'17'H	Lubamatu korpuse avamine,
'18'H	Manipulatsioon riistvaraga,
'19'H kuni '1F'H	H RFU (reserveeritud kasutuseks tulevikus),
'2x'H	Anduriga seotud turbemurdekate sündmused,
'20'H	Üksikasjad puuduvad,
'21'H	Autentimisriike,
'22'H	Salvestatud andmete terviklikkusriike,
'23'H	Sisemine andmeedastusriike,
'24'H	Lubamatu korpuse avamine,
'25'H	Manipulatsioon riistvaraga,
'26'H kuni '2F'H	RFU (tulevaste funktsioonide tarvis),
'3x'H	Sõidumeerikurikked,
'30'H	Üksikasjad puuduvad,
'31'H	Sõidukiüksuse siseriike,
'32'H	Printeririike
'33'H	Kuvaririike,
'34'H	Allalaadimisriike,
'35'H	Sensoririike,
'36'H kuni '3F'H	RFU (reserveeritud kasutuseks tulevikus),
'4x'H	Kaardirikked,
'40'H	Üksikasjad puuduvad,
'41'H kuni '4F'H	RFU (reserveeritud kasutuseks tulevikus),
'50'H kuni '7F'H	RFU (reserveeritud kasutuseks tulevikus),
'80'H kuni 'FF'H	Tootjaomane.

2.55. EventFaultRecordPurpose

Kood, mis selgitab, miks sündmus või riike on registreeritud.

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

Väärtuse omistus:

'00'H	üks kümnest hilisemast (või viimasest) sündmusest või rikkest
'01'H	pikim sündmus viimase kümne päeva jooksul
'02'H	üks viiest pikimast sündmusest viimase 365 päeva jooksul
'03'H	viimane sündmus viimase kümne päeva jooksul
'04'H	kõige tõsisem sündmus viimase kümne päeva jooksul
'05'H	üks viiest kõige tõsisemast sündmusest viimase 365 päeva jooksul
'06'H	pärast viimast kalibreerimist toimunud esimene sündmus või riike
'07'H	aktiivne/kestev sündmus või riike
'08'H kuni '7F'H	RFU (reserveeritud kasutuseks tulevikus),
'80'H kuni 'FF'H	Tootjaomane.

2.56. ExtendedSerialNumber

Seadme kordumatu identifikaatsioon. Seda võib kasutada ka seadme avaliku võtme identifikaatorina.

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

serialNumber on seadme seerianumber, mis on kordumatu allpool esitatud tootja, seadmetüübi ja kuu tarvis.

monthYear on tootmise (või seerianumbri omistamise) kuu ja aasta identifikaatsioon.

Väärtuse omistus: binaarkodeeritud kümnendesituses kuu (kaks arvu) ja aasta (kaks viimast arvu).

type seadmetüübi identifikaator.

Väärtuse omistus: tootjaomane, reserveeritud väärtusega FFh'.

manufacturerCode: seadme tootja numbrikood.

2.57. FullCardNumber

Sõidumeerikukaardi täielikult identiv kood.

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

cardType on sõidumeerikukaardi tüüp.

cardIssuingMemberState on kaardi väljaandnud liikmesriigi kood.

cardNumber on kaardi number.

2.58. HighResOdometer

Sõiduki läbisõidumõõdiku näit: Sõiduki töötamise ajal läbitud kogu teepikkus.

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

Väärtuse omistus: kindlaks määramata kahendarv. Väärtus 1/200 km toimeulatuses 0 kuni 21 055 406 km.

2.59. HighResTripDistance

Kogu reisi või selle osa jooksul läbitud vahemaa.

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

Väärtuse omistus: kindlaks määramata kahendarv. Väärtus 1/200 km toimeulatuses 0 kuni 21 055 406 km.

2.60. HolderName

Kaardi omaniku perekonnanimi ja eesnimi (eesnimed).

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


holderSurname on kaardi omaniku perekonnanimi. Perekonnanimi ei hõlma tiitleid.

Väärtuse omistus: kui kaart ei ole isiklik, sisaldab holderSurname sama teavet kui companyName või workshopName või controlBodyName.

holderFirstNames on omaniku eesnimi (eesnimed) ja initsiaalid.

2.61. K-ConstantOfRecordingEquipment

Sõidumeeriku konstant (mõiste m).

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

Väärtuse omistus: impulsse kilomeetris toimeulatuses 0 kuni 64 255 impulssi/km.

2.62. KeyIdentifier

Viitamiseks ja võtme valikuks kasutatav avaliku võtme kordumatu identifikaator. See idendib ka võtme omaniku.

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

Esimene valik sobib sõidukiüksuse või sõidumeerikukaardi avalikule võtmele viitamiseks.

Teine valik sobib sõidukiüksuse avalikule võtmele viitamiseks (kui ei ole võimalik teada sõidukiüksuse seerianumbrit sertifikaadi loomise ajal).

Kolmas valik sobib liikmesriigi avalikule võtmele viitamiseks.

2.63. L-TyreCircumference

Rattarehvide efektiivübermõõt (mõiste u).

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

Väärtuse omistus: kindlaks määramata kahendarv, väärtus 1/8 mm toimeulatuses 0 kuni 8 031 mm.

2.64. Language

Keelt identiv kood.

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

Väärtuse omistus: kahest väiketähest koosnev kood vastavalt standardile ISO 639.

2.65. LastCardDownload

Juhikaardile salvestatud kaardilt viimase (muul eesmärgil kui kontrolliks) allalaadimise kuupäev ja kellaeg. Kuupäeva saab ajakohastada sõidukiüksuse või mis tahes kaardi lugejaga.

`LastCardDownload ::= TimeReal`

Väärtuse omistus: täpsustamata.

2.66. ManualInputFlag

Kood, mis näitab, kas kaardi omanik on juhi tegevusi kaardi sisestamisel käsitsi sisestanud või mitte (näue 081).

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

Väärtuse omistus: täpsustamata.

2.67. ManufacturerCode

Tootjat identiv kood.

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

Väärtuse omistus:

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

2.68. MemberStateCertificate

Euroopa sertifitseerimisasutuse väljaantud liikmesriigi avaliku võtme sertifikaat.

```
MemberStateCertificate ::= Certificate
```

2.69. MemberStatePublicKey

Liikmesriigi avalik võti.

MemberStatePublicKey ::= PublicKey.

2.70. Name

Nimi.

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

codePage määratleb ISO/IEC 8859 osa, mida on nime kodeerimiseks kasutatud,

name on ISO/IEC 8859-codePage'i kohaselt kodeeritud nimi.

2.71. NationAlpha

Tähestikuline viide riigile vastavalt tavapärastele riigikoodidele autode kaitserauakleebistel ja/või nagu neid kasutatakse sõidukite rahvusvaheliselt ühtlustatud kindlustusdokumentides (roheline kaart).

NationAlpha ::= IA5String(SIZE(3))

Väärtuse omistus:

' '	Teave puudub
'A'	Austria
'AL'	Albaania
'AND'	Andorra
'ARM'	Armeenia
'AZ'	Aserbaidžaan
'B'	Belgia
'BG'	Bulgaaria
'BIH'	Bosnia ja Hertsegoviina
'BY'	Valgevene
'CH'	Šveits
'CY'	Küpros
'CZ'	Tšehhi Vabariik
'D'	Saksamaa
'DK'	Taani
'E'	Hispaania
'EST'	Eesti
'F'	Prantsusmaa
'FIN'	Soome
'FL'	Liechtenstein
'FR'	Fääri saared
'UK'	Ühendkuningriik, Alderney, Guernsey, Jersey, Mani saar, Gibraltar
'GE'	Gruusia
'GR'	Kreeka
'H'	Ungari
'HR'	Horvaatia
'I'	Itaalia
'IRL'	Iirimaa
'IS'	Island
'KZ'	Kasahstan
'L'	Luksemburg
'LT'	Leedu
'LV'	Läti
'M'	Malta
'MC'	Monaco

'MD'	Moldova Vabariik
'MK'	Makedoonia
'N'	Norra
'NL'	Madalmaad
'P'	Portugal
'PL'	Poola
'RO'	Rumeenia
'RSM'	San Marino
'RUS'	Venemaa Föderatsioon
'S'	Rootsi
'SK'	Slovakkia
'SLO'	Sloveenia
'TM'	Türkmenistan
'TR'	Türgi
'UA'	Ukraina
'V'	Vatikan
'YU'	Jugoslaavia
'UNK'	Teadmata
'EC'	Euroopa Ühendus
'EUR'	muu Euroopa
'WLD'	muu maailm.

2.72. NationNumeric

Numbriline viide riigile.

NationNumeric ::= INTEGER(0..255)

Väärtuse omistus:

-- Teave puudub	(00)H,
-- Austria	(01)H,
-- Albaania	(02)H,
-- Andorra	(03)H,
-- Armeenia	(04)H,
-- Aserbaidžaan	(05)H,
-- Belgia	(06)H,
-- Bulgaaria	(07)H,
-- Bosnia ja Hertsegoviina	(08)H,
-- Valgevene	(09)H,
-- Šveits	(0A)H,
-- Küpros	(0B)H,
-- Tšehhi Vabariik	(0C)H,
-- Saksamaa	(0D)H,
-- Taani	(0E)H,
-- Hispaania	(0F)H,
-- Eesti	(10)H,
-- Prantsusmaa	(11)H,
-- Soome	(12)H,
-- Liechtenstein	(13)H,
-- Fääri saared	(14)H,
-- Ühendkuningriik	(15)H,
-- Gruusia	(16)H,
-- Kreeka	(17)H,
-- Ungari	(18)H,
-- Horvaatia	(19)H,
-- Itaalia	(1A)H,
-- Iirimaa	(1B)H,
-- Island	(1C)H,

-- Kasahstan	(1D)H,
-- Luksemburg	(1E)H,
-- Leedu	(1F)H,
-- Läti	(20)H,
-- Malta	(21)H,
-- Monaco	(22)H,
-- Moldova Vabariik	(23)H,
-- Makedoonia	(24)H,
-- Norra	(25)H,
-- Madalmaad	(26)H,
-- Portugal	(27)H,
-- Poola	(28)H,
-- Rumeenia	(29)H,
-- San Marino	(2A)H,
-- Venemaa Föderatsioon	(2B)H,
-- Rootsi	(2C)H,
-- Slovakkia	(2D)H,
-- Sloveenia	(2E)H,
-- Türkmenistan	(2F)H,
-- Türgi	(30)H,
-- Ukraina	(31)H,
-- Vatikan	(32)H,
-- Jugoslaavia	(33)H,
-- reserveeritud kasutuseks tulevikus	(34..FC)H,
-- Euroopa Ühendus	(FD)H,
-- muu Euroopa	(FE)H,
-- muu maailm	(FF)H

2.73. NoOfCalibrationRecords

Kalibreerimiskirjete arv, mida saab töökojakaardile salvestada.

NoOfCalibrationRecords ::= INTEGER(0..255)

Väärtuse omistus: vt lõige 3.

2.74. NoOfCalibrationsSinceDownload

Loendur, mis näitab töökojakaardiga tehtud viimase allalaadimise järgset kalibreerimiste arvu (nõue 230).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2¹⁶-1),

Väärtuse omistus: täpsustamata.

2.75. NoOfCardPlaceRecords

Kohakirjete arv, mida saab juhi- või töökojakaardile salvestada.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Väärtuse omistus: vt lõige 3.

2.76. NoOfCardVehicleRecords

Kasutatud sõiduki kirjete arv, mida saab juhi- või töökojakaardile salvestada.

NoOfCardVehicleRecords ::= INTEGER(0..2¹⁶-1)

Väärtuse omistus: vt lõige 3.

2.77. NoOfCompanyActivityRecords

Ettevõtte tegevuskirjete arv, mida saab ettevõtteleardile salvestada.

NoOfCompanyActivityRecords ::= INTEGER(0..2¹⁶-1)

Väärtuse omistus: vt lõige 3.

2.78. NoOfControlActivityRecords

Kontrollitegevuse kirjete arv, mida saab kontrollikaardile salvestada.

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

Väärtuse omistus: vt lõige 3.

2.79. NoOfEventsPerType

Sündmuste arv sündmuse tüübi kohta, mida saab kaardile salvestada.

NoOfEventsPerType ::= INTEGER(0..255)

Väärtuse omistus: vt lõige 3.

2.80. NoOfFaultsPerType

Rikete arv rikketuübi kohta, mida saab kaardile salvestada.

NoOfFaultsPerType ::= INTEGER(0..255)

Väärtuse omistus: vt lõige 3.

2.81. OdometerValueMidnight

Sõiduki läbisõidumõõdiku näit antud päeva keskööl (nõue 090).

OdometerValueMidnight ::= OdometerShort

Väärtuse omistus: täpsustamata.

2.82. OdometerShort

Sõiduki läbisõidumõõdiku näit lühikujul.

OdometerShort ::= INTEGER(0..2²⁴-1)

Väärtuse omistus: kindlaks määramata kahendarv. Väärtus kilomeetrites toimeulatuses 0 kuni 9 999 999 km.

2.83. OverspeedNumber

Kiiruse ületamise sündmuste arv alates viimasest kiiruse ületamise kontrollist.

OverspeedNumber ::= INTEGER(0..255)

Väärtuse omistus: 0 tähendab, et pärast viimast kiiruse ületamise kontrolli ei ole toimunud ühtki kiiruse ületamise sündmust, 1 tähendab, et pärast viimast kiiruse ületamise kontrolli on toimunud üks kiiruse ületamise sündmus ... 255 tähendab, et pärast viimast kiiruse ületamise kontrolli on toimunud 255 või enam kiiruse ületamise sündmust.

2.84. PlaceRecord

Tööpäeva algus- või lõpukohaga seotud teave (nõuded 087, 202, 221).

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

entryTime on kirjega seotud kuupäev ja kellaeg.

entryTypeDailyWorkPeriod on kirjetüüp.

dailyWorkPeriodCountry on sisestatud riik.

dailyWorkPeriodRegion on sisestatud piirkond.

vehicleOdometerValue on läbisõidumõõdiku näit koha sisestamise ajal.

2.85. PreviousVehicleInfo

Teave juhi poolt varem kasutatud sõiduki kohta, kui ta sisestab oma kaardi sõidukiüksusesse (nõue 081).

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

vehicleRegistrationIdentification on sõiduki registreerimisnumber ja sõiduki registreerinud liikmesriik.

cardWithdrawalTime on kaardi väljavõtmise kuupäev ja kellaeg.

2.86. PublicKey

Avalik RSA võti.

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

rsaKeyModulus on võtmepaari moodul.

rsaKeyPublicExponent on võtmepaari avalik eksponent.

2.87. RegionAlpha

Alfabeetiline viide piirkonnale kindlaksmääratud riigis.

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

Väärtuse omistus:

' ' Teave puudub

Hispaania:

'AN'	Andaluusia
'AR'	Aragón
'AST'	Astuuria
'C'	Kantaabria
'CAT'	Kataloonia
'CL'	Castilla-León
'CM'	Castilla-La-Mancha
'CV'	Valencia
'EXT'	Extremadura
'G'	Galicia
'IB'	Baleaarid
'IC'	Kanaarid
'LR'	La Rioja
'M'	Madrid
'MU'	Murcia
'NA'	Navarra
'PV'	Baskimaa.

2.88. RegionNumeric

Numbriline viide piirkonnale kindlaksmääratud riigis.

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

Väärtuse omistus:

'00'H Teave puudub

Hispaania:

'01'H Andaluusia

'02'H Aragón

'03'H Astuuria

'04'H Kantaabria

'05'H Kataloonia

'06'H Castilla-León

'07'H Castilla-La-Mancha

'08'H Valencia

'09'H Extremadura

'0A'H Galicia

'0B'H Balearid

'0C'H Kanaarid

'0D'H La Rioja

'0E'H Madrid

'0F'H Murcia

'10'H Navarra

'11'H Baskimaa.

2.89. RSAKeyModulus

RSA võtmepaari moodul.

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

Väärtuse omistus: määratlemata.

2.90. RSAKeyPrivateExponent

RSA võtmepaari isiklik eksponent.

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

Väärtuse omistus: määratlemata.

2.91. RSAKeyPublicExponent

RSA võtmepaari avalik eksponent.

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

Väärtuse omistus: määratlemata.

2.92. SensorApprovalNumber

Anduri tüübikinnitusnumber.

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

Väärtuse omistus: määratlemata.

2.93. SensorIdentification

Liikumisandurisse salvestatud teave, mis on seotud liikumisanduri identifikaatsiooniga (nõue 077).

```

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

```


sensorSerialNumber on liikumisanduri laiendatud seerianumber (hõlmab osa numbrit ja tootjakoodi).

sensorApprovalNumber on liikumisanduri tüübikinnitusnumber.

sensorSCIdentifier on liikumisanduri turvakomponendi identifikaator.

sensorOSIdentifier on liikumisanduri operatsioonisüsteemi identifikaator.

2.94. SensorInstallation

Liikumisandurisse salvestatud teave, mis on seotud liikumisanduri paigaldamisega (nõue 099).

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

sensorPairingDateFirst on liikumisanduri sõidukiüksusega esimese ühendamise kuupäev.

firstVuApprovalNumber on liikumisanduriga ühendatud esimese sõidukiüksuse tüübikinnitusnumber.

firstVuSerialNumber on liikumisanduriga ühendatud esimese sõidukiüksuse seerianumber.

sensorPairingDateCurrent on liikumisanduri sõidukiüksusega praeguse ühendamise kuupäev.

currentVuApprovalNumber on liikumisanduriga praegu ühendatud sõidukiüksuse tüübikinnitusnumber.

currentVUSerialNumber on liikumisanduriga praegu ühendatud sõidukiüksuse seerianumber.

2.95. SensorInstallationSecData

Töökojakaardile salvestatud teave, mis on seotud liikumisanduri sõidukiüksusega ühendamiseks vajalike turbeandmetega (nõue 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Väärtuse omistus: vastavalt standardile ISO 16844-3.

2.96. SensorOSIdentifier

Liikumisanduri operatsioonisüsteemi identifikaator.

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

Väärtuse omistus: tootjaomane.

2.97. SensorPaired

Sõidukiüksusesse salvestatud teave, mis on seotud sõidukiüksusega ühendatud liikumisanduri identifitseerimisega (nõue 079).

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

sensorSerialNumber on sõidukiüksusega praegu ühendatud liikumisanduri seerianumber.

sensorApprovalNumber on sõidukiüksusega praegu ühendatud liikumisanduri tüübikinnitusnumber.

sensorPairingDateFirst on praegu sõidukiüksusega ühendatud liikumisanduri sõidukiüksusega esimese ühendamise kuupäev.

2.98. **SensorPairingDate**

Liikumisanduri sõidukiüksusega esimese ühendamise kuupäev.

`SensorPairingDate ::= TimeReal`

Väärtuse omistus: Nem meghatřrozott.

2.99. **SensorSerialNumber**

Liikumisanduri seerianumber.

`SensorSerialNumber ::= ExtendedSerialNumber:`

2.100. **SensorSCIdentifier**

Liikumisanduri turvaosa identifikaator.

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

Väärtuse omistus: osa tootja omane.

2.101. **Signature**

Digitaalallkiri.

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

Väärtuse omistus: vastavalt 11. liitele "Ühised turbemehhanismid".

2.102. **SimilarEventsNumber**

Samasuguste sündmuste arv ühel antud päeval (nõue 094).

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

Väärtuse omistus: nulli ei kasutata, 1 tähendab, et sellel päeval on toimunud ja salvestatud ainult üks seda tüüpi sündmus, 2 tähendab, et sellel päeval on toimunud kaks seda tüüpi sündmust (ainult üks on salvestatud), ... 255 tähendab, et sellel päeval on toimunud 255 või rohkem seda tüüpi sündmust.

2.103. **SpecificConditionType**

Eritingimust identiv kood (nõuded 050b, 105a, 212a ja 230a).

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

Väärtuse omistus:

'00'H reserveeritud kasutuseks tulevikus

'01'H Sõidumeerik mittevajalik — Algus

'02'H Sõidumeerik mittevajalik — Lõpp

'03'H PRAAMI-/RONGISÕIT

'04'H .. 'FF'H reserveeritud kasutuseks tulevikus.

2.104. **SpecificConditionRecord**

Juhi- või töökojakaardile või sõidukiüksusesse salvestatud teave, mis on seotud eritingimusega (nõuded 105a, 212a ja 230a).

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

entryTime on sisestamise kuupäev ja kellaaeg.

specificConditionType on eritingimust identiv kood.

2.105. Speed

Sõiduki kiirus (km/h).

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

Väärtuse omistus: kilomeetrit tunnis toimeulatuses 0 kuni 220 km/h.

2.106. SpeedAuthorised

Sõiduki lubatud suurim kiirus (mõiste bb).

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

2.107. SpeedAverage

Eelnevalt määratletud ajavahemiku keskmine kiirus (km/h).

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

2.108. SpeedMax

Eelnevalt määratletud ajavahemikul mõõdetud suurim kiirus.

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

2.109. TDesSessionKey

Kolmik DES-seansivõti.

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

Väärtuse omistus: täpsustamata.

2.110. TimeReal

Kombineeritud kuupäeva- ja ajakirje väli, kus kuupäev ja kellaaeg on väljendatud sekundites, mis on möödunud 1. jaanuari 1970. aasta universaalajast 00 tundi 00 minutit 00 sekundit.

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

Väärtuse omistus — okteti joondus: 1. jaanuari 1970. aasta universaalaja keskööst möödunud sekundite arv.

Suurim võimalik kuupäev/aeg on aastal 2106.

2.111. TyreSize

Rehvimõõtmete kindlaksmääramine.

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

Väärtuse omistus: vastavalt 31. märtsi 1992. aasta direktiivile 92/23/EMÜ, EÜT L 129, lk 95..

2.112. VehicleIdentificationNumber

Sõiduki valmistajetähise (VIN), mis osutab sõidukile kui tervikule, tavaliselt kere või raami seerianumber.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Väärtuse omistus: vastavalt standardile ISO 3779.

2.113. VehicleRegistrationIdentification

Euroopas unikaalne sõiduki identifitseerimine (sõiduki registreerimisnumber ja liikmesriik).

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

vehicleRegistrationNation on riik, kus sõiduk on registreeritud.

vehicleRegistrationNumber on sõiduki registreerimisnumber.

2.114. VehicleRegistrationNumber

Sõiduki registreerimisnumber. Registreerimisnumbri määrab sõidukitele litsentse väljaandev asutus.

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

codePage määratleb ISO/IEC 8859 osa, mida on vehicleRegNumber kodeerimiseks kasutatud,

vehicleRegNumber on ISO/IEC 8859-codePage'i kohaselt kodeeritud sõiduki registreerimisnumber.

Väärtuse omistus: riigimane.

2.115. VuActivityDailyData

Sõidukiüksusesse salvestatud teave, mis on seotud konkreetse kalendripäeval tegevuse muutuse ja/või juhtimistaatuse muutuse ja/või kaardistaatuse muutusega (nõue 084) ning avade staatusega kell 00.00 sellel päeval.

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

noOfActivityChanges on ActivityChangeInfo sõnade arv kogumis activityChangeInfos.

activityChangeInfos on juhi ActivityChangeInfo sõnade kogum, mis on selle päeva kohta sõidukiüksusesse salvestatud. See sisaldab alati kahte ActivityChangeInfo sõna, mis annavad kahe ava staatuse kell 00.00 sellel päeval.

2.116. VuApprovalNumber

Sõidukiüksuse tüübikinnitusnumber.

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

Väärtuse omistus: määratlemata.

2.117. VuCalibrationData

Sõidukiüksusesse salvestatud teave, mis on seotud sõidumeeriku kalibreerimistega (nõue 098).

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

noOfVuCalibrationRecords on kogumis vuCalibrationRecords sisalduv kirjete arv.

vuCalibrationRecords on kalibreerimiskirje kogum.

2.118. VuCalibrationRecord

Sõidukiüksusesse salvestatud teave, mis on seotud sõidumeeriku kalibreerimisega (nõue 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 on kalibreerimise eesmärk.

workshopName, **workshopAddress** on töökoja nimi ja aadress.

workshopCardNumber määrab kindlaks kalibreerimise ajal kasutatud töökojakaardi.

workshopCardExpiryDate on kaardi kehtivusaja lõpp.

vehicleIdentificationNumber on sõiduki valmistajatehase tähis.

vehicleRegistrationIdentification sisaldab sõiduki registreerimisnumbrit ja registreerinud liikmesriiki.

wVehicleCharacteristicConstant on sõidukit iseloomustav koefitsient.

kConstantOfRecordingEquipment on sõidumeeriku konstant.

lTyreCircumference on rehvide tegelik ümbermõõt.

tyreSize on sõidukile paigaldatud rehvide mõõtmete määramine.

authorisedSpeed on sõiduki lubatud kiirus.

oldOdometerValue, **newOdometerValue** on läbisõidumõõdiku vana ja uus näit.

oldTimeValue, **newTimeValue** on kuupäeva ja aja vana ja uus näit.

nextCalibrationDate on CalibrationPurpose'is määratletud järgmise kalibreerimise tüüp, mille peab läbi viima volitatud inspekteerimisasutus.

2.119. VuCardIWData

Sõidukiüksusesse salvestatud teave, mis on seotud juhi- või töökojakaartide sõidukiüksusesse sisestamis- ja väljavõtmistsükklitega (nõue 081).

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

noOfIWRRecords on vuCardIWRRecords'i kogumis sisalduv kirjete arv.

vuCardIWRRecords on kaardi sisestamis- ja väljavõtmistsüklitega seotud kirjete kogum.

2.120. VuCardIWRRecord

Sõidukiüksusesse salvestatud teave, mis on seotud juhi- või töökojakaardi sõidukiüksusesse sisestamis- ja väljavõtmistsükliga (nõue 081).

```
VuCardIWRRecord ::= SEQUENCE {
    cardHolderName                HolderName,
    fullCardNumber                 FullCardNumber,
    cardExpiryDate                 TimeReal,
    cardInsertionTime              TimeReal,
    vehicleOdometerValueAtInsertion OdometerShort,
    cardSlotNumber                 CardsSlotNumber,
    cardWithdrawalTime             TimeReal,
    vehicleOdometerValueAtWithdrawal OdometerShort,
    previousVehicleInfo            PreviousVehicleInfo
    manualInputFlag                ManualInputFlag
}
```

cardHolderName on kaardile salvestatud kaardiomaniku perekonnanimi ja eesnimed.

fullCardNumber on kaardile salvestatud kaardi tüüp, selle väljaandnud liikmesriik ja kaardi number.

cardExpiryDate on kaardile salvestatud kaardi kehtivusaja lõpp.

cardInsertionTime on sisestamise kuupäev ja kellaeg.

vehicleOdometerValueAtInsertion on sõiduki läbisõidumeeriku näit sisestamise ajal.

cardSlotNumber on ava, millesse kaart on sisestatud.

cardWithdrawalTime on väljavõtmise kuupäev ja kellaeg.

vehicleOdometerValueAtWithdrawal on sõiduki läbisõidumeeriku näit kaardi väljavõtmise ajal.

previousVehicleInfo sisaldab kaardile salvestatud teavet juhi poolt enne seda kasutatud sõiduki kohta.

manualInputFlag on tunnus, mis määrab kindlaks, kas kaardiomanik on kaardi sisestamisel sisestanud käsitsi juhtimistevõti.

2.121. VuCertificate

Sõidukiüksuse avaliku võtme sertifikaat.

```
VuCertificate ::= Certificate
```

2.122. VuCompanyLocksData

Ettevõttele salvestatud teave, mis on seotud ettevõtetelukkudega (nõue 104).

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

noOfLocks on kirjetes vuCompanyLocksRecords loetletud lukkude arv.

vuCompanyLocksRecords on ettevõtte lukukirjete kogum.

2.123. VuCompanyLocksRecord

Sõidukiüksusesse salvestatud teave, mis on seotud ühe ettevõtetelukuga (nõue 104).

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

lockInTime, **lockOutTime** on lukustamise ja luku avamise kuupäev ja kellaeg.

companyName, **companyAddress** on lukustamisega seotud ettevõtte nimi ja aadress.

companyCardNumber idendib lukustamisel kasutatud kaardi.

2.124. VuControlActivityData

Sõidukiüksusesse salvestatud teave, mis on seotud kontrollidega, mis on läbi viidud seda sõidukiüksust kasutades (nõue 102).

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

noOfControls on kirjetes vuControlActivityRecords loetletud kontrollide arv.

vuControlActivityRecords on kontrolli tegevuskirjete kogum.

2.125. VuControlActivityRecord

Sõidukiüksusesse salvestatud teave, mis on seotud kontrolliga, mis on läbi viidud seda sõidukiüksust kasutades (nõue 102).

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

controlType on kontrollitüüp.

controlTime on kontrolli kuupäev ja kellaeg.

ControlCardNumber idendib kontrolli ajal kasutatud kontrollikaardi.

downloadPeriodBeginTime on allalaadimise puhul allalaaditud ajavahemiku algusaeg.

downloadPeriodEndTime on allalaadimise puhul allalaaditud ajavahemiku lõpuaeg.

2.126. VuDataBlockCounter

Kaardile salvestatud lugeja, mis idendib järjestikuselt kaardi sisestamis-väljavõtmistsüklid sõidukiüksustes.

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

Väärtuse omistus: järjestikune number suurima väärtusega 9 999, algab uuesti nullist.

2.127. VuDetailedSpeedBlock

Sõidukiüksusesse salvestatud teave, mis on seotud sõiduki üksikasjaliku kiirusega minuti jooksul, mil sõiduk on liikunud, (nõue 093).

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

speedBlockBeginDate on ploki esimese kiirusväärtuse kuupäev ja kellaaeg.

speedsPerSecond on igas sekundis mõõdetud kiiruste kronoloogiline järjestus minutis, millega algab speedBlockBeginDate (kaasa arvatud).

2.128. VuDetailedSpeedData

Sõidukiüksusesse salvestatud teave, mis on seotud sõiduki üksikasjaliku kiirusega.

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

noOfSpeedBlocks on kiirusplokkide arv kogumis vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks on üksikasjalike kiirusplokkide kogum.

2.129. VuDownloadablePeriod

Kõige esimene ja viimane kuupäev, mille kohta on sõidukiüksuses andmeid seoses juhi tegevustega (nõuded 081, 084 või 087).

```
VuDownloadablePeriod ::= SEQUENCE {
    minDownloadableTime          TimeReal
    maxDownloadableTime          TimeReal
}
```

minDownloadableTime on sõidukiüksusesse salvestatud kõige vanem kaardi sisestuse või tegevuse muutuse või kohakirje kuupäev ja kellaaeg.

maxDownloadableTime on sõidukiüksusesse salvestatud kõige hilisem kaardi sisestuse või tegevuse muutuse või kohakirje kuupäev ja kellaaeg.

2.130. VuDownloadActivityData

Sõidukiüksusesse salvestatud teave, mis on seotud selle viimase allalaadimisega (nõue 105).

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

downloadingTime on allalaadimise kuupäev ja kellaaeg.

fullCardNumber idendib allalaadimise lubamiseks kasutatud kaardi.

companyOrWorkshopName on ettevõtte või töökoja nimi.

2.131. VuEventData

Sõidukiüksusesse salvestatud teave, mis on seotud sündmustega (nõue 094, välja arvatud kiiruse ületamise sündmus).

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

noOfVuEvents on kogumis vuEventRecords loetletud sündmuste arv.

vuEventRecords on sündmusekirjete kogum.

2.132. VuEventRecord

Sõidukiüksusesse salvestatud teave, mis on seotud sündmusega (nõue 094, välja arvatud kiiruse ületamise sündmus).

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

eventType on sündmuse tüüp.

eventRecordPurpose on eesmärk, miks see sündmus on registreeritud.

eventBeginTime on sündmuse alguse kuupäev ja kellaeg.

eventEndTime on sündmuse lõpu kuupäev ja kellaeg.

cardNumberDriverSlotBegin idendib sündmuse alguses juhikaardi avasse sisestatud kaardi.

cardNumberCodriverSlotBegin idendib sündmuse alguses kaasjuhi kaardi avasse sisestatud kaardi.

cardNumberDriverSlotEnd idendib sündmuse lõpus juhikaardi avasse sisestatud kaardi.

cardNumberCodriverSlotEnd idendib sündmuse lõpus kaasjuhi kaardi avasse sisestatud kaardi.

similarEventsNumber on samasuguste sündmuste arv sellel päeval.

Seda jada saab kasutada kõigi sündmuste korral, välja arvatud kiiruse ületamise sündmused.

2.133. VuFaultData

Sõidukiüksusesse salvestatud teave, mis on seotud riketega (nõue 096).

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

noOfVuFaults on kogumis vuFaultRecords loetletud rikete arv.

vuFaultRecords on rikkekirjete kogum.

2.134. VuFaultRecord

Sõidukiüksusesse salvestatud teave, mis on seotud rikkega (nõue 096).

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

faultType on sõidumeeriku rikke tüüp.

faultRecordPurpose on eesmärk, miks see rike on registreeritud.

faultBeginTime on rikke alguse kuupäev ja kellaaeg.

faultEndTime on rikke lõpu kuupäev ja kellaaeg.

cardNumberDriverSlotBegin idendib rikke alguses juhikaardi avasse sisestatud kaardi.

cardNumberCodriverSlotBegin idendib rikke alguses kaasjuhi kaardi avasse sisestatud kaardi.

cardNumberDriverSlotEnd idendib rikke lõpus juhikaardi avasse sisestatud kaardi.

cardNumberCodriverSlotEnd idendib rikke lõpus kaasjuhi kaardi avasse sisestatud kaardi.

2.135. VuIdentification

Sõidukiüksusesse salvestatud teave, mis on seotud sõidukiüksuse identimisega (nõue 075).

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

vuManufacturerName on sõidukiüksuse tootja nimi.

vuManufacturerAddress on sõidukiüksuse tootja aadress.

vuPartNumber on sõidukiüksuse osa number.

vuSerialNumber on sõidukiüksuse seerianumber.

vuSoftwareIdentification idendib sõidukiüksuses rakendatud tarkvara.

vuManufacturingDate on sõidukiüksuse tootmiskuupäev.

vuApprovalNumber on sõidukiüksuse tüübikinnitusnumber.

2.136. VuManufacturerAddress

Sõidukiüksuse tootja aadress.

```
VuManufacturerAddress ::= Address
```

Väärtuse omistus: määratlemata.

2.137. VuManufacturerName

Sõidukiüksuse tootja nimi.

```
VuManufacturerName ::= Name
```

Väärtuse omistus: määratlemata.

2.138. VuManufacturingDate

Sõidukiüksuse tootmiskuupäev.

```
VuManufacturingDate ::= TimeReal
```

Väärtuse omistus: määratlemata.

2.139. VuOverSpeedingControlData

Sõidukiüksusesse salvestatud teave, mis on seotud kiiruse ületamise sündmustega pärast viimast kiiruse ületamise kontrolli (nõue 095).

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

lastOverspeedControlTime on viimase kiiruse ületamise kontrolli kuupäev ja kellaaeg.

firstOverspeedSince on sellele kiiruse ületamise kontrollile järgneva esimese kiiruse ületamise kuupäev ja kellaaeg.

numberOfOverspeedSince on kiiruse ületamise sündmuste arv alates viimasest kiiruse ületamise kontrollist.

2.140. VuOverSpeedingEventData

Sõidukiüksusesse salvestatud teave, mis on seotud kiiruse ületamise sündmustega (nõue 094).

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

noOfVuOverSpeedingEvents on kogumis vuOverSpeedingEventRecords loetletud sündmuste arv.

vuOverSpeedingEventRecords on kiiruse ületamise kirjade kogum.

2.141. VuOverSpeedingEventRecord

Sõidukiüksusesse salvestatud teave, mis on seotud kiiruse ületamise sündmustega (nõue 094).

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

eventType on sündmuse tüüp.

eventRecordPurpose on eesmärk, miks see sündmus on registreeritud.

eventBeginTime on sündmuse alguse kuupäev ja kellaaeg.

eventEndTime on sündmuse lõpu kuupäev ja kellaaeg.

maxSpeedValue on sündmuse käigus mõõdetud suurim kiirus.

averageSpeedValue on sündmuse käigus mõõdetud aritmeetiline keskmine kiirus.

cardNumberDriverSlotBegin idendib sündmuse alguses juhikaardi avasse sisestatud kaardi.

similarEventsNumber on samasuguste sündmuste arv sellel päeval.

2.142. VuPartNumber

Sõidukiüksuse osa number.

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

Väärtuse omistus: sõidukiüksuse tootja omane.

2.143. VuPlaceDailyWorkPeriodData

Sõidukiüksusesse salvestatud teave, mis on seotud juhi tööpäeva algus- ja lõpukohaga (nõue 087).

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

noOfPlaceRecords on kogumis vuPlaceDailyWorkPeriodRecords sisalduv kirjete arv.

vuPlaceDailyWorkPeriodRecords on kohaga seotud kirjete kogum.

2.144. VuPlaceDailyWorkPeriodRecord

Sõidukiüksusesse salvestatud teave, mis on seotud juhi tööpäeva algus- ja lõpukohaga (nõue 087).

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

fullCardNumber on juhikaardi tüüp, kaardi väljaandnud liikmesriik ja kaardi number.

placeRecord sisaldab sisestatud kohaga seotud teavet.

2.145. VuPrivateKey

Sõidukiüksuse isiklik võti.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. VuPublicKey

Sõidukiüksuse avalik võti.

```
VuPublicKey ::= PublicKey
```

2.147. VuSerialNumber

Sõidukiüksuse seerianumber (nõue 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. VuSoftInstallationDate

Sõidukiüksuse tarkvaraversiooni installeerimiskuupäev.

```
VuSoftInstallationDate ::= TimeReal
```

Väärtuse omistus: määratlemata.

2.149. VuSoftwareIdentification

Sõidukiüksusesse salvestatud teave, mis on seotud installeeritud tarkvaraga.

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

vuSoftwareVersion on sõidukiüksuse tarkvaraversiooni number.

vuSoftInstallationDate on tarkvaraversiooni installeerimise kuupäev.

2.150. VuSoftwareVersion

Sõidukiüksuse tarkvaraversiooni number.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Väärtuse omistus: määratlemata.

2.151. VuSpecificConditionData

Sõidukiüksusesse salvestatud teave, mis on seotud eritingimustega.

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

noOfSpecificConditionRecords on kogumis specificConditionRecords sisalduv kirjete arv.

specificConditionRecords on eritingimustega seotud kirjete kogum.

2.152. VuTimeAdjustmentData

Sõidukiüksusesse salvestatud teave, mis on seotud korrapärase kalibreerimise väliste aja korrigeerimistega (nõue 101).

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

noOfVuTimeAdjRecords on kogumis vuTimeAdjustmentRecords sisalduv kirjete arv.

vuTimeAdjustmentRecords on aja korrigeerimise kirjete kogum.

2.153. VuTimeAdjustmentRecord

Sõidukiüksusesse salvestatud teave, mis on seotud korrapärase kalibreerimise välise aja korrigeerimisega (nõue 101).

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

oldTimeValue, newTimeValue on kuupäeva ja kellaaja vana ja uus väärtus.

workshopName, workshopAddress on töökoja nimi ja aadress.

workshopCardNumber idendib aja korrigeerimiseks kasutatud töökojakaardi.

2.154. W-VehicleCharacteristicConstant

Sõidukit iseloomustav koefitsient (mõiste k).

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

Väärtuse omistus: impulsse kilomeetris toimeulatuses 0 ... 64 255 impulssi/km.

2.155. WorkshopCardApplicationIdentification

Töökojakaardile salvestatud teave, mis on seotud kaardirakenduse identifitseerimisega (nõue 190).

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

typeOfTachographCardId määratleb rakendatud kaardi tüübi.

cardStructureVersion määratleb kaardi rakendusstruktuuri versiooni.

noOfEventsPerType on sündmuse tüübi kaupa sündmuste arv, mida on võimalik kaardile salvestada.

noOfFaultsPerType on rikketüübi kaupa rikete arv, mida on võimalik kaardile salvestada.

activityStructureLength näitab baitide arvu, mida on võimalik tegevuskirjete salvestamiseks kasutada.

noOfCardVehicleRecords on arv, mitu sõidukikirjet kaart mahutab.

noOfCardPlaceRecords on arv, mitu kohakirjet suudab kaart registreerida.

noOfCalibrationRecords on arv, mitu kalibreerimiskirjet kaart mahutab.

2.156. WorkshopCardCalibrationData

Töökojakaardile salvestatud teave, mis on seotud kaardiga tehtud töökojategevustega (nõuded 227 ja 229).

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

calibrationTotalNumber on kaardiga tehtud kalibreerimiste koguarv.

calibrationPointerNewestRecord on viimase ajakohastatud kalibreerimiskirje indeks.

Väärtuse omistus: number, mis vastab kalibreerimiskirjete lugejale, alates nullist kalibreerimiskirjete esimesel esinemisel struktuuris.

calibrationRecords on kirjete kogum, mis sisaldab teavet kalibreerimise ja/või aja korrigeerimise kohta.

2.157. WorkshopCardCalibrationRecord

Töökojakaardile salvestatud teave, mis on seotud kaardiga tehtud kalibreerimistegevustega (nõue 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 on kalibreerimise eesmärk.

vehicleIdentificationNumber on sõiduki valmistajatehase tähis.

vehicleRegistration sisaldab sõiduki registreerimisnumbrit ja registreerinud liikmesriiki.

wVehicleCharacteristicConstant on sõidukit iseloomustav koefitsient.

kConstantOfRecordingEquipment on sõidumeeriku konstant.

lTyreCircumference on rehvide tegelik ümbermõõt.

tyreSize on sõidukile paigaldatud rehvide mõõtmete määramine.

authorisedSpeed on sõiduki lubatud suurim kiirus.

oldOdometerValue, newOdometerValue on läbisõidumõõdiku vana ja uus väärtus.

oldTimeValue, newTimeValue on kuupäeva ja kellaaja vana ja uus väärtus.

nextCalibrationDate on eesmärgis CalibrationPurpose määratletud järgmise kalibreerimise tüüp, mille peab läbi viima volitatud inspekteerimisasutus.

vuPartNumber, vuSerialNumber ja **sensorSerialNumber** on sõidumeeriku identimiseks vajalikud andmeelemendid.

2.158. WorkshopCardHolderIdentification

Töökojakaardile salvestatud teave, mis on seotud kaardi omaniku identifkatsiooniga (nõue 216).

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

workshopName on kaardi omaniku töökoja nimi.

workshopAddress on kaardi omaniku töökoja aadress.

cardHolderName on omaniku perekonnanimi ja eesnimi (eesnimed) (näit mehaaniku nimi).

cardHolderPreferredLanguage on kaardi omaniku eelistatud keel.

2.159. WorkshopCardPIN

Töökojakaardi PIN-kood (nõue 213).

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

Väärtuse omistus: kaardi omanikule teadaolev PIN-kood, mis on paremal pool täidetud kuni 8 'FF' baidiga.

3. VÄÄRTUS- JA SUURUSULATUSE MÄÄRATLUSED

Lõikes 2 määratletud muutujate väärtuste määramine.

TimeRealRange ::= 2³²-1

3.1. Juhikaardi määratlused:

Muutuja väärtuse nimi	Minimaalne	Maksimaalne
CardActivityLengthRange	5 544 baiti (28 päeva, 93 tegevusmuutust päevas)	13 776 baiti (28 päeva, 240 tegevusmuutust päevas)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2. Töökojakaardi määratlused:

Muutuja väärtuse nimi	Minimaalne	Maksimaalne
CardActivityLengthRange	198 baiti (1 päev, 93 tegevusmuutust)	492 baiti (1 päev, 240 tegevusmuutust)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3. Kontrollikaardi määratlused:

Muutuja väärtuse nimi	Minimaalne	Maksimaalne
NoOfControlActivityRecords	230	520

3.4. Ettevõttekaardi määratlused:

Muutuja väärtuse nimi	Minimaalne	Maksimaalne
NoOfCompanyActivityRecords	230	520

4. MÄRGISTIKUD:

IA5Strings kasutab ASCII tähemärke vastavalt standardile ISO/IEC 8824-1. Loetavuse ja lihtsa viitamise huvides on väärtuste märgid esitatud allpool. Lahknevuse korral on ISO/IEC 8824-1 käesoleva informatiivse märkuse suhtes ülimuslik.

```
! " # $ % & ' ( ) * + , - . / 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 { | } ~
```

Muudes tähemärgistringides (aadress, nimi, sõiduki registreerimisnumber) kasutatakse lisaks tähemärke, mis on määratletud standarditega ISO/IEC 8859-1 (ladina-1 märgistik) koodidega 192 kuni 255 või ISO/IEC 8859-7 (kreeka märgistik).

5. KODEERIMINE

Kui kodeerimisel on kasutatud ASN.1 kodeerimisreegleid, kodeeritakse kõik määratletud andmetüübid vastavalt (ühtlustatud) standardile ISO/IEC 8825-2.

2. liide

SÕIDUMEERIKUKAARTIDE SPETSIFIKAAT

Sisukord

1.	Sissejuhatus	377
1.1.	Lühendid	377
1.2.	Viited	378
2.	Elektrilised ja füüsilised karakteristikud	378
2.1.	Toitepinge ja voolutarbimine	378
2.2.	Programmeerimispinge V_{pp}	379
2.3.	Taktgeneraator ja -sagedus	379
2.4.	Sisend-/väljundkontakt	379
2.5.	Kaardi olekud	379
3.	Riistvara ja andmevahetus	379
3.1.	Sissejuhatus	379
3.2.	Edastusprotokoll	379
3.2.1.	Protokollid	379
3.2.2.	ATR	380
3.2.3.	PTSPTS	381
3.3.	Päasutingimused	381
3.4.	Andmete krüpteerimine	382
3.5.	Käskude ja veakoodide ülevaade	382
3.6.	Käskude kirjeldus	383
3.6.1.	Select file	383
3.6.1.1.	Valik nime (AID) alusel	383
3.6.1.2.	Elementaarfaili valik, kasutades selle failiidentifikaatorit	384
3.6.2.	Read binary	384
3.6.2.1.	Käsk turvalise sõnumivahetuseta	385
3.6.2.2.	Käsk turvalise sõnumivahetusega	385
3.6.3.	Update binary	387
3.6.3.1.	Käsk turvalise sõnumivahetuseta	387
3.6.3.2.	Käsk turvalise sõnumivahetusega	388
3.6.4.	Get challenge	389
3.6.5.	Verify	389
3.6.6.	Get response	390
3.6.7.	PSO: verify certificate	390
3.6.8.	Internal authenticate	391

3.6.9.	External authenticate	392
3.6.10.	Manage security environment	393
3.6.11.	PSO: hash	394
3.6.12.	Perform hash of file	394
3.6.13.	PSO: compute digital signature	395
3.6.14.	PSO: verify digital signature	396
4.	Sõidumeerikukaardi struktuur	396
4.1.	Juhikaardi struktuur	397
4.2.	Töökojakaardi struktuur	399
4.3.	Kontrollikaardi struktuur	401
4.4.	Ettevõttekaardi struktuur	403

1. SISSEJUHATUS

1.1. Lühendid

Käesolevas liites kasutatakse järgmisi lühendeid:

AC	(access conditions) pääsutingimused
AID	(application identifier) rakenduse identifikaator
ALW	(always) alati
APDU	(application protocol data unit) APDU käsk (rakendusprotokolli andmeüksus)
ATR	(answer to reset) lähtestuse vastus
AUT	(authenticated) autenditud
C6, C7	kaardi kontaktid nr 6 ja 7 vastavalt standardile ISO/IEC 7816-2
cc	(clock cycles) taktid
CHV	(card holder verification information) kaardiomaniku tuvastusinfo
CLA	APDU käsu klassibait
DF	(dedicated file) erifail, see võib sisaldada muid faile (elementaar- või erifaile)
EF	(elementary file) elementaarfail
ENC	(encrypted) kodeeritud: pääs on võimalik ainult kodeerimisandmete abil
etu	(elementary time unit) elementaarajühik
IC	(integrated circuit) kiip
ICC	(integrated circuit card) kiipkaart
ID	(identifier) identifikaator
IFD	(interface device) liideseseade
IFS	(information field size) infovälja maht
IFSC	(information field size for the card) kaardi infovälja maht
IFSD	(information field size device (for the terminal) seadme (terminali) infovälja maht
INS	APDU käsu käsibait
Lc	APDU käsu sisendandmete pikkus
Le	oodatavate andmete pikkus (käsu väljundandmed)
MF	(master file) põhifail (DF-juur)
P1-P2	parameetribaidid
NAD	(node address) protokollis T=1 kasutatav sõlmeaadress
NEV	(never) mitte kunagi
PIN	(personal identification number) PIN-kood
PRO SM	(protected with secure messaging) kaitstud turvalise sõnumivahetusega
PTS	(protocol transmission selection) protokolliedastuse valik
RFU	(reserved for future use) reserveeritud kasutuseks tulevikus

RST	(reset (of the card)) (kaardi) lähtestus
SM	(secure messaging) turvaline sõnumivahetus
SW1-SW2	(status bytes) olekubaidid
TS	ATR-almärk
VPP	programmeerimispinge
XXh	väärtus XX kuueteistkümnendsüsteemis
	Konkatenatsioonisümbol 03 04=0304.

1.2. Viited

Käesolevas liites kasutatakse järgmisi viiteid:

EN 726-3	Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994. (Identimiskaartide süsteemid — Telekommunikatsiooni kiipkaardid ja terminalid — 3. osa: Rakendusest sõltumatud kaardinõuded, detsember, 1994.)
ISO/IEC 7816-2	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 2. osa: Kontaktide mõõtmed ja asukoht, esimene väljaanne, 1999.)
ISO/IEC 7816-3	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 3. osa: Elektroonilised signaalid ja edastusprotokoll, 2. väljaanne, 1997.)
ISO/IEC 7816-4	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 4. osa: Valdkondadevahelised andmevahetuskäskud, esimene väljaanne, 1995 + 1. muudatus, 1997.)
ISO/IEC 7816-6	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 4. osa: Valdkondadevahelised andmelemendid, esimene väljaanne, 1996 + 1. parandus, 1998.)
ISO/IEC 7816-8	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First edition: 1999. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 8. osa: Turvalisusega seotud valdkondadevahelised käskud, esimene väljaanne, 1999.)
ISO/IEC 9797	Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. Edition 2: 1994. (Infotehnoloogia — Turvatehnikad — Plokkšifferalgoritmi rakendavat krüptograafilist kontrollifunktsiooni kasutav andmeterviklikuse mehhanism, 2. väljaanne, 1994.)

2. ELEKTRILISED JA FÜÜSIKALISED OMADUSED

TCS_200 Kui ei ole määratletud teisiti, vastavad kõik elektroonilised signaalid standardile ISO/IEC 7816-3.

TCS_201 Kaardi kontaktide asukoht ja mõõtmed vastavad standardile ISO/IEC 7816-2.

2.1. Toitepinge ja voolutarbimine

TCS_202 Kaart töötab vastavalt spetsifikaatidele ja standardis ISO/IEC 7816-3 määratletud voolutarbimise piires.

TCS_203 Kaart töötab pingel $V_{cc} = 3 \text{ V } (+/- 0,3 \text{ V})$ o $V_{cc} = 5 \text{ V } (+/- 0,5 \text{ V})$.

Pinge valik toimub vastavalt standardile ISO/IEC 7816-3.

2.2. Programmeerimispinge V_{pp}

TCS_204 Kontakti C6 juures kaart programmeerimispinget ei vaja. Eeldatakse, et kontakt C6 ei ole ühendatud liideseseadmesse. Kontakt C6 võib olla ühendatud kaardil programmeerimispingega, kuid seda ei maandata. Pinget ei tohi mingil juhul arvesse võtta.

2.3. Taktgeneraator ja -sagedus

TCS_205 Kaart toimib sagedusalal 1–5 MHz. Ühe kaardiseansi ajal võib taktsagedus kõikuda $\pm 2\%$. Taktsageduse genereerib sõidukiüksus, mitte kaart ise. Töötsükkel võib kõikuda 40 ja 60 % vahel.

TCS_206 Kaardifailis EF_{ICC} sisalduvatel tingimustel võib välise taktgeneraatori seisata. Faili EF_{ICC} esimeses baidis on kodeeritud mooduse Clockstop tingimused (üksikasjad vt EN 726-3):

0	1		
3. bitt	2. bitt	1. bitt	
0	0	1	Clockstop lubatud, eelistatud tasand puudub
0	1	1	Clockstop lubatud, eelistatud tasand: 1
1	0	1	Clockstop lubatud, eelistatud tasand: 0
0	0	0	Clockstop ei ole lubatud
0	1	0	Clockstop lubatud ainult tasandil 1
1	0	0	Clockstop lubatud ainult tasandil 0

Bitte 4. kuni 8. ei kasutata.

2.4. Sisend-/väljundkontakt

TCS_207 TCS_207 Sisend-/väljundkontakti C7 kasutatakse andmete saamiseks liideseseadmest ja nende edastamiseks liideseseadmesse. Töötamise ajal on edastamismooduses ainult kas kaart või liideseseade. Kui mõlemad üksused on edastamismooduses, ei tohi kaarti kahjustada. Kui kaart ei edasta andmeid, on see vastuvõtumooduses.

2.5. Kaardi olekud

TCS_208 Toitepinge kohaldamisel töötab kaart kahes olekus:

- toimimisolekus käskude täitmise või digitaalüksusega ühenduses olemise ajal,
- puhkeolekus igal muul ajal; selles olekus säilitab kaart kõik andmed.

3. RIISTVARA JA ANDMEVAHETUS

3.1. Sissejuhatus

Käesolevas lõikes kirjeldatakse nõuetekohase töötamise ja koostalitlusvõime tagamiseks vajalikku sõidumeerikukaartide ja sõidukiüksuste minimaalset funktsionaalsust.

Sõidumeerikukaardid vastavad nii palju kui võimalik olemasolevate ISO/IEC standardite kohaldatavatele normidele (eelkõige ISO/IEC 7816). Kuid määratlemaks mõnd piiratud kasutamist või erinevusi nende olemasolu korral, on käsud ja protokollid täielikult kirjeldatud. Määratletud käsud vastavad täielikult osutatud normidele, kui see ei ole ära märgitud teisiti.

3.2. Edastusprotokoll

TCS_300 Edastusprotokoll vastab standardile ISO/IEC 7816-3. Eelkõige tuvastab sõidukiüksus kaardi saadetud ooteajalaiendid.

3.2.1. Protokollid

TCS_301 Kaart esitab nii protokollid T=0 kui protokollid T=1.

TCS_302 T=0 on vaikeprotokoll, seetõttu on vaja PTS käsku, et muuta see T=1 protokolliks.

TCS_303 Seadmed peavad toetama otsest kodeerimist "direct convention" mõlemas protokollis: seega on otsene kodeerimine kaardi puhul kohustuslik.

TCS_304 Kaardi infovälja mahubait esitatakse ATR signaalis tähemärgis TA3. See väärtus on vähemalt 'F0h' (=240 baiti).

Protokollide suhtes kohaldatakse järgmisi piiranguid:

TCS_305 T=0

- Liideseseade toetab vastust sisend-/väljundsignaalile, kui kaardi lähtestuse puhul on signaali tõususerv vähemalt 400 takti.
- Liideseseade suudab lugeda tähemärke, mida eraldab 12 elementaarajähikut.
- Liideseseade suudab lugeda vigast tähemärki ja selle kordust, kui see on eraldatud 13 elementaarajähikuga. Vigase tähemärgi tuvastamisel võib sisend-/väljundsignaalile anda veasignaali 1. ja 2. elementaarajähiku vahel. Seade toetab 1 elementaarajähiku pikkust viidet.
- Liideseseade aktsepteerib 33baidilist ATR signaali (TS+32)
- Kui ATR signaalis on olemas TC1, peab liideseseadme saadetud tähemärkide tarvis olema täiendav kaitseaeg, kuigi kaardi saadetud tähemärke võib eraldada 12 elementaarajähikuga. See kehtib ka kaardi saadetud ACK tähemärgi kohta pärast liideseseadme saadetud P3 tähemärki.
- Liideseseade võtab arvesse kaardi saadetud NUL tähemärki.
- Liideseseade aktsepteerib ACK tarvis täiendmoodust.
- Käsku GET RESPONSE ei saa kasutada aheltöötlusmooduses andmete saamiseks, mille pikkus võib ületada 255 baiti.

TCS_306 T=1

- Sõlmeaadressi bait: ei kasutata (NAD pannakse asendisse '00').
- Ploki S käsk ABORT: ei kasutata.
- Ploki S programmeerimispinge olekuviga: ei kasutata.
- Andmevälja koguhela pikkus ei ületa 255 baiti (tagatakse liideseseadmega).
- Kohe pärast ATR signaali esitab liideseseade seadme infovälja mahu: pärast ATR signaali edastab liideseseade ploki S infovälja mahu nõude ja kaart saadab tagasi ploki S infovälja mahu. Seadme infovälja mahu soovituslik väärtus on 254 baiti.
- Kaart ei palu infovälja mahu korrigeerimist.

3.2.2. ATR

TCS_307 Seade kontrollib ATR baite vastavalt standardile ISO/IEC 7816-3. ATR signaali kuuluvaid märke, mis on seotud kaardi ajalooaga (historical characters), ei tõendata.

Elementaarse kaheprotokollilise ATR signaali näide vastavalt standardile ISO/IEC 7816-3.

Märk	Väärtus	Märkused
TS	'3Bh'	Näitab otsest kodeerimist ("direct convention")
T0	'85h'	TD1 olemas; 5 ajaloolist baiti olemas
TD1	'80h'	TD2 olemas; tuleb kasutada T=0
TD2	'11h'	TA3 olemas; tuleb kasutada T=1
TA3	'XXh' (vähemalt 'F0h')	Kaardi infovälja maht (IFSC)
TH1 kuni TH5	'XXh'	Kaardi ajaloolised märgid
TCK	'XXh'	Kontrollimärk (ilma OR)

TCS_308 Pärast ATRi valitakse vaikimisi põhifail ja see saab töökataloogiks.

3.2.3. Käsk PTS

TCS_309 Vaikeprotokoll on T=0. T=1 protokoll tekitamiseks peab seade saatma kaardile käsu PTS (tuntud ka kui käsk PPS).

TCS_310 Kuna kaardi puhul on kohustuslikud nii T=0 kui T=1 protokoll, on protokollivahetuseks kohustuslik ka baaskäsk PTS.

Nagu näidatud standardis ISO/IEC 7816-3, võib PTSi kasutada võimaluse korral üleminekuks ATR signaalis kaardi pakutud vaikeedastuskiirusele suuremale kiirusele (TA(1) bait).

Kaardi puhul on suuremad edastuskiirused vabatahtlikud.

TCS_311 Kui kaart toetab ainult vaikeedastuskiirust (või kui valitud edastuskiirust ei toetata), vastab kaart vastavalt standardile ISO/IEC 7816-3 käsule PTS nõuetekohaselt, jättes vahele PPS1 baidi.

Protokollivaliku baaskäsu PTS näited on järgmised:

Märk	Väärtus	Märkused
PPSS	'FFh'	Algmärk
PPS0	'00h' või '01h'	PPS1 kuni PPS3 puuduvad; T0 valimiseks '00h', T1 valimiseks '01h'
PK	'XXh'	Kontrollimärk: 'XXh' = 'FFh' kui PPS0 = '00h' 'XXh' = 'FEh' kui PPS0 = '01h'

3.3. Pääsutingimused

Iga elementaarfaili puhul on määratletud käskude UPDATE_BINARY ja READ_BINARY pääsutingimused.

TCS_312 Tööfaili pääsutingimused peavad olema täidetud enne nende käskude abil faili pääsemist.

Olemasolevate pääsutingimuste määratlused on järgmised:

- ALW: tegevus on alati võimalik ning seda saab piiranguteta teha.
- NEV: tegevus ei ole kunagi võimalik.
- AUT: tuleb avada pääsuõigus, mis vastab edukale välisautentimisele (käsuga EXTERNAL_AUTHENTICATE).
- PRO SM: käsk tuleb edastada krüptograafilise kontrollsummana, kasutades turvalist sõnumivahetust (vt 11. liide).
- AUT ja PRO SM (kombineeritud)

Käskudega (UPDATE_BINARY ja READ_BINARY) võib kaardile panna järgmised pääsutingimused:

	UPDATE_BINARY	READ_BINARY
ALW	jah	jah
NEV	jah	jah
AUT	jah	jah
PRO SM	jah	ei
AUT ja PRO SM	jah	ei

Käsuks READ_BINARY ei ole PRO SM pääsutingimus võimalik. See tähendab, et krüptograafiline kontrollsumma ei ole käsuks READ kunagi kohustuslik. Kuid kasutades selle klassi puhul väärtust 'OC', on võimalik kasutada käsku READ_BINARY koos turvalise sõnumivahetusega, nagu seda on kirjeldatud lõikes 3.6.2.

3.4. Andmete krüpteerimine

Kui on vaja kaitsta failist loetavate andmete konfidentsiaalsust, märgitakse fail kui "krüpteeritud". Krüpteerimisel kasutatakse turvalist sõnumivahetust (vt 11. liide).

3.5. Käskude ja veakoodide ülevaade

Käsud ja failide korraldus on tuletatud standardist ISO/IEC 7816-4 ning need vastavad sellele.

TCS_313 Käesolevas osas kirjeldatakse järgmisi APDU käsu-vastuse paare:

Käsk	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
VÉDELMI MŪVELET VÉGREHAJTŠA: 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 Igas vastusesõnumis saadetakse olekubaidid SW1 SW2 ja need märgistavad käsu töötlusolekut.

SW1	SW2	Tähendus
90	00	Normaalne töötlus
61	XX	Normaalne töötlus. XX = vabade vastusbaitide arv
62	81	Töötlushoiatus. Osa tagasisaadetud andmetest võib olla rikutud
63	CX	Vale CHV (PIN). Järelejäänud katsete lugeja 'X'
64	00	Täitmisviga — säilmälu olek muutumata. Terviklikkusviga
65	00	Täitmisviga — säilmälu olek muudetud
65	81	Täitmisviga — säilmälu olek muudetud — mäluviga
66	88	Turbeviga: vale krüptograafiline kontrollsumma (turvalise sõnumivahetuse ajal) või vale sertifikaat (sertifikaadi tõendamise ajal) või valekrüptogramm (välise autentimise ajal) või vale allkiri (allkirja tõendamise ajal) rossz alikrjş (az alikrjş ellenörzése alatt)
67	00	Vale pikkus (vale Lc või Le)
69	00	Keelatud käsk (T=0 ei ole vastust olemas)
69	82	Turbeoleku nõuded ei ole täidetud
69	83	Autentimismeetod blokeeritud
69	85	Kasutustingimused ei ole täidetud
69	86	Käsk ei ole lubatud (elementaartööfail puudub)
69	87	Oodatavad turvalise sõnumivahetuse andmeobjektid on puudu
69	88	Ebaõiged turvalise sõnumivahetuse andmeobjektid
6A	82	Faili ei leita
6A	86	Valed parameetrid P1-P2
6A	88	Viiteandmeid ei leita
6B	00	Valed parameetrid (nihe elementaarfailist välja)

SW1	SW2	Tähendus
6C	XX	Vale pikkus, SW2 näitab täpset pikkust. Ühtki andmevälja ei saadeta tagasi
6D	00	Veakoodil puudub tugi või see on kehtetu
6E	00	Klassil puudub tugi
6F	00	Muud kontrollivead

3.6. Käskude kirjeldused

Käesolevas peatükis kirjeldatakse sõidumeerikukaartide kohustuslikke käske.

Asjaomased lisäüksikasjad, mis puudutavad seotud krüptograafilisi toiminguid, on esitatud 11. liites "Ühised turbemehhanismid".

Kõiki käske kirjeldatakse kasutatud protokollist (T=0 või T=1) sõltumatult. APDU baidid CLA, INS, P1, P2, Lc ja Le on alati näidatud. Kui kirjeldatud käsu jaoks ei ole vaja Lc või Le baiti, on nendega seotud pikkus, väärtus ja kirjeldus tühi.

TCS_315 Kui nõutakse mõlemat pikkusbaiti (Lc ja Le), tuleb kirjeldatud käsk jagada kaheks osaks, kui IFD kasutab protokollit T=0: kui IFD saadab kirjeldusekohase käsu, kus P3=Lc + data, ja siis saadab käsu GET_RESPONSE (vt punkt 3.6.6), kus P3=Le.

TCS_316 Kui nõutakse mõlemat pikkusbaiti ja Le=0 (turvaline sõnumivahetus):

- Kui kasutatakse protokollit T=1, vastab kaart teatele Le=0, saates kõik olemasolevad väljundiandmed.
- Kui kasutatakse protokollit T=0, saadab liideseseade esimese käsu teatega P3=Lc + data, kaart vastab (sellest järelduvale Le=0) olekubaitidega '61La', kus La on vastusbaitide arv, mida on võimalik kasutada. Seejärel genereerib liideseseade andmete lugemiseks käsu GET RESPONSE, kus P3=La.

3.6.1. *Select file*

See käsk vastab standardile ISO/IEC 7816-4, kuid selle kasutus on normis määratletud käsuga võrreldes piiratud.

Käsku SELECT FILE kasutatakse:

- rakenduse erifaili valimiseks (valida tuleb nime alusel)
- elementaarfaili valimiseks, mis vastab esitatud faili identifikaatorile.

3.6.1.1. *Valik nime alusel (AID)*

Käsk võimaldab valida rakenduse DFi kaardil.

TCS_317 Käsku saab anda faili struktuuris mis tahes kohas (pärast ATRi või mis tahes ajal).

TCS_318 Rakenduse valik lähtestab hetke turbekeskkonna. Pärast rakenduse valiku tegemist ei ole enam ükski avalik võti valitud ning turvaliseks sõnumivahetuseks ei ole enam võimalik kasutada eelmise seansi võtit. Samuti ei kehti enam AUT pääsutingimus.

TCS_319 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Valik nime alusel (AID)
P2	1	'0Ch'	Vastust ei oodata
Lc	1	'NNh'	Kaardile saadetud baitide arv (AID pikkus): '06h' sõidumeerikurakendusele
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' sõidumeerikurakendusele

Vastust käsule SELECT FILE ei ole vaja (T=1 puhul Le puudub, T=0 puhul vastust ei küsita).

TCS_320 Vastusesõnum (vastust ei küsita)

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui rakenduse identifikaatorile vastavat rakendust ei leita, on töötlusolekut kirjeldav vastus '6A82',
- protokollis T=1, kui bait Le on olemas, on olekuvastus '6700',
- protokollis T=0, kui küsitakse vastust pärast käsku SELECT FILE, on olekuvastus '6900',
- kui valitud rakendus loetakse vigaseks (faili atribuutide hulgas on tuvastatud terviklikkusviga), on töötlusoleku vastus '6400' või '6581'.

3.6.1.2. Elementaarfaili valik, kasutades selle faili identifikaatorit

TCS_321 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Efi valik kasutusel oleva DFi alusel
P2	1	'0Ch'	Vastust ei oodata
Lc	1	'02h'	Kaardile saadetud baitide arv
#6-#7	2	'XXXXh'	Faili identifikaator

Vastust käsule SELECT FILE ei ole vaja (T=1 puhul Le puudub, T=0 puhul vastust ei küsita).

TCS_322 Vastusesõnum (vastust ei küsita)

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui faili identifikaatorile vastavat faili ei leita, on töötlusolekut kirjeldav vastus '6A82',
- protokollis T=1, kui bait Le on olemas, on olekuvastus '6700',
- protokollis T=0, kui küsitakse vastust pärast käsku SELECT FILE, on olekuvastus '6900',
- kui valitud fail loetakse vigaseks (faili atribuutide hulgas on tuvastatud terviklikkusviga), on töötlusoleku vastus '6400' või '6581'.

3.6.2. Read Binary

Käsk vastab standardile ISO/IEC 7816-4, kuid selle kasutus on normis määratletud käsuga võrreldes piiratud.

Käsku READ BINARY kasutatakse andmete lugemiseks transparentsest failist.

Kaardi vastus seisneb loetud andmete tagasisaatmises, mis võivad olla soovi korral kaitstud turvalise sõnumivahetuse struktuuriga.

TCS_323 Käsu saab anda ainult siis, kui turbeolek vastab elementaarfaili tarvis määratletud READ funktsiooni turbeattribuutidele.

3.6.2.1. Käsk turvalise sõnumivahetuseta

Käsk võimaldab liideseseadmel lugeda hetkel valitud elementaarfailist andmeid turvalise sõnumivahetuseta.

TCS_324 Selle käsuga ei ole võimalik lugeda andmeid failist, mis on märgitud kui "krüpteeritud".

TCS_325 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	Turvalist sõnumivahetust ei nõuta
INS	1	'B0h'	
P1	1	'XXh'	Nihe baitides faili algusest: kõige tähtsam bait
P2	1	'XXh'	Nihe baitides faili algusest: kõige vähem tähtis bait
Le	1	'XXh'	Vastuseks saadavate andmete pikkus, loetavate baitide arv

Märkus:P1 8. bitt peab olema 0.

TCS_326 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
#1-#X	X	'XX..XXh'	Andmed loetud
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui elementaarfaili ei ole valitud, saadakse töötlusvastus '6986',
- kui valitud faili pääsutingimused ei ole täidetud, katkestatakse käsk sõnumiga '6982',
- kui nihe ei vasta elementaarfaili suurusele (nihe > EFi suurus), saadakse töötlusvastus '6B00',
- kui loetavate andmete suurus ei vasta EFi suurusele (nihe + Le > EFi suurus), saadakse töötlusvastus '6700' või '6Cxx', kus 'xx' näitab täpset pikkust,
- kui faili atribuutide hulgas on tuvastatud terviklikkusviga, peab kaart faili vigaseks ja taastamatuks ning töötlusoleku vastus on '6400' või '6581',
- kui salvestatud andmete hulgas on tuvastatud terviklikkusviga, saadab kaart nõutud andmed tagasi ja töötlusoleku vastus on '6281'.

3.6.2.2. Käsk turvalise sõnumivahetusega

Käsk võimaldab liideseseadmel lugeda hetkel valitud elementaarfailist andmeid turvalise sõnumivahetusega, et tõendada saadud andmete terviklikkust ja kaitsta andmete konfidentsiaalsust, kui elementaarfail on märgitud kui "krüpteeritud".

TCS_327 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'0Ch'	Nõutakse turvalist sõnumivahetust
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (nihe baitides faili algusest): kõige tähtsam bait
P2	1	'XXh'	P2 (nihe baitides faili algusest): kõige vähem tähtis bait
Lc	1	'09h'	Sisendandmete pikkus turvaliseks sõnumivahetuseks
#6	1	'97h'	T _{LE} : oodatava pikkusmääratluse silt
#7	1	'01h'	L _{LE} : oodatavate andmete pikkus
#8	1	'NNh'	Oodatav pikkusmääratlus (algupärane Le): loetavate baitide arv

Bait	Pikkus	Väärtus	Kirjeldus
#9	1	'8Eh'	T _{CC} : krüptograafilise kontrollsumma pikkus
#10	1	'04h'	L _{CC} : järgmise krüptograafilise kontrollsumma pikkus
#11-#14	4	'XX..XXh'	Krüptograafiline kontrollsumma (4 kõige tähtsamat baiti)
Le	1	'00h'	Vastavalt standardile ISO/IEC 7816-4

TCS_328 Vastusesõnum, kui elementaarfail ei ole "krüpteeritud" ja kui turvalise sõnumivahetuse sisendvorming on õige:

Bait	Pikkus	Väärtus	Kirjeldus
#1	1	'81h'	T _{PV} : lihtväärtusega andmete silt
#2	L	'NNh' või '81 NNh'	L _{PV} : vastuseks saadetavate andmete pikkus (= algupärane Le) L on 2 baiti, kui L _{PV} > 127 baiti
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Lihtandmete väärtus
#(2+L+NN)	1	'8Eh'	T _{CC} : krüptograafilise kontrollsumma silt
#(3+L+NN)	1	'04h'	L _{CC} : järgmise krüptograafilise kontrollsumma pikkus
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Krüptograafiline kontrollsumma (4 kõige tähtsamat baiti)
SW	2	'XXXXh'	Olekubaidid (WS1, SW2)

TCS_329 Vastusesõnum, kui elementaarfail on "krüpteeritud" ja kui turvalise sõnumivahetuse sisendvorming on õige:

Bait	Pikkus	Väärtus	Kirjeldus
#1	1	'87h'	T _{PI CG} : krüpteeritud andmete silt (krüptogramm)
#2	L	'MMh' või '81 MMh'	L _{PI CG} : vastuseks saadetavate krüpteeritud andmete pikkus (erineb käsu algupärasest Le-st tädistuse poolest) L on 2 baiti, kui L _{PV CG} > 127 baiti
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Krüpteeritud andmed: tädistuse indikaator ja krüptogramm
#(2+L+MM)	1	'8Eh'	T _{CC} : krüptograafilise kontrollsumma silt
#(3+L+MM)	1	'04h'	L _{CC} : järgmise krüptograafilise kontrollsumma pikkus
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Krüptograafiline kontrollsumma (4 kõige tähtsamat baiti)
SW	2	'XXXXh'	Olekubaidid (WS1, SW2)

Vastuseks tagasi saadetud krüpteeritud andmete esimene bait näitab kasutatud tädistamismoodust. Sõidumeerikurakenduse puhul on tädisindikaatori väärtus alati '01h', mis näitab, et kasutatud tädistamismoodus on üks standardis ISO/IEC 7816-4 määratletud moodustest (üks bait väärtusega 80h', millele järgnevad mõned nullbaidid — ISO/IEC 9797 2. meetod).

Vastuseks võib saata "tavalisi" töötlusolekuid, mis on kirjeldatud turvalise sõnumivahetuse käsu READ BINARY juures (vt punkt 3.6.2.1), kasutades eespool kirjeldatud vastusesõnumi struktuure.

Lisaks sellele võib esineda vigu, mis on eelkõige seotud turvalise sõnumivahetusega. Sellisel juhul saadetakse vastuseks lihtsalt töötlusolek ilma turvalise sõnumivahetuse struktuurita:

TCS_330 Vastusesõnum turvalise sõnumivahetuse vale sisendvormingu korral

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

— Kui hetkel ei ole kasutusel ühtegi seansivõtit, saadakse töötlusvastus '6A88'. See juhtub siis, kui seansivõtit ei ole veel loodud või kui seansivõtme kehtivusaeg on möödunud (sellisel juhul peab liideseseade uue seansivõtme saamiseks läbima taas vastastikuse autentimisprotsessi).

— Kui turvalise sõnumivahetuse vormingus puuduvad mõned oodatavad andmeobjektid (nagu määratletud eespool), saadakse vastuseks töötlusolek '6987' — see viga juhtub siis, kui oodatav silt on kadunud või käsu ülesehitus on vale.

- Kui mõned andmeobjektid on valed, saadakse töötlusvastus '6988': see viga esineb siis, kui vajalikud sildid on olemas, kuid mõne pikkus erineb oodatavast pikkusest.
- Kui krüptograafilise kontrollsumma tõendamine ei õnnestu, saadakse töötlusvastus '6688'.

3.6.3. Update Binary

Käsk vastab standardile ISO/IEC 7816-4, kuid selle kasutus on normis määratletud käsuga võrreldes piiratud.

UPDATE BINARY käsusõnum algatab EF kahendfailis olemasolevate bittide ajakohastamise (kustutamine + kirjutamine) käsus APDU olevate bittidega.

TCS_331 Käsku saab anda ainult siis, kui turbeolek vastab elementaarfaili tarvis määratletud funktsiooni UPDATE turbeatribuutidele (kui funktsiooni UPDATE pääsutingimused hõlmavad võimalust PRO SM, tuleb käsule lisada turvaline sõnumivahetus).

3.6.3.1. Käsk turvalise sõnumivahetusega

Käsk võimaldab liideseadmel kirjutada hetkel valitud elementaarfaili andmeid, kusjuures kaart ei tõenda saadud andmete terviklikkust. Seda lihtmoodust lubatakse kasutada ainult siis, kui seotud fail ei ole tähistatud kui "krüpteeritud".

TCS_332 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	Turvalist sõnumivahetust ei nõuta
INS	1	'D6h'	
P1	1	'XXh'	Nihe baitides faili algusest: kõige tähtsam bait
P2	1	'XXh'	Nihe baitides faili algusest: kõige vähem tähtis bait
Lc	1	'NNh'	Lc ajakohastatavate andmete pikkus. Kirjutatavate baitide arv
#6-#(5+NN)	NN	'XX..XXh'	Kirjutatavad andmed

Märkus: P1 8. bitt peab olema 0.

TCS_333 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui elementaarfaili ei ole valitud, saadakse töötlusvastus '6986',
- kui valitud faili pääsutingimused ei ole täidetud, katkestatakse käsk sõnumiga '6982',
- kui nihe ei vasta elementaarfaili suurusele (nihe > EFi suurus), saadakse töötlusvastus '6B00',
- kui loetavate andmete suurus ei vasta elementaarfaili suurusele (nihe + Le > EFi suurus), saadakse töötlusvastus '6700',
- kui faili atribuutide hulgas on tuvastatud terviklikkusviga, peab kaart faili vigaseks ja taastamatuks ning töötlusoleku vastus on '6400' või '6500',
- kui kirjutamine ebaõnnestub, saadakse töötlusvastus '6581'.

3.6.3.2. Käsk turvalise sõnumivahetusega

Käsk võimaldab liideseseadmel kirjutada hetkel valitud elementaarfaili andmeid, kusjuures kaart tõendab saadud andmete terviklikkust. Kuna konfidentsiaalsust ei nõuta, ei ole andmed krüpteeritud.

TCS_334 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'0Ch'	Nõutakse turvalist sõnumivahetust
INS	1	'D6h'	INS
P1	1	'XXh'	Nihe baitides faili algusest: kõige tähtsam bait
P2	1	'XXh'	Nihe baitides faili algusest: kõige vähem tähtis bait
Lc	1	'XXh'	Turvatud andmevälja pikkus
#6	1	'81h'	T _{PV} : lihtandmete silt
#7	L	'NNh' või '81 NNh'	L _{PV} : edastavate andmete pikkus L on 2 baiti, kui L _{PV} > 127 baiti
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	(Kirjutatavate) lihtandmete väärtus
#(7+L+NN)	1	'8Eh'	T _{CC} : krüptograafilise kontrollsumma silt
#(8+L+NN)	1	'04h'	L _{CC} : järgmise krüptograafilise kontrollsumma pikkus
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Krüptograafiline kontrollsumma (4 kõige tähtsamat baiti)
Le	1	'00h'	Vastavalt standardile ISO/IEC 7816-4

TCS_335 Vastusesõnum turvalise sõnumivahetuse õige sisendvormingu korral

Bait	Pikkus	Väärtus	Kirjeldus
#1	1	'99h'	T _{SW} : olekubaitide silt (kaitstud kontrollsummaga)
#2	1	'02h'	L _{SW} : vastuseks saadetud olekubaitide pikkus
#3-#4	2	'XXXXh'	Olekubaidid (SW1, SW2)
#5	1	'8Eh'	T _{CC} : krüptograafilise kontrollsumma silt
#6	1	'04h'	L _{CC} : järgmise krüptograafilise kontrollsumma pikkus
#7-#10	4	'XX..XXh'	Krüptograafiline kontrollsumma (4 kõige tähtsamat baiti)
SW	2	'XXXXh'	Olekubaidid (WS1, SW2)

Vastuseks võib saata "tavalisi" töötlusolekuid, mis on kirjeldatud turvalise sõnumivahetuse käsu UPDATE BINARY juures (vt punkt 3.6.3.1), kasutades eespool kirjeldatud vastusesõnumi struktuuri.

Lisaks sellele võib esineda vigu, mis on eelkõige seotud turvalise sõnumivahetusega. Sellisel juhul saadetakse vastuseks lihtsalt töötlusolek ilma turvalise sõnumivahetuse struktuurita:

TCS_336 Vastusesõnum vea korral turvalises sõnumivahetuses

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui hetkel ei ole kasutusel ühtegi seansivõtit, saadakse töötlusvastus '6A88',
- kui turvalise sõnumivahetuse vormingus puuduvad mõned oodatavad andmeobjektid (nagu määratletud eespool), saadakse vastuseks töötlusolek '6987' — see viga juhtub siis, kui oodatav silt on kadunud või käsu ülesehitatus on vale,
- kui mõned andmeobjektid on valed, saadakse töötlusvastus '6988': see viga esineb siis, kui vajalikud sildid on olemas, kuid mõne pikkus erineb oodatavast pikkusest,
- kui krüptograafilise kontrollsumma tõendamine ei õnnestu, saadakse töötlusvastus '6688'.

3.6.4. *Get challenge*

Käsk vastab standardile ISO/IEC 7816-4, kuid selle kasutus on normis määratletud käsuga võrreldes piiratud.

Käsk GET CHALLENGE käsib kaardil välja anda pretensiooni, et seda saaks kasutada turvalisusega seotud protseduuris, mille puhul kaardile saadetakse krüptogramm või mõned šifreeritud andmed.

TCS_337 Kaardi väljaantud pretensioon kehtib ainult kaardile saadetava järgmise käsu puhul, mis kasutab pretensiooni.

TCS_338 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (oodatava pretensiooni pikkus)

TCS_339 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
#1-#8	8	'XX..XXh'	Pretensioon
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui Le erineb '08h'-st, saadakse töötlusvastus '6700',
- kui parameetrid P1-P2 on valed, saadakse töötlusvastus '6A86'.

3.6.5. *Verify*

Käsk vastab standardile ISO/IEC 7816-4, kuid selle kasutus on normis määratletud käsuga võrreldes piiratud.

Käsk VERIFY algatab käsuga saadetud kaardiomaniku tuvastusinfo (PIN-kood) andmete võrdlemise kaardile salvestatud kaardiomaniku tuvastusinfoga.

Märkus: kasutaja sisestatud PIN-kood peab paremal pool olema liideseadme poolt täidistatud baitidega "FFh" pikkusega kuni 8 baiti.

TCS_340 Kui käsk on edukas, avatakse kaardiomaniku tuvastusinfole vastavad õigused ja PIN-koodi sisestamise katsete lugeja viiakse tagasi esialgsesse olekusse.

TCS_341 Ebaõnnestunud võrdlus registreeritakse kaardil, piiramaks edasisi katseid kasutada kaardile salvestatud kaardiomaniku tuvastusinfot.

TCS_342 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (tõendatud kaardiomaniku tuvastusinfo on automaatselt teada)
Lc	1	'08h'	Edastatud PIN-koodi pikkus
#6-#13	8	'XX..XXh'	Kaardiomaniku tuvastusinfo (CHV)

TCS_343 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui võrdlusinfot ei leita, saadakse töötlusvastus '6A88',
- kui võrdlusinfo on blokeeritud (PIN-koodi järelejäänud sisestamiskatsete lugeja on nullis), saadakse töötlusvastus '6983'. Kui on jõutud sellisesse olekusse, ei saa kaardiomaniku tuvastusinfot enam kunagi edukalt esitada,
- kui võrdlus ei ole edukas, vähendatakse PIN-koodi järelejäänud katsete lugejat ning saadakse töötlusvastus '63CX' (X > 0 ja X võrdub järelejäänud katsete arvuga. Kui X = 'F', on järelejäänud katsete lugeja suurem kui 'F'),
- kui võrdlusinfo loetakse rikutuks, saadakse töötlusvastus '6400' või '6581'.

3.6.6. **Get response**

Käsk vastab standardile ISO/IEC 7816-4.

Käsku (mis on vajalik ja kasutatav ainult protokollis T=1 puhul) kasutatakse ettevalmistatud andmete edastamiseks kaardilt liideseseadmesse (juhul kui käsk hõlmab nii Lc kui Le).

Käsk GET_RESPONSE tuleb anda kohe pärast käsku, mis andmed ette valmistab, vastasel juhul lähevad andmed kaduma. Pärast käsu GET_RESPONSE andmist ei ole varem ettevalmistatud andmed enam kättesaadavad (välja arvatud siis, kui juhtuvad vead '61xx' või '6Cxx', vt allpool).

TCS_344 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Oodatavate baitide arv

TCS_345 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
#1-#X	X	'XX..XXh'	Andmed
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000'.
- Kui kaart ei ole andmeid ette valmistanud, saadakse töötlusvastus '6900' või '6F00'.
- Kui Le ületab baitide arvu, mida on võimalik kasutada, või kui Le on null, saadakse töötlusvastus '6Cxx', kus 'xx' tähistab täpselt baitide arvu, mida on võimalik kasutada. Sellisel juhul on ettevalmistatud andmed järgmise käsu GET_RESPONSE tarvis kättesaadavad.
- Kui Le ei ole null ja on väiksem kui baitide arv, mida on võimalik kasutada, saadab kaart tavaliselt nõutud andmed ja saadakse töötlusvastus '61xx', kus 'xx' tähistab lisabaitide arvu, mida on võimalik kasutada järgmise käsu GET_RESPONSE korral.
- Kui käsul puudub tugi (protokoll T=1), vastab kaart '6D00'.

3.6.7. **PSO: verify certificate**

Käsk vastab standardile ISO/IEC 7816-8, kuid selle kasutus on normis määratletud käsuga võrreldes piiratud.

Kaart kasutab käsku VERIFY CERTIFICATE selleks, et saada väljastpoolt avalik võti ja kontrollida selle kehtivust.

TCS_346 Kui käsk VERIFY CERTIFICATE on edukas, salvestatakse avalik võti edaspidiseks kasutamiseks. Käsk MSE kasutab seda võtit otseselt turvalisusega seotud käskude korral (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE või VERIFY CERTIFICATE), kasutades seda koos võtme identifikaatoriga (vt punkt 3.6.10).

TCS_347 Igal juhul kasutab käsk VERIFY CERTIFICATE sertifikaadi avamiseks avalikku võtit, mille on käsk MSE eelnevalt valinud. See avalik võti peab olema liikmesriigi või Euroopa võti.

TCS_348 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'2Ah'	PSO (tee turbotoiming)
P1	1	'00h'	P1
P2	1	'AEh'	P2: mitte BER-TLV kodeeritud andmed (andmeelementide konkatensatsioon)
Lc	1	'CEh'	Lc: sertifikaadi pikkus, 194 baiti
#6-#199	194	'XX..XXh'	Sertifikaat: andmeelementide konkatensatsioon (11. liite kirjelduse kohaselt)

TCS_349 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui sertifikaadi tõendamine ei õnnestu, saadakse töötlusvastus '6688'. Sertifikaadi tõendus- ja lahtipakkimisprotsessi on kirjeldatud 11. liites,
- kui turvakeskkonnas ei ole olemas ühtegi avalikku võtit, saadakse töötlusvastus '6A88',
- kui (sertifikaadi lahtipakkimiseks kasutatud) valitud avalik võti loetakse rikutuks, saadakse töötlusvastus '6400' või '6581',
- kui valitud avaliku võtme CHA.LSB (*CertificateHolderAuthorisation.equipmentType*) erineb '00'-st (st see ei ole liikmesriigi või Euroopa võti), saadakse töötlusvastus '6985'.

3.6.8. Internal authenticate

Käsk vastab standardile ISO/IEC 7816-4.

Kasutades käsku INTERNAL AUTHENTICATE saab liideseseade kaardi autentida.

Autentimisprotsess on kirjeldatud 11. liites. See sisaldab järgmisi väiteid:

TCS_350 Käsk INTERNAL AUTHENTICATE kasutab autentimisandmete, sealhulgas K1 (seansivõtme sobivuse esimene element) ja RND1 allkirjastamiseks kaardi (vaikimisi valitud) isiklikku võtit ning allkirja kodeerimiseks ja autentimistõendi loomiseks hetkel valitud avalikku võtit (viimase käsu MSE kaudu) (üksikasjad 11. liites).

TCS_351 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Kaardile saadetud andmete pikkus
#6-#13	8	'XX..XXh'	Kaardi autentimiseks kasutatud pretensioon
#14-#21	8	'XX..XXh'	VU.CHR (vt 11. liide)
Le	1	'80h'	Kaardilt oodatavate andmete pikkus

TCS_352 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
#1-#128	128	'XX..XXh'	Kaardi autentimistõend (vt liide 11)
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui turvakeskkonnas ei ole olemas ühtegi avalikku võtit, saadakse töötlusvastus '6A88',
- kui turvakeskkonnas ei ole olemas ühtegi isiklikku võtit, saadakse töötlusvastus '6A88',
- kui VU.CHR ei vasta kasutusel olevale avaliku võtme identifikaatorile, saadakse töötlusvastus '6A88',
- kui valitud isiklikku võtit loetakse rikutuks, saadakse töötlusvastus '6400' või '6581'.

TCS_353 Kui käsk INTERNAL_AUTHENTICATE on edukas, kustutatakse hetkel kasutatud seansivõti, kui see oli olemas, ning seda ei saa enam kasutada. Uue seansivõtme saamiseks tuleb käsk EXTERNAL_AUTHENTICATE edukalt sooritada.

3.6.9. **External authenticate**

Käsk vastab standardile ISO/IEC 7816-4.

Kasutades käsku EXTERNAL AUTHENTICATE saab kaart liideseadme autentida.

Autentimisprotsessi on kirjeldatud 11. liites. See sisaldab järgmisi väiteid:

TCS_354 Käsk GET CHALLENGE peab olema vahetult enne käsku EXTERNAL_AUTHENTICATE. Kaart annab välja pretensiooni (RND3).

TCS_355 Krüptogrammi tõendamisel kasutatakse RND3 (kaardi väljaantud pretensioon), (vaikimisi valitud) kaardi isiklikku võtit ja eelnevalt käsuga MSE valitud avalikku võtit.

TCS_356 Kaart tõendab krüptogrammi ja kui see on õige, avatakse pääsutingimus AUT.

TCS_357 Sisendkrüptogramm sisaldab teist elementi seansivõtme kokkuleppe K2 tarvis.

TCS_358 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (kasutatav avalik võti on vaikimisi teada ning see on eelnevalt määratud käsuga MSE)
Lc	1	'80h'	Lc (kaardile saadetud andmete pikkus)
#6-#133	128	'XX..XXh'	Krüptogramm (vt 11. liide)

TCS_359 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui turvakeskkonnas ei ole olemas ühtegi avalikku võtit, saadakse töötlusvastus '6A88',
- kui hetkel kasutatava avaliku võtme CHA ei ole sõidumeerikurakenduse identifikaatori ja sõidukiüksuse seadmetüübi konkatenatsioon, saadakse töötlusvastus '6F00' (vt 11. liide),
- kui turvakeskkonnas ei ole olemas ühtegi isiklikku võtit, saadakse töötlusvastus '6A88',
- kui krüptogrammi tõendus on vale, saadakse töötlusvastus '6688',
- kui käsule ei eelne vahetult käsk GET CHALLENGE, saadakse olekuvastus '6985',
- kui valitud isiklikku võtit loetakse rikutuks, saadakse töötlusvastus '6400' või '6581'.

TCS_360 Kui käsk EXTERNAL AUTHENTICATE on edukas ja kui seansivõtme esimese poole saab hiljuti edukalt sooritatud käsust INTERNAL AUTHENTICATE, on seansivõti valmis edaspidiste käskude tarvis, kasutades turvalist sõnumivahetust.

TCS_361 Kui eelmisest käsust INTERNAL AUTHENTICATE ei ole seansivõtme esimest poolt võimalik saada, ei salvestata kaardile seansivõtme teist poolt, mille on saatnud liideseseade. See mehhanism tagab vastastikuse autentimisprotsessi läbiviimise 11. liites määratletud korras.

3.6.10. *Manage security environment*

Käsuga valitakse autentimiseks avalik võti.

Käsk vastab standardile ISO/IEC 7816-8. Käsu kasutamine on piiratud seotud standardi osas.

TCS_362 Käsu MSE andmeväljal osutatud võti kehtib sõidumeeriku DFi igas failis.

TCS_363 Käsu MSE andmeväljal osutatud võti jääb hetkel kasutatavaks avalikuks võtmeks kuni järgmise õige käsuni MSE.

TCS_364 Kui osutatud võtit ei ole (veel) kaardil, jääb turvakeskkond muutumatuks.

TCS_365 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: võti, millele viidatakse, kehtib kõigi krüptograafiliste toimingute puhul
P2	1	'B6h'	P2 (viidatavad andmed puudutavad digitaalalkirja)
Lc	1	'0Ah'	Lc: järgneva andmevälja pikkus
#6	1	'83h'	Viitamissilt avalikul võtmele asümmeetrilistel juhtudel
#7	1	'08h'	Võtmeviite pikkus (võtmeidentifikaator)
#8-#15	08h	'XX..XXh'	Võtmeidentifikaator 11. liite määratluse kohaselt

TCS_366 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui viidatud võtit ei ole kaardil olemas, saadakse töötlusvastus '6A88',
- kui turvalise sõnumivahetuse vormingus puuduvad mõned oodatavad andmeobjektid, saadakse vastuseks töötlusolek '6987'. See võib juhtuda, kui puudub silt '83h',
- kui mõned andmeobjektid on valed, saadakse töötlusvastus '6988'. See võib juhtuda, kui võtmeidentifikaatori pikkus ei ole '08h',
- kui valitud võti loetakse rikutuks, saadakse töötlusvastus '6400' või '6581'.

3.6.11. **PSO: hash**

Käsku kasutatakse mõnede andmete räsiarvutustulemuste edastamiseks kaardile. Käsku kasutatakse digitaalallkirjade tõendamiseks. Räsiväärtus salvestatakse EEPROM mällu järgmise digitaalallkirja tõendamiskäsu tarvis.

Käsk vastab standardile ISO/IEC 7816-8. Käsu kasutamine on piiratud seotud standardi osas.

TCS_367 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'2Ah'	Tee turbetoiming
P1	1	'90h'	Räsikoodi tagasisaatmine
P2	1	'A0h'	Silt: andmeväli sisaldab räsi algoritmiga töödeldavaid andmeobjekte
Lc	1	'16h'	Järgneva andmevälja Lc pikkus
#6	1	'90h'	Räsikoodi silt
#7	1	'14h'	Räsikoodi pikkus
#8-#27	20	'XX..XXh'	Räsikood

TCS_368 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000'-t küld vissza,
- kui mõned oodatavad andmeobjektid (nagu määratletud eespool) puuduvad, saadakse vastuseks töötlusolek '6987'. See võib juhtuda, kui puudub üks silt '90h',
- kui mõned andmeobjektid on valed, saadakse töötlusvastus '6988'. See viga esineb siis, kui vajalik silt on olemas, kuid pikkus erineb '14h'-st.

3.6.12. **Perform hash of file**

Käsk ei vasta standardile ISO/IEC 7816-8. Seega näitab käsu CLA bait, et tegemist on PERFORM SECURITY OPERATION/HASH valmistajaspetsiifilise kasutusega.

TCS_369 Käsku PERFORM HASH OF FILE kasutatakse hetkel valitud transparentse elementaarfaili andmeala töötlemiseks räsi algoritmi abil.

TCS_370 Räsistoimingu tulemus salvestatakse kaardile. Seda saab siis kasutada faili digitaalallkirja saamiseks, kasutades käsku PSO-COMPUTE_DIGITAL_SIGNATURE. Käsk COMPUTE_DIGITAL_SIGNATURE saab seda tulemust kasutada kuni järgmise eduka käsuni PERFORM_HASH_OF_FILE.

TCS_371 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'80h'	CLA
INS	1	'2Ah'	Tee turbetoiming
P1	1	'90h'	Silt: räsi algoritm
P2	1	'00h'	P2: töötlemishetkel valitud transparentse faili andmed räsi algoritmiga

TCS_372 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui rakendus ei ole valitud, saadakse töötlusvastus '6985',
- kui valitud elementaarfail loetakse vigaseks (faili atribuutide või salvestatud andmete terviklikkusviga), on töötlusoleku vastus '6400' või '6581',
- kui valitud fail ei ole transparentne fail, saadakse töötlusvastus '6986'.

3.6.13. PSO: compute digital signature

Käsku kasutatakse eelnevalt arvatud räsikoodi digitaalallkirja arvutamiseks (vt PERFORM_HASH_OF_FILE, punkt 3.6.12).

Käsk vastab standardile ISO/IEC 7816-8. Käsu kasutamine on piiratud seotud standardi osas.

TCS_373 Digitaalallkirja arvutamiseks kasutatakse kaardi isiklikku võtit ja kaart teab seda vaikimisi.

TCS_374 Kaart sooritab digitaalallkirja, kasutades PKCS1-le vastavat täidistamismeetodit (üksikasjad 11. liites).

TCS_375 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'2Ah'	Tee turbetoiming
P1	1	'9Eh'	Vastuseks saadetak digitaalallkiri
P2	1	'9Ah'	Silt: andmeväljal on andmeid, millele tuleb alla kirjutada. Kuna andmevälja ei ole, eeldatakse, et andmed on juba kaardil olemas (faili räsi)
Le	1	'80h'	Oodatava allkirja pikkus

TCS_376 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
#1-#128	128	'XX..XXh'	Eelnevalt arvatud räsi allkiri
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui vaikimisi valitud isiklikku võtit loetakse rikutuks, saadakse töötlusvastus '6400' või '6581'.

3.6.14. PSO: verify digital signature

Käsku kasutatakse sõnumi sisendina vastavalt PKC1-le esitatud digitaalallkirja tõendamiseks, mille räsi on kaardile teada. Allkirja algoritmi teab kaart vaikumisi.

Käsk vastab standardile ISO/IEC 7816-8. Käsu kasutamine on piiratud seotud standardi osas.

TCS_377 Käsk VERIFY DIGITAL SIGNATURE kasutab alati avalikku võtit, mis on valitud eelneva käsuga MANAGE SECURITY ENVIRONMENT, ja eelneva käsuga PSO: HASH sisestatud räsikoodi.

TCS_378 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'2Ah'	Tee turbetoiming
P1	1	'00h'	Silt: andmeväli sisaldab tõendamise seotud andmeobjekte
P2	1	'A8h'	
Lc	1	'83h'	Järgneva andmevälja Lc pikkus
#28	1	'9Eh'	Digitaalallkirja silt
#29-#30	2	'8180h'	Digitaalallkirja pikkus (128 baiti, kodeeritud vastavalt standardile ISO/IEC 7816-6)
#31-#158	128	'XX..XXh'	Digitaalallkirja sisu

TCS_379 Vastusesõnum

Bait	Pikkus	Väärtus	Kirjeldus
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

- Kui käsk on edukas, vastab kaart '9000',
- kui allkirja tõendamine ei õnnestu, saadakse töötlusvastus '6688'. Tõendusprotsess on kirjeldatud 11. liites,
- kui avalikku võtit ei ole valitud, saadakse töötlusvastus '6A88',
- kui mõned oodatavad andmeobjektid (nagu määratletud eespool) puuduvad, saadakse vastuseks töötlusolek '6987'. See võib juhtuda, kui üks nõutavatest siltidest on puudu,
- kui käsu töötlemiseks ei ole võimalik kasutada ühtki räsikoodi (eelneva käsu PSO: HASH tulemusel), saadakse töötlusvastus '6985',
- kui mõned andmeobjektid on valed, saadakse töötlusvastus '6988'. See võib juhtuda, kui ühe nõutava andmeobjekti pikkus on vale,
- kui valitud avalik võti loetakse rikutuks, saadakse töötlusvastus '6400' või '6581'.

4. SÖIDUMEERIKUKAARTIDE STRUKTUUR

Käesolevas lõikes määratletakse sõidumeerikukaartide failstruktuurid pääsetavate andmete salvestamiseks.

Siin ei määratleta kaardi tootja omaseid sisestruktuure, nagu näiteks failipäised, ega ainult sisevajadusteks vajalike andmelementide, näiteks `EuropeanPublicKey`, `CardPrivateKey`, `TDesSessionKey` või `WorkshopCardPin`, säilitamist ega töötlemist.

Sõidumeerikukaartide kasulik salvestusmaht on vähemalt 11 kilobaiti. Võib kasutada suuremat mahtu. Sellisel juhul jääb kaardistruktuur samaks, kuid suurendatakse struktuuri mõnede elementide kirjade arvu. Käesolevas lõikes määratletakse kirjade arvu minimaalsed ja maksimaalsed väärtused.

4.1. Juhikaardi struktuur

TCS_400 Pärast isikustamist on juhikaardil järgmine püsiv failstruktuuri ja failipääsu tingimused:

Fail	Faili tunnus	Pääsutingimused		
		Näit	Kaasajastamine	Kodeeritud
MF	3F00			
EF ICC	0002	ALW	NEV	Ei
EF IC	0005	ALW	NEV	Ei
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Ei
EF Card_Certificate	C100	ALW	NEV	Ei
EF CA_Certificate	C108	ALW	NEV	Ei
EF Identification	0520	ALW	NEV	Ei
EF Card_Download	050E	ALW	ALW	Ei
EF Driving_Licence_Info	0521	ALW	NEV	Ei
EF Events_Data	0502	ALW	PRO SM / AUT	Ei
EF Faults_Data	0503	ALW	PRO SM / AUT	Ei
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Ei
EF Vehicles_Used	0505	ALW	PRO SM / AUT	Ei
EF Places	0506	ALW	PRO SM / AUT	Ei
EF Current_Usage	0507	ALW	PRO SM / AUT	Ei
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Ei
EF Specific_Conditions	0522	ALW	PRO SM / AUT	Ei

TCS_401 Kõik elementaarfaili struktuurid on transparentsed.

TCS_402 Sõidumeeriku erifailis olevaid kõiki faile saab lugeda turvalise sõnumivahetuse teel.

TCS_403 Juhikaardil on järgmine andmestruktuur:

Fail/andmelement	Kirjete arv	Suurus (baitides)		Vaikeväärtused
		Min.	Maks.	
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	
└ eventTypes		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 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruse esitamiseks, on kirjete arvu minimaal- ja maksimumväärtused, mida juhikaardi andmestruktuur peab kasutama:

		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 baiti (28 päeva * 93 tegevusmuutust)	13 776 baiti (28 päeva * 240 tegevusmuutust)

4.2. Töökojakaardi struktuur

TCS_405 Pärast isikustamist on töökojakaardil järgmine püsiv failstruktuur ja faili pääsutingimused:

Fail	Faili tunnus	Pääsutingimused		
		Näit	Kaasajastamine	Kodeeritud
MF	3F00			
EF ICC	0002	ALW	NEV	Ei
EF IC	0005	ALW	NEV	Ei
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Ei
EF Card_Certificate	C100	ALW	NEV	Ei
EF CA_Certificate	C108	ALW	NEV	Ei
EF Identification	0520	ALW	NEV	Ei
EF Card_Download	0509	ALW	ALW	Ei
EF Calibration	050A	ALW	PRO SM / AUT	Ei
EF Sensor_Installation_Data	050B	ALW	NEV	Jah
EF Events_Data	0502	ALW	PRO SM / AUT	Ei
EF Faults_Data	0503	ALW	PRO SM / AUT	Ei
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Ei
EF Vehicles_Used	0505	ALW	PRO SM / AUT	Ei
EF Places	0506	ALW	PRO SM / AUT	Ei
EF Current_Usage	0507	ALW	PRO SM / AUT	Ei
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Ei
EF Specific_Conditions	0522	ALW	PRO SM / AUT	Ei

TCS_406 Kõik elementaarfaili struktuurid on transpertsed.

TCS_407 Sõidumeeriku erifailis olevaid kõiki faile saab lugeda turvalise sõnumivahetuse teel.

TCS_408 Töökojakaardil on järgmine andmestruktuur:

Fail/andmelement	Kirjete arv	Suurus (baitides)		Vaikväärtused
		Min.	Maks.	
MF		11088	29061	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		11055	29028	
EF Application_Identification		11	11	
WorkshopCardApplicationIdentification		11	11	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}

EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		146	146	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		2	2	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		9243	26778	
WorkshopCardCalibrationData		9243	26778	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		9240	26775	
WorkshopCardCalibrationRecord	n ₅	105	105	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
EF Sensor_Installation_Data		16	16	
SensorInstallationSecData		16	16	{00..00}
EF Events_Data		432	432	
CardEventData		432	432	
cardEventRecords	6	72	72	
CardEventRecord	n ₁	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		288	288	
CardFaultData		288	288	
cardFaultRecords	2	144	144	
CardFaultRecord	n ₂	24	24	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		202	496	
CardDriverActivity		202	496	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n ₆	198	492	{00..00}
EF Vehicles_Used		126	250	
CardVehiclesUsed		126	250	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		124	248	
CardVehicleRecord	n ₃	31	31	
vehicleOdometerBegin		3	3	{00..00}

vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		61	81	
CardPlaceDailyWorkPeriod		61	81	
placePointerNewestRecord		1	1	{00}
placeRecords		60	80	
PlaceRecord	n ₄	10	10	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		10	10	
SpecificConditionRecord	2	5	5	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_409 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruse esitamiseks, on kirjade arvu minimaal- ja maksimumväärtused, mida töökojakaardi andmestruktuur peab kasutama:

		Min.	Maks.
n ₁	NoOfEventsPerType	3	3
n ₂	NoOfFaultsPerType	6	6
n ₃	NoOfCardVehicleRecords	4	8
n ₄	NoOfCardPlaceRecords	6	8
n ₆	CardActivityLengthRange	88	255
n ₅	NoOfCalibrationRecords	198 baiti (1 päev * 93 tegevus- muutust)	492 baiti (1 päev * 240 tegevus- muutust)

4.3. Kontrollikaardi struktuur

TCS_410 Pärast isikustamist on kontrollikaardil järgmine püsiv failstruktuuri ja faili pääsustingimused:

Fail	Faili tunnus	Pääsustingimused		
		Näit	Kaasajastamine	Kodeeritud
MF	3F00			
EF ICC	0002	ALW	NEV	Ei
EF IC	0005	ALW	NEV	Ei
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Ei
EF Card_Certificate	C100	ALW	NEV	Ei
EF CA_Certificate	C108	ALW	NEV	Ei
EF Identification	0520	AUT	NEV	Ei
EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	Ei

TCS_411 Kõik elementaarfaili struktuurid on transparentsed.

TCS_412 Sõidumeeriku erifailis olevaid faile saab lugeda turvalise sõnumivahetuse teel.

TCS_413 Kontrollikaardil on järgmine andmestruktuur:

Fail/andmelement	Kirjete arv	Suurus (baitides)		Vaikeväärtused
		Min.	Maks.	
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 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruse esitamiseks, on kirjete arvu minimaal- ja maksimumväärtused, mida kontrollikaardi andmestruktuur peab kasutama:

		Min.	Maks.
n ₇	NoOfControlActivityRecords	230	520

4.4. Ettevõttekaardi struktuur

TCS_415 Pärast isikustamist on ettevõttekaardil järgmine püsiv failistruktuuri ja faili pääsutingimused:

Fail	Faili tunnus	Pääsutingimused		
		Näit	Kaasajastamine	Kodeeritud
MF	3F00			
EF ICC	0002	ALW	NEV	Ei
EF IC	0005	ALW	NEV	Ei
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Ei
EF Card_Certificate	C100	ALW	NEV	Ei
EF CA_Certificate	C108	ALW	NEV	Ei
EF Identification	0520	AUT	NEV	Ei
EF Company_Activity_Data	050D	ALW	PRO SM / AUT	Ei

TCS_416 Kõik elementaarfaili struktuurid on transpertsed.

TCS_417 Sõidumeeriku erifailis olevaid kõiki faile saab lugeda turvalise sõnumivahetuse teel.

TCS_418 Ettevõttekaardil on järgmine andmestruktuur:

Fail/andmelement	Kirjete arv	Suurus (baitides)		Vaikeväärtused
		Min.	Maks.	
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 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruse esitamiseks, on kirjete arvu minimaal- ja maksimumväärtused, mida ettevõttekaardi andmestruktuur peab kasutama:

		Min.	Maks.
n8	NoOfCompanyActivityRecords	230	520

3. liide

PIKTOGRAMMID

PIC_001 Sõidumeerik võib kasutada järgmisi piktogramme ja piktogrammikombinatsioone:






1. PEAMISED PIKTOGRAMMID

	Inimesed	Tegevused	Toimimismoodused
	Ettevõtte		Ettevõtetemoodus
	Kontrollija	Kontrollimine	Kontrollimoodus
	Juht	Juhtimine	Tavamoodus
	Töökoda/katsejaam	Ülevaatus/kalibreerimine	Kalibreerimismoodus
	Tootja		
	Tevékenységék	Kestus	
	Valmisolek	Käesolev valmisolekuaeg	
	Juhtimine	Pidev juhtimisaeg	
	Puhkus	Käesolev puhkeaeg	
	Töö	Käesolev tööaeg	
	Vaheaeg	Kumulatiivne vaheaeg	
	Teadmata		
	Seade	Funktsioonid	
	Juhikaardi ava		
	Kaasjuhi kaardi ava		
	Kaart		
	Kell		
	Kuvar	Kuvamine	
	Välissalvestus	Allalaadimine	
	Toiteallikas		
	Printer/väljatrukk	Trükkimine	
	Andur		
	Rehvi suurus		
	Sõiduk/sõidukiüksus		
	Eritingimused		
	Sõidumeerik mittevajalik		
	PRAAMI-/RONGISÕIT		
	Muud		
	Sündmused		Rikked
	Tööpäeva algus		Tööpäeva lõpp
	Asukoht		Juhi tegevuste kohta käsitsi tehtavad sissekanded
	Turvalisus		Kiirus
	Aeg		Kokku/kokkuvõte
	Täpsustid		
	Päeva kohta		
	Nädala kohta		
	Kahe nädala kohta		
	Alates või kuni		




2. PIKTOGRAMMIKOMBINATSIOONID

Muud	
	Kontrolli koht
	Tööpäeva alguskoht
	Alates
	Sõidukist
	Sõidumeerik mittevajalik — algus
	Tööpäeva lõppkoht
	Kuni
	Sõidumeerik mittevajalik — lõpp







Kaardid

	Juhikaart
	Ettevõttekaart
	Kontrollikaart
	Töökojakaart
	Kaardi number













Juhtimine

	Juhib meeskond
	Juhtimisaeg ühes nädalas
	Juhtimisaeg kahes nädalas








Väljatrükkid

	Juhi ühe päeva tegevuste väljatrükk kaardilt
	Juhi ühe päeva tegevuste väljatrükk sõidukiüksusest
	Sündmuste ja rikete väljatrükk kaardilt
	Sündmuste ja rikete väljatrükk sõidukiüksusest
	Tehniliste andmete väljatrükk
	Kiiruse ületamise väljatrükk






Sündmused

	Kehtetu kaardi sisestamine
	Kaardikonflikt
	Aja kattumine
	Vajaliku kaardita juhtimine
	Kaardi sisestamine juhtimise ajal
	Viimane kaardiseanss nõuetekohaselt sulgemata
	Kiiruse ületamine
	Toiteallika katkestus
	Liikumisandmete viga
	Turbemurre
	Aja korrigeerimine (töökojas)
	Kiiruse ületamise kontroll

Rikked

	Kaardirike (juhikaardi avas)
	Kaardirike (kaasjuhi kaardi avas)
	Kuvaririke
	Allalaadimisriike
	Printeririke
	Sensoririke
	Sõidukiüksuse siserike

Käsitsi tehtavad sissekanded

	Kas on veel sama tööpäev?
	Eelmise tööaja lõpp?
	Kinnita või sisesta tööaja lõpukoht
	Sisesta algusaeg
	Sisesta tööaja alguskoht

Märkus: väljatrükiploki või kirjeidentifikaatori moodustamiseks kasutatavad lisapiktogrammikombinatsioonid on määratletud 4. liites.

4. liide

VÄLJATRÜKID

SISUKORD

1.	Üldosa	409
2.	Andmeplokkide spetsifikaat	409
3.	Väljatrüki spetsifikaat	415
3.1.	Juhi ühe päeva tegevuste väljatrükk kaardilt	416
3.2.	Juhi ühe päeva tegevuste väljatrükk sõidukiüksusest	416
3.3.	Sündmuste ja rikete väljatrükk kaardilt	417
3.4.	Sündmuste ja rikete väljatrükk sõidukiüksusest	417
3.5.	Tehniliste andmete väljatrükk	418
3.6.	Kiiruse ületamise väljatrükk	418

1. ÜLDOSA

Iga väljatrükk moodustatakse, aheldades erinevaid andmeplokke, mida võimaluse korral idenditakse plokiidentifikaatoriga.

Andmeplokk koosneb ühest või mitmest kirjest, mida võimaluse korral idenditakse kirjeidentifikaatoriga.

- PRT_001 Kui plokiidentifikaator eelneb vahetult kirjeidentifikaatorile, kirjeidentifikaatorit ei trükitata.
- PRT_002 Juhul kui andmeühik on tundmata või kui seda ei pea andmepäasuõiguste tõttu trükkima, trükitakse selle asemel tühi-
kud.
- PRT_003 Kui terve rea sisu on tundmata või kui seda ei pea trükkima, jäetakse terve rida välja.
- PRT_004 Numbrilised andmeväljad trükitakse paremjoondatult, tühikud eraldavad tuhandeid ja miljoneid ning eesnull puudub.
- PRT_005 Stringiandmeväljad trükitakse vasakjoondatult ning täidetakse andmeühiku pikkuse ulatuses nullidega või kärbitakse vajaduse korral andmeühiku pikkuseni (nimed ja aadressid).

2. ANDMEPLOKKIDE SPETSIFIKAAT

Käesolevas peatükis on kasutatud järgmisi vormingu märkimistavasid:

- rasvases kirjas trükitud märgid tähistavad trükitavat lihtteksti (trükitakse tavalised märgid),
- tavalised märgid tähistavad muutujaid (piktogrammide või andmed), mis trükkimisel asendatakse nende väärtustega,
- muutujate nimed on täidetud allakriipsutustega, näitamaks andmeühiku pikkust, mida muutuja saab kasutada,
- kuupäevad on määratletud vormingus “pp/kk/aaaa” (päev, kuu, aasta). Võib kasutada ka vormingut “pp.kk.aaaa”,
- termin “kaardi identimine” koosneb järgmistest elementidest: kaarditüüp kaardipiktogrammide kombinatsiooni näol, kaardi väljaandnud liikmesriigi kood, ettepoole viltu kaldjoonemärk ja kaardinumber koos asendusindeksi ja uuendusindeksiga, mis on eraldatud tühikuga:

P	█	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kaardi piktogrammi- kombinatsioon		Väljaandnud liikmesriigi kood				Kaardi numbri esimesed 14 märki (võimaluse korral koos järjestikuse indeksiga)															Asendusindeks		Uuendusindeks	

- PRT_006 Väljatrükkidel kasutatakse järgmisi andmeplokke ja/või andmekirjeid vastavalt järgmistele tähendustele ja vormingutele:

Plokk või kirjenumbr
Tähendus

Andmete vorming

1. Dokumendi trükkimise kuupäev ja kellaeg

☐ dd/mm/yyyy hh:mm (UTC)

2. **Väljatrüki tüüp**
Plokiidentifikaator
Väljatrüki piktogrammikombinatsioon (vt 3. liide) , kiiruspüüriku seadistus (ainult kiiruse ületamise väljatrükk)
3. **Kaardi omaniku identifikatsioon**
Plokiidentifikaator. P = inimeste piktogramm
Kaardi omaniku perekonnanimi
Kaardi omaniku eesnimi (eesnimed) (kui on olemas)
Kaardi identifikatsioon
Kaardi kehtivusaja lõpp (kui on olemas)
Kui kaart ei ole isikustatud ja sellel ei ole kaardi omaniku perekonnanime, tuleb selle asemel trükkida ettevõtte või töökoja või kontrolliasutuse nimi.
4. **Sõiduki identifikatsioon**
Plokiidentifikaator
Valmistajatehase tähis (VIN)
Registreeritud liikmesriik ja sõiduki registreerimisnumber
5. **Sõidukiüksuse identifikatsioon**
Plokiidentifikaator
Sõidukiüksuse tootja nimi
Sõidukiüksuse osa number
6. **Sõidumeeriku viimane kalibreerimine**
Plokiidentifikaator
Töökoja nimi
Töökojakaardi identifikatsioon
Kalibreerimise kuupäev
7. **Viimane kontrollimine (kontrolliametniku poolt)**
Plokiidentifikaator
Kontrollikaardi identifikatsioon
Kontrolli kuupäev, aeg ja tüüp
Kontrollitüüp: kuni neli piktogrammi. Kontrollitüüp võib olla järgmine (või kombinatsioon neist):
☐: kaardilt allalaadimine, ☒: sõidukiüksusest allalaadimine,
☒: trükkimine, ☐: kuvamine.
8. **Toimumise järjestuses salvestatud juhi tegevused kaardil**
Plokiidentifikaator
Päringu kuupäev (kalendripäev väljatrüki alusel) + kaardi igapäevase kohaloleku lugeja
- 8.1. *Aeg, mille jooksul kaart ei olnud sisestatud*
- 8.1a. Kirjeidentifikaator (algusaeg)
- 8.1b. *Teadmata aeg.* Algus- ja lõpuaeg, kestus
- 8.1c. *Tegevus käsitsi sisestatud*
Tegevuse piktogramm, algus- ja lõpuaeg (kaasa arvatud), kestus, vähemalt ühe tunni pikkused puhkeajad on tähistatud tärniga.

-----☒-----
Picto xxx km/h

-----P-----
P Last_Name _____
First_Name _____
Card_Identification _____
dd/mm/yyyy

-----☒-----
☒ VIN _____
Nat/VRN _____

-----☒-----
☒ VU_Manufacturer _____
VU_Part_Number _____

-----☒-----
☒ Last_Name _____
Card_Identification _____
☒ dd/mm/yyyy

-----☒-----
Card_Identification _____
☒ dd/mm/yyyy hh:mm pppp

-----☒-----
dd/mm/yyyy xxx

☒ hh:mm hh:mm hh:mm
A hh:mm hh:mm hh:mm *

- 8.2. *Kaardi sisestamine avasse S*
Kirjeidentifikaator; S = ava piktogramm
Registreerinud liikmesriik ja sõiduki registreerimisnumber
Sõiduki läbisõidumeeriku näit kaardi sisestamisel
- 8.3. *Tegevus (kui kaart oli sisestatud)*
Tegevuse piktogramm, algus- ja lõpuaeg (kaasa arvatud), kestus, meeskonna staatus (meeskonna piktogramm, kui MEESKOND, tühikud, kui ÜKSI), vähemalt ühe tunni pikkused puhkeajad on tähistatud tärniga.
- 8.3a. *Eritingimus. Sisestusaeg, eritingimuse piktogramm (või piktogrammikombinatsioon)*
- 8.4. *Kaardi väljavõtmine*
Sõiduki läbisõidumõõdiku väärtus ja läbitud vahemaa pärast viimast sisestamist, mille kohta on läbisõidumõõdiku väärtus teada
9. **Sõidukiüksuses ava kohta toimumise järjestuses salvestatud juhi tegevused**
Plokiidentifikaator
Päringu kuupäev (kalendripäev väljatrüki alusel)
Sõiduki läbisõidumeeriku näit kell 00:00 ja 24:00
10. **Tegevused avas S**
Plokiidentifikaator
- 10.1. *Aeg, mil avasse S ei olnud ühtki kaarti sisestatud*
Kirjeidentifikaator
Ühtki kaarti pole sisestatud
Sõiduki läbisõidumeeriku näit aja alguses
- 10.2. *Kaardi sisestamine*
Kaardi sisestamiskirje identifikaator
Juhi nimi
Juhi eesnimi
Juhikaardi identifitseerimine
Juhikaardi kehtivuse lõpukuupäev
Eelmise kasutatud sõiduki registreerinud liikmesriik ja registreerimisnumber
Eelmisest sõidukist kaardi väljavõtmise kuupäev ja kellaaeg
Tühi rida
Sõiduki läbisõidumõõdiku näit kaardi sisestamisel, tunnus juhi tegevuste käsitsi sisestamise kohta (M — jah, tühi — ei)
- 10.3. *Tegevus*
Tegevuse piktogramm, algus- ja lõpuaeg (kaasa arvatud), kestus, meeskonna staatus (meeskonna piktogramm, kui MEESKOND, tühikud, kui ÜKSI), vähemalt ühe tunni pikkused puhkeajad on tähistatud tärniga.

-----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. *Eritingimus. Sisestusaeg, eritingimuse piktogramm (või piktogrammikombinatsioon)*
- hh:mm ----- pppp -----
- 10.4. *Kaardi väljavõtmine või "Kaart puudub"-aja lõpp*
Sõiduki läbisõidumõõdiku näit kaardi väljavõtmisel või "kaart puudub"-aja lõpus ja sisestamisest alates või "kaart puudub"-aja algusest läbitud vahemaa
- x xxx xxx km; x xxx km
11. **Päeva kokkuvõte**
 Plokiidentifikaator
- Σ -----
- 11.1. *Sõidukiüksuse kokkuvõte aegadest, mil juhikaardi avas kaarti ei olnud*
 Plokiidentifikaator
- 100 - - -
- 11.2. *Sõidukiüksuse kokkuvõte aegadest, mil kaasjuhi kaardi avas kaarti ei olnud*
 Plokiidentifikaator
- 200 - - -
- 11.3. *Sõidukiüksuse päeva kokkuvõte juhi kohta*
 Kirjeidentifikaator
 Juhiperkonnanimi
 Juhiesnimi (eesnimed)
 Juhikaardi identifikaatsioon
- ☐ Last_Name _____
 First_Name _____
 Card_Identification _____
- 11.4. *Sissekanne tööpäeva algus- ja/või lõpukoha kohta*
 pi = algus/lõpukoha piktogramm, aeg, riik, piirkond
 Läbisõidumõõdik
- pihh:mm Cou Reg
 x xxx xxx km
- 11.5. *Tegevused kokku (kaardilt)*
 Kogu juhtimisaeg, läbitud vahemaa
 Kogu töö- ja valmisolekuage
 Kogu puhke- ja teadmata aeg
 Meeskonnategevuste kogu kestus
- ☐ hhhmm x xxx km
 ✖ hhhmm ☐ hhhmm
 † hhhmm ? hhhmm
 ☐☐ hhhmm
- 11.6. *Tegevusi kokku (ilma kaardita ajad juhikaardi avas)*
 Kogu juhtimisaeg, läbitud vahemaa
 Kogu töö- ja valmisolekuage
 Kogu puhkeage
- ☐ hhhmm x xxx km
 ✖ hhhmm ☐ hhhmm
 † hhhmm
- 11.7. *Tegevused kokku (ilma kaardita ajad kaasjuhi kaardi avas)*
 Kogu töö- ja valmisolekuage
 Kogu puhkeage
- ✖ hhhmm ☐ hhhmm
 † hhhmm

- 11.8. *Tegevused kokku (juhi kohta, arvestades mõlemaid avasid)*
 Kogu juhtimisaeg, läbitud vahemaa
 Kogu juhtimisaeg, läbitud vahemaa
 Kogu puhkeaeg
 Meeskonnategevuste kogu kestus
 Kui nõutakse päevast väljatrükki jooksva päeva kohta, arvutatakse päeva kokkuvõtte trükkimise ajal olemasolevate andmete alusel.
12. **Kaardile salvestatud sündmused ja/või rikked**
- 12.1. Plokiidentifikaator viimased 5 "sündmust ja riket" kaardilt
- 12.2. Plokiidentifikaator kõik registreeritud "sündmused" kaardil
- 12.3. Plokiidentifikaator kõik registreeritud "rikked" kaardil
- 12.4. *Sündmuse- ja/või rikkekirje*
 Kirjeidentifikaator
 Sündmuse/rikke piktogramm, kirje eesmärk, alguse kuupäev ja kellaeg
 Sündmuse/rikke lisakood (kui see on olemas), kestus
 Sõiduki, milles sündmus või rike toimus, registreerimisnumber ja registreerinud liikmesriik
13. **Sõidukiüksusesse salvestatud või seal kestvad sündmused ja/või rikked**
- 13.1. Plokiidentifikaator viimased 5 "sündmust ja riket" sõidukiüksusest
- 13.2. Plokiidentifikaator kõik sõidukiüksuses registreeritud või kestvad "sündmused"
- 13.3. Plokiidentifikaator kõik sõidukiüksuses registreeritud või kestvad "rikked"
- 13.4. *Sündmuse- ja/või rikkekirje*
 Kirjeidentifikaator
 Sündmuse/rikke piktogramm, kirje eesmärk, alguse kuupäev ja kellaeg
 Sündmuse/rikke lisakood (kui see on olemas), sarnaste sündmuste arv sellel päeval, kestus
 Sündmuse või rikke alguses või lõpus sisestatud kaartide identifikatsioon (kuni 4 rida, kordamata samu kaardinumbreid)
 Sündmus, mil ühtki kaarti polnud sisestatud
 Kirje eesmärk (p) on numbrikood, mis selgitab, miks sündmus või rike registreeriti ning see on kodeeritud vastavalt andmeelemendile EventFaultRecordPurpose
- hhmm x xxx km
 hhmm hhmm
 hhmm
 hhmm
- ! x -----
- ! -----
- x -----
- Pic dd/mm/yyyy hh:mm
 ! xxx hhmm
 Nat/VRN _____
- ! A -----
- ! A -----
- x A -----
- Pic (p) dd/mm/yyyy hh:mm
 ! xxx (xxx) hhmm
 Card_Identification _____
 Card_Identification _____
 Card_Identification _____
 Card_Identification _____
 A ---

14. **Sõidukiüksuse identifitseerimine**

Plokiidentifikaator
 Sõidukiüksuse tootja nimi
 Sõidukiüksuse tootja aadress
 Sõidukiüksuse osa number
 Sõidukiüksuse tüübikinnitusnumber
 Sõidukiüksuse seerianumber
 Sõidukiüksuse tootmisaja
 Sõidukiüksuse tarkvaraversiooni ja selle installeerimise kuupäev

```

-----
! Name _____
  Address _____
  PartNumber _____
  Apprv _____
  S/N _____
  yyyy
  v   xx.xx.xx  dd/mm/yyyy
  
```

15. **Sensori identifitseerimine**

Plokiidentifikaator
 Sensori seerianumber
 Sensori tüübikinnitusnumber
 Sensori esimese paigalduse kuupäev

```

-----
! S/N _____
  Apprv _____
  dd/mm/yyyy
  
```

16. **Kalibreerimisandmed**

Plokiidentifikaator

```

-----
T
  
```

16.1. *Kalibreerimiskirje*

Kirjeidentifikaator
 Kalibreerimise teinud töökoda
 Töökoja aadress
 Töökojakaardi identifitseerimine
 Töökojakaardi kehtivuse lõpukuupäev
 Tühi rida
 Kalibreerimise kuupäev + kalibreerimise eesmärk
 Valmistajatehase tähis (VIN)
 Registreeritud liikmesriik ja sõiduki registreerimisnumber
 Sõidukit iseloomustav koefitsient
 Sõidumeeriku konstant
 Rattarehvide efektiivüumbermõõt
 Paigaldatud rehvide mõõtmed
 Kiiruspiiriku seadistus
 Läbisõidumõõdiku uus ja vana näit
 Kalibreerimise eesmärk (p) on numbrikood, mis selgitab, miks need kalibreerimisparameetrid registreeriti, ning see on kodeeritud vastavalt andmelelembile CalibrationPurpose.

```

-----
T Workshop_name _____
  Workshop_address _____
  Card-Identification _____
  dd/mm/yyyy

T dd/mm/yyyy (p)
! VIN _____
  Nat/VRN _____
w xx xxx Imp/km
k xx xxx Imp/km
l xx xxx mm
• TyreSize _____
> xxx km/h
x xxx xxx - x xxx xxx km
  
```

17. **Aja korrigeerimine**

Plokiidentifikaator

```

-----
!
  
```

17.1. *Aja korrigeerimise kirje*

Kirjeidentifikaator
 Vana kuupäev ja kellaaeg
 Uus kuupäev ja kellaaeg
 Aega korrigeeritud töökoda
 Töökoja aadress
 Töökojakaardi identifitseerimine
 Töökojakaardi kehtivuse lõpukuupäev

```

-----
! ! dd/mm/yyyy hh:mm
  ! dd/mm/yyyy hh:mm
T Workshop_name _____
  Workshop_address _____
  Card-Identification _____
  dd/mm/yyyy
  
```


18. **Sõidukiüksuses registreeritud viimane sündmus ja rike**

Plokiidentifikaator

Viimase sündmuse kuupäev ja kellaaeg

Viimase rikke kuupäev ja kellaaeg

```

----- ! x A -----
!  jj/mm/aaaa  hh:mm
x  jj/mm/aaaa  hh:mm

```

19. **Teave kiiruse ületamise kontrolli kohta**

Plokiidentifikaator

Viimase KIIRUSE ÜLETAMISE KONTROLLI kuupäev ja kellaaeg

Esimese kiiruse ületamise kuupäev/aeg ja kiiruse ületamise sündmuste arv pärast seda

```

----- >> -----
>  dd/mm/yyyy  hh:mm
>> dd/mm/yyyy  hh:mm (nnn)

```

20. **Kiiruse ületamise kirje**

20.1. Plokiidentifikaator "esimene kiiruse ületamine pärast viimast kalibreerimist"

```

----- >> T -----

```

20.2. Plokiidentifikaator "5 kõige tõsisemat kiiruse ületamise sündmust viimase 365 päeva jooksul"

```

----- >> (365) -----

```

20.3. Plokiidentifikaator "viimase kümne päeva jooksul toimunud iga päeva kõige tõsisem kiiruse ületamise sündmus"

```

----- >> (10) -----

```

20.4. Kirjeidentifikaator

Kuupäev, aeg ja kestus

Maksimaalne ja keskmine kiirus, sarnaste sündmuste arv sellel päeval

Juhi perekonnanimi

Juhi eesnimi (eesnimed)

Juhikaardi identifitseerimine

```

-----
>> dd/mm/yyyy hh:mm hh:mm
xxx km/h xxx km/h (xxx)
@ Last_Name _____
  First_Name _____
Card_Identification _____

```

20.5. Kui plokis pole ühtki kiiruse ületamise kirjet

```

>> - - -

```

21. **Käsitsi kirjutatud teave**

Plokiidentifikaator

21.1. Kontrolli koht

21.2. Kontrollija allkiri

21.3. Alates

21.4. Kuni

21.5. Juhi allkiri

"Käsitsi kirjutatud teave": käsitsi tehtava kande kohale jäetakse piisavalt tühje ridu, et sinna saaks nõutava teabe või allkirja kirjutada.

```

-----
@ * .....
@ .....
@ + .....
+ @ .....
@ .....

```

3. **VÄLJATRÜKI SPETSIFIKAAT**

Käesolevas peatükis on kasutatud järgmisi märkimistavasid:

N
N
X/Y

Trükiploki- või kirjenumber N

Trükiploki- või kirjenumber N, seda korratakse nii palju kui vaja

Trükiplokid või -kirjed X ja/või Y vastavalt vajadusele ning seda korratakse nii palju kui vaja

3.1. Juhi ühe päeva tegevuste väljatrükk kaardilt

PRT_007 Juhi ühe päeva tegevuste väljatrükk kaardilt vastab järgmisele vormingule:

1	Dokumendi trükkimise kuupäev ja kellaeg
2	Väljatrüki tüüp
3	Kontrollija identifitseerimine (kui sõidukiüksusesse on sisestatud kontrollikaart)
3	Juhi identifitseerimine (kaardilt, millelt tehakse väljatrükk)
4	Sõiduki identifitseerimine (sõidukist, millest tehakse väljatrükk)
5	Sõidukiüksuse identifitseerimine (sõidukiüksusest, millest tehakse väljatrükk)
6	Selle sõidukiüksuse viimane kalibreerimine
7	Kontrollitava juhi eelmine kontrollimine
8	Juhi tegevuste eraldaja
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Juhi tegevused toimumisjärjestuses
11	Päevase kokkuvõtte eraldaja
11.4	Sisestatud kohad kronoloogilises järjestuses
11.5	Tegevused kokku
12.1	Kaardil olevate sündmuste ja rikete eraldaja
12.4	Sündmuse-/rikkekirjed (kaardile salvestatud 5 viimast sündmust või riket)
13.1	Sõidukiüksuses olevate sündmuste ja rikete eraldaja
13.4	Sündmuse-/rikkekirjed (sõidukiüksusesse salvestatud või seal kestvat 5 viimast sündmust või riket)
21.1	Kontrolli koht
21.2	Kontrollija allkiri
21.5	Juhi allkiri

3.2. Juhi ühe päeva tegevuste väljatrükk sõidukiüksusest

PRT_008 Juhi ühe päeva tegevuste väljatrükk sõidukiüksusest vastab järgmisele vormingule:

1	Dokumendi trükkimise kuupäev ja kellaeg
2	Väljatrüki tüüp
3	Kaardiomaniku identifitseerimine (iga kaardi identifitseerimine, mis on sisestatud sõidukiüksusesse)
4	Sõiduki identifitseerimine (sõidukist, millest tehakse väljatrükk)
5	Sõidukiüksuse identifitseerimine (sõidukiüksusest, millest tehakse väljatrükk)
6	Selle sõidukiüksuse viimane kalibreerimine
7	Selle sõidumeeriku viimane kontrollimine
9	Juhi tegevuste eraldaja
10	Juhikaardi ava eraldaja (ava 1)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Tegevused kronoloogilises järjestuses (juhikaardi ava)
10	Kaasjuhi kaardi ava eraldaja (ava 2)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Tegevused kronoloogilises järjestuses (kaasjuhi kaardi ava)
11	Päevase kokkuvõtte eraldaja
11.1	Kokkuvõtte aegadest, mil juhikaardi avas kaarti ei olnud
11.4	Sisestatud kohad kronoloogilises järjestuses
11.6	Tegevused kokku

11.2	Kokkuvõtte aegadest, mil kaasjuhi kaardi avas kaarti ei olnud
11.4	Sisestatud kohad kronoloogilises järjestuses
11.7	Tegevused kokku
11.3	Juhi tegevused kokku, arvestades mõlemaid avasid
11.4	Selle juhi sisestatud kohad kronoloogilises järjestuses
11.7	Selle juhi tegevused kokku
13.1	Sündmuste ja rikete eraldaja
13.4	Sündmuse-/rikkekirjed (sõidukiüksusesse salvestatud või seal kestvat 5 viimast sündmust või riket)
21.1	Kontrolli koht
21.2	Kontrollija allkiri
21.3	Alates (koht juhi tarvis, kellel ei ole kaarti, et ta saaks ära näidata temaga seotud ajad)
21.4	Kuni
21.5	Juhi allkiri

3.3. Sündmuste ja rikete väljatrükk kaardilt

PRT_009 Sündmuste ja rikete väljatrükk kaardilt vastab järgmisele vormingule:

1	Dokumendi trükkimise kuupäev ja kellaeg
2	Väljatrüki tüüp
3	Kontrollija identifitseerimine (kui sõidukiüksusesse on sisestatud kontrollikaart)
3	Juhi identifitseerimine (kaardilt, millelt tehakse väljatrükk)
4	Sõiduki identifitseerimine (sõidukist, millest tehakse väljatrükk)
12.2	Sündmuste eraldaja
12.4	Sündmusekirjed (kõik kaardile salvestatud sündmused)
12.3	Rikete eraldaja
12.4	Rikked (kõik kaardile salvestatud rikked)
21.1	Kontrolli koht
21.2	Kontrollija allkiri
21.5	Juhi allkiri

3.4. Sündmuste ja rikete väljatrükk sõidukiüksusest

PRT_010 Sündmuste ja rikete väljatrükk sõidukiüksusest vastab järgmisele vormingule:

1	Dokumendi trükkimise kuupäev ja kellaeg
2	Väljatrüki tüüp
3	Kaardi omaniku identifitseerimine (iga kaardi identifitseerimine, mis on sisestatud sõidukiüksusesse)
4	Sõiduki identifitseerimine (sõidukist, millest tehakse väljatrükk)
13.2	Sündmuste eraldaja
13.4	Sündmusekirjed (kõik sõidukiüksusesse salvestatud või seal kestvad sündmused)
13.3	Rikete eraldaja
13.4	Rikked (kõik sõidukiüksusesse salvestatud või seal kestvad rikked)
21.1	Kontrolli koht
21.2	Kontrollija allkiri
21.5	Juhi allkiri

3.5. Tehniliste andmete väljatrükk

PRT_011 Tehniliste andmete väljatrükk vastab järgmisele vormingule:

1	Dokumendi trükkimise kuupäev ja kellaeg
2	Väljatrüki tüüp
3	Kaardi omaniku identifkatsioon (iga kaardi identifkatsioon, mis on sisestatud sõidukiüksusesse)
4	Sõiduki identifkatsioon (sõidukist, millest tehakse väljatrükk)
14	Sõidukiüksuse identifkatsioon
15	Sensori identifkatsioon
16	Kalibreerimisandmete eraldaja
16.1	Kalibreerimiskirjed (kõik olemasolevad kirjed kronoloogilises järjestuses)
17	Aja korrigeerimise eraldaja
17.1	Aja korrigeerimise kirjed (kõik olemasolevad kirjed aja korrigeerimise ja kalibreerimisandmete kirjetest)
18	Sõidukiüksuses registreeritud viimane sündmus ja rike

3.6. Kiiruse ületamise väljatrükk

PRT_012 Kiiruse ületamise väljatrükk vastab järgmisele vormingule:

1	Dokumendi trükkimise kuupäev ja kellaeg
2	Väljatrüki tüüp
3	Kaardi omaniku identifkatsioon (iga kaardi identifkatsioon, mis on sisestatud sõidukiüksusesse)
4	Sõiduki identifkatsioon (sõiduki, millelt tehakse väljatrükk)
19	Teave kiiruse ületamise kontrolli kohta
20.1	Kiiruse ületamise andmete eraldaja
20.4 / 20.5	Esimene kiiruse ületamine pärast viimast kalibreerimist
20.2	Kiiruse ületamise andmete eraldaja
20.4 / 20.5	5 kõige tõsisemat kiiruse ületamise sündmust viimase 365 päeva jooksul
20.3	Kiiruse ületamise andmete eraldaja
20.4 / 20.5	Viimase kümne päeva jooksul toimunud iga päeva kõige tõsisem kiiruse ületamine
21.1	Kontrolli koht
21.2	Kontrollija allkiri
21.5	Juhi allkiri

5. liide

KUVAMINE

Käesolevas liites on kasutatud järgmisi vormingu märkimistavasid:

- poolpaks kiri tähistab kuvatavat lihtteksti (kuvaril ei kasutata poolpaksu kirja),
- harilik kiri tähistab muutujaid (piktogrammide või andmed), mis kuvamisel asendatakse nende väärtusega,
 - dd mm yyyy: päev, kuu, aasta,
 - hh: tunnid,
 - mm: minutid,
 - D: kestust tähistav piktogramm,
 - EF: sündmuse- või rikkepiktogrammide kombinatsioon,
 - O: toimimismooduse piktogramm.

DIS_001 Sõidumeerik kuvab andmeid, kasutades järgmisi vorminguid:

Andmed	Vorming
Vaikekuva	
Kohalik aeg	hh:mm
Toimimismoodus	O
Juhiga seotud teave	1 Dhhmm hhmm
Kaasjuhiga seotud teave	2 Dhhmm
Tingimus "sõidumeerik mittevajalik" avatud	OUT
Hoiatuskuva	
Pideva juhtimisaja ületamine	1 0hhmm hhmm
Sündmus või rike	EF
Muud kuvad	
GMT kuupäev	UTC 0dd/mm/yyyy vi UTC 0dd.mm.yyyy
kellaaeg	hh:mm
Juhi pidev juhtimisaeg ja kumulatiivne vaheaeg	1 0hhmm hhmm
Kaasjuhi pidev juhtimisaeg ja kumulatiivne vaheaeg	2 0hhmm hhmm
Juhi kumulatiivne juhtimisaeg eelmisel ja jooksva nädalal	1 0 hhmm
Kaasjuhi kumulatiivne juhtimisaeg eelmisel ja jooksva nädalal	2 0 hhmm

6. liide

VÄLISLIIDESED

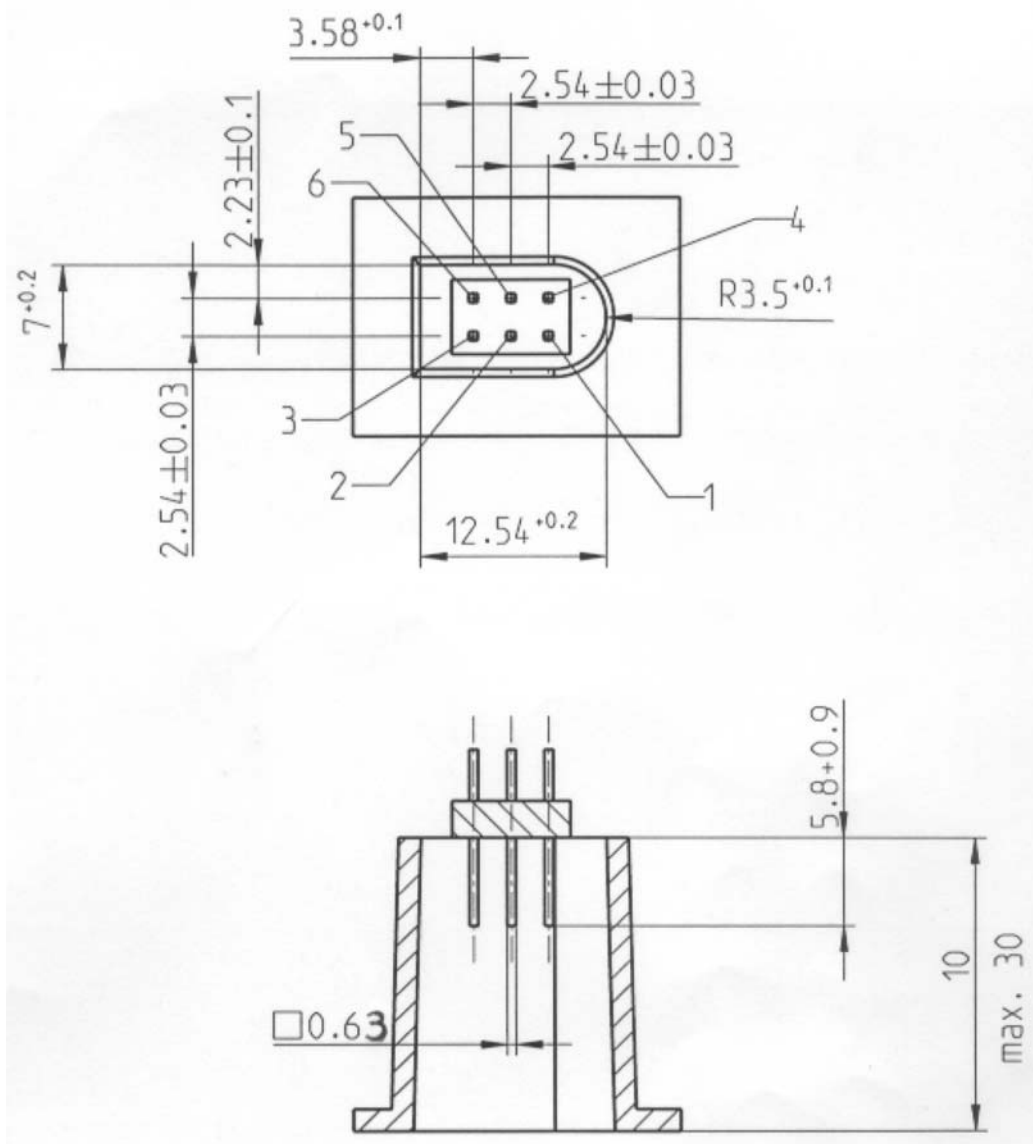
SISUKORD

1.	Riistvara	422
1.1.	Pistik	422
1.2.	Kontakti asukoht	424
1.3.	Plokkskeem	424
2.	Allalaadimisliides	424
3.	Kalibreerimisliides	425

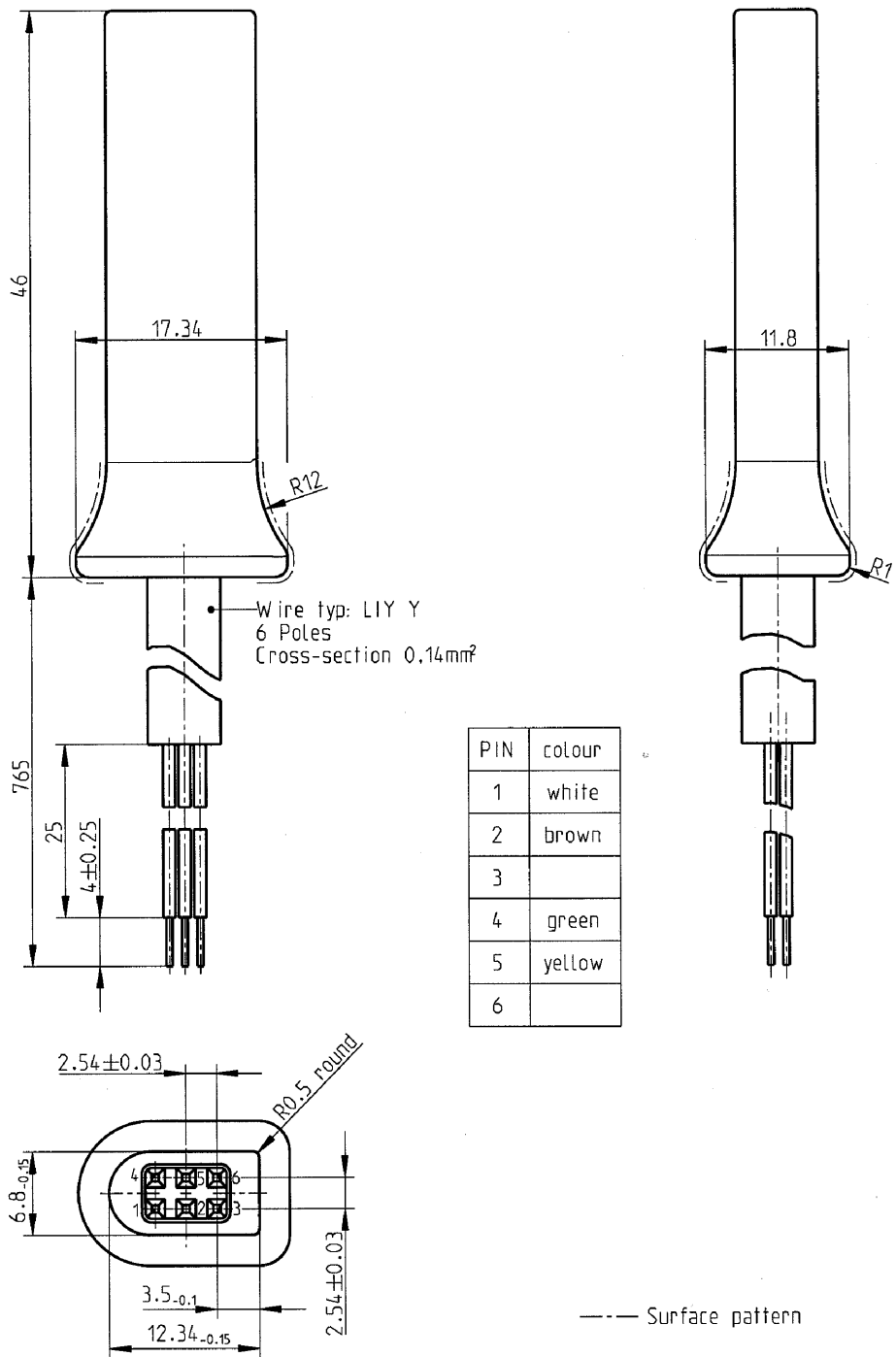
1. RIISTVARA

1.1. Pistik

INT_001 Allalaadimis-/kalibreerimis pistik, millele on juurdepääs esipaneelil, kusjuures selleks ei tule ühtki söidumeeriku osa lahti ühendada, ning see vastab järgmisele joonisele (kõik mõõtmed on millimeetrites):



Järgmisel skeemil on tüüpiline kuue kontaktiga liitepistik:



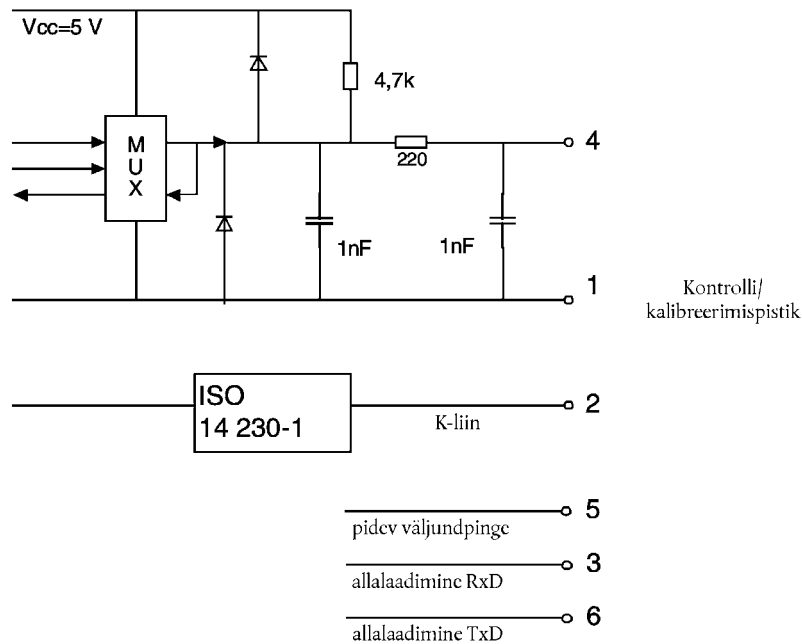
1.2. Kontaktide paigutus

INT_002 Kontaktid paigutatakse vastavalt järgmisele tabelile:

Kontakt	Kirjeldus	Märkus
1	Aku miinuspoolus	Ühendatud sõiduki aku miinuspoolusega
2	Andmeside	K-liin (ISO 14 230-1)
3	RxD — Allalaadimine	Andmete sisend sõidumeerikusse
4	Sisend-/väljundsignaal	Kalibreerimine
5	Pidev väljundpinge	Arvestades seadme kaitseelektronika tekitatud pingelangust, on pingevalutus määratletud kui sõiduki pinge miinus 3V Väljund 40 mA
6	TxD — Allalaadimine	Andmete väljund sõidumeerikust

1.3. Plokkskeem

INT_003 Plokkskeem peab olema järgmine:



2. ALLALAADIMISLIIDES

INT_004 Allalaadimisliides vastab standardi RS232 spetsifikaatidele.

INT_005 Allalaadimisliides kasutab ühte algusbitti, kaheksat andmebiti (kõige vähem tähtis bitt esimesena), ühte paarsusbitti ja ühte lõpubitti.



Andmebaidi ülesehitus

Algusbitt: üks bitt, mille loogikatase on null

Andmebitid: edastatakse kõige vähem tähtis bitt esimesena

Paarsusbitt: paarisus

Lõpubitt: üks bitt, mille loogikatase on üks

Kui edastatakse numbrilisi andmeid, mis koosnevad rohkem kui ühest baidist, edastatakse kõige tähtsam bait esimesena ja kõige vähem tähtis bait viimasena.

INT_006 Edastamiskiirust saab reguleerida vahemikus 9 600 kuni 115 200 bitti sekundis. Edastamisel kasutatakse võimalikult suurt edastamiskiirust, kuid alguskiirus pärast ühenduse loomist on reguleeritud 9 600 bitti sekundis.

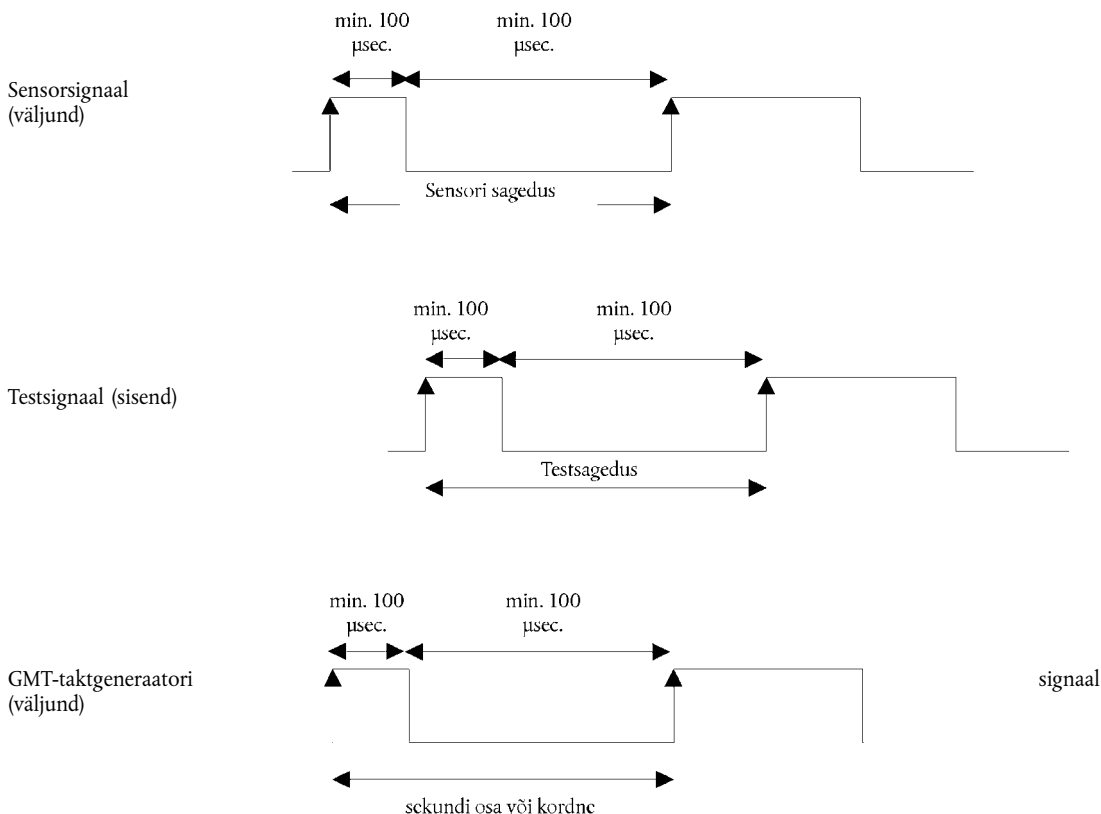
3. KALIBREERIMISLIIDES

INT_007 Andmeside vastab standardile ISO 14.230-1 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 1: Physical layer, First edition: 1999. (Maanteesõidukid — Diagnostilised süsteemid — Võtmesõnaprotokoll 2000 — 1. osa: Füüsiline kiht, esimene väljaanne, 1999.)

INT_008 Sisend-/väljundsignaal vastab järgmisele elektrilisele spetsifikaadile:

Parameeter	Minimaalne	Tüüpiline	Maksimaalne	Märkus
U_{low} (sisend)			1,0 V	$I = 750 \mu A$
U_{high} (väljund)	4 V			$I = 200 \mu A$
Sagedus			4 kHz	
U_{low} (sisend)			1,0 V	$I = 1 \text{ mA}$
U_{high} (väljund)	4 V			$I = 1 \text{ mA}$

INT_009 Sisend-/väljundsignaal vastab järgmistele ajastusskeemidele:



7. liide

ANDMETE ALLALAADIMISPROTOKOLLID

SISUKORD

1.	Sissejuhatus	428
1.1.	Kohaldamisala	428
1.2.	Lühendid ja märkused	428
2.	Sõidukiüksuses olevate andmete allalaadimine	429
2.1.	Allalaadimiskord	429
2.2.	Andmete allalaadimisprotokoll	429
2.2.1.	Sõnumi struktuur	429
2.2.2.	Sõnumitüübid	430
2.2.2.1.	Start communication request (SID 81)	432
2.2.2.2.	Positive response start communication (SID C1)	432
2.2.2.3.	Start diagnostic session request (SID 10)	432
2.2.2.4.	Positive response start diagnostic (SID 50)	432
2.2.2.5.	Link control service (SID 87)	432
2.2.2.6.	Link control positive response (SID C7)	432
2.2.2.7.	Request upload (SID 35)	432
2.2.2.8.	Positive response request upload (SID 75)	432
2.2.2.9.	Transfer data request (SID 36)	432
2.2.2.10.	Positive response transfer data (SID 76)	433
2.2.2.11.	Transfer exit request (SID 37)	433
2.2.2.12.	Positive response request transfer exit (SID 77)	433
2.2.2.13.	Stop communication request (SID 82)	433
2.2.2.14.	Positive response stop communication (SID C2)	433
2.2.2.15.	Acknowledge sub message (SID 83)	433
2.2.2.16.	Negative response (SID 7F)	433
2.2.3.	Sõnumivoog	434
2.2.4.	Ajastamine	435
2.2.5.	Vea töötlemine	435
2.2.5.1.	Side algusetapp	435
2.2.5.2.	Sideetapp	435
2.2.6.	Vastusesõnumi sisu	438
2.2.6.1.	Positive response transfer data overview	438
2.2.6.2.	Positive response transfer data activities	439
2.2.6.3.	Positive response transfer data events and faults	440

2.2.6.4.	Positive response transfer data detailed speed	441
2.2.6.5.	Positive response transfer data technical data	441
2.3.	Välisandmekandja faili salvestamine	442
3.	Sõidumeerikukaartidelt allalaadimise protokoll	442
3.1.	Kohaldamisala	442
3.2.	Mõisted	442
3.3.	Allalaadimine kaardilt	442
3.3.1.	Initsialiseerimisjada	443
3.3.2.	Allkirjastamata andmefailide jada	443
3.3.3.	Allkirjastatud andmefailide jada	443
3.3.4.	Kalibreerimislugeja lähtestusjada	444
3.4.	Andmete salvestusvorming	444
3.4.1.	Sissejuhatus	444
3.4.2.	Failivorming	444
4.	Sõidumeerikukaardilt allalaadimine sõidukiüksuse kaudu	445

1. SISSEJUHATUS

Käesolevas liites määratletakse kord, mida tuleb täita erinevate andmetüüpide allalaadimiseks välisandmekandjale, ja protokollid, mida tuleb rakendada, tagamaks andmete nõuetekohase edastuse ja allalaaditud andmete vormingu täieliku vastavuse, mis võimaldab mis tahes kontrollijal inspekteerida neid andmeid ning kontrollida enne analüüsimist nende autentsust ja terviklikkust.

1.1. Kohaldamisala

Andmeid võib alla laadida välisandmekandjale:

- sõidukiüksusest sõidukiüksusega ühendatud eriotstarbelise seadme (IDE) abil,
- sõidumeerikukaardilt eriotstarbelise seadme abil, millel on kaardiliidese seade (IFD),
- sõidumeerikukaardilt sõidukiüksuse kaudu sõidukiüksusega ühendatud eriotstarbelise seadme abil.

Andmaks võimaluse tõendada allalaaditud andmete, mis on salvestatud välisandmekandjale, autentsust ja terviklikkust, laaditakse andmed alla koos neile lisatud allkirjaga kooskõlas 11. liitega "Ühised turvemehhanismid". Samuti laaditakse alla allikseadme (sõidukiüksus või kaart) identifikatsioon ja selle turbesertifikaadid (liikmesriik ja seade). Andmete tõendaja peab sõltumatult omama usaldusväärset Euroopa avalikku võtit.

DDP_001 Ühe allalaadimiseseansi ajal allalaaditud andmed tuleb välisandmekandjal salvestada ühte faili.

1.2. Lühendid ja märkused

Käesolevas liites kasutatakse järgmisi lühendeid:

AID	(application identifier) rakenduse identifikaator
ATR	(answer to reset) lähtestuse vastus
CS	(checksum byte) kontrollsummabait
DF	(dedicated file) erifail
DS_	(diagnostic session) diagnostiline seanss
EF	(elementary file) elementaarfail
ESM	(external storage medium) välisandmekandja
FID	(file identifier) faili identifikaator
FMT	(format byte) vormingubait — sõnumipäise esimene bait
ICC	(integrated circuit card) kiipkaart
IDE	(intelligent dedicated equipment) eriotstarbeline seade. Seadet kasutatakse andmete allalaadimiseks välisandmekandjale (nt personaalarvuti).
IFD	(interface device) liideseseade
KWP	(keyword protocol 2000) võtmesõnaprotokoll 2000
LEN	(length byte) pikkusbait — sõnumipäise viimane bait
PPS	(protocol parameter selection) protokolliparameetri valik
PSO	(perform security operation) tee turbetoiming
SID	(service identifier) teenuse identifikaator
SRC	(source byte) lähtebait
TGT	(target byte) sihtbait
TLV	(tag length value) sildi pikkuse väärtus
TREP	(transfer response parameter) vastuse edastusparameeter
TRTP	(transfer request parameter) nõude edastusparameeter
VU	(vehicle unit) sõidukiüksus.

2. SÕIDUKIÜKSUSES OLEVATE ANDMETE ALLALAADIMINE

2.1. Allalaadimiskord

Sõidukiüksuses olevate andmete allalaadimiseks peab operaator tegema järgmised operatsioonid:

- asetama oma sõidumeerikukaardi sõidukiüksuse kaardiavasse ⁽¹⁾,
- ühendama eriotstarbelise seadme sõidukiüksuse allalaadimispistikuga,
- looma ühenduse eriotstarbelise seadme ja sõidukiüksuse vahel,
- valima eriotstarbelises seadmes allalaaditavad andmed ja saatma nõude sõidukiüksusele,
- sulgema allalaadimisseansi.

2.2. Andmete allalaadimisprotokoll

Protokoll on struktureeritud ülem-alluv-põhimõttel, kus eriotstarbelisel seadmel on ülema ja sõidukiüksusel alluva roll.

Sõnumi struktuur, tüübid ja -voog põhinevad peamiselt standardil Võtmesõnaprotokoll 2000 (KWP) (ISO 14230-2 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 2: Data link layer. Maanteesõidukid — Diagnostilised süsteemid — Võtmesõnaprotokoll 2000 — 2. osa: Lülikiht.).

Rakenduse kiht põhineb peamiselt standardi ISO 14229-1 praegu kehtival 22. veebruari 2001. aasta 6. versioonil (Road vehicles — Diagnostic systems — Part 1: Diagnostic services. Maanteesõidukid — Diagnostilised süsteemid — 1. osa: Diagnostikateenused.).

2.2.1. Sõnumi struktuur

DDP_002 Kõigi eriotstarbelise seadme ja sõidukiüksuse vahel vahetatud sõnumite vormingustruktuur koosneb kolmest osast:

- vormingubaidist (FMT), sihtbaidist (TGT), lähtebaidist (SRC) ja võimaluse korral pikkusbaidist (LEN) koosnev päis,
- andmeväli, mis koosneb teenuse identifikaatorbaidist (SID) ja muutuvast arvust andmebaididest, mis võivad sisaldada vabatahtlikku diagnostilise seansi baiti (DS_) või vabatahtlikku edastusparameetribaiti (TRTP või TREP),
- kontrollsummabaidist (CS) koosnev kontrollsumma.

Päis				Andmeväli					Kontroll-summa
FMT	TGT	SRC	LEN	SID	DATA	CS
4 baiti				Maksimaalselt 225 baiti					1 bait

Baidid TGT ja SRC väljendavad sõnumi saaja ja lähetaja füüsilist aadressi. Kuueteistkümmendarvudena on eriotstarbelise seadme väärtus F0h ja sõidukiüksuse väärtus EEh.

Bait LEN on andmevälja osa pikkus.

Kontrollsummabait on 8bitistes rühmades kõigi sõnumibaitide, välja arvatud bait CS ise, summa moodul 256.

Baidid FMT, SID, DS_, TRTP ja TREP määratletakse käesolevas dokumendis edaspidi.

⁽¹⁾ Sisestatud kaart käivitab kohased pääsuõigused allalaadimisfunktsioonile ja andmetele.

DDP_003 Juhul kui sõnumis edastatavate andmete pikkus ületab andmevälja osa mahu, saadetakse sõnum mitme allsõnumina. Igal allsõnumil on päis, sama SID, TREP ja kahebaidiline allsõnumi lugeja, mis näitab allsõnumi numbrit sõnumis. Vigade kontrollimise ja katkestamise võimaldamiseks saadab eriotstarbeline seade iga allsõnumi kohta jaatussõnumi. Eriotstarbeline seade võib allsõnumi aktsepteerida, paluda seda uuesti saata, nõuda sõidukiüksusel alustada edastamist uuesti või see katkestada.

DDP_004 Kui viimane allsõnum sisaldab andmeväljal täpselt 255 baiti, tuleb sellele liita viimane allsõnum tühja andmeväljaga (välja arvatud SID, TREP ja allsõnumi lugeja), näitamaks sõnumi lõppu.

Näide:

Päis	SID	TREP	Sõnum			CS
4 baiti	Pikem kui 255 baiti					

edastatakse:

Päis	SID	TREP	00	01	Allsõnum 1	CS
4 baiti	255 baiti					

Päis	SID	TREP	00	01	Allsõnum 2	CS
4 baiti	255 baiti					

...

Päis	SID	TREP	xx	yy	Allsõnum n	CS
4 baiti	Lühem kui 255 baiti					

või kui:

Päis	SID	TREP	00	01	Allsõnum 1	CS
4 baiti	255 baiti					

Päis	SID	TREP	00	02	Allsõnum 2	CS
4 baiti	255 baiti					

...

Päis	SID	TREP	xx	yy	Allsõnum n	CS
4 baiti	255 baiti					

Päis	SID	TREP	xx	yy+1	CS	
4 baiti	4 baiti					

2.2.2. Sõnumitüübid

Sõidukiüksuse ja eriotstarbelise seadme vahelise andmete allalaadimise sideprotokolli tarvis on vaja vahetada 8 erinevat sõnumitüüpi.

Järgmises tabelis on ülevaade nende sõnumite kohta.

Sõnumi struktuur	Päis maksimaalselt 4 baiti				Andmed maksimaalselt 255 baiti			Kontoll- summa 1 bait
	FMT	TGT	SRC	LEN	SID	DS/TRTP	DATA	
IDE ->	<- VU							
Start communication request	81	EE	F0		81			E0
Positive response start communication	80	F0	EE	03	C1		8F,EA	9B
Start diagnostic session request	80	EE	F0	02	10	81		F1
Positive response start diagnostic	80	F0	EE	02	50	81		31
Link control service								
Verify Baud rate (stage 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	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
Positive response verify Baud rate	80	F0	EE	02	C7		01	28
Transition baud rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00, 00,00,FF,FF, FF,FF	99
Positive response request upload	80	F0	EE	03	75		00,FF	D5
Transfer data request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events and faults	80	EE	F0	02	36	03		99
Detailed speed	80	EE	F0	02	36	04		9A
Technical data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06		9C
Positive response transfer data	80	F0	EE	Len	76	TREP	Data	CS
Request transfer exit	80	EE	F0	01	37			96
Positive response request transfer exit	80	F0	EE	01	77			D6
Stop communication request	80	EE	F0	01	82			E1
Positive response stop communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Subfunction not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect message length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Märkused:

- Sid Req = vastava nõude SID (teenuse identifikaator).
- TREP = vastava nõude TRTP (nõude edastusparameeter).
- Mustad lahtrid tähistavad seda, et ei edastata midagi.
- Terminit üleslaadimine (IDE seisukohast) kasutatakse standardiga ISO 14229 vastavuse eesmärgil. See tähendab sama kui allalaadimine (sõidukiüksuse seisukohast).
- Võimalikke kahebaidilisi allsõnumilugejaid ei ole käesolevas tabelis näidatud.

2.2.2.1. *Start communication request (SID 81)*

DDP_005 Eriotstarbeline seade annab selle sõnumi sideühenduse loomiseks sõidukiüksusega. Alghenduse luuakse alati kiirusega 9 600 boodi (kuni edastuskiiruse muutuseni, kasutades kohast käsku Link control service).

2.2.2.2. *Positive response start communication (SID C1)*

DDP_006 Sõidukiüksus annab selle sõnumi sideühenduse loomise nõude positiivse vastusena. Sõnum sisaldab mõlemat võtmebaiti "8F" ja "EA", mis näitavad, et üksus toetab protokollil, millel on sihi-, lähte- ja pikkusteabega päis.

2.2.2.3. *Start diagnostic session request (SID 10)*

DDP_007 Eriotstarbeline seade annab Start Diagnostic Session Request-sõnumi, et nõuda sõidukiüksusega uut diagnostilist seanssi. Allfunktsioon "default session" (81h) näitab, et tuleb avada standardne diagnostiline seanss.

2.2.2.4. *Positive response start diagnostic (SID 50)*

DDP_008 Sõidukiüksus saadab sõnumi Positive Response Start Diagnostic nõude Diagnostic Session Request positiivse vastusena.

2.2.2.5. *Link control service (SID 87)*

DDP_052 Eriotstarbeline seade kasutab käsku Link Control Service edastuskiiruse muutmise algatamiseks. See toimub kahes etapis. Esimeses etapis teeb eriotstarbeline seade ettepaneku edastuskiiruse muutmiseks, näidates ära uue kiiruse. Saades sõidukiüksusest positiivse vastuse, saadab eriotstarbeline seade sõidukiüksusele edastuskiiruse muutuse kinnituse (teine etapp). Seejärel lülitub eriotstarbeline seade uuele edastuskiirusele. Pärast kinnituse saamist lülitub sõidukiüksus uuele edastuskiirusele.

2.2.2.6. *Link control positive response (SID C7)*

DDP_053 Sõidukiüksus annab sõnumi Link Control Positive Response nõude Link Control Service positiivse vastusena (esimene etapp). Kinnitusele ei vastata (teine etapp).

2.2.2.7. *Request upload (SID 35)*

DDP_009 Eriotstarbeline seade annab sõnumiga Request Upload sõidukiüksusele teada, et nõutakse allalaadimist. Täitmaks standardi ISO 14229 nõudeid, esitatakse nõutud andmetega koos üksikasjad nende aadressi, suuruse ja vormingu kohta. Kuna eriotstarbeline seade neid enne allalaadimist ei tea, pannakse mäluadress nullile, vorming on krüpteerimata ja tihendamata ning mälu suurus pannakse maksimaalsele.

2.2.2.8. *Positive response request upload (SID 75)*

DDP_010 Sõidukiüksus saadab sõnumi Positive Response Request Upload näitamaks eriotstarbelisele seadmele, et sõidukiüksus on valmis andmeid alla laadima. Täitmaks standardi ISO 14229 nõudeid, kaasatakse positiivse vastuse sõnumisse andmed, mis näitavad eriotstarbelisele seadmele, et edaspidised sõnumid Positive Response Transfer Data sisaldavad maksimaalselt 00FFh baite.

2.2.2.9. *Transfer data request (SID 36)*

DDP_011 Eriotstarbeline seade saadab sõnumi Transfer Data Request, määratlemaks sõidukiüksusele, mis tüüpi andmeid hakatakse alla laadima. Ühebaadiline Transfer Request Parameter (TRTP) näitab edastustüüpi.

Andmeedastuse tüüpe on kuus:

- ülevaade (TRTP 01),
- tegevused konkreetsel kuupäeval (TRTP 02),
- sündmused ja rikked (TRTP 03),
- üksikasjalik kiirus (TRTP 04),
- tehnilised andmed (TRTP 05),
- allalaadimine kaardilt (TRTP 06).

DDP_054 Eriotstarbeline seade peab nõudma ülevaadet andmevastuse kohta (TRTP 01) allalaadimiseajal, sest ainult see tagab sõidukiüksuse sertifikaatide registreerimise allalaaditud faili (ning võimaldab töendada digitaalalkirja).

Teisel juhul (TRTP 02) sisaldab sõnum Transfer Data Request viidet allalaaditavale kuupäevale (TimeReal-vormingus).

2.2.2.10. *Positive response transfer data (SID 76)*

DDP_012 Sõidukiüksus saadab sõnumi Positive Response Transfer Data nõude Transfer Data Request positiivse vastusena. Sõnum sisaldab nõutud andmeid ja parameetri Transfer Response Parameter (TREP), mis vastab nõude TRTPle.

DDP_055 Esimesel juhul (TREP 01) saadab sõidukiüksus andmeid, mis aitavad eriotstarbelise seadme operaatoril valida, milliseid andmeid ta edaspidi soovib alla laadida. Selles sõnumis sisaldub järgmine teave:

- turbesertifikaadid,
- sõiduki identifikatsioon,
- sõidukiüksuse käesolev kuupäev ja kellaeg,
- vähimad ja suurimad allalaaditavad andmed (sõidukiüksuse andmed),
- viide selle kohta, kas sõidukiüksuses on kaarte,
- eelmine allalaadimine ettevõttele,
- ettevõtetelukud,
- eelmised kontrollimised.

2.2.2.11. *Request transfer exit (SID 37)*

DDP_013 Eriotstarbeline seade annab sõnumiga Request Transfer Exit sõidukiüksusele teada, et allalaadimiseajal on lõpetatud.

2.2.2.12. *Positive response request transfer exit (SID 77)*

DDP_014 Sõidukiüksus saadab sõnumi Positive Response Request Transfer Exit nõude Request Transfer Exit jaatusena.

2.2.2.13. *Stop communication request (SID 82)*

DDP_015 Eriotstarbeline seade annab sõnumi Stop Communication Request sideühenduse katkestamiseks sõidukiüksusega.

2.2.2.14. *Positive response stop communication (SID C2)*

DDP_016 Sõidukiüksus saadab sõnumi Positive Response Stop Communication side lõpetamisnõude jaatusena.

2.2.2.15. *Acknowledge submessage (SID 83)*

DDP_017 Eriotstarbeline seade saadab sõnumi Acknowledge Submessage, kinnitamaks mitmete allsõnumitena edastatud sõnumi iga osa kättesaamist. Andmeväli sisaldab sõidukiüksuselt saadud teenuse identifikaatorit ja kahebaidilist koodi järgmiselt:

- MsgC +1 jaatab allsõnumi nr MsgC korrektset kättesaamist.
Eriotstarbelise seadme nõue sõidukiüksusele saata järgmine allsõnum,
- MsgC väljendab probleemi allsõnumi nr MsgC kättesaamisel.
Eriotstarbelise seadme nõue sõidukiüksusele saata allsõnum uuesti,
- FFFF nõuab sõnumi lõpetamist.

Eriotstarbeline seade saab seda kasutada lõpetamiseks sõnumi saatmine sõidukiüksuselt mis tahes põhjusel.

Sõnumi viimase allsõnumi (LEN bait < 255) jaatamiseks võib kasutada ükskõik millist nendest koodidest või selle võib jätta jaatamata.

Sõidukiüksuse mitmest allsõnumist koosnevad vastused on:

- Positive Response Transfer Data (SID 76)

2.2.2.16. *Negative Response (SID 7F)*

DDP_018 Sõidukiüksus saadab eespool osutatud nõudesõnumitele sõnumi Negative Response, kui sõidukiüksus ei saa nõuet täita. Sõnumi andmeväljad sisaldavad vastuse teenuse identifikaatorit (7F), nõude teenuse identifikaatorit ja negatiivset vastust määratlevat koodi. Kasutada saab järgmisi koodi:

- 10 üldine keeldumine
Tegevust ei saa läbi viia allpool käsitlemata põhjustel.
- 11 teenusel puudub tugi
Nõude teenuse identifikaator ei ole arusaadav.
- 12 allfunktsioonil puudub tugi
Nõude DS_ või TRTP ei ole arusaadav või ei ole edastamiseks rohkem allsõnumeid.
- 13 sõnumi pikkus vale
Vastuvõetud sõnumi pikkus on vale.
- 22 tingimused pole õiged või nõudejada viga
Nõutav teenus ei ole aktiivne või nõudesõnumi jada ei ole korrektne.
- 31 nõue väljaspool ulatust
Nõude kirje parameeter (andmeväli) ei ole kehtiv.
- 50 üleslaadimist ei aktsepteerita
Nõuet ei saa täita (sõidukiüksus on ebakohases toimimismooduses või sõidukiüksuse siserike).
- 78 vastus ootel
Nõutavat tegevust ei saa õigeaegselt täita ja sõidukiüksus ei ole valmis uut nõuet aktsepteerima.
- FA andmed ei ole kasutatavad
Andmeedastusnõude andmeobjekt ei ole sõidukiüksuses kasutatav (nt kaart ei ole sisestatud, ...).

2.2.3. Sõnumivoog

Tüüpiline sõnumivoog tavalise andmete allalaadimise käigus on järgmine:

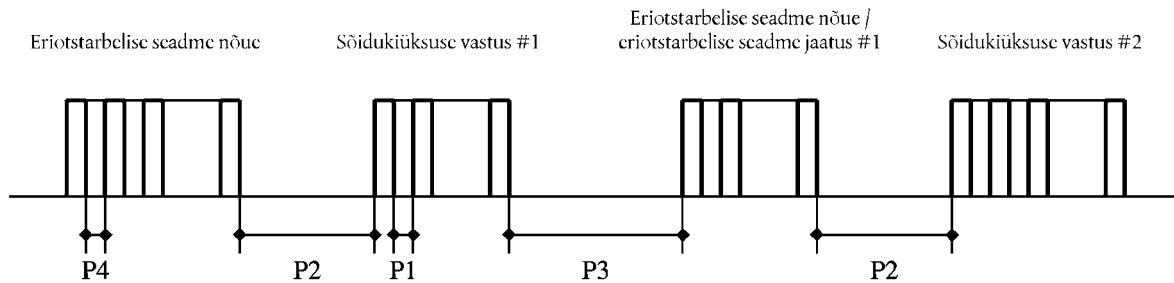
IDE		VU
Start communication request	⇒ ⇐	Positive response
Start diagnostic service request	⇒ ⇐	Positive response
Request upload	⇒ ⇐	Positive response
Transfer data request overview	⇒ ⇐	Positive response
Data request #2	⇒	Positive response #1 Positive response #2 Positive response #m Positive response (Data field < 255 Bytes)
Acknowledge submessage #1	⇐	
Acknowledge submessage #2	⇒	
Acknowledge submessage #m	⇐	
Acknowledge submessage (optional)	⇒	
...		
Transfer data request #n	⇒ ⇐	Positive response
Request transfer exit	⇒ ⇐	Positive response
Stop communication request	⇒ ⇐	Positive response

2.2.4. Ajastamine

DDP_019 Normaalse töötamise ajal on asjakohased järgmisel joonisel näidatud ajastusparameetrid:

Joonis 1

Sõnumivoog, ajastamine



kus

P1 = sõidukiüksuse vastuses baitidevaheline aeg.

P2 = aeg eriotstarbelise seadme nõude lõpu ja sõidukiüksuse vastuse alguse vahel või eriotstarbelise seadme jaatuse lõpu ja sõidukiüksuse järgmise vastuse alguse vahel.

P3 = aeg sõidukiüksuse vastuse lõpu ja eriotstarbelise seadme uue nõude alguse vahel või sõidukiüksuse vastuse lõpu ja eriotstarbelise seadme jaatuse alguse vahel või eriotstarbelise seadme nõude lõpu ja eriotstarbelise seadme uue nõude alguse vahel, kui sõidukiüksus ei vasta.

P4 = eriotstarbelise seadme nõudes baitidevaheline aeg.

P5 = P3 laiendatud väärtus allalaadimiseks kaardilt.

Ajastusparameetrite lubatud väärtused on näidatud järgmises tabelis (võtmesõnaprotokolli laiendatud ajastusparameetrite kogum, kasutatakse kiiremaks edastuseks füüsilisel adresserimisel).

Ajastusparameeter	Väikseim piirväärtus (ms)	Suurim piirväärtus (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minutit

(*) Kui sõidukiüksus annab negatiivse vastuse, mis sisaldab koodi "nõue korrektselt vastu võetud, vastus ootel", laiendatakse seda väärtust samale suurimale piirväärtusele kui P3 puhul.

2.2.5. Vea töötlemine

Kui sõnumivahetuse käigus toimub viga, muudetakse sõnumivoog skeemi sõltuvalt sellest, milline seade on vea tuvastanud ja milline sõnum on vea genereerinud.

Joonistel 2 ja 3 on näidatud vastavalt sõidukiüksuse ja eriotstarbelise seadme vea töötlemiskorda.

2.2.5.1. Side algusetapp

DDP_020 Kui eriotstarbeline seade tuvastab ajastuse või bitivooga seotud vea side algusetapis, ootab see enne nõude taasesitamist vähemalt aja P3.

DDP_021 Kui sõidukiüksus tuvastab vea eriotstarbelisest seadmest tulevas jadas, ei saada see vastust ja ootab uut sõnumit Start Communication Request maksimaalselt aja P3 jooksul.

2.2.5.2. Sideetapp

Võib määratleda kaks erinevat veatöötamise valdkonda.

1. Sõidukiüksus tuvastab eriotstarbelise seadme edastusvea.

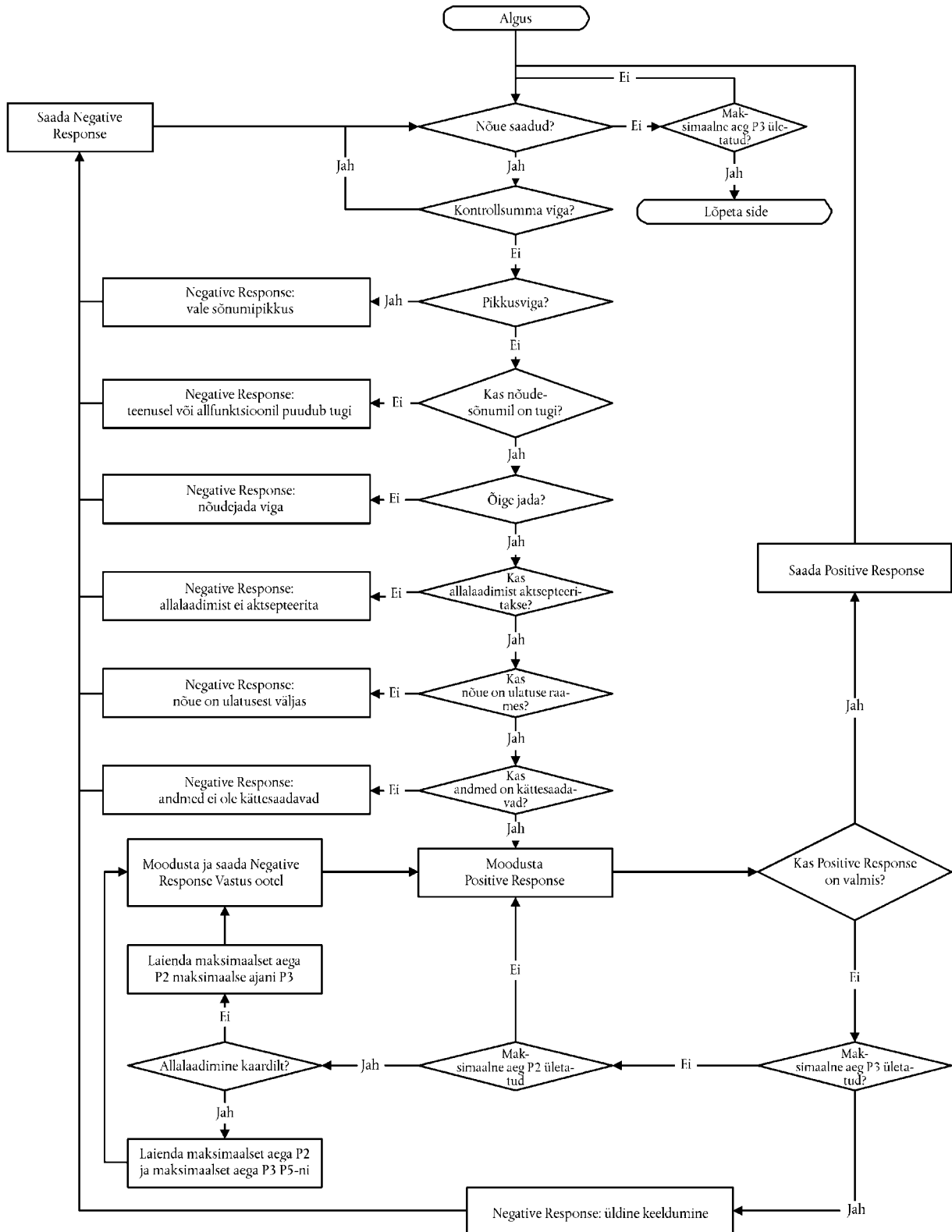
DDP_022 Iga saadud sõnumi puhul tuvastab sõidukiüksus ajastusvead, baidivormingu vead (nt algus- ja lõpubiiti rikkumised) ja kaardrivead (saadud vale arv baite, vale kontrollsummabait).

DDP_023 Kui sõidukiüksus tuvastab ühe eespool mainitud vigadest, ei saada see vastust ja eirab saadud sõnumit.

DDP_024 Sõidukiüksus võib tuvastada saadud sõnumivormingus või sisus muid vigu (nt sõnumil puudub tugi) isegi siis, kui sõnum vastab pikkus- ja kontrollsummanõuetele; sellisel juhul saadab sõidukiüksus eriotstarbelisele seadmele sõnumi Negative Response, määratledes vea olemuse.

Joonis 2

Sõidukiüksuse veatõtlus

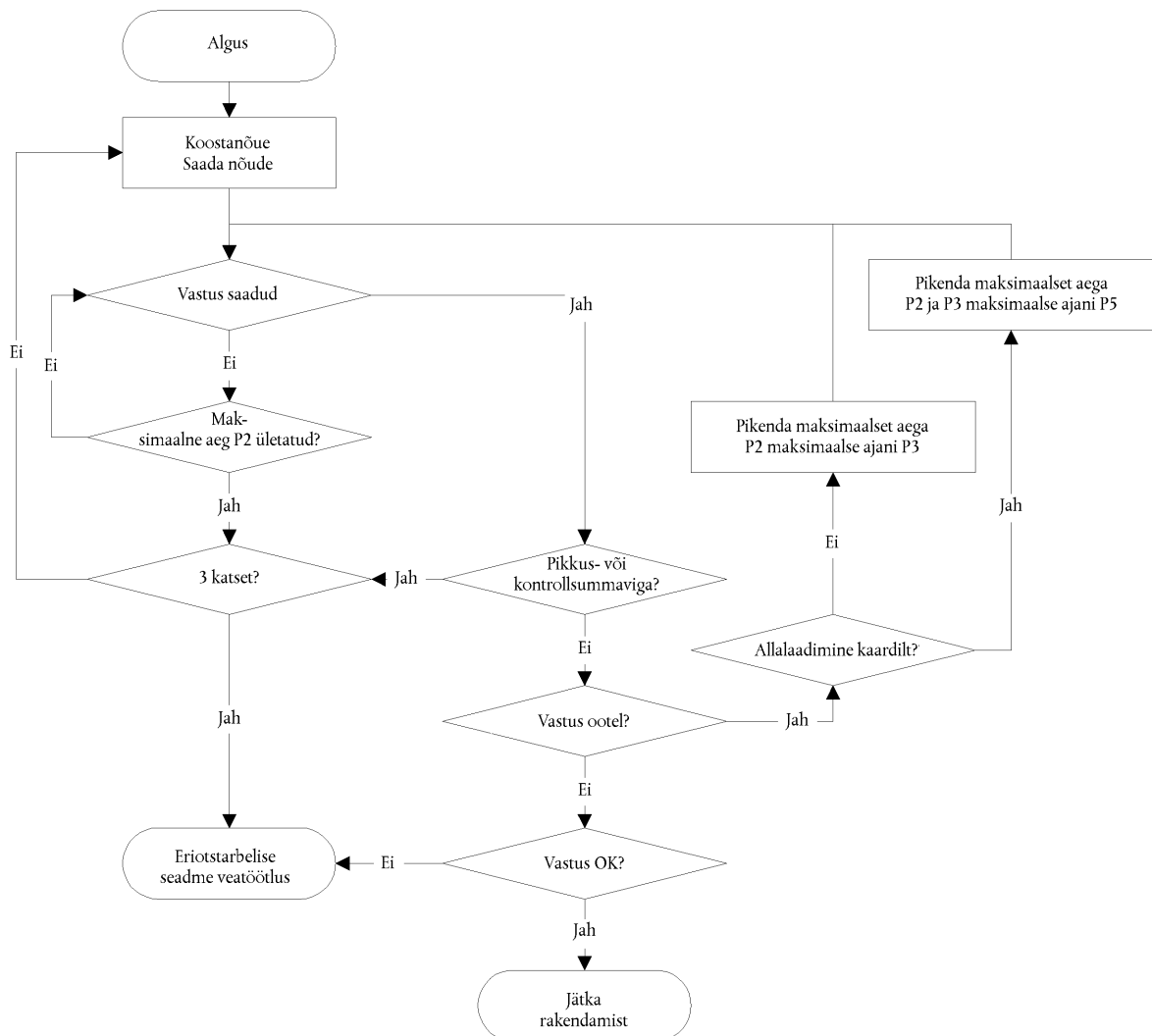


2. Eriotstarbeline seade tuvastab sõidukiüksuse edastusvea.

- DDP_025 Iga saadud sõnumi puhul tuvastab eriotstarbeline seade ajastusvead, baidivormingu vead (nt algus- ja lõpubiti rikkumised) ja kaadrivead (saadud vale arv baite, vale kontrollsummabait).
- DDP_026 Eriotstarbeline seade tuvastab jadavead, nt allsõnumi lugeja vale suurenemine järjestikku saadud sõnumites.
- DDP_027 Kui eriotstarbeline seade tuvastab vea või kui sõidukiüksus ei vastanud maksimaalse aja P2 jooksul, edastatakse sõnum uuesti kokku kuni 3 korda. Selle vea tuvastamise eesmärgil käsitletakse allsõnumi jaatust sõidukiüksusele saadetud nõudena.
- DDP_028 Eriotstarbeline seade ootab enne iga edastuse algust vähemalt minimaalse aja P3; ooteaega mõõdetakse vea tuvastamise järgsest viimasest arvutuslikust lõpubitist.

Joonis 3

Eriotstarbelise seadme veatöötlus



2.2.6. Vastusesõnumi sisu

Käesolevas lõikes määratletakse erinevate positiivsete vastusesõnumite andmeväljade sisu.

Andmeelemendid on määratletud 1. liite andmesõnastikus.

2.2.6.1. Positive response transfer data overview

DDP_029 Sõnumi "positive response transfer data overview" andmeväljas on järgmised andmed järgmises järjestuses, kus teenuseid-identifikaator on "76h" ja identifikaator TREP "01h", järgitakse ka kohast jagamist allsõnumiteks ja nende lugemist:

Andmeelement	Pikkus (baitides)	Selgitus	
MemberStateCertificate	194	Sõidukiüksuse turbesertifikaadid	
VUCertificate	194		
VehicleIdentificationNumber	17	Sõiduki identifitseerimine	
VehicleRegistrationIdentification	1		
vehicleRegistrationNation vehicleRegistrationNumber	14		
CurrentDateTime	4	Sõidukiüksuse käesolev kuupäev ja kellaeg	
VuDownloadablePeriod		Allalaaditav ajavahemik	
minDownloadableTime maxDownloadableTime	4 4		
CardSlotsStatus	1	Sõidukiüksusesse sisestatud kaarditüübid	
VuDownloadActivityData		Eelmine allalaadimine sõidukiüksusest	
downloadingTime	4		
fullCardNumber companyOrWorkshopName	18 36		
VuCompanyLocksData		Kõik salvestatud ettevõtetelud. Kui see osa on tühi, saadetakse ainult noOfLocks = 0.	
noOfLocks	1		
...	(98)		
Vu Company Locks Record	lockInTime lockOutTime companyName companyAddress companyCardNumber		4 4 36 36 18
...			
...			
VuControlActivityData		Kõik sõidukiüksusesse salvestatud kontrollikirjed. Kui see osa on tühi, saadetakse ainult noOfControls = 0.	
noOfControls	1		
...	(31)		
Vu Control Activity Record	controlType controlTime controlCardNumber downloadPeriodBeginTime downloadPeriodEndTime		1 4 18 4 4
...			
Signature	128	RSA allkiri kõigile andmetele (välja arvatud sertifikaadid) alates VehicleIdentificationNumber kuni viimase VuControlActivityRecord viimase baidini.	

2.2.6.2. Positive response transfer data activities

DDP_030 Sõnumi "positive response transfer data activities" andmeväljas on järgmised andmed järgmises järjestuses, kus teenuseid-identifikaator on "76h" ja identifikaator TREP "02h", järgitakse ka kohast jagamist allsõnumiteks ja nende lugemist:

Andmeelement	Pikkus (baitides)	Selgitus
TimeReal	4	Allalaaditud päeva kuupäev
OdometerValueMidnight	3	Läbisõidumõõdiku väärtus allalaaditud päeva lõpus
VuCardIWData noOfVuCardIWRecords	2	Andmed kaartide sisestus-/väljavõtmistsüklite kohta.
...	(129)	
VuCardIWRecord		
cardHolderName	36	– Kui selles osas ei ole kättesaadavaid andmeid, saadetakse ainult noOfVuCardIWRecords = 0.
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	– Kui VuCardIWRecord on üle kella 00:00 (kaardi sisestamine eelmisel päeval)
cardExpiryDate	4	või üle kella 24:00
cardInsertionTime	4	(kaardi väljavõtmine järgmisel päeval),
vehicleOdometerValueAtInsertion	3	esitatakse see täielikult kahe hõlmava päeva ulatuses.
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification	1	
vehicleRegistrationNation	14	
vehicleRegistrationNumber	4	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData noOfActivityChanges	2	Allalaaditava päeva avastaatus kell 00:00 ja salvestatud tegevusmuutused.
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData noOfPlaceRecords	1	Allalaaditava päeval salvestatud kohtadega seotud andmed. Kui see osa on tühi, saadetakse ainult noOfPlaceRecords = 0.
...	(28)	
VuPlaceDailyWorkPeriodRecord		
fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData noOfSpecificConditionRecords	2	Allalaaditava päeval salvestatud eritingimuste andmed.
...	(5)	Kui see osa on tühi, saadetakse ainult noOfSpecificConditionRecords = 0.
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	RSA allkiri kõigile andmetele alates TimeReal kuni viimase eritingimuskirje viimase baidini.

2.2.6.3. Positive response transfer data events and faults

DDP_031 Sõnumi "positive response transfer data events and faults" andmeväljas on järgmised andmed järgmises järjestuses, kus teenuseidentifikaator on '76h' ja identifikaator TREP '03h', järgitakse ka kohast jagamist allsõnumiteks ja nende lugemist:

Andmeelement		Pikkus (baitides)	Selgitus	
VuFaultData				
NoOfVuFaults		1	Kõik sõidukiüksusesse salvestatud või seal kestvad rikked. Kui see osa on tühi, saadetakse ainult noOfVuFaults = 0.	
...		(82)		
VuFaultRecord	FaultType	1		
	FaultRecordPurpose	1		
	FaultBeginTime	4		
	FaultEndTime	4		
	CardNumberDriverSlotBegin	18		
	cardNumberCodriverSlotBegin	18		
	CardNumberDriverSlotEnd	18		
CardNumberCodriverSlotEnd	18			
...				
VuEventData				
NoOfVuEvents		1	Kõik sõidukiüksusesse salvestatud või seal kestvad sündmused (välja arvatud kiiruse ületamine). Kui see osa on tühi, saadetakse ainult 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	Viimase kiiruse ületamise kontrolliga seotud andmed (andmete puudumisel vaikeväärtus).	
FirstOverspeedSince		4		
NumberOfOverspeedSince		1		
VuOverSpeedingEventData				
NoOfVuOverSpeedingEvents		1	Kõik sõidukiüksusesse salvestatud kiiruse ületamise sündmused. Kui see osa on tühi, saadetakse ainult noOfVuOverSpeedingEvents = 0.	
...		(31)		
VuOverSpeedingEventRecord	EventType	1		
	EventRecordPurpose	1		
	EventBeginTime	4		
	EventEndTime	4		
	MaxSpeedValue	1		
	AverageSpeedValue	1		
	CardNumberDriverSlotBegin	18		
	SimilarEventsNumber	1		
...				
VuTimeAdjustmentData				
NoOfVuTimeAdjRecords		1	Kõik sõidukiüksusesse salvestatud aja korrigeerimise sündmused (väljaspool täiskalibreerimise kaadrit). Kui see osa on tühi, saadetakse ainult noOfVuTimeAdjRecords = 0.	
...		(98)		
VuTimeAdjustmentRecord	OldTimeValue	4		
	NewTimeValue	4		
	WorkshopName	36		
	WorkshopAddress	36		
	WorkshopCardNumber	18		
...				
Signature		128		RSA allkiri kõigile andmetele alates noOfVuFaults kuni viimase aja reguleerimise kirje viimase baidini.

2.2.6.4. Positive response transfer data detailed speed

DDP_032 Sõnumi "positive response transfer data detailed speed" andmeväljas on järgmised andmed järgmises järjestuses, kus teeneidentifikaator on "76h" ja identifikaator TREP "04h", järgitakse ka kohast jagamist allsõnumiteks ja nende lugemist:

Andmeelement		Pikkus (baitides)	Selgitus
VuDetailedSpeedData			
NoOfSpeedBlocks		2	Kõik sõidukiüksusesse salvestatud aja korrigeerimise sündmused (väljaspool täiskalibreerimise kaadrit). Kui see osa on tühi, saadetakse ainult noOfVuTimeAdjRecords = 0.
..			
VuDetailedSpeedBlock	SpeedBlockBeginDate speedsPerSecond	4 60	
..			
Signature		128	RSA allkiri kõigile andmetele alates noOfVuFaults kuni viimase aja korrigeerimise kirje viimase baidini.

2.2.6.5. Positive response transfer data technical data

DDP_033 Positive Response Transfer Data Technical Data andmeväljas esitatakse järgmised andmed järgmises järjestuses, kus SID on 76h ja TREP 05h ning võetakse arvesse kohast jagamist allsõnumiks ning nende lugemist:

Andmeelement		Pikkus (baitides)	Selgitus
VuIdentification			
vuManufacturerName		36	Kõik sõidukiüksusesse salvestatud kalibreerimiskirjed.
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	Kõik sõidukiüksusesse salvestatud kalibreerimiskirjed.
...		(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 allkiri kõigile andmetele alates vuManufacturerName kuni viimase VuCalibrationRecord viimase baidini.

2.3. Välisandmekandja faili salvestamine

DDP_034 Kui allalaadimisseanss sisaldas sõidukiüksuse andmete edastamist, salvestab eriotstarbeline seade kõik sõidukiüksusest allalaadimisseansi käigus saadud andmed koos sõnumitega Positive Response Transfer Data ühte füüsilisse faili. Salvestavate andmete hulgast jäetakse välja sõnumipäised, allsõnumi lugejad, tühjad allsõnumid ja kontrollsummad, kuid salvestatakse teenuse identifikaator ja TREP (ainult esimese allsõnumi omad, kui on mitu allsõnumit).

3. SÕIDUMEERIKUKAARTIDELT ALLALAADIMISE PROTOKOLL

3.1. Kohaldamisala

Käesolevas lõikes kirjeldatakse kaardiandmete otsest allalaadimist sõidumeerikukaardilt eriotstarbelisse seadmesse. Eriotstarbeline seade ei ole turvakeskkonna osa; seetõttu ei toimu kaardi ja eriotstarbelise seadme vahel autentimist.

3.2. Mõisted

Allalaadimisseanss: igasugune kiipkaardiandmete allalaadimine. Seanss hõlmab terviklikku korda alates liideseseadme tehtavast kiipkaardi nullimisest kuni kiipkaardi deaktiveerimiseni (kaardi väljavõtmine või uus lähtestus).

Allkirjastatud andmefail: fail kiipkaardilt. Fail edastatakse liideseseadmesse lihttekstina. Fail räsitakse ja allkirjastatakse kiipkaardil ning allkiri edastatakse liideseseadmesse.

3.3. Allalaadimine kaardilt

DDP_035 Sõidumeerikukaardilt allalaadimine hõlmab järgmisi etappe:

- kaardi elementaarfailides (ICC ja IC) oleva üldteabe allalaadimine. See on vabatahtlik teave ning seda ei turvata digitaalallkirjaga,
- elementaarfailide Card_Certificate a CA_Certificate allalaadimine. See teave ei ole turvatud digitaalallkirjaga,

Nende failide allalaadimine on iga allalaadimisseansi puhul kohustuslik.

- muude rakendusandmete (sõidumeeriku erifailis olevate) elementaarfailide allalaadimine, välja arvatud elementaarfail Card_Download. See teave on turvatud digitaalallkirjaga,
 - iga allalaadimisseansi puhul on kohustuslik alla laadida vähemalt elementaarfailid Application_Identifier JA ID,
 - juhikaardilt allalaadimisel on kohustuslik alla laadida ka järgmised elementaarfailid:
 - Events_Data,
 - Faults_Data,
 - Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - Control_Activity_Data,
 - Specific_Conditions.
- juhikaardilt allalaadimisel ajakohastatakse kuupäev LastCardDownload elementaarfailis Card_Download;
- töökojakaardilt allalaadimisel lähtestatakse kalibreerimisluigeja elementaarfailis Card_Download.

3.3.1. Initsialiseerimisjada

DDP_036 Eriotstarbeline seade initsialiseerib jada järgmiselt:

Kaart	Suund	IDE/IFD	Tähendus/märkused
	↵	Riistvara lähtestus	
ATR	⇒		

Soovi korral võib suuremale edastuskiirusele üleminekuks kasutada PPSi, kui kiipkaart seda toetab.

3.3.2. Allkirjastamata andmefailide jada

DDP_037 ICC, IC, Card_Certificate ja CA_Certificate allalaadimisjada on järgmine:

Kaart	Suund	IDE/IFD	Tähendus/märkused
	↵	Select file	Faili valik failiidentifikaatorite alusel
OK	⇒		
	↵	Read Binary	Kui fail sisaldab rohkem andmeid, kui mahub kaardilugeja või kaardi puhvrise, tuleb käsku korrata kuni kogu faili lugemiseni.
File data OK (Faili andmed korras)	⇒	Store data to ESM (salvesta andmed välisandmekandjale)	vastavalt punktile 3.4 (andmete salvestusvorming)

Märkus: enne elementaarfaili Card_Certificate valimist peab olema valitud sõidumeerikurakendus (valitakse rakenduse identifikaatori kaudu).

3.3.3. Allkirjastatud andmefailide jada

DDP_038 Iga järgmise faili puhul, mis tuleb alla laadida koos allkirjaga, kasutatakse järgmist jada:

Kaart	Suund	IDE/IFD	Tähendus/märkused
	↵	Select file	
OK	⇒		
	↵	Perform Hash of File	Arvutab valitud faili andmete räsiväärtuse, kasutades ettenähtud räsalgoritmi vastavalt 11. liitele. See käsk ei ole ISO käsk.
Arvuta faili räsi ja salvesta räsiväärtus ajutiselt			
OK	⇒		
	↵	Read Binary	Kui fail sisaldab rohkem andmeid, kui mahub kaardilugeja või kaardi puhvrise, tuleb käsku korrata kuni kogu faili lugemiseni.
File data OK (Faili andmed korras)	⇒	Salvesta saadud andmed välisandmekandjale	vastavalt punktile 3.4 (andmete salvestusvorming)
	↵	PSO: Compute Digital Signature	
Tee turbetoiming "compute digital signature", kasutades ajutiselt salvestatud räsiväärtust			
Allkiri OK	⇒	Liida andmed varem salvestatud andmetele välisandmekandjal	vastavalt punktile 3.4 (andmete salvestusvorming)

3.3.4. Kalibreerimislugeja lähtestusjada

DDP_039 Töökojakaardi elementaarfaili Card_Download NoOfCalibrationsSinceDownload lugeja lähtestusjada on järgmine:

Kaart	Suund	IDE/IFD	Tähendus/märkused
OK	↵	Select File EF Card_Download	Vali failiidentifikaatorite alusel
	↵	Update Binary NoOfCalibrationsSinceDownload = '00 00'	
Lähtestab kaardi allalaadimisnumbri			
OK	↵		

3.4. Andmete salvestusvorming

3.4.1. Sissejuhatus

DDP_040 Allalaaditud andmed tuleb salvestada vastavalt järgmistele tingimustele:

- andmed salvestatakse transparentsena. See tähendab, et baitide järjestus ning bittide järjestus baidis, mis edastatakse kaardilt, peab salvestamisel säilima,
- kõik ühe allalaadimiseansi ajal kaardilt allalaaditud failid salvestatakse välisandmekandjal ühte faili.

3.4.2. Failivorming

DDP_041 Failivorming on mitmete sildi pikkusväärtuse objektide konkatenatsioon.

DDP_042 Elementaarfaili silt on identifikaator pluss liide "00".

DDP_043 Elementaarfaili allkirja silt on faili identifikaator pluss liide "01".

DDP_044 Pikkus on kahebaidiline väärtus. Väärtus määratleb baitide arvu väärtuseväljal. Väärtuseväli "FF FF" on väärtuse edaspidiseks kasutamiseks.

DDP_045 Kui faili ei laadita alla, ei salvestata seoses failiga mitte midagi (ei silti ega nullpikkust).

DDP_046 Allkiri salvestatakse vahetult järgmise sildi pikkusväärtuse objektina pärast sildi pikkusväärtuse objekti, mis sisaldab faili andmeid.

Määratlus	Tähendus	Pikkus
FID (2 baiti) "00"	EFi silt (FID)	3 baiti
FID (2 baiti) "01"	EFi allkirja silt (FID)	3 baiti
xx xx	Väärtusevälja pikkus	2 baiti

Näidisandmed allalaaditud failis välisandmekandjal:

Silt	Pikkus	Väärtus
00 02 00	00 11	Elementaarfaili ICC andmed
C1 00 00	00 C2	Elementaarfaili Card_Certificate andmed
		...
05 05 00	0A 2E	Elementaarfaili Vehicles_Used andmed
05 05 01	00 80	Elementaarfaili Vehicles_Used allkiri

4. SÕIDUMEERIKUKAARDILT ALLALAADIMINE SÕIDUKIÜKSUSE KAUDU

- DDP_047 Sõidukiüksus peab võimaldama alla laadida liideseseadmesse sisestatud ja sellega ühendatud juhikaardi sisu.
- DDP_048 Liideseseade saadab sõidukiüksusele selle mooduse algatamiseks sõnumi Transfer Data Request Card Download (vt punkt 2.2.2.9).
- DDP_049 Seejärel laadib sõidukiüksus alla kogu kaardi failide kaupa vastavalt lõikes 3 määratletud kaardi allalaadimisprotokollile ning edastab kaardilt saadud andmed välisandmekandjale kohases sildi pikkusväärtuse failivormingus (vt punkt 3.4.2), mis on kaitstud sõnumiga Positive Response Transfer Data.
- DDP_050 Liideseseade teeb väljavõtte sõnumist Positive Response Transfer Data (lõigates välja kõik päised, SIDid, TREPId, allsõnumi lugejad ja kontrollsummad) ning salvestab selle ühte füüsilisse faili lõike 2.3 kohaselt.
- DDP_051 Seejärel ajakohastab sõidukiüksus vastavalt kohaldatavusele juhikaardil faili `Control_Activity_Data` või `Card_Download`.
-

8. liide

KALIBREERIMISPROTOKOLL

SISUKORD

1.	Sissejuhatus	448
2.	Lühendid, mõisted ja viited	448
3.	Ülevaade teenustest	448
3.1.	Võimalikud teenused	448
3.2.	Vastusekoodid	449
4.	Sideteenused	449
4.1.	Teenus StartCommunication	449
4.2.	Teenus StopCommunication	451
4.2.1.	Sõnumi kirjeldus	451
4.2.2.	Sõnumivorming	452
4.2.3.	Parameetri määratlus	453
4.3.	Teenus TesterPresent	453
4.3.1.	Sõnumi kirjeldus	453
4.3.2.	Sõnumivorming	453
5.	Haldusteenused	454
5.1.	Teenus StartDiagnosticSession	454
5.1.1.	Sõnumi kirjeldus	454
5.1.2.	Sõnumivorming	455
5.1.3.	Parameetri määratlus	456
5.2.	Teenus SecurityAccess	456
5.2.1.	Sõnumi kirjeldus	456
5.2.2.	Sõnumivorming — SecurityAccess — requestSeed	457
5.2.3.	Sõnumivorming — SecurityAccess — sendKey	458
6.	Andmeedastusteenused	459
6.1.	Teenus DataByIdentifier	459
6.1.1.	Sõnumi kirjeldus	459
6.1.2.	Sõnumivorming	459
6.1.3.	Parameetri määratlus	460
6.2.	Teenus WriteDataByIdentifier	461
6.2.1.	Sõnumi kirjeldus	461
6.2.2.	Sõnumivorming	461
6.2.3.	Parameetri määratlus	462
7.	Testimpulsside juhtimine — sisend-/väljundsignaali juhtimise funktsionaalne üksus	462
7.1.	Teenus InputOutputControlByIdentifier	462

7.1.1.	Sõnumi kirjeldus	462
7.1.2.	Sõnumivorming	463
7.1.3.	Parameetri määratlus	464
8.	Andmekirjete vormingud	465
8.1.	Edastatavad parameetriväärtused	465
8.2.	dataRecords vormingud	466

1. SISSEJUHATUS

Käesolevas liites kirjeldatakse, kuidas toimub andmevahetus sõidukiüksuse ja testimisseadme vahel K-liini kaudu, mis moodustab 6. liites kirjeldatud kalibreerimisliidese osa. Selles kirjeldatakse ka sisend-/väljundsignaali juhtme kontrollimist kalibreerimispistikul.

K-liiniga side loomist kirjeldatakse 4. jaos "Sideteenused".

Käesolevas liites kasutatakse erinevatel tingimustel K-liini rakendusala määratlemiseks mõistet diagnostilised *seansid*. Vaikeseanss on StandardDiagnosticSession, mille käigus saab sõidukiüksusest lugeda kõiki andmeid, kuid sinna ei saa andmeid kirjutada.

Diagnostilise seansi valikut on kirjeldatud 5. jaos "Haldusteenused".

CPR_001 "ECUProgrammingSession" võimaldab andmeid sõidukiüksusesse sisestada. Kalibreerimisandmete sisestamiseks (nõuded 097 ja 098) peab sõiduk lisaks olema toimimismooduses CALIBRATION.

K-liini kaudu andmete edastamist on kirjeldatud 6. jaos "Andmeedastusteenused". Andmeedastusvorminguid on üksikasjalikult kirjeldatud 8. jaos "Andmekirjete vormingud".

CPR_002 "ECUAdjustmentSession" võimaldab valida kalibreerimise sisend-/väljundsignaalliini sisend-/väljundmooduse K-liini liidese kaudu. Kalibreerimise sisend-/väljundsignaalliini juhtimist on kirjeldatud 7. jaos "Testimpulsside juhtimine — Sisend-/väljundsignaali juhtimise funktsionaalne üksus".

CPR_003 Käesolevas dokumendis on testimisseadme aadressiks märgitud 'tt'. Kuigi võib olla testimisseadmete eelistatud aadresse, peab sõidukiüksus vastama korrektselt mis tahes testimisseadme aadressile. Sõidukiüksuse füüsiline aadress on 0xEE.

2. MÕISTED, MÄÄRATLUSED JA VIITED

Protokollid, sõnumid ja veakoodid põhinevad peamiselt standardi ISO 14229-1 praegu kehtival 22. veebruari 2001. aasta 6. versioonil (Road vehicles — Diagnostic systems — Part 1: Diagnostic services. Maanteesõidukid — Diagnostilised süsteemid — 1. osa: Diagnostikateenused.).

Teenuse identifikaatorite, teenusenõuete ja -vastuste ning standardparameetrite tarvis kasutatakse baitkodeerimist ja kuueteistkümnendväärtusi.

Testimisseade on seade, mida kasutatakse programmeerimis-/kalibreerimisandmete sisestamiseks sõidukiüksusesse.

Klient ja *server* viitavad vastavalt testimisseadmele ja sõidukiüksusele.

ECU tähendab *elektroonilist kontrolliüksust* ja see viitab sõidukiüksusele.

Viited

ISO 14230-2: Road Vehicles — Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer. First edition: 1999. Vehicles — Diagnostic Systems. (Maanteesõidukid — Diagnostilised süsteemid — Võtmesõnaprotokoll 2000 — 2. osa: Lülikiht. Esimene väljaanne: 1999. Sõidukid — Diagnostilised süsteemid.)

3. ÜLEVAADE TEENUSTEST

3.1. Võimalikud teenused

Järgmises tabelis on ülevaade teenustest, mis on sõidumeerikus olemas ja on määratletud käesolevas dokumendis.

CPR_004 Tabelis on teenused, mida on võimalik kasutada blokeerimata diagnostilise seansi ajal.

— Esimeses veerus on võimalikud teenused,

— teises veerus on käesoleva liite jao number, kus see teenus on täpsemalt määratletud,

- kolmandas veerus määratakse nõudesõnumite teenuse identifikaatori väärtused,
- neljandas veerus määratletakse "StandardDiagnosticSession" (SD) teenused, mida igas sõidukiüksuses tuleb rakendada,
- viiendas veerus määratletakse "ECUAdjustmentSession" (ECUAS) teenused, mida tuleb rakendada, et oleks võimalik juhtida sisend-/väljundsignaali sõidukiüksuse kalibreerimispistiku esipaneelil,
- kuuendas veerus määratletakse "ECUProgrammingSession" (ECUPS) teenused, mida tuleb rakendada, et oleks võimalik programmeerida parameetreid sõidukiüksuses.

Tabel 1

Teenuseidentifikaatori väärtuse kokkuvõte

Diagnostilise teenuse nimi	Jao nr	Nõude SID väärtus	Diagnostilised seansid		
			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		■	

■ Sümbol näitab, et teenus on selles diagnostilises seansis kohustuslik.
Sümboli puudumine näitab, et teenus ei ole selles diagnostilises seansis lubatud.

3.2. Vastusekoodid

Iga teenuse vastusekoodid on määratletud.

4. SIDETEENUSED

Mõned teenused on vajalikud side loomiseks ja pidamiseks. Need ei esine rakenduskihis. Võimalikud teenused on esitatud järgmises tabelis.

Tabel 2

Sideteenused

Teenuse nimi	Kirjeldus
StartCommunication	Klient nõuab sideseansi alustamist serveri(te)ga
StopCommunication	Klient nõuab käimasoleva sideseansi lõpetamist
TesterPresent	Klient näitab serverile, et ta on veel aktiivne

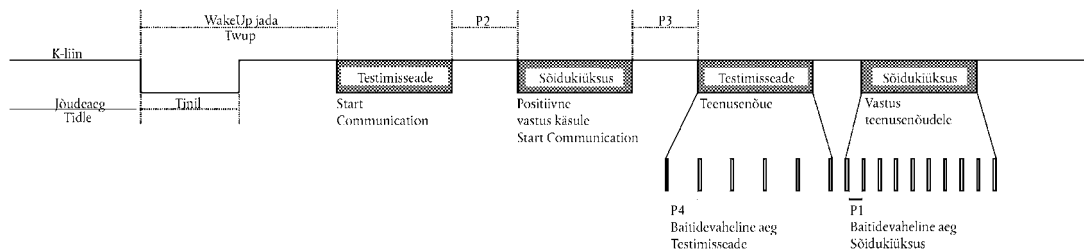
CPR_005 Teenust StartCommunication kasutatakse side alustamiseks. Mis tahes teenuse läbiviimiseks tuleb algatada side ja sideparameetrid peavad olema soovitud mooduseks kohased.

4.1. Teenus StartCommunication

CPR_006 Saades StartCommunication indikatsiooniprimitiivi, kontrollib sõidukiüksus, kas nõutud sideühenduse saab olemasolevatel tingimustel luua. Sideühenduse loomiseks kehtivaid tingimusi on kirjeldatud dokumendis ISO 14230-2.

CPR_007 Seejärel viib sõidukiüksus läbi kõik toimingud, mis on vajalikud sideühenduse loomiseks, ja saadab StartCommunication vastuseprimitiivi koos valitud Positive Response parameetritega.

- CPR_008 Kui sõidukiüksus, mis on juba initsialiseeritud (ja on lülitunud diagnostilisse seanssi), saab uue nõude StartCommunication (nt toimumise tõttu testimisseadmes), aktsepteeritakse nõue ja sõidukiüksus initsialiseeritakse uuesti.
- CPR_009 Kui mis tahes põhjusel ei saa sideühendust luua, jätkab sõidukiüksus sama tööd, mida see tegi vahetult enne katset luua sideühendus.
- CPR_010 Nõudesõnum StartCommunication peab olema füüsiliselt adresseeritud.
- CPR_011 Sõidukiüksuse initsialiseerimine teenuste läbiviimiseks toimub "kiirinitsialiseerimise" meetodil,
- enne mis tahes tegevust on siin jõudeajas,
 - seejärel saadab testimisseade initsialiseerimisjada,
 - kogu vajalik teave sideühenduse loomiseks sisaldub sõidukiüksuse vastuses.
- CPR_012 Pärast initsialiseerimise lõpetamist
- reguleeritakse kõik sideparameetrid tabelis 4 määratletud väärtustele vastavalt võtmebaitidele,
 - sõidukiüksus ootab testimisseadme esimest nõuet,
 - sõidukiüksus on diagnoosimise vaikemooduses, s.o StandardDiagnosticSession'is,
 - kalibreerimise sisend-/väljundsignaalliin on vaikeolekus, s.o välja lülitatud.
- CPR_014 Andmeedastuskiirus K-liinis on 10 400 boodi.
- CPR_016 Testimisseade alustab kiire initsialiseerimise, edastades K-liinil WakeUp jada. Jada algab Tinil-aja pikkuse loogilise tasandi pidamisega nullis pärast K-liini jõudeaega. Testimisseade edastab teenuse StartCommunication esimese biti pärast seda, kui signaali esimesest laskuvast servast on kulunud aeg Twup.



- CPR_017 Kiire initsialiseerimise ja üldise edastamise ajastusväärtused on allpool olevates tabelites. Jõudeajal on erinevad võimalused:
- esimene edastus pärast sisselülitamist $T_{idle} = 300$ ms.
 - pärast teenuse StopCommunication lõpetamist $T_{idle} = P3$ min.
 - pärast edastamise lõpetamist P3 maksimaalväärtusele vastava ooteaja möödumisel $T_{idle} = 0$.

Tabel 3

Kiire initsialiseerimise ajastusväärtused

Parameeter	Minimaalväärtus	Maksimaalväärtus
Tinil	25 ± 1 ms	26 ms
Twup	50 ± 1 ms	51 ms

Tabel 4

Edastamise ajastusväärtused

Ajastusparameeter	Parameetri kirjeldus	Alumised piirväärtused (ms)	Ülemised piirväärtused (ms)
		minimaalne	maksimaalne
P1	Sõidukiüksuse vastuse baitidevaheline aeg	0	20
P2	Testimisseadme nõude ja sõidukiüksuse vastuse või sõidukiüksuse kahe vastuse vaheline aeg	25	250
P3	Sõidukiüksuse vastuste ja testimisseadme uue nõude vaheline aeg	55	5 000
P4	Testimisseadme nõude baitidevaheline aeg	5	20

CPR_018 Kiire initsialiseerimise sõnumivorming on järgmistes tabelites.

Tabel 5

Nõudesõnum StartCommunication

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	81	FMT
#2	Sihtaadressibait	EE	TGT
#3	Allikaadressibait	tt	SRC
#4	Nõude StartCommunication teenuseidentifikaator	81	SCR
#5	Kontrollsumma	00-FF	CS

Tabel 6

Nõudele StartCommunication saadetak positiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	Nõude StartCommunication positiivse vastuse teenuseidentifikaator	C1	SCRPR
#6	1. võtmebait	EA	KB1
#7	2. võtmebait	8F	KB2
#8	Kontrollsumma	00-FF	CS

CPR_019 Nõudesõnumile StartCommunication negatiivset vastust ei ole; kui sõidukiüksuse initsialiseerimisel ei ole edastada positiivset vastusesõnumit, ei edastata midagi ja see jääb tavalisse toimimismoodusesse.

4.2. Teenus StopCommunication

4.2.1. Sõnumi kirjeldus

Selle sidekihi teenuse eesmärk on lõpetada sideseanss.

CPR_020 Saades StopCommunication indikatsioonipritiivi, kontrollib sõidukiüksus, kas hetketingimused võimaldavad sidet lõpetada. Sellisel juhul viib sõidukiüksus läbi kõik tegevused, mis on vajalikud side lõpetamiseks.

- CPR_021 Kui sidet on võimalik lõpetada, annab sõidukiüksus enne side lõpetamist StopCommunication vastuseprimitiivi koos valitud positiivse vastuse (Positive Response) parameetritega.
- CPR_022 Kui mingil põhjusel side lõpetamine ei ole võimalik, annab sõidukiüksus StopCommunication vastuseprimitiivi koos valitud negatiivse vastuse (Negative Response) parameetritega.
- CPR_023 Kui sõidukiüksus tuvastab aja P3max lõppemise, lõpetatakse side ilma igasuguse vastuseprimitiivi andmiseta.

4.2.2. Sõnumivorming

- CPR_024 StopCommunication primitiivide sõnumivormingud on järgmistes tabelites.

Tabel 7

Nõudesõnum StopCommunication

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Allikaadressibait	tt	SRC
#4	Lisapikkusebait	01	LEN
#5	Nõude StopCommunication teenuseidentifikaator	82	SPR
#6	Kontrollsumma	00-FF	CS

Tabel 8

Nõudele StopCommunication saadetak positiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	01	LEN
#5	Nõude StopCommunication positiivse vastuse teenuseidentifikaator	C2	SPRPR
#6	Kontrollsumma	00-FF	CS

Tabel 9

Nõudele StopCommunication saadetak negatiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	Negatiivse vastuse teenuseidentifikaator	7F	NR
#6	Nõude StopCommunication teenuseidentifikaator	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Kontrollsumma	00-FF	CS

4.2.3. Parameetri määratlus

Käesolev teenus ei nõua ühegi parameetri määramist.

4.3. Teenus TesterPresent

4.3.1. Sõnumi kirjeldus

Testimisseade kasutab teenust TesterPresent näitamaks serverile, et see on veel valmisolekus ning et server ei läheks automaatselt tagasi tavalisse toimimismoodusesse ega peataks juhuslikult side. Perioodiliselt saadetav teenus hoiab diagnostilise seansi/side aktiivsesena, lähtestades P3 taimeri iga kord, kui see teenusenõue saadakse.

4.3.2. Sõnumivorming

CPR_079 TesterPresent primitiivide sõnumivormingud on järgmistes tabelites.

Tabel 10

Nõudesõnum TesterPresent

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Allikaadressibait	tt	SRC
#4	Lisapikkusebait	02	LEN
#5	Nõude TesterPresent teenuseidentifikaator	3E	TP
#6	Sub Function = responseRequired = [yes no]	01 02	RESPREQ_Y RESPREQ_NO
#7	Kontrollsumma	00-FF	CS

CPR_080 Kui parameeter responseRequired on reguleeritud jaatavalt, vastab server järgmise positiivse vastusesõnumiga. Kui see on reguleeritud eitavalt, server vastust ei saada.

Tabel 11

Nõudele TesterPresent saadetav positiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	01	LEN
#5	Nõude TesterPresent positiivse vastuse teenuseidentifikaator	7E	TPPR
#6	Kontrollsumma	00-FF	CS

CPR_081 Teenus toetab järgmisi negatiivsete vastuste koode:

Tabel 12

Nõudele TesterPresent saadetak negatiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	Negatiivse vastuse teenuseidentifikaator	7F	NR
#6	Nõude TesterPresent teenuseidentifikaator	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat incorrectMessageLength]	12 13	RC_SFNS_IF RC_IML
#8	Kontrollsumma	00-FF	CS

5. HALDUSTEENUSED

Kasutatavad teenused on esitatud järgmises tabelis.

Tabel 13

Haldusteenused

Teenuse nimi	Kirjeldus
StartDiagnosticSession	Klient nõuab sõidukiüksusega diagnostilise seansi alustamist
SecurityAccess	Klient nõuab pääsu funktsioonidele, mida saavad kasutada ainult volitatud kasutajad

5.1. Teenus StartDiagnosticSession

5.1.1. Sõnumi kirjeldus

CPR_025 Teenust StartDiagnosticSession kasutatakse selleks, et oleks võimalik serveris läbi viia erinevaid diagnostilisi seansse. Diagnostiline seanss võimaldab kasutada konkreetseid teenuseid vastavalt tabelile 17. Seanss võib võimaldada sõiduki tootja omaseid teenuseid, mis ei ole käesoleva dokumendi osaks. Rakenduseeskirjad vastavad järgmistele nõuetele:

- sõidukiüksuses on alati täpselt üks diagnostiline seanss aktiivne,
- sõidukiüksus käivitab toite sisselülitamisel alati seansi StandardDiagnosticSession. Kui ühtki muud diagnostilist seanssi ei käivitata, töötab StandardDiagnosticSession, kuni sõidukiüksus on toitega ühendatud,
- kui testimisseade nõuab diagnostilist seanssi, mis on juba käivitatud, saadab sõidukiüksus positiivse vastuse sõnumi,
- alati kui testimisseade nõuab uut diagnostilist seanssi, saadab sõidukiüksus alustuseks StartDiagnosticSession positiivse vastusesõnumi enne uue seansi aktiveerumist sõidukiüksuses. Kui sõidukiüksus ei saa uut nõutud diagnostilist seanssi käivitada, vastab see StartDiagnosticSession negatiivse vastusesõnumiga ning hetkeseanss jätkub.

CPR_026 Diagnostiline seanss käivitatakse ainult siis, kui on loodud side kliendi ja sõidukiüksuse vahel.

CPR_027 Tabelis 4 määratletud ajastusparameetrid aktiveeritakse pärast edukat käsku StartDiagnosticSession, mille diagnosticSession parameeter on nõudesõnumis reguleeritud asendisse StandardDiagnosticSession, kui enne oli aktiivne mõni muu diagnostiline seanss.

5.1.2. Sõnumivorming

CPR_028 StartDiagnosticSession primitiivide sõnumivormingud on järgmistes tabelites.

Tabel 14

Nõudesõnum StartDiagnosticSession

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Allikaadressibait	tt	SRC
#4	Lisapikkusebait	02	LEN
#5	Nõude StartDiagnosticSession teenuseidentifikaator	10	STDS
#6	diagnosticSession = (üks väärtus tabelist 17)	xx	DS_...
#7	Kontrollsumma	00-FF	CS

Tabel 15

Nõudele StartDiagnosticSession saadetav positiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	02	LEN
#5	Nõude StartDiagnosticSession positiivse vastuse teenuseidentifikaator	50	STDSPR
#6	DiagnosticSession = (sama väärtus kui baidis nr 6 tabelis 14)	xx	DS_...
#7	Kontrollsumma	00-FF	CS

Tabel 16

Nõudele StartDiagnosticSession saadetav negatiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	Negatiivse vastuse teenuseidentifikaator	7F	NR
#6	Nõude StartDiagnosticSession teenuseidentifikaator	10	STDS
#7	ResponseCode = (subFunctionNotSupported ^(a))	12	RC_SFNS
	incorrectMessageLength ^(b))	13	RC_IML
	conditionsNotCorrect ^(c))	22	RC_CNC
#8	Kontrollsumma	00-FF	CS

^(a) Nõudesõnumi baiti nr 6 sisestatud väärtusel puudub tugi, st seda ei ole tabelis 17.

^(b) Sõnumi pikkus on vale.

^(c) Nõude StartDiagnosticSession kriteeriumid ei ole täidetud.

5.1.3. Parameetri määratlus

CPR_029 Teenus StartDiagnosticSession kasutab serveri(te) konkreetse käitumise valimiseks parameetrit *diagnosticSession* (DS_). Käesolevas dokumendis on määratletud järgmised diagnostilised seansid.

Tabel 17

diagnosticSession väärtuste määratlused

Hex	Kirjeldus	Mnemoonika
81	StandardDiagnosticSession See diagnostiline seans võimaldab kõiki teenuseid, mis on määratletud tabeli 1 4. veerus "SD". Need teenused võimaldavad lugeda andmeid serverilt (sõidukiüksusest). See diagnostiline seans on aktiveeritud pärast side loomise edukat lõpetamist kliendi (testimiseseade) ja serveri (sõidukiüksus) vahel. Käesolevas jaos määratletud muud diagnostilised seansid võivad käesoleva diagnostilise seansi üle kirjutada.	SD
85	ECUProgrammingSession See diagnostiline seans võimaldab kõiki teenuseid, mis on määratletud tabeli 1 6. veerus "ECUPS". Need teenused toetavad serveri (sõidukiüksuse) mälu programmeerimist. Käesolevas osas määratletud muud diagnostilised seansid võivad käesoleva diagnostilise seansi üle kirjutada.	ECUPS
87	ECUAdjustmentSession See diagnostiline seans võimaldab kõiki teenuseid, mis on määratletud tabeli 1 5. veerus "ECUAS". Need teenused toetavad serveri (sõidukiüksuse) sisend-/väljundsignaali juhtimist. Käesolevas osas määratletud muud diagnostilised seansid võivad käesoleva diagnostilise seansi üle kirjutada.	ECUAS

5.2. Teenus SecurityAccess

Kalibreerimisandmete kirjutamine või pääs kalibreerimise sisend-/väljundliinile on võimalik ainult siis, kui sõidukiüksus on KALIBREERIMISE mooduses. Enne pääsu lubamist KALIBREERIMISE moodusesse tuleb lisaks kehtiva töökojakaardi sisestamisele sõidukiüksusesse sisestada sõidukiüksusesse ka kohane PIN-kood.

Teenuse SecurityAccess abil saab sisestada PIN-koodi ja näidata testimisseadmele, kas sõidukiüksus on KALIBREERIMISE mooduses või mitte.

PIN-koodi sisestamine alternatiivsete meetodite abil on lubatud.

5.2.1. Sõnumi kirjeldus

Teenus SecurityAccess koosneb teenusesõnumist requestSeed, millele järgneb teenusesõnum sendKey. Teenus SecurityAccess tuleb läbi viia pärast teenust StartDiagnosticSession.

- CPR_033 Testimiseseade kasutab teenuse sõnumit requestSeed, et kontrollida, kas sõidukiüksus on valmis PIN-koodi aktsepteerima.
- CPR_034 Kui sõidukiüksus on juba KALIBREERIMISE mooduses, vastab see nõudele, saates "seemnejada" 0x0000, kasutades teenuse SecurityAccess positiivset vastust..
- CPR_035 Kui sõidukiüksus on valmis töökojakaardi abil PIN-koodi kontrollimiseks, vastab see nõudele, saates "seemnejada", mis on suurem kui 0x0000, kasutades teenuse SecurityAccess positiivset vastust.
- CPR_036 Kui sõidukiüksus ei ole valmis testimisseadmelt PIN-koodi aktsepteerimiseks, sest sisestatud töökojakaart ei ole kehtiv või töökojakaarti ei ole sisestatud või sõidukiüksus ootab PIN-koodi muu meetodi abil, vastab see nõudele negatiivse vastusega, mille vastusekood on reguleeritud vastuses conditionsNotCorrectOrRequestSequenceError.
- CPR_037 Seejärel kasutab testimisseade teenusesõnumit sendKey, et edastada sõidukiüksusele PIN-kood. Andmaks aega kaardi autentimisprotsessi toimumiseks kasutab sõidukiüksus negatiivset vastust koodiga requestCorrectlyReceived-ResponsePending, et pikendada vastamiseks kuluvat aega. Kuid vastamiseks kulub maksimaalset aega ei või ületada viit minutit. Kohe pärast nõutud teenuse lõpetamist saadab sõidukiüksus positiivse vastusesõnumi või negatiivse vastusesõnumi, mille vastusekood on sellest erinev. Sõidukiüksus võib korrata negatiivset vastusekoodi requestCorrectlyReceived-ResponsePending kuni nõutud teenuse lõpetamiseni ja lõpliku vastusesõnumi saatamiseni.

CPR_038 Sõidukiüksus vastab sellele nõudele, kasutades teenuse SecurityAccess positiivset vastust ainult KALIBREERIMISE mooduses.

CPR_039 Järgmistel juhtudel saadab sõidukiüksus sellele nõudele negatiivse vastuse, mille vastusekood on:

- subFunctionNot supported: allfunktsiooni parameetri (accessType) kehtetu vorming,
- conditionsNotCorrectOrRequestSequenceError: sõidukiüksus ei ole valmis sisestatud PIN-koodi aktsepteerima,
- invalidKey: PIN-kood ei ole kehtiv, kuid PIN-koodi lubatud sisestusarv ei ole ületatud,
- exceededNumberOfAttempts: PIN-kood ei ole kehtiv ja PIN-koodi lubatud sisestusarv on ületatud,
- generalReject: PIN-kood on õige, kuid vastastikune autentimine töökojakaardiga ebaõnnestus.

5.2.2. Sõnumivorming — SecurityAccess — requestSeed

CPR_040 SecurityAccess requestSeed primitiivide sõnumivormingud on järgmistes tabelites.

Tabel 18

Nõude SecurityAccess sõnum requestSeed

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Allikaadressibait	tt	SRC
#4	Lisapikkusebait	02	LEN
#5	Nõude SecurityAccess teenuseidentifikaator	27	SA
#6	accessType — requestSeed	7D	AT_RSD
#7	Kontrollsumma	00-FF	CS

Tabel 19

Nõude SecurityAccess sõnumile requestSeed saadetak positiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	04	LEN
#5	Nõude SecurityAccess positiivse vastuse teenuseidentifikaator	67	SAPR
#6	accessType — requestSeed	7D	AT_RSD
#7	“Seemne” tähtsaim bait	00-FF	SEEDH
#8	“Seemne” kõige vähem tähtis bait	00-FF	SEEDL
#9	Kontrollsumma	00-FF	CS

Tabel 20

Nõudele SecurityAccess saadetakv negatiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	Negatiivse vastuse teenuseidentifikaator	7F	NR
#6	Nõude SecurityAccess teenuseidentifikaator	27	SA
#7	responseCode = (conditionsNotCorrectOrRequestSequenceError incorrectMessageLength)	22	RC_CNC
		13	RC_IML
#8	Kontrollsumma	00-FF	CS

5.2.3. Sõnumivorming — SecurityAccess — sendKey

CPR_041 SecurityAccess sendKey primitiivide sõnumivormingud on järgmistes tabelites.

Tabel 21

Nõude SecurityAccess sõnum sendKey

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Allikaadressibait	tt	SRC
#4	Lisapikkusebait	m+2	LEN
#5	Nõude SecurityAccess teenuseidentifikaator	27	SA
#6	accessType — sendKey	7E	AT_SK
#7 kuni #m+6	1. võti (tähtsaim bait)	xx	KEY
	
	Võti nr "m" (kõige vähem tähtis bait, m peab olema vähemalt 4 ja kuni 8)	xx	
#m+7	Kontrollsumma	00-FF	CS

Tabel 22

Nõude SecurityAccess sõnumile sendKey saadetakv positiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	02	LEN
#5	Nõude SecurityAccess positiivse vastuse teenuseidentifikaator	67	SAPR
#6	accessType — sendKey	7E	AT_SK
#7	Kontrollsumma	00-FF	CS

Tabel 23

Nõudele SecurityAccess saadetak negatiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	Negatiivse vastuse teenuseidentifikaator	7F	NR
#6	Nõude SecurityAccess teenuseidentifikaator	27	SA
#7	ResponseCode = (generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending)	78	RC_RCR_RP
#8	Kontrollsumma	00-FF	CS

6. ANDMEEDASTUSTEENUSED

Kasutatavad teenused on esitatud järgmises tabelis.

Tabel 24

Andmeedastusteenused

Teenuse nimi	Kirjeldus
ReadDataByIdentifier	Klient nõuab, et edastataks identifikaatorile recordDataIdentifier pääsu abil kirje hetkeväärtus
WriteDataByIdentifier	Klient nõuab kirje kirjutamist identifikaatorile recordDataIdentifier pääsu kaudu

6.1. Teenus ReadDataByIdentifier

6.1.1. Sõnumi kirjeldus

CPR_050 Klient kasutab teenust ReadDataByIdentifier andmekirjete väärtuste nõudmiseks serverilt. Andmed idendib recordDataIdentifier. Sõidukiüksuse tootja ülesanne on tagada, et serveri tingimused oleksid selle teenuse täitmise ajal täidetud.

6.1.2. Sõnumivorming

CPR_051 ReadDataByIdentifier primitiivide sõnumivormingud on järgmistes tabelites.

Tabel 25

Nõudesõnum ReadDataByIdentifier

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Allikaadressibait	tt	SRC
#4	Lisapikkusebait	03	LEN
#5	Nõude ReadDataByIdentifier teenuseidentifikaator	22	RDBI
#6 ja #7	recordDataIdentifier = (väärtus tabelist 28)	xxxx	RDI_...
#8	Kontrollsumma	00-FF	CS

Tabel 26

Nõudele ReadDataByIdentifier saadetak positiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	m+3	LEN
#5	Nõude ReadDataByIdentifier positiivse vastuse teenuseidentifikaator	62	RDBIPR
#6 ja #7	recordDataIdentifier = (sama väärtus kui baitides #6 ja #7 tabelis 25)	xxxx	RDI_...
#8 kuni #m+7	DataRecord() = (data#1 : data#m)	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrollsumma	00-FF	CS

Tabel 27

Nõudele ReadDataByIdentifier saadetak negatiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	Negatiivse vastuse teenuseidentifikaator	7F	NR
#6	Nõude ReadDataByIdentifier teenuseidentifikaator	22	RDBI
#7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Kontrollsumma	00-FF	CS

6.1.3. Parameetri määratlus

CPR_052 Nõudesõnumis ReadDataByIdentifier idendib parameeter recordDataIdentifier (RDI_) andmekirje.

CPR_053 Käesolevas dokumendis määratletud recordDataIdentifier väärtused on esitatud järgmises tabelis.

recordDataIdentifier tabel koosneb neljast veerust ja paljudest ridadest.

- Esimene veerg (Hex) sisaldab kolmandas veerus määratletud identifikaatorile recordDataIdentifier omistatud kuuestkümnendsüsteemis väärtust.
- Teises veerus (andmeelement) määratletakse 1. liite andmeelement, millel recordDataIdentifier põhineb (mõnikord on vaja transkodeerida).
- Kolmandas veerus (kirjeldus) määratletakse vastava identifikaatori recordDataIdentifier nimi.
- Neljandas veerus (mnemoonika) määratletakse selle identifikaatori recordDataIdentifier mnemoonika.

Tabel 28

Identifikaatori ecorecordDataIdentifier väärtuste määratlused

Hex	Andmeelement	Identifikaatori RecordDataIdentifier nimi (vt vorming jaos 8.2)	Mnemoonika
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 ReadDataByIdentifier positiivne vastusesõnum kasutab parameetrit dataRecord (DREC_) recordDataIdentifier'i identitud andmekirje väärtuse esitamiseks kliendile (testimiseade). Andmevormingud on määratletud 8. jaos. Lisaks võib rakendada kasutaja valitavaid sõidukiüksuseomaseid dataRecords parameetreid, nagu andmed sisendi ja väljundi kohta ning siseandmed, kuid need ei ole käesolevas dokumendis määratletud.

6.2. Teenus WriteDataByIdentifier

6.2.1. Sõnumi kirjeldus

CPR_056 lient kasutab teenust WriteDataByIdentifier andmekirjete väärtuste kirjutamiseks serverile. Andmed idendib recordDataIdentifier. Sõidukiüksuse tootja ülesanne on tagada, et serveri tingimused oleksid selle teenuse täitmise ajal täidetud. Tabelis 28 loetletud parameetrite ajakohastamiseks peab sõidukiüksus olema KALIBREERIMISE mooduses.

6.2.2. Sõnumivorming

CPR_057 WriteDataByIdentifier primitiivide sõnumivormingud on järgmistes tabelites.

Tabel 29

Nõudesõnum WriteDataByIdentifier

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Allikaadressibait	tt	SRC
#4	Lisapikkusebait	m+3	LEN
#5	Nõude WriteDataByIdentifier teenuseidentifikaator	2E	WDBI
#6 ja #7	recordDataIdentifier = (väärtus tabelist 28)	xxxx	RDI_...
#8 kuni #m+7	DataRecord() = (data#1 : data#m)	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrollsumma	00-FF	CS

Tabel 30

Nõudele WriteDataByIdentifier saadetakse positiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	Nõude WriteDataByIdentifier positiivse vastuse teenuseidentifikaator	6E	WDBIPR
#6 ja #7	recordDataIdentifier = (sama väärtus kui baitides #6 ja #7 tabelis 29)	xxxx	RDI_...
#8	Kontrollsumma	00-FF	CS

Tabel 31

Nõudele WriteDataByIdentifier saadetakse negatiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	Negatiivse vastuse teenuseidentifikaator	7F	NR
#6	Nõude WriteDataByIdentifier teenuseidentifikaator	2E	WDBI
#7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Kontrollsumma	00-FF	CS

6.2.3. Parameetri määratlus

Parameeter recordDataIdentifier (RDI_) on määratletud tabelis 28.

Nõudesõnum ReadDataByIdentifier kasutab parameetrit dataRecord (DREC_) identifikaatori recordDataIdentifier identidud andmekirje väärtuste esitamiseks serverile (sõidukiüksus). Andmevormingud on määratletud 8. jaos.

7. TESTIMPULSSIDE JUHTIMINE — SISEND-/VÄLJUNDSIGNAALI JUHTIMISE FUNKTSIONAALNE ÜKSUS

Kasutatavad teenused on esitatud järgmises tabelis.

Tabel 32

Sisend-/väljundsignaali juhtimise funktsionaalne üksus

Teenuse nimi	Kirjeldus
InputOutputControlByIdentifier	Klient nõuab serveriomase sisend-/väljundsignaali juhtimist

7.1. Sõnumi kirjeldus**7.1.1. Sõnumi kirjeldus**

Esipistiku kaudu on ühendus, mis võimaldab sobiva testimisseadme abil juhtida või kontrollida testimpulssi.

CPR_058 Kalibreerimise sisend-/väljundsignaalliini võib konfigurioneerida K-liini käsuga, kasutades liini tarvis nõutava sisend- või väljundfunktsiooni valimiseks teenust InputOutputControlByIdentifier. Kasutatavad liini olekud on:

- blokeeritud,
- speedSignalInput, kus kalibreerimise sisend-/väljundsignaalliini kasutatakse kiirusesignaali (testsignaali) sisestamiseks, asendades liikumisanduri kiirusesignaali,
- realTimeSpeedSignalOutputSensor, kus kalibreerimise sisend-/väljundsignaalliini kasutatakse liikumisanduri kiirusesignaali väljastamiseks,
- RTCOutput, kus kalibreerimise sisend-/väljundsignaalliini kasutatakse GMT kellasignaali väljastamiseks.

CPR_059 Liini oleku konfigureerimiseks peab sõidukiüksus olema sisenenud reguleerimisseansi ja olema KALIBREERIMISE mooduses. Reguleerimisseansist või KALIBREERIMISE moodusest väljumisel peab sõidukiüksus tagama, et kalibreerimise sisend-/väljundsignaalliin läheb tagasi "blokeeritud" (vaike-) olekusse.

CPR_060 Kui sõidukiüksuse reaalaja kiirusesignaali sisendliinis võetakse vastu kiiruseimpulssi, kui kalibreerimise sisend-/väljundsignaalliin on reguleeritud sisendile, reguleeritakse kalibreerimise sisend-/väljundsignaalliin väljundile või lülitatakse välja.

CPR_061 Järjestus on järgmine:

- teenuse StartCommunication abil side loomine,
- teenuse StartDiagnosticSession abil reguleerimisseansi sisenemine ja KALIBREERIMISE mooduses olemine (nende kahe toiminguga järjestus ei ole oluline),
- teenuse InputOutputControlByIdentifier abil sisendsignaali muutmine väljundsignaaliks.

7.1.2. Sõnumivorming

CPR_062 InputOutputControlByIdentifier primitiivide sõnumivormingud on järgmistes tabelites.

Tabel 33

Nõudesõnumit InputOutputControlByIdentifier

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Allikaadressibait	tt	SRC
#4	Lisapikkusebait	xx	LEN
#5	Nõude InputOutputControlByIdentifier teenuseindikaator	2F	IOCBI
#6 ja 7	InputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 või #8-kuni #9-ig	ControlOptionRecord = (inputOutputControlParameter — üks väärtus tabelist 36 controlState — üks väärtus tabelist 38 (vt allpool olev märkus))	xx xx	COR_... IOCP_... CS_...
#9 või #10	Kontrollsumma	00-FF	CS

Märkus: parameeter controlState on olemas ainult mõnedel juhtudel (vt 7.1.3).

Tabel 34

Nõudele InputOutputControlByIdentifier saadetav positiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	xx	LEN
#5	Nõudele inputOutputControlByIdentifier saadetava positiivse vastuse teenuseidentifikaator	6F	IOCBIPR
#6 ja 7	inputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 või #8-kuni #9-ig	controlStatusRecord = (inputOutputControlParameter (sama väärtus kui baidis #8 tabelis 33) controlState (sama väärtus kui baidis #9 tabelis 33)) (kui on olemas)	xx xx	CSR_ IOCP_ CS_...
#9 või #10	Kontrollsumma	00-FF	CS

Tabel 35

Nõudele InputOutputControlByIdentifier saadetav negatiivne vastusesõnum

Bait nr	Parameetri nimi	Hex-väärtus	Mnemoonika
#1	Vormingubait — füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Allikaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	Negatiivse vastuse teenuseidentifikaator	7F	NR
#6	Nõude InputOutputControlByIdentifier teenuseindikaator	2F	IOCBI
#7	responseCode = (incorrectMessageLength conditionsNotCorrect requestOutOfRange deviceControlLimitsExceeded)	13 22 31 7A	RC_IML RC_CNC RC_ROOR RC_DCLE
#8	Kontrollsumma	00-FF	CS

7.1.3. Parameetri määratlus

CPR_064 Parameeter inputOutputControlParameter (IOCP_) on määratletud järgmises tabelis.

Tabel 36

Parameetri inputOutputControlParameter väärtuste määratlused

Hex	Kirjeldus	Mnemoonika
00	ReturnControlToECU Väärtus näitab serverile (sõidukiüksus), et testimisseade ei juhi enam kalibreerimise sisend-/väljundsignaalliini.	RCTECU
01	ResetToDefault Väärtus näitab serverile (sõidukiüksus), et sellele on esitatud nõue viia kalibreerimise sisend-/väljundsignaalliin tagasi vaikeolekusse.	RTD
03	ShortTermAdjustment Väärtus näitab serverile (sõidukiüksus), et sellele on esitatud nõue reguleerida kalibreerimise sisend-/väljundsignaalliin väärtusele, mis sisaldub parameetris controlState.	STA

CPR_065 Parameeter controlState on olemas ainult siis, kui inputOutputControlParameter on reguleeritud väärtusele ShortTermAdjustment ning see on määratletud järgmises tabelis.

Tabel 37

Väärtuste controlState määratlused

Moodus	Hex-väärtus	Kirjeldus
Blokeeritud	00	Sisend-/väljundliin on blokeeritud (vaikeolek)
Aktiveeritud	01	Kalibreerimise sisend-/väljundliin aktiveeritud sisendina speedSignalInput
Aktiveeritud	02	Kalibreerimise sisend-/väljundliin aktiveeritud andurina realTimeSpeedSignalOutputSensor
Aktiveeritud	03	Kalibreerimise sisend-/väljundliin aktiveeritud väljundina RTCOutput

8. ANDMEKIRJETE VORMINGUD

Käesolevas jaos on üksikasjad:

- üldeskirjade kohta, mida kohaldatakse erinevate parameetrite suhtes, mida sõidukiüksus edastab testimisseadmele,
- vormingute kohta, mida kasutatakse andmete edastamiseks 6. jaos kirjeldatud andmeedastusteenuste kaudu.

CPR_067 Sõidukiüksus toetab kõiki idenditud parameetreid.

CPR_068 Sõidukiüksuse poolt testimisseadmele nõudesõnumile vastuseks edastatud andmed peavad olema mõõdetavad (st nõutud parameetri hetkeväärtuse on mõõtnud või täheldanud sõidukiüksus).

8.1. Edastatavad parameetriväärtused

CPR_069 Tabelis 38 on määratletud väärtused, mida kasutatakse edastatud parameetri kehtivuse kindlaksmääramiseks.

CPR_070 "Error indicator" alasse jäävate väärtuste puhul näitab sõidukiüksus viivitamata, et kehtivaid parameetreid hetkel ei ole seoses mingi veaga sõidumeerikus.

CPR_071 "Not available" alasse jäävate väärtuste puhul edastab sõidukiüksus sõnumi, mis sisaldab parameetrit, mis ei ole kasutatav või mida see moodul ei toeta. "Not requested" alasse jäävate väärtuste puhul edastab seade käsusõnumi ja idendib need parameetrid, mille puhul vastuvõtvast seadmest vastust ei oodata.

CPR_072 Kui parameetri kehtivate andmete edastamist segab osa rike, tuleks selle parameetri andmete asemel kasutada veaindikaatorit tabeli 38 kohaselt. Kuid kui mõõdetud või arvutatud väärtus on ületanud väärtuse, mis on kehtiv, kuid ületab määratletud parameetri vahemiku, ei tohiks veaindikaatorit kasutada. Andmed tuleks edastada, kasutades kohaseid parameetri minimaal- või maksimaalväärtusi.

Tabel 38

dataRecords vahemikud

Vahemiku nimetus	1 bait (Hex-väärtus)	2 baiti (Hex-väärtus)	4 baiti (Hex-väärtus)	ASCII
Kehtiv signaal	00 kuni FA	0000 kuni FAFF	00000000 kuni FFFFFFFF	1 kuni 254
Parameetriomane indikaator	FB	FB00 kuni FBFF	FB000000 kuni FBFFFFFF	puudub
Edaspidiste indikaatorbittide kasutamiseks	FC kuni FD	FC00 kuni FDFF	FC000000 kuni FDFFFFFF	puudub
Veaindikaator	FE	FE00 kuni FEFF	FE000000 kuni FEFFFFFF	0
Mitte kasutatav või mitte nõutud	FF	FF00 kuni FFFF	FF000000 kuni FFFFFFFF	FF

CPR_073 ASCII koodides kodeeritud parameetrite tarvis jäetakse piirajana ASCII märk “*”.

8.2. dataRecords vormingud

Järgnevates tabelites 40 kuni 44 on üksikasjalikult esitatud vormingud, mida kasutatakse teenustes ReadDataByIdentifier ja WriteDataByIdentifier.

CPR_074 Tabelis 39 on iga parameetri, mille on määratlenud selle recordDataIdentifier, pikkus, eraldusvõime ja toimeulatus.

Tabel 39

dataRecords vorming

Parameeter	Andme-pikkus (baitides)	Eristusvõime	Toimeulatus
TimeDate	8	Üksikasjad tabelis 40	
HighResolutionTotalVehicleDistance	4	5 m/bitt, 0 m nihe	0 kuni + 21 055 406 km
Kfactor	2	0,001 impulssi/m/bitt, nihe 0	0 kuni 64,255 impulssi/m
LfactorTyreCircumference	2	0,123 10 ⁻³ /bitt, nihe 0	0 kuni 8 031 m
WvehicleCharacteristicFactor	2	0,001 impulssi/m/bitt, nihe 0	0 kuni 64,255 impulssi/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Üksikasjad tabelis 41	
SpeedAuthorised	2	1/256 km/h/bitt, nihe 0	0 kuni 250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Üksikasjad tabelis 44	
VIN	17	ASCII	ASCII

CPR_075 Tabelis 40 on üksikasjad parameetri TimeDate erinevate baitide vormingute kohta.

Tabel 40

TimeDate üksikasjalik vorming (parameetri recordDataIdentifier väärtus F00B)

Bait	Parameetri määratlus	Eristusvõime	Toimeulatus
1	Sekundid	0,25 s/bitt, 0 s nihe	0 kuni 59,75 s
2	Minutid	1 min/bitt, 0 min nihe	0 kuni 59 min
3	Tunnid	1 h/bitt, 0 h nihe	0 kuni 23 tundi
4	Kuu	1 kuu/bitt, 0 kuud nihe	1 kuni 12 kuud
5	Päev	0,25 päeva/bitt, 0 päeva nihe (vt märkus allpool olevas tabelis 41)	0,25 kuni 31,75 päeva
6	Aasta	1 aasta/bitt, + aasta 1985 nihe (vt märkus allpool olevas tabelis 41)	aasta 1985 kuni 2235
7	Kohalik minutinihe	1 min/bitt, -125 min nihe	-59 kuni 59 min
8	Kohalik tunni nihe	1 h/bitt, -125 nihe	-23 kuni +23 tundi

CPR_076 Tabelis 41 on üksikasjad parameetri NextCalibrationDate erinevate baitide vormingute kohta.

Tabel 41

NextCalibrationDate üksikasjalik vorming (parameetri recordDataIdentifier väärtus F022)

Bait	Parameetri määratlus	Eristusvõime	Toimeulatus
1	Kuu	1 kuu/bitt, 0 kuud nihe	1 kuni 12 kuud
2	Päev	0,25 päeva/bitt, 0 päeva nihe (vt märkus allpool)	0,25 kuni 31,75 päeva
3	Aasta	1 aasta/bit, + 1985. aasta nihe (vt märkus allpool)	1985. kuni 2235. aasta

Märkus parameetri "päev" kasutamise kohta:

1. Kuupäeva väärtus 0 on kehtetu. Väärtusi 1, 2, 3 ja 4 kasutatakse kuu esimese päeva identimiseks; 5, 6, 7 ja 8 idendivad kuu teist päeva jne.
2. See parameeter ei mõjuta ega eespool olevat tunniparameetrit.

Märkus parameetri "aasta" baidi kasutamise kohta:

Aasta väärtus 0 tähistab aastat 1985; väärtus 1 tähistab aastat 1986 jne.

CPR_078 Tabelis 42 on üksikasjad parameetri VehicleRegistrationNumber erinevate baitide vormingute kohta.

Tabel 42

VehicleRegistrationNumber üksikasjalik vorming (parameetri recordDataIdentifier väärtus F07E)

Bait	Parameetri määratlus	Eristusvõime	Toimeulatus
1	Koodilehekülg (vastavalt 1. liitele)	ASCII	01 kuni 0A
2 kuni 14	Sõiduki registreerimisnumber (vastavalt 1. liitele)	ASCII	ASCII

9. liide

TÜÜBIKINNITUS — MINIMAALSELT NÕUTAVATE KATSETE NIMEKIRI

SISUKORD

1.	Sissejuhatus	469
1.1.	Tüüvikinnitus	469
1.2.	Viited	469
2.	Sõidukiüksuse funktsionaalsed katsed	470
3.	Liikumisanduri funktsionaalsed katsed	473
4.	Sõidumeerikukaartide funktsionaalsed katsed	475
5.	Koostalitlusvõime katsed	476

1. SISSEJUHATUS

1.1. Tüübikinnitus

Sõidumeeriku (või selle osa) või sõidumeerikukaardi EMÜ tüübikinnitus põhineb järgmisel:

- turvalisuse sertifitseerimine, mille viib läbi ITSECI asutus, võrreldes seda käesoleva lisa 10. liitele täielikult vastava turvaeesmärgiga,
- funktsionaalsuse sertifitseerimine, mille viib läbi liikmesriigi asutus, kes tõendab, et katsetatud seade vastab täielikult käesolevale lisale funktsioonide, mõõtmistäpsuse ja keskkonnaomaduste poolest,
- koostalitlusvõime sertifitseerimine, mille viib läbi pädev asutus, kes tõendab, et sõidumeerik (või sõidumeerikukaart) on täielikult koostalitlev vajaliku sõidumeerikukaardi (või sõidumeeriku) mudelitega (vt käesoleva lisa VIII peatükk).

Käesolevas liites määratletakse, millised katsed peab liikmesriigi asutus funktsionaalsete katsete käigus vähemalt läbi viima ja millised katsed peab pädev asutus koostalitlusvõimekatsete käigus vähemalt läbi viima. Nende katsete või katsetüüpide läbiviimiseks vajalik kord ei ole täpsemalt määratletud.

Käesolev liide ei hõlma turvalisuse sertifitseerimise aspekte. Kui mõned tüübikinnituseks vajalikud katsed viiakse läbi turvalisuse hindamise ja sertifitseerimise käigus, ei tule neid katseid uuesti teha. Sellisel juhul võib kontrollida vaid nende turvakatsete tulemusi. Olgu öeldud, et turvalisuse tõendamise käigus eeldatavasti katsetatavad (või eeldatavasti läbiviidavad katsetega lähedalt seotud) nõuded on käesolevas liites tähistatud tärniga (*).

Käesolevas liites käsitletakse sõidumeeriku osadena liikumisanduri ja sõidukiüksuse tüübikinnitust eraldi. Liikumisanduri iga mudeli ja sõidukiüksuse iga mudeli vahelist koostalitlusvõimet ei nõuta, seetõttu võib liikumisandurile tüübikinnituse anda ainult seoses sõidukiüksuse tüübikinnitusega ja vastupidi.

1.2. Viited

Käesolevas liites kasutatakse järgmisi viiteid:

- | | |
|---------------|---|
| IEC 68-2-1 | Environmental testing — Part 2: Tests — Tests A: Cold. 1990 + Amendment 2: 1994. (Keskkonnavalas katsed — 2. osa: Katsed — Katsed A: külm. 1990 + 2. muudatus 1994.) |
| IEC 68-2-2 | Environmental testing — Part 2: Tests — Tests B: Dry heat. 1974 + Amendment 2: 1994. (Keskkonnavalas katsed — 2. osa: Katsed — Katsed B: kuiv kuumus. 1974 + 2. muudatus 1994.) |
| IEC 68-2-6 | Basic environmental testing procedures — Test methods — Test Fc and guidance: Vibration (sinusoidal). 6th edition: 1985. (Keskkonnavalaste katsete põhikord — Katsemeetodid — Katse Fc ja juhised: vibratsioon (sinusoidne). 6. väljaanne, 1985.) |
| IEC 68-2-14 | Basic environmental testing procedures — Test methods — Test N: Change of temperature. Modification 1: 1986. (Keskkonnavalaste katsete põhikord — Katsemeetodid — Katse N: temperatuuri muutus. 1. muudatus, 1986.) |
| IEC 68-2-27 | Basic environmental testing procedures — Test methods — Test Ea and guidance: Shock. Edition 3: 1987. (Keskkonnavalaste katsete põhikord — Katsemeetodid — Katse Ea ja juhised: löögid. 3. väljaanne, 1987.) |
| IEC 68-2-30 | Basic environmental testing procedures — Test methods — Test Db and guidance: Damp heat, cyclic (12 + 12 — hour cycle). Modification 1: 1985. (Keskkonnavalaste katsete põhikord — Katsemeetodid — Katse Db ja juhised: tsükliline niiske kuumus (12+12-tunnine tsükkel). 1. muudatus, 1985.) |
| IEC 68-2-35 | Basic environmental testing procedure — Test methods — Test Fda: Random vibration wide band — Reproducibility High. Modification 1: 1983. (Keskkonnavalaste katsete põhikord — Katsemeetodid — Katse Fda: lairibas toimuv juhuslik vibratsioon — Kõrge reprodutseeritavus. 1. muudatus, 1983.) |
| IEC 529 | Degrees of protection provided by enclosures (IP code). Edition 2: 1989. (Kaitsepiirete kaitsemäärad (IP-kood). 2. väljaanne, 1989.) |
| IEC 61000-4-2 | Electromagnetic Compatibility (EMC) — Testing and measurement techniques — Electrostatic discharge immunity test: 1995/Amendment 1: 1998. (Elakromagnetiline ühilduvus — Katse- ja mõõtetehnikad — Elektrostaatilise lahenduse häirekindluskatse: 1995/ 1. muudatus, 1998.) |
| ISO 7637-1 | Road vehicles — Electrical disturbance by conduction and coupling — Part 1: Passenger cars and light commercial vehicles with nominal 12 V supply voltage — Electrical transient conduction along supply lines only. Edition 2: 1990. (Maanteeõidukid — Juhtivusest ja ühendamisest tingitud elektrilised häired — 1. osa: 12voldise nimivõltpingega sõiduaudod ja väikesed tarbesõidukid — Ainult toiteliinide siirdeelektrijuhtivus. 2. väljaanne, 1990.) |

- ISO 7637-2 Road vehicles — Electrical disturbance by conduction and coupling — Part 1: Passenger cars and light commercial vehicles with nominal 12 V supply voltage — Electrical transient conduction along supply lines only. Edition 2: 1990. (Maanteesõidukid — Juhtivusest ja ühendamisest tingitud elektrilised häired — 1. osa: 12- või 24voldise nimitoitepingega sõiduaudod ja väikesed tarbesõidukid — Ainult toiteliinide siirdeelektrijuhtivus. Teine väljaanne, 1990.)
- ISO 7637-3 Road vehicles — Electrical disturbance by conduction and coupling — Part 3: Vehicles with 12 V or 24 V supply voltage — Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines. First Edition: 1995 + Cor 1: 1995. (Maanteesõidukid — Juhtivusest ja ühendamisest tingitud elektrilised häired — 3. osa: 12- või 24voldise toitepingega sõidukid — Siirdeelektridastus mahtvusliku või induktiivse sidestusega muude liinide kui toiteliinide kaudu. Esimene väljaanne, 1995 + 1. parandus, 1995.)
- ISO/IEC 7816-1 Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics. First edition: 1998. (Identimiskaardid — Kontaktidega kiipkaardid — 1. osa: Füüsilised karakteristikud. Esimene väljaanne, 1998.)
- ISO/IEC 7816-2 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 2. osa: Kontaktide mõõtmed ja asukoht. Esimene väljaanne, 1999.)
- ISO/IEC 7816-3 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 3. osa: Elektroonilised signaalid ja edastusprotokoll. Teine väljaanne, 1997.)
- ISO/IEC 10373 Identification cards — Test methods. First edition: 1993. (Identimiskaardid — Katsemeetodid. Esimene väljaanne, 1993.)

2. SÕIDUKIÜKSUSE FUNKTSIONAALSED KATSED

Nr	Katse	Kirjeldus	Seotud nõuded
1.	Halduslik kontrollimine		
1.1.	Dokumendid	Dokumentide korrektsus	
1.2.	Tootja katsetulemused	Kokkupaneku ajal tootja tehtud katsete tulemused. Kirjalikud tõendid	070, 071, 073
2.	Visuaalne kontroll		
2.1.	Vastavus dokumentidele		
2.2.	Tunnusmärgid/tähistused		168, 169
2.3.	Materjalid		163 kuni 167
2.4.	Plommid		251
2.5.	Välisliidesed		
3.	Funktsionaalsed katsed		
3.1.	Olemasolevad funktsioonid		002, 004, 244
3.2.	Toimimismoodused		006*, 007*, 008*, 009*, 106, 107
3.3.	Funktsioonid ja andmepääsuõigused		010*, 011*, 240, 246, 247
3.4.	Kaartide sisestamise ja väljavõtmise seire		013, 014, 015*, 016*, 106
3.5.	Kiiruse ja vahemaa mõõtmine		017 kuni 026
3.6.	Aja mõõtmine (katse 20 °C juures)		027 kuni 032
3.7.	Juhi tegevuste seire		033 kuni 043, 106
3.8.	Juhtimisstaatuse seire		044, 045, 106
3.9.	Käitsi tehtavad sissekanded		046 kuni 050b
3.10.	Ettevõtetelukkude juhtimine		051 kuni 055
3.11.	Kontrollitegevuste seire		056, 057
3.12.	Sündmuste ja/või rikete avastamine		059 kuni 069, 106

Nr	Katse	Kirjeldus	Seotud nõuded
3.13.	Seadme identimisandmed		075*, 076*, 079
3.14.	Juhikaardi sisestamise ja väljavõtmise andmed		081* kuni 083*
3.15.	Andmed juhi tegevuse kohta		084* kuni 086*
3.16.	Kohaandmed		087* kuni 089*
3.17.	Läbisõidumõõdiku andmed		090* kuni 092*
3.18.	Üksikasjalikud andmed kiiruse kohta		093*
3.19.	Andmed sündmuste kohta		094*, 095
3.20.	Andmed rikete kohta		096*
3.21.	Kalibreerimisandmed		097*, 098*
3.22.	Andmed aja korrigeerimise kohta		100*, 101*
3.23.	Andmed kontrollitegevuse kohta		102*, 103*
3.24.	Andmed ettevõtetelukkude kohta		104*
3.25.	Andmed allalaadimistegevuse kohta		105*
3.26.	Andmed eritingimuste kohta		105a*, 105b*
3.27.	Registreerimine ja salvestamine sõidumeerikukaartidele		108, 109*, 109a*, 110*, 111, 112
3.28.	Kuvamine		072, 106, 113 kuni 128, PIC_001, DIS_001
3.29.	Trükkimine		072, 106, 129 kuni 138, PIC_001, PRT_001 kuni PRT_012
3.30.	Hoiatused		106, 139 kuni 148, PIC_001
3.31.	Andmete allalaadimine välisandmekandjale		072, 106, 149 kuni 151
3.32.	Andmete väljastamine lisavälisseadmetele		152, 153
3.33.	Kalibreerimine		154*, 155*, 156*, 245
3.34.	Kella reguleerimine		157*, 158*
3.35.	Lisafunktsioonide põhjustatud häired		003, 269

Nr	Katse	Kirjeldus	Seotud nõuded
4.	Keskkonnaalased katsed		
4.1.	Temperatuur	<p>Funktsionaalsuse tõendamine järgmisel alusel:</p> <ul style="list-style-type: none"> — IEC 68-2-1, katse Ad, katse kestus madalamal temperatuuril ($-20\text{ }^{\circ}\text{C}$) 72 tundi, 1 tund töötab, 1 tund ei tööta — IEC 68-2-2, katse Bd, katse kestus kõrgemal temperatuuril ($+70\text{ }^{\circ}\text{C}$) 72 tundi, 1 tund töötab, 1 tund ei tööta <p>Temperatuuritsüklid: tõendada, et sõidukiüksus suudab taluda ümbritseva temperatuuri kiireid muutusi IEC 68-2-14 katse Na alusel, 20 tsüklit, iga kord muutub temperatuur madalalt temperatuurilt ($-20\text{ }^{\circ}\text{C}$) kõrgele temperatuurile ($+70\text{ }^{\circ}\text{C}$) ning püsib kaks tundi nii madalal kui kõrgel temperatuuril</p> <p>Madalal temperatuuril, kõrgel temperatuuril ja temperatuuritsüklite ajal võib läbi viia vähendatud katsete kogumi (nende katsete puhul, mis on määratletud käesoleva tabeli 3. osas)</p>	159
4.2.	Niiskus	<p>Tõendada IEC 68-2-30, katse Db alusel, et sõidukiüksus suudab taluda tsüklilist niiskust (kuumuskatse), kuus 24tunnist tsüklit, igas tsüklis kõigub temperatuur vahemikus $+25\text{ }^{\circ}\text{C}$ kuni $+55\text{ }^{\circ}\text{C}$ ning suhteline niiskus on $+25\text{ }^{\circ}\text{C}$ juures 97 % ja $+55\text{ }^{\circ}\text{C}$ juures 93 %</p>	160
4.3.	Vibratsioon	<p>1. Sinusoidne vibratsioon:</p> <p>tõendada, et sõidukiüksus suudab taluda järgmiste omadustega sinusoidset vibratsiooni:</p> <p>püsinihe sagedusalas 5 kuni 11 Hz: maksimaalne 10 mm</p> <p>püsikiirendus sagedusalas 11 kuni 300 Hz: 5 g</p> <p>Seda nõuet tõendatakse IEC 68-2-6, katse Fc alusel, minimaalne katseaeg 3×12 tundi (12 tundi telje kohta)</p> <p>2. Juhuslik vibratsioon:</p> <p>tõendada, et sõidukiüksus suudab taluda järgmiste omadustega juhuslikku vibratsiooni:</p> <p>sagedus 5–150 Hz, tase $0,02\text{ g}^2/\text{Hz}$</p> <p>Seda nõuet tõendatakse IEC 68-2-35, katse Ffda alusel, minimaalne katseaeg 3×12 tundi (12 tundi telje kohta), 1 tund töötab, 1 tund ei tööta</p> <p>Eespool kirjeldatud kaks katset tehakse katsetatava seadmetüübi kahe erineva näidisega</p>	163
4.4.	Kaitse vee ja võõrkehade eest	<p>Tõendada, et sõidukiüksuse kaitseindeks vastavalt standardile IEC 529 on vähemalt IP 40, kui see on töötamistingimustes paigaldatud sõidukile</p>	164, 165
4.5.	Kaitse ülepinge eest	<p>Tõendada, et sõidukiüksus suudab taluda järgmist toitepinget:</p> <p>24V versioonid: 34 V temperatuuril $+40\text{ }^{\circ}\text{C}$ 1 tund</p> <p>12V versioonid: 17 V temperatuuril $+40\text{ }^{\circ}\text{C}$ 1 tund</p>	161
4.6.	Kaitse muudetud polaarsuse eest	<p>Tõendada, et sõidukiüksus suudab taluda toitepinge muudetud polaarsust</p>	161

Nr	Katse	Kirjeldus	Seotud nõuded
4.7.	Kaitse lühiste eest	Tõendada, et sisend-/väljundsignaalid on kaitstud lühiste eest toiteallikaga ja maaga	161
5.	Elektromagnetilise ühilduvuse katsed		
5.1.	Elektromagnetiline kiirgus ja vastuvõtlikkus	Vastavus direktiivile 95/54/EMÜ	162
5.2.	Elektrostaatiline lahen-dus	Vastavus standardile IEC 61000-4-2, ± 2 kV (1. tase)	162
5.3.	Juhtivuslike siirete vastuvõtlikkus vooluallikast	24V versioonid: vastavus standardile ISO 7637-2: impulss 1a: $V_s = -100$ V, $R_i = 10$ oomi impulss 2: $V_s = +100$ V, $R_i = 10$ oomi impulss 3a: $V_s = -100$ V, $R_i = 50$ oomi impulss 3b: $V_s = +100$ V, $R_i = 50$ oomi impulss 4: $V_s = -16$ V $V_a = -12$ V, $t_6 = 100$ ms impulss 5: $V_s = +120$ V, $R_i = 2,2$ oomi, $t_d = 250$ ms 12V versioonid: vastavus standardile ISO 7637-1: impulss 1: $V_s = -100$ V, $R_i = 10$ oomi impulss 2: $V_s = +100$ V, $R_i = 10$ oomi impulss 3a: $V_s = -100$ V, $R_i = 50$ oomi impulss 3b: $V_s = +100$ V, $R_i = 50$ oomi impulss 4: $V_s = -6$ V, $V_a = -5$ V, $t_6 = 15$ ms impulss 5: $V_s = +65$ V, $R_i = 3$ oomi, $t_d = 100$ ms Impulssi 5 katsetatakse ainult nende sõidukiüksuste puhul, mis on mõeldud paigaldamiseks sõidukitele, millel puudub ühine väliskaitse koormuse avarilise vähenemise eest	162

3. LIIKUMISANDURI FUNKTSIONAALSED KATSED

nr	Katse	Kirjeldus	Seotud nõuded
1.	Halduslik kontrollimine		
1.1.	Dokumendid	Dokumentide korrektsus	
2.	Visuaalne kontroll		
2.1.	Vastavus dokumentidele		
2.2.	Tunnusmärgid/tähistused		169, 170
2.3.	Materjalid		163 kuni 167
2.4.	Plommid		251
3.	Funktsionaalsed katsed		
3.1.	Anduri identimisandmed		077*
3.2.	Liikumisanduri ja sõidukiüksuse kokkuühendamine		099*, 155
3.3.	Liikumise tuvastamine		
	Liikumise mõõtmistäpsus		022 kuni 026

nr	Katse	Kirjeldus	Seotud nõuded
4.	Keskkonnaalased katsed		
4.1.	Töötamistemperatuur	Töendada funktsionaalsust (nagu määratletud katses nr 3.3) temperatuurivahemikus [-40 °C; +135 °C] järgmistel alustel: — IEC 68-2-1, katse Ad, katse kestus 96 tundi madalamal temperatuuril Tomin — IEC 68-2-2, katse Ad, katse kestus 96 tundi kõrgemal temperatuuril Tomax	159
4.2.	Temperatuuritsüklid	töendada funktsionaalsus (vastavalt katsele 3.3) IEC 68-2-14 katse Na alusel, 20 tsüklit, iga kord muutub temperatuur madalalt temperatuuril (-40 °C) kõrgemale temperatuurile (+135 °C) ning püsib kaks tundi nii madalamal kui kõrgemal temperatuuril Madalamal temperatuuril, kõrgemal temperatuuril ja temperatuuritsüklite ajal võib läbi viia vähendatud katsete kogumi (nende katsete puhul, mis on määratletud katses 3.3)	159
4.3.	Niiskustsüklid	Töendada funktsionaalsus (vastavalt katsele 3.3) IEC 68-2-30, test Db alusel, koos 24tunnist tsüklit, igas tsüklis kõigub temperatuur vahemikus +25 °C kuni +55 °C ning suhteline niiskus on +25 °C juures 97 % ja +55 °C juures 93 %	160
4.4.	Vibratsioon	Töendada funktsionaalsust (vastavalt katsele 3.3) IEC 68-2-6, katse FC, katse kestus 100 sagedustsüklit: püsinihe sagedusalas 10 kuni 57 Hz: maks 1,5 mm püsikiirendus sagedusalas 57 kuni 500 Hz: 20 g	163
4.5.	Mehaaniline löök	Töendada funktsionaalsust (vastavalt katsele 3.3) IEC 68-2-27, katse Ea, kolmel ristteljel mõlemas suunas 3 lööki	163
4.6.	Kaitse vee ja võõrkehade eest	Töendada, et liikumisanduri kaitseindeks vastavalt standardile IEC 529 on vähemalt IP 64, kui see on töötamistingimustes paigaldatud sõidukile	165
4.7.	Kaitse muudetud polaarsuse eest	Töendada, et liikumisandur suudab taluda toitevoolu muudetud polaarsust	161
4.8.	Kaitse lühiste eest	Töendada, et sisend-/väljundsignaalid on kaitstud lühiste eest toiteallikaga ja maaga	161
5.	Elektromagnetiline ühilduvus		
5.1.	Elektromagnetiline kiirgus ja vastuvõtlikkus	Töendada vastavust direktiivile 95/54/EMÜ	162
5.2.	Elektrostaatiline lahen-dus	Vastavus standardile IEC 61000-4-2, ±2 kV (1. tase)	162
5.3.	Juhtivuslike siirete vastuvõtlikkus andmeliini-dest	Vastavus standardile ISO 7637-3 (III tase)	162

4. SÕIDUMEERIKUKAARTIDE FUNKTSIONAALSED KATSED

nr	Katse	Kirjeldus	Seotud nõuded
1.	Halduslik kontrollimine		
1.1.	Dokumendid	Dokumentide korrektsus	
2.	Visuaalne kontroll		
2.1.		Teha kindlaks, et kõik kaitseomadused ja nähtavad andmed on kaardile korrektselt trükitud ja nõuetekohased	171 kuni 181
3.	Füüsilised katsed		
3.1.		Kontrollida kaardi mõõtmeid ja kontaktide asukohti	184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	Protokolli katsed		
4.1.	ATR signaal	Kontrollida, et ATR signaal on nõuetekohane	ISO/IEC 7816-3 TCS 304, 307, 308
4.2.	T=0	Kontrollida, et protokoll T=0 on nõuetekohane	ISO/IEC 7816-3 TCS 302, 303, 305
4.3.	Käsk PTS	Kontrollida, et käsk PTS on nõuetekohane, muutes T=1 T=0-le	ISO/IEC 7816-3 TCS 309–311
4.4.	T=1	Kontrollida, et protokoll T=1 on nõuetekohane	ISO/IEC 7816-3 TCS 303, / 306
5.	Kaardi struktuur		
5.1.		Katsetada, kas kaardi failstruktuur on nõuetekohane, kontrollides kohustuslike failide olemasolu kaardil ja nende pääsutingimusi	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	Funktsionaalsed katsed		
6.1.	Tavaline andmetöötlus	Katsetada vähemalt kord iga lubatud käsu kasutamist (nt katsetada käsku UPDATE BINARY, kus CLA = '00', CLA = '0C ning P1, P2 ja Lc parameetrid on erinevad) Kontrollida, et kaardil on toimingud tegelikult tehtud (nt lugedes selle faili andmeid, mida käsk puudutas)	TCS 313 kuni TCS 379
6.2.	Veasõnumid	Katsetada vähemalt kord iga käsu iga veasõnumit (vastavalt 2. liitele) Katsetada vähemalt kord iga üldviga (v.a '6400' terviklikkusvead, mida kontrollitakse turvalisuse sertifitseerimise ajal)	
7.	Keskkonnaalased katsed		
7.1.		Teha kindlaks, et kaardid toimivad piirtingimustes, mis on määratletud vastavalt standardile ISO/IEC 10373	185 kuni 188 ISO/IEC 7816-1

5. KOOSTALITLUSVÕIME KATSED

nr	Katse	Kirjeldus
1.	Vastastikune autentimine	Kontrollida, et sõidukiüksuse ja sõidumeerikukaardi vaheline vastastikune autentimine toimiks normaalselt
2.	Kirjutamis-/lugemise katsed	Sooritage tüüpiline tegevusjada sõidukiüksuses. Tegevusjada kohandatakse katsetatava kaarditüübiga ning see hõlmab kirjutamist võimalikult paljudesse elementaarfailidesse kaardil Tõendada kaardilt allalaadimise teel, et kõik vastavad kirjed on nõuetekohaselt tehtud Tõendada kaardi igapäevase väljatrüki teel, et kõiki vastavaid kirjeid saab nõuetekohaselt lugeda

10. liide

ÜLDISED TURBE-EESMÄRGID

Käesolevas liites määratletakse liikumisanduri, sõidukiüksuse ja sõidumeerikukaardi turbe-eesmärkide miinimumnõuded.

Turbe-eesmärkide loomiseks, mille alusel saaks taotleda turbesertifitseerimist, peavad tootjad vastavalt vajadusele välja töötama ja täiustama dokumendid, muutmata ega välja jätmata olemasolevaid ohte, eesmärke, menetlusvahendeid ega turbetagamisfunktsioonide spetsifikaate.

SISUKORD

Liikumisanduri üldine turbe-eesmärk

1.	Sissejuhatus	482
2.	Lühendid, mõisted ja viited	482
2.1.	Lühendid	482
2.2.	Mõisted	482
2.3.	Viited	482
3.	Toote põhimõte	483
3.1.	Liikumisanduri kirjeldus ja kasutusmeetod	483
3.2.	Liikumisanduri elutsükkel	484
3.3.	Ohud	484
3.3.1.	Pääsukontrolli ähvardavad ohud	484
3.3.2.	Konstruksiooniga seotud ohud	485
3.3.3.	Töötamisega seotud ohud	485
3.4.	Turbe-eesmärgid	485
3.5.	Infotehnoloogia turbe-eesmärgid	485
3.6.	Füüsilised, personali- või menetlusvahendid	486
3.6.1.	Seadme konstruktsioon	486
3.6.2.	Seadme tarne	486
3.6.3.	Turbeandmete loomine ja üleandmine	486
3.6.4.	Sõidumeeriku paigaldamine, kalibreerimine ja kontrollimine	486
3.6.5.	Seaduste täitmise kontroll	486
3.6.6.	Tarkvara värskendamine	486
4.	Turbetagamisfunktsioonid	486
4.1.	Identimine ja autentimine	486
4.2.	Pääsukontroll	487
4.2.1.	Pääsukontroll	487
4.2.2.	Andmepääsuõigused	487
4.2.3.	Faili struktuur ja pääsutingimused	487
4.3.	Selgituskohustus	487

4.4.	Audit	488
4.5.	Korrektus	488
4.5.1.	Infovoo kontrollipoliitika	488
4.5.2.	Siseandmeedastus	488
4.5.3.	Salvestatud andmete terviklikkus	488
4.6.	Töökindlus	488
4.6.1.	Katsed	488
4.6.2.	Tarkvara	489
4.6.3.	Füüsiline kaitse	489
4.6.4.	Toiteallika katkestused	489
4.6.5.	Lähtestustingimused	489
4.6.6.	Andmete kättesaadavus	489
4.6.7.	Lisarakendused	489
4.7.	Andmevahetus	489
4.8.	Krüptograafiline tugi	489
5.	Turbemehhanismide määratlus	490
6.	Turbemehhanismide miinimumtugevus	490
7.	Kindlusaste	490
8.	Põhimõte	490
Sõidukiüksuse üldine turbe-eesmärk		
1.	Sissejuhatus	492
2.	Lühendid, mõisted ja viited	492
2.1.	Lühendid	492
2.2.	Mõisted	492
2.3.	Viited	492
3.	Toote põhimõte	492
3.1.	Sõidukiüksuse kirjeldus ja kasutusmeetod	492
3.2.	Sõidukiüksuse elutsüklid	494
3.3.	Ohud	494
3.3.1.	Identimis- ja pääsukontrolli ähvardavad ohud	494
3.3.2.	Konstruksiooniga seotud ohud	495
3.3.3.	Töötamisega seotud ohud	495
3.4.	Turbe-eesmärgid	495
3.5.	Infotehnoloogia turbe-eesmärgid	496
3.6.	Füüsilised, personali- või menetlusvahendid	496
3.6.1.	Seadme konstruktsioon	496
3.6.2.	Seadme tarne ja aktiveerimine	496

3.6.3.	Turbeandmete loomine ja üleandmine	496
3.6.4.	Kaarditarne	497
3.6.5.	Sõidumeeriku paigaldamine, kalibreerimine ja kontrollimine	497
3.6.6.	Seadme töötamine	497
3.6.7.	Seaduste täitmise kontroll	497
3.6.8.	Tarkvara värskendamine	497
4.	Turbetagamisfunktsioonid	497
4.1.	Identimine ja autentimine	497
4.1.1.	Liikumisanduri identimine ja autentimine	497
4.1.2.	Kasutaja identimine ja autentimine	498
4.1.3.	Kaugühendatud ettevõtte identimine ja autentimine	499
4.1.4.	Juhtimisseadme identimine ja autentimine	499
4.2.	Pääsukontroll	499
4.2.1.	Pääsukontroll	499
4.2.2.	Pääsuõigused funktsioonidele	499
4.2.3.	Pääsuõigused andmetele	499
4.2.4.	Faili struktuur ja pääsutingimused	500
4.3.	Selgituskohustus	500
4.4.	Audit	500
4.5.	Objekti taaskasutamine	501
4.6.	Korrektus	501
4.6.1.	Infovoo kontroll	501
4.6.2.	Siseandmeedastus	501
4.6.3.	Salvestatud andmete terviklikkus	501
4.7.	Töökindlus	501
4.7.1.	Katsed	501
4.7.2.	Tarkvara	502
4.7.3.	Füüsiline kaitse	502
4.7.4.	Toiteallika katkestused	502
4.7.5.	Lähtestustingimused	502
4.7.6.	Andmete kättesaadavus	502
4.7.7.	Lisarakendused	502
4.8.	Andmevahetus	502
4.8.1.	Andmevahetus liikumisanduriga	502
4.8.2.	Andmevahetus sõidumeerikukaartidega	503
4.8.3.	Andmevahetus välisandmekandjaga (allalaadimisfunktsioon)	503
4.9.	Krüptograafiline tugi	503

5.	Turbemehhanismide määratlus	503
6.	Turbemehhanismide miinimumtugevus	503
7.	Kindlusaste	503
8.	Põhimõte	504

Sõidumeerikukaardi üldine turbe-eesmärk

1.	Sissejuhatus	508
2.	Lühendid, mõisted ja viited	508
2.1.	Lühendid	508
2.2.	Mõisted	509
2.3.	Viited	509
3.	Toote põhimõte	509
3.1.	Sõidumeerikukaardi kirjeldus ja kasutusmeetod	509
3.2.	Sõidumeerikukaardi elutsükkel	509
3.3.	Ohud	510
3.3.1.	Lõppeesmärgid	510
3.3.2.	Manipuleerimisteed	510
3.4.	Turbe-eesmärgid	510
3.5.	Infotehnoloogia turbe-eesmärgid	510
3.6.	Füüsilised, personali- või menetlusvahendid	510
4.	Turbetagamisfunktsioonid	511
4.1.	Vastavus kaitseprofiilidele	511
4.2.	Kasutaja identimine ja autentimine	511
4.2.1.	Kasutaja identifitseerimine	511
4.2.2.	Kasutaja autentimine	511
4.2.3.	Autentimise ebaõnnestumised	511
4.3.	Pääsukontroll	512
4.3.1.	Pääsukontroll	512
4.3.2.	Pääsukontrolli funktsioonid	512
4.4.	Selgituskohustus	512
4.5.	Audit	512
4.6.	Korrektus	512
4.6.1.	Salvestatud andmete terviklikkus	512
4.6.2.	Põhiandmete autentimine	512
4.7.	Töökindlus	513
4.7.1.	Katsed	513
4.7.2.	Tarkvara	513
4.7.3.	Toiteallikas	513

4.7.4.	Lähtestustingimused	513
4.8.	Andmevahetus	513
4.8.1.	Andmevahetus sõidukiüksusega	513
4.8.2.	Andmete eksport mujale kui sõidukiüksusesse (allalaadimisfunktsioon)	513
4.9.	Krüptograafiline tugi	513
5.	Turbemehhanismide määratlus	513
6.	Turbemehhanismide nõutav miinimumtugevus	514
7.	Kindlusaste	514
8.	Põhimõte	514

LIIKUMISANDURI ÜLDINE TURBE-EESMÄRK

1. Sissejuhatus

Käesolev dokument sisaldab liikumisanduri kirjeldust, ohte, millele see peab suutma avaldada vastutoimet, ja turbeeesmärke, mida see peab täitma. Siin on määratletud nõutavad turbetagamisfunktsioonid. Siin on esitatud turbemehhanismide väidetav miinimumtugevus ning arengu- ja hindamiseks nõutav kindlusaste.

Nõuded, millele dokumendis viidatakse, sisalduvad IB lisa põhiosas. Selguse huvides on kohati IB lisa põhinõuded ja turvanõuded duplitseeritud. Kui turbenõude ja IB lisa põhinõude vahel, millele viidatakse selles turbenõudes, on ebaselgus, jääb ülimalikuks IB lisa põhinõue.

IB lisa põhinõuded, millele turbe-eesmärkides ei viidata, ei kuulu turbetagamisfunktsioonide alla.

Ohtudele, eesmärkidele, menetlusvahenditele ja turbetagamisfunktsioonide spetsifikaatidele on antud kordumatud nimed nende jälgitavuseks arengu- ja hindamisdokumentides.

2. Lühendid, mõisted ja viited

2.1. Lühendid

ROM	(read only memory) püsimälu
SEF	(security enforcing function) turbetagamisfunktsioon
TBD	(to be defined) määratletakse hiljem
TOE	(target of evaluation) hindamisobjekt
VU	(vehicle unit) sõidukiüksus

2.2. Mõisted

Digitaalne sõidumeerik	Sõidumeerik
Üksus	Liikumisanduri külge ühendatud seade
Liikumisandmed	Sõidukiüksusega vahetatavad andmed, mis puudutavad kiirust ja läbitud vahemaad
Füüsiliselt eraldatud osad	Sõidukis asuvad liikumisanduri füüsilised osad, mis on vastandiks liikumisanduri korpusasuvatele füüsilistele osadele
Turbeandmed	Konkreetsed andmed, mida on vaja turbetagamisfunktsioonide toetamiseks (nt krüptovõtmed)
Süsteem	Sõidumeerikuga mis tahes kombel seotud seadmed, inimesed või organisatsioonid
Kasutaja	Liikumisandurit kasutav isik (kui ei ole kasutatud väljendis "kasutajaandmed")
Kasutajaandmed	Liikumisanduris salvestatud mis tahes andmed, v.a liikumis- või turbeandmed

2.3. Viited

ITSEC (Information Technology Security Evaluation Criteria) infotehnoloogia turvalisuse hindamiskriteeriumid 1991.

3. Toote põhimõte

3.1. Liikumisanduri kirjeldus ja kasutusmeetod

Liikumisandur on mõeldud paigaldamiseks mootorsõidukitesse. Selle eesmärk on anda sõidukiüksusele turvalised liikumisandmed, mis puudutavad sõiduki kiirust ja läbitud vahemaad.

Liikumisandur on mehaaniliselt liidetud sõiduki liikuva osaga, mille liikumine võib kajastada sõiduki kiirust või läbitud vahemaad. See võib asuda sõiduki käigukastis või mis tahes muus sõiduki osas.

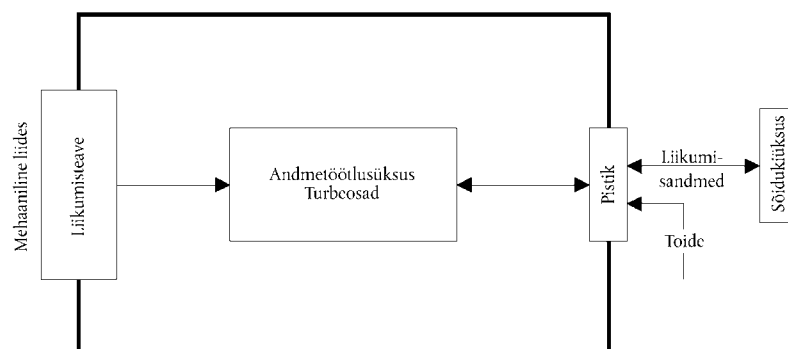
Toimimismooduses on liikumisandur ühendatud sõidukiüksusega.

Halduseesmärkidel võib seda ühendada ka eriseadme külge (tootja määratleb hiljem).

Tüüpilise liikumisanduri kirjeldus on järgmisel joonisel:

Joonis 1

Tüüpiline liikumisandur

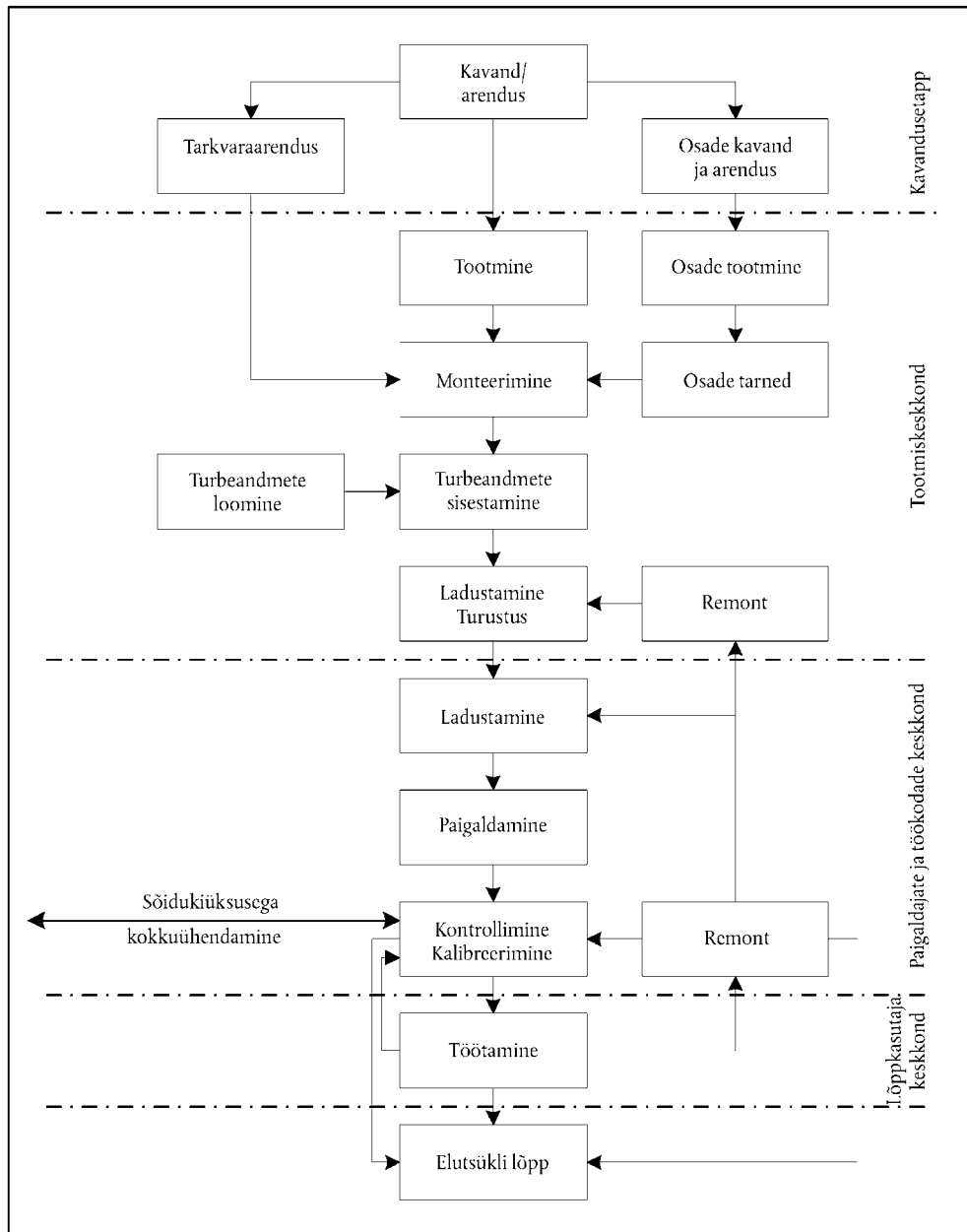


3.2. Liikumisanduri elutsükkel

Liikumisanduri tüüpilise elutsükli kirjeldus on järgmisel joonisel:

Joonis 2

Liikumisanduri tüüpiline elutsükkel



3.3. Ohud

Käesolevas lõikes kirjeldatakse ohtusid, mis võivad liikumisandurit ähvardada.

3.3.1. Pääsukontrolli ähvardavad ohud

T.Access

Kasutajad võivad üritada pääsu funktsioonidele, mis ei ole neile lubatud.

3.3.2. Konstruksiooniga seotud ohud

T.Faults	Riistvara, tarkvara ja sideprotseduuri rikked võivad viia liikumisanduri ettenägematutesse tingimustesse, mis ohustavad selle turvalisust.
T.Tests	Liikumisanduri turvalisust võivad ohustada kehtetuks tunnistamata katsemooduste või olemasolevate tagauste kasutamine
T.Design	Kasutajad võivad üritada saada ebaseaduslikke teadmisi konstruktsiooni kohta tootja materjalide (vargus, altkäemaks, ...) või pöördprojekteerimise abil.

3.3.3. Toimimisega seotud ohud

T.Environment	Kasutajad võivad ohustada liikumisanduri turvalisust, muutes selle tundlikuks keskkonnamõjude (termilised, elektromagnetilised, optilised, keemilised, mehaanilised, ...) suhtes
T.Hardware	Kasutajad võivad üritada muuta liikumisanduri riistvara
T.Mechanical_Origin	Kasutajad võivad üritada manipuleerida liikumisanduri sisendiga (nt ühendada selle lahti käigukastis, ...)
T.Motion_Data	Kasutajad võivad üritada muuta sõiduki liikumisandmeid (signaali lisamine, muutmine, kustutamine, taasesitamine)
T.Power_Supply	Kasutajad võivad rikkuda liikumisanduri turbe-eesmärke, muutes selle toidet (lahtiühendamine, vähendamine, suurendamine)
T.Security_Data	Kasutajad võivad üritada saada ebaseaduslikke teadmisi turbeandmete kohta turbeandmete loomise või transportimise või salvestamise käigus
T.Software	Kasutajad võivad üritada muuta liikumisanduri tarkvara
T.Stored_Data	Kasutajad võivad üritada muuta salvestatud andmeid (turbe- või kasutajaandmed)

3.4. Turbe-eesmärgid

Digitaalse sõidumeerikusüsteemi peamine turbe-eesmärk on järgmine.

O.Main	Kontrolliasutuste kontrollitavad andmed peavad olema kättesaadavad ja kajastama täielikult ning täpselt kontrollitud juhtide tegevusi ja sõidukeid juhtimis-, töötamis-, valmiso- leku- ja puhkeagade ning sõiduki kiiruse osas.
--------	--

Seetõttu on liikumisanduril järgmine turbe-eesmärk, millel on oluline panus üldturbe-eesmärki:

O.Sensor_Main	Liikumisanduri edastatud andmed peavad olema sõidukiüksusele kättesaadavad, võimaldades sõidukiüksusel täielikult ja täpselt teha kindalaks sõiduki liikumine kiiruse ja läbitud vahemaa osas.
---------------	--

3.5. Infotehnoloogia turbe-eesmärgid

Liikumisanduril on järgmised IT-spetsiifilised turbe-eesmärgid, millel on oluline panus peamisse turbe-eesmärki:

O.Access	Liikumisandur peab juhtima ühendatud üksuste pääsu funktsioonidele ja andmetele
O.Audit	Liikumisandur peab auditeerima selle turvalisuse õonestamiseks tehtavaid katseid ja peaks tegema kindalaks nende seose vastavate üksustega
O.Authentication	Liikumisandur peab autentima ühendatud üksused

O.Processing	Liikumisandur peab tagama, et sisendsignaali töötlemine liikumisandmete saamiseks on korrektne.
O.Reliability	Liikumisandur peab osutama usaldusväärseid teenuseid.
O.Secured_Data_Exchange	Liikumisandur peab tagama turvalise andmevahetuse sõidukiüksusega.

3.6. Füüsilised, personali- või menetlusvahendid

Käesolevas lõikes kirjeldatakse füüsilisi, personali- või menetlusnõudeid, mis aitavad kaasa liikumisanduri turvalisusele.

3.6.1. Seadme konstruktsioon

M.Development	Liikumisanduri arendajad peavad tagama, et tööülesannete jagamine arendusperioodil vastab IT turvalisusele.
M.Manufacturing	Liikumisanduri tootjad peavad tagama, et tööülesannete jagamine tootmise ajal vastab IT turvalisusele ning et liikumisandur oleks tootmisprotsessi ajal kaitstud füüsiliste toimete eest, mis võiksid kahjustada IT turvalisust.

3.6.2. Seadme tarne

M.Delivery	Liikumisanduri tootjad, sõidukitootjad ja paigaldajad või töökojad peavad tagama, et liikumisanduri käitlemine vastab IT turvalisusele.
------------	---

3.6.3. Turbeandmete loomine ja üleandmine

M.Sec_Data_Generation	Turbeandmete loomisalgoritmidele peab olema pääs ainult volitatud ja usaldusväärsetel isikutel.
M.Sec_Data_Transport	Turbeandmed tuleb luua, transportida ja sisestada liikumisandurisse nii, et säiliks nende kohane konfidentsiaalsus ja terviklikkus.

3.6.4. Sõidumeeriku paigaldamine, kalibreerimine ja kontrollimine

M.Approved_Workshops	Sõidumeeriku paigaldamise, kalibreerimise ja remondi peavad läbi viima usaldusväärsed ja kinnitatud paigaldajad või töökojad.
M.Mechanical_Interface	Peavad olema vahendid, mille abil saab tuvastada mehaanilise liidese füüsilist rikkumist (nt plommid).
M.Regular_Inspections	Sõidumeerik peab läbima korrapärase ülevaatuse ja seda tuleb kalibreerida.

3.6.5. Seaduste täitmise kontroll

M.Controls	Seaduste täitmise kontrolli tuleb läbi viia regulaarselt ja pisteliselt ning see peab hõlmama turbeauditeid.
------------	--

3.6.6. Tarkvara värskendamine

M.Software_Upgrade	Tarkvara uutele versioonidele tuleb anda turbesertifikaat enne nende rakendamist liikumisanduris.
--------------------	---

4. Turbetagamisfunktsioonid

4.1. Identimine ja autentimine

UIA_101 Liikumisandur peab suutma iga interaktsiooni korral kindlaks määrata iga üksuse, millega see on ühendatud.

UIA_102 Ühendatud üksuse identifitseerimise kuuluvad:

- üksuserühm:
 - sõidukiüksus,
 - juhtimisseade,
 - muud,
- üksuse ID (ainult sõidukiüksuse korral).

UIA_103 Ühendatud sõidukiüksuse ID koosneb sõidukiüksuse tüübikinnitusnumbrist ja sõidukiüksuse seerianumbrist.

UIA_104 Liikumisandur peab suutma autentida mis tahes sõidukiüksuse või juhtimisseadme, millega see on ühendatud:

- üksuse ühendamisel,
- toite taastumisel.

UIA_105 Liikumisandur peab suutma regulaarselt taasautentida sõidukiüksuse, millega see on ühendatud.

UIA_106 Liikumisandur tuvastab ja väldib autentimisandmete kasutamist, mis on kopeeritud või taasesitatud.

UIA_107 Pärast (tootja määratleb hiljem ja mitte üle 20) järjestikuse ebaõnnestunud autentimiskatse tuvastamist turbetagamis-funktsioon:

- loob sündmuse auditikirje,
- hoiatab üksust,
- jätkab liikumisandmete eksportimist mitteturvalises mooduses.

4.2. Pääsukontroll

Pääsukontroll tagab, et teavet loetakse hindamisobjektidest, kirjutatakse sinna või muudetakse seal ainult volitatute poolt.

4.2.1. Pääsukontroll

ACC_101 Liikumisandur kontrollib pääsuõigusi funktsioonidele ja andmetele.

4.2.2. Andmepääsuõigused

ACC_102 Liikumisandur tagab, et liikumisanduri identimisandmeid saab kirjutada ainult ühe korra (nõue 078).

ACC_103 Liikumisandur aktsepteerib ja/või salvestab ainult autentitud üksuste kasutajaandmeid.

ACC_104 Liikumisandur tagab turbeandmetele kohased lugemise ja kirjutamise pääsuõigused.

4.2.3. Faili struktuur ja pääsutingimused

ACC_105 Rakendus- ja andmefailide struktuur ja pääsutingimused luuakse tootmisprotsessi käigus ning need lukustatakse igasuguse edasise muutmise või kustutamise eest.

4.3. Selgituskohustus

ACT_101 Liikumisandur säilitab oma mälus liikumisanduri identimisandmed (nõue 077).

ACT_102 Liikumisandur salvestab oma mällu paigaldusandmed (nõue 099).

ACT_103 Liikumisandur suudab väljastada selgituskohustuse alusel andmeid autentitud üksustele nende taotlusel.

4.4. **Audit**

AUD_101 Liikumisandur loob oma turvalisust ohustavate sündmuste kajastamiseks nende sündmuste auditikirjed.

AUD_102 Liikumisanduri turvalisust ohustavad sündmused on järgmised:

- turbemurdekatsed,
 - autentimise ebaõnnestumine,
 - salvestatud andmete terviklikkusviga,
 - siseandmete edastusviga,
 - loata korpuse avamine,
 - riistvara rikkumine,
- anduri rike.

AUD_103 Auditikirjed sisaldavad järgmisi andmeid:

- sündmuse kuupäev ja kellaaeg,
- sündmuse tüüp,
- ühendatud üksuse identifikatsioon,

kui nõutavad andmed ei ole kättesaadavad, antakse kohane vaikeindikatsioon (tootja määratleb hiljem).

AUD_104 Liikumisandur saadab loodud auditikirjed sõidukiüksusele nende loomise ajal ja võib need ka oma mällu salvestada.

AUD_105 Juhul kui liikumisandur auditikirjed salvestab, tagab see auditimälu ammendumisest sõltumatult 20 auditikirje säilimise ning on suuteline väljastama salvestatud auditikirjed autentitud üksustele nende taotluse korral.

4.5. **Korrektus**

4.5.1. *Infovoa kontroll*

ACR_101 Liikumisandur tagab, et saaks töödelda ainult anduri mehaanilise sisendi kaudu saadud ja sellest tuletatud liikumisandmeid.

4.5.2. *Siseandmeedastus*

Käesoleva lõike nõudeid kohaldatakse ainult siis, kui liikumisandur kasutab füüsiliselt eraldatud osi.

ACR_102 Kui edastatakse andmeid liikumisanduri füüsiliselt eraldatud osade vahel, kaitstakse andmeid muutmise eest.

ACR_103 Kui siseedastuse käigus tuvastatakse andmeedastusviga, korratakse edastust ja turbetagamisfunktsioon loob sündmuse auditikirje.

4.5.3. *Salvestatud andmete terviklikkus*

ACR_104 Liikumisandur kontrollib oma mällu salvestatud kasutajaandmeid terviklikkusvigate osas.

ACR_105 Salvestatud kasutajaandmete terviklikkusvea tuvastamisel loob turbetagamisfunktsioon auditikirje.

4.6. **Töökindlus**

4.6.1 *Katsed*

RLB_101 Kõik tootmisetapile omased katsetusvajadustega seotud käsud, tegevused või katsetuspunktid blokeeritakse või eemaldatakse enne tootmisetapi lõppu. Neid ei saa hilisemaks kasutamiseks taastada.

RLB_102 Liikumisandur teeb esialgse käivitamise ja tavalise töötamise ajal läbi enesekontrollitised, et tõendada oma nõuetekohast töötamist. Liikumisanduri enesekontrollitised hõlmavad turbeandmete terviklikkuse tõendamist ja salvestatud täitmiskoodide (kui need ei ole ROMil) terviklikkuse tõendamist.

RLB_103 Enesekontrollitesti käigus sisevea tuvastamisel loob turbetagamisfunktsioon auditikirje (anduriviga).

4.6.2. Tarkvara

RLB_104 Liikumisanduri tarkvara ei tohi kasutamise käigus olla mingil moel võimalik analüüsida ega siluda.

RLB_105 Välisallikatest pärinevat sisendsignaali ei aktsepteerita täitmiskoodina.

4.6.3. Füüsiline kaitse

RLB_106 Liikumisandur on konstrueeritud nii, et seda saab avada, liikumisandur tuvastab korpuse iga avamise isegi välistoiteallikata minimaalselt 6 kuu jooksul. Sellisel juhul loob turbetagamisfunktsioon sündmuse auditikirje. (Auditikirje loomine ja salvestamine pärast vooluallika taasühendamist on aktsepteeritav.)

Kui liikumisandur on konstrueeritud nii, et seda ei saa avada, konstrueeritakse see nii, et füüsilise rikkumise katseid saab kergesti tuvastada (nt visuaalse kontrollimise teel).

RLB_107 Liikumisandur tuvastab määratletud (tootja määratleb hiljem) riistvararikkumised.

RLB_108 Eespool kirjeldatud juhul loob turbetagamisfunktsioon sündmuse auditikirje ja liikumisandur: (tootja määratleb hiljem).

4.6.4. Toitepinge katkestused

RLB_109 Liikumisandur säilitab turvalise oleku toitepinge katkestusel või muutumisel.

4.6.5. Lähtestustingimused

RLB_110 Toitepinge katkestuse korral või kui toiming enneaegselt lõpetatakse või mis tahes muudel lähtestustingimustel lähtestub liikumisandur vigadeta.

4.6.6. Andmete kättesaadavus

RLB_111 Liikumisandur tagab nõudmise korral pääsu vahenditele ning välistab tarbetud nõuded vahenditele ja nende tarbetu säilitamise.

4.6.7. Lisarakendused

RLB_112 Kui liikumisandur võimaldab muid rakendusi kui sõidumeerikurakendus, on kõik rakendused üksteisest füüsiliselt ja/või loogiliselt eraldatud. Need rakendused ei jaga turbeandmeid. Üheaegselt on aktiivne ainult üks ülesanne.

4.7. Andmevahetus

DEX_101 Liikumisandur ekspordib liikumisandmeid sõidukiüksusesse koos seotud turbeatribuutidega, et sõidukiüksus saaks tõendada oma terviklikkust ja autentsust.

4.8. Krüptograafiline tugi

Käesoleva lõike nõudeid kohaldatakse ainult vajaduse korral sõltuvalt kasutatud turbemehhanismidest ja tootjalahendustest.

CSP_101 Liikumisanduri igasugune krüptograafiline toiming vastab määratletud algoritmile ja määratletud võtmesuurusele.

CSP_102 Kui liikumisandur loob krüptograafilisi võtmeid, vastavad need krüptograafilise võtme määratletud loomisalgoritmidele ja krüptograafilise võtme määratletud suurusele.

CSP_103 Kui liikumisandur jagab krüptograafilisi võtmeid, vastavad need määratletud võtmejagamise meetoditele.

CSP_104 Kui liikumisandur pääseb ligi krüptograafilistele võtmetele, toimub see vastavalt määratletud krüptograafiliste võtmete pääsumeetoditele.

CSP_105 Kui liikumisandur hävitab krüptograafilisi võtmeid, toimub see vastavalt määratletud krüptograafiliste võtmete hävitamise meetoditele.

5. Turbemechanismide määratlus

Liikumisanduri tootjad määratlevad turbemechanismid, mis täidavad liikumisanduri turbetagamisfunktsioone.

6. Turbemechanismide miinimumtugevus

Liikumisanduri turbemechanismide miinimumtugevus on vastavalt ITSECI määratlusele suur.

7. Kindlusaste

Liikumisanduri kindlusastme sihttase on vastavalt ITSECI määratlusele ITSECI tase E3.

8. Põhimõte

Järgmistes tabelites on turbetagamisfunktsioonide põhimõte, näidates:

- milline turbetagamisfunktsioon või vahend avaldab vastutoimet millisele ohule,
- milline turbetagamisfunktsioon täidab millist IT turbe-eesmärki.

	Ohud										IT eesmärgid							
	Pääs	Rikked	Katsed	Konstruksioon	Keskkond	Riistvara	Mehaaniline päritolu	Liikumisandmed	Toiteallikas	Turbeandmed	Tarkvara	Salvestatud andmed	Pääs	Audit	Autentimine	Andmetöötlus	Töökindlus	Turvutatud ande vahetus
Füüsilised, personali- või menetlusvahendid																		
Arendus		x	x	x														
Tootmine			x	x														
Tarnimine						x				x	x							
Turbeandmete loomine									x									
Turbeandmete transport									x									
Kinnitatud töökojad							x											
Mehaaniline liides							x											
Korrapärane ülevaatus						x	x		x		x							
Seaduste täitmise kontroll					x	x	x		x	x	x							
Tarkvara värskendamine										x								
Turbetagamisfunktsioonid																		
Identimine ja autentimine																		
UIA_101 Üksuste identifitseerimine	x							x				x		x				x
UIA_102 Üksuste identiteet	x											x		x				
UIA_103 Sõidukiüksuse identiteet													x					
UIA_104 Üksuste autentimine	x						x					x		x				x
UIA_105 Taasautentimine	x						x					x		x				x
UIA_106 Võltsimiskindel autentimine	x						x					x		x				
UIA_107 Autentimise ebaõnnestumine							x						x				x	
Pääsukontroll																		
ACC_101 Pääsukontrollipoliitika	x								x		x	x						
ACC_102 Liikumisanduri ID											x	x						

SÕIDUKIÜKSUSE ÜLDINE TURBE-EESMÄRK

1. Sissejuhatus

Käesolev dokument sisaldab sõidukiüksuse kirjeldust, ohte, millele see peab suutma avaldada vastutoimet, ja turbeeesmärke, mida see peab täitma. Siin on määratletud nõutavad turbetagamisfunktsioonid. Siin on esitatud turbemehhanismide väidetav miinimumtugevus ning arenguks ja hindamiseks nõutav kindlusaste.

Nõuded, millele dokumendis viidatakse, sisalduvad IB lisa põhiosas. Selguse huvides on kohati IB lisa põhinõuded ja turbenõuded duplitseeritud. Kui turbenõude ja IB lisa põhinõude vahel, millele viidatakse selles turbenõudes, on ebaselgus, jääb ülimuslikuks IB lisa põhinõue.

IB lisa põhinõuded, millele turbe-eesmärkides ei viidata, ei kuulu turbetagamisfunktsioonide alla.

Ohtudele, eesmärkidele, menetlusvahenditele ja turbetagamisfunktsioonide spetsifikaatidele on antud kordumatud nimed nende jälgitavuseks arengu- ja hindamisdokumentides.

2. Lühendid, mõisted ja viited**2.1. Lühendid**

PIN	Isiklik identimisnumber
ROM	(read only memory) püsimälu
SEF	(security enforcing function) turbetagamisfunktsioon
TBD	(to be defined) määratletakse hiljem
TOE	(target of evaluation) hindamisobjekt
VU	(vehicle unit) sõidukiüksus.

2.2. Mõisted

Digitaalne sõidumeerik	Sõidumeerik
Liikumisandmed	Liikumisanduriga vahetatavad andmed, mis puudutavad kiirust ja läbitud vahemaad
Füüsiliselt eraldatud osad	Sõidukis asuvad sõidukiüksuse füüsilised osad, mis on vastandiks sõidukiüksuse korpuses asuvatele füüsilistele osadele
Turbeandmed	Konkreetsed andmed, mida on vaja turbetagamisfunktsioonide toetamiseks (nt krüptovõtmed)
Süsteem	Sõidumeerikuga mis tahes kombineeritud seadmed, inimesed või organisatsioonid
Kasutaja	Kasutajate all tuleb mõista inimesi, kes seadet kasutavad. Sõidukiüksuse tavakasutajad on juhid, kontrollijad, töökojad ja ettevõtted
Kasutajaandmed III.12	peatüki alusel nõutavad sõidukiüksuses registreeritud või sinna salvestatud mis tahes andmed, v.a turbeandmed.

2.3. Viited

ITSEC (Information Technology Security Evaluation Criteria) — infotehnoloogia turvalisuse hindamiskriteeriumid 1991.

3. Toote põhimõte**3.1. Sõidukiüksuse kirjeldus ja kasutusmeetod**

Sõidukiüksus on mõeldud paigaldamiseks mootorsõidukitesse. Selle eesmärk on registreerida, salvestada, kuvada, trükkida ja väljastada juhi tegevustega seotud andmeid.

See on ühendatud liikumisanduriga, millega see vahetab sõiduki liikumisandmeid.

Kasutajad idendivad ennast sõidukiüksusele, kasutades sõidumeerikukaarte.

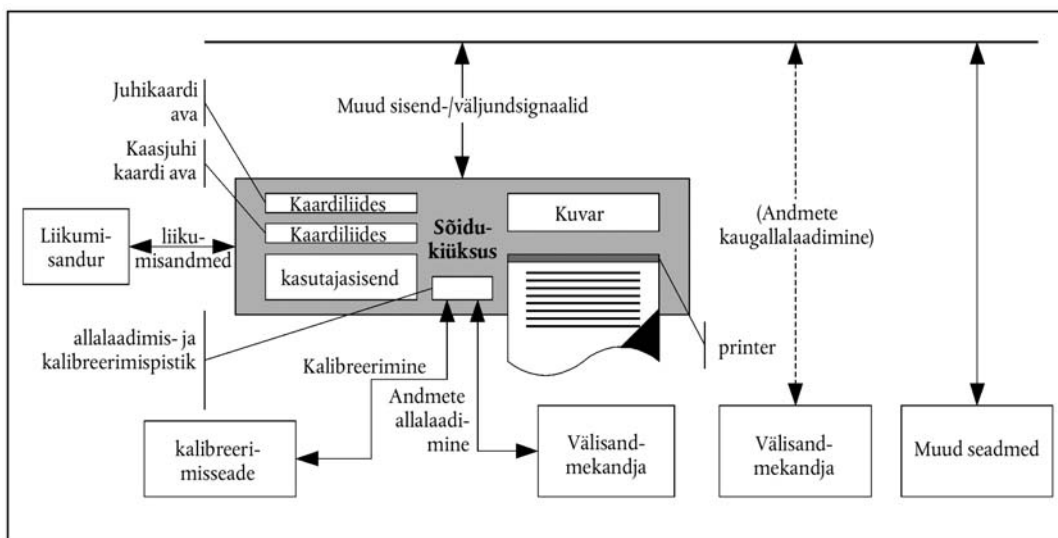
Sõidukiüksus registreerib ja salvestab kasutajategevuse andmed oma andmemällu, see registreerib kasutajategevuse andmed ka sõidumeerikukaartidele.

Sõidukiüksus väljastab andmed kuvarile, printerisse ja välisseadmetesse.

Sõidukisse paigaldatud sõidukiüksuse töökeskkonda on kirjeldatud järgmisel joonisel:

Joonis 1

Sõidukiüksuse töökeskkond



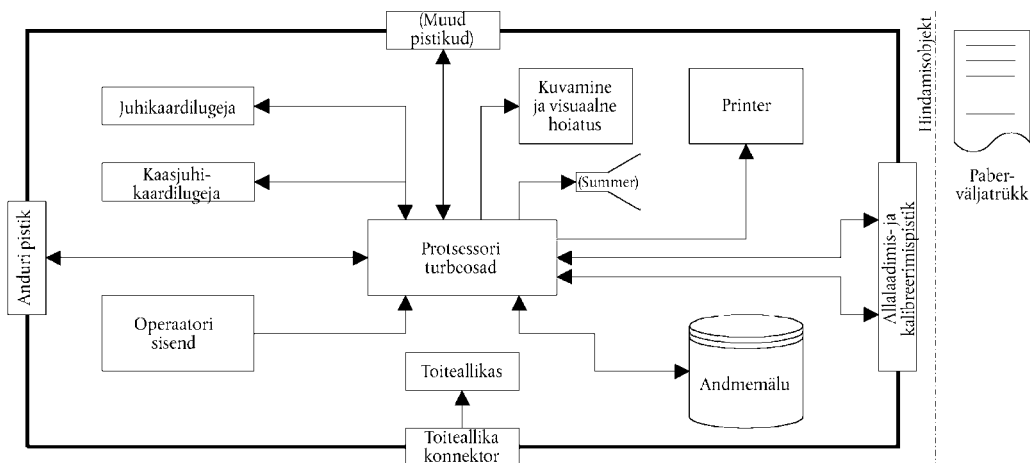
Sõidukiüksuse tildomadused, funktsioonid ja toimimismoodused on kirjeldatud IB lisa II peatükis.

Sõidukiüksuse funktsionaalsed nõuded on määratletud IB lisa III peatükis.

Tüüpilise sõidukiüksuse kirjeldus on järgmisel joonisel:

Joonis 2

Tüüpiline sõidukiüksus (...) valikuline



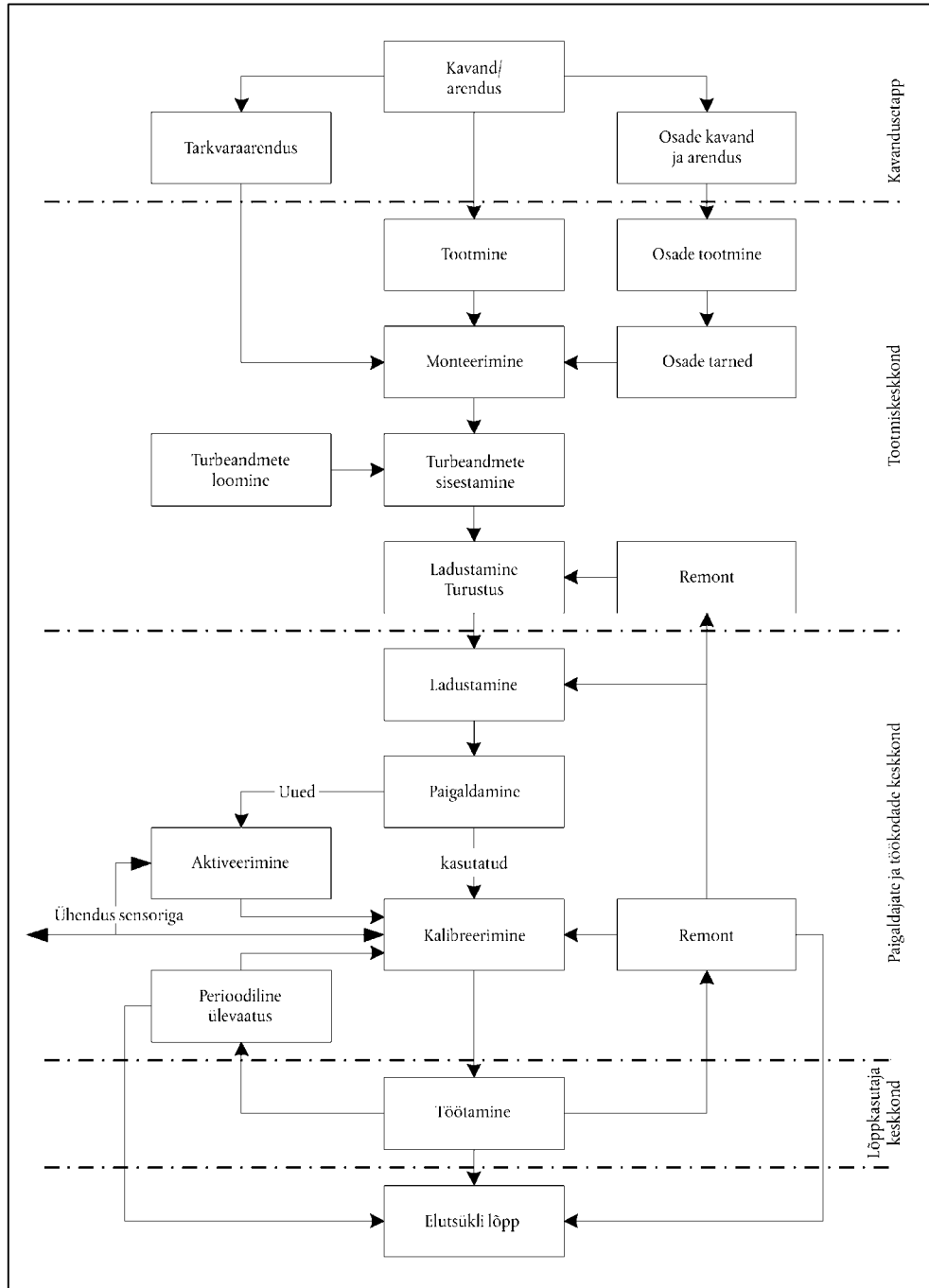
Tuleks märkida, et kuigi printerimehhanism kuulub hindamisobjektide hulka, ei ole saadud paberdokument seda mitte.

3.2. Sõidukiüksuse elutsükl

Sõidukiüksuse tüüpilise elutsükli kirjeldus on järgmisel joonisel:

Joonis 3

Sõidukiüksuse tüüpiline elutsükl



3.3. Ohud

Käesolevas lõikes kirjeldatakse ohtusid, mis võivad sõidukiüksust ohustada.

3.3.1. Identimis- ja pääsukontrolli ähvardavad ohud

T.Access

Kasutajad üritada proovida pääseda ligi funktsioonidele, mis ei ole neile lubatud (nt juhid püüavad pääseda kalibreerimisfunktsiooni).

T.Identification

Kasutajad võivad üritada kasutada mitut identifikaatsiooni või ei idendi ennast üldse.

3.3.2. Konstruksiooniga seotud ohud

T.Faults	Riistvara, tarkvara ja sideprotseduuri rikked võivad viia sõidukiüksuse ettenägematu-tesse tingimustesse, mis ohustavad selle turvalisust.
T.Tests	Sõidukiüksuse turvalisust võivad ohustada kehtetuks tunnistamata katsemooduste või olemasolevate tagauste kasutamine.
T.Design	Kasutajad võivad üritada saada ebaseaduslikke teadmisi konstruktsiooni kohta tootja materjalide (vargus, altkäemaks, ...) või pöördprojekteerimise abil.

3.3.3. Töötamisega seotud ohud

T.Calibration_Parameters	Kasutajad võivad üritada kasutada kalibreerimata seadet (kalibreerimisandmete muutmise või organisatsiooniliste puuduste tõttu).
T.Card_Data_Exchange	Kasutajad võivad üritada muuta andmeid, kui toimub nende vahetus sõidukiüksuse ja sõidumeerikukaartide vahel (signaali lisamine, muutmine, kustutamine, taasesitamine).
T.Clock	Kasutajad võivad proovida muuta sisekella.
T.Environment	Kasutajad võivad ohustada sõidukiüksuse turvalisust, muutes selle tundlikuks keskkonnamõjude (termilised, elektromagnetilised, optilised, keemilised, mehhaanilised, ...) suhtes.
T.Fake_Devices	Kasutajad võivad üritada ühendada sõidukiüksusega võltsseadmeid (liikumisandur, kiipkaardid).
T.Hardware	Kasutajad võivad proovida muuta sõidukiüksuse riistvara.
T.Motion_Data	Kasutajad võivad üritada muuta sõiduki liikumisandmeid (signaali lisamine, muutmine, kustutamine, taasesitamine).
T.Non_Activated	Kasutajad võivad kasutada aktiveerimata seadet.
T.Output_Data	Kasutajad võivad üritada muuta andmeväljastust (trükkimine, kuvamine või allalaadimine).
T.Power_Supply	Kasutajad võivad rikkuda sõidukiüksuse turbe-eesmärke, muutes selle toidet (lahtiühendamine, vähendamine, suurendamine).
T.Security_Data	Kasutajad võivad üritada saada ebaseaduslikke teadmisi turbeandmete kohta turbeandmete loomise või transportimise või salvestamise käigus.
T.Software	Kasutajad võivad üritada muuta sõidukiüksuse tarkvara.
T.Stored_Data	Kasutajad võivad üritada muuta salvestatud andmeid (turva- või kasutajaandmed).

3.4. Turbe-eesmärgid

Digitaalse sõidumeerikusüsteemi peamine turbe-eesmärk on järgmine:

O.Main	Kontrolliasutuste kontrollitavad andmed peavad olema kättesaadavad ja kajastama täielikult ning täpselt kontrollitud juhtide tegevusi ja sõidukeid juhtimis-, töötamis-, valmisoleku- ja puhkeaegade ning sõiduki kiiruse osas.
--------	---

Seetõttu on sõidukiüksusel järgmised turbe-eesmärgid, millel on oluline panus üldturbe-eesmärki:

O.VU_Main	Mõõdetud ja registreeritud ning seejärel kontrolliasutuste kontrollitavad andmed peavad olema kättesaadavad ja kajastama täpselt kontrollitud juhtide tegevusi ja sõidukeid juhtimis-, töötamis-, valmisoleku- ja puhkeegade ning sõiduki kiiruse osas.
O.VU_Export	Sõidukiüksus peab suutma eksportida andmeid välisandmekandjale nii, et oleks võimalik tõendada nende terviklikkust ja autentsust.

3.5. Infotehnoloogia turbe-eesmärgid

Sõidukiüksusel on järgmised IT-spetsiifilised turbe-eesmärgid, millel on oluline panus peamisse turbe-eesmärki:

O.Access	Sõidukiüksus peab juhtima kasutaja pääsu funktsioonidele ja andmetele.
O.Accountability	Sõidukiüksus peab koguma täpseid selgitusandmeid.
O.Audit	Sõidukiüksus peab auditeerima katseid süsteemi turvalisuse õõnestamiseks ja peaks tegema kindalaks nende seose vastavate kasutajatega.
O.Authentication	Sõidukiüksus peaks autentima kasutajad ja ühendatud üksused (kui üksuste vahel on vaja luua usaldusväärne tee).
O.Integrity	Sõidukiüksus peab säilitama salvestatud andmete terviklikkuse.
O.Output	Sõidukiüksus peab tagama, et väljastatud andmed kajastaksid mõõdetud või salvestatud andmeid täpselt.
O.Processing	Sõidukiüksus peab tagama, et sisendsignaali töötlemine kasutajaandmete saamiseks on korrektne.
O.Reliability	Sõidukiüksus peab osutama usaldusväärseid teenuseid.
O.Secured_Data_Exchange	Sõidukiüksus peab tagama turvalise andmevahetuse liikumisanduri ja sõidumeerikaartidega.

3.6. Füüsilised, personali- või menetlusvahendid

Käesolevas lõikes kirjeldatakse füüsilisi, personali- või menetlusnõudeid, mis aitavad kaasa sõidukiüksuse turvalisusele.

3.6.1. Seadme konstruktsioon

M.Development	Sõidukiüksuse arendajad peavad tagama, et tööülesannete jagamine arendusperioodil vastab IT turvalisusele.
M.Manufacturing	Sõidukiüksuse tootjad peavad tagama, et tööülesannete jagamine tootmise ajal vastab IT turvalisusele ning et sõidukiüksus oleks tootmisprotsessi ajal kaitstud füüsiliste toimetete eest, mis võiksid kahjustada IT turvalisust.

3.6.2. Seadme tarne ja aktiveerimine

M.Delivery	Sõidukiüksuse tootjad, sõidukitootjad ja paigaldajad või töökojad peavad tagama, et aktiveerimata sõidukiüksuste käitlemine vastab IT turvalisusele.
M.Activation	Sõidukitootjad ja paigaldajad või töökojad peavad aktiveerima sõidukiüksuse pärast selle paigaldamist sõidukile ja enne kui sõiduk lahkub paigalduskohalt.

3.6.3. Turbeandmete loomine ja üleandmine

M.Sec_Data_Generation	Turbeandmete loomisalgoritmidele peab olema pääs ainult volitatud ja usaldusväärsetel isikutel.
M.Sec_Data_Transport	Turbeandmed tuleb luua, transportida ja sisestada sõidukiüksusesse nii, et säiliks nende kohane konfidentsiaalsus ja terviklikkus.

3.6.4. Kaarditarne

M.Card_Availability	Sõidumeerikukaardid peavad olema kättesaadavad ja tarnitud ainult volitatud isikutele.
M.Driver_Card_Uniqueness	Juhtidel peab samaaegselt olema ainult üks kehtiv juhikaart.
M.Card_Traceability	Kaarditarne peab olema jälgitav (valged nimekirjad, mustad nimekirjad) ning turbeauditite käigus tuleb kasutada musti nimekirju.

3.6.5. Sõidumeeriku paigaldamine, kalibreerimine ja ülevaatus

M.Approved_Workshops	Sõidumeeriku paigaldamise, kalibreerimise ja remondi peavad läbi viima usaldusväärsed ja kinnitatud paigaldajad või töökojad.
M.Regular_Inspections	Sõidumeerik peab läbima korrapärase ülevaate ja seda tuleb kalibreerida.
M.Faithful_Calibration	Kinnitatud paigaldajad ja töökojad peavad kalibreerimise ajal sisestama sõidumeerikusse nõuetekohased sõidukiparameetrid.

3.6.6. Seadme töötamine

M.Faithful_Drivers	Juhid peavad täitma eeskirju ja käituma vastutustundlikult (nt kasutama oma juhikaarte, käsitsi valitavate tegevuste puhul valima õige tegevuse, ...).
--------------------	--

3.6.7. Seaduste täitmise kontroll

M.Controls	Seaduste täitmise kontrolli tuleb läbi viia regulaarselt ja pisteliselt ning see peab hõlmama turvaauditeid.
------------	--

3.6.8. Tarkvara värskendamine

M.Software_Upgrade	Tarkvara uutele versioonidele tuleb anda turbesertifikaat enne nende rakendamist sõidukiüksuses.
--------------------	--

4. Turbetagamisfunktsioonid

4.1. Identimine ja autentimine

4.1.1. Liikumisanduri identimine ja autentimine

UIA_201 Sõidukiüksus peab suutma iga interaktsiooni korral identida liikumisanduri, millega see on ühendatud.

UIA_202 Liikumisanduri identifikatsioon koosneb anduri tüübikinnitusnumbrist ja anduri seerianumbrist.

UIA_203 Sõidukiüksus autendib tema külge ühendatud liikumisanduri:

- liikumisanduri ühendamisel,
- sõidumeeriku igal kalibreerimisel,
- toite taastumisel.

Autentimine on vastastikune ja selle käivitab sõidukiüksus.

UIA_204 Sõidukiüksus taastendib ja taasautendib perioodiliselt (ajavahemiku määratleb tootja hiljem ning sagedamini kui kord tunnis) liikumisanduri, mille külge see on ühendatud, ja tagab, et sõidumeeriku viimase kalibreerimise ajal idenditud liikumisandurit ei ole muudetud.

UIA_205 Sõidukiüksus tuvastab ja väldib autentimisandmete kasutamist, mis on kopeeritud või taasesitatud.

UIA_206 Pärast (tootja määratleb hiljem ja mitte üle 20) järjestikuse ebaõnnestunud autentimiskatse tuvastamist ja/või pärast seda, kui on tuvastatud liikumisanduri loata vahetamine (st mitte sõidumeeriku kalibreerimise käigus), turbetagamisfunktsioon:

- loob sündmuse auditikirje,
- hoiatab kasutajat,
- jätkab liikumisanduri saadetud turvamata liikumisandmete aktsepteerimist ja kasutamist.

4.1.2. Kasutaja identimine ja autentimine

UIA_207 Sõidukiüksus jälgib pidevalt ja valikuliselt kahe kasutaja identifkatsiooni, kontrollides vastavalt seadme Juhikaardi avasse ja Kaasjuhi kaardi avasse sisestatud sõidumeerikukaarte.

UIA_208 Kasutajaidentifikatsioon koosneb järgmistest osadest:

- kasutajarühm:
 - JUHT (juhikaart),
 - KONTROLLIJA (kontrollikaart),
 - TÖÖKODA (töökojakaart),
 - ETTEVÕTE (ettevõttekaart),
 - TEADMATA (kaarti ei ole sisestatud),
- kasutaja ID, mis koosneb järgmistest osadest:
 - kaardi välja andnud liikmesriigi kood ja kaardinumber,
 - TEADMATA kui kasutajarühm on TEADMATA.

TEADMATA identifkatsioonid võivad olla otseselt või kaudselt teada.

UIA_209 Sõidukiüksus autendib oma kasutajad kaardi sisestamisel.

UIA_210 Sõidukiüksus taasautendib oma kasutajad:

- toite taastumisel,
- perioodiliselt või pärast konkreetsete sündmuste toimumist (ajavahemiku määratleb tootja hiljem ning sagedamini kui kord päevas).

UIA_211 Autentimine toimub sisestatud kaardi kui kehtiva sõidumeerikukaardi, mis omab turbeandmeid, mida vaid süsteem suudab jagada, tõestamise teel. Autentimine on vastastikune ja selle käivitab sõidukiüksus.

UIA_212 Lisaks eespool kirjeldatule nõutakse töökodade edukat autentimist PIN-koodi kontrollimise teel. PIN-koodi pikkus on vähemalt 4 tähemärki.

Märkus: juhul kui PIN-kood edastatakse sõidukiüksusesse sõidukiüksuse läheduses olevast välisseadmest, ei ole tarvis PIN-koodi konfidentsiaalsust edastamise ajal kaitsta.

UIA_213 Sõidukiüksus tuvastab ja väldib autentimisandmete kasutamist, mis on kopeeritud või taasesitatud.

UIA_214 Pärast 5 järjestikuse ebaõnnestunud autentimiskatse tuvastamist turbetagamisfunktsioon:

- loob sündmuse auditikirje,
- hoiatab kasutajat,
- oletab, et kasutaja on TEADMATA ja kaart et ei ole kehtiv (mõiste z ning nõue 007).

4.1.3. Kaugühendatud ettevõtte identimine ja autentimine

Ettevõtte kaugühendamisevõimalus on vabatahtlik. Seetõttu kohaldatakse käesolevat lõiget ainult siis, kui see omadus on rakendatud.

- UIA_215 Sõidukiüksus peab iga interaktsiooni korral kaugühendatud ettevõttega suutma identifitseerida selle ettevõtte.
- UIA_216 Kaugühendatud ettevõtte identifitseerimine koosneb ettevõttekaardi väljaandnud liikmesriigi koodist ja ettevõttekaardi numbrist.
- UIA_217 Sõidukiüksus autendib edukalt kaugühendatud ettevõtte enne mis tahes andmeekspordi lubamist.
- UIA_218 Autentimine toimub kehtiva ettevõttekaardi, mis omab turbeandmeid, mida vaid süsteem suudab jagada, ettevõttele kuumise tõestamise teel.
- UIA_219 Sõidukiüksus tuvastab ja väldib autentimisandmete kasutamist, mis on kopeeritud või taasesitatud.
- UIA_220 Pärast 5 järjekordse ebaõnnestunud autentimiskatse tuvastamist sõidukiüksus:

— hoiatab kaugühendatud ettevõtet.

4.1.4. Haldusseadme identimine ja autentimine

Sõidukiüksuse tootjad võivad ette näha sõidukiüksuse lisahaldusfunktsioonide tarvis (nt tarkvara värskendamine, turbeandmete uuesti laadimine, ...) eriseadmeid. Seetõttu kohaldatakse käesolevat lõiget ainult siis, kui see omadus on rakendatud.

- UIA_221 Sõidukiüksus peab iga interaktsiooni korral haldusseadmega suutma identifitseerida selle seadme.
- UIA_222 Enne edasise interaktsiooni lubamist autendib sõidukiüksus edukalt haldusseadme.
- UIA_223 Sõidukiüksus tuvastab ja väldib autentimisandmete kasutamist, mis on kopeeritud või taasesitatud.

4.2. Pääsukontroll

Pääsukontroll tagab, et teavet loetakse hindamisobjektidest, kirjutatakse sinna või muudetakse seal ainult volitatute poolt.

Tuleb märkida, et sõidukiüksuse registreeritud kasutajaandmed ei ole konfidentsiaalsed, kuigi neil on eraelulisi või kaubanduslikult tundlikke aspekte. Seetõttu ei kuulu andmete lugemise pääsuõigustega seotud funktsionaalne nõue (nõue 011) turbetagamiskontrollide hulka.

4.2.1. Pääsukontroll

- ACC_201 Sõidukiüksus juhib ja kontrollib pääsukontrolliõigusi funktsioonidele ja andmetele.

4.2.2. Pääsuõigused funktsioonidele

- ACC_202 Sõidukiüksus jõustab toimimismooduse valikueeskirjad (nõuded 006 kuni 009).
- ACC_203 Sõidukiüksus kasutab funktsioonidele pääsu kontrollieeskirjade jõustamiseks tavamoodust (nõue 010).

4.2.3. Pääsuõigused andmetele

- ACC_204 Sõidukiüksus jõustab pääsueeskirjad sõidukiüksuse identifitseerimisandmete kirjutamisele (nõue 076).
- ACC_205 Sõidukiüksus jõustab pääsueeskirjad sellega ühendatud liikumisanduri identifitseerimisandmete kirjutamisele (nõuded 079 ja 155).
- ACC_206 Pärast sõidukiüksuse aktiveerimist tagab sõidukiüksus, et kalibreerimisandmeid saaks sisestada sõidukiüksusesse ja salvestada selle andmemällu ainult kalibreerimismooduses (nõuded 154 ja 156).
- ACC_207 Pärast sõidukiüksuse aktiveerimist jõustab sõidukiüksus pääsueeskirjad kalibreerimisandmete kirjutamisele ja kustutamisele (nõue 097).

ACC_208 Pärast sõidukiüksuse aktiveerimist tagab sõidukiüksus, et aja korrigeerimise andmeid saaks sisestada sõidukiüksusesse ja salvestada selle andmemällu ainult kalibreerimismooduses (käesolevat nõuet ei kohaldata väikeste ajakorrigeerimiste suhtes, mis on lubatud nõuetega 157 ja 158).

ACC_209 Pärast sõidukiüksuse aktiveerimist jõustab sõidukiüksus pääsueeskirjad aja reguleerimise andmete kirjutamisele ja kustutamisele (nõue 100).

ACC_210 Sõidukiüksus jõustab kohased pääsuõigused turbeandmete lugemisele ja kirjutamisele (nõue 080).

4.2.4. Faili struktuur ja pääsutingimused

ACC_211 Rakendus- ja andmefailide struktuur ja pääsutingimused luuakse tootmisprotsessi käigus ning need lukustatakse igasuguse edasise muutmise või kustutamise eest.

4.3. Selgituskohustus

ACT_201 Sõidukiüksus tagab juhi tegevustega seotud nõuete täitmise (nõuded 081, 084, 087, 105a, 105b, 109 ja 109a).

ACT_202 Sõidukiüksus säilitab pidevalt identimisandmed (nõue 075).

ACT_203 Sõidukiüksus tagab töökodade tegevustega seotud nõuete täitmise (nõuded 098, 101 ja 109).

ACT_204 Sõidukiüksus tagab kontrollijate tegevustega seotud nõuete täitmise (nõuded 102, 103 ja 109).

ACT_205 Sõidukiüksus registreerib läbisõidumõõdiku andmed (nõue 090) ja üksikasjalikud andmed kiiruse kohta (nõue 093).

ACT_206 Sõidukiüksus tagab, et nõuetega 081 kuni 093 ja 102 kuni 105b seotud kasutajaandmeid, mis on kord juba registreeritud, ei muudeta, v. a siis, kui vanimad salvestatud andmed tuleb asendada uute andmetega.

ACT_207 Sõidukiüksus tagab, et see ei muuda sõidumeerikukaardile juba salvestatud andmeid (nõuded 109 ja 109a), v.a vanimate salvestatud andmete asendamine uute andmetega (nõue 110) või 1. liite lõike 2.1 märkuses kirjeldatud juhul.

4.4. Audit

Auditivõimalust nõutakse ainult nende sündmuste tarvis, mis võivad viidata manipuleerimisele või katsele rikkuda turvalisust. Seda ei nõuta õiguste tavakasutamise puhul isegi siis, kui need on seotud turvalisusega.

AUD_201 Sõidukiüksuse turvalisust ohustavate sündmuste puhul registreerib sõidukiüksus need sündmused koos seotud andmetega (nõuded 094, 096 ja 109).

AUD_202 Sõidukiüksuse turvalisust ohustavad sündmused on järgmised:

- turbemurdekatsed,
 - liikumisanduri autentimise ebaõnnestumine,
 - sõidumeerikukaardi autentimise ebaõnnestumine,
 - liikumisanduri loata vahetamine,
 - kaardiandmete sisendi terviklikkusviga,
 - salvestatud kasutajaandmete terviklikkusviga,
 - siseandmete edastusviga,
 - loata korpuse avamine,
 - riistvara rikkumine,

- viimane kaardiseanss nõuetekohaselt sulgemata,
- liikumisandmete veasündmus,
- toiteallika katkestuse sündmus,
- sõidukiüksuse siserike.

AUD_203 Sõidukiüksus jõustab auditikirjete salvestuseeskirjad (nõuded 094 ja 096).

AUD_204 Sõidukiüksus salvestab oma andmemällu liikumisanduri loodud auditikirjed.

AUD_205 Auditikirjeid saab trükkida, kuvada ja alla laadida.

4.5. **Objekti taaskasutamine**

REU_201 Sõidukiüksus tagab ajutiselt salvestatud objektide taaskasutamise nii, et sellega ei kaasneks vastuvõetamatut infovoogu.

4.6. **Korrektus**

4.6.1. *Infovoo kontroll*

ACR_201 Sõidukiüksus tagab nõuetega 081, 084, 087, 090, 093, 102, 104, 105, 105a ja 109 seotud kasutajaandmete töötlemise ainult siis, kui need on pärit õigetest sisenditest:

- sõiduki liikumisandmed,
- sõidukiüksuse reaalaega näitav kell,
- sõidumeeriku kalibreerimisparameetrid,
- sõidumeerikukaardid,
- kasutajasisendid.

ACR_201a Sõidukiüksus tagab, et nõudega 109a seotud kasutajaandmeid saab sisestada ainult aja kohta viimasest kaardi väljavõtmi-
sest kuni praeguse sisestamiseni (nõue 050a).

4.6.2. *Siseandmeedastus*

Käesoleva lõike nõudeid kohaldatakse ainult siis, kui sõidukiüksus kasutab füüsiliselt eraldatud osi.

ACR_202 Kui edastatakse andmeid sõidukiüksuse füüsiliselt eraldatud osade vahel, kaitstakse andmeid muutmise eest.

ACR_203 Kui siseedastuse käigus tuvastatakse andmeedastusviga, korratakse edastust ja turbetagamisfunktsioon loob sündmuse auditikirje.

4.6.3. *Salvestatud andmete terviklikkus*

ACR_204 Sõidukiüksus kontrollib oma andmemällu salvestatud kasutajaandmeid terviklikkusvigade osas.

ACR_205 Salvestatud kasutajaandmete terviklikkusvea tuvastamisel loob turbetagamisfunktsioon auditikirje.

4.7. **Töökindlus**

4.7.1. *Katsed*

RLB_201 Kõik sõidukiüksuse tootmisetapile omased katsetusvajadustega seotud käsud, tegevused või katsetuspunktid blokeeritakse või eemaldatakse enne sõidukiüksuse aktiveerimist. Neid ei saa hilisemaks kasutamiseks taastada.

RLB_202 Sõidukiüksus teeb esialgse käivitamise ja tavalise töötamise ajal läbi enesekontrollitesti, et tõendada selle nõuetekohast töötamist. Sõidukiüksuse enesekontrollitesti hõlmavad turbeandmete terviklikkuse tõendamist ja salvestatud täitmiskoodide (kui need ei ole ROMil) terviklikkuse tõendamist.

RLB_203 Enesekontrollitesti käigus siserikke tuvastamisel turbetagamisfunktsioon:

- loob auditikirje (v.a kalibreerimismooduses) (sõidukiüksuse siserike),
- säilitab salvestatud andmete terviklikkuse.

4.7.2. Tarkvara

RLB_204 Sõidukiüksuse tarkvara ei tohi kasutamise käigus olla mingil moel võimalik analüüsida ega siluda.

RLB_205 Välisallikatest pärinevat sisendsignaali ei aktsepteerita täitmiskoodina.

4.7.3. Füüsiline kaitse

RLB_206 Sõidukiüksus on konstrueeritud nii, et seda saab avada, sõidukiüksus tuvastab korpuse iga avamise, v.a kalibreerimismooduses, isegi välisloiteallikata minimaalselt 6 kuu jooksul. Sellisel juhul loob turbetagamisfunktsioon auditikirje (auditikirje loomine ja salvestamine pärast vooluallika taasühendamist on aktsepteeritav.)

Kui sõidukiüksus on konstrueeritud nii, et seda ei saa avada, konstrueeritakse see nii, et füüsilisi rikkumiskatseid saab kergesti tuvastada (nt visuaalse kontrollimise teel).

RLB_207 Sõidukiüksus tuvastab pärast aktiveerimist määratletud (tootja määratleb hiljem) riistvararikkumised.

RLB_208 Eespool kirjeldatud juhul loob turbetagamisfunktsioon sündmuse auditikirje ja sõidukiüksus: (tootja määratleb hiljem).

4.7.4. Toiteallika katkestused

RLB_209 Sõidukiüksus tuvastab kõrvalekalded toiteallika määratletud väärtustest, sealhulgas katkestused.

RLB_210 Eespool kirjeldatud juhul turbetagamisfunktsioon:

- loob auditikirje (v.a kalibreerimismooduses),
- säilitab sõidukiüksuse turvalise oleku,
- säilitab turbefunktsioonid, mis on seotud veel toimivate osade või protsessidega,
- säilitab salvestatud andmete terviklikkuse.

4.7.5. Lähtestustingimused

RLB_211 Toitepinge katkestuse korral või kui toiming enneaegselt lõpetatakse või mis tahes muudel lähtestustingimustel lähtestub sõidukiüksus vigadeta.

4.7.6. Andmete kättesaadavus

RLB_212 Sõidukiüksus tagab nõudmise korral pääsu vahenditele ning välistab tarbetud nõuded vahenditele ja vahendite tarbetu säilitamise.

RLB_213 Sõidukiüksus peab tagama, et kaarte ei vabastata enne, kui asjaomased andmed on neile salvestatud (nõuded 015 ja 016).

RLB_214 Eespool kirjeldatud juhul loob turbetagamisfunktsioon sündmuse auditikirje.

4.7.7. Lisarakendused

RLB_215 Kui sõidukiüksus võimaldab muid rakendusi kui sõidumeerikurakendus, on kõik rakendused üksteisest füüsiliselt ja/või loogiliselt eraldatud. Need rakendused ei jaga turbeandmeid. Üheaegselt on aktiivne ainult üks ülesanne.

4.8. Andmevahetus

Käesolevas lõikes käsitletakse andmevahetust sõidukiüksuse ja ühendatud seadmete vahel.

4.8.1. Andmevahetus liikumisanduriga

DEX_201 Sõidukiüksus tõendab liikumisandurist imporditud liikumisandmete terviklikkust ja autentsust.

DEX_202 Liikumisandmete terviklikkus- või autentsusvea tuvastamisel turbetagamisfunktsioon:

- loob auditikirje,
- jätkab imporditud andmete kasutamist.

4.8.2. Andmevahetus sõidumeerikukaartidega

DEX_203 Sõidukiüksus tõendab sõidumeerikukaartidelt imporditud andmete terviklikkust ja autentsust.

DEX_204 Kaardiandmete terviklikkus- või autentsusvea tuvastamisel sõidukiüksus:

- loob auditikirje,
- ei kasuta andmeid.

DEX_205 Sõidukiüksus ekspordib andmeid sõidumeeriku kiipkaartidele koos seotud turbeatribuutidega, et kaart saaks tõendada nende terviklikkust ja autentsust.

4.8.3. Andmevahetus välisandmekandjaga (allalaadimisfunktsioon)

DEX_206 Sõidukiüksus loob väliskandjale allalaaditud andmete tarvis päritolutõendi.

DEX_207 Sõidukiüksus annab andmesaajale võimaluse tõendada allalaaditud andmete päritolutõendi.

DEX_208 Sõidukiüksus laadib andmeid alla välisandmekandjale koos seotud turbeatribuutidega nii, et oleks võimalik tõendada allalaaditud andmete terviklikkust ja autentsust.

4.9. Kriptograafiline tugi

Käesoleva lõike nõudeid kohaldatakse ainult vajaduse korral sõltuvalt kasutatud turbemehhanismidest ja tootjalahendus-test.

CSP_201 Sõidukiüksuse igasugune kriptograafiline toiming vastab määratletud algoritmile ja määratletud võtmesuurusele.

CSP_202 Kui sõidukiüksus loob kriptograafilisi võtmeid, vastavad need kriptograafilise võtme määratletud loomisalgoritmidele ja kriptograafilise võtme määratletud suurusele.

CSP_203 Kui sõidukiüksus jagab kriptograafilisi võtmeid, vastavad need määratletud võtmejagamise meetoditele.

CSP_204 Kui sõidukiüksus pääseb ligi kriptograafilistele võtmetele, toimub see vastavalt määratletud kriptograafiliste võtmete pääsumetoditele.

CSP_205 Kui sõidukiüksus hävitab kriptograafilisi võtmeid, toimub see vastavalt määratletud kriptograafiliste võtmete hävitamis-meetoditele.

5. Turbemehhanismide määratlus

Nõutud turbemehhanismid on määratletud 11. liites.

Kõik muud turbemehhanismid määratlevad tootjad.

6. Turbemehhanismide miinimumtugevus

Sõidukiüksuse turbemehhanismide miinimumtugevus on vastavalt ITSECI määratlusele suur.

7. Kindlusaste

Sõidukiüksuse kindlusastme sihttase on vastavalt ITSECI määratlusele ITSECI tase E3.

8. Põhimõte

Järgmistes tabelites on turbetagamisfunktsioonide põhimõte, näidates:

— milline turbetagamisfunktsioon või vahend avaldab vastutoimet millisele ohule,

— milline turbetagamisfunktsioon täidab millist IT turbe-eesmärki.

	Ohud																IT eesmärgid											
	Pääs	Määratus	Rikked	Katsed	Konstruktsioon	Kalibreerimisparameetrid	Kaardandmevahetus	Kell	Keskkond	Võltsesadmed	Riistvara	Liikumisandmed	Aktiveerimata	Väljundandmed	Toiteallikas	Turbeandmed	Tarkvara	Salvestatud andmed	Pääs	Selgitskohustus	Audit	Autentimine	Terviklikkus	Väljund	Andmetöötlus	Töökindlus	Turvaline andmevahetus	
Füüsilised, personali- või menetlusvahendid																												
Arendus			x	x	x																							
Tootmine				x	x																							
Tarnimine												x																
Aktiveerimine	x											x																
Turbeandmete loomine																x												
Turbeandmete transport																x												
Kaardi olemasolu		x																										
Üks juhikaart		x																										
Kaardi jälgitavus		x																										
Kinnitatud töökojad						x	x																					
Korrapärane ülevaatus/ kalibreerimine						x	x				x	x			x													
Usaldusväärsed töökojad						x	x																					
Usaldusväärsed juhid		x																										
Seaduste täitmise kontroll		x				x	x	x	x	x	x	x				x	x											
Tarkvara värskendamine																	x											
Turbetagamisfunktsioonid																												
Identimine ja autentimine																												
UIA_201 Anduri identimine									x	x												x						x
UIA_202 Anduri identifitseerimine									x	x												x						x
UIA_203 Anduri autentimine									x	x												x						x
UIA_204 Anduri taasidentimine ja taasautentimine									x	x												x						x
UIA_205 Võltsimiskindel autentimine									x	x												x						
UIA_206 Autentimise ebaõnnestumine									x	x												x					x	
UIA_207 Kasutajate identimine	x	x							x									x			x							x
UIA_208 Kasutaja identifitseerimine	x	x							x									x			x							x
UIA_209 Kasutaja autentimine	x	x							x									x			x							x
UIA_210 Kasutaja taasautentimine	x	x							x									x			x							x
UIA_211 Autentimisvahendid	x	x							x											x		x						
UIA_212 PIN-koodi kontroll	x	x				x	x														x		x					
UIA_213 Võltsimiskindel autentimine	x	x							x												x		x					

	Ohud																IT eesmärgid												
	Pääs	Määratlus	Rikked	Katsed	Konstruktsioon	Kalibreerimisparameetrid	Kaardandmevahetus	Kell	Keskloond	Võltsseadmed	Riistvara	Liikumisandmed	Aktiveerimata	Väljundandmed	Toiteallikas	Turbeandmed	Tarkvara	Salvestatud andmed	Pääs	Selgituskohustus	Audit	Autentimine	Terviklikkus	Väljund	Andmetöötlus	Töökindlus	Turvaline andmevahetus		
UIA_214 Autentimise ebaõnnestumine	x	x							x											x									
UIA_215 Kaugkasutaja identimine	x	x																x		x							x		
UIA_216 Kaugkasutaja identifitseerimine	x	x																x		x									
UIA_217 Kaugkasutaja autentimine	x	x																x		x							x		
UIA_218 Autentimisvahendid	x	x																x		x									
UIA_219 Võltsimiskindel autentimine	x	x																x		x									
UIA_220 Autentimise ebaõnnestumine	x	x																											
UIA_221 Haldusseadme identimine	x	x																x		x									
UIA_222 Haldusseadme autentimine	x	x																x		x									
UIA_223 Võltsimiskindel autentimine	x	x																x		x									
Pääsukontroll																													
ACC_201 Pääsukontroll	x				x		x									x	x	x											
ACC_202 Pääsuõigused funktsioonidele	x				x		x												x										
ACC_203 Hozziféresi jogok a funkciókhöz	x				x		x												x										
ACC_204 Sõidukiüksuse ID																		x	x										
ACC_205 Ühendatud anduri ID									x									x	x										
ACC_206 Kalibreerimisandmed	x				x													x	x										
ACC_207 Kalibreerimisandmed					x													x	x										
ACC_208 Andmed aja korrigeerimise kohta							x											x	x										
ACC_209 Andmed aja korrigeerimise kohta							x											x	x										
ACC_210 Turbeandmed																x	x	x											
ACC_211 Faili struktuur ja pääsutingimused	x				x											x	x	x											
Selgituskohustus																													
ACT_201 Juhtide selgituskohustus																				x									
ACT_202 Sõidukiüksuse ID andmed																			x	x									
ACT_203 Töökodade selgituskohustus																				x									
ACT_204 Kontrollijate selgituskohustus																				x									
ACT_205 Sõiduki liikumise selgituskohustus																				x									
ACT_206 Selgitusandmete muutmine																		x				x					x		
ACT_207 Selgitusandmete muutmine																		x				x					x		

SÕIDUMEERIKUKAARDI ÜLDINE TURBE-EESMÄRK

1. Sissejuhatus

Käesolev dokument sisaldab sõidumeerikukaardi kirjeldust, ohte, millele see peab suutma avaldada vastutoimet, ja turbeeesmärke, mida see peab täitma. Siin on määratletud nõutavad turbetagamisfunktsioonid. Siin on esitatud turbemehhanismide väidetav miinimumtugevus ning arenguks ja hindamiseks nõutav kindlusaste.

Nõuded, millele dokumendis viidatakse, sisalduvad IB lisa põhiosas. Selguse huvides on kohati IB lisa põhinõuded ja turvanõuded duplitseeritud. Kui turvanõude ja IB lisa nõude vahel, millele viidatakse selles turvanõudes, on ebaselgus, jääb ülimuslikuks IB lisa põhinõue.

IB lisa põhinõuded, millele turbe-eesmärkides ei viidata, ei kuulu turbetagamisfunktsioonide alla.

Sõidumeerikukaart on standardne kiipkaart, millel on sõidumeeriku erirakendus ja mis vastab kiipkaartide suhtes kohaldatavatele ajakohastele funktsionaalsetele ja turvalisuse tagamise nõuetele. Seetõttu hõlmab turbe-eesmärk vaid turvalisuse lisanõudeid, mida vajab sõidumeerikurakendus.

Ohtudele, eesmärkidele, menetlusvahenditele ja turbetagamisfunktsioonide spetsifikaatidele on antud kordumatud nimed nende jälgitavuseks arengu- ja hindamisdokumentides.

2. Lühendid, mõisted ja viited**2.1. Lühendid**

IC	Kiip (elektrooniline osa, mis on mõeldud andmetöötluseks ja/või mälu funktsioonide tarvis)
OS	Operatsioonisüsteem
PIN	Isiklik identimisnumber
ROM	(Read only Memory) püsिमälu
SFP	(Security functions policy) turbetagamisfunktsioon
TBD	(To be defined) määratletakse hiljem
TOE	(Target of evaluation) hindamisobjekt
TSF	(TOE security function) hindamisobjekti turbefunktsioon
VU	(Vehicle unit) sõidukiüksus.

2.2. Mõisted

Digitaalne sõidumeerik	Sõidumeerik.
Tundlikud andmed	Sõidumeerikukaardi salvestatud andmed, mida tuleb kaitsta seoses terviklikkuse, loata muutmise ja konfidentsiaalsusega (kui see on turbeandmete suhtes kohaldatav). Tundlikud andmed hõlmavad turbeandmeid ja kasutajaandmeid.
Turbeandmed	Konkreetsed andmed, mida on vaja turbetagamisfunktsioonide toetamiseks (nt krüptovõtmed).
Süsteem	Sõidumeerikuga mis tahes kombineeritud seadmed, inimesed või organisatsioonid.
Kasutaja	Hindamisobjektiväline mis tahes üksus (inimkasutaja või IT välisüksus), mis suhtleb interaktiivselt hindamisobjektiga (kui ei ole kasutatud väljendis "kasutajaandmed").

Kasutajaandmed	Sõidumeerikukaardile salvestatud tundlikud andmed, v.a turbeandmed. Kasutajaandmed hõlmavad identimisandmeid ja tegevusandmeid.
Identimisandmed	Identimisandmed hõlmavad identimisandmeid ja kaardiomaniku identimisandmeid.
Kaardi identimisandmed	Kaardi identimisega seotud kasutajaandmed vastavalt nõuetele 190, 191, 192, 194, 215, 231 ja 235.
Kaardiomaniku identimisandmed	Kaardiomaniku identimisega seotud kasutajaandmed vastavalt nõuetele 195, 196, 216, 232, ja 236.
Tegevusandmed	Tegevusandmed hõlmavad andmeid kaardi omaniku tegevuste, sündmuste ja rikete ning kontrollitegevuse kohta.
Kaardiomaniku tegevusandmed	Kaardi omaniku tehtud tegevustega seotud kasutajaandmed vastavalt nõuetele 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 ja 237.
Andmed sündmuste ja rikete kohta	Sündmuste ja riketega seotud kasutajaandmed vastavalt nõuetele 204, 205, 207, 208, ja 223.
Andmed kontrollitegevuse kohta	Seaduste jõustamise kontrolliga seotud kasutajaandmed vastavalt nõuetele 210 ja 225.

2.3. Viited

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991 (Infotehnoloogia turvalisuse hindamiskriteeriumid 1991).
IC PP	Smartcard Integrated Circuit Protection Profile — version 2.0 — issue September 1998. (Kiipkaardi kiibi kaitseprofiil — versioon 2.0 — 1998. aasta septembri väljaanne). Registreeritud Prantsusmaa sertifitseerimisasutuses numbri all PP/9806.
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile — version 2.0 — issue June 99. (Sisseehitatud tarkvaraga kiipkaardi kiibi kaitseprofiil — versioon 2.0 — 1999. aasta juuni väljaanne). Registreeritud Prantsusmaa sertifitseerimisasutuses numbri all PP/9911.

3. Toote põhimõte

3.1. Sõidumeerikukaardi kirjeldus ja kasutusmeetod

Sõidumeerikukaart on IC PP ja ES PP kohane kiipkaart, millel on sõidumeerikus kasutamiseks mõeldud rakendus.

Sõidumeerikukaardi põhifunktsioonid on:

- salvestada kaardi identimisandmed ja kaardiomaniku identimisandmed. Sõidukiüksus kasutab neid andmeid kaardiomaniku identimiseks, võimaldab kohaste funktsioonide ja andmepääsuoiguste kasutamist ning tagab kaardiomaniku selgituskohustuse seoses oma tegevustega,
- salvestada kaardiomanikuga seotud andmeid kaardiomaniku tegevuste, sündmuste ja rikete ning kontrollitegevuse kohta.

Seetõttu on sõidumeerikukaart mõeldud kasutamiseks sõidukiüksuse liideseadmes. Seda võib kasutada ka mis tahes kaardilugejas (nt personaalarvutis), millel on täielik pääsuoigus mis tahes kasutajaandmete lugemisele.

Sõidumeerikukaardi elutsükli lõppkasutaja etapis (elutsükli 7. etapp vastavalt ES PP-le) võivad sõidukiüksused ainult kirjutada kasutajaandmeid kaardile.

Sõidumeerikukaardi funktsionaalsed nõuded on määratletud IB lisa põhiosas ja 2. liites.

3.2. Sõidumeerikukaardi elutsükkel

Sõidumeerikukaardi elutsükkel vastab ES PP-s kirjeldatud kiipkaardi elutsüklile.

3.3. Ohud

Lisaks ES PP-s ja IC PP-s loetletud kiipkaardi üldohtudele võivad sõidumeerikukaarti ähvardada järgmised ohud.

3.3.1. Lõppeesmärgid

Manipuleerijate lõppeesmärk on muuta hindamisobjektis salvestatud kasutajaandmeid.

T.Ident_Data	Hindamisobjektis sisalduvate identimisandmete (nt kaarditüüp või kaardi kehtivusaja lõpp või kaardiomaniku identimisandmed) edukas muutmine võimaldaks hindamisobjekti kuritarvitamist ning ohustaks tõsiselt süsteemi üldturbe-eesmärki.
T.Activity_Data	Hindamisobjektis salvestatud tegevusandmete edukas muutmine ohustaks hindamisobjekti turvalisust.
T.Data_Exchange	Tegevusandmete edukas muutmine (lisamine, kustutamine, muutmine) andmete impordi või ekspordi käigus ohustaks hindamisobjekti turvalisust.

3.3.2. Manipuleerimisteed

Hindamisobjektis sisalduvaga võib manipuleerida:

- üritades omandada ebaseaduslikke teadmisi hindamisobjekti riistvara ja tarkvara ning eelkõige selle turbefunktsioonide või turbeandmete kohta. Ebaseaduslikke teadmisi võib omandada, üritades saada enda valdusse projekteerija või tootja materjale (vargus, altkäemaks, ...) või uurides otseselt hindamisobjekti (füüsiline katsetamine, interferentsanalüüs, ...),
- kasutades ära hindamisobjekti konstruktsiooni või valmistuse nõrku kohti (ära kasutada riistvaravigu, tarkvaravigu, edastusvigu, rasketest keskkonnaoludest tingitud vigu hindamisobjektis, ära kasutada turbefunktsioonide nõrku kohti näiteks autentimiskorras, andmepäasukontrollis, krüptograafilistes toimingutes, ...),
- muutes hindamisobjekti või selle turbefunktsioone füüsiliste, elektriliste või loogiliste manipulatsioonide teel või kombineerides neid.

3.4. Turbe-eesmärgid

Kogu digitaalse sõidumeerikusüsteemi peamine turbe-eesmärk on järgmine.

O.Main	Kontrolliasutuste kontrollitavad andmed peavad olema kättesaadavad ja kajastama täielikult ning täpselt kontrollitud juhtide tegevust ja sõidukeid juhtimis-, töötamis-, valmisoleku- ja puhkeaegade ning sõiduki kiiruse osas.
--------	---

Seetõttu on hindamisobjektil järgmised turbe-eesmärgid, millel on oluline panus üldturbe-eesmärki.

O.Card_Identification_Data	Hindamisobjekt peab säilitama kaardi isikustamisprotsessi käigus salvestatud kaardi identimisandmed ja kaardi omaniku identimisandmed,
O.Card_Activity_Storage	Hindamisobjekt peab säilitama sõidukiüksuste poolt kaardile salvestatud kasutajaandmed.

3.5. Infotehnoloogia turbe-eesmärgid

Lisaks ES PP-s ja IC PP-s loetletud kiipkaardi üldturbe-eesmärkidele on hindamisobjekti IT-spetsiifilised turbe-eesmärgid, millel on oluline panus peamistesse turbe-eesmärkidesse, elutsükli lõppkasutajaetapis järgmised.

O.Data_Access	Hindamisobjekt peab võimaldama autentitud sõidukiüksustele pääsuõigusi andmekirjutamisele,
O.Secure_Communications	Hindamisobjekt peab suutma toetada turvalise andmevahetuse protokolle ja korda kaardi ning liideseadme vahel, kui rakendus seda nõuab.

3.6. Füüsilised, personali- või menetlusvahendid

Hindamisobjekti turvalisusega seotud füüsilised, personali- või menetlusnõuded on loetletud ES PP-s ja IC PP-s (keskkonna turbe-eesmärkide peatükid).

4. Turbetagamisfunktsioonid

Käesolevas peatükis on täpsemalt määratletud mõned lubatud toimingud, nagu ES PP määramine või valik, ning esitatakse turbetagamise lisafunktsioonide funktsionaalsed nõuded.

4.1. Vastavus kaitseprofiilidele

CPP_301 Hindamisobjekt vastab IC PP-le.

CPP_302 Hindamisobjekt vastab ES PP-le vastavalt järgnevale täpsustustele.

4.2. Kasutaja identimine ja autentimine

Kaart peab identima üksuse, millesse see on sisestatud, ja teadma, kas tegemist on autenditud sõidukiüksusega või mitte. Kaart võib eksportida mis tahes kasutajaandmeid igasse üksusesse, millega see on ühendatud, v.a kontrollikaart, mis võib eksportida kaardiomaniku identimisandmeid ainult autenditud sõidukiüksustesse (nii et kontrollija on oma nime kuvaril või väljatrükkidel nähes kindel, et tegemist ei ole võltssõidukiüksusega).

4.2.1. Kasutaja identifitseerimine

Omistus (FIA_UID.1.1) *Hindamisobjekti turbefunktsioonide kohaste tegevuste loetelu:* puudub.

Omistus (FIA_ATD.1.1) *Turbeatribuutide loetelu:*

USER_GROUP VEHICLE_UNIT, NON_VEHICLE_UNIT,

USER_ID sõiduki registreerimisnumber ja registreerinud liikmesriigi kood (USER_ID on teada ainult USER_GROUP = VEHICLE_UNIT).

4.2.2. Kasutaja autentimine

Omistus (FIA_UAU.1.1) *Hindamisobjekti turbefunktsioonide kohaste tegevuste loetelu:*

— Juhi- ja töökojakaardid: turbeatribuutidega kasutajaandmete eksport (kaardiandmete allalaadimisfunktsioon),

— Kontrollikaart: turbeatribuutideta kasutajaandmete eksport, v.a kaardiomaniku identimisandmed.

UIA_301 Sõidukiüksuse autentimine toimub turbeandmete, mida vaid süsteem suudab jagada, omamise tõestamise teel.

Valik (FIA_UAU.3.1 ja FIA_UAU.3.2): tuleb vältida.

Omistus (FIA_UAU.4.1) *Identitud autentimismehhanism(id):* mis tahes autentimismehhanism.

UIA_302 Töökojakaardil on lisautentimismehhanism PIN-koodi kontrollimise näol. (See mehhanism on sõidukiüksuse tarbeks ette nähtud selleks, et tagada kaardi omaniku identifitseerimine, see ei ole mõeldud töökojakaardi sisu kaitseks.)

4.2.3. Autentimise ebaõnnestumised

Järgmised omistused kirjeldavad kaardi reaktsiooni iga üksiku kasutaja autentimise ebaõnnestumise korral.

Omistus (FIA_AFL.1.1) *Number: 1, autentimissündmuste loetelu:* liideseadme autentimine.

Omistus (FIA_AFL.1.2) *Tegevuste loetelu:*

— hoiatab ühendatud üksust,

— oletab, et kasutaja on NON_VEHICLE_UNIT.

Järgmised omistused kirjeldavad kaardi reaktsiooni UIA_302 nõutud lisautentimismehhanismi ebaõnnestumise korral.

Omistus (FIA_AFL.1.1) *Number: 5, autentimissündmuste loetelu:* PIN-koodi kontroll (töökojakaart).

Omistus (FIA_AFL.1.2) *Tegevuste loetelu:*

- hoiatab ühendatud üksust,
- blokeerib PIN-koodi kontrollimiskorra nii, et iga järgnev PIN-koodi kontrollikatse ebaõnnestub,
- suudab näidata järgmistele kasutajatele blokeerimispõhjuse.

4.3. Pääsukontroll

4.3.1. Pääsukontroll

Sõidumeerikukaardi suhtes kohaldatakse selle elutsükli lõppkasutajaetapis üht ühist pääsukontrolli turbefunktsiooni AC_SFP.

Omistus (FDP_ACC.2.1) *Pääsukontrolli turbefunktsioon:* AC_SFP.

4.3.2. Pääsukontrolli funktsioonid

Omistus (FDP_ACF.1.1) *Pääsukontrolli turbefunktsioon:* AC_SFP.

Omistus (FDP_ACF.1.1) *Turbeatribuutide nimetatud rühm:* USER_GROUP.

Omistus (FDP_ACF.1.2) *Kontrollitud subjektide ja kontrollitud objektide, mis kasutavad kontrollitud toiminguid kontrollitud objektidel, pääsueeskirjad:*

- GENERAL_READ: Mis tahes kasutaja võib hindamisobjektist lugeda kasutajaandmeid, v.a kaardiomaniku identimisandmed, mida võib kontrollikaartidelt lugeda ainult VEHICLE_UNIT.
- IDENTIF_WRITE: Identimisandmeid võib kirjutada ainult üks kord ja enne kaardi elutsükli 6. etapi lõppu. Ükski kasutaja ei tohi kaardi elutsükli lõppkasutajaetapis kirjutada ega muuta identimisandmeid.
- ACTIVITY_WRITE: Tegevusandmeid võib hindamisobjekti kirjutada vaid VEHICLE_UNIT.
- SOFT_UPGRADE: Ükski kasutaja ei tohi värskendada hindamisobjekti tarkvara.
- FILE_STRUCTURE: Failstruktuur ja pääsutingimused luuakse enne hindamisobjekti elutsükli 6. etapi lõppu ning lukustatakse seejärel igasuguse edasise muutmise või kustutamise eest mis tahes kasutaja poolt.

4.4. Selgituskohustus

ACT_301 Hindamisobjekt säilitab pidevalt identimisandmed.

ACT_302 Hindamisobjekti isikustamise aja ja kuupäeva kohta on viide. Seda viidet ei saa muuta.

4.5. Audit

Hindamisobjekt peab seirama sündmusi, mis viitavad võimalikule turvalisuse rikkumisele.

Omistus (FAU_SAA.1.2) *Määratletud auditeeritavate sündmuste alamrühm:*

- kaardi omaniku autentimise ebaõnnestumine (5 järjestikust edutut PIN-koodi kontrolli),
- enesekontrollitesti viga,
- salvestatud andmete terviklikkusviga,
- tegevusandmete sisendi terviklikkusviga.

4.6. Korrektsus

4.6.1. Salvestatud andmete terviklikkus

Omistus (FDP_SDI.2.2) *Võetavad meetmed:* hoiatab ühendatud üksust.

4.6.2. Põhianandmete autentimine

Omistus (FDP_DAU.1.1) *Objektide või teabetüüpide loetelu:* tegevusandmed.

Omistus (FDP_DAU.1.2) *Subjektide loetelu:* mis tahes.

4.7. Töökindlus

4.7.1. Katsed

Valik (FPT_TST.1.1): esmase käivitamise ajal, tavatöötamise ajal perioodiliselt.

Märkus: esmase käivitamise ajal tähendab enne koodi aktiveerimist (ja mitte ainult toiming ATR ajal).

RLB_301 Hindamisobjekti enesekontrollitestid hõlmavad ROMile salvestamata mis tahes tarkvarakoodi terviklikkuse tõendamist.

RLB_302 Hindamisobjekti turbefunktsioon hoiatab ühendatud üksust vea tuvastamise puhul enesekontrollitesti käigus.

RLB_303 Pärast operatsioonisüsteemi testimise lõpetamist kõik testimisega seotud käsud ja tegevused blokeeritakse või eemaldatakse. Neid turbefunktsioone ei saa alistada ega kasutamiseks taastada. Ainult ühe elutsükli olekuga käskudele puudub teises olekus alati pääs.

4.7.2. Tarkvara

RLB_304 Hindamisobjekti tarkvara ei tohi kasutamise käigus olla mingil moel võimalik analüüsida, siluda ega muuta.

RLB_305 Välisallikatest pärinevat sisendsignaali ei aktsepteerita täitmiskoodina.

4.7.3. Toiteallikas

RLB_306 Hindamisobjekt säilitab turvalise oleku toitepinge katkestusel või muutumisel.

4.7.4. Lähtestustingimused

RLB_307 Toitepinge katkestuse korral (või kui on pingemuutused) hindamisobjektis või kui toiming enneaegselt lõpetatakse või mis tahes muudel lähtestustingimustel lähtestub hindamisobjekt vigadeta.

4.8. Andmevahetus

4.8.1. Andmevahetus sõidukiüksusega

DEX_301 Hindamisobjekt tõendab sõidukiüksusest imporditud andmete terviklikkust ja autentsust.

DEX_302 Imporditud andmete terviklikkus- või autentsusvea tuvastamisel hindamisobjekt:

— hoiatab andmeid saatvat üksust,

— ei kasuta andmeid.

DEX_303 Hindamisobjekt ekspordib kasutajaandmeid sõidukiüksusesse koos seotud turbeatribuutidega, et sõidukiüksus saaks tõendada saadud andmete terviklikkust ja autentsust.

4.8.2. Andmete eksport mujale kui sõidukiüksusesse (allalaadimisfunktsioon)

DEX_304 Hindamisobjekt suudab luua väliskandjale allalaaditud andmete tarvis päritolutõendi.

DEX_305 Hindamisobjekt suudab anda andmesaajale võimaluse tõendada allalaaditud andmete päritolutõendi.

DEX_306 Hindamisobjekt laadib andmeid alla välisandmekandjale koos seotud turbeatribuutidega nii, et oleks võimalik tõendada allalaaditud andmete terviklikkust.

4.9. Krüptograafiline tugi

CSP_301 Kui hindamisobjekti turbefunktsioon loob krüptograafilisi võtmeid, vastavad need krüptograafilise võtme määratletud loomisalgoritmidele ja krüptograafilise võtme määratletud suurusele. Loodud krüptograafiliste seansivõtmete võimalik kasutuskordade arv on piiratud (tootja määratleb hiljem ja mitte üle 240).

CSP_302 Kui hindamisobjekti turbefunktsioon jagab krüptograafilisi võtmeid, vastavad need määratletud krüptograafilise võtme jagamise meetoditele.

5. Turbemehtanismide määratlus

Nõutud turbemehtanismid on määratletud 11. liites.

Hindamisobjekti tootjad määratlevad kõik muud turbemehtanismid.

11. liide

ÜHISED TURBEMECHANISMID

SISUKORD

1.	Üldised punktid	516
1.1.	Viited	516
1.2.	Märkused ja lühendid	517
2.	Krüptograafilised süsteemid ja algoritmid	518
2.1.	Krüptograafilised süsteemid	518
2.2.	Krüptograafilised algoritmid	518
2.2.1.	RSA algoritm	518
2.2.2.	Räsi algoritm	518
2.2.3.	Andmete krüpteerimisalgoritm	518
3.	Võtmed ja sertifikaadid	518
3.1.	Võtmete loomine ja jagamine	518
3.1.1.	RSA võtmete loomine ja jagamine	518
3.1.2.	RSA katsevõtmed	520
3.1.3.	Liikumisanduri võtmed	520
3.1.4.	T-DES seansivõtmete loomine ja jagamine	520
3.2.	Võtmed	520
3.3.	Sertifikaadid	520
3.3.1.	Sertifikaatide sisu	521
3.3.2.	Väljaantud sertifikaadid	522
3.3.3.	Sertifikaadi tõendamine ja lahtipakkimine	523
4.	Vastastikune autentimismehhanism	523
5.	Sõidukiüksusekaartide andmete edastamise konfidentsiaalsus-, terviklikkus- ja autentimismehhanismid	526
5.1.	Turvaline sõnumivahetus	526
5.2.	Turvalise sõnumivahetuse vigade töötlemine	527
5.3.	Krüptograafiliste kontrollsummade arvutusalgoritm	528
5.4.	Krüptogrammide arvutusalgoritm andmeobjektide konfidentsiaalsuse tarvis	528
6.	Andmete allalaadimise digitaalallkirjamehhanismid	529
6.1.	Digitaalallkirja loomine	529
6.2.	Allkirja tõendamine	529

1. ÜLDISED PUNKTID

Käesolevas liites määratletakse turbemehhanismid, mis tagavad:

- sõidukiüksuste ja sõidumeerikukaartide vastastikuse autentimise, sealhulgas seansivõtmega seotud kokkuleppe,
- sõidukiüksuste ja sõidumeerikukaartide vahel edastatud andmete konfidentsiaalsuse, terviklikkuse ja autentimise,
- sõidukiüksustest välisandmekandjatele allalaaditud andmete terviklikkuse ja autentimise,
- sõidumeerikukaartidelt välisandmekandjatele allalaaditud andmete terviklikkuse ja autentimise.

1.1. Viited

Käesolevas liites kasutatakse järgmisi viiteid:

SHA-1	National Institute of Standards and Technology (NIST). FIPS Publication 180-1: Secure Hash Standard. April 1995. (Turvaline räsistandard, aprill 1995.)
PKCS1	RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.0. October 1998. (RSA krüpteerimisstandard, versioon 2.0, oktoober 1998.)
TDES	National Institute of Standards and Technology (NIST). FIPS Publication 46-3: Data Encryption Standard. Draft 1999. (Andmete krüpteerimisstandard, esialgne variant 1999.)
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998. (Kolmekordsete krüpteerimisalgoritmide toimimismoodused, 1998.)
ISO/IEC 7816-4	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 4. osa: Valdkondadevahelised andmevahetuskesused. Esimene väljaanne, 1995 + 1. muudatus, 1997.)
ISO/IEC 7816-6	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 6. osa: Valdkondadevahelised andmelemendid. Esimene väljaanne, 1996 + 1. parandus, 1998.)
ISO/IEC 7816-8	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First edition 1999. (Infotehnoloogia — Identimiskaardid — Kontaktidega kiipkaardid — 8. osa: Turvalisusega seotud valdkondadevahelised käsud. Esimene väljaanne, 1999.)
ISO/IEC 9796-2	Information Technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash function. First edition: 1997. (Infotehnoloogia — Turvatehnikad — Digitaalallkirjad, mille abil saab taastada sõnumeid — 2. osa: Räsifunktsiooni kasutatavad mehhanismid. Esimene väljaanne, 1997.)
ISO/IEC 9798-3	Information Technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm. Second edition 1998. (Infotehnoloogia — Turvatehnikad — Üksuse autentimismehhanismid — 3. osa: Üksuse autentimine, kasutades avaliku võtme algoritmi. Teine väljaanne, 1998.)
ISO 16844-3	Road vehicles — Tachograph systems — Part 3: Motion sensor interface. (Maanteesõidukid — Sõidumeerikusüsteemid — 3. osa: liikumisanduri liides.)

1.2. Märkused ja lühendatud terminid

Käesolevas liites kasutatakse järgmisi märkusi ja lühendeid:

(K_a, K_b, K_c)	võtmekimp, mida kasutab kolmekordne krüpteerimisalgoritm
CA	sertifitseerimisasutus
CAR	sertifitseerimisasutuse viide
CC	krüptograafiline kontrollsumma
CG	krüptogramm
CH	käsu päis
CHA	sertifikaadi omaniku luba
CHR	sertifikaadi omaniku viide
D()	dekrüpteerimine algoritmiga DES
DE	andmeelement
DO	andmeobjekt
d	RSA isiklik võti, isiklik astendaja
e	RSA avalik võti, avalik astendaja
E()	krüpteerimine algoritmiga DES
EQT	seade
Hash()	räsi väärtus, räsi väljund
Hash	räsifunktsioon
KID	võtme identifikaator
Km	TDES võti. Standardis ISO 16844-3 määratletud peavõti
Km _{vu}	sõidukiüksustesse sisestatud TDES-võti
Km _{wc}	töökojakaartidesse sisestatud TDES-võti
m	sõnumit esindav täisarv vahemikus 0 kuni $n-1$
n	RSA võtmed, moodul
PB	täidisbaidid
PI	tädistuse indikaatorbait (krüptogrammis kasutamiseks seoses andmeobjektide konfidentsiaalsusega)
PV	lihtväärtus
s	allkirja esindav täisarv vahemikus 0 kuni $n-1$
SSC	saatejada lugeja
SM	turvaline sõnumivahetus
TCBC	kolmekordse krüpteerimisalgoritmi šifriplokki aheldav toimimismoodus
TDEA	kolmekordne krüpteerimisalgoritm
TLV	sildi pikkuse väärtus
VU	(Vehicle unit) sõidukiüksus
X.C	sertifitseerimisasutuse väljaantud sertifikaat kasutajale X
X.CA	kasutaja X sertifitseerimisasutus
X.CA.PK ₀ X.C	sertifikaadi lahtipakkimistoiming avaliku võtme eraldamiseks. See on infiksoperaator, mille vasakpoolne operand on sertifitseerimisasutuse avalik võti ja parempoolne operand selle sertifitseerimisasutuse väljaantud sertifikaat. Tulemuseks on kasutaja X, kelle sertifikaat on parempoolne operand, avalik võti,

X.PK	kasutaja X avalik võti
X.PK[I]	kasutaja X avalikku võtit kasutades tehtud info I RSA krüpteerimine
X.SK	kasutaja X RSA avalik võti
X.SK[I]	kasutaja X isiklikku võtit kasutades tehtud info I RSA krüpteerimine
'xx'	kuueteistkümnendsüsteemis väärtus
	konkatenatsiooniooperaator.

2. KRÜPTOGRAAFILISED SÜSTEEMID JA ALGORITMID

2.1. Krüptograafilised süsteemid

Sõidukiüksused ja sõidumeerikukaardid kasutavad klassikalist RSA avaliku võtme krüptograafilist süsteemi järgmiste turvemehhanismide osutamiseks:

- autentimine sõidukiüksuste ja kaartide vahel,
- kolmekordsete DES seansivõtmete transpordiks sõidukiüksuste ja sõidumeerikukaartide vahel,
- sõidukiüksustelt või sõidumeerikukaartidelt välisandmekandjatele allalaaditud andmete digitaalallkirjaks.

CSM_002 Sõidukiüksused ja sõidumeerikukaardid kasutavad kolmekordset DES sümmeetrilist krüptograafilist süsteemi andmete terviklikkusemehhanismi osutamiseks sõidukiüksuste ja sõidumeerikukaartide vahelise andmevahetuse ajal ning sõidukiüksuste ja vajaduse korral sõidumeerikukaartide vahelise andmevahetuse konfidentsiaalsuse osutamiseks.

2.2. Krüptograafilised algoritmid

2.2.1. RSA algoritm

CSM_003 RSA algoritm on täielikult määratletud järgmiste suhetega:

$$\begin{aligned} X.SK[m] &= s = m^d \bmod n \\ X.PK[s] &= m = s^e \bmod n \end{aligned}$$

RSA kõikehõlmavam kirjeldus on viites PKCS1.

Avalik eksponent erineb kõigis RSA arvutustes loodud RSA võtmetes e 2-st.

2.2.2. Räsi algoritm

CSM_004 Digitaalallkirja mehhanismid kasutavad SHA-1 räsi algoritmi, nagu see on kirjeldatud viites SHA-1.

2.2.3. Andmete krüpteerimisalgoritm

CSM_005 DESil põhinevaid algoritme kasutatakse šifriplokki aheldavas toimimismooduses.

3. VÕTMED JA SERTIFIKAADID

3.1. Võtmete loomine ja jagamine

3.1.1. RSA võtmete loomine ja jagamine

CSM_006 RSA võtmed luuakse kolme funktsionaalse hierarhilise tasandi kaudu:

- Euroopa tasand,
- liikmesriigi tasand,
- seadme tasand.

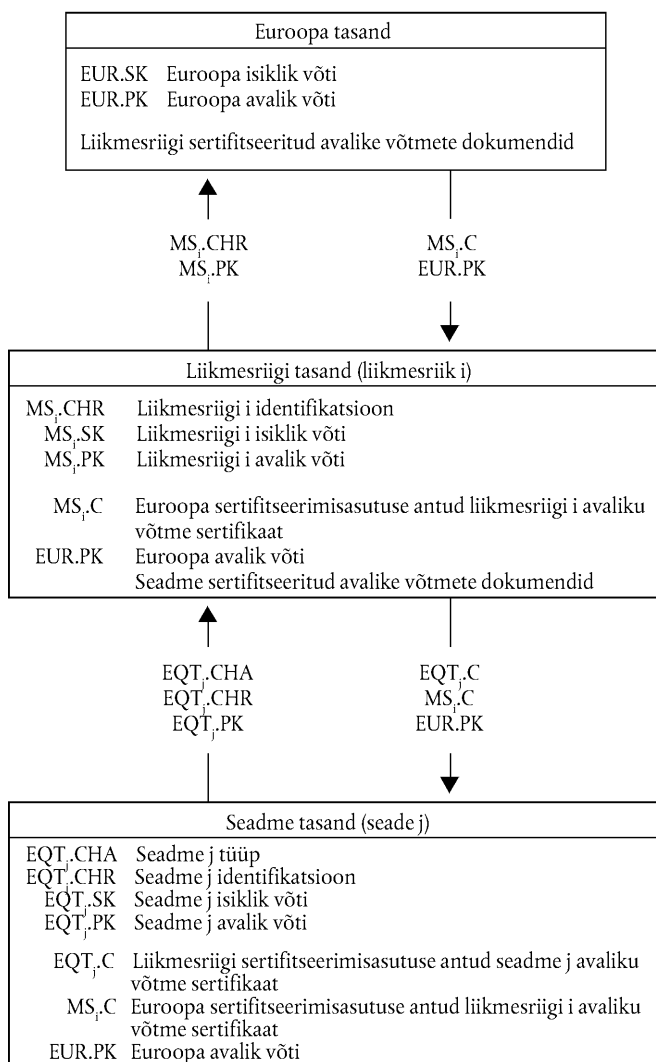
CSM_007 Euroopa tasandil luuakse ühtne Euroopa võtmepaar (EUR.SK ja EUR.PK). Euroopa isiklikku võtit kasutatakse liikmesriikide avalike võtmete muutmiseks. Säilitatakse andmeid kõigi sertifitseeritud võtmete kohta. Sellega tegeleb Euroopa Komisjoni volitustega ja vastutusel Euroopa sertifitseerimisasutus.

CSM_008 Liikmesriigi tasandil luuakse liikmesriigi võtmepaar (MS.SK ja MS.PK). Liikmesriikide avalikud võtmed sertifitseerib Euroopa sertifitseerimisasutus. Liikmesriigi avalikku võtit kasutatakse seadmesse (sõidukiüksus või sõidumeerikukaart) sisestatavate avalike võtmete sertifitseerimiseks. Säilitatakse andmeid kõigi sertifitseeritud avalike võtmete kohta koos seadme identifikaatsiooniga, mille jaoks see on mõeldud. Sellega tegeleb liikmesriigi sertifitseerimisasutus. Liikmesriik võib oma võtmepaari regulaarselt muuta.

CSM_009 Seadme tasandil luuakse üks ühtne võtmepaar (EQT.SK ja EQT.PK) ja see sisestatakse igasse seadmesse. Seadme avalikud võtmed sertifitseerib liikmesriigi sertifitseerimisasutus. Sellega võivad tegelda seadme tootjad, seadme isikustajad või liikmesriigi sertifitseerimisasutused. Seda võtmepaari kasutatakse autentimiseks, digitaalallkirjaks ja krüpteerimisteenusteks.

CSM_010 Loomise, transpordi (kui see toimub) ja ladustamise ajal säilitatakse avalike võtmete konfidentsiaalsus.

Järgmisel joonisel on kokkuvõtlikult esitatud selle protsessi andmevoog:



3.1.2. RSA katsevõtmed

CSM_011 Seadme katsetamise eesmärgil (sealhulgas koostalitlusvõime katse) loob Euroopa sertifitseerimisasutus erineva ühtse Euroopa katsevõtmepaari ja vähemalt kaks liikmesriigi katsevõtmepaari, mille avalikud võtmed sertifitseerib Euroopa isiklik katsevõti. Tootjad sisestavad tüübikinnituskatseid läbivasse seadmesse liikmesriigi ühe katsevõtme sertifitseeritud katsevõtmed.

3.1.3. Liikumisanduri võtmed

Loomise, transpordi (kui see toimub) ja ladustamise ajal säilitatakse allpool kirjeldatud kolme TDES võtme konfidentsiaalsus.

Toetamaks standardile ISO 16844 vastavat sõidumeerikut, tagavad Euroopa sertifitseerimisasutus ja liikmesriigi sertifitseerimisasutused lisaks muule järgmise.

CSM_036 Euroopa sertifitseerimisasutus loob kaks iseseisvat ja kordumatut kolmekordset DES võtit $K_{m_{VU}}$ ja $K_{m_{WC}}$ ja loob K_m :

$$K_m = K_{m_{VU}} \text{ XOR } K_{m_{WC}}$$

Euroopa sertifitseerimisasutus edastab need võtmed kohases turvalises korras liikmesriikide sertifitseerimisasutustele nende taotlusel.

CSM_037 Liikmesriikide sertifitseerimisasutused:

- kasutavad liikumisanduri tootjate taotletud liikumisanduri andmete krüpteerimiseks K_m (K_m -ga krüpteeritavad andmed on määratletud standardis ISO 16844-3),
- edastavad kohases turvalises korras sõidukiüksuste tootjatele $K_{m_{VU}}$ selle sisestamiseks sõidukiüksustesse,
- tagavad $K_{m_{WC}}$ sisestamise kõigisse töökojakaartidesse (elementaarfaili *SensorInstallationSecData* *Sensor_Installation_Data*) kaardi isikustamise käigus.

3.1.4. T-DES seansivõtmete loomine ja jagamine

CSM_012 Sõidukiüksused ja sõidumeerikukaardid loovad ja vahetavad vastastikuse autentimisprotsessi osana vajalikke andmeid ühise kolmekordse DES seansivõtme väljatöötamiseks. Selle andmevahetuse konfidentsiaalsust kaitstakse RSA krüpteerimismehhanismi kaudu.

CSM_013 Seda võtit kasutatakse kõigis järgmistes krüptograafilistes toimingutes, mis kasutavad turvalist sõnumivahetust. Selle kehivus lõpeb seansi lõpus (kaardi väljavõtmine või kaardi lähtestus) ja/või pärast 240 kasutuskorda (võtme üks kasutus = üks turvalist sõnumivahetust kasutatav kaardile saadetud käsk ja vastus sellele).

3.2. Võtmed

CSM_014 RSA võtmetel on (tasandist olenemata) järgmised pikkused: moodul n 1024 bitti, avalik eksponent e maksimaalselt 64 bitti, isiklik eksponent d 1024 bitti.

CSM_015 Kolmekordsete DES võtmete kuju on (K_a, K_b, K_a) , kus K_a ja K_b on sõltumatud 64bitise pikkusega võtmed. Pariteetsusbitte ei panda.

3.3. Sertifikaadid

CSM_016 RSA avaliku võtme sertifikaadid on "non self-descriptive" "Card Verifiable" sertifikaadid (viide ISO/IEC 7816-8).

3.3.1. *Sertifikaatide sisu*

CSM_017 RSA avaliku võtme sertifikaadid koosnevad järgmistest andmetest järgmises järjestuses:

Andmed	Vorming	Baidid	Märkused
CPI	INTEGER	1	Sertifikaadi profiili identifikaator (selles versioonis "01")
CAR	OCTET STRING	8	Sertifitseerimisasutuse viide
CHA	OCTET STRING	7	Sertifikaadi omaniku luba
EOV	TimeReal	4	Sertifikaadi kehtivusaja lõpp. Vabatahtlik, kui ei kasutata, täidetakse "FF".
CHR	OCTET STRING	8	Sertifikaadi omaniku viide
<i>n</i>	OCTET STRING	128	Avalik võti (moodul)
<i>e</i>	OCTET STRING	8	Avalik võti (avalik eksponent)
		164	

Märkused:

1. Sertifikaadi profiili identifikaator (CPI) sätestab autentimissertifikaadi täpse struktuuri. Seda võib kasutada seadmeseselt asjaomase päiseloetelu identimiseks, mis kirjeldab andmeelementide konkatenatsiooni sertifikaadis.

Selle sertifikaadi sisuga seotud päiseloetelu on järgmine:

	'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Laiendatud päiseloetelu silt																		
Päiseloetelu pikkus			CPI silt	CPI pikkus	CAR silt	CAR pikkus	CHA silt	CHA pikkus	EOV silt	EOV pikkus	CHR silt	CHR pikkus	Avaliku võtme silt (konstrueeritud)(sestrojit)	Järgmiste andmeobjektide pikkus	mooduli silt	mooduli pikkus	avaliku eksponendi silt	avaliku eksponendi pikkus

2. Sertifitseerimisasutuse viite (CAR) eesmärk on identifitseerida sertifikaadi väljaandnud sertifitseerimisasutus nii, et seda andmelementi saab kasutada asutuse võtmeidentifikaatoriga üheaegselt, et viidata sertifitseerimisasutuse avalikule võtmele (kodeerimiseks vt allpool "Võtme identifikaator").
3. Sertifikaadi omaniku volitusi (CHA) kasutatakse sertifikaadi omaniku õiguste identimiseks. See koosneb sõidumeerikurakenduse identifikaatorist ja seadme tüübist, mille jaoks sertifikaat on mõeldud (vastavalt andmelemendile EquipmentType, liikmesriigi korral "00").
4. Sertifikaadi omaniku viite (CHR) eesmärk on identifitseerida üheselt sertifikaadi omanik nii, et seda andmelementi saab kasutada subjekti võtmeidentifikaatoriga üheaegselt, et viidata sertifikaadi omaniku avalikule võtmele.
5. Võtmeidentifikaatorid idendivad üheselt sertifikaadi omaniku või sertifitseerimisasutused. Need kodeeritakse järgmiselt.

5.1. Seade (sõidukiüksus või kaart):

Andmed	Seadme seerianumber	Kuupäev	Tüüp	Tootja
Pikkus	4 baiti	2 baiti	1 bait	1 bait
Väärtus	Täisarv	kk aa BCD koodides	Tootjaomane	Tootja kood

Sõidukiüksuse puhul võib tootja sertifikaatide taotlemisel teada või mitte teada selle seadme identifikaatsiooni, millesse võtmed sisestatakse.

Esimesel juhul saadab tootja seadme identifikaatsiooni koos avaliku võtmega oma liikmesriigi asutusele sertifitseerimiseks. Sertifikaat sisaldab siis seadme identifikaatsiooni ja tootja peab tagama, et võtmed ja sertifikaat sisestatakse selleks mõeldud seadmesse. Võtmeidentifikaatoril on eespool näidatud kuju.

Teisel juhul peab tootja üheselt identifitseerima iga sertifikaadi taotluse ja saatma selle identifikaatsiooni koos avaliku võtmega oma liikmesriigi asutusele sertifitseerimiseks. Sertifikaat sisaldab taotluse identifikaatsiooni. Pärast võtme paigaldamist seadmesse peab tootja andma oma liikmesriigi asutusele tagasisidet võtme määramise kohta seadmele (st sertifikaadi taotluse identifikaatsioon, seadme identifikaatsioon). Võtmeidentifikaatoril on järgmine kuju:

Andmed	Seadme seerianumber	Kuupäev	Tüüp	Tootja
Pikkus	4 baiti	2 baiti	1 bait	1 bait
Väärtus	BCD kood	kk aa BCD koodides	'FF'	Tootja kood

5.2. Sertifitseerimisasutus:

Andmed	Asutuse identifikaatsioon	Võtme seerianumber	Lisainfo	Identifikaator
Pikkus	4 baiti	1 bait	2 baiti	1 bait
Väärtus	1 bait: riigi numbrikood 3 baiti: riigi tähtnumbrikood	täisarv	Lisakood (CA omane) 'FF FF', kui ei kasutata	'01'

Võtme seerianumbrit kasutatakse liikmesriigi erinevate võtmete eristamiseks, kui võtit muudetakse.

6. Sertifikaadi tõendajad teavad üheselt, et sertifitseeritud avalik võti on RSA võti, mis on seotud autentimise, digitaalallkirja tõendamise ja konfidentsiaalsete teenuste krüpteerimisega (sertifikaadis ei ole selle määramiseks objekti identifikaatorit).

3.3.2. Väljaantud sertifikaadid

CSM_018 Väljaantud sertifikaat on vastavalt standardile ISO/IEC 9796-2 digitaalallkiri koos osaliselt korratud sertifikaadi sisuga, millele on liidetud sertifitseerimisasutuse viide.

$$X.C = X.CA.SK['6A' || C_r || Hash(Cc) || 'BC'] || C_n || X.CAR$$

Az alõbbi bizonyktvinyntartalommal: $= C_c = C_r || C_n$
106 baiti || 58 baiti

Märkused:

1. Käesolev sertifikaat on 194 baiti pikk.
2. Allkirja peidetud CAR on ka liidetud allkirjale, nii et sertifikaadi tõendamiseks võib valida sertifitseerimisasutuse avaliku võtme.
3. Sertifikaadi tõendaja teab üheselt sertifitseerimisasutuse sertifikaadi allkirjastamiseks kasutatud algoritmi.

4. Selle väljaantud sertifikaadiga seotud päiseloetelu on järgmine:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
CV sertifikaadi siit (konstrueeritud)	järgmiste andmeobjektide pikkus	Allkirja siit	Allkirja pikkus	Jäägi siit	Jäägi pikkus	CAR siit	CAR pikkus

3.3.3. Sertifikaadi tõendamine ja lahtipakkimine

Sertifikaadi tõendamine ja lahtipakkimine koosneb allkirja tõendamisest vastavalt standardile ISO/IEC 9796-2, sertifikaadi sisu ja selles sisalduva avaliku võtme väljaotsimisest: $X.PK = X.CA.PK_n.X.C$ ning sertifikaadi kehtivuse tõendamise teel.

CSM_019 See koosneb järgmistest sammudest:

allkirja tõendamine ja sisu väljaotsimine:

— $X.C$ -st välja otsida allkiri C_n' ja CAR' : $X.C = \text{Metamärk} \parallel C_n' \parallel CAR'$
128 baiti 58 baiti 8 baiti

— CAR' -st valida kohane sertifitseerimisasutuse avalik võti (kui seda ei ole varem muude vahenditega tehtud),

— allkiri avada CA avaliku võtmega: $Sr' = X.CA.PK [\text{Sign}]$,

— kontrollida, et Sr' algaks '6A' ja lõpeks 'BC'

— arvutada Cr' ja H' avaldisest: $Sr' = '6A' \parallel Cr' \parallel H' \parallel 'BC'$
106 baiti 20 baiti

— taastada sertifikaadi sisu $C' = C_r' \parallel C_n'$,

— kontrollida, et $\text{Hash}(C') = H'$

Kui kontrolli tulemused on positiivsed, on tegemist ehtsa sertifikaadiga, mille sisu on C' .

Kontrollida kehtivust. C' -st:

— kontrollida kehtivuse lõpuaega, kui see on kohaldatav,

Otsida välja C' -st avalik võti, võtmeidentifikaator, sertifikaadi omaniku volitused ja sertifikaadi kehtivusaja lõpp.

— $X.PK = n \parallel e$,

— $X.KID = \text{CHR}$

— $X.CHA = \text{CHA}$,

— $X.EOV = \text{EOV}$.

4. VASTASTIKUNE AUTENTIMISMEHCHANISM

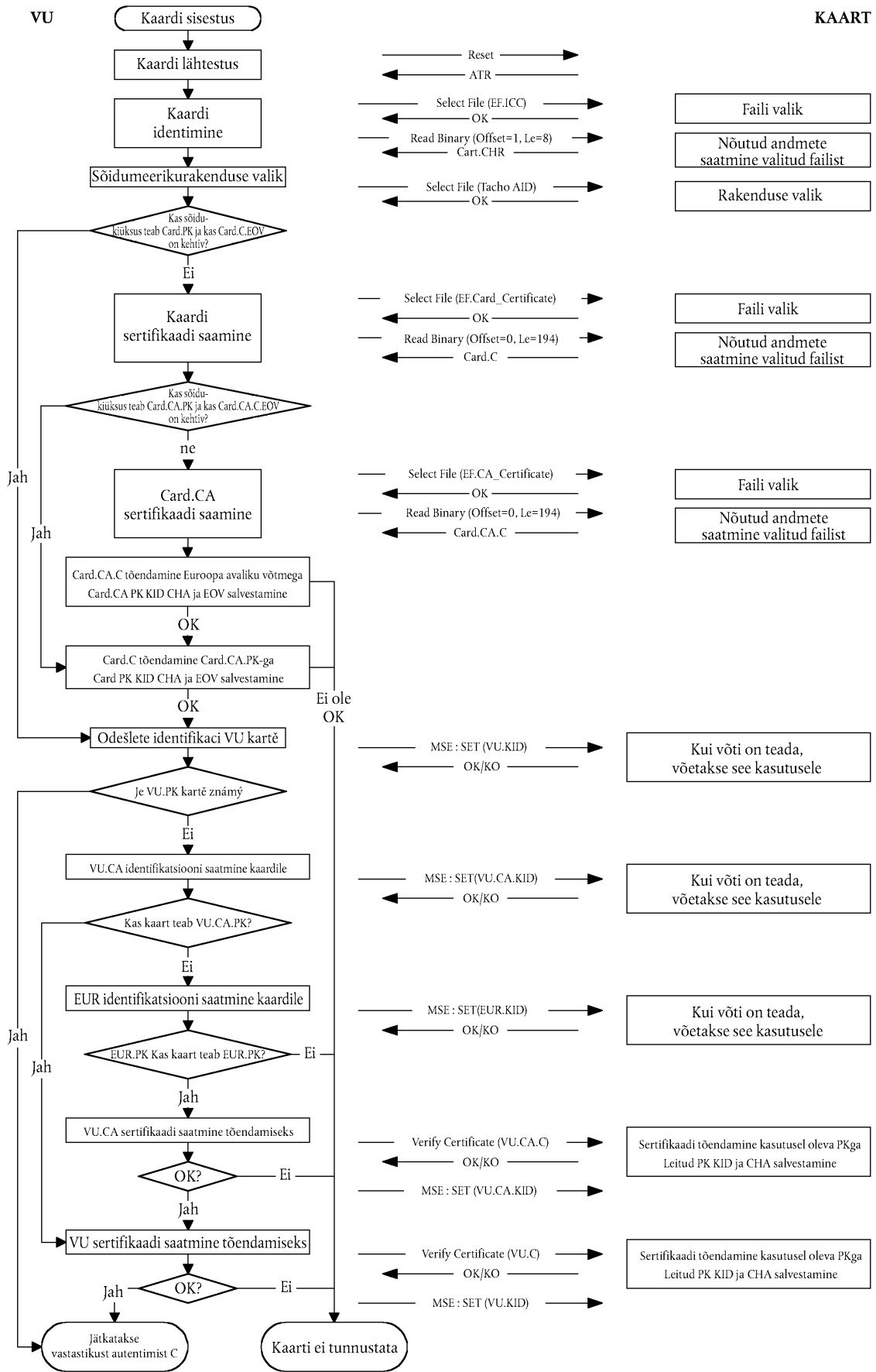
Kaartide ja sõidukiüksuste vaheline vastastikune autentimine põhineb järgmisel põhimõttel.

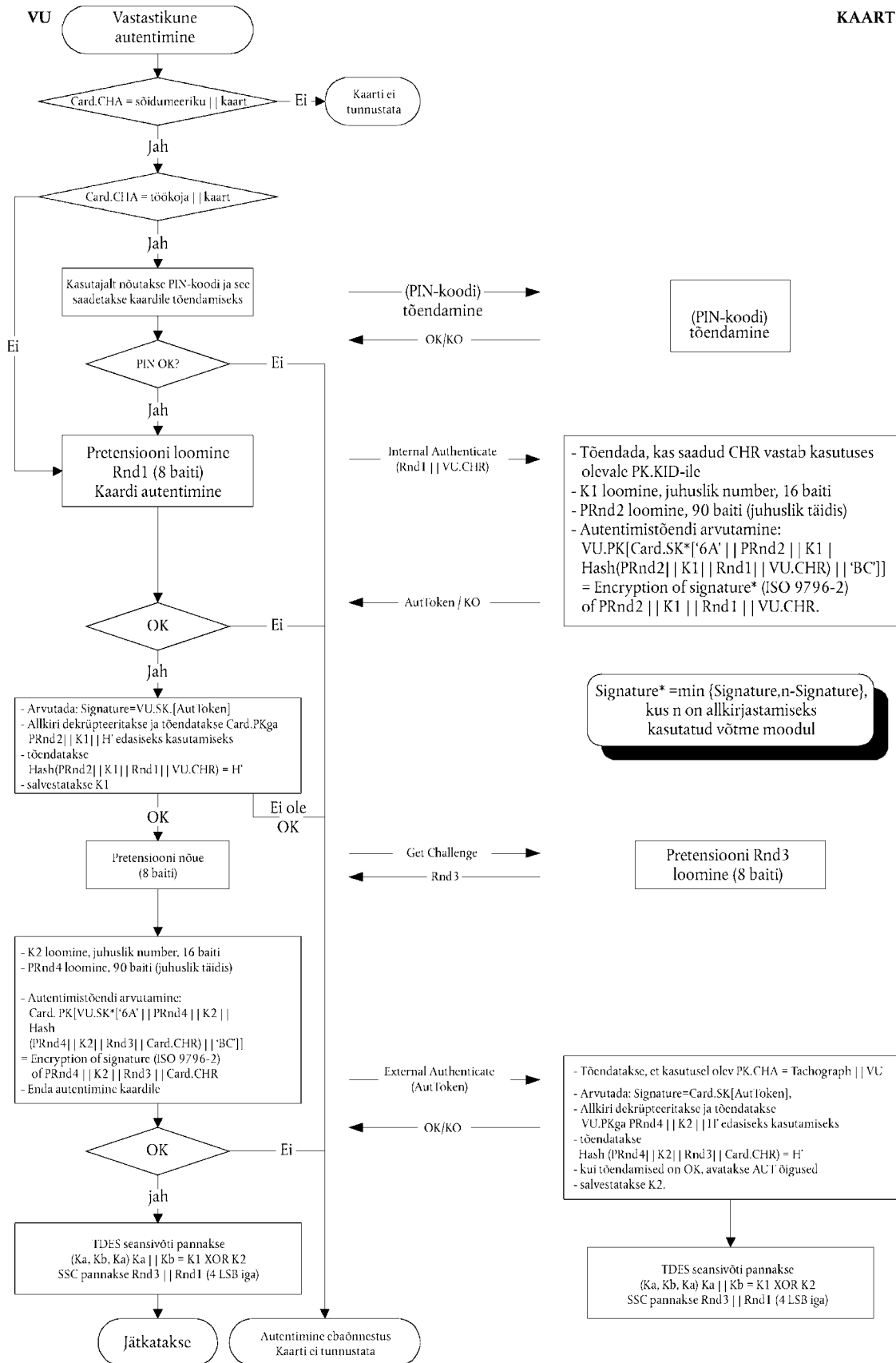
Kumbki pool tõendab teisele, et sel on kehtiv võtmepaar, millest avaliku võtme on sertifitseerinud liikmesriigi sertifitseerimisasutus, mille omakorda on sertifitseerinud Euroopa sertifitseerimisasutus.

Tõendamine toimub isikliku võtmega juhusliku numbriga allkirjastamises, mille on saatnud teine pool, mis peab saadetud juhusliku numbriga allkirja tõendamisel taastama.

Mehhanism käivitub kaardi sisestamisel sõidukiüksusesse. See algab sertifikaatide vahetamise ja avalike võtmete lahtipakkimisega ning lõpeb seansivõtme loomisega.

CSM_020 Kasutatakse järgmist protokollit (nooled näitavad käsked ja vahetatud andmeid (vt 2. liide)).





5. SÕIDUKIÜKSUSEKAARTIDE ANDMETE EDASTAMISE KONFIDENTSIAALSUS-, TERVIKLIKKUS- JA AUTETIMIS-MEHHANISMID

5.1. Turvaline sõnumivahetus

- CSM_021 Sõidukiüksusekaartide andmeedastuse terviklikkust kaitstakse turvalise sõnumivahetusega vastavalt viidetele (ISO/IEC 7816-4) ja (ISO/IEC 7816-8).
- CSM_022 Kui edastamise ajal on vaja andmeid kaitsta, liidetakse käsu või vastusega saadetud andmeelementidele krüptograafiline kontrollsumma. Vastuvõtja tõendab krüptograafilise kontrollsumma.
- CSM_023 Käsu saadetud andmete krüptograafiline kontrollsumma hõlmab käsu päise ja kõiki saadetud andmelemente (= > CLA = '0C', ning kõik andmeobjektid kaitstakse siltidega, kus b1 = 1).
- CSM_024 Vastuse olekubaite kaitstakse krüptograafilise kontrollsummaga, kui vastuses puudub andmeväli.
- CSM_025 Krüptograafiliste kontrollsummade pikkus on neli baiti.

Seetõttu on käskude ja vastuste struktuur, kui kasutatakse turvalist sõnumivahetust, järgmine.

Kasutatud andmeobjektid on standardis ISO/IEC 7816-4 kirjeldatud turvalise sõnumivahetuse andmeobjektide osa:

Silt	Mnemoonika	Tähendus
'81'	T _{PV}	Kodeerimata andmed, mida ei ole kodeeritud BER-TLVs (kaitstakse CCga)
'97'	T _{LE}	Le väärtus turvamata käsus (kaitstakse CCga)
'99'	T _{SW}	Olekuinfo (kaitstakse CCga)
'8E'	T _{CC}	Krüptograafiline kontrollsumma
'87'	T _{PI CG}	Täidistust näitav bait Krüptogramm (kodeerimata andmed, mida ei ole kodeeritud BER-TLVs)

Kui on turvamata käsu-vastuse paar:

Käsu päis	Käsu sisu
CLA INS P1 P2	(L _c -väli) (Andmeväli) (L _e -väli)
neli baiti	L baidid, tähistatud B ₁ kuni B _L

Vastuse sisu	Vastuse saba
(Andmeväli)	SW1 SW2
L _r andmebaidi	kaks baiti

Vastav turvaline käsu-vastuse paar on:

Turvaline käsk:

Käsu päis (CH)	Käsu sisu												
CLA INS P1 P2	(Uus L _c väli)			(Uus andmeväli)							(Uus L _e väli)		
'0C'	Uue andmevälja pikkus			T _{PV}	L _{PV}	PV	T _{LE}	L _{LE}	L _e	T _{CC}	L _{CC}	CC	'00'
				'81'	L _c	Andmeväli	'97'	'01'	L _e	'8E'	'04'	CC	

Andmed tuleb integreerida kontrollsummasse = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = täidisbaidid (80 .. 00) vastavalt standardile ISO-IEC 7816-4 ja ISO 9797 1. meetodile.

Andmeobjektid PV ja LE on olemas ainult siis, kui turvamata käsus on mõned vastavad andmed.

Turvaline vastus:

1. Vastuse andmeväli ei ole tühi ja seda ei tule konfidentsiaalsuse eesmärgil kaitsta:

Vastuse sisu						Vastuse saba
(Uus andmeväli)						uus SW1 SW2
T _{PV}	L _{PV}	PV	T _{CC}	L _{CC}	CC	
'81'	L _r	And- meväli	'8E'	'04'	CC	

Andmed tuleb integreerida kontrollsummasse = T_{PV} || L_{PV} || PV || PB

2. Vastuse andmeväli ei ole tühi ja seda tuleb konfidentsiaalsuse eesmärgil kaitsta:

Vastuse sisu						Vastuse saba
(Uus andmeväli)						uus SW1 SW2
T _{PI CG}	L _{PI CG}	PI CG	T _{CC}	L _{CC}	CC	
'87'		PI CG	'8E'	'04'	CC	

CG krüptogrammis sisalduvad andmed: BER-TLV kodeerimata andmed ja täidisbaidid.

Andmed tuleb integreerida kontrollsummasse = T_{PI CG} || L_{PI CG} || PI CG || PB

3. Vastuse andmeväli on tühi:

Vastuse sisu						Vastuse saba
(Uus andmeväli)						uus SW1 SW2
T _{SW}	L _{SW}	SW	T _{CC}	L _{CC}	CC	
'99'	'02'	Uus SW1 SW2	'8E'	'04'	CC	

Andmed tuleb integreerida kontrollsummasse = T_{SW} || L_{SW} || SW || PB

5.2. Turvalise sõnumivahetuse vigade töötlemine

CSM_026 Kui sõidumeerikukaart tunneb käsu töötlemise ajal ära turvalise sõnumivahetuse vea, tuleb olekubaidid tagasi saata ilma turvalise sõnumivahetusega. Vastavalt standardile ISO/IEC 7816-4 määratletakse turvalise sõnumivahetuse vigade näitamiseks järgmised olekubaidid:

- '66 88' krüptograafilise kontrollsumma tõendamine ebaõnnestus,
- '69 87' turvalise sõnumivahetuse oodatavad andmeobjektid puuduvad,
- '69 88' turvalise sõnumivahetuse andmeobjektid valed.

CSM_027 Kui sõidumeerikukaart saadab olekubaidi tagasi ilma turvalise sõnumivahetuse andmeobjektideta või turvalise sõnumivahetuse vigaste andmeobjektidega, peab sõidukiüksus seansi lõpetama.

5.3. Krüptograafiliste kontrollsummade arvutusalgorithm

CSM_028 Krüptograafiliste kontrollsummade koostamisel kasutatakse retail MAC tüüpi sõnumi tõendamise kontrollsummasid vastavalt ANSI X9.19 koos DES koodiga:

- esimene etapp: esimese kontrollploki y_0 on $E(K_a, SSC)$,
- järgmised etapid: kontrollplokkide y_1, \dots, y_n arvutamiseks kasutatakse K_a ,
- lõppetapp: krüptograafiline kontrollsumma arvutatakse viimasest kontrollplokkist y_n järgmiselt: $E(K_a, D(K_b, y_n))$,

kus $E()$ tähendab kodeerimist DES koodiga ja $D()$ tähendab lahtikodeerimist DES koodiga.

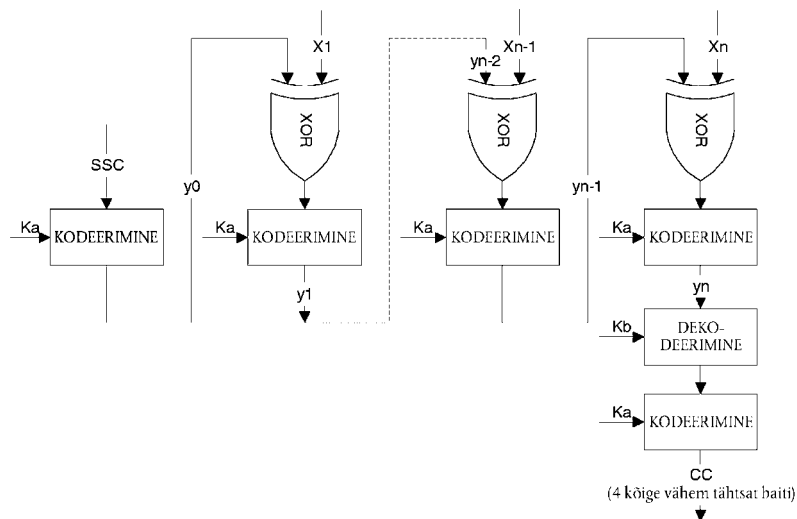
Edastatakse krüptograafilise kontrollsumma neli kõige tähtsamat baiti.

CSM_029 Saatejada lugeja (SSC) häälestatakse võtme kokkuleppeprotseduuri ajal:

SSC algolekusse: $Rnd3$ (4 kõige vähem tähtsat baiti) || $Rnd1$ (4 kõige vähem tähtsat baiti).

CSM_030 Enne MAC_i arvutamist suurendatakse saatejada lugejat iga kord ühe võrra (st esimese käsu saatejada lugeja on esimene $SSC + 1$, esimese vastuse saatejada lugeja on esimene $SSC + 2$).

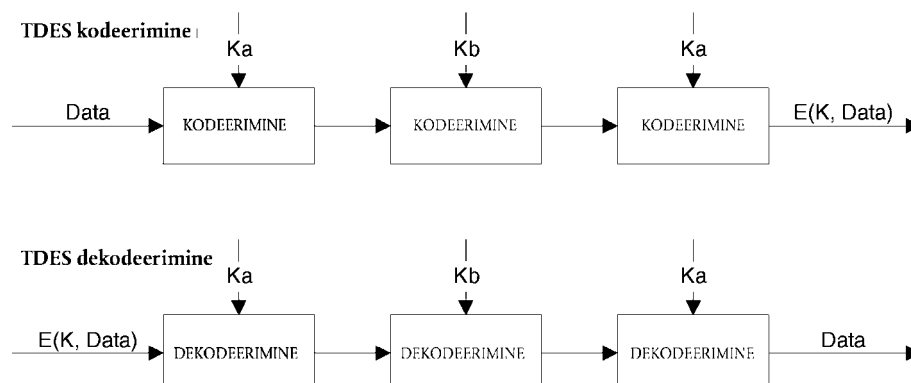
Järgmisel joonisel on näidatud retail MAC_i arvutamine:



5.4. Krüptogrammide arvutusalgorithm andmeobjektide konfidentsiaalsuse tarvis

CSM_031 Krüptogrammide arvutamisel kasutatakse TDEAd TCBC toimimismooduses vastavalt viidetele TDES ja TDES-OP ning nii, et nullvektor on esimene väärtusplokk.

Järgmisel joonisel on näidatud võtmete rakendus TDESis:



6. ANDMETE ALLALAADIMISE DIGITAALALLKIRJAMEHCHANISMID

CSM_032 Programmeeritav eriseade (IDE) salvestab seadmelt (sõidukiüksuselt või kaardilt) ühe allalaadimise käigus saadud andmed ühte füüsilisse andmefaili. See fail peab sisaldama sertifikaate MS_iC ja EQT.C. Fail sisaldab andmeplokkide digitaalallkirju vastavalt 7. liitele "Andmete allalaadimisprotokollid".

CSM_033 Allalaaditud andmete digitaalallkirjades kasutatakse sellise liitega digitaalallkirju, et allalaaditud andmeid saaks soovi korral lugeda mis tahes dešifreerimiseta.

6.1. Digitaalallkirja loomine

CSM_034 Seadme andmeallkirja loomisel kasutatakse viites (PKCS1) määratletud liitega allkirja koos SHA-1 räsifunktsiooniga:

$$\text{Allkiri} = \text{EQT.SK}[\text{'00'} \parallel \text{'01'} \parallel \text{PS} \parallel \text{'00'} \parallel \text{DER}(\text{SHA-1}(\text{Data}))]$$

PS = 'FF' väärtusega baitidest moodustatud täidetud oktetistringid, mille pikkus on 128.

DER(SHA-1(M)) on algoritmi identifikatsiooni kood räsifunktsiooni tarvis ja räsiväärtuse kodeerimine standardi ASN.1 DigestInfo andmetüübi kohaseks (DER — tunnustatud kodeerimiseeskirjad):

'30' || '21' || '30' || '09' || '06' || '05' || '2B' || '0E' || '03' || '02' || '1A' || '05' || '00' || '04' || '14' || Räsi väärtus.

6.2. Allkirja tõendamine

CSM_035 Andmeallkirja tõendamiseks allalaaditud andmetel kasutatakse viites (PKCS1) määratletud liitega allkirja koos SHA-1 räsifunktsiooniga.

Tõendaja peab teadma sõltumatult (ja see peab olema usaldusväärne) Euroopa avalikku võtit EUR.PK.

Järgmises tabelis on esitatud protokoll, mida võib täita kontrollikaarti omav programmeeritav eriseade, et tõendada välisele andmekandjale allalaaditud ja seal salvestatud andmete terviklikkust. Kontrollikaarti kasutatakse digitaalallkirjade dešifreerimiseks. Antud juhul ei tohi seda funktsiooni rakendada programmeeritavas eriseadmes.

Seade, mis on analüüsitud andmed alla laadinud ja need allkirjastanud, on tähistatud EQT.

