Euroopa Liidu

Teataja

L 139

Eestikeelne väljaanne

Õigusaktid

59. aastakäik

26. mai 2016

Sisukord

[1] EMPs kohaldatav tekst

II

(Muud kui seadusandlikud aktid)

MÄÄRUSED

KOMISJONI RAKENDUSMÄÄRUS (EL) 2016/799,

18. märts 2016,

millega rakendatakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 165/2014, millega sätestatakse sõidumeerikute ja nende komponentide konstruktsiooni, katsetamise, paigaldamise, kasutamise ja parandamise nõuded

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 4. veebruari 2014. aasta määrust (EL) nr 165/2014 autovedudel kasutatavate sõidumeerikute kohta, ([1]) eriti selle artiklit 11 ja artikli 12 lõiget 7,

ning arvestades järgmist:

(1) Määrusega (EL) nr 165/2014 on ette nähtud võtta kasutusele teise põlvkonna digitaalsed sõidumeerikud ehk arukad sõidumeerikud, millel on ühendus ülemaailmse satelliitnavigatsioonisüsteemi (GNSS) seadmega, varajast avastamist võimaldav kaugsideseade ja liides intelligentsete transpordisüsteemidega. Tuleks kehtestada arukate sõidumeerikute konstruktsiooni käsitlevate tehniliste nõuete kirjeldus.

(2) Määruse (EL) nr 165/2014 artikli 9 lõikes 4 ette nähtud varajase avastamise kaugsideseade peaks kooskõlas nõukogu direktiiviga 96/53/EÜ ([2]) edastama teeäärsele kontrolliametnikule digitaalse sõidumeeriku andmed ja teabe komplektse sõiduki (veduk ja haagised või poolhaagised) massi ja teljekoormuste kohta. See peaks võimaldama kontrolliasutustel sõidukeid kiirelt ja tõhusalt kontrollida ja vähendama elektrooniliste seadmete hulka sõiduki kabiinis.

(3) Vastavalt direktiivile 96/53/EÜ tuleks varajase avastamise kaugsideseadmes kasutada Euroopa Standardikomitee (CEN) DSRC standardeid, ([3]) millele on osutatud nimetatud direktiivis, ning sagedusala 5795–5805 MHz. Kuna seda sagedusala kasutatakse ka elektroonilises teemaksusüsteemis, peaksid kontrolliametnikud hoiduma varajase avastamise kaugsideseadme kasutamisest teemaksu kogumise punktis, et hoida ära teemaksu- ja kontrollirakenduste vahelisi tõrkeid.

(4) Arukates sõidumeerikutes tuleks praeguste turvaaukude parandamiseks võtta kasutusele uued turvamehhanismid digitaalsete sõidumeerikute turvataseme säilitamiseks. Üks selline turvaauk on digitaalsete sertifikaatide aegumiskuupäeva puudumine. Turvaküsimustega seotud parima tava järgimiseks soovitatakse hoiduda aegumiskuupäevata digitaalsete sertifikaatide kasutamisest. Sõidukiseadme nõuetekohane tööiga tavapärasel käitamisel peaks olema 15 aastat alates sõidukiseadme digitaalsete sertifikaatide väljaandmise kuupäevast. Selle perioodi möödudes tuleks sõidukiseade välja vahetada.

([1]) ELT L 60, 28.2.2014, lk 1.

([2]) Nõukogu 25. juuli 1996. aasta direktiiv 96/53/EÜ, millega kehtestatakse teatavatele ühenduses liikuvatele maanteesõidukitele siseriiklikus ja rahvusvahelises liikluses lubatud maksimaalmõõtmed ning rahvusvahelises liikluses lubatud täismass (EÜT L 235, 17.9.1996, lk 59).

([3]) Euroopa Standardikomitee (CEN) sihtotstarbelise lähitoimeside (DSRC) standardid EN 12253, EN 12795, EN 12834 ja EN 13372 ning ISO 14906.

(5) Aruka sõidumeeriku tõhusa töö üks põhielement on usaldusväärse turvatud asukohateabe esitamine. Seepärast on asjakohane arukate sõidumeerikute turvalisuse suurendamiseks tagada nende ühilduvus Galileo programmi raames pakutavate lisandväärtusteenustega, mis on sätestatud Euroopa Parlamendi ja nõukogu määruses (EL) nr 1285/2013 ([1]).

(6) Vastavalt määruse (EL) nr 165/2014 artikli 8 lõikele 1, artikli 9 lõikele 1 ning artikli 10 lõigetele 1 ja 2 tuleks nimetatud määrusega kehtestatud turvamehhanisme kohaldada 36 kuud pärast vajalike asjaomaste rakendusaktide jõustumist, et võimaldada tootjatel töötada välja uue põlvkonna arukad sõidumeerikud ja saada pädevatelt asutustelt nende jaoks tüübikinnitustunnistus.

(7) Määruse (EL) nr 165/2014 kohaselt peaks sõidukile, mis on registreeritud liikmesriigis esmakordselt 36 kuud pärast käesoleva komisjoni määruse jõustumist, olema paigaldatud arukas sõidumeerik, mis vastab käesoleva komisjoni määruse nõuetele. Igal juhul peab kõikidele sõidukitele, mida kasutatakse muus liikmesriigis kui see, kus sõiduk on registreeritud, olema paigaldatud nõuetekohane arukas sõidumeerik 15 aastat pärast kõnealuste nõuete kohaldamise alguskuupäeva.

(8) Komisjoni määrusega (EÜ) nr 68/2009 ([2]) oli lubatud kasutada M1- ja N1-kategooria sõidukites 31. detsembril 2013 lõppenud üleminekuperioodil adapterit, mis võimaldab paigaldada sellistele sõidukitele sõidumeeriku. Tulenevalt tehnilistest raskustest seoses kõnealuse adapteri kasutamisele alternatiivi leidmisega on autotööstuse ja sõidumeerikute valdkonna eksperdid jõudnud koos komisjoniga järeldusele, et alternatiivne lahendus adapteri asendamiseks ei ole teostatav, ilma et sellega kaasneksid asjaomases tööstusharus suured kulutused, mis on turu suurust arvesse võttes ebaproportsionaalsed. Seepärast tuleks lubada kasutada kõnealust adapterit M1- ja N1-kategooria sõidukites piiramata aja jooksul.

(9) Käesolevas määruses sätestatud meetmed on kooskõlas määruse (EL) nr 165/2014 artikli 42 lõikes 3 nimetatud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Sisu ja reguleerimisala

1. Käesoleva määrusega nähakse ette sätted, mis on vajalikud sõidumeerikut käsitlevate selliste nõuete ühetaoliseks kohaldamiseks, mis hõlmavad järgmisi aspekte:

a) sõiduki asukoha salvestamine sõidukijuhi igapäevase tööaja konkreetsetel hetkedel;

b) aruka sõidumeerikuga seotud võimaliku manipuleerimise või väärkasutuse varajane avastamine kaugside teel;

c) liides intelligentsete transpordisüsteemidega;

d) sõidumeerikut käsitleva tüübikinnitusmenetlusega seotud haldus- ja tehnilised nõuded, mis muu hulgas hõlmavad turvamehhanisme.

2. Aruka sõidumeeriku ja selle komponentide konstruktsiooni, katsetamise, paigaldamise, kontrollimise, kasutamise ja parandamise puhul järgitakse käesoleva määruse IC lisas sätestatud tehnilisi nõudeid.

3. Muu sõidumeeriku kui aruka sõidumeeriku konstruktsiooni, katsetamise, paigaldamise, kontrollimise, kasutamise ja parandamise puhul järgitakse jätkuvalt nõukogu määruse (EMÜ) nr 3821/85 ([3]) I või IB lisa asjaomaseid nõudeid.

([1]) Euroopa Parlamendi ja nõukogu 11. detsembri 2013. aasta määrus (EL) nr 1285/2013 Euroopa satelliitnavigatsioonisüsteemide rajamise ja kasutamise kohta, millega tunnistatakse kehtetuks nõukogu määrus (EÜ) nr 876/2002 ning Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 683/2008 (ELT L 347, 20.12.2013, lk 1).

([2]) Komisjoni 23. jaanuari 2009. aasta määrus (EÜ) nr 68/2009, millega kohandatakse üheksandat korda tehnika arenguga nõukogu määrust (EMÜ) nr 3821/85 maanteevedudel kasutatavate sõidumeerikute kohta (ELT L 21, 24.1.2009, lk 3).

([3]) Nõukogu 20. detsembri 1985. aasta määrus (EMÜ) nr 3821/85 autovedudel kasutatavate sõidumeerikute kohta (EÜT L 370, 31.12.1985, lk 8).

4. Vastavalt nõukogu direktiivi 96/53/EÜ artiklile 10d edastab varajase avastamise kaugsideseade pettuste varajase tuvastamise võimaldamiseks ka sõidukisisese kaalumissüsteemi abil saadud massiandmed.

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse määruse (EL) nr 165/2014 artiklis 2 sätestatud mõisteid.

Peale selle kasutatakse järgmisi mõisteid:

1) *digitaalne sõidumeerik* või *esimese põlvkonna sõidumeerik* – digitaalne sõidumeerik, mis ei ole arukas sõidumeerik;

2) *GNSSi välisseade* – mitmeosalise sõidukiseadme osa, mis sisaldab GNSSi vastuvõtjat ja muid komponente, mis on vajalikud sõidukiseadme muusse osasse edastatavate asukohaandmete kaitsmiseks;

3) *teatmik* – täielik elektrooniline või paberkandjal toimik, mis sisaldab kõiki andmeid, mille tootja või tema esindaja on esitanud tüübikinnitusasutusele sõidumeeriku või selle komponendi tüübikinnituse saamiseks ning mis sisaldab määruse (EL) nr 165/2014 artikli 12 lõikes 3 nimetatud sertifikaate ja käesoleva määruse IC lisas määratletud katsete tulemusi, samuti jooniseid, fotosid ja muid asjakohaseid dokumente;

4) *teabepakett* – elektrooniline või paberkandjal teatmik, millele tüübikinnitusasutus on oma ülesannete täitmise käigus lisanud mis tahes muid dokumente, sealhulgas tüübikinnitusmenetluse lõppedes antava EÜ tüübikinnitustunnistuse sõidumeeriku või selle komponendi kohta;

5) *teabepaketi sisukord* – dokument, mis sisaldab teabepaketi sisu nummerdatud loetelu kõikide selle paketi asjakohaste osade kohta; nimetatud dokumendis tuuakse eraldi välja EÜ tüübikinnitusmenetluse järjestikused etapid, sealhulgas teabepaketi võimaliku muutmise ja ajakohastamise kuupäevad;

6) *varajase avastamise kaugsideseade* – sõidukiseadme osa, mida kasutatakse sihtotstarbeliseks teeäärseks kontrollimiseks;

7) *arukas sõidumeerik* või *teise põlvkonna sõidumeerik* – digitaalne sõidumeerik, mis vastab määruse (EL) nr 165/2014 artiklite 8, 9 ja 10 ning käesoleva määruse IC lisa sätetele;

8) *sõidumeeriku komponent* või *komponent* – üks järgmistest elementidest: sõidukiseade, liikumisandur, sõidumeerikukaart, salvestusleht, GNSSi välisseade ja varajase avastamise kaugsideseade;

9) *tüübikinnitusasutus* – liikmesriigi asutus, kes on pädev viima läbi sõidumeerikut või selle komponenti käsitleva tüübikinnitusmenetluse, andma loa, andma välja tüübikinnitustunnistuse ja vajaduse korral selle tühistama, toimima teiste liikmesriikide tüübikinnitusasutuste kontaktpunktina ning tagama, et tootjad täidavad oma kohustusi seoses käesoleva määruse nõuete järgimisega.

Artikkel 3

Asukohapõhised teenused

1. Tootjad tagavad aruka sõidumeeriku ühilduvuse Galileo süsteemi ja Euroopa Geostatsionaarse Navigatsioonilisasüsteemi (EGNOS) positsioneerimisteenustega.

2. Tootjad võivad lisaks lõikes 1 nimetatud süsteemidele tagada ühilduvuse ka muude satelliitnavigatsioonisüsteemidega.

Artikkel 4

Sõidumeerikut või selle komponenti käsitlev tüübikinnitusmenetlus

1. Tootja või tema esindaja esitab sõidumeerikut, selle komponenti või komponentide rühma käsitleva tüübikinnitustaotluse liikmesriigi määratud tüübikinnitusasutusele. Taotlus koosneb teatmikust, mis sisaldab teavet kõikide asjaomaste komponentide kohta, sealhulgas vajaduse korral muude sõidumeeriku koosseisu kuuluvate komponentide tüübikinnitustunnistusi, samuti kõiki muid asjakohaseid dokumente.

2. Liikmesriik annab tüübikinnituse iga sõidumeeriku, selle komponendi või komponentide rühma puhul, mis vastab artikli 1 lõikes 2 või lõikes 3 osutatud haldus- ja tehnilistele nõuetele. Sellisel juhul väljastab tüübikinnitusasutus taotlejale tüübikinnitustunnistuse, mis vastab käesoleva määruse II lisas sätestatud näidisele.

3. Tüübikinnitusasutus võib tootjalt või tema esindajalt nõuda lisateabe esitamist.

4. Tootja või tema esindaja teeb tüübikinnitusasutusele ja määruse (EL) nr 165/2014 artikli 12 lõikes 3 nimetatud sertifikaatide väljaandmise eest vastutavatele üksustele kättesaadavaks tüübikinnitusmenetluse rahuldavaks läbiviimiseks vajaliku arvu sõidumeerikuid või sõidumeeriku komponente.

5. Kui tootja või tema esindaja taotleb sõidumeeriku konkreetse komponendi või komponentide rühma tüübikinnitust, esitab ta tüübikinnitusasutusele sõidumeeriku muud komponendid, mille kohta on juba antud tüübikinnitus, samuti muud sõidumeeriku komplekteerimiseks vajalikud osad, et võimaldada tüübikinnitusasutusel viia läbi vajalikke katseid.

Artikkel 5

Tüübikinnituse muutmine

1. Tootja või tema esindaja teavitab algse tüübikinnituse andnud tüübikinnitusasutust viivitamata kõikidest muudatustest sõidumeeriku tarkvaras või riistvaras või selle tootmisel kasutatud materjalide omadustes, mis on esitatud teabepaketis, ning esitab taotluse tüübikinnituse muutmiseks.

2. Tüübikinnitusasutus võib vastavalt muudatuse olemusele kehtivat tüübikinnitust muuta või laiendada või anda välja uue tüübikinnituse.

Tüübikinnitust muudetakse juhul, kui muudatus sõidumeeriku tarkvaras või riistvaras või selle tootmisel kasutatud materjalide omadustes on tüübikinnitusasutuse hinnangul väike. Sellisel juhul väljastab tüübikinnitusasutus teabepaketi muudetud dokumendid, milles on esitatud tehtud muudatuse sisu ja heakskiitmise kuupäev. Selle nõude täitmiseks piisab teabepaketi ajakohastatud konsolideeritud versioonist, millele on lisatud tehtud muudatuse üksikasjalik kirjeldus.

Tüübikinnitust laiendatakse juhul, kui muudatus sõidumeeriku tarkvaras või riistvaras või selle tootmisel kasutatud materjalide omadustes on tüübikinnitusasutuse hinnangul ulatuslik. Sellisel juhul võib tüübikinnitusasutus nõuda uute katsete tegemist ja teavitada sellest tootjat või tema esindajat. Kui kõnealuste katsete tulemused on rahuldavad, annab tüübikinnitusasutus välja muudetud tüübikinnitustunnistuse, mis sisaldab heakskiidetud laiendusele viitavat numbrit. Tüübikinnitustunnistuses esitatakse laienduse põhjendus ja heakskiitmise kuupäev.

3. Teabepaketi sisukorras esitatakse tüübikinnituse viimase laiendamise või muutmise või selle ajakohastatud versiooni viimase konsolideerimise kuupäev.

4. Uus tüübikinnitus on vajalik juhul, kui tüübikinnitusega sõidumeeriku või selle komponendi puhul taotletava muudatuse tõttu tuleb välja anda uus turvasertifikaat või koostalitlusvõime sertifikaat.

Artikkel 6

Jõustumine

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

Seda kohaldatakse alates 2. märtsist 2016.

Lisasid kohaldatakse alates 2. märtsist 2019, välja arvatud 16. liide, mida kohaldatakse alates 2. märtsist 2016.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 18. märts 2016

Komisjoni nimel
president
Jean-Claude JUNCKER

IC LISA

Konstruktsiooni-, katsetus-, paigaldus- ja kontrollinõuded

SISSEJUHATUS

Digitaalse sõidumeeriku süsteemi esimene põlvkond on kasutusel alates 1. maist 2006. Seda on lubatud kasutada riigisisestel vedudel kuni selle kasutusea lõpuni. Seevastu rahvusvaheliste vedude puhul peab 15 aastat pärast komisjoni käesoleva määruse jõustumist olema kõigile sõidukitele paigaldatud nõuetekohane teise põlvkonna arukas sõidumeerik, mis võetakse kasutusele käesoleva määruse alusel.

Käesolev lisa sisaldab teise põlvkonna sõidumeerikutele ja sõidumeerikukaartidele esitatavaid nõudeid. Alates kõnealuste meerikute kasutuselevõtu kuupäevast peab esmakordselt registreeritavatele sõidukitele olema paigaldatud teise põlvkonna sõidumeerik ning tuleb hakata välja andma teise põlvkonna sõidumeerikukaarte.

Teise põlvkonna sõidumeerikusüsteemi tõrgeteta kasutuselevõtu soodustamiseks

— konstrueeritakse teise põlvkonna sõidumeerikukaardid nii, et neid saab kasutada ka esimese põlvkonna sõidukiseadmetes, ning

— ei nõuta kehtivate esimese põlvkonna sõidumeerikukaartide väljavahetamist kasutuselevõtu kuupäeval.

See võimaldab juhtidel jätta alles oma kordumatu juhikaart ja kasutada seda mõlemas süsteemis.

Teise põlvkonna sõidumeerikute kalibreerimiseks kasutatakse siiski ainult teise põlvkonna töökojakaarte.

Käesolev lisa sisaldab kõiki nõudeid, mis on seotud esimese ja teise põlvkonna sõidumeerikusüsteemide koostalitlusvõimega.

15. liide sisaldab täiendavaid üksikasju kahe süsteemi samaaegse kasutamise kohta.

Liidete loetelu

1. MÕISTED

Käesolevas lisas kasutatakse järgmisi mõisteid:

a) aktiveerimine –

etapp, kus töökojakaardi kasutamisel sõidumeerik täielikult käivitub ning rakenduvad kõik selle funktsioonid, kaasa arvatud turvafunktsioonid;

b) autentimine –

funktsioon, mille eesmärk on väidetav isikusamasus kindlaks teha ja tõendada;

c) autentsus –

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

d) sisseehitatud test –

vajaduse korral tehtav test, mille käivitab kasutaja või välisseade;

e) kalendripäev –

ööpäev kellaajast 00.00 kellaajani 24.00. Kõik kalendripäevad on seotud koordineeritud maailmaajaga (UTC);

f) aruka sõidumeeriku kalibreerimine –

andmemälus sisalduvate sõiduki parameetrite ajakohastamine või kinnitamine. Sõiduki parameetrid on sõiduki identimisandmed (VIN (valmistajatehase tähis), VRN (sõiduki registreerimisnumber) ja sõiduki registreerinud liikmesriik) ning sõiduki omadused (sõidukit iseloomustav koefitsient, sõidumeeriku konstant, rehvide efektiivümbermõõt, rehvimõõt, kiiruspiiriku seadistus (kui piirik on olemas), tegelik koordineeritud maailmaaeg, läbisõidumõõdiku hetkenäit); sõidumeeriku kalibreerimise käigus salvestatakse andmemällu kõigi tüübikinnitusega seotud plommide tüübid ja identifikaatorid;

kui ajakohastatakse või kinnitatakse üksnes koordineeritud maailmaaega, loetakse seda aja korrigeerimiseks ja mitte kalibreerimiseks, eeldusel et see ei ole vastuolus nõudega 409;

sõidumeeriku kalibreerimiseks on vaja kasutada töökojakaarti;

g) kaardi number –

16-kohaline tähtnumbriline number, millega identitakse üheselt sõidumeerikukaart asjaomases liikmesriigis. Kaardi number sisaldab kaardi järjekorraindeksit (kui see on olemas) ning kaardi asendus- ja pikendusindeksit;

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

h) kaardi järjekorraindeks –

kaardi numbri 14. tähtnumbriline märk, mida kasutatakse selliste kaartide eristamiseks, mis on välja antud ettevõttele, töökojale või kontrolliasutusele, kellele võib välja anda mitu sõidumeerikukaarti. Kaardi numbri esimese 13 märgi abil saab asjaomase ettevõtte, töökoja või kontrolliasutuse üheselt identida;

i) kaardi pikendusindeks –

kaardi numbri 16. tähtnumbriline märk, mis sõidumeerikukaardi igal pikendamisel suureneb;

j) kaardi asendusindeks –

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

k) sõidukit iseloomustav koefitsient –

numbriline parameeter, mis vastab sõidukit sõidumeerikuga ühendava osa (käigukasti väljundvõll või -telg) tekitatud väljundsignaali väärtusele, kui sõiduk läbib nõudes 414 määratletud standardsetes katsetingimustes ühe kilomeetri pikkuse vahemaa. Kõnealust koefitsienti väljendatakse impulssides kilomeetri kohta (w = … imp/km);

l) ettevõttekaart –

sõidumeerikukaart, mille liikmesriigi ametiasutus väljastab veoettevõtjale, kellel on vaja käitada sõidukeid, millele on paigaldatud sõidumeerik, ning mis võimaldab tuvastada veoettevõtjat ning kuvada, alla laadida ja trükkida asjaomase veoettevõtja lukustatud sõidumeerikusse salvestatud andmeid;

m) sõidumeeriku konstant –

numbriline parameeter, mis vastab ühe kilomeetri pikkuse vahemaa näitamiseks ja registreerimiseks vajaliku sisendsignaali väärtusele; konstanti väljendatakse impulssides kilomeetri kohta (k = … imp/km);

n) sõidumeerikus arvutatud pidev juhtimisaeg ([1]) –

pidev juhtimisaeg arvutatakse konkreetse juhi jooksva kumulatiivse juhtimisajana alates viimasest 45-minutilisest või pikemast VALMISOLEKU või PUHKEPAUSI/PUHKUSE või TEADMATA ([2]) perioodist (see periood võib olla jagatud vastavalt Euroopa Parlamendi ja nõukogu määrusele (EÜ) nr 561/2006 ([3])). Arvutustes võetakse vajaduse korral arvesse juhikaardile salvestatud eelnevaid tegevusi. Kui juht ei ole oma kaarti sisestanud, tehakse arvutused mälus olevate andmete põhjal, mis on seotud asjaomase kaardipesaga ja jooksva perioodiga, mil kaarti ei ole sisestatud;

o) kontrollikaart –

liikmesriigi ametiasutuse poolt riiklikule pädevale kontrolliasutusele väljastatud sõidumeerikukaart, mille abil on võimalik kontrolliasutust ning vajaduse korral kontrolliametnikku tuvastada ning mis võimaldab juurdepääsu mällu või juhikaardile salvestatud andmetele ja vajaduse korral töökojakaardi andmetele nende lugemiseks, trükkimiseks ja/või allalaadimiseks.

Samuti võimaldab see juurdepääsu teeäärse kalibreerimiskontrolli funktsioonile ja varajase avastamise kaugsidelugejas olevatele andmetele;

p) sõidumeerikus arvutatud kumulatiivne puhkepauside aeg ([1]) –

kumulatiivne puhkepauside aeg arvutatakse konkreetse juhi jooksva kumulatiivse ajana 15 minutit või kauem kestvate VALMISOLEKU või PUHKEPAUSI/PUHKUSE või TEADMATA ([2]) perioodide põhjal alates viimasest 45-minutilisest või pikemast VALMISOLEKU või PUHKEPAUSI/PUHKUSE või TEADMATA ([2]) perioodist (see periood võib olla jagatud vastavalt määrusele (EÜ) nr 561/2006).

Arvutustes võetakse vajaduse korral arvesse juhikaardile salvestatud eelnevaid tegevusi. Negatiivse pikkusega teadmata perioode (teadmata perioodi algus > teadmata perioodi lõpp), mis on seotud kahe eri sõidumeeriku kattuvate aegadega, ei võeta arvutamisel arvesse.

Kui juht ei ole oma kaarti sisestanud, tehakse arvutused mälus olevate andmete põhjal, mis on seotud asjaomase kaardipesaga ja jooksva perioodiga, mil kaarti ei ole sisestatud;

([1]) Pideva juhtimisaja ja kumulatiivse puhkepauside aja sellise arvutamise eesmärk on võimaldada sõidumeerikul arvutada pidevat juhtimisaega hoiatamise eesmärgil. See ei piira nende aegade juriidilist tõlgendamist. Pideva juhtimisaja ja kumulatiivse puhkepauside aja arvutamiseks võib kasutada alternatiivseid meetodeid, et asendada käesolevad määratlused, kui need on teiste asjakohaste õigusaktide ajakohastamise tulemusena aegunud.

([2]) TEADMATA periood vastab perioodile, mil juhikaart ei olnud sõidumeerikusse sisestatud ja mille kohta puuduvad käsitsi tehtud sissekanded juhi tegevuse kohta.

([3]) Euroopa Parlamendi ja nõukogu 15. märtsi 2006. aasta määrus (EÜ) nr 561/2006, mis käsitleb teatavate autovedusid käsitlevate sotsiaalõigusnormide ühtlustamist ja millega muudetakse nõukogu määrusi (EMÜ) nr 3821/85 ja (EÜ) nr 2135/98 ning tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 3820/85 (ELT L 102, 11.4.2006, lk 1).

q) andmemälu –

sõidumeerikusse ehitatud elektrooniline mäluseade;

r) digitaalallkiri –

andmeplokile lisatud andmed või andmeploki krüptograafiline muundamine, mille põhjal andmeploki saajal on võimalik tõendada andmeploki autentsust ja terviklust;

s) allalaadimine –

sõidukiseadme andmemällu või sõidumeeriku mälukaardile salvestatud andmefailide osaline või täielik kopeerimine koos digitaalse allkirjaga, tingimusel et selle protsessiga ei muudeta ega kustutata salvestatud andmeid.

Arukate sõidumeerikute sõidukiseadmete ning andmefailide allalaadimiseks ette nähtud seadmete tootjad võtavad kõik asjakohased meetmed tagamaks, et selliste andmete allalaadimine põhjustab transpordiettevõtjale ja juhile minimaalselt viivitusi.

Üksikasjaliku kiirusfaili allalaadimine ei pruugi olla määruse (EÜ) nr 561/2006 nõuete täitmise kindlakstegemiseks vajalik, kuid seda faili võib kasutada muul eesmärgil, näiteks õnnetuse uurimisel;

t) juhikaart –

liikmesriigi ametiasutuse poolt konkreetsele juhile väljastatud sõidumeerikukaart, mille abil on võimalik juhti tuvastada ja mis võimaldab juhi tegevuse andmete salvestamist;

u) rehvide efektiivümbermõõt –

iga sõidukit vedava ratta (veoratta) ühe täispöördega läbitud keskmine vahemaa. Vahemaad tuleb mõõta nõudes 414 määratletud standardsetes katsetingimustes ning seda väljendatakse kujul „l = … mm“. Sõidukitootja võib asendada vahemaa mõõtmise teoreetiliste arvutustega, milles võetakse arvesse normaalses sõidukorras koormata sõiduki massi jaotumist telgede vahel ([1]). Teoreetiliste arvutuste meetodid kinnitab liikmesriigi pädev asutus ning see peab toimuma enne sõidumeeriku aktiveerimist;

v) sündmus –

aruka sõidumeeriku tuvastatud väärtalitlus, mille põhjuseks võib olla pettusekatse;

w) GNSSi välisseade –

mitmeosalise sõidukiseadme puhul seade, mis sisaldab GNSSi vastuvõtjat ning sõidukiseadme muule osale edastatavate asukohaandmete kaitsmiseks vajalikke muid komponente;

x) viga –

aruka sõidumeeriku tuvastatud väärtalitlus, mille põhjuseks võib olla seadme rike või tõrge;

y) GNSSi vastuvõtja –

elektroonikaseade, mis võtab vastu ühe või mitme globaalse satelliitnavigatsioonisüsteemi (ingliskeelne lühend GNSS) signaale ja töötleb neid digitaalselt, et saada teavet asukoha, kiiruse ja aja kohta;

z) paigaldamine –

sõidumeeriku paigaldamine sõidukisse;

([1]) Muudetud määrus (EL) nr 1230/2012, millega rakendatakse Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 661/2009 seoses mootorsõidukite ja nende haagiste masside ja mõõtmete tüübikinnitusnõuetega ning millega muudetakse Euroopa Parlamendi ja nõukogu direktiivi 2007/46/EÜ (ELT L 353, 21.12.2012, lk 31).

aa) koostalitlusvõime –

süsteemide ja nende aluseks olevate äriprotsesside võime andmeid vahetada ning teavet jagada;

bb) liides –

süsteemide vahel asuv seade, mille kaudu on võimalik süsteemide ühendamine ja vastastoime;

cc) asukoht –

sõiduki geograafilised koordinaadid kindlal ajahetkel;

dd) liikumisandur –

sõidumeeriku osa, mis edastab sõiduki kiirust ja/või läbitud vahemaad kajastavat signaali;

ee) kehtetu kaart –

kaart, millel on avastatud rike või mille esialgne autentimine ebaõnnestus või mille kehtivusaeg ei ole veel alanud või on juba lõppenud;

ff) avatud standard –

standardit kirjeldavas dokumendis sätestatud standard, mis on tasuta või sümboolse tasu eest kättesaadav ning mida on lubatud paljundada, levitada ja kasutada tasuta või sümboolse tasu eest;

gg) sõidumeerik mittevajalik –

sõidumeeriku kasutamist ei nõuta vastavalt nõukogu määruse (EÜ) nr 561/2006 sätetele;

hh) kiiruse ületamine –

sõiduki suurima lubatud kiiruse ületamine, mis on määratletud kui olukord, kus sõiduki mõõdetud kiirus ületab 60 sekundist pikema perioodi vältel kiiruspiiriku puhul ette nähtud ülemmäära, mis on sätestatud nõukogu direktiivi 92/6/EMÜ ([1]) uusimas muudetud redaktsioonis;

ii) perioodiline kontroll –

selliste toimingute kogum, mille eesmärk on kontrollida, kas sõidumeerik töötab nõuetekohaselt, kas selle seaded vastavad sõiduki parameetritele ning kas sõidumeeriku külge ei ole kinnitatud manipulatsiooniseadmeid;

jj) printer –

sõidumeeriku osa, mis trükib välja salvestatud andmed;

kk) varajase avastamise eesmärgil toimuv kaugside –

sihipäraste teeäärsete kontrollide ajal varajase avastamise kaugsideseadme ja varajase avastamise kaugsidelugeja vahel toimuv side, mille eesmärk on kaugelt tuvastada sõidumeeriku võimalikku manipuleerimist või väärkasutamist;

ll) kaugsideseade –

sõidukiseadmel olev varustus, mida kasutatakse sihipäraste teeäärsete kontrollide tegemiseks;

([1]) Nõukogu 10. veebruari 1992. aasta direktiiv 92/6/EMÜ (teatava kategooria mootorsõidukitele kiiruspiirikute paigaldamise ja nende kasutamise kohta ühenduses (EÜT L 57, 2.3.1992, lk 27).

mm) varajase avastamise kaugsidelugeja –

süsteem, mida kontrolliametnikud sihipäraste teeäärsete kontrollide käigus kasutavad;

nn) pikendamine –

uue sõidumeerikukaardi väljaandmine, kui olemasoleva kaardi kehtivusaeg hakkab lõppema või kui kaart ei ole töökorras ja on tagastatud kaarte välja andvale asutusele. Pikendamise puhul tuleb alati olla kindel, et üheaegselt ei ole kasutatavad kaks kehtivat kaarti;

oo) remont –

liikumisanduri, sõidukiseadme või juhtme remont, mille käigus asjaomane osa tuleb toiteallikast või muudest sõidumeeriku osadest lahti ühendada või avada või mis eeldab liikumisanduri või sõidukiseadme avamist;

pp) kaardi asendamine –

uue sõidumeerikukaardi väljaandmine eesmärgiga asendada olemasolev kaart, mille kohta on teatatud, et see on kadunud, varastatud või ei ole töökorras ning mida ei ole kaarte välja andvale asutusele tagastatud. Asendamisega kaasneb alati risk, et üheaegselt eksisteerib kaks kehtivat kaarti;

qq) turvalisuse sertifitseerimine –

protsess, mille käigus ühiste kriteeriumide täitmist kontrolliv sertifitseerimisasutus tõendab, et uurimisalune sõidumeerik (või selle osa) või sõidumeerikukaart vastab sellega seotud kaitseprofiilis määratletud turvanõuetele;

rr) enesekontrollitest –

sõidumeeriku tehtavad regulaarsed ja automaatsed katsed vigade avastamiseks;

ss) aja mõõtmine –

koordineeritud maailmaaja (UTC) kuupäeva ja kellaaja pidev digitaalne salvestamine;

tt) aja korrigeerimine –

regulaarne hetkeaja automaatne korrigeerimine maksimaalselt ühe minuti võrra või kalibreerimise ajal toimuv korrigeerimine;

uu) rehvimõõt –

rehvide (väliste veorataste) mõõtmed, nagu on määratud vastavalt nõukogu direktiivi 92/23/EMÜ ([1]) uusimale muudetud redaktsioonile;

vv) sõiduki identimisandmed –

sõiduki identimise numbrid: sõiduki registreerimisnumber (VRN) koos viitega sõiduki registreerinud liikmesriigile ja valmistajatehase tähis (VIN) ([2]);

ww) nädal sõidumeerikus tehtavate arvutuste jaoks –

ajavahemik alates UTC kellaajast 00.00 esmaspäeval kuni UTC kellaajani 24.00 pühapäeval;

([1]) Nõukogu 31. märtsi 1992. aasta direktiiv 92/23/EMÜ mootorsõidukite ja nende haagiste rehvide ja nende paigaldamise kohta (EÜT L 129, 14.5.1992, lk 95).

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

xx) töökojakaart –

sõidumeerikukaart, mille liikmesriigi ametiasutus väljastab asjaomases liikmesriigis tunnustatud sõidumeerikutootja, paigaldaja, sõidukitootja või töökoja määratud töötajatele ja mis võimaldab kaardiomanikku tuvastada ning sõidumeerikut katsetada, kalibreerida, aktiveerida ja/või sellest andmeid alla laadida;

yy) adapter –

seade, mis edastab sõiduki kiirust ja/või läbitud vahemaad pidevalt kajastavat signaali ja mida ei kasutata sõltumatuks liikumise tuvastamiseks ning

— mis paigaldatakse ja mida kasutatakse ainult selliste M1- ja N1-kategooria sõidukite puhul (nagu on määratletud Euroopa Parlamendi ja nõukogu direktiivi 2007/46/EÜ ([1]) II lisa uusimas muudetud redaktsioonis), mis on kasutusele võetud pärast 1. maid 2006;

— mis paigaldatakse sõidukile juhul, kui tehniliselt ei ole võimalik paigaldada ühtki olemasolevat muud tüüpi liikumisandurit, mis muus osas vastab käesoleva lisa ja selle 1.–15. liite sätetele;

— mis paigaldatakse sõidukiseadme ning kiiruse-/vahemaaimpulsse genereeriva sisseehitatud anduri või muu liidestatud seadme vahele;

— mis sõidukiseadme seisukohalt toimib samal viisil nagu käesoleva lisa ja selle 1.–16. liite sätetele vastav sõidukiseadmega ühendatud liikumisandur.

Sellise adapteri kasutamine eespool kirjeldatud sõidukites võimaldab paigaldada ja nõuetekohaselt kasutada kõigile käesoleva lisa nõuetele vastavaid sõidukiseadmeid.

Selliste sõidukite puhul koosneb arukas sõidumeerik juhtmetest, adapterist ja sõidukiseadmest;

zz) andmeterviklus –

salvestatud andmete õigsus ja kooskõla, mida näitab asjaolu, et andmekirje kahe uuenduse vahel ei ole andmeid mingil viisil muudetud. Terviklus eeldab, et andmed on originaali täpne koopia, st neid ei ole sõidumeerikukaardile või eriotstarbelisse seadmesse kirjutamise või sealt lugemise või mis tahes sidekanali kaudu edastamise käigus rikutud;

aaa) andmekaitse –

üldised tehnilised meetmed, millega tagatakse Euroopa Parlamendi ja nõukogu direktiivis 95/46/EÜ ([2]) ning Euroopa Parlamendi ja nõukogu direktiivis 2002/58/EÜ ([3]) sätestatud põhimõtete nõuetekohane rakendamine;

bbb) aruka sõidumeeriku süsteem –

sõidumeerik, sõidumeerikukaardid ning kõik konstrueerimise, paigaldamise, kasutamise, katsetamise ja kontrollimise käigus otseselt või kaudselt vastastoimes olevad seadmed, näiteks kaardid, kaugsidelugeja ning mis tahes muud seadmed, mis on vajalikud andmete allalaadimiseks, analüüsimiseks, kalibreerimiseks, genereerimiseks, turvaelementide haldamiseks või kasutuselevõtuks jne;

ccc) kasutuselevõtu kuupäev –

36 kuud pärast Euroopa Parlamendi ja nõukogu määruse (EL) nr 165/2014 ([4]) artiklis 11 osutatud üksikasjalike sätete jõustumist.

([1]) Euroopa Parlamendi ja nõukogu 5. septembri 2007. aasta direktiiv 2007/46/EÜ, millega kehtestatakse raamistik mootorsõidukite ja nende haagiste ning selliste sõidukite jaoks mõeldud süsteemide, osade ja eraldi seadmestike kinnituse kohta (raamdirektiiv) (ELT L 263, 9.10.2007, lk 1).

([2]) Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (ELT L 281, 23.11.1995, lk 31).

([3]) Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (ELT L 201, 31.7.2002, lk 37).

([4]) Euroopa Parlamendi ja nõukogu 4. veebruari 2014. aasta määrus (EL) nr 165/2014 autovedudel kasutatavate sõidumeerikute kohta, millega tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 3821/85 autovedudel kasutatavate sõidumeerikute kohta ning muudetakse Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 561/2006, mis käsitleb teatavate autovedusid käsitlevate sotsiaalõigusnormide ühtlustamist EMPs kohaldatav tekst (ELT L 60, 28.2.2014, lk 1).

Nimetatud tähtaja möödumisel peavad esmakordselt registreeritavad sõidukid vastama järgmistele nõuetele:

— *neile on paigaldatud satelliitnavigatsioonisüsteemil põhineva positsioneerimisteenusega ühendatud sõidumeerik,*

— *need peavad suutma sõiduki liikumise ajal edastada sihipäraseks teeäärseks kontrolliks kasutatavaid andmeid pädevale kontrolliasutusele*

— *ja need võivad olla varustatud standarditud liidesega, mis võimaldab välisel seadmel töörežiimis kasutada sõidumeerikuga salvestatud või genereeritud andmeid;*

ddd) kaitseprofiil –

ühistele kriteeriumidele vastavas sertifitseerimisprotsessis kasutatav dokument, milles esitatakse rakendusest sõltumatu kirjeldus teabe kaitset tagavate turvanõuete kohta;

eee) GNSSi täpsus –

sõidumeeriku abil toimuva globaalsel satelliitnavigatsioonisüsteemil (GNSS) põhineva asukoha salvestamisega seotud horisontaalse täpsuse kadu (HDOP), milleks võetakse kasutatavate GNSSide puhul saadud HDOP väärtustest väikseim.

2. SÕIDUMEERIKU ÜLDOMADUSED JA FUNKTSIOONID

2.1. **Üldomadused**

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

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

1) Sõidumeerik koosneb juhtmetest, liikumisandurist ja sõidukiseadmest.

2) Liikumisanduri ja sõidukiseadme vaheline liides peab vastama 11. liites esitatud nõuetele.

3) Sõidukiseade peab olema ühendatud globaalse(te) satelliitnavigatsioonisüsteemi(de)ga, nagu on kirjeldatud 12. liites.

4) Sõidukiseade peab pidama sidet 14. liites kirjeldatud varajase avastamise kaugsidelugejaga.

5) Sõidukiseade võib sisaldada 13. liites kirjeldatud ITSi liidest.

Sõidukiseade võib olla täiendavate liideste ja/või valikulise ITSi liidese kaudu ühendatud muude seadmetega.

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

Sõidumeeriku kasutajad idendivad seadmes oma isiku sõidumeerikukaardi abil.

7) Sõidumeerik annab vastavalt kasutaja tüübile ja/või isikusamasusele valikulised õigused andmetele ja funktsioonidele juurdepääsuks.

Sõidumeerik registreerib ja salvestab andmed andmemällu, kaugsideseadmesse 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]), 12. juuli 2002. aasta direktiivile 2002/58/EÜ (milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris) ([2]) ning määruse (EL) nr 165/2014 artiklile 7.

2.2. **Funktsioonid**

8) Sõidumeerikuga tagatakse järgmised funktsioonid:

— kaartide sisestamise ja väljavõtmise seire,

— kiiruse, vahemaa ja asukoha mõõtmine,

— aja mõõtmine,

— juhi tegevuse seire,

— juhtimisstaatuse seire,

— juhi tegevuse käsitsi sissekandmine:

  — tööpäeva algus- ja/või lõppkoha sissekandmine,

  — juhi tegevuse sissekandmine,

  — eritingimuste sissekandmine,

— ettevõttelukkude haldamine,

— kontrollitegevuse seire,

— sündmuste ja/või vigade tuvastamine,

— sisseehitatud ja enesekontrollitestid,

— andmemälust lugemine,

— andmete registreerimine ja säilitamine mälus,

— sõidumeerikukaartidelt lugemine,

— registreerimine ja säilitamine sõidumeerikukaartidel,

— kuvamine,

— trükkimine,

— hoiatamine,

— andmete allalaadimine välisandmekandjale,

— kaugside pidamine sihipäraseks teeäärseks kontrolliks,

— andmete väljastamine lisaseadmetele,

— kalibreerimine,

— teeäärne kalibreerimiskontroll,

— aja korrigeerimine.

([1]) EÜT L 281, 23.11.1995, lk 31.
([2]) EÜT L 201, 31.7.2002, lk 37.

2.3. **Kasutusrežiimid**

9) Sõidumeerikul on neli kasutusrežiimi:

— töörežiim,

— kontrollirežiim,

— kalibreerimisrežiim,

— ettevõtterežiim.

10) Vastavalt kaardiliidesesse sisestatud kehtivale sõidumeerikukaardile peab sõidumeerik lülituma allpool nimetatud kasutusrežiimi. Kui sisestatud kaart on kehtiv, ei ole sõidumeerikukaardi põlvkond kasutusrežiimi kindlakstegemisel oluline. Teise põlvkonna sõidukiseadmesse sisestatud esimese põlvkonna töökojakaart loetakse alati kehtetuks.

Kasutusrežiim		Juhikaardi pesa				
		Kaart puudub	Juhikaart	Kontrollikaart	Töökojakaart	Ettevõttekaart
Kaasjuhikaardi pesa	Kaart puudub	Töörežiim	Töörežiim	Kontrollirežiim	Kalibreerimisrežiim	Ettevõtterežiim
	Juhikaart	Töörežiim	Töörežiim	Kontrollirežiim	Kalibreerimisrežiim	Ettevõtterežiim
	Kontrollikaart	Kontrollirežiim	Kontrollirežiim	Kontrollirežiim - (*)	Töörežiim	Töörežiim
	Töökojakaart	Kalibreerimisrežiim	Kalibreerimisrežiim	Töörežiim	Kalibreerimisrežiim (*)	Töörežiim
	Ettevõttekaart	Ettevõtterežiim	Ettevõtterežiim	Töörežiim	Töörežiim	Ettevõtterežiim (*)

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

11) Sõidumeerik eirab sisestatud kehtetuid kaarte, ent kehtivusaja ületanud kaartidel olevate andmete kuvamine, trükkimine ja allalaadimine on võimalik.

12) Kõik punktis 2.2 loetletud funktsioonid peavad toimima igas kasutusrežiimis, välja arvatud järgmised erandid:

— kalibreerimisfunktsioon on võimalik ainult kalibreerimisrežiimis,

— teeäärse kalibreerimiskontrolli funktsioon on võimalik ainult kontrollirežiimis,

— ettevõttelukkude haldamise funktsioon on võimalik ainult ettevõtterežiimis,

— kontrollitegevuse seire funktsioon toimib ainult kontrollirežiimis,

— allalaadimisfunktsioon ei ole võimalik töörežiimis, välja arvatud nõudes 193 sätestatud juhtudel ning välja arvatud juhul, kui andmeid laaditakse alla juhikaardilt ja sõidukiseadmesse ei ole sisestatud ühtki teist kaarti.

13) Sõidumeerik võib väljastada kuvarile, printerisse või välisliidese kaudu mis tahes andmeid, välja arvatud järgmised erandid:

— töörežiimis jäetakse sisestatud sõidumeerikukaardile mittevastavad isikuandmed (perekonnanimi ja eesnimi või eesnimed) esitamata ja sisestatud sõidumeerikukaardile mittevastava kaardi number jäetakse osaliselt esitamata (esitamata jäetakse iga teine tähemärk vasakult paremale),

— ettevõtterežiimis saab juhiga seotud andmeid (nõuded 102, 105 ja 108) esitada ainult aegade kohta, mida ükski ettevõte ei ole lukustanud (see on määratud ettevõttekaardi numbri esimese 13 kohaga),

— kui sõidumeerikus kaarti ei ole, saab juhiga seotud andmeid esitada ainult jooksva ning kaheksa viimase kalendripäeva kohta,

— sõidukiseadmest pärit isikuandmeid esitatakse sõidukiseadme ITSi liidese kaudu üksnes juhul, kui selle kohta on olemas selle juhi kontrollitud nõusolek, kellega andmed on seotud,

— sõidukiseadme kasutusaeg tavakasutuses on 15 aastat alates sõidukiseadme sertifikaadi väljaandmise kuupäevast, kuid seejärel võib sõidukiseadet kasutada veel kolme kuu jooksul üksnes andmete allalaadimise eesmärgil.

2.4. **Turvalisus**

Süsteemi turbe-eesmärk on kaitsta andmemälu, et takistada lubamatut juurdepääsu andmetele ja nendega manipuleerimist ning avastada kõik katsed seda teha, kaitsta liikumisanduri ja sõidukiseadme vahel vahetatud andmete terviklust ja autentsust, kaitsta sõidumeeriku ja sõidumeerikukaartide vahel vahetatavate andmete terviklust ja autentsust, kaitsta sõidumeeriku ja GNSSi välisseadme vahel vahetatavate andmete terviklust ja autentsust, kaitsta kontrolli eesmärgil kaugside teel toimuva varajase avastamise käigus vahetatavate andmete konfidentsiaalsust, terviklust ja autentsust ning tõendada allalaaditud andmete terviklust ja autentsust.

14) Süsteemi turvalisuse saavutamiseks peavad järgmised osad vastama turvanõuetele, mida on vastavalt 10. liitele kirjeldatud nende kaitseprofiilis:

— sõidukiseade,

— sõidumeerikukaart,

— liikumisandur,

— GNSSi välisseade (asjaomane profiil on vajalik ja kohaldatav üksnes GNSSi välisseadme olemasolu korral).

3. SÕIDUMEERIKU KONSTRUKTSIOONI- JA FUNKTSIONAALSED NÕUDED

3.1. **Kaartide sisestamise ja väljavõtmise seire**

15) Sõidumeerik seirab kaardiliideseid, et tuvastada kaartide sisestamine ja väljavõtmine.

16) Kaardi sisestamisel kontrollib sõidumeerik, kas sisestatud kaart on kehtiv sõidumeerikukaart ning kui on, idendib kaardi tüübi ja kaardi põlvkonna.

Kui sama kaardinumbri, aga suurema pikendusindeksiga kaart on juba sõidumeerikusse sisestatud, tunnistatakse kaart kehtetuks.

Kui sama kaardinumbri ja pikendusindeksiga, aga suurema asendusindeksiga kaart on juba sõidumeerikusse sisestatud, tunnistatakse kaart kehtetuks.

17) Sõidumeerik loeb esimese põlvkonna sõidumeerikukaardi kehtetuks pärast seda, kui esimese põlvkonna sõidumeerikukaardi kasutamise võimalus on töökojas tõkestatud kooskõlas 15. liitega (nõue MIG_003).

18) Teise põlvkonna sõidumeerikusse sisestatud esimese põlvkonna töökojakaart loetakse alati kehtetuks.

19) Sõidumeerik konstrueeritakse nii, et kui sõidumeerikukaart sisestatakse nõuetekohaselt kaardiliidesesse, lukustatakse see kindlasse asendisse.

20) Sõidumeerikukaardi saab välja võtta ainult siis, kui sõiduk on peatunud ja asjaomased andmed on kaardile salvestatud. Kaardi väljavõtmiseks on vaja kasutajapoolset konkreetset tegevust.

3.2. **Kiiruse, asukoha ja vahemaa mõõtmine**

21) Põhilised kiiruse ja vahemaa mõõtmised tehakse liikumisanduriga (mis võib olla sisse ehitatud adapterisse).

22) Funktsioon mõõdab pidevalt vahemaad ning peab suutma esitada läbisõidumõõdiku näidu, mis vastab sõiduki läbitud kogu vahemaale, kasutades liikumisanduri edastatud impulsse.

23) Funktsioon mõõdab pidevalt sõiduki kiirust ja peab suutma esitada selle näidu, kasutades liikumisanduri edastatud impulsse.

24) 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.

25) Käesoleva määruse sätetele vastava sõidumeerikuga varustatud sõidukitesse paigaldatud kiiruse (kiirusmõõdik) ja kogu läbitud vahemaa (läbisõidumõõdik) kuvamisseadmed peavad vastama käesolevas lisas (vt punktid 3.2.1 ja 3.2.2) sätestatud suurima lubatud hälbe nõuetele.

26) Selleks et avastada liikumisandmetega manipuleerimine, toetatakse liikumisandurist saadud teavet GNSSi vastuvõtjast ning variandina liikumisandurist sõltumatust allikast saadud sõiduki liikumist käsitleva teabega.

27) Funktsioon mõõdab sõiduki asukohta, et võimaldada järgmiste andmete automaatset registreerimist:

— juhi ja/või kaasjuhi tööpäeva alguskoht;

— juhi iga kolme tunni pideva juhtimisaja täitumise asukohad;

— juhi ja/või kaasjuhi tööpäeva lõppkoht.

3.2.1. *Läbitud vahemaa mõõtmine*

28) Läbitud vahemaad võib mõõta kas

— nii edaspidi kui tagurpidi sõitmise summana või

— ainult edaspidi sõitmisena.

29) Sõidumeerik mõõdab vahemaad vahemikus 0 kuni 9 999 999,9 km.

30) Vahemaad mõõdetakse järgmise hälbe piires (vahemaa vähemalt 1 000 m):

— ± 1 % enne paigaldamist,

— ± 2 % paigaldamisel ja perioodilise kontrolli ajal,

— ± 4 % kasutamisel.

31) Mõõdetud vahemaa puhul on eristusvõime vähemalt 0,1 km.

3.2.2. *Kiiruse mõõtmine*

32) Sõidumeerik mõõdab kiirust vahemikus 0 kuni 220 km/h.

33) Et tagada kasutamisel kuvatava kiiruse jäämine suurima lubatud hälbe ± 6 km/h piiresse ning võttes arvesse

— sisendandmete erinevustest (rehvierinevused, …) tingitud hälvet ± 2 km/h,

— paigaldamisel või perioodilise kontrolli käigus tehtud mõõtmiste hälvet ± 1 km/h,

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

Märkus: andmesalvestusega seotud eristusvõimest tulenevalt on sõidumeeriku salvestatud kiiruse lisahälve ± 0,5 km/h.

34) Kiirust mõõdetakse korrektselt tavahälbe raames kahe sekundi jooksul alates kiiruse muutumise lõpphetkest, kui kiirus on muutunud kiirusega kuni 2 m/s^2.

35) Kiiruse mõõtmisel on eristusvõime vähemalt 1 km/h.

3.2.3. *Asukoha mõõtmine*

36) Sõidumeerik mõõdab GNSSi vastuvõtja abil sõiduki absoluutset asukohta.

37) Absoluutset asukohta mõõdetakse geograafilistes laius- ja pikkuskraadides ja -minutites eristusvõimega 1/10 minutit.

3.3. **Aja mõõtmine**

38) Aja mõõtmise funktsioon mõõdab aega pidevalt ning esitab digitaalselt kuupäeva ja kellaaja koordineeritud maailmaajas.

39) Koordineeritud maailmaajas kuupäeva ja kellaaega kasutatakse andmete dateerimiseks sõidumeerikus (salvestused, andmevahetus) ja kõikides 4. liites „Väljatrükid“ täpsustatud väljatrükkides.

40) Kohaliku aja näitamiseks peab saama kuvatava aja nihet muuta poole tunni kaupa. Kuvatavat aega võib muuta üksnes pooltundide lisamise või mahaarvamise kaudu.

41) Tüübikinnitustingimustele vastav ajanihe ei tohi ületada ± 2 sekundit päevas ilma aja korrigeerimiseta.

42) Mõõdetud aja puhul peab eristusvõime olema vähemalt 1 sekund.

43) Tüübikinnitustingimustes ei tohi aja mõõtmist mõjutada alla 12 kuu pikkune välise toitevoolu katkestus.

3.4. **Juhi tegevuse seire**

44) Funktsioon seirab pidevalt ja eraldi ühe juhi ja ühe kaasjuhi tegevust.

45) Juhi tegevus on JUHTIMINE, TÖÖ, VALMISOLEK ja PUHKEPAUS/PUHKUS.

46) Juht ja/või kaasjuht peavad saama käsitsi valida TÖÖ, VALMISOLEKU ja PUHKEPAUSI/PUHKUSE.

47) Kui sõiduk liigub, valitakse juhi tarvis automaatselt JUHTIMINE ja kaasjuhi tarvis valitakse automaatselt VALMISOLEK.

48) Kui sõiduk peatub, valitakse juhi tarvis automaatselt TÖÖ.

49) Kui sõiduk peatus ja toimus automaatne üleminek TÖÖLE, loetakse sellele järgneva 120 sekundi jooksul toimuvat tegevuse esimest muudatust PUHKUSEKS või VALMISOLEKUKS sõiduki seisaku ajal toimunuks (sellega võib kaasneda TÖÖLE ülemineku tühistamine).

50) See funktsioon väljastab salvestusfunktsioonidele tegevuse muudatusi ühe minuti täpsusega.

51) Kui mis tahes JUHTIMISE tegevus on toimunud nii kalendriminutile vahetult eelneva kui ka järgneva minuti jooksul, läheb terve minut JUHTIMISE alla.

52) Kui kalendriminutit ei saa nõude 051 alusel lugeda JUHTIMISE minutiks, läheb kogu minut selles minutis toimunud pikima kestva tegevuse alla (võrdse pikkusega tegevuste puhul arvestatakse viimast tegevust).

53) Funktsioon jälgib püsivalt ka pidevat juhtimisaega ja juhi kumulatiivset puhkepauside aega.

3.5. **Juhtimisstaatuse seire**

54) Funktsioon seirab püsivalt ja automaatselt juhtimisstaatust.

55) Kui meerikusse sisestatakse kaks kehtivat juhikaarti, valitakse automaatselt juhtimisstaatus MEESKOND, igal muul juhul valitakse juhtimisstaatus ÜKSI.

3.6. **Juhtide sissekanded**

3.6.1. *Sissekanne tööpäeva algus- ja/või lõppkoha kohta*

56) Funktsioon võimaldab juhil ja/või kaasjuhil sisestada oma tööpäeva algus- ja/või lõppkohad.

57) Kohad on määratletud riikidena ja vajaduse korral ka piirkondadena, mis sisestatakse või kinnitatakse käsitsi.

58) Juhikaardi väljavõtmisel soovitab sõidumeerik (kaas)juhil sisestada „tööpäeva lõppkoha“.

59) Seejärel sisestab juht sõiduki asukoha sel hetkel ning seda käsitatakse ajutise sissekandena.

60) Tööpäeva algus- ja/või lõppkohti saab sisestada menüükäskude abil. Kui kalendriminuti jooksul tehakse rohkem kui üks selline sissekanne, salvestatakse püsivalt üksnes selle aja jooksul viimasena sisestud alguskoht ja viimasena sisestatud lõppkoht.

3.6.2. *Käsitsi tehtavad sissekanded juhi tegevuse kohta ja juhi nõusolek ITSiga liidestamiseks*

61) Juhikaardi (või töökojakaardi) sisestamisel ja üksnes sel ajal on võimalik sisestada sõidumeerikusse tegevusi käsitsi. Tegevuste käsitsi sisestamisel kasutatakse sõidukiseadme seadistusele vastava ajavööndi (reguleeritud koordineeritud maailmaaeg) kohalikku kellaaega ja kuupäeva.

Juhi- või töökojakaardi sisestamisel meenutatakse kaardi omanikule,

— mis kuupäeval ja ajal ta viimati oma kaardi välja võttis ja

— variandina seda, milline on sõidukiseadmes seadistatud kohalik aeg.

Sõidukiseadme jaoks tundmatu juhikaardi või töökojakaardi esmakordsel sisestamisel küsitakse kaardi omanikult nõusolekut sõidumeerikuga seotud isikuandmete edastamiseks valikulise ITSi liidese kaudu.

Kui juhikaart (töökojakaart) on sisestatud, saab juhi (töökoja) nõusoleku küsimise menüükäskudega igal ajal sisse või välja lülitada.

Tegevuste sisestamisel kehtivad järgmised piirangud:

— tegevuse liik peab olema TÖÖ, VALMISOLEK või PUHKEPAUS/PUHKUS;

— iga tegevuse algus- ja lõpuaeg peab jääma kaardi eelmise väljavõtmise ja praeguse sisestamise vahelisse perioodi;

— tegevused ei tohi omavahel ajaliselt kattuda.

Vajaduse korral on sissekandeid võimalik käsitsi teha varem kasutamata juhikaardi (või töökojakaardi) esimest korda sisestamisel.

Tegevuste käsitsi sisestamise menetlus sisaldab nii palju järjestikusi samme, kui on vaja tegevuse liigi ning algus- ja lõpuaja kindlaksmääramiseks. Kaardi eelmise väljavõtmise ja praeguse sisestamise vahelise perioodi mis tahes hetkel on kaardi omanikul võimalik tegevust mitte deklareerida.

Kaardi sisestamisega seotud sissekannete ajal ja juhul, kui see on vajalik, on kaardi omanikul võimalik esitada:

— eelmise tööpäeva lõppkoht koos asjakohase ajaga (sellega kirjutatakse üle kaardi eelmise väljavõtmise ajal tehtud sissekanne),

— praeguse tööpäeva alguskoht koos asjakohase ajaga.

Kui kaardi omanik ei sisesta kaardi sisestamisega seotud käsitsi sissekannete tegemise ajal tööpäeva alguse või lõpu kohta, siis käsitatakse seda kinnitusena, et tema vastavas tööperioodis ei ole pärast viimast kaardi väljavõtmist muutusi toimunud. Järgmisel korral, kui sisestatakse eelmise tööpäeva lõppkoht, kirjutatakse üle kaardi eelmise väljavõtmise ajal tehtud ajutine sissekanne.

Koha sisestamise korral registreeritakse see asjakohasel sõidumeerikukaardil.

Käsitsi sisestamine katkestatakse, kui:

— kaart võetakse välja või

— kui sõiduk liigub ja kaart on juhikaardi pesas.

Lubatud on lisakatkestused, nt seansi lõpetamine, kui kasutaja on olnud teatava aja jooksul tegevusetu. Kui käsitsi sisestamine katkestatakse, kinnitab sõidumeerik kõik juba tehtud terviklikud kohta ja tegevust käsitlevad sissekanded (üheselt mõistetav koht ja aeg või tegevuse liik ning algus- ja lõpuaeg).

Kui teine juhi- või töökojakaart sisestatakse ajal, kui tegevuse käsitsi sisestamine eelmisele sisestatud kaardile ei ole veel lõppenud, lubatakse lõpetada eelmisele kaardile käsitsi tehtavad sissekanded, enne kui alustatakse käsitsi sisestamist teisele kaardile.

Kaardi omanikul on võimalik teha käsitsi sissekandeid, järgides järgmist minimaalset menetlust:

— Kronoloogilises järjestuses sisestatakse käsitsi tegevused, mis on tehtud kaardi eelmise väljavõtmise ja praeguse sisestamise vahele jääval ajavahemikul.

— Esimese tegevuse algusajaks määratakse kaardi väljavõtmise aeg. Iga järgmise sissekande puhul määratakse algusaeg automaatselt, et see järgneks vahetult eelmise sissekande lõpuajale. Iga tegevuse puhul valitakse liik ja lõpuaeg.

Menetlus lõpeb, kui käsitsi sisestatud tegevuse lõpuaeg vastab kaardi sisestamise ajale. Sõidumeerik võib seejärel valikuliselt lubada kaardi omanikul käsitsi sisestatud tegevusi muuta, kuni andmed spetsiaalse käsu valimisega kinnitatakse. Pärast seda on mis tahes muudatuste tegemine keelatud.

3.6.3. *Eritingimuste sisestamine*

62) Sõidumeerik võimaldab juhil sisestada reaalajas kaks järgmist eritingimust:

— „SÕIDUMEERIK MITTEVAJALIK“ (algus, lõpp),

— „PARVLAEVA-/RONGISÕIT“ (algus, lõpp).

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

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

Avatud tingimus „SÕIDUMEERIK MITTEVAJALIK“ välistab järgmised sündmused ja hoiatused:

— vajaliku kaardita juhtimine,

— pideva juhtimisajaga seotud hoiatused.

„PARVLAEVA-/RONGISÕIDU“ alguse tunnus määratakse enne, kui sõiduki mootor parvlaeval/rongil välja lülitatakse.

Avatud tingimus „PARVLAEVA-/RONGISÕIT“ peab lõppema mis tahes järgmise olukorra tekkimisel:

— juht lõpetab tingimuse „PARVLAEVA-/RONGISÕIT“ KÄSITSI;

— juht võtab oma kaardi välja;

Avatud tingimus „PARVLAEVA-/RONGISÕIT“ lõpeb siis, kui see ei ole vastavalt määruses (EÜ) nr 561/2006 esitatud reeglitele enam kehtiv.

3.7. **Ettevõttelukkude haldamine**

63) Funktsioon võimaldab ettevõtte paigaldatud lukke hallata, et ettevõtterežiimis oleks ligipääs andmetele ainult sellel ettevõttel.

64) Ettevõttelukk koosneb alguse kuupäevast/ajast (lukustamine) ja lõpu kuupäevast/ajast (luku avamine), mis on seotud ettevõtte identimisega ettevõttekaardi numbri alusel (lukustamisel).

65) Lukustada ja lukku avada saab ainult reaalajas.

66) Lukku saab avada ainult see ettevõte, kelle lukk on peal (idenditud ettevõttekaardi numbri esimese 13 koha alusel), või

67) on luku avamine automaatne, kui teine ettevõte paneb oma luku peale.

68) Juhul kui ettevõte paneb luku peale ja kui eelmine lukk oli sama ettevõtte oma, eeldatakse, et eelmine lukk ei ole avatud ja on ikka veel peal.

3.8. **Kontrollitegevuse seire**

69) Funktsioon seirab kontrollirežiimis tehtud KUVAMIST, TRÜKKIMIST, sõidukiseadmest ja kaardilt ALLA LAADIMIST ning TEEÄÄRSET KALIBREERIMISKONTROLLI.

70) Funktsioon seirab kontrollirežiimis ka KIIRUSE ÜLETAMISE KONTROLLI. Kiiruse ületamise kontroll loetakse toimunuks, kui kontrollirežiimis on printerile või kuvarile saadetud väljatrükk „kiiruse ületamine“ või kui „sündmuste ja vigade“ andmed on sõidukiseadme andmemälust alla laaditud.

3.9. **Sündmuste ja/või vigade avastamine**

71) Funktsiooniga tuvastatakse järgmised sündmused ja/või vead.

3.9.1. *Sündmus „kehtetu kaardi sisestamine“*

72) Sündmus käivitub mis tahes kehtetu kaardi sisestamisel, juba vahetatud juhikaardi sisestamisel ja/või sisestatud kehtiva kaardi kehtivusaja lõppemisel.

3.9.2. *Sündmus „kaardikonflikt“*

73) Sündmus käivitub siis, kui tekib mis tahes kehtivate kaartide kombinatsioon, mida järgmises tabelis tähistab X.

Kaardikonflikt		Juhikaardi pesa				
		Kaart puudub	Juhikaart	Kontrollikaart	Töökojakaart	Ettevõttekaart
Kaasjuhikaardi pesa	Kaart puudub					
	Juhikaart				X	
	Kontrollikaart			X	X	X
	Töökojakaart		X	X	X	X
	Ettevõttekaart			X	X	X

3.9.3. *Sündmus „aja kattumine“*

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

3.9.4. *Sündmus „vajaliku kaardita juhtimine“*

75) Sündmus käivitub järgmises tabelis X-ga tähistatud mis tahes kehtivate sõidumeerikukaartide kombinatsiooni puhul, kui juhi tegevus muutub JUHTIMISEKS või kui muudetakse kasutusrežiimi sel ajal, kui juhi tegevus on JUHTIMINE.

Vajaliku kaardita juhtimine		Juhikaardi pesa				
		Kaart puudub (või kehtetu kaart)	Juhikaart	Kontrollikaart	Töökojakaart	Ettevõttekaart
Kaasjuhikaardi pesa	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

3.9.5. *Sündmus „kaardi sisestamine juhtimise ajal“*

76) Sündmus käivitub sõidumeerikukaardi sisestamisel mis tahes pesasse, kui juhi tegevus on JUHTIMINE.

3.9.6. *Sündmus „viimane kaardiseanss nõuetekohaselt sulgemata“*

77) Sündmus käivitub siis, kui kaardi sisestamisel tuvastab sõidumeerik, et vaatamata punkti 3.1 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.

3.9.7. *Sündmus „kiiruse ületamine“*

78) Sündmus käivitub kõigil lubatava kiiruse ületamise juhtudel.

3.9.8. *Sündmus „voolukatkestus“*

79) Sündmus käivitub liikumisanduri ja/või sõidukiseadme toitevoolu iga katkestuse korral, mis kestab kauem kui 200 millisekundit, välja arvatud kalibreerimis- ja kontrollirežiimis. Katkestusläve määratleb tootja. Sündmust ei käivita pingelangus toiteallikas seoses sõiduki mootori käivitamisega.

3.9.9. *Sündmus „kaugsideseadmega side pidamise viga“*

80) Sündmus käivitub juhul, kui kaugsideseade ei kinnita sõidukiseadmest saadetud kaugsideandmete vastuvõtmist rohkem kui kolmel saatmiskatsel, **välja arvatud kalibreerimisrežiimis**.

3.9.10. *Sündmus „asukohateabe mittelaekumine GNSSi vastuvõtjast“*

81) Sündmus käivitub juhul, kui rohkem kui kolme kumulatiivse juhtimisaja tunni jooksul puudub (sisemisest või välisest) GNSSi vastuvõtjast saadav asukohateave, **välja arvatud kalibreerimisrežiimis**.

3.9.11. *Sündmus „GNSSi välisseadmega side pidamise viga“*

82) Sündmus käivitub juhul, kui sõiduki liikumise ajal katkeb GNSSi välisseadme ja sõidukiseadme vaheline side rohkem kui 20 järjestikuseks minutiks, **välja arvatud kalibreerimisrežiimis**.

3.9.12. *Sündmus „liikumisandmete viga“*

83) Sündmus käivitub normaalse andmevahetuse katkemisel liikumisanduri ja sõidukiseadme vahel ja/või liikumisanduri ja sõidukiseadme vahelise andmevahetuse ajal tekkiva andmete tervikluse või andmete autentsuse vea puhul, **välja arvatud kalibreerimisrežiimis**.

3.9.13. *Sündmus „vastuolu sõiduki liikumisandmetes“*

84) Sündmus käivitub juhul, kui liikumisanduri järgi arvutatud liikumisandmed on vastuolus sisemise GNSSi vastuvõtja või GNSSi välisseadme või variandina vastavalt 12. liitele muude sõltumatute allikate järgi arvutatud liikumisandmetega, **välja arvatud kalibreerimisrežiimis**. Sündmus ei käivitu parvlaeva-/rongisõidu ajal, tingimuse SÕIDUMEERIK MITTEVAJALIK korral ega juhul, kui GNSSi vastuvõtjalt asukohateavet ei laeku.

3.9.14. *Sündmus „turvalisuse rikkumise katse“*

85) Sündmus käivitub mis tahes muu sündmuse korral, mis mõjutab liikumisanduri ja/või sõidukiseadme ja/või GNSSi välisseadme 10. liite nõuete kohast turvalisust, välja arvatud kalibreerimisrežiimis.

3.9.15. *Sündmus „ajakonflikt“*

86) Sündmus käivitub juhul, kui sõidukiseade tuvastab sõidukiseadme ajamõõtmisfunktsiooni ja GNSSi vastuvõtjast saadud ajateabe vahel rohkem kui ühe minuti suuruse lahknevuse, välja arvatud kalibreerimisrežiimis. Sündmus registreeritakse koos sõidukiseadme sisemise kella väärtusega ning sellega kaasneb automaatne aja korrigeerimine. Kui ajakonflikti sündmus on käivitunud, ei käivita sõidukiseade järgmise 12 tunni jooksul muid ajakonflikti sündmusi. Sündmus ei käivitu juhul, kui GNSSi vastuvõtja ei ole viimase 30 päeva jooksul tuvastanud kehtivat GNSSi signaali. Kui GNSSi vastuvõtjalt saadav asukohateave jälle kättesaadavaks muutub, toimub automaatne aja korrigeerimine.

3.9.16. *Viga „kaart“*

87) Viga käivitub siis, kui sõidumeerikukaardil esineb töötamise ajal tõrkeid.

3.9.17. *Viga „sõidumeerik“*

88) Viga käivitub iga järgneva tõrke puhul, välja arvatud kalibreerimisrežiimis:

— sõidukiseadme sisetõrge,

— printeri tõrge,

— kuvari tõrge,

— allalaadimise tõrge,

— anduri tõrge,

— GNSSi vastuvõtja või GNSSi välisseadme tõrge,

— kaugsideseadme tõrge.

3.10. **Sisseehitatud ja enesekontrollitestid**

89) Sõidumeerik tuvastab ise vigu enesekontrollitestide ja sisseehitatud testide abil järgmise tabeli kohaselt.

Testitav alakoost	Enesekontrollitest	Sisseehitatud test
Tarkvara		Terviklus
Andmemälu	Juurdepääs	Juurdepääs, andmeterviklus
Kaardiliidese seadmed	Juurdepääs	Juurdepääs
Klaviatuur		Käsitsi kontroll
Printer	(tootja otsustada)	Väljatrükk
Kuvar		Visuaalne kontroll
Allalaadimine (viiakse läbi ainult allalaadimise ajal)	Nõuetekohane toimimine	
Andur	Nõuetekohane toimimine	Nõuetekohane toimimine
Kaugsideseade	Nõuetekohane toimimine	Nõuetekohane toimimine
GNSSi seade	Nõuetekohane toimimine	Nõuetekohane toimimine

3.11. **Andmemälust lugemine**

90) Sõidumeerik suudab lugeda kõiki andmeid, mis on tema andmemällu salvestatud.

3.12. **Andmete registreerimine ja salvestamine andmemällu**

Käesoleva lõike kohaldamisel:

— 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 tegevuse muudatusega. Seetõttu hõlmab 365 päeva vähemalt 2 190 (kaas)juhti, 2 190 kaardi sisestamis- ja väljavõtmistsüklit ja 93 440 tegevuse muudatust;

— on keskmine asukohtade arv päeva kohta määratletud vähemalt kuue tööpäeva alguskohaga, kuue kohaga, kus juhil täitub kolm tundi pidevat juhtimisaega, ning kuue tööpäeva lõppkohaga, nii et 365 päeva hõlmab vähemalt 6 570 asukohta;

— ajad salvestatakse täpsusega üks minut, kui ei ole määratletud teisiti;

— läbisõidumõõdiku näidud salvestatakse täpsusega üks kilomeeter;

— kiirused salvestatakse täpsusega 1 km/h;

— asukohad (laiused ja pikkused) salvestatakse kraadides ja minutites täpsusega 1/10 minutit, arvestades seotud GNSSi täpsust ja andmehõive aega.

91) Tüübikinnitustingimuste kohaselt ei tohi andmemällu salvestatud andmeid mõjutada alla 12 kuu pikkune välise toitevoolu katkestus. Lisaks ei tohi 14. liites määratletud välisesse kaugsideseadmesse salvestatud andmeid mõjutada alla 28 päeva pikkune toitevoolu katkestus.

92) Sõidumeerik peab suutma registreerida ja salvestada oma andmemällu otseselt või kaudselt allpool nimetatud andmeid.

3.12.1. *Seadme identimisandmed*

3.12.1.1. Sõidukiseadme identimisandmed

93) Sõidumeerik suudab salvestada oma andmemällu järgmisi sõidukiseadme identimisandmeid:

— tootja nimi,

— tootja aadress,

— osa number,

— seerianumber,

— sõidukiseadme põlvkond,

— suutlikkus kasutada esimese põlvkonna sõidumeerikukaarte,

— tarkvaraversiooni number,

— tarkvaraversiooni installeerimise kuupäev,

— seadme tootmisaasta,

— tüübikinnitusnumber.

94) Sõidukiseadme tootja registreerib ja salvestab sõidukiseadme identimisandmed üks kord ja alatiseks, välja arvatud tarkvaraga seotud andmed ja tüübikinnitusnumber, mida võib muuta tarkvara ajakohastamisel, ning teave esimese põlvkonna sõidumeerikukaartide kasutamise suutlikkuse kohta.

3.12.1.2. Liikumisanduri identimisandmed

95) Liikumisandur suudab salvestada oma mällu järgmisi identimisandmed:

— tootja nimi,

— seerianumber,

— tüübikinnitusnumber.

— sisseehitatud turvakomponendi identifikaator (nt sisekiibi/protsessori osa number),

— operatsioonisüsteemi identifikaator (nt tarkvaraversiooni number).

96) Liikumisanduri tootja registreerib ja salvestab liikumisanduri identimisandmed üks kord ja alatiseks liikumisandurisse.

97) Sõidukiseade suudab salvestada oma andmemällu järgmisi andmeid liikumisandurite 20 viimase ühendamise kohta (kui ühel kalendripäeval tehakse mitu ühendamist, salvestatakse mällu ainult selle päeva esimene ja viimane ühendamine).

Iga ühendamise kohta registreeritakse järgmised andmed:

— liikumisanduri identimisandmed:

— seerianumber,

— tüübikinnitusnumber;

— liikumisanduri ühendamisandmed:

— ühendamise kuupäev.

3.12.1.3. Globaalsete satelliitnavigatsioonisüsteemide identimisandmed

98) GNSSi välisseade suudab salvestada oma mällu järgmisi identimisandmed:

— tootja nimi,

— seerianumber,

— tüübikinnitusnumber.

— sisseehitatud turvakomponendi identifikaator (nt sisekiibi/protsessori osa number),

— operatsioonisüsteemi identifikaator (nt tarkvaraversiooni number).

99) GNSSi välisseadme tootja registreerib ja salvestab identimisandmed üks kord ja alatiseks GNSSi välisseadmesse.

100) Sõidukiseade suudab salvestada oma andmemällu järgmisi andmeid GNSSi välisseadmete 20 viimase ühendamise kohta (kui ühel kalendripäeval tehakse mitu ühendamist, salvestatakse mällu ainult selle päeva esimene ja viimane ühendamine).

Iga ühendamise kohta registreeritakse järgmised andmed:

— GNSSi välisseadme identimisandmed:

— seerianumber,

— tüübikinnitusnumber.

— GNSSi välisseadme ühendamisandmed:

— ühendamise kuupäev.

3.12.2. *Võtmed ja sertifikaadid*

101) Sõidumeerik suudab salvestada mitmeid krüptograafilisi võtmeid ja sertifikaate, mida on kirjeldatud 11. liite A ja B osas.

3.12.3. *Juhi- või töökojakaardi sisestamise ja väljavõtmise andmed*

102) 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 numbri, kaardi välja andnud liikmesriigi ja kaardi kehtivusaja lõpu, nagu need on kaardile salvestatud,

— kaardi põlvkonna,

— sisestamise kuupäeva ja aja,

— sõiduki läbisõidumeeriku näidu kaardi sisestamise ajal,

— pesa, 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:

— VRN ja sõiduki registreerinud liikmesriik,

— sõidukiseadme põlvkond (kui on teada),

— kaardi väljavõtmise kuupäev ja kellaaeg,

— kaardi väljavõtmise kuupäev ja kellaaeg, tunnuse, mis näitab, kas juht on tegevusi käsitsi sisestanud või mitte.

103) Need andmed peavad andmemälus säilima vähemalt 365 päeva.

104) Kui salvestusmaht on ammendatud, asendatakse vanimad andmed uute andmetega.

3.12.4. *Andmed juhi tegevuse kohta*

105) 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:

— juhtimisstaatuse (MEESKOND, ÜKSI),

— kaardipesa (JUHT, KAASJUHT),

— kaardi staatuse asjaomases pesas (SISESTATUD, SISESTAMATA),

— tegevuse (JUHTIMINE, VALMISOLEK, TÖÖ, PUHKEPAUS/PUHKUS),

— muudatuse kuupäeva ja aja.

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

Juhi käsitsi sisestatud andmeid tegevuse kohta andmemälus ei salvestata.

106) Andmemälus peavad andmed juhi tegevuse kohta säilima vähemalt 365 päeva.

107) Kui salvestusmaht on ammendatud, asendatakse vanimad andmed uute andmetega.

3.12.5. *Tööpäeva alguskoht, lõppkoht ja/või kolme järjestikuse sõidutunni täitumise koht*

108) Sõidumeerik registreerib ja salvestab oma andmemällu:

— juhi ja/või kaasjuhi tööpäeva alguskohad;

— juhi iga kolme tunni pideva juhtimisaja täitumise asukohad;

— juhi ja/või kaasjuhi tööpäeva lõppkohad.

109) Kui vastaval ajal ei ole GNSSi vastuvõtja teave sõiduki asukoha kohta saadaval, kasutab sõidumeerik viimast teadaolevat asukohta ning sellega seotud kuupäeva ja kellaaega.

110) Koos iga asukohaga registreerib ja salvestab sõidumeerik oma andmemällu:

— (kaas)juhi kaardi numbri ja kaardi välja andnud liikmesriigi,

— kaardi põlvkonna,

— sisestamise kuupäeva ja kellaaja,

— sissekande liik (algus, lõpp või kolm tundi pidevat juhtimisaega),

— vajaduse korral seotud GNSSi täpsuse, kuupäeva ja kellaaja,

— sõiduki läbisõidumõõdiku näidu.

111) Tööpäeva alguskohtade, lõppkohtade ja/või kolme järjestikuse sõidutunni täitumise kohtade andmed peavad andmemälus säilima vähemalt 365 päeva.

112) Kui salvestusmaht on ammendatud, asendatakse vanimad andmed uute andmetega.

3.12.6. *Läbisõidumõõdiku andmed*

113) Sõidumeerik registreerib oma andmemällu sõiduki läbisõidumõõdiku näidu ja vastava kuupäeva iga kalendripäeva kesköö.

114) Andmemälus peavad läbisõidumõõdiku kesköised näidud säilima vähemalt 365 kalendripäeva.

115) Kui salvestusmaht on ammendatud, asendatakse vanimad andmed uute andmetega.

3.12.7. *Üksikasjalikud andmed kiiruse kohta*

116) Sõidumeerik registreerib ja salvestab oma andmemällu sõiduki hetkekiiruse ning vastava kuupäeva ja aja kord sekundis vähemalt viimase 24 tunni jooksul, mil seda sõidukit on juhitud.

3.12.8. *Andmed sündmuste kohta*

Käesoleva lõigu kohaldamisel registreeritakse aega sekundilise täpsusega.

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

Sündmus	Salvestusreegel	Sündmuse kohta registreeritavad andmed
Kehtetu kaardi sisestamine	— 10 viimast sündmust	— sündmuse kuupäev ja kellaaeg, — sündmuse tekitanud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Kaardikonflikt	— 10 viimast sündmust	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — kummagi konflikti tekitanud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond
Vajaliku kaardita juhtimine	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval

Sündmus	Salvestusreegel	Sündmuse kohta registreeritavad andmed
Kaardi sisestamine juhtimise ajal	— viimane sündmus iga kümne viimase päeva kohta, mil sündmus toimus	— sündmuse kuupäev ja kellaaeg, — kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Viimane kaardiseanss nõuetekohaselt sulgemata	— 10 viimast sündmust	— kaardi sisestamise kuupäev ja kellaaeg, — kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — kaardilt loetud andmed viimase seansi kohta: — kaardi sisestamise kuupäev ja kellaaeg, — VRN, sõiduki registreerinud liikmesriik ja sõidukiseadme põlvkond
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 kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse ajal mõõdetud suurim kiirus, — sündmuse ajal mõõdetud kiiruste aritmeetiline keskmine, — juhikaardi tüüp, number, väljaandnud liikmesriik ja põlvkond (vajaduse korral), — samasuguste sündmuste arv sellel päeval
Voolukatkestus (2)	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Kaugsideseadmega side pidamise viga	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Asukohateabe mittelaekumine GNSSi vastuvõtjast	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval

Sündmus	Salvestusreegel	Sündmuse kohta registreeritavad andmed
Liikumisandmete viga	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Vastuolu sõiduki liikumisandmetes	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Turvalisuse rikkumise katse	— 10 viimast sündmust iga sündmuse tüübi kohta.	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg vajaduse korral, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — sündmuse tüüp
Ajakonflikt	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sõidumeeriku kuupäev ja kellaaeg, — GNSSi kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval

(1) Sõidumeerik registreerib ja salvestab oma andmemällu ka:

— viimase KIIRUSE ÜKLETAMISE 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.

3.12.9. *Andmed vigade kohta*

Käesoleva lõigu kohaldamisel registreeritakse aega sekundilise täpsusega.

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

Viga	Salvestusreegel	Vea kohta registreeritavad andmed
Kaardi viga	— 10 viimast juhikaardi viga	— vea alguse kuupäev ja kellaaeg, — vea lõpu kuupäev ja kellaaeg, — kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond,
Sõidumeeriku vead	— 10 viimast viga iga veatüübi kohta, — esimene viga pärast viimast kalibreerimist	— vea alguse kuupäev ja kellaaeg, — vea lõpu kuupäev ja kellaaeg, — vea tüüp, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond

3.12.10. *Kalibreerimisandmed*

119) Sõidumeerik registreerib ja salvestab oma andmemällu andmed, mis on seotud:

— teadaolevate kalibreerimisparameetritega aktiveerimise ajal,

— esimese kalibreerimisega pärast aktiveerimist,

— esimese kalibreerimisega selles sõidukis (määratakse kindlaks VINi alusel),

— 20 viimase kalibreerimisega (kui ühel kalendripäeval tehakse mitu kalibreerimist, salvestatakse mällu ainult selle päeva esimene ja viimane kalibreerimine).

120) Iga kalibreerimise kohta registreeritakse järgmised andmed:

— kalibreerimise eesmärk (aktiveerimine, esimene paigaldamine, paigaldamine, perioodiline kontroll),

— töökoja nimi ja aadress,

— töökojakaardi number, kaardi välja andnud liikmesriik ja kaardi aegumise kuupäev,

— sõiduki identimistunnus,

— ajakohastatud või kinnitatud parameetrid: sõidukit iseloomustav koefitsient, sõidumeeriku konstant, rehvide efektiivümbermõõt, rehvimõõt, kiiruspiiriku seadistus, läbisõidumõõdik (vana ja uus näit), kuupäev ja kellaaeg (vana ja uus näit),

— kõigi paigaldatud plommid liigid ja identifikaatorid.

121) Lisaks registreerib ja salvestab sõidumeerik oma andmemällu selle, kas ta suudab kasutada esimese põlvkonna sõidumeerikukaarte (mis on veel aktiivsed või mitte).

122) Liikumisandur registreerib ja salvestab oma mällu järgmised andmed liikumisanduri paigaldamise kohta:

— esimene sõidukiseadmega ühendamine (kuupäev, aeg, sõidukiseadme tüübikinnitusnumber, sõidukiseadme seerianumber),

— viimane sõidukiseadmega ühendamine (kuupäev, aeg, sõidukiseadme tüübikinnitusnumber, sõidukiseadme seerianumber).

123) GNSSi välisseade registreerib ja salvestab oma mällu järgmised andmed GNSSi välisseadme paigaldamise kohta:

— esimene sõidukiseadmega ühendamine (kuupäev, aeg, sõidukiseadme tüübikinnitusnumber, sõidukiseadme seerianumber),

— viimane sõidukiseadmega ühendamine (kuupäev, aeg, sõidukiseadme tüübikinnitusnumber, sõidukiseadme seerianumber).

3.12.11. *Andmed aja korrigeerimise kohta*

124) Sõidumeerik registreerib ja salvestab oma andmemällu andmed, mis on seotud kalibreerimisrežiimis väljaspool korralist kalibreerimist (mõiste f) tehtud aja korrigeerimistega:

— viimane aja korrigeerimine,

— viis suurimat aja korrigeerimist.

125) Aja iga korrigeerimise kohta registreeritakse järgmised andmed:

— kuupäev ja kellaaeg, vana näit,

— kuupäev ja kellaaeg, uus näit,

— töökoja nimi ja aadress,

— töökojakaardi number, kaardi välja andnud liikmesriik, kaardi põlvkond ja kaardi aegumise kuupäev.

3.12.12. *Andmed kontrollitegevuse kohta*

126) Sõidumeerik registreerib ja salvestab oma andmemällu andmed, mis on seotud viimase 20 kontrollitegevusega:

— kontrolli kuupäev ja kellaaeg,

— kontrollikaardi number, kaardi välja andnud liikmesriik ja kaardi põlvkond,

— kontrolli tüüp (kuvamine ja/või trükkimine ja/või sõidukiseadme andmete allalaadimine ja/või kaardi andmete allalaadimine ja/või teeäärne kalibreerimiskontroll).

127) Allalaadimise korral registreeritakse ka esimese ja viimase allalaadimise kuupäev.

3.12.13. *Andmed ettevõttelukkude kohta*

128) Sõidumeerik registreerib ja salvestab oma andmemällu viimase 255 ettevõtteluku kohta järgmised andmed:

— lukustamise kuupäev ja aeg,

— luku avamise kuupäev ja aeg,

— ettevõttekaardi number, kaardi välja andnud liikmesriik ja kaardi põlvkond,

— ettevõtte nimi ja aadress.

Andmed, mis on varem lukustatud lukuga, mis kõrvaldatakse mälust eespool sätestatud piiri tõttu, loetakse mittelukustatuks.

3.12.14. *Andmed allalaadimistegevuse kohta*

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

— allalaadimise kuupäev ja kellaaeg,

— ettevõtte- või töökojakaardi number, kaardi välja andnud liikmesriik ja kaardi põlvkond,

— ettevõtte või töökoja nimi.

3.12.15. *Andmed eritingimuste kohta*

130) Sõidumeerik registreerib oma andmemälus järgmised andmed, mis on seotud eritingimustega:

— sisestamise kuupäev ja kellaaeg,

— eritingimuse tüüp.

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

3.12.16. *Sõidumeerikukaardi andmed*

132) Sõidumeerik salvestab sõidukiseadmes kasutatud erinevate sõidumeerikukaartide kohta järgmised andmed:

— sõidumeerikukaardi number ja seerianumber,

— sõidumeerikukaardi tootja,

— sõidumeerikukaardi tüüp,

— sõidumeerikukaardi versioon.

133) Sõidumeerik peab suutma salvestada vähemalt 88 sellist kirjet.

3.13. **Sõidumeerikukaartidelt lugemine**

134) Sõidumeerik suudab lugeda esimese ja teise põlvkonna 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 juhtimisaega, kumulatiivset puhkepauside aega ning eelmise ja jooksva nädala kumulatiivset juhtimisaega,

— trükkimaks vajalikud väljatrükid, mis on seotud juhikaardile salvestatud andmetega,

— laadimaks alla juhikaardi andmed välisandmekandjatele.

Kõnealust nõuet kohaldatakse esimese põlvkonna sõidumeerikukaartide suhtes üksnes juhul, kui töökoda ei ole nende kasutamist tõkestanud.

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

3.14. **Registreerimine ja salvestamine sõidumeerikukaartidele**

3.14.1. *Registreerimine ja salvestamine esimese põlvkonna sõidumeerikukaartidele*

136) Kui töökoda ei ole esimese põlvkonna sõidumeerikukaartide kasutamist tõkestanud, registreerib ja salvestab sõidumeerik andmeid täpselt samuti, nagu seda teeks esimese põlvkonna sõidumeerik.

137) Sõidumeerik määrab „kaardiseansi andmed“ juhi- või töökojakaardil kohe pärast kaardi sisestamist.

138) Sõidumeerik ajakohastab kehtival juhi-, töökoja-, ettevõtte- ja/või kontrollikaardil salvestatud andmed kõigi vajalike andmetega, mis on seotud ajaga, mil kaart on sisestatud, ja kaardi omanikuga. Neile kaartidele salvestatavaid andmeid on kirjeldatud 4. peatükis.

139) Sõidumeerik ajakohastab andmed juhi tegevuse ja asukoha kohta (punktide 4.5.3.1.9 ja 4.5.3.1.11 kohaselt), mis on salvestatud kehtivatele juhi- ja/või töökojakaartidele, kaardi omaniku käsitsi sisestatud andmetega tegevuse ja asukoha kohta.

140) Esimese põlvkonna sõidumeerikute jaoks määratlemata sündmusi juhi- ja töökojakaartidele ei salvestata.

141) Sõidumeerikukaartide ajakohastamine toimub nii, et vajaduse korral ja võttes arvesse kaardi tegelikku salvestusmahtu asendatakse vanimad andmed uusimate andmetega.

142) Kirjutamisvea korral üritab sõidumeerik maksimaalselt kolm korda kasutada sama kirjutamiskäsku; kui see ikkagi ei õnnestu, tunnistatakse kaart vigaseks ja kehtetuks.

143) Enne juhikaardi vabastamist ja pärast kõigi asjakohaste andmete salvestamist kaardile lähtestab sõidumeerik „kaardiseansi andmed“.

3.14.2. *Registreerimine ja salvestamine teise põlvkonna sõidumeerikukaartidele*

144) Teise põlvkonna sõidumeerikukaardid sisaldavad kahte erinevat kaardirakendust, millest esimene langeb kokku esimese põlvkonna sõidumeerikukaartide rakendusega TACHO ning teine on 4. peatükis ja 2. liites kirjeldatud rakendus „TACHO_G2“.

145) Sõidumeerik määrab „kaardiseansi andmed“ juhi- või töökojakaardil kohe pärast kaardi sisestamist.

146) Sõidumeerik ajakohastab kehtiva juhi-, töökoja-, ettevõtte- ja/või kontrollikaardi kahes kaardirakenduses salvestatud andmed kõigi vajalike andmetega, mis on seotud ajaga, mil kaart on sisestatud, ja kaardi omanikuga. Neile kaartidele salvestatavaid andmeid on kirjeldatud 4. peatükis.

147) Sõidumeerik ajakohastab kehtivale juhi- ja/või töökojakaardile salvestatud andmed juhi tegevuse kohtade ja asukohtade kohta (punktide 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 ja 4.5.3.2.11 kohaselt) kaardi omaniku käsitsi sisestatud tegevuse ja kohtade andmetega.

148) Sõidumeerikukaartide ajakohastamine toimub nii, et vajaduse korral ja kaardi tegelikku salvestusmahtu arvesse võttes asendatakse vanimad andmed uusimate andmetega.

149) Kirjutamisvea korral üritab sõidumeerik maksimaalselt kolm korda kasutada sama kirjutamiskäsku; kui see ikkagi ei õnnestu, tunnistatakse kaart vigaseks ja kehtetuks.

150) Enne juhikaardi vabastamist ja pärast kõigi asjakohaste andmete salvestamist kahte kaardirakendusse lähtestab sõidumeerik „kaardiseansi andmed“.

3.15. **Kuvamine**

151) Kuvaril on vähemalt 20 tähemärki.

152) Tähemärk on vähemalt 5 mm kõrge ja 3,5 mm lai.

153) Kuvar toetab 1. liite 4. peatükis „Märgistikud“ kirjeldatud märgistikke. Kuvar võib kasutada lihtsustatud glüüfe (nt rõhumärkidega tähemärke võib kuvada rõhumärkideta või väiketähti võib näidata suurtähtedena).

154) Kuvar on varustatud piisava mittepimestava valgustusega.

155) Suuruste näidud on nähtavad väljastpoolt sõidumeerikut.

156) 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.

157) 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.

158) Sõiduki liikumise ajal on kuvar alati SISSE lülitatud.

159) Sõidumeerikul võib olla ka manuaalne või automaatne funktsioon kuvari VÄLJA lülitamiseks, kui sõiduk ei liigu.

Kuvamisvorming on määratletud 5. liites.

3.15.1. *Vaikekuva*

160) Kui muud teavet ei ole tarvis kuvada, näitab sõidumeeriku kuvar vaikimisi järgmisi andmeid:

— kohalik aeg (koordineeritud maailmaaeg + juhipoolne reguleerimine),

— kasutusrežiim,

— juhi hetketegevus ja kaasjuhi hetketegevus,

— Teave juhi kohta:

— kui juhi hetketegevus on JUHTIMINE, siis jooksev pidev juhtimisaeg ja jooksev kumulatiivne puhkepauside aeg,

— kui juhi hetketegevus ei ole JUHTIMINE, siis tegevuse jooksev kestus (alates selle valimisajast) ja jooksev kumulatiivne puhkepauside aeg.

161) Iga juhiga seotud andmete kuva on selge, lihtne ja üheselt mõistetav. Juhul kui juhi ja kaasjuhiga seotud teavet ei saa kuvada üheaegselt, kuvab sõidumeerik vaikimisi juhiga seotud teavet ja võimaldab kasutajal kuvada kaasjuhiga seotud teavet.

162) Juhul kui kuvari laius ei võimalda vaikimisi kuvada kasutusrežiimi, kuvab sõidumeerik uut kasutusrežiimi lühidalt režiimi muutumise korral.

163) Kaardi sisestamisel kuvab sõidumeerik lühidalt kaardi omaniku nime.

164) Kui avatakse tingimus „SÕIDUMEERIK MITTEVAJALIK“ või „PARVLAEVA-/RONGISÕIT“, peab kuvar vaikimisi näitama, et see tingimus on avatud, kasutades asjaomast piktogrammi (on lubatav, et juhi hetketegevust sel ajal ei näidata).

3.15.2. *Hoiatuskuva*

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

3.15.3. *Pääs menüüsse*

166) Sõidumeerikul on kohases menüüstruktuuris vajalikud käsud.

3.15.4. *Muud kuvad*

167) Soovi korral peab valikuliselt saama kuvada:

— kuupäeva ja kellaaega koordineeritud maailmaajas ning määratud kohalikku aega,

— kuue väljatrüki sisu samas vormingus kui väljatrükk ise,

— juhi pidevat juhtimisaega ja kumulatiivset puhkepauside aega,

— kaasjuhi pidevat juhtimisaega ja kumulatiivset puhkepauside aega,

— juhi kumulatiivset juhtimisaega eelmisel ja jooksval nädalal,

— kaasjuhi kumulatiivset juhtimisaega eelmisel ja jooksval nädalal,

valikuliselt:

— kaasjuhi tegevuse jooksvat kestust (alates selle valimisajast),

— juhi kumulatiivset juhtimisaega jooksval nädalal,

— kaasjuhi kumulatiivset juhtimisaega jooksval tööpäeval,

— juhi kumulatiivset juhtimisaega jooksval tööpäeval.

168) 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.

3.16. **Trükkimine**

169) Sõidumeerik suudab trükkida andmeid oma andmemälust ja/või sõidumeerikukaartidelt vastavalt seitsmele järgmisele väljatrükile:

— juhi ühe päeva tegevuste väljatrükk kaardilt,

— juhi ühe päeva tegevuste väljatrükk sõidukiseadmest,

— sündmuste ja vigade väljatrükk kaardilt,

— sündmuste ja vigade väljatrükk sõidukiseadmest,

— tehniliste andmete väljatrükk,

— kiiruse ületamise väljatrükk,

— sõidumeerikukaardi andmete ajalugu seoses konkreetse sõidukiseadmega (vt punkt 3.12.16).

Nende väljatrükkide üksikasjalikku vormingut ja sisu on kirjeldatud 4. liites.

Väljatrüki lõpus võib esitada täiendavaid andmeid.

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

170) „Juhi ühe päeva tegevuste väljatrükk kaardilt“ ning „sündmuste ja vigade väljatrükk kaardilt“ on võimalikud ainult siis, kui sõidumeerikusse on sisestatud juhi- või töökojakaart. Enne trükkimise alustamist ajakohastab sõidumeerik asjaomasele kaardile salvestatud andmed.

171) Selleks et teha „juhi ühe päeva tegevuste väljatrükk kaardilt“ või „sündmuste ja vigade väljatrükk kaardilt“, sõidumeerik:

— valib automaatselt juhi- või töökojakaardi, kui ainult üks neist kaartidest on sisestatud,

— või annab käsu valida allikkaart või valida kaart juhikaardi pesas, kui sõidumeerikusse on korraga sisestatud kaks kaarti.

172) Printer suudab trükkida ühes reas 24 tähemärki.

173) Tähemärk on vähemalt 2.1 mm kõrge ja 1,5 mm lai.

174) Printer toetab 1. liite 4. peatükis „Märgistikud“ kirjeldatud märgistikke.

175) Printerid konstrueeritakse nii, et väljatrükkide kujutustäpsus välistab lugemisel igasugused arusaamatused.

176) Väljatrükid säilitavad normaalsetes niiskus- (10–90 %) ja temperatuuritingimustes oma mõõtmed ja kirjed.

177) Sõidumeerikus kasutataval tüübikinnitusega paberil on asjaomane tüübikinnitusmärk ja viide, millist tüüpi sõidumeerikus (sõidumeerikutes) seda võib kasutada.

178) Tavalistes säilitustingimustes, pidades silmas valguse intensiivsust, niiskust ja temperatuuri, jäävad väljatrükid selgelt loetavaks ja identitavaks vähemalt kahe aasta jooksul.

179) Väljatrükid peavad vastama vähemalt 9. liites määratletud testikirjeldusele.

180) Neile dokumentidele peab olema võimalik lisada ka käsitsi kirjutatud märkusi, näiteks juhi allkirja.

181) „Paberi lõppemise“ sündmuse korral alustab sõidumeerik paberi lisamisel väljatrükki uuesti algusest või jätkab trükkimist, esitades üheselt mõistetava viite eelnevalt trükitud osale.

3.17. **Hoiatused**

182) Mis tahes sündmuse ja/või vea tuvastamise korral annab sõidumeerik juhile hoiatuse.

183) Hoiatuse voolukatkestuse sündmuse kohta võib lükata edasi ajani, mil toiteallikas taas külge ühendatakse.

184) Sõidumeerik hoiatab juhti 15 minutit enne lubatud pikima pideva juhtimisaja täitumist ja selle täitumisel.

185) Hoiatused on visuaalsed. Lisaks nähtavatele hoiatustele võib esitada ka kuuldavaid hoiatusi.

186) Visuaalsed hoiatused on kasutajale selgelt äratuntavad, need asuvad juhi vaateväljas ning on selgesti loetavad nii päeval kui ka öösel.

187) Visuaalsed hoiatused võivad olla sõidumeeriku sees ja/või olla sellest väljaspool.

188) Viimasel juhul on hoiatusel sümbol „T".

189) Hoiatus kestab vähemalt 30 sekundit, kui kasutaja ei ole sellele sõidumeeriku ühele või mitmele eriklahvile vajutades reageerinud. Esimene reageerimine ei kustuta hoiatuse põhjuse kuva, millele on viidatud järgmises lõikes.

190) Hoiatuse põhjus kuvatakse sõidumeerikul ja see jääb nähtavaks, kuni kasutaja on sellele reageerinud, kasutades sõidumeeriku eriklahvi või -käsku.

191) Võib anda lisahoiatusi, kui need ei aja juhti segadusse seoses eelnevalt määratletud hoiatustega.

3.18. Andmete allalaadimine välisandmekandjale

192) Vajaduse korral suudab sõidumeerik alla laadida oma andmemälust või juhikaardilt andmeid välisandmekandjale kalibreerimise/allalaadimise pistmiku kaudu. Enne allalaadimise alustamist ajakohastab sõidumeerik asjaomasele kaardile salvestatud andmed.

193) Lisaks sellele ja valitava funktsioonina võib sõidumeerik mis tahes kasutusrežiimis muul teel alla laadida andmeid ettevõttele, mis on autenditud kõnealuse kanali kaudu. Sellisel juhul kohaldatakse allalaadimise puhul ettevõtterežiimis kehtivaid andmetele juurdepääsu õigusi.

194) Allalaadimine ei tohi salvestatud andmeid muuta ega kustutada.

195) Kalibreerimise/allalaadimise pistiku elektrilist liidest on kirjeldatud 6. liites.

196) Allalaadimisprotokolle on kirjeldatud 7. liites.

3.19. Sihipärastes teeäärsetes kontrollides kasutatav kaugside

197) Kui süüde on sisse lülitatud, salvestab sõidukiseade iga 60 sekundi järel kaugsideseadmesse kõige uuemad andmed, mis on vajalikud sihipäraste teeäärsete kontrollide tegemiseks. Sellised andmed krüpteeritakse ja allkirjastatakse vastavalt 11. ja 14. liitele.

198) Kaugside teel kontrollitavad andmed peavad olema kaugsidelugejatele kättesaadavad juhtmevaba sideühenduse kaudu vastavalt 14. liitele.

199) Sihipärasteks teeäärseteks kontrollideks vajalikud andmed on seotud järgmisega:

— viimane turvarikkumise katse;

— pikim voolukatkestus;

— anduri tõrge,

— liikumisandmete viga,

— vastuolu sõiduki liikumisandmetes,

— sõitmine ilma kehtiva kaardita;

— kaardi sisestamine juhtimise ajal,

— aja korrigeerimise andmed,

— kalibreerimisandmed, sealhulgas kahe viimase salvestatud kalibreerimiskirje kuupäevad,

— sõiduki registreerimisnumber,

— sõidumeerikuga salvestatud kiirus.

3.20. **Andmete väljastamine lisavälisseadmetele**

200) Sõidumeerik võib olla varustatud ka standarditud liidesega, mis võimaldab välisseadmel tava- või kalibreerimisrežiimis kasutada sõidumeerikuga salvestatud või esitatud andmeid.

13. liites on esitatud valitava intelligentse transpordisüsteemi (ITS) liidese kirjeldus ja standardnõuded. Samal ajal võib kasutusel olla muid sarnaseid liideseid, kui need vastavalt täielikult 13. liites esitatud nõuetele minimaalse andmeloendi, turvalisuse ja juhi nõusoleku kohta.

Kõnealuse liidese kaudu kättesaadavaks tehtavate ITSi andmete suhtes kohaldatakse järgmisi nõudeid:

— need andmed valitakse sõidumeeriku andmesõnastiku olemasolevate andmete seast (1. liide);

— andmete üks alamhulk on märgistatud „isikuandmetena“;

— „isikuandmete“ alamhulk on kasutatav üksnes juhul, kui võimaldatud on juhi kontrollitav nõusolek, millega ta annab loa oma isikuandmete väljumiseks sõiduki võrgust;

— kui juhikaart on sisestatud, saab juhi nõusoleku menüükäskudega igal ajal sisse või välja lülitada;

— andmete hulka ja alamhulka edastatakse Bluetoothi traadita protokolliga sõiduki kabiini ümbruses värskendussagedusega 1 minut;

— välisseadme ühendus ITSi liidesega kaitstakse vähemalt neljakohalise spetsiaalse juhusliku PIN-koodiga, mis on salvestatud iga sõidukiseadme kuvarisse ja on selle kaudu kasutatav;

— ITSi liidese olemasolu ei tohi ühelgi juhul häirida sõidukiseadme nõuetekohast toimimist ja turvalisust.

Lisaks olemasolevate andmete seast valitud andmetele, mida käsitatakse miinimumloendina, võidakse väljastada muid andmeid, mis ei kuulu isikuandmete hulka.

Sõidumeerik teatab juhi nõusolekust muudele välisseadmetele.

Kui sõiduki süüde on SISSE lülitatud, edastatakse neid andmeid pidevalt.

201) Tagasiühilduvuse saavutamiseks võib sõidumeerikuid varustada määruse (EMÜ) nr 3821/85 uusima muudetud redaktsiooni lisas 1B kirjeldatud jadaühenduse liidesega. Sellegipoolest on isikuandmete edastamise korral siiski nõutav juhi nõusolek.

3.21. **Kalibreerimine**

202) Kalibreerimisfunktsioon võimaldab:

— ühendada liikumisanduri automaatselt sõidukiseadmega,

— ühendada vajaduse korral GNSSi välisseadme automaatselt sõidukiseadmega,

— kohandada sõidumeeriku konstanti (k) digitaalselt vastavalt sõidukit iseloomustavale koefitsiendile (w),

— korrigeerida hetkeaega sisestatud töökojakaardi kehtivusaja piires,

— korrigeerida läbisõidumõõdiku hetkenäitu,

— ajakohastada andmemällu salvestatud liikumisanduri identimisandmeid,

— ajakohastada vajaduse korral andmemällu salvestatud GNSSi välisseadme identimisandmeid,

— ajakohastada kõigi paigaldatud plommide tüüpe ja identifikaatoreid,

— ajakohastada või kinnitada muid sõidumeerikule tuntud parameetreid: sõiduki identimisandmeid, sõidukit iseloomustavat koefitsienti, rehvide efektiivümbermõõtu, rehvimõõtu ja kiiruspiiriku seadeid (vajaduse korral).

203) Lisaks võimaldab kalibreerimisfunktsioon tõkestada sõidumeerikus esimese põlvkonna sõidumeerikukaartide kasutamise, kui on täidetud 15. liites esitatud tingimused.

204) Liikumisanduri ühendamine sõidukiseadmega hõlmab vähemalt:

— liikumisanduris olevate liikumisanduri paigaldusandmete ajakohastamist (vajaduse korral),

— vajalike liikumisanduri identimisandmete kopeerimist liikumisandurist sõidukiseadme andmemällu.

205) GNSSi välisseadme ühendamine sõidukiseadmega hõlmab vähemalt:

— GNSSi välisseadmes olevate GNSSi välisseadme paigaldusandmete ajakohastamist (vajaduse korral),

— vajalike GNSSi välisseadme identimisandmete, sh GNSSi välisseadme seerianumbri, kopeerimist GNSSi välisseadmest sõidukiseadme andmemällu.

Ühendamisele järgneb GNSSi asukohateabe kontrollimine.

206) Kalibreerimisfunktsioon peab suutma sisestada vajalikke andmeid kalibreerimise/allalaadimise pistiku kaudu vastavalt 8. liites määratletud kalibreerimisprotokollile. Kalibreerimisfunktsioon võib sisestada vajalikke andmeid ka muul viisil.

3.22. **Teeäärne kalibreerimiskontroll**

207) Teeäärse kalibreerimiskontrolli funktsioon võimaldab vastava päringu tegemise ajal lugeda liikumisanduri seerianumbrit (võib olla sisse ehitatud adapterisse) ja sõidukiseadmega ühendatud GNSSi välisseadme seerianumbrit (vajaduse korral).

208) Kõnealune lugemine peab olema võimalik vähemalt sõidukiseadme kuvaril menüükäskude abil.

209) Teeäärse kalibreerimiskontrolli funktsioon võimaldab ka K-liini liidese kaudu valida 6. liites kirjeldatud kalibreerimise sisend-/väljundsignaaliliini sisend-/väljundrežiimi. Seda tehakse seansiga ECUAdjustmentSession, nagu on kirjeldatud 8.liite 7. jaos „Testimpulsside juhtimine – Sisend-/väljundsignaali juhtimise funktsionaalne üksus".

3.23. **Aja korrigeerimine**

210) Aja korrigeerimise funktsioon võimaldab hetkeaega automaatselt korrigeerida. Sõidumeerikus kasutatakse aja korrigeerimiseks kahte kellaaja allikat: 1) sõidukiseadme sisemine kell, 2) GNSSi vastuvõtja.

211) Sõidukiseadme sisemise kella aega korrigeeritakse automaatselt uuesti maksimaalselt 12tunniste intervallidega. Kui nimetatud aeg on möödunud ja GNSSi signaal puudub, seadistatakse aega kohe, kui sõidukiseade saab vastavalt sõiduki süüte lülitusolekule juurdepääsu GNSSi vastuvõtjast lähtuvale kehtivale ajateabele. Sõidukiseadme sisemise kella aja automaatseks seadistamiseks kasutatav etalonaeg saadakse GNSSi vastuvõtjast. Ajakonflikti sündmus käivitub juhul, kui hetkeaeg erineb GNSSi vastuvõtja edastatud ajateabest rohkem kui ühe (1) minuti võrra.

212) Kalibreerimisrežiimis võimaldab aja korrigeerimise funktsioon hetkeaega ka käsitsi korrigeerida.

3.24. **Tööomadused**

213) Sõidukiseade on täielikult toimiv temperatuurivahemikus – 20 °C kuni 70 °C, GNSSi välisseade temperatuurivahemikus – 20 °C kuni 70 °C ja liikumisandur temperatuurivahemikus – 40 °C kuni 135 °C. Andmemälu sisu säilib temperatuuril kuni – 40 °C.

214) Sõidumeerik on täielikult toimiv õhuniiskuse vahemikus 10–90 %.

215) Arukal sõidumeerikul kasutatavad plommid peavad taluma samasuguseid tingimusi nagu need sõidumeeriku osad, millele nad on kinnitatud.

216) Sõidumeerik on kaitstud ülepinge, toiteallika polaarsuse vahetuse ja lühiste eest.

217) Liikumisandurid kas:

— reageerivad magnetväljale, mis häirib sõiduki liikumise jälgimist – sel juhul registreeritakse ja salvestatakse sõidukiseadmes anduri tõrge (nõue 88), või

— sisaldavad tajurit, mis on magnetvälja vastu kaitstud või mida magnetväli ei mõjuta.

218) Sõidumeerik ja GNSSi välisseade vastavad ÜRO Euroopa Majanduskomisjoni eeskirjale nr 10 ning on kaitstud elektrostaatiliste lahenduste ja siirete eest.

3.25. **Materjalid**

219) Sõidumeeriku kõik koostisosad on tehtud piisavalt stabiilsetest ja piisava mehaanilise tugevusega materjalidest, millel on stabiilsed elektrilised ja magnetilised omadused.

220) Normaalsete kasutustingimuste tagamiseks tuleb seadme kõiki sisemisi osi kaitsta niiskuse ja tolmu eest.

221) Sõidukiseade ja GNSSi välisseade vastavad standardi IEC 60529:1989 (sh 1. muudatus: 1999 ja 2. muudatus: 2013) kohaselt kaitseklassile IP 40 ja liikumisandur kaitseklassile IP 64.

222) Sõidumeerik peab ergonoomilise väliskujunduse poolest vastama kohaldatavale tehnilisele kirjeldusele.

223) Sõidumeerikut kaitstakse juhusliku rikkumise eest.

3.26. **Märgistus**

224) Kui sõidumeerik kuvab sõiduki läbisõidumõõdiku näitu ja kiirust, kasutatakse selle kuvaril järgmist märgistust:

— vahemaa näidu lähedal vahemaa mõõtühik, mida näidatakse lühendiga km,

— kiiruse näidu lähedal lühend km/h.

Sõidumeeriku võib lülitada kuvama kiirust miilides tunnis, sellisel juhul näidatakse kiiruse mõõtühikut lühendi mph abil. Sõidumeeriku võib lülitada kuvama vahemaad miilides, sellisel juhul näidatakse vahemaa mõõtühikut lühendi mi abil.

225) Sõidumeeriku igale eraldi osale kinnitatakse kirjeldav tahvel, millel on järgmised üksikasjad:

— seadme tootja nimi ja aadress,

— tootja osa number ja seadme valmistamisaasta,

— seadme seerianumber,

— seadme tüübikinnitusmärk.

226) Kui kõigi eespool nimetatud üksikasjade esitamiseks ei ole ruumi, on kirjeldaval tahvlil vähemalt tootja nimi või logo ja seadme osa number.

4. SÕIDUMEERIKUKAARTIDE KONSTRUKTSIOONI- JA FUNKTSIONAALSED NÕUDED

4.1. **Nähtavad andmed**

Esipoolel on:

227) vastavalt kaardi tüübile kaardi välja andnud liikmesriigi ametlikus keeles või ametlikes keeltes suurelt trükitult sõna „juhikaart“ või „kontrollikaart“ või „töökojakaart“ või „ettevõttekaart“;

228) kaardi välja andnud liikmesriigi nimi (vabatahtlik);

229) kaardi välja andnud liikmesriigi rahvusvaheline tähis negatiivina sinises ristkülikus, mida ümbritseb kaksteist kollast tähte. Tähised on järgmised:

b	Belgia	LV	Läti
BG	Bulgaaria	L	Luksemburg
CZ	Tšehhi Vabariik	LT	Leedu
CY	Küpros	M	Malta
DK	Taani	NL	Madalmaad

D EST	Saksamaa Eesti	a PL	Austria Poola
GR	Kreeka	P RO SK SLO	Portugal Rumeenia Slovakkia Sloveenia
E	Hispaania	FIN	Soome
F HR H	Prantsusmaa Horvaatia Ungari	S	Rootsi
IRL	Iirimaa	UK	Ühendkuningriik
I	Itaalia		

230) 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		
4.b	Kaardi kehtivusaja lõpp		
4.c	Kaardi välja andnud asutuse nimi (võib trükkida kaardi pöördele)		
4.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)	Paigaldaja foto (ei ole kohustuslik)

	Juhikaart	Kontrollikaart	Ettevõtte- või töökojakaart
7.	Omaniku allkiri (ei ole kohustuslik)		
8.	Kaardi omaniku alaline elukoht või postiaadress (ei ole kohustuslik)	Kontrolliasutuse postiaadress	Ettevõtte või töökoja postiaadress

231) kuupäev kirjutatakse vormingus „pp/kk/aaaa“ või „pp.kk.aaaa“ (päev, kuu, aasta).

Tagumisel küljel on:

232) selgitus kaardi esiküljel olevate nummerdatud punktide kohta;

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

234) Sõidumeerikukaartidele trükitakse järgmine taustavärv:

— juhikaart: valge,

— kontrollikaart: sinine,

— töökojakaart: punane,

— ettevõttekaart: kollane.

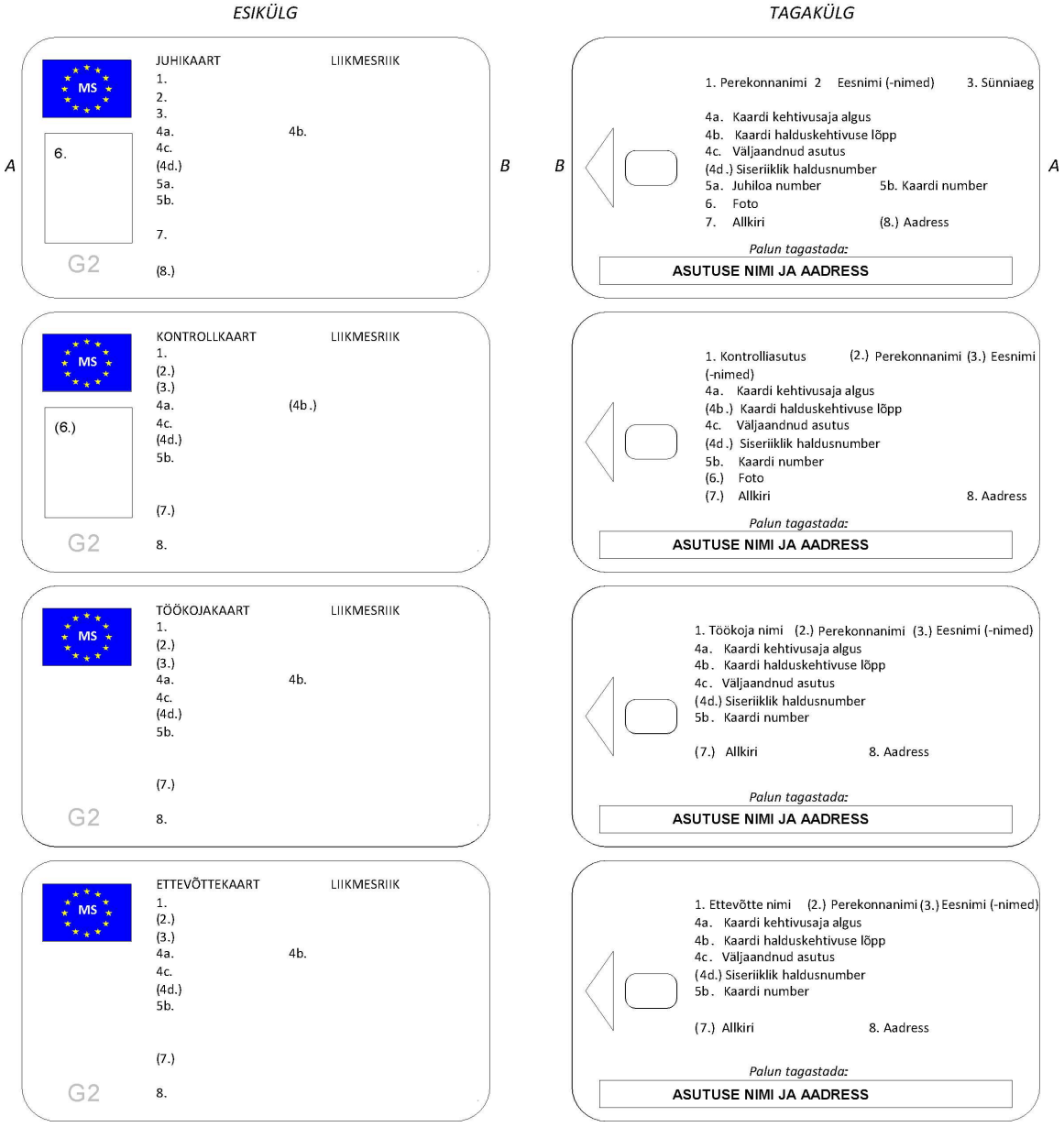
235) Sõidumeerikukaartidel on vähemalt järgmised omadused, kaitsmaks neid võltsimise ja rikkumise eest:

— peente giljoššmustrite ja vikerkaaretrükiga taustaturvamärk,

— foto piirkonnas kattuvad taustaturvamärk ja foto,

— vähemalt üks kahevärviline mikrokirjas rida.

ÜHENDUSE SÕIDUMEERIKUKAARTIDE NÄIDISED



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

237) Määruse (EL) nr 165/2014 artikli 26 lõikes 4 osutatud ajutised kaardid peavad vastama käesoleva lisa nõuetele.

4.2. Turvalisus

Süsteemi turvalisuse eesmärk on kaitsta kaartide ja sõidumeeriku vahel vahetatud andmete terviklikkust ja autentsust, kaitstes kaartidelt alla laaditud andmete terviklust ja autentsust, lubades teatavaid kirjutamisoperatsioone teha kaartidele ainult sõidumeerikul, dekrüpteerides teatud andmeid, välistades kaartidele salvestatud andmete igasuguse võltsimise, takistades manipuleerimist ning tuvastades igasuguse katse seda teha.

238) Süsteemi turvalisuse saavutamiseks peavad sõidumeerikukaardid vastama turvanõuetele, mis on määratletud 10. ja 11. liites.

239) Sõidumeerikukaardid peavad olema loetavad muude seadmetega, näiteks personaalarvutid.

4.3. **Standardid**

240) Sõidumeerikukaardid vastavad järgmistele standarditele:

— ISO/IEC 7810 *Identification cards – Physical characteristics* („Identimiskaardid. Füüsikalised omadused“);

— ISO/IEC 7816 *Identification cards – Integrated circuit cards* („Identimiskaardid. Kiipkaardid“):

— *Part 1: Physical characteristics* („Osa 1: Füüsikalised omadused“),

— *Part 2: Dimensions and position of the contacts* („Osa 2: Kontaktide mõõtmed ja asetus“) (ISO/IEC 7816-2:2007),

— *Part 3: Electrical interface and transmission protocols* („Osa 3: Elektriline liides ja edastusprotokollid“) (ISO/IEC 7816-3:2006),

— *Part 4: Organisation, security and commands for interchange* („Osa 4: Andmevahetuse ülesehitus, turvalisus ja käsud“) (ISO/IEC 7816-4:2013 + 1. parandus: 2014),

— *Part 6: Interindustry data elements for interchange* („Osa 6: Valdkondadevahelised andmeelemendid“) (ISO/IEC 7816-6:2004 + 1. parandus: 2006),

— *Part 8: Commands for security operations* („Osa 8: Turvatoimingute käsud“) (ISO/IEC 7816-8:2004).

— Sõidumeerikukaarte testitakse vastavalt standardile ISO/IEC 10373-3:2010 *Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices* („Identimiskaardid. Katsemeetodid. Osa 3: Kontaktidega kiipkaardid ja seotud liideseseadmed“).

4.4. **Keskkonnaalased ja elektrilised spetsifikatsioonid**

241) Sõidumeerikukaardid suudavad nõuetekohaselt toimida kõigis ühenduse territooriumil tavaliselt esinevates kliimatingimustes ning vähemalt temperatuurivahemikus – 25 °C kuni + 70 °C aeg-ajalt esineva maksimumtemperatuuriga kuni + 85 °C, kusjuures „aeg-ajalt“ tähendab kuni neli tundi korraga ja kuni sada korda kaardi kasutusea jooksul.

242) Sõidumeerikukaardid toimivad nõuetekohaselt õhuniiskuse vahemikus 10–90 %.

243) Sõidumeerikukaardid toimivad nõuetekohaselt viis aastat, kui neid kasutatakse vastavalt keskkonnaalastele ja elektrilistele spetsifikatsioonidele.

244) Toimimise ajal vastavad kaardid ÜRO Euroopa Majanduskomisjoni eeskirjale nr 10, mis käsitleb elektromagnetilist ühilduvust, ning neid kaitstakse elektrostaatiliste lahenduste eest.

4.5. **Andmete salvestamine**

Käesolevas lõike kohaldamisel:

— ajad salvestatakse täpsusega üks minut, kui ei ole määratletud teisiti;

— läbisõidumõõdiku näidud salvestatakse täpsusega üks kilomeeter;

— kiirused salvestatakse täpsusega 1 km/h;

— asukohad (laius ja pikkus) salvestatakse kraadides ja minutites eristusvõimega 1/10 minutit.

Andmesalvestusnõuetele vastavaid sõidumeerikukaartide funktsioone, käske ja loogilisi struktuure on kirjeldatud 2. liites.

Kui ei ole määratletud teisiti, korraldatakse andmete salvestamine sõidumeerikukaartidele nii, et teatud liiki kirjetele eraldatud mälumahu ammendumise korral asendatakse uute andmetega kõige vanemad salvestatud andmed.

245) Käesolevas lõikes määratletakse erineva kasutusotstarbega andmefailide minimaalne salvestusmaht. Sõidumeerikukaardid peavad suutma näidata sõidumeerikule nende andmefailide tegelikku salvestusmahtu.

246) Kõiki sõidumeerikukaartidele salvestatavaid lisaandmeid, mis on seotud muude kaardil olla võivate rakendustega, salvestatakse vastavalt direktiivile 95/46/EÜ, direktiivile 2002/58/EÜ ning määruse (EL) nr 165/2014 artiklile 7.

247) Sõidumeerikukaardi iga põhifail (MF) sisaldab kuni viit elementaarfaili (EF), mida kasutatakse kaardi haldamiseks, rakenduste ja kiibi identimiseks, ning kahte erifaili (DF):

— DF Tachograph, mis sisaldab esimese põlvkonna sõidukiseadmetele kasutatavat rakendust ja on olemas ka esimese põlvkonna sõidumeerikukaartidel,

— DF Tachograph_G2, mis sisaldab ainult teise põlvkonna sõidukiseadmetele kasutatavat rakendust ja on olemas ainult teise põlvkonna sõidumeerikukaartidel.

Kõik üksikasjad sõidumeerikukaartide struktuuri kohta on esitatud 2. liites.

4.5.1. *Identimiseks ja kaardihalduseks kasutatavad elementaarfailid*

4.5.2. *Kiipkaardi identimine*

248) Sõidumeerikukaardid suudavad salvestada järgmisi kiipkaardi identimisandmeid:

— kella peatamine,

— kaardi seerianumber (sealhulgas tootmisandmed),

— kaardi tüübikinnitusnumber,

— kaardi tunnus (ID),

— paigaldaja tunnus,

— kiibi identifikaator.

4.5.2.1. Kiibi identimine

249) Sõidumeerikukaardid suudavad salvestada järgmisi kiibi identimisandmeid:

— kiibi seerianumber,

— kiibi tootmisandmed.

4.5.2.2. DIR (ainult teise põlvkonna sõidumeerikukaartidel)

250) Sõidumeerikukaardid suudavad salvestada rakenduste identimise andmeobjekte, mida on kirjeldatud 2. liites.

4.5.2.3. ATRi teave (tingimuslik, ainult teise põlvkonna sõidumeerikukaartidel)

251) Sõidumeerikukaardid suudavad salvestada järgmisi laiendatud andmeobjekte:

— 2. liites kirjeldatud laiendatud andmeobjektid juhul, kui sõidumeerikukaart toetab laiendatud väljasid.

4.5.2.4. Laiendatud teave (tingimuslik, ainult teise põlvkonna sõidumeerikukaartidel)

252) Sõidumeerikukaardid suudavad salvestada järgmisi laiendatud andmeobjekte:

— 2. liites kirjeldatud laiendatud andmeobjektid juhul, kui sõidumeerikukaart toetab laiendatud väljasid.

4.5.3. *Juhikaart*

4.5.3.1. Rakendus Tachograph (kasutatav esimese ja teise põlvkonna sõidukiseadmetes)

4.5.3.1.1. Rakenduse identimisandmed

253) Juhikaart suudab salvestada järgmisi rakenduse identimisandmeid:

— sõidumeeriku rakenduse identimisandmed,

— sõidumeerikukaardi tüübi identimisandmed.

4.5.3.1.2. Võtmed ja sertifikaadid

254) Juhikaart suudab salvestada mitmeid krüptograafilisi võtmeid ja sertifikaate, mida on kirjeldatud 11. liite A osas.

4.5.3.1.3. Kaardi identimisandmed

255) Juhikaart suudab salvestada järgmisi kaardi identimisandmeid:

— kaardi number,

— väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,

— kaardi kehtivusaja algus, kaardi kehtivusaja lõpp.

4.5.3.1.4. Kaardi omaniku identimisandmed

256) Juhikaart suudab salvestada järgmisi kaardi omaniku identimisandmeid:

— omaniku perekonnanimi,

— omaniku eesnimi (eesnimed),

— sünniaeg,

— eelistatav keel.

4.5.3.1.5. Kaardilt alla laadimine

257) Juhikaart suudab salvestada järgmisi andmeid kaardilt alla laadimise kohta:

— viimase kaardilt alla laadimise (muul eesmärgil kui kontrolliks) kuupäev ja kellaaeg.

258) Juhikaart peab mahutama ühe sellise kirje.

4.5.3.1.6. Teave juhiloa kohta

259) Juhikaart suudab salvestada järgmisi andmeid juhiloa kohta:

— väljaandnud liikmesriik, väljaandnud asutuse nimi,

— juhiloa number (kaardi väljaandmise päeval).

4.5.3.1.7. Andmed sündmuste kohta

Käesoleva lõigu kohaldamisel salvestatakse kellaaeg sekundilise täpsusega.

260) Juhikaart suudab salvestada andmeid, 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),

— voolukatkestus,

— liikumisandmete viga,

— turvalisuse rikkumise katsed.

261) Juhikaart suudab salvestada nende sündmuste kohta järgmisi andmeid:

— sündmuse kood,

— sündmuse alguse kuupäev ja kellaaeg (või kaardi sisestamise aeg, kui sündmus sel ajal kestis),

— sündmuse lõpu kuupäev ja kellaaeg (või kaardi väljavõtmise aeg, kui sündmus sel ajal kestis),

— sõiduki, milles sündmus toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.

Märkus: sündmuse „aja kattumine“ kohta:

— sündmuse alguse kuupäev ja kellaaeg peavad vastama kaardi eelmisest sõidukist väljavõtmise kuupäevale ja kellaajale,

— sündmuse lõpu kuupäev ja kellaaeg peavad vastama kaardi praegusesse sõidukisse sisestamise kuupäevale ja kellaajale,

— sõiduki andmed peavad vastama sellele sõidukile, mis sündmuse põhjustas.

Märkus: sündmuse „viimane kaardiseanss nõuetekohaselt sulgemata“ kohta:

— sündmuse alguse kuupäev ja kellaaeg peavad vastama nõuetekohaselt sulgemata kaardiseansi kaardi sisestamise kuupäevale ja ajale,

— sündmuse lõpu kuupäev ja kellaaeg peavad vastama kaardiseansi, mille ajal sündmus tuvastati (praegune seanss), kaardi sisestamise kuupäevale ja ajale,

— sõiduki andmed peavad vastama sõidukile, milles seanssi ei suletud nõuetekohaselt.

262) Juhikaart peab suutma salvestada andmeid iga sündmusetüübi viimase kuue sündmuse kohta (st 36 sündmust).

4.5.3.1.8. Andmed vigade kohta

Käesoleva lõigu kohaldamisel registreeritakse aega sekundilise täpsusega.

263) Juhikaart suudab salvestada andmeid, mis on seotud kaardi sisestamisel sõidumeeriku tuvastatud järgmiste vigadega:

— kaardi viga (kui see kaart on sündmuse põhjustaja),

— sõidumeeriku viga.

264) Juhikaart suudab salvestada nende vigade kohta järgmisi andmeid:

— vea kood,

— vea alguse kuupäev ja kellaaeg (või kaardi sisestamise aeg, kui viga sel ajal kestis),

— vea lõpu kuupäev ja kellaaeg (või kaardi väljavõtmise aeg, kui viga sel ajal kestis),

— sõiduki, milles viga toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.

265) Juhikaart peab suutma salvestada andmeid iga veatüübi viimase kaheteistkümne vea kohta (st 24 viga).

4.5.3.1.9. Andmed juhi tegevuse kohta

266) Juhikaart suudab salvestada iga päeva kohta, mil kaarti on kasutatud või mille kohta juht on tegevused käsitsi sisestanud, järgmisi andmeid:

— kuupäev,

— tööpäevade loendur (mida suurendatakse igal kalendripäeval ühe võrra),

— juhi poolt läbitud kogu vahemaa sellel päeval,

— juhi staatus kell 00.00,

— iga kord, kui juht on muutnud tegevust ja/või juhtimisstaatust ja/või on oma kaardi sisestanud või välja võtnud:

— juhtimisstaatus (MEESKOND, ÜKSI),

— kaardipesa (JUHT, KAASJUHT),

— kaardi staatus (SISESTATUD, SISESTAMATA),

— tegevus (JUHTIMINE, VALMISOLEK, TÖÖ, PUHKEPAUS/PUHKUS),

— muudatuse kellaaeg.

267) Juhikaardi mälu peab suutma säilitada vähemalt 28 päeva andmed juhi tegevuse kohta (keskmine juhi tegevus on määratletud 93 muudatusega päevas).

268) Nõuetes 261, 264 ja 266 loetletud andmed salvestatakse nii, et tegevuseotsinguid saab teha toimumise järjestuses isegi ajalise kattumise korral.

4.5.3.1.10. Andmed kasutatud sõidukite kohta

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

— sõiduki esimese kasutamise kuupäev ja kellaaeg (st sõiduki selle kasutusaja kaardi esimene sisestamine või 00.00, kui kasutusaeg sel ajal jätkub),

— sõiduki läbisõidumeeriku näit sel ajal,

— sõiduki viimase kasutamise kuupäev ja kellaaeg (st sõiduki selle kasutusaja kaardi viimane väljavõtmine või 23.59, kui kasutamisaeg sel ajal jätkub),

— sõiduki läbisõidumeeriku näit sel ajal,

— VRN ja sõiduki registreerinud liikmesriik.

270) Juhikaart peab suutma salvestada vähemalt 84 sellist kirjet.

4.5.3.1.11. Tööpäeva algus- ja/või lõppkoht

271) Juhikaart suudab salvestada järgmised andmed, mis on seotud juhi sisestatud tööpäeva algus- ja/või lõppkohaga:

— sisestamise kuupäev ja kellaaeg (või sisestamisega seotud kuupäev/aeg, kui sisestamine toimub käsitsi),

— sisestuse tüüp (algus või lõpp, sisestustingimus),

— sisestatud riik või piirkond,

— sõiduki läbisõidumõõdiku näit.

272) Juhikaardi mälu peab mahutama vähemalt 42 paari selliseid kirjeid.

4.5.3.1.12. Andmed kaardiseansi kohta

273) Juhikaart suudab salvestada selle sõidukiga seotud andmeid, kus avati praegune seanss:

— seansi avamise (st kaardi sisestamise) kuupäev ja kellaaeg sekundilise täpsusega,

— VRN ja sõiduki registreerinud liikmesriik.

4.5.3.1.13. Andmed kontrollitegevuse kohta

274) Juhikaart suudab salvestada järgmisi kontrollitegevustega seotud andmeid:

— kontrolli kuupäev ja kellaaeg,

— kontrollikaardi number ja kaardi välja andnud liikmesriik,

— kontrolli tüüp (kuvamine ja/või trükkimine ja/või sõidukiseadme andmete allalaadimine ja/või kaardi andmete allalaadimine (vt märkus)),

— allalaadimise korral allalaaditud ajavahemik,

— sõiduki, milles kontroll toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.

Märkus: kaardilt alla laadimine registreeritakse ainult juhul, kui see toimub sõidumeeriku kaudu.

275) Juhikaart peab mahutama ühe sellise kirje.

4.5.3.1.14. Andmed eritingimuste kohta

276) Juhikaart suudab salvestada järgmisi andmeid, mis on seotud kaardi sisestamisel (mis tahes pesasse) sisestatud eritingimustega:

— sisestamise kuupäev ja kellaaeg,

— eritingimuse tüüp.

277) Juhikaart peab suutma salvestada vähemalt 56 sellist kirjet.

4.5.3.2. Teise põlvkonna rakendus Tachograph (ei ole kasutatav esimese põlvkonna sõidukiseadmes)

4.5.3.2.1. Rakenduse identimisandmed

278) Juhikaart suudab salvestada järgmisi rakenduse identimisandmeid:

— sõidumeeriku rakenduse identimisandmed,

— sõidumeerikukaardi tüübi identimisandmed.

4.5.3.2.2. Võtmed ja sertifikaadid

279) Juhikaart suudab salvestada mitmeid krüptograafilisi võtmeid ja sertifikaate, mida on kirjeldatud 11. liite B osas.

4.5.3.2.3. Kaardi identimisandmed

280) Juhikaart suudab salvestada järgmisi kaardi identimisandmeid:

— kaardi number,

— väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,

— kaardi kehtivusaja algus, kaardi kehtivusaja lõpp.

4.5.3.2.4. Kaardi omaniku identimisandmed

281) Juhikaart suudab salvestada järgmisi kaardi omaniku identimisandmeid:

— omaniku perekonnanimi,

— omaniku eesnimi (eesnimed),

— sünniaeg,

— eelistatav keel.

4.5.3.2.5. Kaardilt alla laadimine

282) Juhikaart suudab salvestada järgmisi andmeid kaardilt alla laadimise kohta:

— viimase kaardilt alla laadimise (muul eesmärgil kui kontrolliks) kuupäev ja kellaaeg.

283) Juhikaart peab mahutama ühe sellise kirje.

4.5.3.2.6. Teave juhiloa kohta

284) Juhikaart suudab salvestada järgmisi andmeid juhiloa kohta:

— väljaandnud liikmesriik, väljaandnud asutuse nimi,

— juhiloa number (kaardi väljaandmise päeval).

4.5.3.2.7. Andmed sündmuste kohta

Käesoleva lõigu kohaldamisel salvestatakse kellaaeg sekundilise täpsusega.

285) Juhikaart suudab salvestada andmeid, 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),

— voolukatkestus,

— kaugsideseadmega side pidamise viga,

— GNSSi vastuvõtja asukohateabe puudumise sündmus,

— GNSSi välisseadmega side pidamise viga,

— liikumisandmete viga,

— vastuolu sõiduki liikumisandmetes,

— turvalisuse rikkumise katsed,

— ajakonflikt.

286) Juhikaart suudab salvestada nende sündmuste kohta järgmisi andmeid:

— sündmuse kood,

— sündmuse alguse kuupäev ja kellaaeg (või kaardi sisestamise aeg, kui sündmus sel ajal kestis),

— sündmuse lõpu kuupäev ja kellaaeg (või kaardi väljavõtmise aeg, kui sündmus sel ajal kestis),

— sõiduki, milles sündmus toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.

Märkus: sündmuse „aja kattumine“ kohta:

— sündmuse alguse kuupäev ja kellaaeg peavad vastama kaardi eelmisest sõidukist väljavõtmise kuupäevale ja kellaajale,

— sündmuse lõpu kuupäev ja kellaaeg peavad vastama kaardi praegusesse sõidukisse sisestamise kuupäevale ja kellaajale,

— sõiduki andmed peavad vastama sellele sõidukile, mis sündmuse põhjustas.

Märkus: sündmuse „viimane kaardiseanss nõuetekohaselt sulgemata“ kohta:

— sündmuse alguse kuupäev ja kellaaeg peavad vastama nõuetekohaselt sulgemata kaardiseansi kaardi sisestamise kuupäevale ja ajale,

— sündmuse lõpu kuupäev ja kellaaeg peavad vastama kaardiseansi, mille ajal sündmus tuvastati (praegune seanss), kaardi sisestamise kuupäevale ja ajale,

— sõiduki andmed peavad vastama sõidukile, milles seanssi ei suletud nõuetekohaselt.

287) Juhikaart peab suutma salvestada andmeid iga sündmusetüübi viimase kuue sündmuse kohta (st 66 sündmust).

4.5.3.2.8. Andmed vigade kohta

Käesoleva lõigu kohaldamisel registreeritakse aega sekundilise täpsusega.

288) Juhikaart suudab salvestada andmeid, mis on seotud kaardi sisestamisel sõidumeeriku tuvastatud järgmiste vigadega:

— kaardi viga (kui see kaart on sündmuse põhjustaja),

— sõidumeeriku viga.

289) Juhikaart suudab salvestada nende vigade kohta järgmisi andmeid:

— vea kood,

— vea alguse kuupäev ja kellaaeg (või kaardi sisestamise aeg, kui viga sel ajal kestis),

— vea lõpu kuupäev ja kellaaeg (või kaardi väljavõtmise aeg, kui viga sel ajal kestis),

— sõiduki, milles viga toimus, registreerimisnumber ja selle sõiduki registreerinud liikmesriik.

290) Juhikaart peab suutma salvestada andmeid iga veatüübi viimase kaheteistkümne vea kohta (st 24 viga).

4.5.3.2.9. Andmed juhi tegevuse kohta

291) Juhikaart suudab salvestada iga päeva kohta, mil kaarti on kasutatud või mille kohta juht on tegevused käsitsi sisestanud, järgmisi andmeid:

— kuupäev,

— tööpäevade loendur (mida suurendatakse igal kalendripäeval ühe võrra),

— juhi poolt läbitud kogu vahemaa sellel päeval,

— juhi staatus kell 00.00,

— kõik korrad, mil juht on muutnud tegevust ja/või juhtimisstaatust ja/või on oma kaardi sisestanud või välja võtnud:

— juhtimisstaatus (MEESKOND, ÜKSI),

— kaardipesa (JUHT, KAASJUHT),

— kaardi staatus (SISESTATUD, SISESTAMATA),

— tegevus (JUHTIMINE, VALMISOLEK, TÖÖ, PUHKEPAUS/PUHKUS),

— muudatuse kellaaeg.

292) Juhikaardi mälu peab suutma säilitada vähemalt 28 päeva andmed juhi tegevuse kohta (keskmine juhi tegevus on määratletud 93 tegevuse muudatusega päevas).

293) Nõuetes 286, 289 ja 291 loetletud andmed salvestatakse nii, et tegevuseotsinguid saab teha toimumise järjestuses isegi ajalise kattumise korral.

4.5.3.2.10. Andmed kasutatud sõidukite kohta

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

— sõiduki esimese kasutamise kuupäev ja kellaaeg (st sõiduki selle kasutusaja kaardi esimene sisestamine või 00.00, kui kasutusaeg sel ajal jätkub),

— sõiduki läbisõidumeeriku näit esimese kasutamise ajal,

— sõiduki viimase kasutamise kuupäev ja kellaaeg (st sõiduki selle kasutusaja kaardi viimane väljavõtmine või 23.59, kui kasutamisaeg sel ajal jätkub),

— sõiduki läbisõidumeeriku näit viimase kasutamise ajal,

— VRN ja sõiduki registreerinud liikmesriik,

— sõiduki VIN.

295) Juhikaart peab suutma salvestada vähemalt 84 sellist kirjet.

4.5.3.2.11. Tööpäeva algus- ja/või lõppkoht

296) Juhikaart suudab salvestada järgmised andmed, mis on seotud juhi sisestatud tööpäeva algus- ja/või lõppkohaga:

— sisestamise kuupäev ja kellaaeg (või sisestamisega seotud kuupäev/aeg, kui sisestamine toimub käsitsi),

— sisestuse tüüp (algus või lõpp, sisestustingimus),

— sisestatud riik või piirkond,

— sõiduki läbisõidumõõdiku näit,

— sõiduki asukoht,

— GNSSi täpsus, kuupäev ja kellaaeg asukoha määramise ajal.

297) Juhikaardi mälu peab mahutama vähemalt 84 paari selliseid kirjeid.

4.5.3.2.12. Andmed kaardiseansi kohta

298) Juhikaart suudab salvestada selle sõidukiga seotud andmeid, kus avati praegune seanss:

— seansi avamise (st kaardi sisestamise) kuupäev ja kellaaeg sekundilise täpsusega,

— VRN ja sõiduki registreerinud liikmesriik.

4.5.3.2.13. Andmed kontrollitegevuse kohta

299) Juhikaart suudab salvestada järgmisi kontrollitegevustega seotud andmeid:

— kontrolli kuupäev ja kellaaeg,

— kontrollikaardi number ja kaardi välja andnud liikmesriik,

— kontrolli tüüp (kuvamine ja/või trükkimine ja/või sõidukiseadme 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 alla laadimine ainult siis, kui see on toimunud sõidumeeriku kaudu.

300) Juhikaart peab mahutama ühe sellise kirje.

4.5.3.2.14. Andmed eritingimuste kohta

301) Juhikaart suudab salvestada järgmisi andmeid, mis on seotud kaardi sisestamisel (mis tahes pesasse) sisestatud eritingimustega:

— sisestamise kuupäev ja kellaaeg,

— eritingimuse tüüp.

302) Juhikaart peab suutma salvestada vähemalt 56 sellist kirjet.

4.5.3.2.15. Andmed kasutatud sõidukiseadmete kohta

303) Juhikaart suudab salvestada järgmisi andmeid sõidukiseadmete kohta, milles kaarti on kasutatud:

— sõidukiseadme kasutamise alguse kuupäev ja kellaaeg (st kaardi esimene sisestamine sõidukiseadmesse sellel kasutusajal),

— sõidukiseadme tootja nimi,

— sõidukiseadme tüüp,

— sõidukiseadme tarkvaraversiooni number.

304) Juhikaart peab suutma salvestada vähemalt 84 sellist kirjet.

4.5.3.2.16. Kolme järjestikuse sõidutunni täitumiskohtade andmed

305) Juhikaart suudab salvestada järgmisi andmeid, mis on seotud sõiduki asukohaga ajal, kui juhil täitub kolm järjestikust sõidutundi:

— kuupäev ja kellaaeg, mil kaardi omanikul täitub kolm järjestikust sõidutundi,

— sõiduki asukoht,

— GNSSi täpsus, kuupäev ja kellaaeg asukoha määramise ajal.

306) Juhikaart peab suutma salvestada vähemalt 252 sellist kirjet.

4.5.4. *Töökojakaart*

4.5.4.1. Rakendus Tachograph (kasutatav esimese ja teise põlvkonna sõidukiseadmetes)

4.5.4.1.1. Rakenduse identimisandmed

307) Töökojakaart suudab salvestada järgmisi rakenduse identimisandmeid:

— sõidumeeriku rakenduse identimisandmed,

— sõidumeerikukaardi tüübi identimisandmed.

4.5.4.1.2. Võtmed ja sertifikaadid

308) Töökojakaart suudab salvestada mitmeid krüptograafilisi võtmeid ja sertifikaate, mida on kirjeldatud 11. liite A osas.

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

4.5.4.1.3. Kaardi identimisandmed

310) Töökojakaart suudab salvestada järgmisi kaardi identimisandmeid:

— kaardi number,

— väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,

— kaardi kehtivusaja algus, kaardi kehtivusaja lõpp.

4.5.4.1.4. Kaardi omaniku identimisandmed

311) Töökojakaart suudab salvestada järgmisi kaardi omaniku identimisandmeid:

— töökoja nimi,

— töökoja aadress,

— omaniku perekonnanimi,

— omaniku eesnimi (eesnimed),

— eelistatav keel.

4.5.4.1.5. Kaardilt alla laadimine

312) Töökojakaart suudab salvestada kaardilt alla laadimise andmeid samal viisil nagu juhikaart.

4.5.4.1.6. Andmed kalibreerimise ja aja korrigeerimise kohta

313) Töökojakaart suudab salvestada andmeid kalibreerimiste ja/või aja korrigeerimiste kohta, mis on tehtud siis, kui kaart oli sisestatud sõidumeerikusse.

314) Iga kalibreerimiskirje peab sisaldama järgmisi andmeid:

— kalibreerimise eesmärk (aktiveerimine, esimene paigaldamine, paigaldamine, perioodiline kontroll),

— sõiduki identimistunnus,

— ajakohastatud või kinnitatud parameetrid (sõidukit iseloomustav koefitsient, sõidumeeriku konstant, rehvide efektiivümbermõõt, rehvimõõt, kiiruspiiriku seadistus, läbisõidumõõdik (vana ja uus näit), kuupäev ja kellaaeg (vana ja uus näit)),

— sõidumeeriku identimisandmed (sõidukiseadme osa number, sõidukiseadme seerianumber, liikumisanduri seerianumber).

315) Töökojakaart peab suutma salvestada vähemalt 88 sellist kirjet.

316) Töökojakaardil on loendur, mis näitab kaardiga tehtud kõigi kalibreerimiste arvu.

317) Töökojakaardil on loendur, mis näitab kaardiga tehtud viimase allalaadimise järgset kalibreerimiste arvu.

4.5.4.1.7. Andmed sündmuste ja vigade kohta

318) Töökojakaart suudab salvestada andmeid sündmuste ja vigade kohta samal viisil nagu juhikaart.

319) Töökojakaart suudab salvestada andmeid iga sündmusetüübi viimase kolme sündmuse kohta (st 18 sündmust) ja iga veatüübi viimase kuue vea kohta (st 12 viga).

4.5.4.1.8. Andmed juhi tegevuse kohta

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

321) Töökojakaart peab mahutama vähemalt juhi ühe keskmise tegevuspäeva andmed.

4.5.4.1.9. Andmed kasutatud sõidukite kohta

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

323) Töökojakaart peab suutma salvestada vähemalt 4 sellist kirjet.

4.5.4.1.10. Andmed tööpäeva alguse ja/või lõpu kohta

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

325) Töökojakaart peab mahutama vähemalt kolm paari selliseid kirjeid.

4.5.4.1.11. Andmed kaardiseansi kohta

326) Töökojakaart suudab salvestada kaardiseansi andmeid samal viisil nagu juhikaart.

4.5.4.1.12. Andmed kontrollitegevuse kohta

327) Töökojakaart suudab salvestada kontrollitegevuse andmeid samal viisil nagu juhikaart.

4.5.4.1.13. Andmed eritingimuste kohta

328) Töökojakaart suudab salvestada eritingimustega seotud andmeid samal viisil nagu juhikaart.

329) Töökojakaart peab suutma salvestada vähemalt 2 sellist kirjet.

4.5.4.2. Teise põlvkonna rakendus Tachograph (ei ole kasutatav esimese põlvkonna sõidukiseadmes)

4.5.4.2.1. Rakenduse identimisandmed

330) Töökojakaart suudab salvestada järgmisi rakenduse identimisandmeid:

— sõidumeeriku rakenduse identimisandmed,

— sõidumeerikukaardi tüübi identimisandmed.

4.5.4.2.2. Võtmed ja sertifikaadid

331) Töökojakaart suudab salvestada mitmeid krüptograafilisi võtmeid ja sertifikaate, mida on kirjeldatud 11. liite B osas.

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

4.5.4.2.3. Kaardi identimisandmed

333) Töökojakaart suudab salvestada järgmisi kaardi identimisandmeid:

— kaardi number,

— väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,

— kaardi kehtivusaja algus, kaardi kehtivusaja lõpp.

4.5.4.2.4. Kaardi omaniku identimisandmed

334) Töökojakaart suudab salvestada järgmisi kaardi omaniku identimisandmeid:

— töökoja nimi,

— töökoja aadress,

— omaniku perekonnanimi,

— omaniku eesnimi (eesnimed),

— eelistatav keel.

4.5.4.2.5. Kaardilt alla laadimine

335) Töökojakaart suudab salvestada kaardilt alla laadimise andmeid samal viisil nagu juhikaart.

4.5.4.2.6. Andmed kalibreerimise ja aja korrigeerimise kohta

336) Töökojakaart suudab salvestada andmeid kalibreerimiste ja/või aja korrigeerimiste kohta, mis on tehtud siis, kui kaart oli sisestatud sõidumeerikusse.

337) Iga kalibreerimiskirje peab sisaldama järgmisi andmeid:

— kalibreerimise eesmärk (aktiveerimine, esimene paigaldamine, paigaldamine, perioodiline kontroll),

— sõiduki identimistunnus,

— ajakohastatud või kinnitatud parameetrid (sõidukit iseloomustav koefitsient, sõidumeeriku konstant, rehvide efektiivümbermõõt, rehvimõõt, kiiruspiiriku seadistus, läbisõidumõõdik (vana ja uus näit), kuupäev ja kellaaeg (vana ja uus näit),

— sõidumeeriku identimisandmed (sõidukiseadme osa number, sõidukiseadme seerianumber, liikumisanduri seerianumber, kaugsideseadme seerianumber ja GNSSi välisseadme seerianumber, kui see on vajalik),

— kõigi paigaldatud plommide liigid ja identifikaatorid,

— sõidukiseadme suutlikkus kasutada esimese põlvkonna sõidumeerikukaarte (võimaldatud või mitte).

338) Töökojakaart peab suutma salvestada vähemalt 88 sellist kirjet.

339) Töökojakaardil on loendur, mis näitab kaardiga tehtud kõigi kalibreerimiste arvu.

340) Töökojakaardil on loendur, mis näitab kaardiga tehtud viimase allalaadimise järgset kalibreerimiste arvu.

4.5.4.2.7. Andmed sündmuste ja vigade kohta

341) Töökojakaart suudab salvestada andmeid sündmuste ja vigade kohta samal viisil nagu juhikaart.

342) Töökojakaart suudab salvestada andmeid iga sündmusetüübi viimase kolme sündmuse kohta (st 33 sündmust) ja iga veatüübi viimase kuue vea kohta (st 12 viga).

4.5.4.2.8. Andmed juhi tegevuse kohta

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

344) Töökojakaart peab mahutama vähemalt juhi ühe keskmise tegevuspäeva andmed.

4.5.4.2.9. Andmed kasutatud sõidukite kohta

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

346) Töökojakaart peab suutma salvestada vähemalt 4 sellist kirjet.

4.5.4.2.10. Andmed tööpäeva alguse ja/või lõpu kohta

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

348) Töökojakaart peab mahutama vähemalt kolm paari selliseid kirjeid.

4.5.4.2.11. Andmed kaardiseansi kohta

349) Töökojakaart suudab salvestada kaardiseansi andmeid samal viisil nagu juhikaart.

4.5.4.2.12. Andmed kontrollitegevuse kohta

350) Töökojakaart suudab salvestada kontrollitegevuse andmeid samal viisil nagu juhikaart.

4.5.4.2.13. Andmed kasutatud sõidukiseadmete kohta

351) Töökojakaart suudab salvestada järgmisi andmeid erinevate sõidukiseadmete kohta, milles kaarti on kasutatud:

— sõidukiseadme kasutamise alguse kuupäev ja kellaaeg (st kaardi esimene sisestamine sõidukiseadmesse sellel kasutusajal),

— sõidukiseadme tootja nimi,

— sõidukiseadme tüüp,

— sõidukiseadme tarkvaraversiooni number.

352) Töökojakaart peab suutma salvestada vähemalt 4 sellist kirjet.

4.5.4.2.14. Kolme järjestikuse sõidutunni täitumiskohtade andmed

353) Töökojakaart suudab salvestada järgmisi andmeid, mis on seotud sõiduki asukohaga ajal, kui juhil täitub kolm järjestikust sõidutundi:

— kuupäev ja kellaaeg, mil kaardi omanikul täitub kolm järjestikust sõidutundi,

— sõiduki asukoht,

— GNSSi täpsus, kuupäev ja kellaaeg asukoha määramise ajal.

354) Töökojakaart peab suutma salvestada vähemalt 18 sellist kirjet.

4.5.4.2.15. Andmed eritingimuste kohta

355) Töökojakaart suudab salvestada eritingimustega seotud andmeid samal viisil nagu juhikaart.

356) Töökojakaart peab suutma salvestada vähemalt 2 sellist kirjet.

4.5.5. *Kontrollikaart*

4.5.5.1. Rakendus Tachograph (kasutatav esimese ja teise põlvkonna sõidukiseadmetes)

4.5.5.1.1. Rakenduse identimisandmed

357) Kontrollikaart suudab salvestada järgmisi rakenduse identimisandmeid:

— sõidumeeriku rakenduse identimisandmed,

— sõidumeerikukaardi tüübi identimisandmed.

4.5.5.1.2. Võtmed ja sertifikaadid

358) Kontrollikaart suudab salvestada mitmeid krüptograafilisi võtmeid ja sertifikaate, mida on kirjeldatud 11. liite A osas.

4.5.5.1.3. Kaardi identimisandmed

359) Kontrollikaart suudab salvestada järgmisi kaardi identimisandmeid:

— kaardi number,

— väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,

— kaardi kehtivusaja algus, kaardi kehtivusaja lõpp (kui see on olemas).

4.5.5.1.4. Kaardi omaniku identimisandmed

360) Kontrollikaart suudab salvestada järgmisi kaardi omaniku identimisandmeid:

— kontrolliasutuse nimi,

— kontrolliasutuse aadress,

— omaniku perekonnanimi,

— omaniku eesnimi (eesnimed),

— eelistatav keel.

4.5.5.1.5. Andmed kontrollitegevuse kohta

361) Kontrollikaart suudab salvestada järgmisi andmeid kontrollitegevuse kohta:

— kontrolli kuupäev ja kellaaeg,

— kontrolli tüüp (kuvamine ja/või trükkimine ja/või sõidukiseadme andmete allalaadimine ja/või kaardi andmete allalaadimine ja/või teeäärne kalibreerimiskontroll),

— allalaaditud ajavahemik (kui see on olemas),

— kontrollitud VRN ja sõiduki registreerinud liikmesriik,

— kontrollitud juhikaardi number ja kaardi välja andnud liikmesriik.

362) Kontrollikaart peab suutma salvestada vähemalt 230 sellist kirjet.

4.5.5.2. Rakendus Tachograph G2 (ei ole kasutatav esimese põlvkonna sõidukiseadmes)

4.5.5.2.1. Rakenduse identimisandmed

363) Kontrollikaart suudab salvestada järgmisi rakenduse identimisandmeid:

— sõidumeeriku rakenduse identimisandmed,

— sõidumeerikukaardi tüübi identimisandmed.

4.5.5.2.2. Võtmed ja sertifikaadid

364) Kontrollikaart suudab salvestada mitmeid krüptograafilisi võtmeid ja sertifikaate, mida on kirjeldatud 11. liite B osas.

4.5.5.2.3. Kaardi identimisandmed

365) Kontrollikaart suudab salvestada järgmisi kaardi identimisandmeid:

— kaardi number,

— väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,

— kaardi kehtivusaja algus, kaardi kehtivusaja lõpp (kui see on olemas).

4.5.5.2.4. Kaardi omaniku identimisandmed

366) Kontrollikaart suudab salvestada järgmisi kaardi omaniku identimisandmeid:

— kontrolliasutuse nimi,

— kontrolliasutuse aadress,

— omaniku perekonnanimi,

— omaniku eesnimi (eesnimed),

— eelistatav keel.

4.5.5.2.5. Andmed kontrollitegevuse kohta

367) Kontrollikaart suudab salvestada järgmisi andmeid kontrollitegevuse kohta:

— kontrolli kuupäev ja kellaaeg,

— kontrolli tüüp (kuvamine ja/või trükkimine ja/või sõidukiseadme andmete allalaadimine ja/või kaardi andmete allalaadimine ja/või teeäärne kalibreerimiskontroll),

— allalaaditud ajavahemik (kui see on olemas),

— kontrollitud VRN ja sõiduki registreerinud liikmesriik,

— kontrollitud juhikaardi number ja kaardi välja andnud liikmesriik.

368) Kontrollikaart peab suutma salvestada vähemalt 230 sellist kirjet.

4.5.6. *Ettevõttekaart*

4.5.6.1. Rakendus Tachograph (kasutatav esimese ja teise põlvkonna sõidukiseadmetes)

4.5.6.1.1. Rakenduse identimisandmed

369) Ettevõttekaart suudab salvestada järgmisi rakenduse identimisandmeid:

— sõidumeeriku rakenduse identimisandmed,

— sõidumeerikukaardi tüübi identimisandmed.

4.5.6.1.2. Võtmed ja sertifikaadid

370) Ettevõttekaart suudab salvestada mitmeid krüptograafilisi võtmeid ja sertifikaate, mida on kirjeldatud 11. liite A osas.

4.5.6.1.3. Kaardi identimisandmed

371) Ettevõttekaart suudab salvestada järgmisi kaardi identimisandmeid:

— kaardi number,

— väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,

— kaardi kehtivusaja algus, kaardi kehtivusaja lõpp (kui see on olemas).

4.5.6.1.4. Kaardi omaniku identimisandmed

372) Ettevõttekaart suudab salvestada järgmisi kaardi omaniku identimisandmeid:

— ettevõtte nimi,

— ettevõtte aadress.

4.5.6.1.5. Andmed ettevõtte tegevuse kohta

373) Ettevõttekaart suudab salvestada järgmisi andmeid ettevõtte tegevuse kohta:

— tegevuse kuupäev ja kellaaeg,

— tegevuse tüüp (sõidukiseadme lukustamine ja/või luku avamine ja/või sõidukiseadme andmete allalaadimine ja/või kaardi andmete allalaadimine),

— allalaaditud ajavahemik (kui see on olemas),

— VRN ja sõiduki registreerinud liikmesriigi ametiasutus,

— kaardi number ja kaardi välja andnud liikmesriik (kaardi andmete allalaadimise korral).

374) Ettevõttekaart peab suutma salvestada vähemalt 230 sellist kirjet.

4.5.6.2. Rakendus Tachograph G2 (ei ole kasutatav esimese põlvkonna sõidukiseadmes)

4.5.6.2.1. Rakenduse identimisandmed

375) Ettevõttekaart suudab salvestada järgmisi rakenduse identimisandmeid:

— sõidumeeriku rakenduse identimisandmed,

— sõidumeerikukaardi tüübi identimisandmed.

4.5.6.2.2. Võtmed ja sertifikaadid

376) Ettevõttekaart suudab salvestada mitmeid krüptograafilisi võtmeid ja sertifikaate, mida on kirjeldatud 11. liite B osas.

4.5.6.2.3. Kaardi identimisandmed

377) Ettevõttekaart suudab salvestada järgmisi kaardi identimisandmeid:

— kaardi number,

— väljaandnud liikmesriik, väljaandnud asutuse nimi, väljaandmise kuupäev,

— kaardi kehtivusaja algus, kaardi kehtivusaja lõpp (kui see on olemas).

4.5.6.2.4. Kaardi omaniku identimisandmed

378) Ettevõttekaart suudab salvestada järgmisi kaardi omaniku identimisandmeid:

— ettevõtte nimi,

— ettevõtte aadress.

4.5.6.2.5. Andmed ettevõtte tegevuse kohta

379) Ettevõttekaart suudab salvestada järgmisi andmeid ettevõtte tegevuse kohta:

— tegevuse kuupäev ja kellaaeg,

— tegevuse tüüp (sõidukiseadme lukustamine ja/või luku avamine ja/või sõidukiseadme andmete allalaadimine ja/või kaardi andmete allalaadimine),

— allalaaditud ajavahemik (kui see on olemas),

— VRN ja sõiduki registreerinud liikmesriigi ametiasutus,

— kaardi number ja kaardi välja andnud liikmesriik (kaardi andmete allalaadimise korral).

380) Ettevõttekaart peab suutma salvestada vähemalt 230 sellist kirjet.

5. SÕIDUMEERIKU PAIGALDAMINE

5.1. **Paigaldamine**

381) Uued sõidumeerikud tarnitakse paigaldajatele või sõidukitootjatele aktiveerimata kujul, kusjuures kõik punktis 3.21 loetletud kalibreerimisparameetrid on häälestatud kohastele ja kehtivatele vaikeväärtustele. Kui ükski konkreetne väärtus ei ole kohane, häälestatakse kirjatähelised parameetrid stringile „?“ ja numbrilised parameetrid arvule „0“. Sõidumeeriku turvalisusega seotud osade tarnimist võib turvalisuse sertifitseerimise käigus vajaduse korral piirata.

382) Enne aktiveerimist võimaldab sõidumeerik kasutada kalibreerimisfunktsiooni isegi siis, kui see ei ole kalibreerimisrežiimis.

383) Enne aktiveerimist ei registreeri ega salvesta sõidumeerik punktides 3.12.3, 3.12.9 ja 3.12.12 kuni 3.12.15 osutatud andmeid.

384) Sõidukitootjad eelhäälestavad paigaldamise ajal kõik teadaolevad parameetrid.

385) Sõidukitootjad või paigaldajad aktiveerivad paigaldatud sõidumeeriku hiljemalt enne sõiduki kasutuselevõtmist määruse (EÜ) nr 561/2006 reguleerimisalas.

386) Sõidumeerik aktiveeritakse automaatselt, kui töökojakaart sisestatakse esimest korda ühte kaardiliidestest.

387) Konkreetsed ühendamisoperatsioonid, mis võivad olla vajalikud liikumisanduri ja sõidukiseadme vahel, toimuvad automaatselt enne aktiveerimist või selle ajal.

388) Samuti toimuvad vajadusel GNSSi välisseadme ja sõidukiseadme ühendamisoperatsioonid automaatselt enne aktiveerimist või selle ajal.

389) Pärast aktiveerimist on sõidumeeriku funktsioonid ja andmetele juurdepääsu õigused täielikult kasutatavad.

390) Pärast aktiveerimist edastab sõidumeerik kaugsideseadmele turvatud andmed, mis on vajalikud sihipäraste teeäärsete kontrollide tegemiseks.

391) Pärast aktiveerimist toimivad täielikult sõidumeeriku registreerimis- ja salvestusfunktsioonid.

392) Paigaldamisele järgneb kalibreerimine. Esimene kalibreerimine ei pruugi tingimata hõlmata sõiduki registreerimisnumbri (VRN) sisestamist, kui kalibreerimist tegev tunnustatud töökoda seda ei tea. Sellises olukorras ja ainult sel ajal on sõiduki omanikul võimalik sisestada enne sõiduki kasutamist määruse (EÜ) nr 561/2006 reguleerimisalas VRN, kasutades ettevõttekaarti (nt kasutades sõidukiseadmes masina ja inimese vahelise liidese asjakohase menüüstruktuuri käske) [1]. Sellise sissekande mis tahes ajakohastamine või kinnitamine on võimalik üksnes töökojakaardi abil.

393) GNSSi välisseadme paigaldamine eeldab selle ühendamist sõidukiseadmega ja sellele järgnevat GNSSi asukohateabe kontrollimist.

394) Sõidumeerik peab asuma sõidukis sellises kohas, et juhil oleks oma kohalt juurdepääs vajalikele funktsioonidele.

[1] ELT L 102, 11.4.2006, lk 1.

5.2. **Paigaldustahvel**

395) Pärast seda, kui sõidumeerikut on paigaldamise ajal kontrollitud, kinnitatakse sellele püsiva graveeringu või trükikirjaga paigaldustahvel, mis on selgelt nähtav ja millele on kerge juurde pääseda. Juhul, kui see ei ole võimalik, paigaldatakse tahvel sõiduki B-sambale nii, et see oleks selgelt nähtav. Sõidukite puhul, millel ei ole B-sammast, tuleks paigaldustahvel kinnitada sõiduki juhipoolse ukse raamile nii, et see oleks igal juhul selgelt nähtav.

Iga kord pärast tunnustatud paigaldaja või töökoja tehtud kontrolli kinnitatakse eelmise tahvli asemele uus tahvel.

396) Tahvlile kantakse vähemalt järgmised üksikasjad:

— tunnustatud paigaldaja või töökoja nimi, aadress või ärinimi;

— sõidukit iseloomustav koefitsient kujul „w = … imp/km“;

— sõidumeeriku konstant kujul „k = … imp/km“;

— sõidumeeriku konstant kujul „l = … mm“;

— rehvimõõt;

— kuupäev, millal mõõdeti sõidukit iseloomustav koefitsient ja rehvide efektiivümbermõõt;

— sõiduki valmistajatehase tähis;

— GNSSi välisseadme olemasolu (või puudumine);

— GNSSi välisseadme seerianumber;

— kaugsideseadme seerianumber;

— kõigi paigaldatud plommide seerianumber;

— sõiduki osa, millele on paigaldatud adapter (kui see on olemas);

— sõiduki osa, millele on paigaldatud liikumisandur, kui see ei ole ühenduses käigukastiga või kui ei kasutata adapterit;

— adapteri ja sellesse sisenevaid impulsse edastava sõidukiosa vahelise kaabli värvus;

— adapteris paikneva liikumisanduri seerianumber.

397) M1- ja N1-kategooria sõidukitel, millele on paigaldatud adapter kooskõlas komisjoni määruse (EÜ) nr 68/2009 ([1]) uusima muudetud redaktsiooniga, ning juhul, kui ei ole võimalik lisada kogu nõudes 396 kirjeldatud vajalikku teavet, võib kasutada lisatahvlit. Sellisel juhul sisaldab lisatahvel vähemalt nõudes 396 kirjeldatud nelja viimast taanet.

Lisatahvli kasutamise korral paigaldatakse see nõudes 396 kirjeldatud esimese põhitahvli kõrvale või juurde ja sellele tagatakse samaväärne kaitse. Peale selle on lisatahvlil kirjas tahvli paigaldanud tunnustatud paigaldaja või töökoja nimi, aadress või kaubanimi ning paigaldamise kuupäev.

([1]) Komisjoni 23. jaanuari 2009. aasta määrus (EÜ) nr 68/2009, millega kohandatakse üheksandat korda tehnika arenguga nõukogu määrust (EMÜ) nr 3821/85 maanteevedudel kasutatavate sõidumeerikute kohta (ELT L 21, 24.1.2009, lk 3).

5.3. **Plommid**

398) Plommitakse järgmise osad:

— mis tahes ühendus, mis lahtiühendamise korral põhjustaks tuvastamatuid muudatusi või tuvastamatut andmekadu (näiteks liikumisanduri paigaldus käigukastile, M1/N1-kategooria sõidukite adapter, väline GNSSi ühendus või sõidukiseade);

— paigaldustahvel, kui see ei ole kinnitatud nii, et seda ei saa eemaldada sellel olevat märgistust kahjustamata.

399) 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 tunnustatud paigaldaja või töökoda (kooskõlas 6. peatükiga) paneb pärast kiiruspiiriku või mis tahes muu liiklusohutusseadme paigaldamist uue plommi kohe või muudel juhtudel seitsme päeva jooksul.

400) Plommide eemaldamise korral koostatakse alati pädevale asutusele esitamiseks kirjalik avaldus, milles esitatakse eemaldamise põhjus.

401) Plommidel on tootja määratud identimisnumber. See number on kordumatu ja erineb kõigist muude plommitootjate määratud plomminumbritest.

Kõnealune kordumatu identimisnumber on määratletud järgmiselt: eemaldamiskindlalt peale kantud märgistus MM NNNNNN, kus MM on tootja kordumatu identimiskood (andmebaasis registreerimist haldab EK) ning NNNNNN on tähtnumbriline plommi number, mis on tootja tegevusalas kordumatu.

402) Plommidele jäetakse vaba ruumi, kuhu tunnustatud paigaldaja, töökoda või sõidukitootja saab panna erimärgi vastavalt määruse (EL) nr 165/2014 artikli 22 lõikele 3.

Nimetatud märk ei tohi katta plommi identimisnumbrit.

403) Plommitootjad registreeritakse spetsiaalses andmebaasis ning nad avaldavad oma plommide identimisnumbrid vastavalt Euroopa Komisjoni kehtestatud korrale.

404) Tunnustatud töökojad ja sõidukitootjad kasutavad määruse (EL) nr 165/2014 kohaselt tegutsedes ainult eespool nimetatud andmebaasi kantud plommitootjate plomme.

405) Plommitootjad ja nende toodete turustajad tagavad määruse (EL) nr 165/2014 kohaselt kasutamiseks müüdud plomme käsitlevate dokumentide täieliku jälgitavuse ning on valmis esitama need vajaduse korral riigi pädevatele asutustele.

406) Plommide kordumatud identimisnumbrid peavad olema paigaldustahvlil nähtavad.

6. KONTROLL, ÜLEVAATUS JA REMONT

Nõuded määruse (EL) nr 165/2014 artikli 22 lõikes 5 osutatud asjaolude kohta, millal plomme võib eemaldada, on määratletud käesoleva lisa jaotises 5.3.

6.1. **Paigaldajate, töökodade ja sõidukitootjate tunnustamine**

Liikmesriigid tunnustavad, kontrollivad korrapäraselt ja sertifitseerivad asutusi, kes:

— paigaldavad,

— kontrollivad,

— teevad ülevaatust,

— teevad remonti.

Töökojakaarte antakse nõuetekohaselt põhjendatud vastuväidete puudumise korral välja ainult neile paigaldajatele ja/või töökodadele, kes on saanud kooskõlas käesoleva lisaga tunnustuse sõidumeerikute aktiveerimiseks ja/või kalibreerimiseks ja:

— kes ei vasta ettevõttekaardi saamise tingimustele

— ning kelle muu ametialane tegevus ei ohusta vastavalt 10. liite nõuetele süsteemi üldist turvalisust.

6.2. **Uute või parandatud seadmete kontroll**

407) Iga uue või parandatud seadme puhul tuleb kontrollida selle nõuetekohast töötamist ning näitude ja salvestuste täpsust punktides 3.2.1, 3.2.2, 3.2.3 ja 3.3 sätestatud piires; selleks seade kalibreeritakse ja plommitakse vastavalt jaotisele 5.3.

6.3. **Paigaldusjärgne kontroll**

408) Sõidukile paigaldamisel peab kogu seadeldis (sealhulgas sõidumeerik) vastama punktides 3.2.1, 3.2.2, 3.2.3 ja 3.3 sätestatud lubatud hälbe nõuetele.

6.4. **Perioodiline kontroll**

409) Sõidukile paigaldatud meeriku korraline ülevaatus toimub pärast seadme iga remonti või pärast sõidukit iseloomustava koefitsiendi või rehvide efektiivümbermõõdu iga muudatust või kui seadme koordineeritud maailmaaja näit erineb õigest ajast enam kui 20 minutit või kui muutub VRN ja kord kahe aasta jooksul (24 kuud) pärast viimast ülevaatust.

410) Ülevaatuse käigus kontrollitakse järgmist:

— sõidumeeriku nõuetekohane toimimine, sealhulgas andmete sõidumeerikukaardile salvestamise funktsioon ja side kaugsidelugejatega;

— punktides 3.2.1 ja 3.2.2 sätestatud lubatud hälbe nõuete järgimine paigaldamisel;

— punktides 3.2.3 ja 3.3 sätestatud nõuete järgimine;

— sõidumeeriku tüübikinnitusmärgi olemasolu;

— nõudes 396 määratletud paigaldustahvli ja nõudes 225 määratletud kirjeldava tahvli olemasolu;

— rehvimõõt ja rehvide tegelik ümbermõõt;

— manipuleerimisseadmete puudumine seadmel;

— plommide nõuetekohane asetus, hea seisukord, identimisnumbrite kehtivus (plommi tootja on kantud EK andmebaasi) ja identimisnumbrite vastavus paigaldustahvlil olevale märgistusele (vt nõue 401).

411) Kui leitakse, et pärast viimast kontrolli on toimunud mõni punktis 3.9 („Sündmuste ja/või vigade avastamine“) loetletud sündmus ning sõidumeeriku tootjad ja/või riiklikud ametiasutused peavad seda seadme turvalisust ohustavaks, teeb töökoda järgmist:

a. võrdleb käigukastiga ühendatud liikumisanduri indentimisandmeid sõidukiseadmes registreeritud ühendatud liikumisanduri omadega;

b. kontrollib, kas paigaldustahvlil esitatud teave vastab sõidukiseadme kirjes sisalduvale teabele;

c. kontrollib, kas liikumisanduri seerianumber ja tüübikinnitusnumber, mis on trükitud liikumisandurile, vastavad sõidukiseadme andmemälus sisalduvale teabele;

d. võrdleb GNSSi välisseadme (kui seda kasutatakse) kirjeldavale tahvlile kantud identimisandmeid sõidukiseadme andmemälus sisalduvate andmetega.

412) Töökojad märgivad kontrolliaruannetesse kõik katkiste plommide või manipuleerimisseadmete leiud. Töökoda säilitab aruandeid vähemalt kaks aastat ja teeb need taotluse korral pädevale asutusele kättesaadavaks.

413) Kõnealuste ülevaatuste käigus tehakse kalibreerimine ning asendatakse ennetavalt plommid, mille paigaldamine kuulub töökoja ülesannete hulka.

6.5. **Vigade mõõtmine**

414) 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 vahemaa on vähemalt 1 000 m;

— katsetamiseks võib kasutada alternatiivseid meetodeid, näiteks sobivat katsestendi, eeldusel et selle täpsus on võrreldav.

6.6. **Remont**

415) Töökojal peab olema võimalik sõidumeerikust andmeid alla laadida, et anda need tagasi kohasele veoettevõttele.

416) Tunnustatud 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 säilitab iga väljaantud tõendi koopiat vähemalt kaks aastat.

7. KAARDI VÄLJAANDMINE

Liikmesriikide kehtestatud kaardi väljaandmisprotsess vastab järgmistele nõuetele.

417) Taotluse esitanule esmakordselt väljaantud sõidumeerikukaardi numbris on järjestikune indeks (vajaduse korral), asendusindeks ja uuendusindeks, mis on „0“.

418) Ühele kontrolliasutusele või ühele töökojale või ühele veoettevõttele väljaantud kõigi mittenimeliste sõidumeerikukaartide numbrites on esimesed 13 kohta ühesugused ning kõigil on erinev järjestikune indeks.

419) Olemasoleva sõidumeerikukaardi asendamiseks välja antud sõidumeerikukaardil on asendatud kaardiga sama number, välja arvatud asendusindeks, mis suureneb ühe võrra (järjekorras 0, …, 9, A, …, Z).

420) Olemasoleva sõidumeerikukaardi asendamiseks väljaantud sõidumeerikukaardi kehtivusaja lõpp on sama kui asendatud kaardil.

421) Olemasoleva sõidumeerikukaardi pikendamiseks väljaantud sõidumeerikukaardil on pikendatud kaardiga sama number, välja arvatud asendusindeks, mis on nullitud, ja uuendusindeks, mis suureneb ühe võrra (järjekorras 0, …, 9, A, …, Z).

422) Haldusandmete muutmiseks vahetatud sõidumeerikukaardi puhul kohaldatakse pikendamiseeskirju, kui see toimub samas liikmesriigis, või esmakordse väljaandmise eeskirju, kui see toimub teises liikmesriigis.

423) Mittenimelisel töökoja- või kontrollikaardil märgitakse „kaardi omaniku perekonnanime“ väljale töökoja või kontrolliasutuse nimi või vastavalt liikmesriigi otsusele paigaldaja või kontrolliametniku nimi.

424) Liikmesriigid vahetavad andmeid elektrooniliselt, et tagada sõidumeeriku jaoks väljaantava juhikaardi kordumatus vastavalt määruse (EL) nr 165/2014 artiklile 31.

8. SÕIDUMEERIKU JA SÕIDUMEERIKUKAARDI TÜÜBIKINNITUS

8.1. **Üldnõuded**

Käesolevas peatükis tähendab „sõidumeerik“ „sõidumeerikut või selle osa“. Liikumisandurit, GNSSi välisseadet või kaugsideseadet sõidukiseadmega ühendava(te) juhtme(te) puhul tüübikinnitust ei nõuta. Sõidumeerikus kasutatavat paberit käsitatakse sõidumeeriku osana.

Iga tootja võib taotleda oma osa tüübikinnitust seoses mis tahes tüüpi liikumisanduri või GNSSi välisseadmega ja vastupidi, eeldusel et iga osa vastab käesoleva lisa nõuetele. Teise variandina võivad tootjad taotleda ka sõidumeeriku tüübikinnitust.

425) Sõidumeerik esitatakse tüübikinnituseks koos kõigi integreeritud lisaseadmetega.

426) Sõidumeeriku ja sõidumeerikukaartide tüübikinnitus hõlmab turvalisusega seotud katseid, funktsionaalseid katseid ja koostalitlusvõime katseid. Iga katse positiivsed tulemused kinnitatakse kohase tunnistusega.

427) Liikmesriikide tüübikinnitusasutused ei anna tüübikinnitustunnistust, kui neil ei ole:

— turvasertifikaati,

— funktsionaalsuse sertifikaati,

— koostalitlusvõime sertifikaati

sõidumeeriku või sõidumeerikukaardi kohta, mille tüübikinnitust taotletakse.

428) 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.

429) 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.

430) Varem tüübikinnituse saanud sõidumeeriku tarkvara värskendamiseks tehtavate tarkvaramuudatuste tüübikinnitusest ei tohi keelduda juhul, kui sellised muudatused mõjutavad ainult käesolevas lisas käsitlemata funktsioone. Sõidumeeriku tarkvara värskendus ei pea hõlmama uute märgistike lisamist, kui see ei ole tehniliselt teostatav.

8.2. **Turvasertifikaat**

431) Turvasertifikaat antakse käesoleva lisa 10. liite nõuete kohaselt. Sertifitseerimisele kuuluvad sõidumeeriku osad on sõidukiseade, liikumisandur, GNSSi välisseade ja sõidumeerikukaardid.

432) Erakorralistel asjaoludel, kui turvalisuse sertifitseerimise asutused keelduvad uue seadme sertifitseerimisest turbemehhanismi aegumise tõttu ja ei ole olemas määrusega kooskõlas olevat alternatiivset lahendust, jätkatakse tüübikinnituse andmist üksnes kõnealustel erilistel ja erakorralistel asjaoludel.

433) Kõnealustel asjaoludel teavitab asjaomane liikmesriik viivitamatult Euroopa Komisjoni, mis algatab kaheteistkümne kalendrikuu jooksul pärast tüübikinnituse andmist menetluse, et tagada turvalisuse algse taseme taastamine.

8.3. **Funktsionaalsuse sertifikaat**

434) Iga tüübikinnituse taotleja esitab liikmesriigi tüübikinnitusasutusele kõik materjalid ja dokumendid, mida see asutus peab vajalikuks.

435) Tootjad esitavad funktsionaalseid katseid tegema määratud labori nõutud asjakohased tüübikinnitust vajavate toodete näidised ja dokumendid ühe kuu jooksul pärast asjakohase taotluse esitamist. Kõik sellisest taotlusest tulenevad kulud kannab taotluse esitaja. Laborid tagavad mis tahes tundliku äriteabe käsitlemisel konfidentsiaalsuse.

436) Tootjale antakse funktsionaalsuse sertifikaat ainult pärast seda, kui vähemalt 9. liites määratletud kõik funktsionaalsed katsed on edukalt läbitud.

437) Funktsionaalsuse sertifikaadi annab tüübikinnitusasutus. Sertifikaadil esitatakse lisaks selle saaja nimele ja mudeli identimisandmetele üksikasjalik nimekiri sooritatud katsetest ja saadud tulemustest.

438) Sõidumeeriku mis tahes osa funktsionaalsuse sertifikaadis osutatakse ka sõidumeeriku kõikide teiste asjaomase osa sertifitseerimise eesmärgil katsetatud ühilduvate tüübikinnitusega osade tüübikinnitusnumbritele.

439) Sõidumeeriku osa funktsionaalsuse sertifikaadis esitatakse ka viide ISO või CENi standardile, millele vastavuse suhtes funktsionaalset liidest on kontrollitud.

8.4. **Koostalitlusvõime sertifikaat**

440) Koostalitlusvõime katseid teeb üks labor Euroopa Komisjoni järelevalve all ja vastutusel.

441) Labor registreerib tootjate esitatud koostalitlusvõime katsete taotlused nende saabumise järjekorras.

442) Taotlused registreeritakse ametlikult ainult siis, kui laboril on:

— kõik koostalitlusvõime katseteks vajalikud materjalid ja dokumendid,

— vastav turvasertifikaat,

— vastav funktsionaalsuse sertifikaat.

Tootjale teatatakse taotluse registreerimiskuupäev.

443) Labor ei tee koostalitlusvõime katseid sõidumeerikutega või sõidumeerikukaartidega, millel ei ole turvasertifikaati ega funktsionaalsuse sertifikaati, välja arvatud nõudes 432 kirjeldatud erakorralistel asjaoludel.

444) Iga tootja, kes taotleb koostalitlusvõime katsete tegemist, on kohustatud jätma katsete eest vastutavale laborile kõik tema poolt katsete tegemiseks esitatud materjalid ja dokumendid.

445) Koostalitlusvõime katsed tehakse vastavalt käesoleva lisa 9. liite nõuetele sõidumeeriku või sõidumeerikukaardi kõigi tüüpidega:

— mille tüübikinnitus on veel kehtiv või

— mille tüüp on kinnitamisel ja millel on kehtiv koostalitlusvõime sertifikaat.

446) Koostalitlusvõime katsed hõlmavad kõiki sõidumeerikute või sõidumeerikukaartide põlvkondi, mis on veel kasutusel.

447) Labor annab koostalitlusvõime sertifikaadi tootjale ainult pärast seda, kui kõik koostalitlusvõime katsed on edukalt sooritatud.

448) Kui koostalitlusvõime katsed ei ole ühe või mitme sõidumeeriku või sõidumeerikukaardi puhul edukad, 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 turvasertifikaat ja funktsionaalsuse sertifikaat veel kehtivad.

449) 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 funktsionaalsuse sertifikaadi.

450) Mis tahes osa, mis võiks olla koostalitlusvõime vea põhjuseks, ei kasutata kasumi teenimiseks ega turgu valitseva seisundi saamiseks.

8.5. Tüübikinnitustunnistus

451) Liikmesriigi tüübikinnitusasutus võib anda tüübikinnitustunnistuse kohe, kui ta on saanud kolm nõutavat sertifikaati.

452) Sõidumeeriku mis tahes osa tüübikinnitustunnistuses osutatakse ka sõidumeeriku kõikide teiste koostalitlusvõimeliste tüübikinnitusega osade tüübikinnitusnumbritele.

453) Tüübikinnitusasutus saadab tüübikinnitustunnistuse koopia koostalitlusvõime katsete eest vastutavale laborile samal ajal, kui ta annab selle tootjale.

454) Koostalitlusvõime katsete tegemise pädeval laboril on avalik veebisait, 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.

8.6. **Erandkord: esimeste koostalitlusvõime sertifikaatide andmine 2. põlvkonna sõidumeerikutele ja sõidumeerikukaartidele**

455) Kuni nelja kuu jooksul pärast esimeste 2. põlvkonna sõidumeerikute ja 2. põlvkonna sõidumeerikukaartide (juhi-, töökoja-, kontrolli- ja ettevõttekaardid) tunnistamist koostalitlusvõimelisteks loetakse sellel ajavahemikul registreeritud taotlustele antud koostalitlusvõime sertifikaati ajutiseks (kaasa arvatud kõige esimene).

456) Kui selle aja lõpuks on kõik asjaomased tooted tunnistatud omavahel koostalitlusvõimelisteks, muutuvad vastavad koostalitlusvõime sertifikaadid lõplikeks.

457) Kui selle aja jooksul leitakse koostalitlusvõime vigu, teeb koostalitlusvõime katsete eest vastutav labor kindlaks probleemide põhjused kõigi seotud tootjate abil ning soovitab neil teha vajalikud muudatused.

458) Kui selle aja lõpuks esineb veel koostalitlusvõime probleeme, teeb koostalitlusvõime katsete eest vastutav labor koostöös kõigi seotud tootjate ja vastavad funktsionaalsuse sertifikaadid andnud tüübikinnitusasutustega kindlaks koostalitlusvõime vigade 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.

459) Kõik koostalitusvõime katsete taotlused, mis labor on registreerinud esimese ajutise koostalitusvõime sertifikaadi andmise järgse nelja kuu möödumise ja nõudes 455 osutatud komisjoni otsuse tegemise kuupäeva vahelisel ajal, lükatakse edasi esialgsete koostalitusvõime probleemide lahendamiseni. Seejärel töödeldakse neid taotlusi nende registreerimise järjekorras.

1. liide

ANDMESÕNASTIK

SISUKORD

1. SISSEJUHATUS

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

1.1. **Andmetüüpide määratlemise viis**

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

ASN.1 tüübinimetused on antud 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 alfabeetilistest tähemärkidest koosnev ühtne jada, olenemata sellest, kuidas kasutatakse nimes suurtähti vastava tähenduse edasiandmiseks,

— üldiselt on andmetüüpide nimed seotud nende andmetüüpide nimedega, millest need on moodustatud, seadmetega, kuhu andmed on salvestatud, ja andmetega seotud funktsioonidega.

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

Võimaldamaks erinevat tüüpi kodeerimiseeskirjade kasutamist, on käesolevas liites mõnel ASN.1 kohasel tüübil piiratud väärtusvahemiku identifikaator. Väärtusvahemiku identifikaatorid on määratletud 3. peatükis ja 2. liites.

1.2. **Viited**

Käesolevas liites kasutatakse järgmisi viiteid.

ISO 639 *Codes for the representation of names of language*. („Keelenimetuste tähised“). Esimene väljaanne, 1988.

ISO 3166 Maade ja nende jaotiste nimetuste tähised. Osa 1: Maatähised. 2013.

ISO 3779 *Road vehicles – Vehicle identification number (VIN) – Content and structure* („Maanteesõidukid. Valmistajatehase tähis (VIN). Sisu ja struktuur“). 2009.

ISO/IEC 7816-5 *Identification cards – Integrated circuit cards – Part 5: Registration of application providers* („Identimiskaardid. Kiipkaardid. Osa 5: Rakendusepakkujate registreerimine“).

Teine väljaanne, 2004.

ISO/IEC 7816-6 *Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange* („Identimiskaardid. Kiipkaardid. Osa 6: Valdkondadevahelised andmeelemendid“). 2004 + 1. tehniline parandus: 2006.

ISO/IEC 8824-1 *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation* („Infotehnoloogia. Abstraktne süntaksi esitus 1 (ASN.1): põhiesituse spetsifikaat“). 2008 + 1. tehniline parandus: 2012 + 2. tehniline parandus: 2014.

ISO/IEC 8825-2 *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)* („Infotehnoloogia. ASN.1 kodeerimisreeglid: pakitud kodeerimisreeglite (PER) spetsifikaat“). 2008.

ISO/IEC 8859-1 *Information technology – 8 bit single-byte coded graphic character sets – Part 1: Latin alphabet No.1* („Infotehnoloogia. 8-bitilised ühebaidilised kodeeritud graafilised märgistikud. Osa 1: 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* („Infotehnoloogia. 8-bitilised ühebaidilised kodeeritud graafilised märgistikud. Osa 7: Ladina/kreeka tähestik“). 2003.

ISO 16844-3 *Road vehicles – Tachograph systems – Motion Sensor Interface* („Maanteesõidukid. Sõidumeerikusüsteemid. Liikumisanduri liides"). 2004 + 1. tehniline parandus: 2006.

TR-03110-3 *BSI / ANSSI Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications* („BSI / ANSSI tehniline suunis TR-03110-3. Täiustatud turbemehhanismid masinloetavate reisidokumentide jaoks ja eIDASi luba. Osa 3: Ühine spetsifikaat"). Versioon 2.20, 3. veebruar 2015.

2. ANDMETÜÜPIDE MÄÄRATLUSED

Kõigi järgnevate andmetüüpide puhul täidetakse andmeelement sisuga „teadmata" või „mittekohaldatav" vaikimisi baitidega „FF".

Kõiki andmetüüpe kasutatakse nii 1. kui ka 2. põlvkonna rakendustes, kui ei ole määratletud teisiti.

2.1. **ActivityChangeInfo**

See andmetüüp võimaldab kodeerida kahebaidilise sõna piires kaardipesa staatuse kell 00.00 ja/või juhi staatuse kell 00.00 ja/või tegevuse muutuse ja/või juhtimisstaatuse muutused ja/või juhi või kaasjuhi kaardi staatuse muutused. See andmetüüp on seotud IC lisa nõuetega 105, 266, 291, 320, 321, 343 ja 344.

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

Väärtuse omistus — okteti joondus: 'scpaatttttttttt'B (16 bitti)

Andmemälu (või kaardipesa staatuse) kirjeteks:

's'B Kaardipesa:

'0'B: JUHT,

'1'B: KAASJUHT,

'c'B Juhtimisstaatus:

'0'B: ÜKSI,

'1'B: MEESKOND,

'p'B Juhikaardi (või töökojakaardi) staatus asjaomases kaardipesas:

'0'B: SISESTATUD, kaart on sisestatud,

'1'B: SISESTAMATA, ühtki kaarti ei ole sisestatud (või kaart on välja võetud),

'aa'B Tegevus:

'00'B: PUHKEPAUS/PUHKUS,

'01'B: VALMISOLEK,

'10'B: TÖÖ,

'11'B: JUHTIMINE,

'ttttttttttt'B Muutuse aeg: minutite arv alates kellaajast 00.00 sellel päeval.

Salvestamiseks juhikaardile (või töökojakaardile) (ja juhi staatus):

‘s’B	Kaardipesa (ei ole asjakohane, kui p = 1, välja arvatud allpool oleva märkuse korral):
	‘0’B: JUHT,
	‘1’B: KAASJUHT,
‘c’B	Juhtimisstaatus (kui p = 0) või
	Järgmine tegevusstaatus (kui p = 1):
	‘0’B: ÜKSI,
	‘0’B: TEADMATA,
	‘1’B: MEESKOND,
	‘1’B: TEADA (= sisestatud käsitsi)
‘p’B	Kaardi staatus:
	‘0’B: SISESTATUD, kaart on sisestatud sõidumeerikusse,
	‘1’B: SISESTAMATA, kaarti ei ole sisestatud (või kaart on välja võetud),
‘aa’B	Tegevus (ei ole asjakohane, kui p = 1 ja c = 0, välja arvatud allpool oleva märkuse korral):
	‘00’B: PUHKEPAUS/PUHKUS,
	‘01’B: VALMISOLEK,
	‘10’B: TÖÖ,
	‘11’B: JUHTIMINE,
‘ttttttttttt’B	Muutuse aeg: minutite arv alates kellaajast 00.00 sellel päeval.

Märkus „kaardi väljavõtmise“ korral:

Kui kaart võetakse välja:

— ‘s’ on asjakohane ja näitab kaardipesa, 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 4. peatükis kindlaks määratud märgistiku,

address on kindlaksmääratud märgistikku kasutav kodeeritud aadress.

2.3. **AESKey**

2. põlvkond:

AESi võti pikkusega 128, 192 või 256 bitti.

```
AESKey ::= CHOICE {
   aes128Key                          AES128Key,
   aes192Key                          AES192Key,
   aes256Key                          AES256Key
}
```

Väärtuse omistus: täpsustamata.

2.4. **AES128Key**

2. põlvkond:

AES128 võti.

```
AES128Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes128Key                          OCTET STRING (SIZE(16))
}
```

length näitab AES128 võtme pikkust oktettides.

aes128Key on AESi võti pikkusega 128 bitti.

Väärtuse omistus:

pikkuse väärtus on 16.

2.5. **AES192Key**

2. põlvkond:

AES192 võti.

```
AES192Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes192Key                          OCTET STRING (SIZE(24))
}
```

length näitab AES192 võtme pikkust oktettides.

aes192Key on AESi võti pikkusega 192 bitti.

Väärtuse omistus:

pikkuse väärtus on 24.

2.6. **AES256Key**

2. põlvkond:

AES256 võti.

```
AES256Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes256Key                               OCTET STRING (SIZE(32))
}
```

length näitab AES256 võtme pikkust oktettides.

aes256Key on AESi võti pikkusega 256 bitti.

Väärtuse omistus:

pikkuse väärtus on 32.

2.7. **BCDString**

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

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

BCDString kasutab „hstring“-esitust. Vasakpoolseim kuueteistkümnendesituse number on esimese okteti kõige tähtsam pooloktett. Täiskordse arvu oktettide saamiseks sisestatakse vajaduse korral alates esimese okteti kõige vasakpoolsema poolokteti asukohast 0-väärtusega sabapooloktetid.

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

2.8. **CalibrationPurpose**

Kood, mis seletab, miks registreeriti kalibreerimisparameetrite kogum. See andmetüüp on seotud IB lisa nõuetega 097 ja 098 ning IC lisa nõudega 119.

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

Väärtuse omistus:

1. põlvkond:

‘00’H	reserveeritud väärtus,
‘01’H	aktiveerimine: sõidukiseadme aktiveerimishetkel teadaolevate kalibreerimisparameetrite registreerimine,
‘02’H	esimene paigaldus: sõidukiseadme esimene kalibreerimine pärast selle aktiveerimist,
‘03’H	paigaldus: sõidukiseadme esimene kalibreerimine praeguses sõidukis,
‘04’H	perioodiline kontroll.

2. põlvkond:

lisaks 1. põlvkonna puhul kasutatavatele väärtustele kasutatakse järgmisi väärtusi:

‘05’H	VRNi sisestamine ettevõtte poolt,
‘06’H	aja korrigeerimine ilma kalibreerimiseta,
‘07’H kuni ‘7F’H	RFU (reserveeritud tulevikus kasutamiseks),
‘80’H kuni ‘FF’H	tootjaomane.

2.9. **CardActivityDailyRecord**

Kaardile salvestatud teave, mis on seotud juhi tegevusega konkreetsel kalendripäeval. See andmetüüp on seotud IC lisa nõuetega 266, 291, 320 ja 343.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 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 STRINGi pikkus (vt CardActivityLengthRange, 2. liite 4. peatükk). Kui see kirje on vanim kirje päeva kohta, peab andmetüübi activityPreviousRecordLength väärtus olema 0.

activityRecordLength on selle kirje kogupikkus baitides. Maksimumväärtuse määrab ära neid andmeid sisaldava OCTET STRINGi pikkus.

activityRecordDate on kirje kuupäev.

activityDailyPresenceCounter on kaardi selle päeva kasutuskordade loendur.

activityDayDistance on kogu läbitud vahemaa sellel päeval.

activityChangeInfo on juhi ActivityChangeInfo andmete kogum sellel päeval. See võib sisaldada maksimaalselt 1440 väärtust (üks tegevusmuutus minutis). Selles kogumis on alati activityChangeInfo väärtus, mis näitab juhi staatust kell 00.00.

2.10. **CardActivityLengthRange**

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

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

Väärtuse omistus: vt 2. liide.

2.11. **CardApprovalNumber**

Kaardi tüübikinnitusnumber:

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

Väärtuse omistus:

tüübikinnitusnumber esitatakse Euroopa Komisjoni vastaval veebisaidil avaldatud kujul, nt vajaduse korral koos sidekriipsudega. Tüübikinnitusnumber joondatakse vasakule.

2.12. **CardCertificate**

1. põlvkond:

kaardi avaliku võtme sertifikaat.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Kaardile salvestatud teave, mis on seotud kaardi kiibi identimisega (IC lisa nõue 249). Andmetüübid icSerialNumber ja icManufacturingReferences võimaldavad koos kaardi kiipi kordumatult identida. Andmetüüp icSerialNumber üksinda ei võimalda kaardi kiipi kordumatult identida.

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

icSerialNumber on kiibi seerianumber.

icManufacturingReferences on kiibi tootja identifikaator.

2.14. **CardConsecutiveIndex**

Kaardi järjekorraindeks (mõiste h).

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

Väärtuse omistus: (vt IC lisa 7. peatükk).

Kasvamise järjekord: '0, …, 9, A, …, Z, a, …, z'

2.15. **CardControlActivityDataRecord**

Juhi- või töökojakaardile salvestatud teave, mis on seotud juhi suhtes läbi viidud viimase kontrolliga (IC lisa nõuded 274, 299, 327 ja 350).

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

controlType on kontrolli tüüp.

controlTime on kontrolli kuupäev ja kellaaeg.

controlCardNumber on kontrolli läbi viinud kontrolliametniku FullCardNumber.

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

controlDownloadPeriodBegin ja **controlDownloadPeriodEnd** on allalaadimise puhul alla laaditud andmetega seotud ajavahemik.

2.16. CardCurrentUse

Teave kaardi tegeliku kasutamise kohta (IC lisa nõuded 273, 298, 326 ja 349).

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

sessionOpenTime on aeg, mil kaart sisestati käsilolevaks seansiks. Kaardi väljavõtmisel määratakse selle elemendi väärtuseks null.

sessionOpenVehicle on hetkel kasutatava sõiduki identimistunnus, mis on määratud kaardi sisestamisel. Kaardi väljavõtmisel määratakse selle elemendi väärtuseks null.

2.17. CardDriverActivity

Juhi- või töökojakaardile salvestatud teave, mis on seotud juhi tegevusega (IC lisa nõuded 267, 268, 292, 293, 321 ja 344).

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

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

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

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

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

2.18. CardDrivingLicenceInformation

Juhikaardile salvestatud teave, mis on seotud andmetega kaardi omaniku juhiloa kohta (IC lisa nõuded 259 ja 284).

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

drivingLicenceIssuingAuthority on juhiloa väljaandmise eest vastutav asutus.

drivingLicenceIssuingNation on juhiloa välja andnud asutuse riik.

drivingLicenceNumber on juhiloa number.

2.19. **CardEventData**

Juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omanikuga seotud sündmustega (IC lisa nõuded 260, 285, 318 ja 341).

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

CardEventData on kirjete cardEventRecord jada EventFaultType'i väärtuse kasvavas järjestuses (välja arvatud kirjed, mis on seotud turvalisuse rikkumise katsetega, mis kogutakse kokku jada viimasesse kogumisse).

cardEventRecords on konkreetset tüüpi (või turvalisuse rikkumise katsete puhul konkreetse kategooria) sündmuste kirjete kogum.

2.20. **CardEventRecord**

Juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omanikuga seotud sündmusega (IC lisa nõuded 261, 286, 318 ja 341).

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

eventType on sündmuse tüüp.

eventBeginTime on sündmuse alguse kuupäev ja kellaaeg.

eventEndTime on sündmuse lõpu kuupäev ja kellaaeg.

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

2.21. **CardFaultData**

Juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omanikuga seotud vigadega (IC lisa nõuded 263, 288, 318 ja 341).

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

CardFaultData on jada, mis koosneb sõidumeeriku veakirjete kogumist, millele järgneb kaardi veakirjete kogum.

cardFaultRecords on konkreetse veakategooria (sõidumeerik või kaart) veakirjete kogum.

2.22. **CardFaultRecord**

Juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omanikuga seotud veaga (IC lisa nõuded 264, 289, 318 ja 341).

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

faultType on vea tüüp.

faultBeginTime on vea alguse kuupäev ja kellaaeg.

faultEndTime on vea lõpu kuupäev ja kellaaeg.

faultVehicleRegistration on selle sõiduki VRN, milles viga tekkis, ja selle sõiduki registreerinud liikmesriik.

2.23. **CardIccIdentification**

Kaardile salvestatud teave, mis on seotud kiipkaardi identimisega (IC lisa nõue 248).

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

clockStop on 2. liites määratletud režiim Clockstop.

cardExtendedSerialNumber on kiipkaardi kordumatu seerianumber, mis on täpsemalt määratletud andmetüübiga ExtendedSerialNumber.

cardApprovalNumber on kaardi tüübikinnituse number.

cardPersonaliserID on koodina ManufacturerCode kodeeritud kaardi tunnus.

embedderIcAssemblerId esitab teavet paigaldaja / kiibi koostaja kohta.

icIdentifier on kaardil oleva kiibi ja kiibi tootja identifikaator vastavalt standardile ISO/IEC 7816-6.

2.24. **CardIdentification**

Kaardile salvestatud teave, mis on seotud kaardi identimisega (IC lisa nõuded 255, 280, 310, 333, 359, 365, 371 ja 377).

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

cardIssuingMemberState on kaardi väljaandnud liikmesriigi kood.

cardNumber on kaardi number.

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.

2.25. CardMACertificate

2. põlvkond:

kaardi avaliku võtme, mida kasutatakse vastastikuseks autentimiseks sõidukiseadmega, sertifikaat. Sertifikaadi struktuuri on kirjeldatud 11. liites.

```
CardMACertificate ::= Certificate
```

2.26. 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 kordumatu identimistunnus liikmesriigis.

ownerIdentification on ettevõtte, töökoja või kontrolliasutuse unikaalne identimistunnus liikmesriigis.

cardConsecutiveIndex on kaardi järjekorraindeks.

cardReplacementIndex on kaardi asendusindeks.

cardRenewalIndex on kaardi pikendusindeks.

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

2.27. **CardPlaceDailyWorkPeriod**

Juhi- või töökojakaardile salvestatud teave, mis on seotud tööpäeva algus- ja/või lõpukohtadega (IC lisa nõuded 272, 297, 325 ja 348).

```
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.

2.28. **CardPrivateKey**

1. põlvkond:

kaardi privaatvõti.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Kaardi avalik võti.

```
CardPublicKey ::= PublicKey
```

2.30. **cardRenewalIndex**

Kaardi pikendusindeks (mõiste i).

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

Väärtuse omistus: (vt käesoleva lisa 7. peatükk).

‘0’ esimene väljaanne.

Kasvamise järjekord: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

Kaardi asendusindeks (mõiste j).

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

Väärtuse omistus: (vt käesoleva lisa 7. peatükk).

‘0’ originaalkaart.

Kasvamise järjekord: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

2. põlvkond:

kaardi avaliku allkirjavõtme sertifikaat. Sertifikaadi struktuuri on kirjeldatud 11. liites.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Sõidukiseadme kahe kaardipesa eristuskood.

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

Väärtuse omistus: täpsustamata.

2.34. **CardSlotsStatus**

Kood, mis tähistab sõidukiseadme kahte kaardipesasse sisestatud kaartide tüüpi.

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

Väärtuse omistus — okteti joondus: 'ccccdddd'B

'cccc'B kaasjuhikaardi pesasse sisestatud kaardi tüübi identimistunnus,

'dddd'B juhikaardi pesasse sisestatud kaardi tüübi identimistunnus,

järgmiste identimiskoodidega:

'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 ettevõttekaart.

2.35. **CardSlotsStatusRecordArray**

2. põlvkond:

CardSlotsStatus ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (CardSlotsStatus). **Väärtuse omistus:** vt RecordType.

recordSize on kirje CardSlotsStatus maht baitides.

noOfWRecords on kirjete kogumis sisalduv kirjete arv.

records on CardSlotsStatus-kirjete kogum.

2.36. **CardStructureVersion**

Kood, mis näitab sõidumeerikukaardi rakendusstruktuuri versiooni.

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

Väärtuse omistus: 'aabb'H:

'aa'H struktuurimuutuste indeks.

'00'H 1. põlvkonna rakendustele

'01'H 2. põlvkonna rakendustele

'bb'H muutuste indeks seoses andmeelementide kasutamisega, mis on antud struktuuri tarvis määratletud suurima kaaluga baidiga.

'00'H 1. põlvkonna rakenduste sellel versioonile

'00'H 2. põlvkonna rakenduste sellel versioonile

2.37. **CardVehicleRecord**

Juhi- või töökojakaardile salvestatud teave, mis on seotud sõiduki kasutusajaga kalendripäevas (IC lisa nõuded 269, 294, 322 ja 345).

1. põlvkond:

```
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 VRN ja sõiduki registreerinud liikmesriik.

vuDataBlockCounter on loenduri VuDataBlockCounter väärtus sõiduki kasutusaja viimasel väljavõttel.

2. põlvkond:

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

Lisaks 1. põlvkonnale kasutatakse järgmist andmeelementi:

VehicleIdentificationNumber on sõidukit kui tervikut tähistav valmistajatehase tähis.

2.38. **CardVehiclesUsed**

Juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omaniku kasutatud sõidukitega (IC lisa nõuded 270, 295, 323 ja 346).

```
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.

2.39. **CardVehicleUnitRecord**

2. põlvkond:

juhi- või töökojakaardile salvestatud teave, mis on seotud kasutatud sõidukiseadmega (IC lisa nõuded 303 ja 351).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                           TimeReal,
   manufacturerCode                    ManufacturerCode,
   deviceID                            INTEGER(0..255),
   vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp on sõidukiseadme kasutamise alguse kuupäev ja kellaaeg (st kaardi esimene sisestamine sõidukiseadmesse sellel kasutusajal).

manufacturerCode on sõidukiseadme tootja tunnus.

deviceID on tootja sõidukiseadme tüübi tunnus. Selle väärtus on tootjaomane.

vuSoftwareVersion on sõidukiseadme tarkvaraversiooni number.

2.40. **CardVehicleUnitsUsed**

2. põlvkond:

juhi- või töökojakaardile salvestatud teave, mis on seotud kaardi omaniku kasutatud sõidukiseadmetega (IC lisa nõuded 306 ja 352).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord on viimase ajakohastatud sõidukiseadme kirje indeks.

Väärtuse omistus: number, mis vastab sõidukiseadme kirjete lugejale, alates nullist sõidukiseadme kirje esimesel esinemisel struktuuris.

cardVehicleUnitRecords on kirjete kogum, mis sisaldab teavet kasutatud sõidukiseadmete kohta.

2.41. **Certificate**

Sertifitseerimisasutuse väljaantud avaliku võtme sertifikaat.

1. põlvkond:

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

Väärtuse omistus: digitaalallkiri koos andmetüübi CertificateContent osalise taaskasutamisega vastavalt 11. liitele „Ühised turbemehhanismid“: allkiri (128 baiti) || avaliku võtme jääk (58 baiti) || sertifitseerimisasutuse viitenumber (8 baiti).

2. põlvkond:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Väärtuse omistus: vt 11. liide.

2.42. **CertificateContent**

1. põlvkond:

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 identib sertifikaadi väljaandnud asutuse. See viitab ka selle sertifitseerimisasutuse avalikule võtmele.

certificateHolderAuthorisation identib sertifikaadi omaniku õigused.

certificateEndOfValidity on kuupäev, mil sertifikaadi halduskehtivus lõpeb.

certificateHolderReference identib kaardi omaniku. See viitab ka tema avalikule võtmele.

publicKey on selle sertifikaadiga tõendatud avalik võti.

2.43. **CertificateHolderAuthorisation**

Sertifikaadi omaniku õiguste identimine.

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

1. põlvkond:

tachographApplicationID on sõidumeerikurakenduse identifikaator.

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

equipmentType on seadmetüübi, mille jaoks sertifikaat on ette nähtud, identimistunnus.

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

2. põlvkond:

tachographApplicationID tähistab 2. põlvkonna sõidumeerikukaardi rakendusidentifikaatori (AID) kuut kõige tähtsamat baiti. Sõidumeerikukaardi rakenduse AID spetsifikatsioon on esitatud punktis 6.2.

Väärtuse omistus: 'FF 53 4D 52 44 54'.

equipmentType on sertifikaadis käsitletud 2. põlvkonna seadme tüübi identimistunnus.

Väärtuse omistus: vastavalt andmetüübile EquipmentType.

2.44. **CertificateRequestID**

Sertifitseerimistaotluse unikaalne identimistunnus. Seda saab kasutada ka sõidukiseadme avaliku võtme identifikaatorina, kui sõidukiseadme, mille jaoks võti on ette nähtud, seerianumber ei ole sertifikaadi loomise ajal teada.

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

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

requestMonthYear on sertifitseerimistaotluse kuu ja aasta identimistunnus.

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

crIdentifier on laiendatud seerianumbrilt pärineva sertifitseerimistaotluse eristamisidentifikaator.

Väärtuse omistus: 'FFh'.

manufacturerCode on sertifikaati taotleva tootja numbrikood.

2.45. **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 (sõltub konkreetsest sertifitseerimisasutusest).

caIdentifier on identifikaator, mis eristab sertifitseerimisasutuse võtme identifikaatorit muudest võtmeidentifikaatoritest.

Väärtuse omistus: '01h'.

2.46. **CompanyActivityData**

Ettevõttekaardile salvestatud teave, mis on seotud kaardiga tehtud tegevusega (IC lisa nõuded 373 ja 379).

```
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 ettevõtte ühe tegevusega seotud teabe jada.

companyActivityType on ettevõtte tegevuse tüüp.

companyActivityTime on ettevõtte tegevuse kuupäev ja kellaaeg.

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

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

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

2.47. **CompanyActivityType**

Kood, mis näitab ettevõtte tegevust ettevõttekaardi kasutamisel.

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

2.48. **CompanyCardApplicationIdentification**

Ettevõttekaardile salvestatud teave, mis on seotud kaardirakenduse identimisega (IC lisa nõuded 369 ja 375).

```
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.

2.49. **CompanyCardHolderIdentification**

Ettevõttekaardile salvestatud teave, mis on seotud kaardi omaniku identimisega (IC lisa nõuded 372 ja 378).

```
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.

2.50. **ControlCardApplicationIdentification**

Kontrollikaardile salvestatud teave, mis on seotud kaardirakenduse identimisega (IC lisa nõuded 357 ja 363).

```
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.

2.51. **ControlCardControlActivityData**

Kontrollikaardile salvestatud teave, mis on seotud kaardiga tehtud kontrollitegevusega (IC lisa nõuded 361 ja 367).

```
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 kirjete lugejale, alates nullist kontrollitegevuse kirje esimesel esinemisel struktuuris.

controlActivityRecords on kõigi kontrollitegevuse kirjete kogum.

controlActivityRecord on ühe kontrolliga seotud teabe jada.

controlType on kontrolli tüüp.

controlTime on kontrolli kuupäev ja kellaaeg.

controlledCardNumber on kontrollitud kaardi number ja kaardi välja andnud liikmesriik.

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

controlDownloadPeriodBegin ja **controlDownloadPeriodEnd** on tegelikult alla laaditud andmetega seotud ajavahemik.

2.52. **ControlCardHolderIdentification**

Kontrollikaardile salvestatud teave, mis on seotud kaardi omaniku identimisega (IC lisa nõuded 360 ja 366).

```
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.

2.53. **ControlType**

Kontrolli käigus läbi viidud tegevuste kood. See andmetüüp on seotud IC lisa nõuetega 126, 274, 299, 327 ja 350.

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

1. põlvkond:

Väärtuse omistus — okteti joondus: ‘cvpdxxxx’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 sõidukiseadmest allalaadimine:

‘0’B: selle kontrollitegevuse käigus ei ole sõidukiseadmest alla laaditud,

‘1’B: selle kontrollitegevuse käigus on sõidukiseadmest 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 kasutamata.

2. põlvkond:

Väärtuse omistus – okteti joondus: ‘cvpdexxx’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 sõidukiseadmest allalaadimine:

‘0’B: selle kontrollitegevuse käigus ei ole sõidukiseadmest alla laaditud,

‘1’B: selle kontrollitegevuse käigus on sõidukiseadmest 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

‘e’B	teeäärne kalibreerimiskontroll:
	‘0’B: selle kontrollitegevuse käigus ei ole kalibreerimisparameetreid kontrollitud,
	‘1’B: selle kontrollitegevuse käigus kontrolliti kalibreerimisparameetreid
‘xxx’B	reserveeritud kasutuseks tulevikus.

2.54. **CurrentDateTime**

Sõidumeeriku jooksev kuupäev ja kellaaeg.

```
CurrentDateTime ::= TimeReal
```

Väärtuse omistus: täpsustamata.

2.55. **CurrentDateTimeRecordArray**

2. põlvkond:

Jooksev kuupäev ja kellaaeg ning metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (CurrentDateTime). **Väärtuse omistus:** vt RecordType.

recordSize on kirje CurrentDateTime maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on jooksva kuupäeva ja kellaaja kirjete kogum.

2.56. **DailyPresenceCounter**

Juhi- või töökojakaardile salvestatud loendur, mis suureneb ühe võrra igal kalendripäeval, millal kaart on sõidukiseadmesse sisestatud. See andmetüüp on seotud IC lisa nõuetega 266, 299, 320 ja 343.

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

Väärtuse omistus: järjestikune number suurima väärtusega 9999, algab uuesti nullist. Kaardi esmakordse väljaandmise ajal on see number 0.

2.57. **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.

2.58. **DateOfDayDownloaded**

2. põlvkond:

allalaadimise kuupäev ja kellaaeg.

```
DateOfDayDownloaded ::= TimeReal
```

Väärtuse omistus: täpsustamata.

2.59. **DateOfDayDownloadedRecordArray**

2. põlvkond:

Allalaadimise kuupäev ja kellaaeg ning metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (DateOfDayDownloaded). **Väärtuse omistus:** vt RecordType.

recordSize on kirje CurrentDateTime maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on allalaadimise kuupäeva ja kellaaja kirjete kogum.

2.60. **Distance**

Läbitud vahemaa (sõiduki läbisõidumõõdiku kahe näidu vahe arvutamise tulemus kilomeetrites).

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

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

2.61. **DriverCardApplicationIdentification**

Juhikaardile salvestatud teave, mis on seotud kaardirakenduse identimisega (IC lisa nõuded 253 ja 278).

1. põlvkond:

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

noOfFaultsPerType on veatüübi kaupa vigade 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. põlvkond:

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

Lisaks 1. põlvkonnale kasutatakse järgmisi andmeelemente:

noOfGNSSCDRecords on arv, mitu GNSSi pideva juhtimisaja kirjet kaart mahutab.

noOfSpecificConditionRecords on arv, mitu eritingimuste kirjet kaart mahutab.

2.62. DriverCardHolderIdentification

Juhikaardile salvestatud teave, mis on seotud kaardi omaniku identimisega (IC lisa nõuded 256 ja 281).

```
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.

2.63. DSRCSecurityData

2. põlvkond:

Lihttekstina esitatav teave ja MAC, mis saadetakse DSRC kaudu sõidumeerikust kaugpäringusaatjasse (*Remote Interrogator*, RI); üksikasjalik teave on esitatud 11. liite B osa 13. peatükis.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength on DER-TLV-kodeeringu osa, mille väärtuseks määratakse '81 10' (vt 11. liite B osa 13. peatükk).

currentDateTime on sõidukiseadme jooksev kuupäev ja kellaaeg.

counter loendab RTM-sõnumeid.

vuSerialNumber on sõidukiseadme seerianumber.

dSRCMKVersionNumber on DSRC peavõtme versiooni number, millest on tuletatud konkreetse sõidukiseadme DSRC võtmed.

tagLengthMac on DER-TLV-kodeeringusse kuuluva MAC-andmeobjekti silt ja pikkus. Sildi väärtuseks määratakse '8E', pikkuse kirjes kodeeritakse MACi pikkus oktettides (vt 11. liite B osa 13. peatükk).

mac on RTM-sõnumi vahenduselt arvutatud MAC (vt 11. liite B osa 13. peatükk).

2.64. EGFCertificate

2. põlvkond:

GNSSi välisseadme avaliku võtme, mida kasutatakse vastastikuseks autentimiseks sõidukiseadmega, sertifikaat. Sertifikaadi struktuuri on kirjeldatud 11. liites.

```
EGFCertificate ::= Certificate
```

2.65. EmbedderIcAssemblerId

Esitab teavet kiibi paigaldaja kohta.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode mooduli paigaldaja kahetäheline riigikood vastavalt standardile ISO 3166.

moduleEmbedder idendib mooduli paigaldaja.

manufacturerInformation tootja sisemiseks kasutamiseks.

2.66. EntryTypeDailyWorkPeriod

Kood tööpäeva kohakirje alguse ja lõpu eristamiseks ja kirjetingimus.

1. põlvkond

```
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. põlvkond

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Väärtuse omistus: vastavalt standardile ISO/IEC8824-1.

2.67. EquipmentType

Kood sõidumeerikurakenduse erinevate sõidumeerikutüüpide eristamiseks.

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

1. põlvkond:

```
--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/IEC8824-1.

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

2. põlvkond:

Kasutatakse samu väärtusi nagu 1. põlvkonna puhul koos järgmiste täiendustega:

```
--GNSS Facility                          (8),
--Remote Communication Module            (9),
--ITS interface module                   (10),
--Plaque                                 (11), -- may be used in SealRecord
--M1/N1 Adapter                          (12), -- may be used in SealRecord
--European Root CA (ERCA)                (13),
--Member State CA (MSCA)                 (14),
--External GNSS connection               (15), -- may be used in SealRecord
--Unused                                 (16), -- used in SealDataVu
--RFU                                    (17..255)
```

Märkus: Kirjete Plaque, Adapter ja External GNSS connection 2. põlvkonna väärtusi ning kirjete Vehicle Unit ja Motion Sensor 1. põlvkonna väärtusi võib vajaduse korral kasutada kirjes *SealRecord*.

2.68. **EuropeanPublicKey**

1. põlvkond:

Euroopa avalik võti.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

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

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

Väärtuse omistus:

'00'H	üks kümnest hiliseimast (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 rike
'07'H	aktiivne/kestev sündmus või rike
'08'H to '7F'H	reserveeritud tulevikus kasutamiseks
'80'H to 'FF'H	tootjaomane

2.70. **EventFaultType**

Sündmust või viga täpsustav kood.

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

Väärtuse omistus:

1. põlvkond:

'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	voolukatkestus,
'09'H	liikumisandmete viga,
'0A'H	vastuolu sõiduki liikumisandmetes,
'0B' to '0F'H	reserveeritud tulevikus kasutamiseks,

	sõidukiseadmega seotud turvalisuse rikkumise katseid käsitlevad sündmused,
‘1x’H	üksikasjad puuduvad,
‘10’H	liikumisanduri autentimistõrge,
‘11’H	sõidumeerikukaardi autentimistõrge,
‘12’H	liikumisanduri lubamatu muutus,
‘13’H	kaardi andmesisestuse terviklikkusviga,
‘14’H	salvestatud kasutajaandmete terviklikkuse viga,
‘15’H	sisemine andmeedastusviga,
‘16’H	korpuse lubamatu avamine,
‘17’H	manipulatsioon riistvaraga,
‘18’H	reserveeritud tulevikus kasutamiseks,
‘19’H to ‘1F’H	
‘2x’H	anduriga seotud turvalisuse rikkumise katseid käsitlevad sündmused,
‘20’H	üksikasjad puuduvad,
‘21’H	autentimistõrge,
‘22’H	salvestatud andmete terviklikkuse viga,
‘23’H	sisemine andmeedastusviga,
‘24’H	korpuse lubamatu avamine,
‘25’H	manipulatsioon riistvaraga,
‘26’H to ‘2F’H	reserveeritud tulevikus kasutamiseks,
‘3x’H	sõidumeerikuvead,
‘30’H	üksikasjad puuduvad,
‘31’H	sõidukiseadme siseviga,
‘32’H	printeri viga,
‘33’H	kuvari viga,
‘34’H	allalaadimise viga,
‘35’H	anduri viga,
‘36’H to ‘3F’H	reserveeritud tulevikus kasutamiseks,
‘4x’H	kaardivead,
‘40’H	üksikasjad puuduvad,
‘41’H to ‘4F’H	reserveeritud tulevikus kasutamiseks,
‘50’H to ‘7F’H	reserveeritud tulevikus kasutamiseks,
‘80’H to ‘FF’H	tootjaomane.

2. põlvkond:

Kasutatakse samu väärtusi nagu 1. põlvkonna puhul koos järgmiste täiendustega:

‘0B’H	ajakonflikt (GNSSi kellaaja ja sõidukiseadme sisekella võrdlus)
‘0C’ to ‘0F’H	reserveeritud tulevikus kasutamiseks,
‘5x’H	GNSSiga seotud vead,
‘50’H	üksikasjad puuduvad,
‘51’H	GNSSi sisemise vastuvõtja viga,
‘52’H	GNSSi välisvastuvõtja viga,
‘53’H	GNSSi välisseadmega side pidamise viga,
‘54’H	GNSSi asukohaandmed puuduvad,
‘55’H	GNSSi seadmega manipuleerimise tuvastamine,
‘56’H	GNSSi välisseadme sertifikaat aegunud,
‘57’H to ‘5F’H	reserveeritud tulevikus kasutamiseks,
‘6x’H	kaugsidemooduliga seotud vead,
‘60’H	üksikasjad puuduvad,
‘61’H	kaugsidemooduli viga,
‘62’H	kaugsidemooduliga side pidamise viga,
‘63’H to ‘6F’H	reserveeritud tulevikus kasutamiseks,
‘7x’H	ITSi liidese vead,
‘70’H	üksikasjad puuduvad,
‘71’H to ‘7F’H	reserveeritud tulevikus kasutamiseks.

2.71. **ExtendedSealIdentifier**

2. põlvkond:

Laiendatud plommiidentifikaatori abil identitakse plommi (IC lisa nõue 401).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode on plommi tootja kood.

sealIdentifier plommi identifikaator, mis on tootja puhul kordumatu.

2.72. **ExtendedSerialNumber**

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

1. põlvkond:

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

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

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

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

type on seadmetüübi identifikaator.

Väärtuse omistus: tootjaomane, reserveeritud väärtusega 'FFh'.

manufacturerCode on tüübikinnitusega seadme tootjat identiv kood.

2. põlvkond:

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

serialNumber vt 1. põlvkond.

monthYear vt 1. põlvkond.

type idendib seadme tüübi.

manufacturerCode vt 1. põlvkond.

2.73. **FullCardNumber**

Sõidumeerikukaarti 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.

2.74. **FullCardNumberAndGeneration**

2. põlvkond:

Sõidumeerikukaarti ja selle põlvkonda täielikult identiv kood.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identib sõidumeerikukaardi.

generation näitab kasutatava sõidumeerikukaardi põlvkonda.

2.75. **Generation**

2. põlvkond:

Näitab kasutatava sõidumeerikukaardi põlvkonda.

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

Väärtuse omistus:

'00'H	reserveeritud tulevikus kasutamiseks
'01'H	1. põlvkond
'02'H	2. põlvkond
'03'H .. 'FF'H	reserveeritud tulevikus kasutamiseks

2.76. **GeoCoordinates**

2. põlvkond:

Geokoordinaadid kodeeritakse täisarvudena. Nendeks arvudeks on laiuskraadide puhul koodi ±DDMM.M kordarvud ja pikkuskraadide puhul koodi ±DDDMM.M kordarvud. Siin tähistavad ±DD ja ±DDD kraade ning MM.M tähistab minuteid.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude kodeeritakse koodi ±DDMM.M esituse kordarvuna (kordaja 10).

longitude pikkus kodeeritakse koodi ±DDDMM.M esituse kordarvuna (kordaja 10).

2.77. **GNSSAccuracy**

2. põlvkond:

GNSSi asukohaandmete täpsus (mõiste eee)). Täpsus kodeeritakse täisarvuna ning on GSA NMEA lausest saadud X.Y väärtuse kordarv (kordaja 10).

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

2. põlvkond:

juhi- või töökojakaardile salvestatud teave, mis on seotud sõiduki asukohaga GNSSi järgi hetkel, kui juhil täitub kolm järjestikust sõidutundi (IC lisa nõuded 306 ja 354).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord            INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords         SET SIZE(NoOfGNSSCDRecords) OF
                                        GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord viimase ajakohastatud GNSSi pideva juhtimisaja kirje indeks.

Väärtuse omistus: number, mis vastab GNSSi pideva juhtimisaja kirjete lugejale, alates nullist GNSSi pideva juhtimisaja kirje esimesel esinemisel struktuuris.

gnssContinuousDrivingRecords kirjete kogum, mis sisaldab teavet kuupäeva, kellaaja ja sõiduki asukoha kohta hetkel, kui täitub kolm järjestikust sõidutundi.

2.79. **GNSSContinuousDrivingRecord**

2. põlvkond:

juhi- või töökojakaardile salvestatud teave, mis on seotud sõiduki asukohaga GNSSi järgi hetkel, kui juhil täitub kolm järjestikust sõidutundi (IC lisa nõuded 305 ja 353).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssPlaceRecord                      GNSSPlaceRecord
}
```

timeStamp on kuupäev ja kellaaeg, mil kaardi omanikul täitub kolm järjestikust sõidutundi.

gnssPlaceRecord sisaldab sõiduki asukohaga seotud teavet.

2.80. **GNSSPlaceRecord**

2. põlvkond:

teave, mis on seotud sõiduki asukohaga GNSSi järgi (IC lisa nõuded 108, 109, 110, 296, 305, 347 ja 353).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssAccuracy                         GNSSAccuracy,
   geoCoordinates                       GeoCoordinates
}
```

timeStamp on kuupäev ja kellaaeg, mil määrati kindlaks sõiduki asukohta GNSSi järgi.

gnssAccuracy on GNSSi asukohaandmete täpsus.

geoCoordinates on GNSSi abil registreeritud asukoht.

2.81. **HighResOdometer**

Sõiduki läbisõidumõõdiku näit: sõiduki töötamise ajal läbitud kogu vahemaa.

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

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

2.82. **HighResTripDistance**

Kogu reisi või selle osa jooksul läbitud vahemaa.

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

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

2.83. **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.

2.84. **InternalGNSSReceiver**

2. põlvkond:

teave selle kohta, kas GNSSi vastuvõtja asub sõidukiseadmes või sellest väljaspool. Väärtuse *True* korral asub GNSSi vastuvõtja sõidukiseadmes. Väärtuse *False* korral asub GNSSi vastuvõtja sõidukiseadmest väljaspool.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Sõidumeeriku konstant (mõiste m).

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

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

2.86. **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 sõidukiseadme või sõidumeerikukaardi avalikule võtmele viitamiseks.

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

Kolmas valik sobib liikmesriigi avalikule võtmele viitamiseks.

2.87. **KMWCKey**

2. põlvkond:

AESi võti ja selle versiooniteave, mida kasutatakse sõidukiseadme ja liikumisanduri ühendamiseks. Üksikasjalik teave on esitatud 11. liites.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                             AESKey,
   keyVersion                          INTEGER (SIZE(1))
}
```

kMWCKey on AESi võtme pikkus, mis on ühendatud sõidukiseadme ja liikumisanduri ühendamisel kasutatava võtmega.

keyVersion näitab AESi võtme versiooni.

2.88. **Language**

Keelt identiv kood.

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

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

2.89. **LastCardDownload**

Juhikaardile salvestatud kaardilt viimase (muul eesmärgil kui kontrolliks) allalaadimise kuupäev ja kellaaeg (IC lisa nõuded 257 ja 282). Seda kuupäeva saab ajakohastada sõidukiseade või mis tahes kaardilugeja.

```
LastCardDownload ::= TimeReal
```

Väärtuse omistus: täpsustamata.

2.90. **LinkCertificate**

2. põlvkond:

Euroopa juursertifitseerimisasutuse võtmepaaride vahelise lingi sertifikaat.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Rattarehvide efektiivümbermõõt (mõiste u).

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

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

2.92. **MAC**

2. põlvkond:

8, 12 või 16 baidi pikkune krüptograafiline kontrollsumma, mis vastab 11. liites kirjeldatud šifrikomplektidele.

```
MAC ::= CHOICE {
   mac8                                 OCTET STRING (SIZE(8)),
   mac12                                OCTET STRING (SIZE(12)),
   mac16                                OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Kood, mis näitab, kas kaardi omanik on juhi tegevusi kaardi sisestamisel käsitsi sisestanud või mitte (IB lisa nõue 081 ja IC lisa nõue 102).

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

Väärtuse omistus: täpsustamata.

2.94. **ManufacturerCode**

Tüübikinnitusega seadme tootjat identiv kood.

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

Koostalitlusvõime katseid tegev labor säilitab ja avaldab tootjakoodide loetelu oma veebisaidil (IC lisa nõue 454).

Sõidumeerikute arendajatele määratakse ajutiselt tootjakood (ManufacturerCode), kui on esitatud taotlus koostalitlusvõime katseid tegevale laborile.

2.95. **ManufacturerSpecificEventFaultData**

2. põlvkond:

tootjaomased veakoodid, mis lihtsustavad vigade analüüsi ja sõidukiseadmete hooldust.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                     ManufacturerCode,
   manufacturerSpecificErrorCode        OCTET STRING(SIZE(3))
}
```

manufacturerCode on sõidukiseadme tootja tunnus.

manufacturerSpecificErrorCode on tootjaomane veakood.

2.96. **MemberStateCertificate**

Euroopa sertifitseerimisasutuse väljaantud liikmesriigi avaliku võtme sertifikaat.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

2. põlvkond:

liikmesriigi sertifikaat ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (MemberStateCertificate). **Väärtuse omistus:** vt RecordType.

recordSize on kirje MemberStateCertificate maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv. Selle väärtuseks määratakse 1, kuna sertifikaadid võivad olla erineva pikkusega.

records on liikmesriigi sertifikaatide kogum.

2.98. **MemberStatePublicKey**

1. põlvkond:

liikmesriigi avalik võti.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Nimi.

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

codePage määratleb 4. peatükis kindlaks määratud märgistiku,

name on kindlaksmääratud märgistiku abil kodeeritud nimi.

2.100. **NationAlpha**

Tähestikuline viide riigile vastavalt rahvusvahelises liikluses sõidukitel kasutatavatele eristusmärkidele (ÜRO maanteeliiklust käsitlev Viini 1968. aasta konventsioon).

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

Koodid Nation Alpha ja Nation Numeric sisalduvad loetelus, mida säilitatakse koostalitlusvõime katseid tegema määratud labori veebisaidil vastavalt IC lisa nõudele 440.

2.101. **NationNumeric**

Numbriline viide riigile.

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

Väärtuse omistus: vt andmetüüp 2.100 (NationAlpha).

Eespool kirjeldatud koodi Nation Alpha või Nation Numeric määratlust muudetakse või ajakohastatakse üksnes pärast seda, kui määratud laborile on arvamuse esitanud tüübikinnitusega digitaalsete sõidumeerikute ja arukate sõidumeerikute sõidukiseadmete tootjad.

2.102. **NoOfCalibrationRecords**

Kalibreerimiskirjete arv, mida saab töökojakaardile salvestada.

1. põlvkond:

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

Väärtuse omistus: vt 2. liide.

2. põlvkond:

$$\texttt{NoOfCalibrationRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Väärtuse omistus: vt 2. liide.

2.103. **NoOfCalibrationsSinceDownload**

Loendur, mis näitab töökojakaardiga tehtud viimase allalaadimise järgset kalibreerimiste arvu (IC lisa nõuded 317 ja 340).

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

Väärtuse omistus: täpsustamata.

2.104. **NoOfCardPlaceRecords**

Kohakirjete arv, mida saab juhi- või töökojakaardile salvestada.

1. põlvkond:

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

Väärtuse omistus: vt 2. liide.

2. põlvkond:

$$\texttt{NoOfCardPlaceRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Väärtuse omistus: vt 2. liide.

2.105. **NoOfCardVehicleRecords**

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

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

Väärtuse omistus: vt 2. liide.

2.106. **NoOfCardVehicleUnitRecords**

2. põlvkond:

kasutatud sõidukiseadmete kirjete arv, mida saab juhi- või töökojakaardile salvestada.

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

Väärtuse omistus: vt 2. liide.

2.107. **NoOfCompanyActivityRecords**

Ettevõtte tegevuskirjete arv, mida saab ettevõttekaardile salvestada.

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

Väärtuse omistus: vt 2. liide.

2.108. **NoOfControlActivityRecords**

Kontrollitegevuse kirjete arv, mida saab kontrollikaardile salvestada.

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

Väärtuse omistus: vt 2. liide.

2.109. **NoOfEventsPerType**

Sündmuste arv sündmuse tüübi kohta, mida saab kaardile salvestada.

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

Väärtuse omistus: vt 2. liide.

2.110. **NoOfFaultsPerType**

Vigade arv veatüübi kohta, mida saab kaardile salvestada.

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

Väärtuse omistus: vt 2. liide.

2.111. **NoOfGNSSCDRecords**

2. põlvkond:

GNSSi pideva juhtimisaja kirjete arv, mida saab kaardile salvestada.

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

Väärtuse omistus: vt 2. liide.

2.112. **NoOfSpecificConditionRecords**

2. põlvkond:

eritingimuste kirjete arv, mida saab kaardile salvestada.

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

Väärtuse omistus: vt 2. liide.

2.113. **OdometerShort**

Sõiduki läbisõidumõõdiku näit lühikujul.

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

Väärtuse omistus: kindlaks määramata kahendarv. Väärtus 1/200 km vahemikus 0 kuni 9 999 999 km.

2.114. **OdometerValueMidnight**

Sõiduki läbisõidumõõdiku näit antud päeva kesköö (IB lisa nõue 090 ja IC lisa nõue 113).

```
OdometerValueMidnight ::= OdometerShort
```

Väärtuse omistus: täpsustamata.

2.115. **OdometerValueMidnightRecordArray**

2. põlvkond:

OdometerValueMidnight ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (OdometerValueMidnight). **Väärtuse omistus:** vt RecordType.

recordSize on kirje OdometerValueMidnight maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on OdometerValueMidnight-kirjete kogum.

2.116. **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.

2.117. **PlaceRecord**

Tööpäeva algus- või lõpukohaga seotud teave (IC lisa nõuded 108, 271, 296, 324 ja 347).

1. põlvkond:

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

entryTime on kirjega seotud kuupäev ja kellaaeg.

entryTypeDailyWorkPeriod on kirje tüüp.

dailyWorkPeriodCountry on sisestatud riik.

dailyWorkPeriodRegion on sisestatud piirkond.

vehicleOdometerValue on läbisõidumõõdiku näit koha sisestamise ajal.

2. põlvkond:

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

Lisaks 1. põlvkonnale kasutatakse järgmist komponenti:

entryGNSSPlaceRecord on registreeritud asukoht ja kellaaeg.

2.118. **PreviousVehicleInfo**

Teave juhi poolt varem kasutatud sõiduki kohta, kui ta sisestab oma kaardi sõidukiseadmesse (IB lisa nõue 081 ja IC lisa nõue 102).

1. põlvkond:

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

vehicleRegistrationIdentification on VRN ja sõiduki registreerinud liikmesriik.

cardWithdrawalTime on kaardi väljavõtmise kuupäev ja kellaaeg.

2. põlvkond:

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

Lisaks 1. põlvkonnale kasutatakse järgmist andmeelementi:

vuGeneration näitab sõidukiseadme põlvkonda.

2.119. **PublicKey**

1. põlvkond:

avalik RSA võti.

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

rsaKeyModulus on võtmepaari moodul.

rsaKeyPublicExponent on võtmepaari avalik eksponent.

2.120. **RecordType**

2. põlvkond:

viide kirje tüübile. Seda andmetüüpi kasutatakse RecordArray-kirjetes.

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

Väärtuse omistus:

'01'H	ActivityChangeInfo,
'02'H	CardSlotsStatus,
'03'H	CurrentDateTime,
'04'H	MemberStateCertificate,
'05'H	OdometerValueMidnight,
'06'H	DateOfDayDownloaded,
'07'H	SensorPaired,
'08'H	Signature,
'09'H	SpecificConditionRecord,
'0A'H	VehicleIdentificationNumber,
'0B'H	VehicleRegistrationNumber,
'0C'H	VuCalibrationRecord,
'0D'H	VuCardIWRecord,
'0E'H	VuCardRecord,
'0F'H	VuCertificate,
'10'H	VuCompanyLocksRecord,
'11'H	VuControlActivityRecord,
'12'H	VuDetailedSpeedBlock,
'13'H	VuDownloadablePeriod,
'14'H	VuDownloadActivityData,
'15'H	VuEventRecord,
'16'H	VuGNSSCDRecord,
'17'H	VuITSConsentRecord,
'18'H	VuFaultRecord,
'19'H	VuIdentification,
'1A'H	VuOverSpeedingControlData,
'1B'H	VuOverSpeedingEventRecord,
'1C'H	VuPlaceDailyWorkPeriodRecord,
'1D'H	VuTimeAdjustmentGNSSRecord,
'1E'H	VuTimeAdjustmentRecord,
'1F'H	VuPowerSupplyInterruptionRecord,
'20'H	SensorPairedRecord,
'21'H	SensorExternalGNSSCoupledRecord,
'22'H to '7F'H	reserveeritud tulevikus kasutamiseks,
'80'H to 'FF'H	tootjaomane.

2.121. **RegionAlpha**

Alfabeetiline viide piirkonnale kindlaksmääratud riigis.

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

1. põlvkond:

Väärtuse omistus:

```
‘   ’         No information available,
Spain:
‘AN ’         Andalucía,
‘AR ’         Aragón,
‘AST’         Asturias,
‘C  ’         Cantabria,
‘CAT’         Cataluña,
‘CL ’         Castilla-León,
‘CM ’         Castilla-La-Mancha,
‘CV’          Valencia,
‘EXT’         Extremadura,
‘G  ’         Galicia,
‘IB ’         Baleares,
‘IC ’         Canarias,
‘LR ’         La Rioja,
‘M  ’         Madrid,
‘MU ’         Murcia,
‘NA ’         Navarra,
‘PV ’         País Vasco
```

2. põlvkond:

NationAlpha-koodid sisalduvad loetelus, mida säilitatakse koostalitlusvõime katseid tegema määratud labori veebisaidil.

2.122. **RegionNumeric**

Numbriline viide piirkonnale kindlaksmääratud riigis.

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

1. põlvkond:

Väärtuse omistus:

```
‘00’H         No information available,
Spain:
‘01’H         Andalucía,
‘02’H         Aragón,
‘03’H         Asturias,
‘04’H         Cantabria,
‘05’H         Cataluña,
‘06’H         Castilla-León,
‘07’H         Castilla-La-Mancha,
‘08’H         Valencia,
‘09’H         Extremadura,
‘0A’H         Galicia,
‘0B’H         Baleares,
‘0C’H         Canarias,
‘0D’H         La Rioja,
‘0E’H         Madrid,
‘0F’H         Murcia,
‘10’H         Navarra,
‘11’H         País Vasco
```

2. põlvkond:

RegionNumeric-koodid sisalduvad loetelus, mida säilitatakse koostalitlusvõime katseid tegema määratud labori veebisaidil.

2.123. **RemoteCommunicationModuleSerialNumber**

2. põlvkond:

kaugsidemooduli seerianumber.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

1. põlvkond:

RSA võtmepaari moodul.

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

Väärtuse omistus: määratlemata.

2.125. **RSAKeyPrivateExponent**

1. põlvkond:

RSA võtmepaari privaateksponent.

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

Väärtuse omistus: määratlemata.

2.126. **RSAKeyPublicExponent**

1. põlvkond:

RSA võtmepaari avalik eksponent.

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

Väärtuse omistus: määratlemata.

2.127. **RtmData**

2. põlvkond:

selle andmetüübi määratluse kohta vt 14. liide.

2.128. **SealDataCard**

2. põlvkond:

selles andmetüübis salvestatakse teavet sõiduki erinevatele osadele kinnitatud plommide kohta ning see on ette nähtud kaardile salvestamiseks. See andmetüüp on seotud IC lisa nõudega 337.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords on andmeelemendis sealRecords olevate kirjete arv.

sealRecords on plommikirjete kogum.

2.129. **SealDataVu**

2. põlvkond:

selles andmetüübis salvestatakse teavet sõiduki erinevatele osadele kinnitatud plommide kohta ning see on ette nähtud sõidukiseadmesse salvestamiseks.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords on plommikirjete kogum. Kui kasutusel on vähem kui viis plommi, määratakse kõigis kasutamata sealRecords-kirjetes kirje EquipmentType väärtuseks 16, st kasutamata.

2.130. **SealRecord**

2. põlvkond:

selles andmetüübis salvestatakse osale kinnitatud plommi kohta. See andmetüüp on seotud IC lisa nõudega 337.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType näitab, millist tüüpi seadmele plomm on kinnitatud.

extendedSealIdentifier on seadmele kinnitatud plommi identifikaator.

2.131. **SensorApprovalNumber**

Anduri tüübikinnitusnumber.

1. põlvkond:

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

Väärtuse omistus: määratlemata.

2. põlvkond:

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

Väärtuse omistus:

tüübikinnitusnumber esitatakse Euroopa Komisjoni vastaval veebisaidil avaldatud kujul, nt vajaduse korral koos sidekriipsudega. Tüübikinnituse number joondatakse vasakule.

2.132. **SensorExternalGNSSApprovalNumber**

2. põlvkond:

GNSSi välisseadme tüübikinnitusnumber.

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

Väärtuse omistus:

tüübikinnitusnumber esitatakse Euroopa Komisjoni vastaval veebisaidil avaldatud kujul, nt vajaduse korral koos sidekriipsudega. Tüübikinnituse number joondatakse vasakule.

2.133. **SensorExternalGNSSCoupledRecord**

2. põlvkond:

Sõidukiseadmesse salvestatud teave, mis on seotud sõidukiseadmega ühendatud GNSSi välisseadme identimisega (IC lisa nõue 100).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber on sõidukiseadmega ühendatud GNSSi välisseadme seerianumber.

sensorApprovalNumber on selle GNSSi välisseadme tüübikinnitusnumber.

sensorCouplingDate on GNSSi välisseadme sõidukiseadmega ühendamise kuupäev.

2.134. **SensorExternalGNSSIdentification**

2. põlvkond:

teave, mis on seotud GNSSi välisseadme identimisega (IC lisa nõue 98).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber on GNSSi välisseadme laiendatud seerianumber.

sensorApprovalNumber on GNSSi välisseadme tüübikinnitusnumber.

sensorSCIdentifier GNSSi välisseadme turvakomponendi identifikaator.

sensorOSIdentifier on GNSSi välisseadme operatsioonisüsteemi identifikaator.

2.135. **SensorExternalGNSSInstallation**

2. põlvkond:

GNSSi välisseadmesse salvestatud teave, mis on seotud GNSSi välisseadme paigaldusega (IC lisa nõue 123).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst on GNSSi välisseadme esmakordse sõidukiseadmega ühendamise kuupäev.

firstVuApprovalNumber on GNSSi välisseadme ühendatud esimese sõidukiseadme tüübikinnitusnumber.

firstVuSerialNumber on GNSSi välisseadme ühendatud esimese sõidukiseadme seerianumber.

sensorCouplingDateCurrent on GNSSi välisseadme ja sõidukiseadme hetkel toimiva ühenduse loomise kuupäev.

currentVuApprovalNumber on hetkel GNSSi välisseadmega ühendatud sõidukiseadme tüübikinnitusnumber.

currentVUSerialNumber on hetkel GNSSi välisseadmega ühendatud sõidukiseadme seerianumber.

2.136. **SensorExternalGNSSOSIdentifier**

2. põlvkond:

GNSSi välisseadme operatsioonisüsteemi identifikaator.

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

Väärtuse omistus: tootjaomane.

2.137. **SensorExternalGNSSSCIdentifier**

2. põlvkond:

seda andmetüüpi kasutatakse näiteks GNSSi välisseadme krüpteerimismooduli identimiseks.

GNSSi välisseadme turvakomponendi identifikaator.

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

Väärtuse omistus: sõltub osa tootjast.

2.138. **SensorGNSSCouplingDate**

2. põlvkond:

GNSSi välisseadme sõidukiseadmega ühendamise kuupäev.

```
SensorGNSSCouplingDate ::= TimeReal
```

Väärtuse omistus: määratlemata.

2.139. **SensorGNSSSerialNumber**

2. põlvkond:

seda andmetüüpi kasutatakse nii sõidukiseadmes kui ka sellest väljaspool asuva GNSSi vastuvõtja seerianumbri salvestamiseks.

GNSSi vastuvõtja seerianumber.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Liikumisandurisse salvestatud teave, mis on seotud liikumisanduri identimisega (IB lisa nõue 077 ja IC lisa nõue 95).

```
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.

2.141. **SensorInstallation**

Liikumisandurisse salvestatud teave, mis on seotud liikumisanduri paigaldusega (IB lisa nõue 099 ja IC lisa nõue 122).

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

sensorPairingDateFirst on liikumisanduri esmakordse sõidukiseadmega ühendamise kuupäev.

firstVuApprovalNumber on liikumisanduriga ühendatud esimese sõidukiseadme tüübikinnitusnumber.

firstVuSerialNumber on liikumisanduriga ühendatud esimese sõidukiseadme seerianumber.

sensorPairingDateCurrent on liikumisanduri ja sõidukiseadme hetkel toimiva ühenduse loomise kuupäev.

currentVuApprovalNumber on hetkel liikumisanduriga ühendatud sõidukiseadme tüübikinnitusnumber.

currentVUSerialNumber on hetkel liikumisanduriga ühendatud sõidukiseadme seerianumber.

2.142. **SensorInstallationSecData**

Töökojakaardile salvestatud teave, mis on seotud liikumisanduri sõidukiseadmetega ühendamiseks vajalike turbeandmetega (IC lisa nõuded 308 ja 331).

1. põlvkond:

```
SensorInstallationSecData ::= TdesSessionKey
```

Väärtuse omistus: vastavalt standardile ISO 16844-3.

2. põlvkond:

vastavalt 11. liites esitatud kirjeldusele peab töökojakaart mahutama kuni kolme võtit sõidukiseadme ja liikumisanduri ühendamiseks. Neil võtmetel on erinevad versioonid.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                            KMWCKey,
   kMWCKey2                            KMWCKey OPTIONAL,
   kMWCKey3                            KMWCKey OPTIONAL
}
```

2.143. **SensorOSIdentifier**

Liikumisanduri operatsioonisüsteemi identifikaator.

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

Väärtuse omistus: tootjaomane.

2.144. **SensorPaired**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud sõidukiseadmega ühendatud liikumisanduri identimisega (IB lisa nõue 079).

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

sensorSerialNumber on hetkel sõidukiseadmega ühendatud liikumisanduri seerianumber.

sensorApprovalNumber on hetkel sõidukiseadmega ühendatud liikumisanduri tüübikinnitusnumber.

sensorPairingDateFirst on hetkel sõidukiseadmega ühendatud liikumisanduri esmakordse sõidukiseadmega ühendamise kuupäev.

2.145. **SensorPairedRecord**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud sõidukiseadmega ühendatud liikumisanduri identimisega (IC lisa nõue 97).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber on sõidukiseadmega ühendatud liikumisanduri seerianumber.

sensorApprovalNumber on selle liikumisanduri tüübikinnitusnumber.

sensorPairingDate on selle liikumisanduri ja sõidukiseadme ühendamise kuupäev.

2.146. **SensorPairingDate**

Liikumisanduri ja sõidukiseadme esmakordse ühendamise kuupäev.

```
SensorPairingDate ::= TimeReal
```

Väärtuse omistus: määratlemata.

2.147. **SensorSCIdentifier**

Liikumisanduri turvaosa identifikaator.

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

Väärtuse omistus: sõltub osa tootjast.

2.148. **SensorSerialNumber**

Liikumisanduri seerianumber.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Digitaalallkiri.

1. põlvkond:

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

Väärtuse omistus: vastavalt 11. liitele „Ühised turbemehhanismid“.

2. põlvkond:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Väärtuse omistus: vastavalt 11. liitele „Ühised turbemehhanismid“.

2.150. **SignatureRecordArray**

2. põlvkond:

allkirjade kogum ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (Signature). **Väärtuse omistus:** vt RecordType.

recordSize on kirje Signature maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv. Selle väärtuseks määratakse 1, kuna allkirjad võivad olla erineva pikkusega.

records on allkirjade kogum.

2.151. **SimilarEventsNumber**

Samasuguste sündmuste arv ühel antud päeval (IB lisa nõue 094 ja IC lisa nõue 117).

```
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.

2.152. **SpecificConditionRecord**

Juhi- või töökojakaardile või sõidukiseadmesse salvestatud teave, mis on seotud eritingimusega (IC lisa nõuded 130, 276, 301, 328 ja 355).

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

entryTime on sisestamise kuupäev ja kellaaeg.

specificConditionType on eritingimust identiv kood.

2.153. **SpecificConditions**

Juhi- või töökojakaardile või sõidukiseadmesse salvestatud teave, mis on seotud eritingimusega (IC lisa nõuded 131, 277, 302, 329 ja 356).

2. põlvkond:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                       SpecificConditionRecord
}
```

conditionPointerNewestRecord on viimase ajakohastatud eritingimuse kirje indeks.

Väärtuse omistus: number, mis vastab eritingimuse kirjete lugejale, alates nullist eritingimuse kirje esimesel esinemisel struktuuris.

specificConditionRecords on registreeritud eritingimusi käsitlevat teavet sisaldavate kirjete kogum.

2.154. **SpecificConditionType**

Eritingimust identiv kood (IB lisa nõuded 050b, 105a, 212a ja 230a ning IC lisa nõue 62).

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

1. põlvkond:

Väärtuse omistus:

‘00’H	reserveeritud tulevikus kasutamiseks
‘01’H	sõidumeerik mittevajalik – algus
‘02’H	sõidumeerik mittevajalik – lõpp
‘03’H	parvlaeva-/rongisõit
‘04’H .. ‘FF’H	reserveeritud tulevikus kasutamiseks

2. põlvkond:

Väärtuse omistus:

‘00’H	reserveeritud tulevikus kasutamiseks
‘01’H	sõidumeerik mittevajalik – algus
‘02’H	sõidumeerik mittevajalik – lõpp
‘03’H	parvlaeva-/rongisõit – algus
‘04’H	parvlaeva-/rongisõit – lõpp
‘05’H .. ‘FF’H	reserveeritud tulevikus kasutamiseks

2.155. **Speed**

Sõiduki kiirus (km/h).

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

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

2.156. **SpeedAuthorised**

Sõiduki lubatud suurim kiirus (mõiste hh).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Eelnevalt määratletud ajavahemiku keskmine kiirus (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Eelnevalt määratletud ajavahemikul mõõdetud suurim kiirus.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

2. põlvkond:

selle andmetüübi määratluse kohta vt 14. liide.

2.160. **TachographPayloadEncrypted**

2. põlvkond:

Sõidumeeriku DER-TLV-krüpteeringuga andmete kasulik koormus, st krüpteeritud kujul RTM-sõnumis saadetavad andmed. Krüpteerimise kohta vt 11. lisa B osa 13. peatükk.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag on DER-TLV-kodeeringu osa, mille väärtuseks määratakse ‘87’ (vt 11. liite B osa 13. peatükk).

length on DER-TLV-kodeeringu osa, millega kodeeritakse andmeelementide paddingContentIndicatorByte ja encryptedData pikkus.

paddingContentIndicatorByte väärtuseks määratakse ‘00’.

encryptedData on 11. liite B osa 13. peatükis kirjeldatud krüpteeritud tachographPayload. Selle andmeelemendi pikkus oktettides on alati 16 kordarv.

2.161. **TDesSessionKey**

1. põlvkond:

kolmekordne DES-seansivõti.

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

Väärtuse omistus: täpsustamata.

2.162. **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 kesköösti möödunud sekundite arv.

Suurim võimalik kuupäev/aeg on aastal 2106.

2.163. **TyreSize**

Rehvimõõtmete tähis.

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

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

2.164. **VehicleIdentificationNumber**

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

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

Väärtuse omistus: vastavalt standardile ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

2. põlvkond:

VehicleIdentificationNumber ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (VehicleIdentificationNumber). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VehicleIdentificationNumber maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on sõiduki valmistajatehase tähiste kogum.

2.166. **vehicleRegistrationIdentification**

Euroopas unikaalne sõiduki identimistunnus (VRN ja liikmesriik).

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

vehicleRegistrationNation on riik, kus sõiduk on registreeritud.

vehicleRegistrationNumber on sõiduki registreerimisnumber (VRN).

2.167. **VehicleRegistrationNumber**

Sõiduki registreerimisnumber (VRN). Registreerimisnumbri määrab sõidukitele litsentse väljaandev asutus.

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

codePage määratleb 4. peatükis kindlaks määratud märgistiku,

vehicleRegNumber on kindlaksmääratud märgistikku kasutades kodeeritud VRN.

Väärtuse omistus: riigiomane.

2.168. **VehicleRegistrationNumberRecordArray**

2. põlvkond:

VehicleRegistrationNumber ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (VehicleRegistrationNumber). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VehicleRegistrationNumber maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on sõiduki registreerimisnumbrite kogum.

2.169. **VuAbility**

2. põlvkond:

Sõidukiseadmesse salvestatud teave, mis näitab, kas sõidukiseade suudab kasutada 1. põlvkonna sõidumeerikukaarte või mitte (IC lisa nõue 121).

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

Väärtuse omistus – okteti joondus: 'xxxxxxxa'B (8 bitti)

Seoses 1. põlvkonna kasutamise suutlikkusega:

‘a’B	suutlikkus kasutada 1. põlvkonna sõidumeerikukaarte:
	‘0’ B esimese põlvkonna toetus on olemas,
	‘1’B esimese põlvkonna toetus puudub,
‘xxxxxxx’B	reserveeritud tulevikus kasutamiseks

2.170. **VuActivityDailyData**

1. põlvkond:

Sõidukiseadmesse salvestatud teave, mis on seotud konkreetsel kalendripäeval tegevuse muutuse ja/või juhtimisstaatuse muutuse ja/või kaardistaatuse muutusega (IB lisa nõue 084 ja IC lisa nõuded 105, 106, 107) ning kaardipesade 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 sõidukiseadmesse salvestatud. See sisaldab alati kahte ActivityChangeInfo sõna, mis näitavad kahe kaardipesa staatust kell 00.00 sellel päeval.

2.171. **VuActivityDailyRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud konkreetsel kalendripäeval tegevuse muutuse ja/või juhtimisstaatuse muutuse ja/või kaardistaatuse muutusega (IC lisa nõuded 105, 106, 107) ning kaardipesade staatusega kell 00.00 sellel päeval.

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

recordType tähistab kirje tüüpi (ActivityChangeInfo). **Väärtuse omistus:** vt RecordType.

recordSize on kirje ActivityChangeInfo maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on ActivityChangeInfo sõnade kogum, mis on selle päeva kohta sõidukiseadmesse salvestatud. See sisaldab alati kahte ActivityChangeInfo sõna, mis näitavad kahe kaardipesa staatust kell 00.00 sellel päeval.

2.172. **VuApprovalNumber**

Sõidukiseadme tüübikinnitusnumber.

1. põlvkond:

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

Väärtuse omistus: määratlemata.

2. põlvkond:

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

Väärtuse omistus:

tüübikinnitusnumber esitatakse Euroopa Komisjoni vastaval veebisaidil avaldatud kujul, nt vajaduse korral koos sidekriipsudega. Tüübikinnituse number joondatakse vasakule.

2.173. **VuCalibrationData**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud sõidumeeriku kalibreerimistega (IB lisa nõue 098).

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

noOfVuCalibrationRecords on kogumis vuCalibrationRecords sisalduv kirjete arv.

vuCalibrationRecords on kalibreerimiskirjete kogum.

2.174. **VuCalibrationRecord**

Sõidukiseadmesse salvestatud teave, mis on seotud sõidumeeriku kalibreerimisega (IB lisa nõue 098 ja IC lisa nõuded 119 ja 120).

1. põlvkond:

```
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 identib kindlaks kalibreerimise ajal kasutatud töökojakaardi.

workshopCardExpiryDate on kaardi kehtivusaja lõpp.

vehicleIdentificationNumber on VIN.

vehicleRegistrationIdentification sisaldab VRNi ja registreerinud liikmesriiki.

wVehicleCharacteristicConstant on sõidukit iseloomustav koefitsient.

kConstantOfRecordingEquipment on sõidumeeriku konstant.

lTyreCircumference on rattarehvide efektiivümbermõõt.

tyreSize on sõidukile paigaldatud rehvide mõõtmete tähis.

authorisedSpeed on sõiduki lubatud kiirus.

oldOdometerValue, newOdometerValue on läbisõidumõõdiku vana ja uus väärtus.

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

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

2. põlvkond:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

Lisaks 1. põlvkonnale kasutatakse järgmist andmeelementi:

sealDataVu esitab teavet sõiduki erinevatele osadele kinnitatud plommide kohta.

2.175. **VuCalibrationRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud sõidumeeriku kalibreerimistega (IC lisa nõuded 119 ja 120).

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

recordType tähistab kirje tüüpi (VuCalibrationRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuCalibrationRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on kalibreerimiskirjete kogum.

2.176. **VuCardIWData**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud juhi- või töökojakaartide sõidukiseadmesse sisestamise ja väljavõtmise tsüklitega (IB lisa nõue 081 ja IB lisa nõue 103).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords on kogumis vuCardIWRecords sisalduv kirjete arv.

vuCardIWRecords on kaardi sisestamise ja väljavõtmise tsüklitega seotud kirjete kogum.

2.177. **VuCardIWRecord**

Sõidukiseadmesse salvestatud teave, mis on seotud juhi- või töökojakaartide sõidukiseadmesse sisestamise ja väljavõtmise tsükliga (IB lisa nõue 081 ja IB lisa nõue 102).

1. põlvkond:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   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 kellaaeg.

vehicleOdometerValueAtInsertion on sõiduki läbisõidumeeriku näit sisestamise ajal.

cardSlotNumber on kaardipesa, millesse kaart on sisestatud.

cardWithdrawalTime on väljavõtmise kuupäev ja kellaaeg.

vehicleOdometerValueAtWithdrawal on sõiduki läbisõidumeeriku näit kaardi väljavõtmise ajal.

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

manualInputFlag on tunnus, mis näitab, kas kaardiomanik on kaardi sisestamisel sisestanud käsitsi juhtimistegevusi.

2. põlvkond:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

Elemendi fullCardNumber asemel kasutatakse 2. põlvkonna andmestruktuuris järgmist andmeelementi.

fullCardNumberAndGeneration on kaardile salvestatud teave juhikaardi tüübi, kaardi väljaandnud liikmesriigi, kaardi numbri ja põlvkonna kohta.

2.178. **VuCardIWRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud juhi- või töökojakaartide sõidukiseadmesse sisestamise ja väljavõtmise tsüklitega (IC lisa nõue 103).

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

recordType tähistab kirje tüüpi (VuCardIWRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuCardIWRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on kaardi sisestamise ja väljavõtmise tsüklitega seotud kirjete kogum.

2.179. **VuCardRecord**

2. põlvkond:

sõidukiseadmesse salvestatud teave kasutatud sõidumeerikukaardi kohta (IC lisa nõue 132).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber loetakse kaardi põhifaili (MF) all olevast failist EF_ICC.

cardPersonaliserID loetakse kaardi põhifaili (MF) all olevast failist EF_ICC.

typeOfTachographCardId loetakse erifaili DF_Tachograph_G2 all olevast failist EF_Application_Identification.

cardStructureVersion loetakse erifaili DF_Tachograph_G2 all olevast failist EF_Application_Identification.

cardNumber loetakse erifaili DF_Tachograph_G2 all olevast failist EF_Identification.

2.180. **VuCardRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave selles sõidukiseadmes kasutatava sõidumeerikukaardi kohta. Seda teavet kasutatakse sõidukiseadme ja kaardi vaheliste probleemide analüüsimiseks (IC lisa nõue 132).

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

recordType tähistab kirje tüüpi (VuCardRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuCardRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on sõidukiseadmes kasutatavate sõidumeerikukaartidega seotud kirjete kogum.

2.181. **VuCertificate**

Sõidukiseadme avaliku võtme sertifikaat.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

2. põlvkond:

VuCertificate ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (VuCertificate). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuCertificate maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv. Selle väärtuseks määratakse 1, kuna sertifikaadid võivad olla erineva pikkusega.

records on sõidukiseadme sertifikaatide kogum.

2.183. **VuCompanyLocksData**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud ettevõttelukkudega (IB lisa nõue 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                          INTEGER(0..255),
   vuCompanyLocksRecords              SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks on kirjes vuCompanyLocksRecords loetletud lukkude arv.

vuCompanyLocksRecords on ettevõtte lukukirjete kogum.

2.184. **VuCompanyLocksRecord**

Sõidukiseadmesse salvestatud teave, mis on seotud ühe ettevõttelukuga (IB lisa nõue 104 ja IC lisa nõue 128).

1. põlvkond:

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

lockInTime, lockOutTime on lukustamise ja luku avamise kuupäev ja kellaaeg.

companyName, companyAddress on lukustamisega seotud ettevõtte nimi ja aadress.

companyCardNumber identib lukustamisel kasutatud kaardi.

2. põlvkond:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumberAndGeneration     FullCardNumberAndGeneration
}
```

Elemendi companyCardNumber asemel kasutatakse 2. põlvkonna andmestruktuuris järgmist andmeelementi.

companyCardNumberAndGeneration identib lukustamisel kasutatud kaardi ja selle põlvkonna.

2.185. **VuCompanyLocksRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud ettevõttelukkudega (IC lisa nõue 128).

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

recordType tähistab kirje tüüpi (VuCompanyLocksRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuCompanyLocksRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv. Väärtus 0..255.

records on ettevõtte lukukirjete kogum.

2.186. **VuControlActivityData**

1. põlvkond:

Sõidukiseadmesse salvestatud teave, mis on seotud seda sõidukiseadet kasutades läbi viidud kontrollidega (IB lisa nõue 102).

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

noOfControls on kirjes vuControlActivityRecords loetletud kontrollide arv.

vuControlActivityRecords on kontrollitegevuse kirjete kogum.

2.187. **VuControlActivityRecord**

Sõidukiseadmesse salvestatud teave, mis on seotud seda sõidukiseadet kasutades läbi viidud kontrolliga (IB lisa nõue 102 ja IC lisa nõue 126).

1. põlvkond:

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

controlType on kontrolli tüüp.

controlTime on kontrolli kuupäev ja kellaaeg.

controlCardNumber identib kontrolli ajal kasutatud kontrollikaardi.

downloadPeriodBeginTime on allalaadimise puhul allalaaditud ajavahemiku algusaeg.

downloadPeriodEndTime on allalaadimise puhul allalaaditud ajavahemiku lõpuaeg.

2. põlvkond:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Elemendi controlCardNumber asemel kasutatakse 2. põlvkonna andmestruktuuris järgmist andmeelementi.

controlCardNumberAndGeneration identib kontrollimiseks kasutatud kontrollikaardi ja selle põlvkonna.

2.188. **VuControlActivityRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud seda sõidukiseadet kasutades läbi viidud kontrollidega (IC lisa nõue 126).

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

recordType tähistab kirje tüüpi (VuControlActivityRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuControlActivityRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on sõidukiseadme kontrollitegevuse kirjete kogum.

2.189. **VuDataBlockCounter**

Kaardile salvestatud loendur, mis identib järjestikku kaardi sisestamis-väljavõtmistsüklid sõidukiseadmes.

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

Väärtuse omistus: järjestikune number suurima väärtusega 9999, algab uuesti nullist.

2.190. **VuDetailedSpeedBlock**

Sõidukiseadmesse salvestatud teave, mis on seotud sõiduki üksikasjaliku kiirusega minuti jooksul, mil sõiduk on liikunud (IB lisa nõue 093 ja IC lisa nõue 116).

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

speedBlockBeginDate on ploki esimese kiiruseväärtuse kuupäev ja kellaaeg.

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

2.191. **VuDetailedSpeedBlockRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud sõiduki üksikasjaliku kiirusega.

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

recordType tähistab kirje tüüpi (VuDetailedSpeedBlock). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuDetailedSpeedBlock maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on üksikasjalike kiirusplokkide kogum.

2.192. **VuDetailedSpeedData**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud sõiduki üksikasjaliku kiirusega.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                     INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks               SET SIZE(noOfSpeedBlocks) OF
                                       VuDetailedSpeedBlock
}
```

noOfSpeedBlocks on kiirusplokkide arv kogumis vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks on üksikasjalike kiirusplokkide kogum.

2.193. **VuDownloadablePeriod**

Kõige esimene ja viimane kuupäev, mille kohta on sõidukiseadmes juhi tegevusega seotud andmeid (IB lisa nõue 081, 084 või 087 ja IC lisa nõuded 102, 105, 108).

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

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

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

2.194. **VuDownloadablePeriodRecordArray**

2. põlvkond:

VUDownloadablePeriod ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (VuDownloadablePeriod). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuDownloadablePeriod maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on kirjete VuDownloadablePeriod kogum.

2.195. **VuDownloadActivityData**

Sõidukiseadmesse salvestatud teave, mis on seotud viimase allalaadimisega seadmest (IB lisa nõue 105 ja IC lisa nõue 129).

1. põlvkond:

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

downloadingTime on allalaadimise kuupäev ja kellaaeg.

fullCardNumber identib allalaadimise lubamiseks kasutatud kaardi.

companyOrWorkshopName on ettevõtte või töökoja nimi.

2. põlvkond:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   companyOrWorkshopName               Name
}
```

Elemendi fullCardNumber asemel kasutatakse 2. põlvkonna andmestruktuuris järgmist andmeelementi.

fullCardNumberAndGeneration identib allalaadimise lubamiseks kasutatud kaardi ja selle põlvkonna.

2.196. **VuDownloadActivityDataRecordArray**

2. põlvkond:

teave, mis on seotud viimase allalaadimisega sõidukiseadmest (IC lisa nõue 129).

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

recordType tähistab kirje tüüpi (VuDownloadActivityData). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuDownloadActivityData maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records allalaadimistegevuse kirjete kogum.

2.197. **VuEventData**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud sündmustega (IB lisa 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.

2.198. **VuEventRecord**

Sõidukiseadmesse salvestatud teave, mis on seotud sündmusega (IB lisa nõue 094 ja IC lisa nõue 117, välja arvatud kiiruse ületamise sündmus).

1. põlvkond:

```
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 kellaaeg.

eventEndTime on sündmuse lõpu kuupäev ja kellaaeg.

cardNumberDriverSlotBegin identib sündmuse alguses juhikaardi pesasse sisestatud kaardi.

cardNumberCodriverSlotBegin identib sündmuse alguses kaasjuhikaardi pesasse sisestatud kaardi.

cardNumberDriverSlotEnd identib sündmuse lõpus juhikaardi pesasse sisestatud kaardi.

cardNumberCodriverSlotEnd identib sündmuse lõpus kaasjuhikaardi pesasse sisestatud kaardi.

similarEventsNumber on samasuguste sündmuste arv sellel päeval.

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

2. põlvkond:

```
VuEventRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventRecordPurpose                  EventFaultRecordPurpose,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin   FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd     FullCardNumberAndGeneration,
   similarEventsNumber                 SimilarEventsNumber,
   manufacturerSpecificEventFaultData  ManufacturerSpecificEventFaultData
}
```

Lisaks 1. põlvkonnale kasutatakse järgmisi andmeelemente:

manufacturerSpecificEventFaultData sisaldab täiendavat tootjaomast teavet sündmuse kohta.

Elementide cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd ja cardNumberCodriverSlotEnd asemel kasutatakse 2. põlvkonna andmestruktuuris järgmisi andmeelemente:

cardNumberAndGenDriverSlotBegin identib sündmuse alguses juhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

cardNumberAndGenCodriverSlotBegin identib sündmuse alguses kaasjuhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

cardNumberAndGenDriverSlotEnd identib sündmuse lõpus juhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

cardNumberAndGenCodriverSlotEnd identib sündmuse lõpus kaasjuhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

Kui esineb sündmuse aja konflikt, tõlgendatakse elemente eventBeginTime ja eventEndTime järgmiselt:

eventBeginTime on kuupäev ja kellaaeg sõidumeeriku järgi.

eventEndTime on kuupäev ja kellaaeg GNSSi järgi.

2.199. **VuEventRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud sündmustega (IC lisa nõue 117, välja arvatud kiiruse ületamise sündmus).

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

recordType tähistab kirje tüüpi (VuEventRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuEventRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on sündmusekirjete kogum.

2.200. **VuFaultData**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud vigadega (IB lisa nõue 096).

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

noOfVuFaults on kogumis vuFaultRecords loetletud vigade arv.

vuFaultRecords on veakirjete kogum.

2.201. **VuFaultRecord**

Sõidukiseadmesse salvestatud teave, mis on seotud ühe veaga (IB lisa nõue 096 ja IC lisa nõue 118).

1. põlvkond:

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

faultType on sõidumeeriku vea tüüp.

faultRecordPurpose on vea registreerimise eesmärk.

faultBeginTime on vea alguse kuupäev ja kellaaeg.

faultEndTime on vea lõpu kuupäev ja kellaaeg.

cardNumberDriverSlotBegin identib vea alguses juhikaardi pesasse sisestatud kaardi.

cardNumberCodriverSlotBegin identib vea alguses kaasjuhikaardi pesasse sisestatud kaardi.

cardNumberDriverSlotEnd identib vea lõpus juhikaardi pesasse sisestatud kaardi.

cardNumberCodriverSlotEnd identib vea lõpus kaasjuhikaardi pesasse sisestatud kaardi.

2. põlvkond:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Lisaks 1. põlvkonnale kasutatakse järgmist andmeelementi:

manufacturerSpecificEventFaultData sisaldab täiendavat tootjaomast teavet vea kohta.

Elementide cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd ja cardNumberCodriverSlotEnd asemel kasutatakse 2. põlvkonna andmestruktuuris järgmisi andmeelemente:

cardNumberAndGenDriverSlotBegin identib vea alguses juhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

cardNumberAndGenCodriverSlotBegin identib vea alguses kaasjuhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

cardNumberAndGenDriverSlotEnd identib vea lõpus juhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

cardNumberAndGenCodriverSlotEnd identib vea lõpus kaasjuhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

2.202. **VuFaultRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud vigadega (IC lisa nõue 118).

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

recordType tähistab kirje tüüpi (VuFaultRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuFaultRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on veakirjete kogum.

2.203. **VuGNSSCDRecord**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud sõiduki asukohaga GNSSi järgi hetkel, kui juhil täitub kolm järjestikust sõidutundi (IC lisa nõuded 108, 110).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp on kuupäev ja kellaaeg, mil kaardi omanikul täitub kolm järjestikust sõidutundi.

cardNumberAndGenDriverSlot identib juhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

cardNumberAndGenCodriverSlot identib kaasjuhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

gnssPlaceRecord sisaldab sõiduki asukohaga seotud teavet.

2.204. **VuGNSSCDRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud sõiduki asukohaga GNSSi järgi hetkel, kui juhil täitub kolm järjestikust sõidutundi (IC lisa nõuded 108 ja 110).

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

recordType tähistab kirje tüüpi (VuGNSSCDRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuGNSSCDRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on GNSSi pideva juhtimisaja kirjete kogum.

2.205. **VuIdentification**

Sõidukiseadmesse salvestatud teave, mis on seotud sõidukiseadme identimisega (IB lisa nõue 075 ja IC lisa nõuded 93 ja 121).

1. põlvkond:

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

vuManufacturerName on sõidukiseadme tootja nimi.

vuManufacturerAddress on sõidukiseadme tootja aadress.

vuPartNumber on sõidukiseadme osa number.

vuSerialNumber on sõidukiseadme seerianumber.

vuSoftwareIdentification identib sõidukiseadmes rakendatud tarkvara.

vuManufacturingDate on sõidukiseadme tootmise kuupäev.

vuApprovalNumber on sõidukiseadme tüübikinnitusnumber.

2. põlvkond:

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

Lisaks 1. põlvkonnale kasutatakse järgmisi andmeelemente:

vuGeneration näitab sõidukiseadme põlvkonda.

vuAbility esitab teavet selle kohta, kas sõidukiseade toetab 1. põlvkonna sõidumeerikukaarte või mitte.

2.206. **VuIdentificationRecordArray**

2. põlvkond:

VuIdentification ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (VuIdentification). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuIdentification maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on kirjete VuIdentification kogum.

2.207. **VuITSConsentRecord**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud juhi nõusolekuga intelligentsete transpordisüsteemide kasutamiseks.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identib kaardi ja selle põlvkonna. See peab olema juhi- või töökojakaart.

consent on tunnus, mis näitab, kas juht on andnud nõusoleku intelligentsete transpordisüsteemide kasutamise kohta koos selle sõiduki/sõidukiseadmega.

Väärtuse omistus:

TRUE näitab juhi nõusolekut intelligentsete transpordisüsteemide kasutamisega

FALSE näitab juhi keeldumist intelligentsete transpordisüsteemide kasutamisest

2.208. **VuITSConsentRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud juhi nõusolekuga intelligentsete transpordisüsteemide kasutamiseks (IC lisa nõue 200).

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

recordType tähistab kirje tüüpi (VuITSConsentRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuITSConsentRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on ITSi nõusolekukirjete kogum.

2.209. **VuManufacturerAddress**

Sõidukiseadme tootja aadress.

```
VuManufacturerAddress ::= Address
```

Väärtuse omistus: määratlemata.

2.210. **VuManufacturerName**

Sõidukiseadme tootja nimi.

```
VuManufacturerName ::= Name
```

Väärtuse omistus: määratlemata.

2.211. **VuManufacturingDate**

Sõidukiseadme tootmise kuupäev.

```
VuManufacturingDate ::= TimeReal
```

Väärtuse omistus: määratlemata.

2.212. **VuOverSpeedingControlData**

Sõidukiseadmesse salvestatud teave, mis on seotud pärast viimast kiiruse ületamise kontrolli toimunud kiiruse ületamise sündmusega (IB lisa nõue 095 ja IC lisa nõue 117).

```
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.

2.213. **VuOverSpeedingControlDataRecordArray**

2. põlvkond:

VuOverSpeedingControlData ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (VuOverSpeedingControlData). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuOverSpeedingControlData maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on kiiruse ületamise kontrolli andmekirjete kogum.

2.214. **VuOverSpeedingEventData**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud kiiruse ületamise sündmustega (IB lisa 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 kirjete kogum.

2.215. **VuOverSpeedingEventRecord**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud kiiruse ületamise sündmusega (IB lisa nõue 094 ja IC lisa nõue 117).

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

eventType on sündmuse tüüp.

eventRecordPurpose on sündmuse registreerimise eesmärk.

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 identib sündmuse alguses juhikaardi pesasse sisestatud kaardi.

similarEventsNumber on samasuguste sündmuste arv sellel päeval.

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud kiiruse ületamise sündmusega (IB lisa nõue 094 ja IC lisa nõue 117).

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

Elemendi cardNumberDriverSlotBegin asemel kasutatakse 2. põlvkonna andmestruktuuris järgmist andmeelementi.

cardNumberAndGenDriverSlotBegin identib sündmuse alguses juhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

2.216. **VuOverSpeedingEventRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud kiiruse ületamise sündmustega (IC lisa nõue 117).

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

recordType tähistab kirje tüüpi (VuOverSpeedingEventRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuOverSpeedingEventRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on kiiruse ületamise kirjete kogum.

2.217. **VuPartNumber**

Sõidukiseadme osa number.

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

Väärtuse omistus: sõltub sõidukiseadme tootjast.

2.218. **VuPlaceDailyWorkPeriodData**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud juhtide tööpäeva algus- ja lõpukohaga (IB lisa nõue 087 ja IC lisa nõuded 108 ja 110).

```
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.

2.219. **VuPlaceDailyWorkPeriodRecord**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud juhi tööpäeva algus- ja lõpukohaga (IB lisa nõue 087 ja IC lisa nõuded 108 ja 110).

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

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

placeRecord sisaldab sisestatud kohaga seotud teavet.

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud juhi tööpäeva algus- ja lõpukohaga (IB lisa nõue 087 ja IC lisa nõuded 108 ja 110).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Elemendi fullCardNumber asemel kasutatakse 2. põlvkonna andmestruktuuris järgmist andmeelementi.

fullCardNumberAndGeneration on kaardile salvestatud teave juhikaardi tüübi, kaardi väljaandnud liikmesriigi, kaardi numbri ja põlvkonna kohta.

2.220. **VuPlaceDailyWorkPeriodRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud juhtide tööpäeva algus- ja lõpukohaga (IC lisa nõuded 108 ja 110).

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

recordType tähistab kirje tüüpi (VuPlaceDailyWorkPeriodRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuPlaceDailyWorkPeriodRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on kohaga seotud kirjete kogum.

2.221. **VuPrivateKey**

1. põlvkond:

sõidukiseadme privaatvõti.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

1. põlvkond:

sõidukiseadme avalik võti.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Sõidukiseadme seerianumber (IB lisa nõue 075 ja IC lisa nõue 93).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Sõidukiseadme tarkvaraversiooni installeerimise kuupäev.

```
VuSoftInstallationDate ::= TimeReal
```

Väärtuse omistus: määratlemata.

2.225. **VuSoftwareIdentification**

Sõidukiseadmesse salvestatud teave, mis on seotud installeeritud tarkvaraga.

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

vuSoftwareVersion on sõidukiseadme tarkvara versiooninumber.

vuSoftInstallationDate on tarkvaraversiooni installeerimise kuupäev.

2.226. **VuSoftwareVersion**

Sõidukiseadme tarkvara versiooninumber.

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

Väärtuse omistus: määratlemata.

2.227. **VuSpecificConditionData**

1. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud eritingimustega.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords on kogumis specificConditionRecords sisalduv kirjete arv.

specificConditionRecords on eritingimustega seotud kirjete kogum.

2.228. **VuSpecificConditionRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud eritingimustega (IC lisa nõue 130).

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

recordType tähistab kirje tüüpi (SpecificConditionRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje SpecificConditionRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on eritingimustega seotud kirjete kogum.

2.229. **VuTimeAdjustmentData**

1. põlvkond:

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

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

noOfVuTimeAdjRecords on kogumis vuTimeAdjustmentRecords sisalduv kirjete arv.

vuTimeAdjustmentRecords on aja korrigeerimise kirjete kogum.

2.230. **VuTimeAdjustmentGNSSRecord**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud aja korrigeerimisega GNSSi ajaandmete põhjal (IC lisa nõuded 124 ja 125).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal
}
```

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

2.231. **VuTimeAdjustmentGNSSRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud aja korrigeerimisega GNSSi ajaandmete põhjal (IC lisa nõuded 124 ja 125).

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

recordType tähistab kirje tüüpi (VuTimeAdjustmentGNSSRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuTimeAdjustmentGNSSRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on GNSSi põhjal tehtud aja korrigeerimise kirjete kogum.

2.232. **VuTimeAdjustmentRecord**

Sõidukiseadmesse salvestatud teave, mis on seotud korrapärase kalibreerimise välise aja korrigeerimisega (IB lisa nõue 101 ja IC lisa nõuded 124 ja 125).

1. põlvkond:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   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 identib aja korrigeerimiseks kasutatud töökojakaardi.

2. põlvkond:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Elemendi workshopCardNumber asemel kasutatakse 2. põlvkonna andmestruktuuris järgmist andmeelementi.

workshopCardNumberAndGeneration identib aja korrigeerimiseks kasutatud töökojakaardi ja selle põlvkonna.

2.233. **VuTimeAdjustmentRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud korrapärase kalibreerimise väliste aja korrigeerimistega (IC lisa nõuded 124 ja 125).

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

recordType tähistab kirje tüüpi (VuTimeAdjustmentRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuTimeAdjustmentRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on aja korrigeerimise kirjete kogum.

2.234. **WorkshopCardApplicationIdentification**

Töökojakaardile salvestatud teave, mis on seotud kaardirakenduse identimisega (IC lisa nõuded 307 ja 330).

1. põlvkond:

```
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 veatüübi kaupa vigade 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. põlvkond:

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

Lisaks 1. põlvkonnale kasutatakse järgmisi andmeelemente:

noOfGNSSCDRecords on arv, mitu GNSSi pideva juhtimisaja kirjet kaart mahutab.

noOfSpecificConditionRecords on arv, mitu eritingimuste kirjet kaart mahutab.

2.235. **WorkshopCardCalibrationData**

Töökojakaardile salvestatud teave, mis on seotud kaardiga tehtud töökojategevusega (IC lisa nõuded 314, 316, 337 ja 339).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   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.

2.236. **WorkshopCardCalibrationRecord**

Töökojakaardile salvestatud teave, mis on seotud kaardiga tehtud kalibreerimisega (IC lisa nõuded 314 ja 337).

1. põlvkond:

```
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 VIN.

vehicleRegistration sisaldab VRNi ja registreerinud liikmesriiki.

wVehicleCharacteristicConstant on sõidukit iseloomustav koefitsient.

kConstantOfRecordingEquipment on sõidumeeriku konstant.

lTyreCircumference on rattarehvide efektiivümbermõõt.

tyreSize on sõidukile paigaldatud rehvide mõõtmete tähis.

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 kirjes CalibrationPurpose määratletud järgmise kalibreerimise tüüp, mille peab läbi viima volitatud inspekteerimisasutus.

vuPartNumber, vuSerialNumber ja sensorSerialNumber on sõidumeeriku identimiseks vajalikud andmeelemendid.

2. põlvkond:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

Lisaks 1. põlvkonnale kasutatakse järgmisi andmeelemente:

sensorGNSSSerialNumber identib GNSSi välisseadme.

rcmSerialNumber identib kaugsidemooduli.

sealDataCard esitab teavet sõiduki erinevatele osadele kinnitatud plommide kohta.

2.237. **WorkshopCardHolderIdentification**

Töökojakaardile salvestatud teave, mis on seotud kaardi omaniku identimisega (IC lisa nõuded 311 ja 334).

```
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.

2.238. **WorkshopCardPIN**

Töökojakaardi PIN-kood (IC lisa nõuded 309 ja 332).

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

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

2.239. **W-VehicleCharacteristicConstant**

Sõidukit iseloomustav koefitsient (mõiste k).

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

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

2.240. **VuPowerSupplyInterruptionRecord**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud voolukatkestuse sündmustega (IC lisa nõue 117).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType on sündmuse tüüp.

eventRecordPurpose on sündmuse registreerimise eesmärk.

eventBeginTime on sündmuse alguse kuupäev ja kellaaeg.

eventEndTime on sündmuse lõpu kuupäev ja kellaaeg.

cardNumberAndGenDriverSlotBegin identib sündmuse alguses juhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

cardNumberAndGenDriverSlotEnd identib sündmuse lõpus juhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

cardNumberAndGenCodriverSlotBegin identib sündmuse alguses kaasjuhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

cardNumberAndGenCodriverSlotEnd identib sündmuse lõpus kaasjuhikaardi pesasse sisestatud kaardi ja selle põlvkonna.

similarEventsNumber on samasuguste sündmuste arv sellel päeval.

2.241. **VuPowerSupplyInterruptionRecordArray**

2. põlvkond:

sõidukiseadmesse salvestatud teave, mis on seotud voolukatkestuse sündmustega (IC lisa nõue 117).

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

recordType tähistab kirje tüüpi (VuPowerSupplyInterruptionRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje VuPowerSupplyInterruptionRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on voolukatkestusega seotud sündmusekirjete kogum.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

2. põlvkond:

Kogum SensorExternalGNSSCoupledRecord ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (SensorExternalGNSSCoupledRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje SensorExternalGNSSCoupledRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on kirjete SensorExternalGNSSCoupledRecord arv.

2.243. **VuSensorPairedRecordArray**

2. põlvkond:

Kogum SensorPairedRecord ja metaandmed, mida kasutatakse allalaadimisprotokollis.

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

recordType tähistab kirje tüüpi (SensorPairedRecord). **Väärtuse omistus:** vt RecordType.

recordSize on kirje SensorPairedRecord maht baitides.

noOfRecords on kirjete kogumis sisalduv kirjete arv.

records on anduri ühendamise kirjete arv.

3. VÄÄRTUS- JA SUURUSVAHEMIKE MÄÄRATLUSED

2. peatükis määratletud muutujate väärtuste määratlus.

```
TimeRealRange ::= 2^32-1
```

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 (Address, Name, VehicleRegsitrationNumber) kasutatakse lisaks järgmiste koodilehekülgega määratud kaheksabitiliste standardmärgistike kümnendarvude märke koodidega 161–255: standardmärgistik	Koodilehekülg (kümnendarv)
ISO/IEC 8859-1 (ladina-1/Lääne-Euroopa)	1
ISO/IEC 8859-2 (ladina-2/Kesk-Euroopa)	2
ISO/IEC 8859-3 (ladina-3/Lõuna-Euroopa)	3
ISO/IEC 8859-5 (ladina/kirillitsa)	5
ISO/IEC 8859-7 (ladina/kreeka)	7
ISO/IEC 8859-9 (ladina-5/türgi)	9
ISO/IEC 8859-13 (ladina-7 / balti segu)	13
ISO/IEC 8859-15 (ladina-9)	15
ISO/IEC 8859-16 (ladina-10/Kagu-Euroopa)	16
KOI8-R (ladina/kirillitsa)	80
KOI8-U (ladina/kirillitsa)	85

5. KODEERIMINE

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

6. OBJEKTI JA RAKENDUSE IDENTIFIKAATORID

6.1. **Objekti identifikaatorid**

Käesolevas punktis loetletud objekti identifikaatorid (OID) on asjakohased üksnes 2. põlvkonna puhul. Nende OID-e spetsifikatsioon on esitatud tehnilises suunises TR-03110-3 ning täielikkuse huvides on seda siin korratud. Kõnealused OID-d sisalduvad bsi-de alampuus:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Sõidukiseadme autentimisprotokolli identifikaatorid

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}
id-TA-ECDSA                 OBJECT IDENTIFIER ::= {id-TA 2}
id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}
id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}
id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Näide: kui sõidukiseadme autentimiseks kasutatakse protokolli SHA-384, siis tuleb kasutada objekti identifikaatorit (ASN.1 esituses) `bsi-de protocols(2) smartcard(2) 2 2 4`. Selle objekti identifikaatori väärtus punktesituses on `0.4.0.127.0.7.2.2.2.2.4`.

	Punktesitus	Baitesitus
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	‘04 00 7F 00 07 02 02 02 02 03’
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	‘04 00 7F 00 07 02 02 02 02 04’
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	‘04 00 7F 00 07 02 02 02 02 05’

Kiibi autentimisprotokolli identifikaatorid

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}
id-CA-ECDH                          OBJECT IDENTIFIER ::= {id-CA 2}
id-CA-ECDH-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-CA-ECDH 2}
id-CA-ECDH-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-CA-ECDH 3}
id-CA-ECDH-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Näide: oletame, et kiibi autentimiseks kasutatakse algoritmi ECDH, mille tulemuseks on 128 biti pikkune AESi seansivõti. Pärast kasutatakse seda seansivõtit andmete konfidentsiaalsuse tagamiseks CBC-režiimis ja andmete autentsuse tagamiseks koos CMAC-algoritmiga. Seega tuleb kasutada objekti identifikaatorit (ASN.1 esituses) `bsi-de protocols(2) smartcard(2) 3 2 2`. Selle objekti identifikaatori väärtus punktesituses on `0.4.0.127.0.7.2.2.3.2.2`.

	Punktesitus	Baitesitus
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	‘04 00 7F 00 07 02 02 03 02 02’
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	‘04 00 7F 00 07 02 02 03 02 03’
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	‘04 00 7F 00 07 02 02 03 02 04’

6.2. Rakenduse identifikaatorid

2. põlvkond:

GNSSi välisseadme (2. põlvkond) rakenduse identifikaator (AID) esitatakse kujul ‘FF 44 54 45 47 4D’. See on standardi ISO/IEC 7816-4 kohaselt omandiõigusega kaitstud AID.

Märkus: viimase viie baidiga kodeeritakse aruka sõidumeeriku GNSSi välisseadme DTEGM.

Teise põlvkonna sõidumeerikukaartide rakenduse identifikaator esitatakse kujul ‘FF 53 4D 52 44 54’. See on standardi ISO/IEC 7816-4 kohaselt omandiõigusega kaitstud AID.

2. liide

SÕIDUMEERIKUKAARTIDE SPETSIFIKAAT

SISUKORD

1. SISSEJUHATUS

1.1. **Lühendid**

Käesolevas liites kasutatakse järgmisi lühendeid.

AC	(*access conditions*) juurdepääsutingimused
AES	(*Advanced Encryption Standard*) täiustatud krüpteerimisstandard
AID	(*application identifier*) rakenduse identifikaator
ALW	(*always*) alati
APDU	(*application protocol data unit*) rakendusprotokolli andmeühik (käsk)
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
DSRC	(*dedicated short range communication*) sihtotstarbeline lähitoimeside
DF	(*dedicated file*) erifail. Erifail võib sisaldada muid faile (elementaar- või erifaile)
ECC	(*elliptic curve cryptography*) elliptiliste kõverate krüptograafia
EF	(*elementary file*) elementaarfail
etu	(*elementary time unit*) elementaarajaühik
G1	1. põlvkond
G2	2. põlvkond
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 korraldusbait
Lc	APDU käsu sisendandmete pikkus
Le	oodatavate andmete pikkus (käsu väljundandmed)
MF	(*master file*) põhifail (juur-DF)
NAD	(*node address*) protokollis T = 1 kasutatav sõlmeaadress
NEV	(*never*) mitte kunagi
P1-P2	parameetribaidid
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 tulevikus kasutamiseks
RST	(*reset (of the card)*) (kaardi) lähtestus
SFID	elementaarfaili lühike identifikaator
SM	(*secure messaging*) turvaline sõnumivahetus
SW1-SW2	(*status bytes*) olekubaidid
TS	ATRi algmärk
VPP	programmeerimispinge
VU	(*vehicle unit*) sõidukiseade
XXh	väärtus XX kuueteistkümnendsüsteemis
'XXh'	väärtus XX kuueteistkümnendsüsteemis
||	konkatenatsioonisümbol 03||04 = 0304

1.2. **Viited**

Käesolevas liites kasutatakse järgmisi viiteid.

ISO/IEC 7816-2 *Identification cards – Integrated circuit cards – Part 2: Dimensions and location of the contacts* („Identimiskaardid. Kiipkaardid. Osa 2: Kontaktide mõõtmed ja asukoht"). ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 *Identification cards – Integrated circuit cards – Part 3: Electrical interface and transmission protocols* („Identimiskaardid. Kiipkaardid. Osa 3: Elektriline liides ja edastusprotokollid"). ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 *Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange* („Identimiskaardid. Kiipkaardid. Osa 4: Andmevahetuse ülesehitus, turvalisus ja käsud"). ISO/IEC 7816-4:2013 + 1. parandus: 2014.

ISO/IEC 7816-6 *Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange* („Identimiskaardid. Kiipkaardid. Osa 6: Valdkondadevahelised andmeelemendid"). ISO/IEC 7816-6:2004 + 1. parandus: 2006.

ISO/IEC 7816-8 *Identification cards – Integrated circuit cards – Part 8: Commands for security operations* („Identimiskaardid. Kiipkaardid. Osa 8: Turvatoimingute käsud"). ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function* („Infotehnoloogia. Turvameetodid. Sõnumiautentimiskoodid (MACid). Osa 2: Sihtotstarbelist räsifunktsiooni kasutavad mehhanismid"). ISO/IEC 9797-2:2011.

2. ELEKTRILISED JA FÜÜSIKALISED OMADUSED

TCS_01 Kui ei ole määratletud teisiti, vastavad kõik elektroonilised signaalid standardile ISO/IEC 7816-3.

TCS_02 Kaardi kontaktide asukoht ja mõõtmed vastavad standardile ISO/IEC 7816-2.

2.1. **Toitepinge ja voolutarbimine**

TCS_03 Kaart töötab vastavalt spetsifikatsioonile ja standardis ISO/IEC 7816-3 määratletud voolutarbimise piires.

TCS_04 Kaart töötab pingel Vcc = 3V (± 0,3V) või Vcc = 5V (± 0,5 V).

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

2.2. **Programmeerimispinge V_{pp}**

TCS_05 Kontaktil C6 kaart programmeerimispinget ei vaja. Eeldatakse, et kontakt C6 ei ole liideseseadmes ühendatud. Kontakt C6 võib olla ühendatud kaardil pingega V_{cc}, kuid seda ei maandata. Seda pinget ei tohi mingil juhul interpreteerida.

2.3. **Taktgeneraator ja -sagedus**

TCS_06 Kaart toimib sagedusalas 1–5 MHz ja võib toetada kõrgemaid sagedusi. Ühe kaardiseansi ajal võib taktsagedus kõikuda ± 2 %. Taktsageduse genereerib sõidukiseade, mitte kaart ise. Töötsükkel võib kõikuda 40 ja 60 % vahel.

TCS_07 Kaardifailis EF ICC sisalduvatel tingimustel võib välise taktgeneraatori seisata. Faili EF ICC esimeses baidis on kodeeritud režiimi Clockstop tingimused:

Madal	Kõrge		
3. bitt	2. bitt	1. bitt	
0	0	1	Clockstop lubatud, tasandi eelistus puudub
0	1	1	Clockstop lubatud, eelistatud kõrge tasand
1	0	1	Clockstop lubatud, eelistatud madal tasand
0	0	0	Clockstop ei ole lubatud
0	1	0	Clockstop lubatud ainult kõrgel tasandil
1	0	0	Clockstop lubatud ainult madalal tasandil

Bitte 4–8 ei kasutata.

2.4. **Sisend-/väljundkontakt**

TCS_08 Sisend-väljundkontakti C7 kasutatakse andmete saamiseks liideseseadmest ja nende edastamiseks liideseseadmesse. Töötamise ajal on edastamisrežiimis ainult kaart või liideseseade. Kui mõlemad seadmed on edastamisrežiimis, ei tohi kaarti kahjustada. Kui kaart ei edasta andmeid, on see vastuvõturežiimis.

2.5. **Kaardi olekud**

TCS_09 Toitepinge andmisel töötab kaart kahes olekus:

käskude täitmise või digitaalseadmega ühenduses olemise ajal tööolekus,

igal muul ajal puhkeolekus; selles olekus säilitab kaart kõik andmed.

3. RIISTVARA JA ANDMEVAHETUS

3.1. **Sissejuhatus**

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

Sõidumeerikukaardid vastavad võimalikult suures ulatuses olemasolevate ISO/IEC standardite (eelkõige ISO/IEC 7816) kohaldatavatele normidele. Sellegipoolest on esitatud käskude ja protokollide täielik kirjeldus, et määratleda mõnd piiratud kasutusala või võimalikke erinevusi. Kirjeldatud käsud vastavad täielikult osutatud normidele, kui ei ole märgitud teisiti.

3.2. **Edastusprotokoll**

TCS_10 Edastusprotokoll vastab protokolli T = 0 ja T = 1 puhul standardile ISO/UEC 7816-3. Eelkõige tuvastab sõidukiseade kaardi saadetud ooteajalaiendid.

3.2.1. *Protokollid*

TCS_11 Kaart võimaldab kasutada nii protokolli **T = 0** kui ka protokolli **T = 1**. Lisaks võib kaart toetada muid kontaktipõhiseid protokolle.

TCS_12 **T = 0** on vaikeprotokoll, seetõttu on vaja käsku **PTS**, et muuta see protokolliks **T = 1**.

TCS_13 Seadmed peavad toetama **otsest kodeerimist** (*direct convention*) mõlemas protokollis: seega on otsene kodeerimine kaardi puhul kohustuslik.

TCS_14 **Kaardi infovälja mahu**bait esitatakse ATR-signaalis tähemärgis TA3. See väärtus on vähemalt 'F0h' (= 240 baiti).

Protokollide suhtes kohaldatakse järgmisi piiranguid.

TCS_15 **T = 0**

— Liideseseade toetab vastust sisend-/väljundsignaalile, kui kaardi lähtestuse puhul on signaali tõususerv vähemalt 400 takti.

— Liideseseade suudab lugeda tähemärke, mida eraldab 12 elementaarajaühikut.

— Liideseseade suudab lugeda vigast tähemärki ja selle kordust, kui see on eraldatud 13 elementaarajaühikuga. Vigase tähemärgi tuvastamisel võib sisend-/väljundsignaalile anda veasignaali 1. ja 2. elementaarajaühiku vahel. Seade toetab 1 elementaarajaühiku 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 elementaarajaühikuga. See kehtib ka kaardi saadetud ACK-tähemärgi kohta pärast liideseseadme saadetud P3-tähemärki.

— Liideseseade võtab arvesse kaardi saadetud NUL-tähemärki.

— Liideseseade aktsepteerib ACK tarvis täiendrežiimi.

— Käsku GET RESPONSE ei saa kasutada aheltöötlusrežiimis selliste andmete saamiseks, mille pikkus võib ületada 255 baiti.

TCS_16 **T = 1**

— Sõlmeaadressi bait: ei kasutata (NAD väärtuseks määratakse '00').

— Ploki S käsk ABORT: ei kasutata.

— Ploki S programmeerimispinge olekuviga: ei kasutata.

— Andmevälja ahela kogupikkus ei ületa 255 baiti (tagatakse liideseseadmega).

— Kohe pärast ATR-signaali esitab liideseseade seadme infovälja mahu (IFSD): 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_17 Seade kontrollib ATR-baite vastavalt standardile ISO/IEC 7816-3. ATR-signaalis olevaid märke, mis on seotud kaardi ajalooga (*Historical Characters*), ei kontrollita.

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 ajalooga seotud baiti olemas.
TD1	'80h'	TD2 olemas; kasutatakse protokolli T = 0
TD2	'11h'	TA3 olemas; kasutatakse protokolli T = 1
TA3	'XXh' (vähemalt 'F0h')	Kaardi infovälja maht (IFSC)
TH1 kuni TH5	'XXh'	Kaardi ajalooga seotud märgid
TCK	'XXh'	Kontrollimärk (välja arvatud OR)

TCS_18 Pärast lähtestuse vastust (ATR) valitakse vaikimisi põhifail ja see saab töökataloogiks.

3.2.3. *PTS*

TCS_19 Vaikeprotokoll on T = 0. Protokolli T = 1 kasutamiseks peab seade saatma kaardile käsu PTS (kasutatakse ka nimetust PPS).

TCS_20 Kuna kaardi puhul on kohustuslikud nii protokoll T = 0 kui ka T = 1, on protokollivahetuseks kohustuslik ka baaskäsk PTS.

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

Kaardi puhul on suuremad edastuskiirused vabatahtlikud.

TCS_21 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; '00h' korral valitakse T0, '01h' korral valitakse T1.
PK	'XXh'	Kontrollimärk: 'XXh' = 'FFh', kui PPS0 = '00h', 'XXh' = 'FEh' kui PPS0 = '01h'.

3.3. **Juurdepääsueeskirjad**

TCS_22 Juurdepääsueeskiri määrab kindlaks juurdepääsurežiimile (nt käsk) vastavad turbetingimused. Kui need turbetingimused on täidetud, toimub vastava käsu töötlemine.

TCS_23 Sõidumeerikukaardi jaoks kasutatakse järgmisi turbetingimusi.

Lühend	Tähendus
ALW	Tegevus on alati võimalik ning seda saab piiranguteta teha. Käsu ja vastuse APDU saadetakse lihttekstina, st ilma turvalise sõnumivahetuseta.
NEV	Tegevus ei ole kunagi võimalik.
PLAIN-C	Käsu APDU saadetakse lihttekstina, st ilma turvalise sõnumivahetuseta.
PWD	Tegevus on võimalik ainult juhul, kui töökojakaardi PIN-kood on kontrolli läbinud, st kui kaardi sisemine turbeolek „PIN_Verified“ on määratud. Käsk tuleb saata ilma turvalise sõnumivahetuseta.
EXT-AUT-G1	Tegevus on võimalik ainult juhul, kui 1. põlvkonna autentimiseks kasutatav käsk EXTERNAL AUTHENTICATE on edukalt täidetud (vt ka 11. liite A osa).
SM-MAC-G1	APDU (käsk ja vastus) puhul peab 1. põlvkonna turvaline sõnumivahetus toimuma režiimis „ainult autentimine“ (vt 11. liite A osa).
SM-C-MAC-G1	Käsu APDU puhul peab 1. põlvkonna turvaline sõnumivahetus toimuma režiimis „ainult autentimine“ (vt 11. liite A osa).
SM-R-ENC-G1	Vastuse APDU puhul peab 1. põlvkonna turvaline sõnumivahetus toimuma režiimis „ainult autentimine“ (vt 11. liite A osa), st sõnumi autentimise koodi tagasi ei saadeta.
SM-R-ENC-MAC-G1	Vastuse APDU puhul peab 1. põlvkonna turvaline sõnumivahetus toimuma režiimis „krüpteerimine ja autentimine“ (vt 11. liite A osa).
SM-MAC-G2	APDU (käsk ja vastus) puhul peab 2. põlvkonna turvaline sõnumivahetus toimuma režiimis „ainult autentimine“ (vt 11. liite B osa).
SM-C-MAC-G2	Käsu APDU puhul peab 2. põlvkonna turvaline sõnumivahetus toimuma režiimis „ainult autentimine“ (vt 11. liite B osa).
SM-R-ENC-MAC-G2	Vastuse APDU puhul peab 2. põlvkonna turvaline sõnumivahetus toimuma režiimis „krüpteerimine ja autentimine“ (vt 11. liite B osa).

TCS_24 Neid turbetingimusi saab siduda järgmiselt:

AND: kõik turbetingimused peavad olema täidetud;

OR: vähemalt üks turbetingimus peab olema täidetud.

Failisüsteemi juurdepääsueeskirju (käsud SELECT, READ BINARY ja UPDATE BINARY) on kirjeldatud 4. peatükis. Ülejäänud käskude juurdepääsueeskirjad on esitatud järgmistes tabelites.

TCS_25 Erifaili Tachograph G1 rakendustes kasutatakse järgmisi juurdepääsueeskirju.

Käsk	Juhikaart	Töökojakaart	Kontrollikaart	Ettevõttekaart
External Authenticate				
— 1. põlvkonna autentimiseks	ALW	ALW	ALW	ALW
— 2. põlvkonna autentimiseks	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Ei kohaldata	Ei kohaldata	Ei kohaldata	Ei kohaldata
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ei kohaldata	Ei kohaldata
PSO: Hash	Ei kohaldata	Ei kohaldata	ALW	Ei kohaldata
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ei kohaldata	Ei kohaldata
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ei kohaldata	Ei kohaldata	ALW	Ei kohaldata
Verify	Ei kohaldata	ALW	Ei kohaldata	Ei kohaldata

TCS_26 Erifaili Tachograph_G2 rakendustes kasutatakse järgmisi juurdepääsueeskirju.

Käsk	Juhikaart	Töökojakaart	Kontrollikaart	Ettevõttekaart
External Authenticate				
— 1. põlvkonna autentimiseks	Ei kohaldata	Ei kohaldata	Ei kohaldata	Ei kohaldata
— 2. põlvkonna autentimiseks	ALW	PWD	ALW	ALW
Internal Authenticate	Ei kohaldata	Ei kohaldata	Ei kohaldata	Ei kohaldata

Käsk	Juhikaart	Töökojakaart	Kontrollikaart	Ettevõttekaart
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Ei kohaldata	ALW	ALW	Ei kohaldata
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ei kohaldata	Ei kohaldata
PSO: Hash	Ei kohaldata	Ei kohaldata	ALW	Ei kohaldata
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ei kohaldata	Ei kohaldata
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ei kohaldata	Ei kohaldata	ALW	Ei kohaldata
Verify	Ei kohaldata	ALW	Ei kohaldata	Ei kohaldata

TCS_27 Põhifailis kasutatakse järgmisi juurdepääsueeskirju.

Käsk	Juhikaart	Töökojakaart	Kontrollikaart	Ettevõttekaart
External Authenticate				
— 1. põlvkonna autentimiseks	Ei kohaldata	Ei kohaldata	Ei kohaldata	Ei kohaldata
— 2. põlvkonna autentimiseks	ALW	PWD	ALW	ALW
Internal Authenticate	Ei kohaldata	Ei kohaldata	Ei kohaldata	Ei kohaldata
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Ei kohaldata	Ei kohaldata	Ei kohaldata	Ei kohaldata

Käsk	Juhikaart	Töökojakaart	Kontrollikaart	Ettevõttekaart
PSO: Compute Digital Signature	Ei kohaldata	Ei kohaldata	Ei kohaldata	Ei kohaldata
PSO: Hash	Ei kohaldata	Ei kohaldata	Ei kohaldata	Ei kohaldata
PSO: Hash of File	Ei kohaldata	Ei kohaldata	Ei kohaldata	Ei kohaldata
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Ei kohaldata	ALW	Ei kohaldata	Ei kohaldata

TCS_28 Sõidumeerikukaart võib, aga ei pruugi vastu võtta turbetingimustes määratust kõrgema turbetasemega käsku. Seega kui turbetingimus on ALW (või PLAIN-C), võib kaart käsu vastu võtta turvalise sõnumivahetusega (krüpteerimis- ja/või autentimisrežiim). Kui turbetingimus nõuab koos autentimisrežiimiga turvalist sõnumivahetust, võib sõidumeerikukaart autentimis- ja krüpteerimisrežiimis käsu vastu võtta sama põlvkonna turvalise sõnumivahetusega.

Märkus: käskude kirjelduses on esitatud rohkem teavet erinevate sõidumeerikukaardi tüüpide ja erifailide toetatud käskude kohta.

3.4. **Käskude ja veakoodide ülevaade**

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

Käesolevas punktis kirjeldatakse järgmisi käsu-vastuse APDU paare. Käskude variandid, mida toetab nii 1. kui ka 2. põlvkonna rakendus, on täpsustatud vastava käsu kirjelduses.

Käsk	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	

Käsk	INS
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 Igas vastusesõnumis saadetakse olekubaidid SW1 ja SW2, millega märgitakse 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	00	Autentimise ebaõnnestumine (hoiatus)
63	CX	Vale CHV (PIN). Järelejäänud katsete loendur on ‘X’.
64	00	Täitmisviga – säilmälu olek muutmata. Terviklusviga.
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 vale krüptogramm (välise autentimise ajal) või vale allkiri (allkirja kontrollimise ajal).
67	00	Vale pikkus (vale Lc või Le).
68	82	Turvalist sõnumivahetust ei toetata.
68	83	Oodatakse ahela viimast käsku.
69	00	Keelatud käsk (protokollis T = 0 ei ole vastust).
69	82	Turbeoleku nõuded ei ole täidetud.
69	83	Autentimismeetod blokeeritud.
69	85	Kasutustingimused ei ole täidetud.
69	86	Käsk ei ole lubatud (kasutatav elementaarfail puudub).

SW1	SW2	Tähendus
69	87	Oodatavad turvalise sõnumivahetuse andmeobjektid on puudu.
69	88	Ebaõiged turvalise sõnumivahetuse andmeobjektid.
6A	80	Andmeväljal on ebaõiged parameetrid.
6A	82	Faili ei leitud.
6A	86	Valed parameetrid P1-P2.
6A	88	Viiteandmeid ei leitud.
6B	00	Valed parameetrid (nihe elementaarfailist välja).
6C	XX	Vale pikkus, SW2 näitab täpset pikkust. Ühtki andmevälja ei saadeta tagasi.
6D	00	Käsukoodil puudub tugi või see on kehtetu.
6E	00	Klassil puudub tugi.
6F	00	Muud kontrollivead.

TCS_30 Kui ühes käsu APDU-s on täidetud rohkem kui üks veatingimus, võib kaart tagastada ükskõik millise asjaomase olekubaidi.

3.5. **Käskude kirjeldus**

Käesolevas punktis kirjeldatakse sõidumeerikukaartide kohustuslikke käske.

Asjaomased lisaüksikasjad, mis puudutavad 1. ja 2. põlvkonna sõidumeerikutega seotud krüptograafilisi toiminguid, on esitatud 11. liites „Ühised turbemehhanismid“.

Kõiki käske on kirjeldatud kasutatavast 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 pikkuse, väärtuse ja kirjelduse lahter tühi.

TCS_31 Kui nõutakse mõlemat pikkusbaiti (Lc ja Le), tuleb kirjeldatud käsk jagada kaheks osaks, kui liideseseade kasutab protokolli T = 0: liideseseade saadab kirjeldusekohase käsu, kus P3 = Lc + data, ja siis saadab käsu GET_RESPONSE (vt punkt 3.5.6), kus P3 = Le.

TCS_32 Kui nõutakse mõlemat pikkusbaiti ja Le = 0 (turvaline sõnumivahetus):

— kui kasutatakse protokolli T = 1, saadab kaart vastuseks teatele Le = 0 kõik olemasolevad väljundandmed;

— kui kasutatakse protokolli T = 0, saadab liideseseade esimese käsu teatega P3 = Lc + data, kaart vastab (sellest järelduvale teatele Le = 0) olekubaitidega '**61La**', kus La on vastusbaitide arv, mida on võimalik kasutada. Seejärel genereerib liideseseade andmete lugemiseks käsu GET RESPONSE, kus P3 = La.

TCS_33 Vastavalt standardile ISO/IEC 7816-4 võib sõidumeerikukaart valitava funktsioonina toetada ka laiendatud väljasid. Laiendatud väljasid toetav sõidumeerikukaart:

— näitab laiendatud väljade toetust lähtestuse vastuses (ATR);

— esitab toetatud puhvrimahu elementaarfailis ATR/INFO oleva laiendatud välju käsitleva teabe kaudu, vt TCS_146;

— teatab elementaarfailis Extended_Length, kas ta toetab laiendatud väljasid protokolli T = 1 ja/või T = 0 korral, vt TCS_147;

— toetab laiendatud väljasid 1. ja 2. põlvkonna sõidumeerikurakenduste puhul.

Märkused.

Kõigi käskude kirjeldus on esitatud lühikese välja kohta. Laiendatud väljaga APDU-de kasutamine nähtub standardist ISO/IEC 7816-4.

Üldiselt on käskude kirjeldus esitatud lihtteksti jaoks, st ilma turvalise sõnumivahetuseta; turvalise sõnumivahetuse spetsifikatsioon on esitatud 11. liites. Käsu juurdepääsueeskirjade põhjal on selge, kas käsk peab turvalist sõnumivahetust toetama või mitte ning kas käsk peab toetama 1. ja/või 2. põlvkonna turvalist sõnumivahetust. Mõne käsuvariandi kirjeldus on esitatud koos turvalise sõnumivahetusega, et näitlikustada turvalise sõnumivahetuse kasutamist.

TCS_34 Sõidukiseade kasutab seansi jaoks sõidukiseadme ja kaardi vahelist 2. põlvkonna täieliku vastastikuse autentimise protokolli, mis hõlmab (vajaduse korral) sertifikaadi kontrolli, erifailis Tachograph, erifailis Tachograph_G2 või põhifailis.

3.5.1. *SELECT*

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

Käsku SELECT kasutatakse:

— rakenduse erifaili valimiseks (valida tuleb nime alusel);

— elementaarfaili valimiseks, mis vastab esitatud faili identifikaatorile.

3.5.1.1. Valik nime alusel (AID)

Käsk võimaldab valida kaardil rakenduse erifaili.

TCS_35 Seda käsku saab anda faili struktuuris mis tahes kohas (pärast ATRi või mis tahes ajal).

TCS_36 Rakenduse valik lähtestab hetke turbekeskkonna. Pärast rakenduse valimist ei ole enam ükski avalik võti valitud. Samuti ei kehti enam juurdepääsutingimus EXT-AUT-G1. Kui käsk täideti ilma turvalise sõnumivahetuseta, ei ole varasemad turvalise sõnumivahetuse seansi võtmed enam kasutatavad.

TCS_37 **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’sõidumeerikurakenduse korral
#6-#(5+NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ 1. põlvkonna sõidumeerikurakenduse korral AID: ‘FF 53 4D 52 44 54’ 2. põlvkonna sõidumeerikurakenduse korral

Käsk SELECT ei vaja vastust (T = 1 puhul Le puudub, T = 0 puhul vastust ei küsita).

TCS_38 **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 töötlusvastus '**6A82**'.

— Protokollis T = 1, kui bait Le on olemas, on töötlusvastus '**6700**'.

— Protokollis T = 0, kui küsitakse vastust pärast käsku SELECT, on töötlusvastus '**6900**'.

— Kui valitud rakendus loetakse vigaseks (faili atribuutide hulgas on tuvastatud terviklusviga), on töötlusvastus '**6400**' või '**6581**'.

3.5.1.2. Elementaarfaili valik, kasutades selle faili identifikaatorit

TCS_39 **Käsusõnum**

TCS_40 Selle käsuvariandi puhul peab sõidumeerikukaart toetama 2. põlvkonna turvalist sõnumivahetust vastavalt 11. liite B osale.

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

Käsk SELECT ei vaja vastust (T = 1 puhul Le puudub, T = 0 puhul vastust ei küsita).

TCS_41 **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 töötlusvastus '**6A82**'.

— Protokollis T = 1, kui bait Le on olemas, on töötlusvastus '**6700**'.

— Protokollis T = 0, kui küsitakse vastust pärast käsku SELECT, on töötlusvastus '**6900**'.

— Kui valitud fail loetakse vigaseks (faili atribuutide hulgas on tuvastatud terviklusviga), on töötlusvastus '**6400**' või '**6581**'.

3.5.2. *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.

3.5.2.1. Käsk koos nihkega P1-P2

Käsk võimaldab liideseseadmel lugeda hetkel valitud elementaarfailist andmeid turvalise sõnumivahetuseta.

Märkus: seda ilma turvalise sõnumivahetuseta käsku saab kasutada ainult sellise faili lugemiseks, mis toetab lugemise juurdepääsuõiguste režiimis turbetingimust ALW.

TCS_42 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'B0h'	Binaarfaili lugemine
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_43 **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 turbetingimused 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 > EF), saadakse töötlusvastus '**6700**' või '**6Cxx**', kus 'xx' näitab täpset pikkust.

— Kui faili atribuutide hulgas on tuvastatud terviklusviga, peab kaart faili vigaseks ja taastamatuks ning töötlusvastus on '**6400**' või '**6581**'.

— Kui salvestatud andmete hulgas on tuvastatud terviklusviga, saadab kaart nõutud andmed tagasi ja töötlusvastus on '**6281**'.

3.5.2.1.1. Käsk turvalise sõnumivahetusega (näited)

Käsk võimaldab liideseseadmel lugeda hetkel valitud elementaarfailist andmeid turvalise sõnumivahetusega, et kontrollida saadud andmete terviklust ja kaitsta andmete konfidentsiaalsust, kui kasutatakse turbetingimust SM-R-ENC-MAC-G1 (1. põlvkond) või SM-R-ENC-MAC-G2 (2. põlvkond).

TCS_44 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'0Ch'	Nõutakse turvalist sõnumivahetust
INS	1	'B0h'	Binaarfaili lugemine
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	'XXh'	Sisendandmete pikkus turvaliseks sõnumivahetuseks
#6	1	'97h'	$_{TLE}$: oodatava pikkusmääratluse silt
#7	1	'01h'	$_{LLE}$: oodatavate andmete pikkus
#8	1	'NNh'	Oodatav pikkusmääratlus (algne Le): loetavate baitide arv
#9	1	'8Eh'	T_{CC}: krüptograafilise kontrollsumma silt
#10	1	'XXh'	$_{LCC}$: järgmise krüptograafilise kontrollsumma pikkus '04h' 1. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite A osa) Olenevalt AES-i võtme pikkusest '08h', '0Ch' või '10h' 2. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite B osa)
#11-#(10+L)	L	'XX..XXh'	krüptograafiline kontrollsumma
Le	1	'00h'	Vastavalt standardile ISO/IEC 7816-4

TCS_45 **Vastusesõnum juhul, kui tingimus SM-R-ENC-MAC-G1 (1. põlvkond) / SM-R-ENC-MAC-G2 (2. põlvkond) ei ole nõutav ja turvalise sõnumivahetuse sisendvorming on õige:**

Bait	Pikkus	Väärtus	Kirjeldus
#1	1	'99h'	Töötlusvastuse silt (SW1-SW2) – 1. põlvkonna turvalise sõnumivahetuse korral vabatahtlik
#2	1	'02h'	Töötlusvastuse pikkus
#3 – #4	2	'XX XXh'	Kaitsmata vastuse APDU töötlusvastus
#5	1	'81h'	$_{TPV}$: lihtväärtusega andmete silt
#6	L	'NNh' või '81 NNh'	$_{LPV}$: vastuseks saadetavate andmete pikkus (= algne Le) L on 2 baiti, kui LPV > 127 baiti

Bait	Pikkus	Väärtus	Kirjeldus
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Lihtandmete väärtus
#(6+L+NN)	1	'8Eh'	T_{CC}: krüptograafilise kontrollsumma silt
#(7+L+NN)	1	'XXh'	$_{LCC}$: järgmise krüptograafilise kontrollsumma pikkus '04h' 1. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite A osa) Olenevalt AES-i võtme pikkusest '08h', '0Ch' või '10h' 2. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite B osa)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	krüptograafiline kontrollsumma
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

TCS_46 **Vastusesõnum juhul, kui tingimus SM-R-ENC-MAC-G1 (1. põlvkond) / SM-R-ENC-MAC-G2 (2. põlvkond) on nõutav ja turvalise sõnumivahetuse sisendvorming on õige:**

Bait	Pikkus	Väärtus	Kirjeldus
#1	1	'87h'	$_{TPI\ CG}$: krüpteeritud andmete silt (krüptogramm)
#2	L	'MMh' või '81 MMh'	$_{LPI\ CG}$: vastuseks saadetavate krüpteeritud andmete pikkus (erineb käsu algsest Le-st täidise poolest). L on 2 baiti, kui LPI CG > 127 baiti.
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Krüpteeritud andmed: täidise indikaator ja krüptogramm
#(2+L+MM)	1	'99h'	Töötlusvastuse silt (SW1-SW2) – 1. põlvkonna turvalise sõnumivahetuse korral vabatahtlik
#(3+L+MM)	1	'02h'	Töötlusvastuse pikkus
#(4+L+MM) – #(5+L+MM)	2	'XX XXh'	Kaitsmata vastuse APDU töötlusvastus
#(6+L+MM)	1	'8Eh'	T_{CC}: krüptograafilise kontrollsumma silt
#(7+L+MM)	1	'XXh'	$_{LCC}$: järgmise krüptograafilise kontrollsumma pikkus '04h' 1. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite A osa) Olenevalt AES-i võtme pikkusest '08h', '0Ch' või '10h' 2. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite B osa)
#(8+L+MM)-#(7+N+L+MM)	N	'XX..XXh'	krüptograafiline kontrollsumma
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

Käsu READ BINARY võidakse saata tavalised töötlusvastused, mis on loetletud punktis TCS_43 sildi '99h' vastavalt punktis TCS_59 esitatud kirjeldusele, kasutades turvalise sõnumivahetuse vastuse struktuuri.

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

TCS_47 **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 (vastavalt eespool esitatud kirjeldusele), saadakse töötlusvastus '**6987**': see viga tekib siis, kui oodatud silt puudub või kui käsu tekst ei ole nõuetekohaselt konstrueeritud.

— Kui mõned andmeobjektid on valed, saadakse töötlusvastus '**6988**': see viga tekib siis, kui kõik vajalikud sildid on olemas, aga mõned pikkused erinevad oodatust.

— Kui krüptograafilise kontrollsumma tõendamine ei õnnestu, saadakse töötlusvastus '**6688**'.

3.5.2.2. Käsk koos elementaarfaili lühikese identifikaatoriga

See käsuvariant võimaldab liideseseadmel kasutada elementaarfaili valimiseks lühikest identifikaatorit ja lugeda sellest elementaarfailist andmeid.

TCS_48 Sõidumeerikukaart peab seda käsuvarianti toetama kõigi elementaarfailide puhul, millele on ette nähtud lühike identifikaator. Nende elementaarfaili lühikeste identifikaatorite spetsifikatsioon on esitatud 4. peatükis.

TCS_49 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'B0h'	Binaarfaili lugemine
P1	1	'XXh'	8. biti väärtus on 1. 7. ja 6. biti väärtus on 00. Bitid 5–1 sisaldavad vastava elementaarfaili lühikese identifikaatori koodi
P2	1	'XXh'	Kodeerib parameetris P1 osutatud elementaarfailis nihke vahemikus 0–255 baiti
Le	1	'XXh'	Vastuseks saadavate andmete pikkus. Loetavate baitide arv.

Märkus: 2. põlvkonna sõidumeerikurakenduses kasutatavate elementaarfaili lühikeste identifikaatorite spetsifikatsioon on esitatud 4. peatükis.

Kui parameetris P1 on kodeeritud elementaarfaili lühike identifikaator ja käsu täitmine õnnestub, muutub identifikaatoriga tähistatud elementaarfail valitud elementaarfailiks (elementaartööfail).

TCS_50 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui elementaarfaili identifikaatorile vastavat faili ei leita, on töötlusvastus '**6A82**'.

— Kui valitud faili turbetingimused 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 > EF), saadakse töötlusvastus '**6700**' või '**6Cxx**', kus 'xx' näitab täpset pikkust.

— Kui faili atribuutide hulgas on tuvastatud terviklusviga, peab kaart faili vigaseks ja taastamatuks ning töötlusvastus on '**6400**' või '**6581**'.

— Kui salvestatud andmete hulgas on tuvastatud terviklusviga, saadab kaart nõutud andmed tagasi ja töötlusvastus on '**6281**'.

3.5.2.3. Paaritu korraldusbaidiga käsk

See käsuvariant võimaldab liideseseadmel lugeda andmeid 32 768 baidi suurusest või suuremast elementaarfailist.

TCS_51 Kui sõidumeerikukaart toetab 32 768 baidi suuruseid või suuremaid elementaarfaile, peab see toetama seda käsuvarianti kõnealuste elementaarfailide puhul. Sõidumeerikukaart võib seda käsuvarianti toetada ka muude elementaarfailide puhul, aga see ei ole kohustuslik, välja arvatud elementaarfail Sensor_Installation_Data, vt punktid TCS_156 ja TCS_160.

TCS_52 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'B1h'	Binaarfaili lugemine
P1	1	'00h'	Elementaartööfail
P2	1	'00h'	
Lc	1	'NNh'	Lc nihke andmeobjekti pikkus.
#6-#(5+NN)	NN	'XX..XXh'	Nihke andmeobjekt: Silt '54h' Pikkus '01h' või '02h' Väärtus nihe
Le	1	'XXh'	Loetavate baitide arv.

Liideseseade kodeerib nihke andmeobjekti pikkuse minimaalse võimaliku oktettide arvuga, st et pikkusebaidi '01h' kasutamise korral kodeerib liideseseade nihke vahemikus 0–255 ja pikkusebaidi '02h' kasutamise korral kodeerib liideseseade nihke vahemikus 256–65 535 baiti.

TCS_53 **Vastusesõnum**

Bait	Pikkus	Väärtus	Kirjeldus
#1-#L	L	'XX..XXh'	Loetud andmed sisalduvad valikulises andmeobjektis sildiga '53h'.
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui elementaarfaili ei ole valitud, saadakse töötlusvastus '**6986**'.

— Kui valitud faili turbetingimused 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 > EF), saadakse töötlusvastus '**6700**' või '**6Cxx**', kus 'xx' näitab täpset pikkust.

— Kui faili atribuutide hulgas on tuvastatud terviklusviga, peab kaart faili vigaseks ja taastamatuks ning töötlusvastus on '**6400**' või '**6581**'.

— Kui salvestatud andmete hulgas on tuvastatud terviklusviga, saadab kaart nõutud andmed tagasi ja töötlusvastus on '**6281**'.

3.5.2.3.1. Käsk turvalise sõnumivahetusega (näide)

Järgmine näide kirjeldab turvalise sõnumivahetuse kasutamist juhul, kui kehtib turbetingimus SM-MAC-G2.

TCS_54 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'0Ch'	Nõutakse turvalist sõnumivahetust
INS	1	'B1h'	Binaarfaili lugemine
P1	1	'00h'	Elementaartööfail
P2	1	'00h'	
Lc	1	'XXh'	Turvatud andmevälja pikkus
#6	1	'B3h'	BER-TLV-s kodeeritud lihtandmete silt
#7	1	'NNh'	L_{PV}: edastavate andmete pikkus
#(8)-#(7+NN)	NN	'XX..XXh'	BER-TLV-s kodeeritud lihtandmed, st nihke andmeobjekt sildiga '54'
#(8+NN)	1	'97h'	T_{LE}: oodatava pikkusmääratluse silt
#(9+NN)	1	'01h'	L_{LE}: oodatavate andmete pikkus
#(10+NN)	1	'XXh'	Oodatav pikkusmääratlus (algne Le): loetavate baitide arv
#(11+NN)	1	'8Eh'	T_{CC}: krüptograafilise kontrollsumma silt
#(12+NN)	1	'XXh'	L_{CC}: järgmise krüptograafilise kontrollsumma pikkus Olenevalt AES-i võtme pikkusest '08h', '0Ch' või '10h' 2. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite B osa)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Krüptograafiline kontrollsumma
Le	1	'00h'	Vastavalt standardile ISO/IEC 7816-4

TCS_55 Vastusesõnum käsu õnnestumise korral

Bait	Pikkus	Väärtus	Kirjeldus
#1	1	'B3h'	BER-TLV-s kodeeritud lihtandmed
#2	L	'NNh' või '81 NNh'	L_{PV}: vastuseks saadetavate andmete pikkus (= algne Le) L on 2 baiti, kui L_{PV} > 127 baiti
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	BER-TLV-s kodeeritud lihtandmete väärtus, st loetud andmed sisalduvad valikulises andmeobjektis sildiga '53h'.
#(2+L+NN)	1	'99h'	Kaitsmata vastuse APDU töötlusvastus
#(3+L+NN)	1	'02h'	Töötlusvastuse pikkus
#(4+L+NN) – #(5+L+NN)	2	'XX XXh'	Kaitsmata vastuse APDU töötlusvastus
#(6+L+NN)	1	'8Eh'	T_{CC}: krüptograafilise kontrollsumma silt
#(7+L+NN)	1	'XXh'	L_{CC}: järgmise krüptograafilise kontrollsumma pikkus Olenevalt AES-i võtme pikkusest '08h', '0Ch' või '10h' 2. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite B osa)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Krüptograafiline kontrollsumma
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

3.5.3. *UPDATE BINARY*

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

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

3.5.3.1. Käsk koos nihkega P1-P2

Käsk võimaldab liideseseadmel kirjutada hetkel valitud elementaarfaili andmeid, kusjuures kaart ei tõenda saadud andmete terviklust.

Märkus: seda ilma turvalise sõnumivahetuseta käsku saab kasutada ainult sellise faili ajakohastamiseks, mis toetab ajakohastamise juurdepääsuõiguste režiimis turbetingimust ALW.

TCS_56 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'D6h'	Binaarfaili ajakohastamine

Bait	Pikkus	Väärtus	Kirjeldus
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_57 **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 turbetingimused ei ole täidetud, katkestatakse käsk sõnumiga '**6982**'.

— Kui nihe ei vasta elementaarfaili suurusele (nihe > EFi suurus), saadakse töötlusvastus '**6B00**'.

— Kui kirjutatavate andmete suurus ei vasta elementaarfaili suurusele (nihe + Lc > EF), saadakse töötlusvastus '**6700**'.

— Kui faili atribuutide hulgas on tuvastatud terviklusviga, peab kaart faili vigaseks ja taastamatuks ning töötlusvastus on '**6400**' või '**6500**'.

— Kui kirjutamine ebaõnnestub, saadakse töötlusvastus '**6581**'.

3.5.3.1.1. Käsk turvalise sõnumivahetusega (näited)

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

TCS_58 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'0Ch'	Nõutakse turvalist sõnumivahetust
INS	1	'D6h'	Binaarfaili ajakohastamine
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

Bait	Pikkus	Väärtus	Kirjeldus
#6	1	'81h'	T_{PV}: lihtväärtusega andmete silt
#7	L	'NNh' või '81 NNh'	L_{PV}: edastavate andmete pikkus. L on 2 baiti, kui LPV > 127 baiti
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Lihtandmete väärtus (kirjutatavad andmed)
#(7+L+NN)	1	'8Eh'	T_{CC}: krüptograafilise kontrollsumma silt
#(8+L+NN)	1	'XXh'	L_{CC}: järgmise krüptograafilise kontrollsumma pikkus '04h' 1. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite A osa) Olenevalt AES-i võtme pikkusest '08h', '0Ch' või '10h' 2. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite B osa)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Krüptograafiline kontrollsumma
Le	1	'00h'	Vastavalt standardile ISO/IEC 7816-4

TCS_59 **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'	Kaitsmata vastuse APDU töötlusvastus
#5	1	'8Eh'	T_{CC}: krüptograafilise kontrollsumma silt
#6	1	'XXh'	L_{CC}: järgmise krüptograafilise kontrollsumma pikkus '04h' 1. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite A osa) Olenevalt AES-i võtme pikkusest '08h', '0Ch' või '10h' 2. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite B osa)
#7-#(6+L)	L	'XX..XXh'	Krüptograafiline kontrollsumma
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

Vastuseks võib saata „tavalisi" töötlusvastuseid, mida on kirjeldatud turvalise sõnumivahetuseta käsu UPDATE BINARY juures (vt punkt 3.5.3.1), kasutades eespool kirjeldatud vastusesõnumi struktuuri.

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

TCS_60 **Vastusesõnum turvalise sõnumivahetuse vea korral**

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 (vastavalt eespool esitatud kirjeldusele), saadakse töötlusvastus '**6987**': see viga tekib siis, kui oodatud silt puudub või kui käsu tekst ei ole nõuetekohaselt konstrueeritud.

— Kui mõned andmeobjektid on valed, saadakse töötlusvastus '**6988**': see viga tekib siis, kui kõik vajalikud sildid on olemas, aga mõned pikkused erinevad oodatust.

— Kui krüptograafilise kontrollsumma kontrollimine ei õnnestu, saadakse töötlusvastus '**6688**'.

3.5.3.2. Käsk koos elementaarfaili lühikese identifikaatoriga

See käsuvariant võimaldab liideseseadmel kasutada elementaarfaili valimiseks lühikest identifikaatorit ja kirjutada sellest elementaarfailist saadud andmeid.

TCS_61 Sõidumeerikukaart peab seda käsuvarianti toetama kõigi elementaarfailide puhul, millele on ette nähtud lühike identifikaator. Nende elementaarfaili lühikeste identifikaatorite spetsifikatsioon on esitatud 4. peatükis.

TCS_62 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'D6h'	Binaarfaili ajakohastamine
P1	1	'XXh'	8. biti väärtus on 1. 7. ja 6. biti väärtus on 00. Bitid 5–1 sisaldavad vastava elementaarfaili lühikese identifikaatori koodi
P2	1	'XXh'	Kodeerib parameetris P1 osutatud elementaarfailis nihke vahemikus 0–255 baiti
Lc	1	'NNh'	Lc ajakohastatavate andmete pikkus. Kirjutatavate baitide arv.
#6-#(5+NN)	NN	'XX..XXh'	Kirjutatavad andmed

TCS_63 **Vastusesõnum**

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

Märkus: 2. põlvkonna sõidumeerikurakenduses kasutatavate elementaarfaili lühikeste identifikaatorite spetsifikatsioon on esitatud 4. peatükis.

Kui parameetris P1 on kodeeritud elementaarfaili lühike identifikaator ja käsu täitmine õnnestub, muutub identifikaatoriga tähistatud elementaarfail valitud elementaarfailiks (elementaartööfail).

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui elementaarfaili identifikaatorile vastavat faili ei leita, on töötlusvastus '**6A82**'.

— Kui valitud faili turbetingimused ei ole täidetud, katkestatakse käsk sõnumiga '**6982**'.

— Kui nihe ei vasta elementaarfaili suurusele (nihe > EFi suurus), saadakse töötlusvastus '**6B00**'.

— Kui kirjutatavate andmete suurus ei vasta elementaarfaili suurusele (nihe + Lc > EF), saadakse töötlusvastus '**6700**'.

— Kui faili atribuutide hulgas on tuvastatud terviklusviga, peab kaart faili vigaseks ja taastamatuks ning töötlusvastus on '**6400**' või '**6581**'.

— Kui kirjutamine ebaõnnestub, saadakse töötlusvastus '**6581**'.

3.5.3.3. Paaritu korraldusbaidiga käsk

See käsuvariant võimaldab liideseseadmel kirjutada andmeid 32 768 baidi suurusesse või suuremasse elementaarfaili.

TCS_64 Kui sõidumeerikukaart toetab 32 768 baidi suuruseid või suuremaid elementaarfaile, peab see toetama seda käsuvarianti kõnealuste elementaarfailide puhul. Sõidumeerikukaart võib seda käsuvarianti toetada ka muude elementaarfailide puhul, aga see ei ole kohustuslik.

TCS_65 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'D7h'	Binaarfaili ajakohastamine
P1	1	'00h'	Elementaartööfail
P2	1	'00h'	
Lc	1	'NNh'	Lc käsu andmeväljal olevate andmete pikkus
#6-#(5+NN)	NN	'XX..XXh'	Nihke andmeobjekt sildiga '54h' || Kirjutatavaid andmeid sisaldav valikuline andmeobjekt sildiga '53h'

Liideseseade kodeerib nihke andmeobjekti ja valikulise andmeobjekti pikkuse minimaalse võimaliku oktettide arvuga, st et pikkusebaidi '01h' kasutamise korral kodeerib liideseseade nihke/pikkuse vahemikus 0–255 ja pikkusebaidi '02h' kasutamise korral kodeerib liideseseade nihke/pikkuse vahemikus 256–65 535 baiti.

TCS_66 **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 turbetingimused ei ole täidetud, katkestatakse käsk sõnumiga '**6982**'.

— Kui nihe ei vasta elementaarfaili suurusele (nihe > EFi suurus), saadakse töötlusvastus '**6B00**'.

— Kui kirjutatavate andmete suurus ei vasta elementaarfaili suurusele (nihe + Lc > EF), saadakse töötlusvastus '**6700**'.

— Kui faili atribuutide hulgas on tuvastatud terviklusviga, peab kaart faili vigaseks ja taastamatuks ning töötlusvastus on '**6400**' või '**6500**'.

— Kui kirjutamine ebaõnnestub, saadakse töötlusvastus '**6581**'.

3.5.3.3.1. Käsk turvalise sõnumivahetusega (näide)

Järgmine näide kirjeldab turvalise sõnumivahetuse kasutamist juhul, kui kehtib turbetingimus SM-MAC-G2.

TCS_67 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'0Ch'	Nõutakse turvalist sõnumivahetust
INS	1	'D7h'	Binaarfaili ajakohastamine
P1	1	'00h'	Elementaartööfail
P2	1	'00h'	
Lc	1	'XXh'	Turvatud andmevälja pikkus
#6	1	'B3h'	BER-TLV-s kodeeritud 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'	BER-TLV-s kodeeritud lihtandmed, st nihke andmeobjekt sildiga '54' || Kirjutatavaid andmeid sisaldav valikuline andmeobjekt sildiga '53h'
#(7+L+NN)	1	'8Eh'	T_{CC}: krüptograafilise kontrollsumma silt
#(8+L+NN)	1	'XXh'	L_{CC}: järgmise krüptograafilise kontrollsumma pikkus Olenevalt AES-i võtme pikkusest '08h', '0Ch' või '10h' 2. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite B osa)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Krüptograafiline kontrollsumma
Le	1	'00h'	Vastavalt standardile ISO/IEC 7816-4

TCS_68 Vastusesõnum käsu õnnestumise 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'	Kaitsmata vastuse APDU töötlusvastus
#5	1	'8Eh'	T_{CC}: krüptograafilise kontrollsumma silt

Bait	Pikkus	Väärtus	Kirjeldus
#6	1	'XXh'	L_{CC}: järgmise krüptograafilise kontrollsumma pikkus Olenevalt AES-i võtme pikkusest '08h', '0Ch' või '10h' 2. põlvkonna turvalise sõnumivahetuse korral (vt 11. liite B osa)
#7-#(6+L)	L	'XX..XXh'	Krüptograafiline kontrollsumma
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

3.5.4. *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_69 Kaardi väljaantud pretensioon kehtib ainult kaardile saadetava järgmise käsu puhul, mis kasutab pretensiooni.

TCS_70 **Käsusõnum**

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

TCS_71 **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**'.

3.5.5. *VERIFY*

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

Seda käsku peab toetama ainult töökojakaart.

Muudel sõidumeerikukaartidel ei ole selle käsu rakendamine kohustuslik, kuid neil kaartidel ei kasutata isikustatud viidet kaardiomaniku tuvastusinfole. Seetõttu ei suuda nimetatud kaardid seda käsku täita. Töökojakaardist erinevate sõidumeerikukaartide käitumist selle käsu saatmise korral, st vastuseks veakoodi saatmist käesolevas spetsifikatsioonis ei käsitleta.

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

TCS_72 Kasutaja sisestatud PIN-kood peab koosnema ASCII märkidest ning peab paremal pool olema liideseseadme poolt täidistatud baitidega 'FFh' pikkusega kuni 8 baiti, vt ka 1. liites andmetüüpi WorkshopCardPIN.

TCS_73 1. ja 2. põlvkonna sõidumeerikurakendused peavad kasutama sama kaardiomaniku tuvastusinfo võrdluskoodi.

TCS_74 Sõidumeerikukaart kontrollib, kas käsk on õigesti kodeeritud. Kui käsk ei ole õigesti kodeeritud, ei võrdle kaart kaardiomaniku tuvastusinfo väärtusi, ei vähenda allesjäänud tuvastuskatsete loenduri näitu ning ei lähtesta turbeolekut „PIN_Verified", vaid katkestab käsu täitmise. Käsk on õigest kodeeritud siis, kui baitidel CLA, INS, P1, P2, Lc on ettenähtud väärtused, Le puudub ja käsu andmeväli on õige pikkusega.

TCS_75 Kui käsk on edukas, viiakse tuvastuskatsete loendur tagasi esialgsesse olekusse. Allesjäänud tuvastuskatsete loenduri algnäidu väärtus on 5. Kui käsu täitmine õnnestub, määrab kaart sisemise turbeoleku „PIN_Verified". Kaart lähtestab selle turbeoleku kaardi lähtestamise korral või juhul, kui käsus edastatud kaardiomaniku tuvastusinfo kood ei vasta salvestatud võrdluskoodile.

Märkus: kaardiomaniku tuvastusinfo sama võrdluskoodi ja üldise turbeoleku kasutamine välistab vajaduse, et töökoja töötaja peaks pärast mõne teise sõidumeerikurakenduse erifaili valimist PIN-koodi uuesti sisestama.

TCS_76 Ebaõnnestunud võrdlus registreeritakse kaardil, st allesjäänud tuvastuskatsete loenduri väärtus väheneb ühe võrra, piiramaks edasisi katseid kasutada kaardiomaniku tuvastusinfot.

TCS_77 **Käsusõnum**

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

TCS_78 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui kaardiomaniku tuvastusinfo võrdluskoodi ei leita, saadakse töötlusvastus '**6A88**'.

— Kui kaardiomaniku tuvastusinfo on blokeeritud (allesjäänud tuvastuskatsete loendur on nulli jõudnud), saadetakse töötlusvastus '**6983**'. Kui on jõutud sellisesse olekusse, ei saa kaardiomaniku tuvastusinfot enam kunagi edukalt esitada.

— Kui võrdluses vastavust ei tuvastata, vähendatakse allesjäänud katsete loenduri näitu ning saadakse töötlusvastus '**63CX**' (X > 0 ja X võrdub järelejäänud katsete arvuga).

— Kui leitakse, et kaardiomanik tuvastusinfo võrdluskood on rikutud, saadakse töötlusvastus '**6400**' või '**6581**'.

— Kui Lc erineb '08h'-st, saadakse töötlusvastus '**6700**'.

3.5.6. *GET RESPONSE*

Käsk vastab standardile ISO/IEC 7816-4.

Käsku (mis on vajalik ja kasutatav ainult protokolli T = 0 puhul) kasutatakse ettevalmistatud andmete edastamiseks kaardilt liideseseadmesse (juhul kui käsk hõlmab nii baiti Lc kui ka 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 tekib viga '**61xx**' või '**6Cxx**' – vt allpool).

TCS_79 **Käsusõnum**

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

TCS_80 **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 jaoks endiselt 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 veel võimalik kasutada järgmise käsu GET RESPONSE korral.

— Kui käsul puudub tugi (protokoll T = 1), vastab kaart '**6D00**'.

3.5.7. *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.

3.5.7.1. 1. põlvkonna käsu ja vastuse paar

TCS_81 Seda käsuvarianti toetab ainult 1. põlvkonna sõidumeerikurakendus.

TCS_82 Kui käsk VERIFY CERTIFICATE on edukas, salvestatakse avalik võti edaspidiseks kasutamiseks. Käsk MSE (vt punkt 3.5.11) kasutab selle võtme identifikaatorit otseselt turbega seotud käskude korral (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE või VERIFY CERTIFICATE).

TCS_83 Igal juhul kasutab käsk VERIFY CERTIFICATE sertifikaadi avamiseks avalikku võtit, mille käsk MSE on eelnevalt valinud. See avalik võti peab olema liikmesriigi või Euroopa võti.

TCS_84 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'2Ah'	Turbetoimingu tegemine
P1	1	'00h'	P1
P2	1	'AEh'	P2: mitte BER-TLV kodeeritud andmed (andmeelementide konkatenatsioon)
Lc	1	'C2h'	Lc: sertifikaadi pikkus, 194 baiti
#6-#199	194	'XX..XXh'	Sertifikaat: andmeelementide konkatenatsioon (11. liite kirjelduse kohaselt)

TCS_85 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui sertifikaadi kontrollimine ebaõnnestub, saadakse töötlusvastus '**6688**'. Sertifikaadi kontrollimise ja lahtipakkimise protsessi on seoses 1. ja 2. põlvkonnaga kirjeldatud 11. liites.

— Kui turbekeskkonnas ei ole ühtegi avalikku võtit, saadakse töötlusvastus '**6A88**'.

— Kui (sertifikaadi lahtipakkimiseks kasutatud) valitud avalik võti loetakse rikutuks, saadakse töötlusvastus '**6400**' või '**6581**'.

— Ainult 1. põlvkond: kui (sertifikaadi lahtipakkumiseks kasutatud) avaliku võtme andmetüübi CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) väärtus ei ole '00' (st see ei ole liikmesriigi ega Euroopa võti), saadakse töötlusvastus '**6985**'.

3.5.7.2. 2. põlvkonna käsu ja vastuse paar

Olenevalt kõvera suurusest võivad elliptiliste kõverate krüptograafia (ECC) sertifikaadid olla nii pikad, et neid ei ole võimalik ühes APDU-s edastada. Sellisel juhul tuleb kasutada standardi ISO/IEC 7816-4 kohast käskude ahelat, edastades sertifikaati kahe järjestikuse APDU käsuga „PSO: Verify Certificate".

Sertifikaadi struktuur ja domeeni parameetrid on määratletud 11. liites.

TCS_86 Käsku on võimalik täita põhifailis, erifailis Tachograph ja erifailis Tachograph_G2, vt ka punkt TCS_33.

TCS_87 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'X0h'	Klassibait, mis näitab käskude ahela loomist: '00h' ahela ainus või viimane käsk '10h' mitte ahela viimane käsk
INS	1	'2Ah'	Turbetoimingu tegemine
P1	1	'00h'	
P2	1	'BEh'	Kirjeldust sisaldava sertifikaadi kontrollimine
Lc	1	'XXh'	Käsu andmevälja pikkus, vt punktid TCS_88 ja TCS_89.
#6-#5+L	L	'XX..XXh'	DER-TLV-s kodeeritud andmed: esimesel kohal olev andmeobjekt „ECC Certificate Body", mis on ühendatud teisel kohal oleva andmeobjektiga „ECC Certificate Signature", või selle konkatenatsiooni osa. Silti '7F21' ja sellele vastavat pikkust ei edastata. Nende andmeobjektide järjekord on fikseeritud.

TCS_88 Lühikeste APDU-de suhtes kehtivad järgmised nõuded: liideseseade peab kasutama minimaalset vajalikku APDU-de arvu, mis on vajalik käsu sisu edastamiseks, ning edastama käsu esimese APDU-ga maksimaalselt suure arvu baite vastavalt kaardi infovälja mahubaidi väärtusele, vt punkt TCS_14. Kui liideseseade käitub teisiti, siis ei kuulu kaardi käitumine nõude kohaldamisalasse.

TCS_89 Laiendatud APDU-de suhtes kehtivad järgmised nõuded: kui sertifikaat ei mahu ühte APDU-sse, peab kaart toetama käskude ahelat. Liideseseade peab kasutama minimaalset vajalikku APDU-de arvu, mis on vajalik käsu sisu edastamiseks, ning edastama käsu esimese APDU-ga maksimaalselt suure arvu baite. Kui liideseseade käitub teisiti, siis ei kuulu kaardi käitumine nõude kohaldamisalasse.

Märkus: vastavalt 11. liitele salvestab kaart sertifikaadi või sertifikaadi olulise sisu ning ajakohastab oma andmekirjet currentAuthenticatedTime.

Vastusesõnumi struktuur ja olekubaidid on määratletud punktis TCS_85.

TCS_90 Lisaks punktis TCS_85 loetletud veakoodidele võib kaart saata järgmisi veakoode:

— Kui (sertifikaadi lahtipakkimiseks kasutatud) valitud avaliku võtme CHA.LSB (CertificateHolderAuthorisation.equipmentType) ei sobi 11. liite kohaselt sertifikaadi tõendamiseks, saadakse töötlusvastus '**6985**'.

— Kui kaardi ajakirje currentAuthenticatedTime on hilisem kui sertifikaadi aegumise kuupäev, saadakse töötlusvastus '**6985**'.

— Kui oodatakse ahela viimast käsku, vastab kaart '**6883**'.

— Kui käsu andmeväljal saadetakse ebaõiged parameetrid, vastab kaart '**6A80**' (sama vastust kasutatakse ka juhul, kui andmeobjekte ei saadeta nõutud järjekorras).

3.5.8. *INTERNAL AUTHENTICATE*

Käsk vastab standardile ISO/IEC 7816-4.

TCS_91 Kõik sõidumeerikukaardid peavad seda käsku toetama 1. põlvkonna erifailis Tachograph. Käsk võib olla kasutatav põhifailis ja/või erifailis Tachograph_G2, aga see pole kohustuslik. Kui käsku kasutatakse, tuleb see lõpetada sobiva veakoodiga, sest juurdepääs 1. põlvkonna autentimisprotokollis kasutatavale kaardi privaatvõtmele (Card.SK) on võimalik ainult 1. põlvkonna erifailis Tachograph.

Kasutades käsku INTERNAL AUTHENTICATE, saab liideseseade kaardi autentida. Autentimisprotsessi on kirjeldatud 11. liites. See sisaldab järgmisi väiteid:

TCS_92 Käsk INTERNAL AUTHENTICATE kasutab autentimisandmete, sealhulgas K1 (seansivõtme sobivuse esimene element) ja RND1 allkirjastamiseks kaardi (vaikimisi valitud) privaatvõtit ning allkirja kodeerimiseks ja autentimistõendi loomiseks hetkel valitud avalikku võtit (viimase käsu MSE kaudu) (üksikasjad 11. liites).

TCS_93 **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_94 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui turbekeskkonnas ei ole ühtegi avalikku võtit, saadakse töötlusvastus '**6A88**'.

— Kui turbekeskkonnas ei ole ühtegi privaatvõtit, saadakse töötlusvastus '**6A88**'.

— Kui VU.CHR ei vasta kasutusel olevale avaliku võtme identifikaatorile, saadakse töötlusvastus '**6A88**'.

— Kui valitud privaatvõti loetakse rikutuks, saadakse töötlusvastus '**6400**' või '**6581**'.

TCS_95 Kui käsk INTERNAL AUTHENTICATE on edukas, kustutatakse aktiivne seansivõti, kui see oli olemas, ning seda ei saa enam kasutada. Uue seansivõtme saamiseks tuleb 1. põlvkonna autentimismehhanismi käsk EXTERNAL AUTHENTICATE edukalt täita.

3.5.9. *EXTERNAL AUTHENTICATE*

Käsk vastab standardile ISO/IEC 7816-4.

Kasutades käsku EXTERNAL AUTHENTICATE saab kaart liideseseadme autentida. Autentimisprotsessi seoses 1. ja 2. põlvkonna sõidumeerikutega (sõidukiseadme autentimine) on kirjeldatud 11. liites.

TCS_96 Seda 1. põlvkonna vastastikuse autentimise mehhanismi käsuvarianti toetab ainult 1. põlvkonna sõidumeerikurakendus.

TCS_97 Teise põlvkonna sõidumeeriku ja kaardi vastastikuse autentimise käsuvarianti on võimalik täita põhifailis, erifailis Tachograph ja erifailis Tachograph:G2, vt ka punkt TCS_34.

TCS_98 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Vaikimisi teada olevad võtmed ja algoritmid
P2	1	'00h'	
Lc	1	'XXh'	Lc (kaardile saadetud andmete pikkus)
#6-#(5+L)	L	'XX..XXh'	1. põlvkonna autentimine: krüptogramm (vt 11. liite A osa) 2. põlvkonna autentimine: liideseseadme genereeritud allkiri (vt 11. liite B osa)

TCS_99 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui hetkel kasutatava avaliku võtme CHA ei ole sõidumeerikurakenduse identifikaatori ja sõidukiseadme tüübi konkatenatsioon, saadakse töötlusvastus '**6F00**'.

— Kui käsule ei eelne vahetult käsk GET CHALLENGE, saadakse töötlusvastus '**6985**'.

1. põlvkonna sõidumeerikurakendus võib vastuseks saata järgmisi täiendavaid veakoode:

— Kui turbekeskkonnas ei ole ühtegi avalikku võtit, saadakse töötlusvastus '**6A88**'.

— Kui turbekeskkonnas ei ole ühtegi privaatvõtit, saadakse töötlusvastus '**6A88**'.

— Kui krüptogrammi kontrollimine ebaõnnestub, saadakse töötlusvastus '**6688**'.

— Kui valitud privaatvõti loetakse rikutuks, saadakse töötlusvastus '**6400**' või '**6581**'.

2. põlvkonna autentimise käsuvariandi vastuseks võib saada järgmise täiendava veakoodi:

— Kui allkirja kontrollimine ebaõnnestub, vastab kaart '**6300**'.

3.5.10. *GENERAL AUTHENTICATE*

Käsku kasutatakse koos 11. liite B osas kirjeldatud 2. põlvkonna kiibi autentimisprotokolliga ning see vastab standardile ISO/IEC 7816-4.

TCS_100 Käsku on võimalik täita põhifailis, erifailis Tachograph ja erifailis Tachograph_G2, vt ka punkt TCS_34.

TCS_101 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Vaikimisi teada olevad võtmed ja protokoll
P2	1	'00h'	
Lc	1	'NNh'	Lc: järgneva andmevälja pikkus
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	DER-TLV-s kodeeritud lühiajalise avaliku võtme väärtus (vt 11. liide) Sõidukiseade saadab andmeobjekte selles järjekorras.

TCS_102 **Vastusesõnum**

Bait	Pikkus	Väärtus	Kirjeldus
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	DER-TLV-s kodeeritud dünaamilised autentimisandmed: nonss ja autentimistõend (vt 11. liide)
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kaardi vastus '**6A80**' näitab, et andmeväli sisaldab valesid parameetreid.

— Kaart vastab '**6982**', kui käsu EXTERNAL AUTHENTICATE täitmine ebaõnnestus.

Dünaamilise autentimise andmeobjekt '7Ch'

— peab olemas olema juhul, kui toiming õnnestub, st olekubaidid on '**9000**',

— peab puuduma juhul, kui esineb täitmisviga või kontrollimisviga, st olekubaidid on vahemikus '**6400**' – '**6FFF**', ja

— võib puududa hoiatuse korral, st olekubaidid on vahemikus '**6200**' – '**63FF**'.

3.5.11. *MANAGE SECURITY ENVIRONMENT*

Käsuga valitakse autentimiseks avalik võti.

3.5.11.1. Esimese põlvkonna käsu ja vastuse paar

Käsk vastab standardile ISO/IEC 7816-4. Käsu kasutamist on seotud standardiga võrreldes piiratud.

TCS_103 Seda käsku toetab ainult 1. põlvkonna sõidumeerikurakendus.

TCS_104 MSE andmeväljal viidatud võti jääb aktiivseks avalikuks võtmeks kuni antakse järgmine korrektne MSE käsk, valitakse erifail või kaart lähtestatakse.

TCS_105 Kui osutatud võtit ei ole (veel) kaardil, jääb turbekeskkond muutumatuks.

TCS_106 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: kõigi krüptograafiliste toimingute puhul kehtiv võti, millele viidatakse
P2	1	'B6h'	P2 (digiallkirja käsitlevad viidatavad andmed)
Lc	1	'0Ah'	Lc: järgneva andmevälja pikkus
#6	1	'83h'	Avalikule võtmele viitamise silt asümmeetrilistel juhtudel
#7	1	'08h'	Võtmeviite pikkus (võtmeidentifikaator)
#8-#15	8	'XX..XXh'	11. liite määratlusele vastav võtmeidentifikaator

TCS_107 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui viidatud võtit ei ole kaardil, saadakse töötlusvastus '**6A88**'.

— Kui turvalise sõnumivahetuse vormingus puuduvad mõned oodatavad andmeobjektid, saadakse töötlusvastus '**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**'.

3.5.11.2. Teise põlvkonna käsu ja vastuse paarid

Seoses 2. põlvkonna autentimisega toetab sõidumeerikukaart järgmist MSE-d: standardile ISO/IEC 7816-4 vastavad määramiskäsu versioonid. Esimese põlvkonna autentimisel neid käsuversioone ei toetata.

3.5.11.2.1. MSE:SET AT kiibi autentimiseks

Järgmist käsku MSE:SET AT kasutatakse pärast käsu GENERAL AUTHENTICATE andmist toimuva kiibi autentimise parameetrite valimiseks.

TCS_108 Käsku on võimalik täita põhifailis, erifailis Tachograph ja erifailis Tachograph_G2, vt ka punkt TCS_34.

TCS_109 **Käsusõnum MSE:SET AT kiibi autentimiseks**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'22h'	

Bait	Pikkus	Väärtus	Kirjeldus
P1	1	'41h'	Määratakse sisemiseks autentimiseks
P2	1	'A4h'	Autentimine
Lc	1	'NNh'	Lc: järgneva andmevälja pikkus
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	DER-TLV-s kodeeritud krüptograafilise mehhanismi viide: kiibi autentimise objekti identifikaator (ainult väärtus, silti '06h' ei kasutata). Objekti identifikaatorite väärtuste kohta vt 1. liide; kasutatakse baidiesitust. 11. liites on esitatud juhiseid objekti identifikaatori valimiseks.

3.5.11.2.2. MSE:SET AT sõidukiseadme autentimiseks

Järgmist käsku MSE:SET AT kasutatakse sõidukiseadme autentimise parameetrite ja võtmete valimiseks järgneva käsu EXTERNAL AUTHENTICATE jaoks.

TCS_110 Käsku on võimalik täita põhifailis, erifailis Tachograph ja erifailis Tachograph_G2, vt ka punkt TCS_34.

TCS_111 **Käsusõnum MSE:SET AT sõidukiseadme autentimiseks**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Määratakse väliseks autentimiseks
P2	1	'A4h'	Autentimine
Lc	1	'NNh'	Lc: järgneva andmevälja pikkus
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	DER-TLV-s kodeeritud krüptograafilise mehhanismi viide: sõidukiseadme autentimise objekti identifikaator (ainult väärtus, silti '06h' ei kasutata). Objekti identifikaatorite väärtuste kohta vt 1. liide; kasutatakse baidiesitust. 11. liites on esitatud juhiseid objekti identifikaatori valimiseks.
		'83h' + '08h' + 'XX..XXh'	DER-TLV-kodeeritud sõidukiseadme avaliku võtme viide, mis vastab sertifikaadis osutatud sertifikaadi omaniku viitenumbrile
		'91h' + L_{91} + 'XX..XXh'	DER-TLV-s kodeeritud sõidukiseadme lühiajalise avaliku võtme lühivorm, mida kasutatakse kiibi autentimisel (vt 11. liide)

3.5.11.2.3. MSE:SET DST

Järgmist käsku MSE:SET DST kasutatakse avaliku võtme määramiseks ühel järgmistest eesmärkidest:

— järgneva käsuga „PSO: Verify Digital Signature“ esitatud allkirja kontrollimine või

— järgneva käsuga „PSO: Verify Certificate“ esitatud sertifikaadi allkirja kontrollimine.

TCS_112 Käsku on võimalik täita põhifailis, erifailis Tachograph ja erifailis Tachograph_G2, vt ka punkt TCS_33.

TCS_113 **Käsusõnum MSE:SET DST**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Määratud kontrollimiseks
P2	1	‘B6h’	Digitaalallkiri
Lc	1	‘NNh’	Lc: järgneva andmevälja pikkus
#6-#(5+L)	L	‘83h’ + ‘08h’ + ‘XX...XXh’	DER-TLV-s kodeeritud avaliku võtme viitenumber, st avaliku võtme sertifikaadis sisalduv sertifikaadi omaniku viitenumber (vt 11. liide)

Kõigi käsuversioonide puhul kasutatakse allpool esitatud sõnumi struktuuri ja olekubaite.

TCS_114 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart ‘**9000**’. Protokoll on valitud ja käivitatud.

— ‘**6A80**’ näitab, et käsi andmeväli sisaldab valesid parameetreid.

— ‘**6A88**’ näitab, et viiteandmed (nt viidatud võti) ei ole kättesaadavad.

3.5.12. *PSO: HASH*

Käsku kasutatakse mõnede andmete räsiarvutustulemuste edastamiseks kaardile. Käsku kasutatakse digitaalallkirjade kontrollimiseks. Räsiväärtus salvestatakse ajutiselt järgneva käsu „PSO: Verify Digital Signature“ jaoks.

Käsk vastab standardile ISO/IEC 7816-8. Käsu kasutamist on seotud standardiga võrreldes piiratud.

Seda käsku peab toetama ainult kontrollikaart erifailis Tachograph ja erifailis Tachograph_G2.

Muudel sõidumeerikukaartidel ei ole selle käsu rakendamine kohustuslik. Käsu kasutatavus põhifailis ei ole kohustuslik.

Kontrollikaardi 1. põlvkonna rakendus toetab ainult algoritmi SHA-1.

TCS_115 Ajutiselt salvestatud räsiväärtus kustutatakse juhul, kui käsuga „PSO: HASH“ arvutatakse uus räsiväärtus, kui valitakse erifail või kui sõidumeerikukaart lähtestatakse.

TCS_116 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'2Ah'	Turbetoimingu tegemine
P1	1	'90h'	Räsikoodi tagasisaatmine
P2	1	'A0h'	Silt: andmeväli sisaldab räsialgoritmiga töödeldavaid andmeobjekte
Lc	1	'XXh'	Järgneva andmevälja Lc pikkus
#6	1	'90h'	Räsikoodi silt
#7	1	'XXh'	Räsikoodi pikkus L: '14h' 1. põlvkonna rakenduse korral (vt 11. liite A osa) '20h', '30h' või '40h' 2. põlvkonna rakenduse korral (vt 11. liite B osa)
#8-#(7+L)	L	'XX..XXh'	Räsikood

TCS_117 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui mõned oodatavad (eespool määratletud) andmeobjektid puuduvad, saadakse töötlusvastus '**6987**'. See võib juhtuda, kui puudub üks silt '90h'.

— Kui mõned andmeobjektid on valed, saadakse töötlusvastus '**6988**'. See viga tekib siis, kui vajalik silt on olemas, aga algoritmi SHA-1 korral ei ole pikkus '14h', SHA-256 korral '20h', SHA-384 korral '30h' või SHA-512 korral'40h' (2. põlvkonna rakendus).

3.5.13. *PERFORM HASH OF FILE*

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

Seda käsku peavad toetama ainult juhikaart ja töökojakaart erifailis Tachograph ja erifailis Tachograph_G2.

Muudel sõidumeerikukaartidel ei ole selle käsu rakendamine kohustuslik. Kui käsku rakendatakse ettevõtte- või kontrollikaardil, peab käsu rakendamine vastama käesoleva punkti nõuetele.

Käsu kasutatavus põhifailis ei ole kohustuslik. Kui seda kasutatakse, peab käsu rakendamine vastama käesoleva punkti nõuetele, st räsiväärtuse arvutamist ei lubata ja käsk lõpetatakse sobiva veakoodiga.

TCS_118 Käsku PERFORM HASH OF FILE kasutatakse hetkel valitud transparentse elementaarfaili andmeala töötlemiseks räsialgoritmi abil.

TCS_119 Sõidumeerikukaart peab toetama seda käsku ainult seoses 4. peatükis erifailide Tachograph ja Tachograph_G2 all loetletud elementaarfailidega, arvestades allpool nimetatud erandeid. Sõidumeerikukaart ei tohi seda käsku toetada seoses erifaili Tachograph_G2 elementaarfailiga Sensor_Installation_Data.

TCS_120 Räsitoimingu tulemus salvestatakse ajutiselt kaardile. Seda saab siis kasutada faili digitaalallkirja saamiseks, kasutades käsku PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Ajutiselt salvestatud faili räsiväärtus kustutatakse juhul, kui käsuga „PSO: Hash of File“ arvutatakse uus räsiväärtus, kui valitakse erifail või kui sõidumeerikukaart lähtestatakse.

TCS_122 Sõidumeeriku 1. põlvkonna rakendus peab toetama algoritmi SHA-1.

TCS_123 Sõidumeeriku 2. põlvkonna rakendus peab toetama algoritme SHA-1 ja SHA-2 (256, 384 ja 512 bitti).

TCS_124 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	‘80h’	CLA
INS	1	‘2Ah’	Turbetoimingu tegemine
P1	1	‘90h’	Silt: Hash
P2	1	‘XXh’	P2: näitab, millist algoritmi kasutatakse hetkel valitud transparentse faili andmete räsitöötlemiseks: ‘00h’ SHA-1 korral ‘01h’ SHA-256 korral ‘02h’ SHA-384 korral ‘03h’ SHA-512 korral

TCS_125 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart ‘**9000**’.

— Kui see käsk ei ole elementaartööfailis lubatud (erifaili Tachograph_G2 elementaarfaili Sensor_Installation_Data), saadakse töötlusvastus ‘**6985**’.

— Kui valitud elementaarfail loetakse vigaseks (faili atribuutide või salvestatud andmete terviklusviga), on töötlusvastus ‘**6400**’ või ‘**6581**’.

— Kui valitud fail ei ole transparentne fail või kui elementaartööfail puudub, saadakse töötlusvastus ‘**6986**’.

3.5.14. *PSO: COMPUTE DIGITAL SIGNATURE*

Käsku kasutatakse eelnevalt arvutatud räsikoodi digitaalallkirja arvutamiseks (vt PERFORM HASH OF FILE, punkt 3.5.13).

Seda käsku peavad toetama ainult juhikaart ja töökojakaart erifailis Tachograph ja erifailis Tachograph_G2.

Muudel sõidumeerikukaartidel võib seda käsku soovi korral rakendada, aga neil ei tohi olla allkirjavõtit. Seetõttu ei saa need kaardid käsku edukalt täita, vaid lõpetavad selle sobiva veakoodiga.

Käsu kasutatavus põhifailis ei ole kohustuslik. Kui seda kasutatakse, peab käsk lõppema sobiva veakoodiga.

Käsk vastab standardile ISO/IEC 7816-8. Käsu kasutamist on seotud standardiga võrreldes piiratud.

TCS_126 Käsuga ei arvutata eelnevalt käsuga PSO: HASH sisestatud räsikoodiga.

TCS_127 Digitaalallkirja arvutamiseks kasutatakse kaardi privaatvõtit ja kaart teab seda vaikimisi.

TCS_128 1. põlvkonna sõidumeerikurakendus kasutab digitaalallkirja andmiseks PKCS1-le vastavat täidistamismeetodit (üksikasjad 11. liites).

TCS_129 2. põlvkonna sõidumeerikurakendus arvutab elliptilisel kõveral põhineva digitaalallkirja (üksikasjad 11. liites).

TCS_130 **Käsusõnum**

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

TCS_131 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui vaikimisi valitud privaatvõti loetakse rikutuks, saadakse töötlusvastus '**6400**' või '**6581**'.

— Kui eelmise käsuga „Perform Hash of File" leitud räsiväärtus ei ole kasutatav, saadakse töötlusvastus '**6985**'.

3.5.15. *PSO: VERIFY DIGITAL SIGNATURE*

Käsku kasutatakse kaardile teadaoleva räsiväärtusega sisendiks oleva digitaalallkirja kontrollimiseks. Allkirja algoritmi teab kaart vaikimisi.

Käsk vastab standardile ISO/IEC 7816-8. Käsu kasutamist on seotud standardiga võrreldes piiratud.

Seda käsku peab toetama ainult kontrollikaart erifailis Tachograph ja erifailis Tachograph_G2.

Muudel sõidumeerikukaartidel ei ole selle käsu rakendamine kohustuslik. Käsu kasutatavus põhifailis ei ole kohustuslik.

TCS_132 Käsk VERIFY DIGITAL SIGNATURE kasutab alati avalikku võtit, mis on valitud eelneva käsuga „Manage Security Environment MSE: Set DST" ja eelnevalt käsuga PSO: HASH sisestatud räsikoodiga.

TCS_133 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'00h'	CLA
INS	1	'2Ah'	Turbetoimingu tegemine
P1	1	'00h'	
P2	1	'A8h'	Silt: andmeväli sisaldab kontrollimisega seotud andmeobjekte
Lc	1	'83h'	Järgneva andmevälja Lc pikkus
6	1	'9Eh'	Digitaalallkirja silt
#7-#8	2	'81 XXh'	Digitaalallkirja pikkus: 1. põlvkonna sõidumeerikurakenduse korral 11. liite A osa kohaselt kodeeritud 128 baiti 2. põlvkonna sõidumeerikurakenduse korral sõltub valitud kõverast (vt 11. liite B osa)
#9-#(8+L)	L	'XX..XXh'	Digitaalallkirja sisu

TCS_134 **Vastusesõnum**

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

— Kui käsk on edukas, vastab kaart '**9000**'.

— Kui allkirja kontrollimine ebaõnnestub, saadakse töötlusvastus '**6688**'. Kontrollimise protsessi on kirjeldatud 11. liites.

— Kui avalikku võtit ei ole valitud, saadakse töötlusvastus '**6A88**'.

— Kui mõned oodatavad (eespool määratletud) andmeobjektid puuduvad, saadakse töötlusvastus '**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, mõne kohustusliku andmeobjekti pikkus on vale.

— Kui valitud avalik võti loetakse rikutuks, saadakse töötlusvastus '**6400**' või '**6581**'.

3.5.16. *PROCESS DSRC MESSAGE*

Käsku kasutatakse DSRC-sõnumi tervikluse ja autentsuse kontrollimiseks ning sõidukiseadmest DSCR-lingi kaudu kontrolliasutusele või töökojale edastatud andmete dešifreerimiseks. Kaart tuletab DSRC-sõnumi turvamiseks kasutatava krüpteerimisvõtme ja MACi võtme vastavalt 11. liite B osa 13. peatükis esitatud kirjeldusele.

Seda käsku peavad toetama ainult kontrollikaart ja töökojakaart erifailis Tachograph_G2.

Muudel sõidumeerikukaartidel võib seda käsku soovi korral rakendada, aga neil ei tohi olla DSRC peavõtit. Seetõttu ei saa need kaardid käsku edukalt täita, vaid lõpetavad selle sobiva veakoodiga.

Käsu kasutatavus põhifailis ja/või erifailis Tachograph ei ole kohustuslik. Kui seda kasutatakse, peab käsk lõppema sobiva veakoodiga.

TCS_135 DSRC peavõti on kasutatav ainult erifailis Tachograph_G2, st kontrolli- ja töökojakaart peavad toetama käsu täitmist ainult erifailis Tachograph_G2.

TCS_136 Käsk peab piirduma DSRC andmete dekrüpteerimise ja krüptograafilise kontrollsumma kontrollimisega, aga ei tohi sisendandmeid tõlgendada.

TCS_137 Käsu andmevälja andmeobjektide järjekord on käesoleva spetsifikaadiga fikseeritud.

TCS_138 **Käsusõnum**

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	'80h'	Valmistajaspetsiifiline CLA
INS	1	'2Ah'	Turbetoimingu tegemine
P1	1	'80h'	Vastuse andmed: lihtväärtus
P2	1	'B0h'	Käsu andmed: BER-TLV-s kodeeritud lihtväärtus, mis sisaldab turvalise sõnumivahetuse andmeobjekte
Lc	1	'NNh'	Järgneva andmevälja Lc pikkus
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	DER-TLV-s kodeeritud täidise sisu indikaatorbait, millele järgneb krüpteeritud sõidumeerikuandmete sisu. Täidise sisu indikaatorbaidi jaoks kasutatakse väärtust '00h' (standardi ISO/IEC 7816-4:2013 tabeli 52 kohaselt „täiendav näit puudub"). Krüpteerimismehhanismi kohta vt 11. liite B osa 13. peatükk. Pikkuse L_{87} lubatud väärtused on AESi kohase ploki pikkuse täiskordsed arvud, millele liidetakse täidise sisu indikaatorbaidi jaoks 1, st vahemik on 17–193 baiti. *Märkus:* turvalise sõnumivahetuse andmeobjekti sildi '87h' kohta vt standardi ISO/IEC 7816-4:2013 tabel 49.
		'81h' + '10h'	DER-TLV-s kodeeritud kontrolliviite mall järgmiste andmeelementide konkatenatsiooni konfidentsiaalsusega seotud pesastamise jaoks (vt 1. liide „DSRCSecurityData" ja 11. liite B osa 13. peatükk): — 4-baidine ajatempel — 3-baidine loendur — 8-baidine sõidukiseadme seerianumber — 1-baidine DSRC peavõtme versioon *Märkus:* turvalise sõnumivahetuse andmeobjekti sildi '81h' kohta vt standardi ISO/IEC 7816-4:2013 tabel 49.
		'8Eh' + L_{8E} + 'XX..XXh'	DER-TLV-s kodeeritud DSRC-sõnumiga saadetav MAC. MACi algoritmi ja arvutamise kohta vt 11. liite B osa 13. peatükk. *Märkus:* turvalise sõnumivahetuse andmeobjekti sildi '8Eh' kohta vt standardi ISO/IEC 7816-4:2013 tabel 49.

TCS_139 **Vastusesõnum**

Bait	Pikkus	Väärtus	Kirjeldus
#1-#L	L	'XX..XXh'	Puuduvad (vea korral) või dešifreeritud andmed (täidis eemaldatud)
SW	2	'XXXXh'	Olekubaidid (SW1, SW2)

— Kui käsk on edukas, vastab kaart '**9000**'.

— '**6A80**' näitab, et käsu andmeväljal on ebaõigeid parameetreid (sama vastust kasutatakse ka juhul, kui andmeobjekte ei saadeta nõutud järjekorras).

— '**6A88**' näitab, et viiteandmed ei ole kättesaadavad, st viidatud DSRC peavõti ei ole kasutatav.

— '**6900**' näitab, et krüptograafilise kontrollsumma kontrollimine või andmete dekrüpteerimine ebaõnnestus.

4. SÕIDUMEERIKUKAARTIDE STRUKTUUR

Käesolevas peatükis määratletakse juurdepääsetavate andmete salvestamiseks kasutatavad sõidumeerikukaartide failistruktuurid.

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

TCS_140 2. põlvkonna sõidumeerikukaart peab sisaldama põhifaili (MF) ning sama tüüpi 1. ja 2. põlvkonna sõidumeerikurakendust (st juhikaardi rakendusi).

TCS_141 Sõidumeerikukaart peab toetama vähemalt vastavate rakenduste jaoks ette nähtud minimaalset kirjete arvu ning ei tohi toetada rohkem kirjeid, kui on vastavate rakenduste jaoks ette nähtud maksimaalne kirjete arv.

Erinevate rakenduste maksimaalne ja minimaalne kirjete arv on esitatud käesolevas peatükis.

Käesolevas peatükis käsitletud juurdepääsueeskirjade turbetingimuste kohta leiate teavet punktis 3.3. Üldjuhul tähistab lugemise juurdepääsurežiim („read") käsku READ BINARY paaris INS-baidiga ja, kui see on toetatud, paaritu INS-baidiga, välja arvatud töökojakaardil oleva elementaarfaili Sensor_Installation_Data puhul, vt punktid TCS_156 ja TCS_160. Ajakohastamise juurdepääsurežiim („update") tähistab käsku UPDATE BINARY paaris INS-baidiga ja, kui see on toetatud, paaritu INS-baidiga ning valimise juurdepääsurežiim („select") tähistab käsku SELECT.

4.1. **Põhifail (MF)**

TCS_142 Pärast isikustamist on põhifailil järgmine püsiv failistruktuur ja järgmised püsivad failile juurdepääsu eeskirjad.

Märkus: elementaarfaili lühike identifikaator SFID on esitatud kümnendarvuna, st arvule 30 vastab kahendsüsteemis arv 11110.

			Juurdepääsueeskirjad	
Fail	**Faili ID**	**SFID**	**Lugemine / valimine**	**Ajakohastamine**
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (conditional)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (conditional)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

Tabelis kasutatakse turbetingimuse kohta järgmist lühendit:

SC1 ALW OR SM-MAC-G2

TCS_143 Kõik elementaarfaili struktuurid on transparentsed.

TCS_144 Põhifailil on järgmine andmestruktuur:

Fail / andmeelement	Kirjete arv	Maht (baiti) Min	Maks	Standard-väärtused
MF		*63*	*184*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
EF DIR		*20*	*20*	
See TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
See TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
See TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Elementaarfail DIR sisaldab järgmisi rakendusega seotud andmeobjekte:61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'

TCS_146 Elementaarfail ATR/INFO peab olemas olema juhul, kui sõidumeerikukaardi lähtestuse vastuses (ATR) on märgitud, et kaart toetab laiendatud väljasid. Sellisel juhul peab EF ATR/INFO sisaldama laiendatud andmeobjekti (DO'7F66') vastavalt standardi ISO/IEC 7816-4:2013 punktile 12.7.1.

TCS_147 Elementaarfail Extended_Length peab olemas olema juhul, kui sõidumeerikukaardi lähtestuse vastuses (ATR) on märgitud, et kaart toetab laiendatud väljasid. Sellisel juhul peab elementaarfail sisaldama järgmist andmeobjekti:'02 01 xx', kus väärtus 'xx' näitab, kas laiendatud väljad on toetatud protokolliga T = 1 ja/või protokolliga T = 0.

Väärtus '01' näitab, et laiendatud väljad on toetatud protokolliga T = 1.

Väärtus '10' näitab, et laiendatud väljad on toetatud protokolliga T = 0.

Väärtus '11' näitab, et laiendatud väljad on toetatud protokolliga T = 1 ja T = 0.

4.2. Juhikaardi rakendused

4.2.1. *Juhikaardi 1. põlvkonna rakendus*

TCS_148 Pärast isikustamist on 1. põlvkonna juhikaardirakendusel järgmine püsiv failistruktuur ja järgmised faili juurdepääsueeskirjad:

Fail	Faili ID	Juurdepääsueeskirjad		
		Lugemine	Valimine	Ajakohastamine
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'050Eh'	SC2	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

Tabelis kasutatakse turbetingimuse kohta järgmisi lühendeid:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

TCS_149 Kõik elementaarfaili struktuurid on transparentsed.

TCS_150 Juhikaardi 1. põlvkonna rakendusel on järgmine andmestruktuur:

Fail / andmeelement	Kirjete arv	Maht (baiti) Min	Maht (baiti) Maks	Standard-väärtused
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
└CardVehiclesUsed		*2606*	*6202*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*2604*	*6200*	
└─CardVehicleRecord	n_3	*31*	*31*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
└CardPlaceDailyWorkPeriod		*841*	*1121*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*840*	*1120*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
└SpecificConditionRecord	56	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_151 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruste esitamiseks, on kirjete arvu minimaal- ja maksimaalväärtused, mida juhikaardi 1. põlvkonna rakenduse 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)

4.2.2. *Juhikaardi 2. põlvkonna rakendus*

TCS_152 Pärast isikustamist on 2. põlvkonna juhikaardirakendusel järgmine püsiv failistruktuur ja järgmised faili juurdepääsueeskirjad:

Märkus: elementaarfaili lühike identifikaator SFID on esitatud kümnendarvuna, st arvule 30 vastab kahendsüsteemis arv 11110.

			Juurdepääsueeskirjad	
Fail	**Faili ID**	**SFID**	**Lugemine / valimine**	**Ajakohastamine**
└─ DF Tachograph_G2			SC1	
├─ EF Application_Identification	‘0501h’	1	SC1	NEV
├─ EF CardMA_Certificate	‘C100h’	2	SC1	NEV
├─ EF CardSignCertificate	‘C101h’	3	SC1	NEV
├─ EF CA_Certificate	‘C108h’	4	SC1	NEV
├─ EF Link_Certificate	‘C109h’	5	SC1	NEV
├─ EF Identification	‘0520h’	6	SC1	NEV
├─ EF Card_Download	‘050Eh’	7	SC1	SC1
├─ EF Driving_Licence_Info	‘0521h’	10	SC1	NEV
├─ EF Events_Data	‘0502h’	12	SC1	SM-MAC-G2
├─ EF Faults_Data	‘0503h’	13	SC1	SM-MAC-G2
├─ EF Driver_Activity_Data	‘0504h’	14	SC1	SM-MAC-G2
├─ EF Vehicles_Used	‘0505h’	15	SC1	SM-MAC-G2
├─ EF Places	‘0506h’	16	SC1	SM-MAC-G2
├─ EF Current_Usage	‘0507h’	17	SC1	SM-MAC-G2
├─ EF Control_Activity_Data	‘0508h’	18	SC1	SM-MAC-G2
├─ EF Specific_Conditions	‘0522h’	19	SC1	SM-MAC-G2
├─ EF VehicleUnits_Used	‘0523h’	20	SC1	SM-MAC-G2
└─ EF GNSS_Places	‘0524h’	21	SC1	SM-MAC-G2

Tabelis kasutatakse turbetingimuse kohta järgmist lühendit:

SC1 ALW OR SM-MAC-G2

TCS_153 Kõik elementaarfaili struktuurid on transparentsed.

TCS_154 Juhikaardi 2. põlvkonna rakendusel on järgmine andmestruktuur:

Fail / andmeelement	Kirjete arv	Maht (baiti) Min	Maks	Standard-väärtused
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
CardVehiclesUsed		*4034*	*9602*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*4032*	*9600*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
CardPlaceDailyWorkPeriod		*1766*	*2354*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		*1764*	*2352*	
PlaceRecord	n_4	*21*	*21*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruste esitamiseks, on kirjete arvu minimaal- ja maksimaalväärtused, mida juhikaardi 2. põlvkonna rakenduse 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)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. Töökojakaardi rakendused

4.3.1. *Töökojakaardi 1. põlvkonna rakendus*

TCS_156 Pärast isikustamist on 1. põlvkonna töökojakaardirakendusel järgmine püsiv failistruktuur ja järgmised faili juurdepääsueeskirjad:

		Juurdepääsueeskirjad		
Fail	**Faili ID**	**Lugemine**	**Valimine**	**Ajakohastamine**
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'0509h'	SC2	SC1	**SC1**
├─EF Calibration	'050Ah'	SC2	SC1	SC3
├─EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

Tabelis kasutatakse turbetingimuste kohta järgmisi lühendeid:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC4 Paaris INS-baidiga käsu READ BINARY korral:

(PLAIN-C AND SM-R-ENC-G1) OR (SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR

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

Paaritu INS-baidiga käsu READ BINARY korral (kui seda toetatakse): NEV

TCS_157 Kõik elementaarfaili struktuurid on transparentsed.

TCS_158 Töökojakaardi 1. põlvkonna rakendusel on järgmine andmestruktuur:

Fail / andmeelement	Kirjete arv	Maht (baiti) Min	Maks	Standard-väärtused
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

EF Sensor_Installation_Data		*16*	*16*	
└SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
└CardEventData		*432*	*432*	
└cardEventRecords	6	*72*	*72*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└CardFaultData		*288*	*288*	
└cardFaultRecords	2	*144*	*144*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└CardDriverActivity		*202*	*496*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
└CardVehiclesUsed		*126*	*250*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*124*	*248*	
└CardVehicleRecord	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
└vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
└CardPlaceDailyWorkPeriod		*61*	*81*	
├placePointerNewestRecord		1	1	{00}
└placeRecords		*60*	*80*	
└PlaceRecord	n_4	*10*	*10*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
└vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	*2*	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruste esitamiseks, on kirjete arvu minimaal- ja maksimaalväärtused, mida töökojakaardi 1. põlvkonna rakenduse 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_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 day * 93 activity changes)	492 bytes (1 day * 240 activity changes)

4.3.2. *Töökojakaardi 2. põlvkonna rakendus*

TCS_160 Pärast isikustamist on 2. põlvkonna töökojakaardirakendusel järgmine püsiv failistruktuur ja järgmised faili juurdepääsueeskirjad:

Märkus: elementaarfaili lühike identifikaator SFID on esitatud kümnendarvuna, st arvule 30 vastab kahendsüsteemis arv 11110.

			Juurdepääsueeskirjad		
Fail	**Faili ID**	**SFID**	**Lugemine**	**Valimine**	**Ajakohastamine**
└DF Tachograph_G2			SC1	SC1	
├EF Application_Identification	'0501h'	1	SC1	SC1	NEV
├EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
├EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
├EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
├EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
├EF Identification	'0520h'	6	SC1	SC1	NEV
├EF Card_Download	'0509h'	7	SC1	SC1	SC1
├EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
├EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-	NEV
├EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
├EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
├EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
├EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
├EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
├EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
├EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
├EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
├EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
└EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

Tabelis kasutatakse turbetingimuste kohta järgmisi lühendeid:

SC1 ALW OR SM-MAC-G2

SC5 Paaris INS-baidiga käsu READ BINARY korral: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

Paaritu INS-baidiga käsu READ BINARY korral (kui seda toetatakse): NEV

TCS_161 Kõik elementaarfaili struktuurid on transparentsed.

TCS_162 Töökojakaardi 2. põlvkonna rakendusel on järgmine andmestruktuur:

Fail / andmeelement	Kirjete arv	Maht (baiti) Min	Maks	Standard-väärtused
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		46	46	
noOfSealRecords		1	1	{00}
SealRecords		45	45	
SealRecord	5	9	9	
equipmentType		1	1	{00}
extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
CardEventData		*792*	*792*	
cardEventRecords	11	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
CardVehiclesUsed		*194*	*386*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*192*	*384*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

TCS_163 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruste esitamiseks, on kirjete arvu minimaal- ja maksimaalväärtused, mida töökojakaardi 2. põlvkonna rakenduse 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_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 baiti (1 päev * 93 tegevusmuutust)	492 baiti (1 päev * 240 tegevusmuutust)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Kontrollikaardi rakendused

4.4.1. *Kontrollikaardi 1. põlvkonna rakendus*

TCS_164 Pärast isikustamist on 1. põlvkonna kontrollikaardirakendusel järgmine püsiv failistruktuur ja järgmised faili juurdepääsueeskirjad:

		Juurdepääsueeskirjad		
Fail	**Faili ID**	**Lugemine**	**Valimine**	**Ajakohastamine**
└─DF Tachograph	'0500h'			
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

Tabelis kasutatakse turbetingimuste kohta järgmisi lühendeid:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_165 Kõik elementaarfaili struktuurid on transparentsed.

TCS_166 Kontrollikaardi 1. põlvkonna rakendusel on järgmine andmestruktuur:

Fail / andmeelement	Kirjete arv	Maht (baiti) Min	Maks	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruste esitamiseks, on kirjete arvu minimaal- ja maksimaalväärtused, mida kontrollikaardi 1. põlvkonna rakenduse andmestruktuur peab kasutama:

		Min	Maks
n_7	NoOfControlActivityRecords	230	520

4.4.2. *Kontrollikaardi 2. põlvkonna rakendus*

TCS_168 Pärast isikustamist on 2. põlvkonna kontrollikaardirakendusel järgmine püsiv failistruktuur ja järgmised faili juurdepääsueeskirjad.

Märkus: elementaarfaili lühike identifikaator SFID on esitatud kümnendarvuna, st arvule 30 vastab kahendsüsteemis arv 11110.

			Juurdepääsueeskirjad	
Fail	**Faili ID**	**SFID**	**Lugemine / valimine**	**Ajakohastamine**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

Tabelis kasutatakse turbetingimuse kohta järgmist lühendit:

SC1 ALW OR SM-MAC-G2

TCS_169 Kõik elementaarfaili struktuurid on transparentsed.

TCS_170 Kontrollikaardi 2. põlvkonna rakendusel on järgmine andmestruktuur:

Fail / andmeelement	Kirjete arv	Maht (baiti) Min	Maks	
DF Tachograph_G2		*11410*	*25161*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruste esitamiseks, on kirjete arvu minimaal- ja maksimaalväärtused, mida kontrollikaardi 2. põlvkonna rakenduse andmestruktuur peab kasutama:

		Min	Maks
n_7	NoOfControlActivityRecords	230	520

4.5. Ettevõttekaardi rakendused

4.5.1. *Ettevõttekaardi 1. põlvkonna rakendus*

TCS_172 Pärast isikustamist on 1. põlvkonna ettevõttekaardirakendusel järgmine püsiv failistruktuur ja järgmised faili juurdepääsueeskirjad.

		Juurdepääsueeskirjad		
Fail	**Faili ID**	**Lugemine**	**Valimine**	**Ajakohastamine**
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

Tabelis kasutatakse turbetingimuste kohta järgmisi lühendeid:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_173 Kõik elementaarfaili struktuurid on transparentsed.

TCS_174 Ettevõttekaardi 1. põlvkonna rakendusel on järgmine andmestruktuur:

Fail / andmeelement	**Kirjete arv**	**Maht (baiti) Min**	**Maks**	**Standard-väärtused**
└DF Tachograph		*11114*	*24454*	
├EF Application_Identification		*5*	*5*	
└CompanyCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfCompanyActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
└MemberStateCertificate		194	194	{00..00}
├EF Identification		*139*	*139*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└CompanyCardHolderIdentification		*74*	*74*	
├companyName		36	36	{00, 20..20}
├companyAddress		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}
├EF Company_Activity_Data		*10582*	*23922*	
└CompanyActivityData		*10582*	*23922*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*23920*	
└companyActivityRecord	n_8	*46*	*46*	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├downloadPeriodBegin		4	4	{00..00}
└downloadPeriodEnd		4	4	{00..00}

TCS_175 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruste esitamiseks, on kirjete arvu minimaal- ja maksimaalväärtused, mida ettevõttekaardi 1. põlvkonna rakenduse andmestruktuur peab kasutama:

		Min	Maks
n_8	NoOfCompanyActivityRecords	230	520

4.5.2. *Ettevõttekaardi 2. põlvkonna rakendus*

TCS_176 Pärast isikustamist on 2. põlvkonna ettevõttekaardirakendusel järgmine püsiv failistruktuur ja järgmised faili juurdepääsueeskirjad.

Märkus: elementaarfaili lühike identifikaator SFID on esitatud kümnendarvuna, st arvule 30 vastab kahendsüsteemis arv 11110.

			Juurdepääsueeskirjad	
Fail	**Faili ID**	**SFID**	**Lugemine / valimine**	**Ajakohastamine**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

Tabelis kasutatakse turbetingimuse kohta järgmist lühendit:

SC1 ALW OR SM-MAC-G2

TCS_177 Kõik elementaarfaili struktuurid on transparentsed.

TCS_178 Ettevõttekaardi 2. põlvkonna rakendusel on järgmine andmestruktuur:

Fail / andmeelement	Kirjete arv	Maht (baiti) Min	Maks	Standard-väärtused
DF Tachograph_G2		*11338*	*25089*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_179 Järgmised väärtused, mida kasutati eespool olevas tabelis suuruste esitamiseks, on kirjete arvu minimaal- ja maksimaalväärtused, mida ettevõttekaardi 2. põlvkonna rakenduse andmestruktuur peab kasutama:

		Min	Maks
n_8	NoOfCompanyActivityRecords	230	520

3. liide

PIKTOGRAMMID

PIC_001 Sõidumeerikus võib vabal valikul kasutada järgmisi piktogramme ja nende kombinatsioone (või nendega üheselt samastamiseks piisavalt sarnaseid piktogramme ja kombinatsioone).

1. PEAMISED PIKTOGRAMMID

	Inimesed	**Toimingud**	**Kasutusrežiimid**
	Ettevõte		Ettevõtterežiim
	Kontrollija	Kontrollimine	Kontrollirežiim
	Sõidukijuht	Juhtimine	Töörežiim
	Töökoda/katsetamiskoht	Ülevaatus/kalibreerimine	Kalibreerimisrežiim
	Tootja		
	Tegevused	**Kestus**	
	Valmisolek	Jooksev valmisolekuaeg	
	Juhtimine	Katkematu juhtimisaeg	
	Puhkus	Jooksev puhkeaeg	
	Muu töö	Jooksev tööaeg	
	Puhkepaus	Kumulatiivne puhkepauside aeg	
	Teadmata		
	Seadmed	**Funktsioonid**	
	Juhikaardi pesa		
	Kaasjuhikaardi pesa		
	Kaart		
	Kell		
	Ekraan	Kuvamine	
	Väline salvestusseade	Allalaadimine	
	Toide		
	Printer/väljatrükk	Trükkimine	
	Andur		
	Rehvimõõt		
	Sõiduk/sõidukiseade		
	GNSSi seade		
	Kaugsidega avastamisseade		
	Liides intelligentsete transpordisüsteemide jaoks		
	Eritingimused		
	Sõidumeerik mittevajalik		
	Parvlaeva-/rongisõit		

Muu

!	Sündmused	⤫	Rikked
⏵	Tööpäeva algus	⏯	Tööpäeva lõpp
●	Asukoht		
M	Juhi toimingute käsitsi sissekandmine		
🔒	Turvalisus		
›	Kiirus		
🕒	Aeg		
Σ	Kokku/kokkuvõte		

Täpsustid

24h	Päeva kohta
|	Nädala kohta
||	Kahe nädala kohta
+	Alates või kuni

2. PIKTOGRAMMIDE KOMBINATSIOONID

Muu

🏛●	Kontrolli koht		
●⏵	Tööpäeva alguskoht	⏯●	Tööpäeva lõppkoht
🕒+	Alates	+🕒	Kuni
🚙+	Sõidukist		
OUT+	Sõidumeerik mittevajalik – algus	+OUT	Sõidumeerik mittevajalik – lõpp

Kaardid

👤💳	Juhikaart
🏢💳	Ettevõttekaart
🏛💳	Kontrollikaart
T💳	Töökojakaart
💳– – –	Kaart puudub

Juhtimine

👤👤	Juhib meeskond
👤 |	Juhtimisaeg nädalas
👤 ||	Juhtimisaeg kahe nädala kohta

Väljatrükid

24h 💳T	Juhi ühe päeva tegevuse väljatrükk kaardilt
24h 🚙T	Juhi ühe päeva tegevuse väljatrükk sõidukiseadmest
! ⤫ 💳T	Sündmuste ja rikete väljatrükk kaardilt
! ⤫ 🚙T	Sündmuste ja rikete väljatrükk sõidukiseadmest
T 🕒 T	Tehniliste andmete väljatrükk
›› T	Kiiruse ületamise väljatrükk

Sündmused

	Kehtetu kaardi sisestamine
	Kaardikonflikt
	Ajaline kattumine
	Vajaliku kaardita juhtimine
	Kaardi sisestamine juhtimise ajal
	Viimane kaardiseanss nõuetekohaselt lõpetamata
	Kiiruse ületamine
	Voolukatkestus
	Viga liikumisandmetes
	Vastuolu sõiduki liikumisandmetes
	Turvalisuse rikkumine
	Aja korrigeerimine (töökojas)
	Kiiruse ületamise kontroll

Rikked

	Kaardirike (juhikaardi pesa)
	Kaardirike (kaasjuhikaardi pesa)
	Ekraanirike
	Allalaadimisrike
	Printeririke
	Anduririke
	Sõidukiseadme siserike
	GNSSi rike
	Kaugsidega avastamisseadme rike

Käsitsi tehtavad sissekanded

	Veel sama tööpäev?
	Eelmise tööpäeva lõpp?
	Kinnita või sisesta tööpäeva lõppkoht
	Sisesta algusaeg
	Sisesta tööpäeva alguskoht

Märkus: väljatrükiploki või kirjeidentifikaatori moodustamiseks kasutatavad piktogrammide lisakombinatsioonid on määratletud 4. liites.

4. liide

VÄLJATRÜKID

SISUKORD

1. ÜLDOSA

Väljatrüki moodustamiseks luuakse ahel eri andmeplokkidest, mis võimaluse korral tähistatakse plokiidentifikaatoriga.

Andmeplokk koosneb ühest või mitmest kirjest, mis võimaluse korral tähistatakse kirjeidentifikaatoriga.

PRT_001 Kui plokiidentifikaator eelneb vahetult kirjeidentifikaatorile, siis kirjeidentifikaatorit ei trükita.

PRT_002 Juhul kui andmeühik on tundmatu või kui seda ei tohi juurdepääsuõigustest tulenevalt trükkida, trükitakse selle asemel tühikud.

PRT_003 Kui terve rea sisu on tundmatu või kui seda ei pea trükkima, jäetakse terve rida välja.

PRT_004 Numbrilised andmeväljad trükitakse paremjoondatult, tuhanded ja miljonid eraldatakse tühikuga ning nulle ette ei lisata.

PRT_005 Stringiandmeväljad trükitakse vasakjoondatult ning täidetakse andmeühiku pikkuses nullidega või kärbitakse vajaduse korral andmeühiku pikkuseni (nimed ja aadressid).

PRT_006 Kui pika teksti tõttu tekib reavahetus, tuleks uue rea esimese märgina trükkida erimärk (rea vertikaaltelje keskel asuv punkt „•“).

2. ANDMEPLOKKIDE SPETSIFIKATSIOON

Käesolevas peatükis on kasutatud järgmisi vormingu märkimistavasid:

— **poolpaksu kirjaga** tähistatakse trükitavat lihtteksti (trükkimisel kasutatakse tavalist kirja),

— tavalise kirjaga tähistatakse muutujaid (piktogrammid või andmed), mis trükkimisel asendatakse nende väärtusega,

— muutujate nimetused külgnevad alakriipsudega, et näidata muutuja jaoks kasutada olevat andmeühiku pikkust,

— kuupäevad on esitatud vormingus „pp/kk/aaaa“ (päev, kuu, aasta); võib kasutada ka vormingut „pp.kk.aaaa“,

— mõiste „kaardi identimisandmed“ hõlmab järgmisi elemente: kaardi tüüp kaardipiktogrammide kombinatsiooni näol, kaardi välja andnud liikmesriigi kood, kaldkriips ja kaardi number koos asendusindeksi ja pikendusindeksiga, mis on eraldatud tühikuga:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kaardipiktogrammide kombinatsioon		Väljaandnud liikmesriigi kood				Kaardi numbri esimesed 14 märki (võib sisaldada järjekorraindeksit)														Asendusindeks		Pikendusindeks

PRT_007 Väljatrükkidel kasutatakse järgmisi andmeplokke ja/või andmekirjeid vastavalt järgmistele tähendustele ja vormingutele.

Ploki või kirje number Tähendus	Andmete vorming

1 ***Dokumendi trükkimise kuupäev ja kellaaeg.***

```
▼ pp/kk/aaaa tt:mm (UTC)
```

2 ***Väljatrüki tüüp.***

Plokiidentifikaator

Väljatrüki piktogrammikombinatsioon (vt 3. liide), kiiruspiiriku seadistus (ainult kiiruse ületamiste väljatrükk)

```
----------▼----------
Pikto xxx km/h
```

3 ***Kaardi omaniku identimisandmed.***

Plokiidentifikaator (P = inimeste piktogramm)

Kaardi omaniku perekonnanimi

Kaardi omaniku eesnimi (eesnimed) (kui on olemas)

Kaardi identimisandmed

Kaardi aegumiskuupäev (kui on) ja kaardi põlvkonna number (GEN 1 või GEN 2) (*)

```
----------P----------
P Perekonnanimi_________
  Eesnimi_______________
Kaardi_identimisandmed__

  pp/kk/aaaa - GEN 2
```

Kui kaart ei ole isiklik ja sellel ei ole kaardi omaniku perekonnanime, tuleb selle asemel trükkida ettevõtte, töökoja või kontrolliasutuse nimi.

(*) Kaardi põlvkonna numbri saab trükkida ainult aruka sõidumeerikuga.

4 ***Sõiduki identimisandmed.***

Plokiidentifikaator

VIN

Registreerinud liikmesriik ja VRN

```
----------🚘----------
🚘 VIN_______________
  Riik/VRN_________
```

5 ***Sõidukiseadme (VU) identimisandmed.***

Plokiidentifikaator

VU tootja nimi

VU osa number

VU põlvkonna number (*)

```
----------⊟----------
⊟ VU_tootja_______
VU_osa_number_____
GEN 2
```

(*) VU põlvkonna numbri saab trükkida ainult aruka sõidumeerikuga.

6 ***Sõidumeeriku viimane kalibreerimine***

Plokiidentifikaator

Töökoja nimi

Töökojakaardi identimisandmed

Kalibreerimise kuupäev

```
----------▼----------
▼ Nimi_________________
Kaardi_identimisandmed__
▼ pp/kk/aaaa
```

7 ***Viimane kontrollimine (kontrolliametniku poolt)***

Plokiidentifikaator
Kontrollikaardi identimisandmed
Kontrolli kuupäev, aeg ja tüüp

```
----------▯----------
Kaardi_identimisandmed__
▯ pp/kk/aaaa tt:mm ppppp
```

Kontrolli tüüp: kuni viis piktogrammi. Kontrolli tüüp võib olla järgmine (või kombinatsioon neist):

▮: kaardilt alla laadimine, ↧: sõidukiseadmest alla laadimine, ▼: trükkimine, ▯: kuvamine, ⊤: teeäärne kalibreerimiskontroll.

8 ***Toimumise järjestuses kaardile salvestatud juhi tegevused***

Plokiidentifikaator
Päringu kuupäev (väljatrüki tegemise kalendripäev) + kaardi igapäevase olemasolu loendur

```
----------⊙----------
    pp/kk/aaaa  xxx
```

8a *Tingimus „Sõidumeerik mittevajalik" päeva alguses* (kui asjaomane tingimus ei ole avatud, jätta tühjaks)

```
----------OUT----------
```

8.1 *Aeg, mille jooksul kaart ei olnud sisestatud*

8.1a Kirjeidentifikaator (algusaeg)
8.1b *Teadmata periood*. Algusaeg, kestus
8.1c *Tegevus käsitsi sisestatud*.
Tegevuse piktogramm, algusaeg, kestus

```
  --------------------
?       tt:mm tttmm
A       tt:mm tttmm
```

8.2 *Kaardi sisestamine pesasse S*

Kirje identifikaator; S = pesa piktogramm
Registreerinud liikmesriik ja VRN
Sõiduki läbisõidumõõdiku näit kaardi sisestamisel

```
  ---------S---------
🚙 Riik/VRN__________
  x xxx xxx km
```

8.3 *Tegevus (kui kaart oli sisestatud)*

Tegevuse piktogramm, algusaeg, kestus, meeskonna staatus (meeskonna piktogramm, kui MEESKOND, tühikud, kui ÜKSI)

```
A       tt:mm tttmm ⊙⊙
```

8.3a *Eritingimus*. Sisestusaeg, eritingimuse piktogramm (või piktogrammikombinatsioon)

```
        tt:mm ---pppp---
```

8.4 *Kaardi väljavõtmine*

Sõiduki läbisõidumõõdiku näit ja läbitud vahemaa pärast viimast sisestamist, mille kohta on läbisõidumõõdiku näit teada

```
  x xxx xxx km; x xxx km
```

9 ***Sõidukiseadmes kaardipesa kohta salvestatud juhi tegevused toimumise järjestuses***

Plokiidentifikaator
Päringu kuupäev (kalendripäev väljatrüki alusel)
Sõiduki läbisõidumõõdiku näit kell 00:00 ja 24:00

```
----------⊙----------
       pp/kk/aaaa
x xxx xxx - x xxx xxx km
```

10 ***Tegevused kaardipesas S***

Plokiidentifikaator

```
----------S----------
```

10a *Tingimus „Sõidumeerik mittevajalik" päeva alguses* (kui asjaomane tingimus ei ole avatud, jätta tühjaks)

```
----------OUT----------
```

10.1 *Periood, mil kaardipesasse S ei olnud ühtki kaarti sisestatud*

Kirjeidentifikaator
Ühtki kaarti pole sisestatud
Sõiduki läbisõidumõõdiku näit aja alguses

```
  --------------------
⊙▮---
  x xxx xxx km
```

10.2 *Kaardi sisestamine*

Kaardi sisestamiskirje identifikaator
Juhi perekonnanimi

```
  --------------------
⊙ Perekonnanimi_______
```

	Juhi eesnimi	Eesnimi_____
	Juhikaardi identimisandmed	Kaardi_identimisandmed__
	Kaardi aegumiskuupäev (kui on) ja kaardi põlvkonna number (GEN 1 või GEN 2) (*)	pp/kk/aaaa - GEN 2
	Eelmise kasutatud sõiduki registreerinud liikmesriik ja VRN	+Riik/VRN_____
	Eelmisest sõidukist kaardi väljavõtmise kuupäev ja kellaaeg	pp/kk/aaaa tt:mm
	Tühi rida	
	Sõiduki läbisõidumõõdiku näit kaardi sisestamisel, tunnus juhi tegevuste käsitsi sisestamise kohta (M – jah, tühi – ei)	x xxx xxx **km** M
	Kui päeval, mille kohta väljatrükk koostatakse, juhikaarti ei sisestatud, kasutatakse plokis 10.2 läbisõidumõõdiku näitu viimasest kaardi sisestamise ajast enne seda päeva	
10.3	*Tegevus*	
	Tegevuse piktogramm, algusaeg, kestus, meeskonna staatus (meeskonna piktogramm, kui MEESKOND, tühikud, kui ÜKSI)	A tt:mm tttmm
10.3a	*Eritingimus*. Sisestusaeg, eritingimuse piktogramm (või piktogrammikombinatsioon)	tt:mm ---pppp---
10.4	*Kaardi väljavõtmine või aja „Kaart puudub" lõpp*	
	Sõiduki läbisõidumõõdiku näit kaardi väljavõtmisel või aja „Kaart puudub" lõpus ja sisestamisest alates või aja „Kaart puudub" algusest läbitud vahemaa	x xxx xxx **km**; x xxx **km**

(*) Kaardi põlvkonna numbri saab trükkida ainult aruka sõidumeerikuga.

11	***Päeva kokkuvõte***	
	Plokiidentifikaator	----------Σ----------
11.1	***VU kokkuvõte aegadest, mil juhikaardi pesas kaarti ei olnud***	
	Plokiidentifikaator	1----
11.2	***VU kokkuvõte aegadest, mil kaasjuhikaardi pesas kaarti ei olnud***	
	Plokiidentifikaator	2----
11.3	***VU päeva kokkuvõte juhi kohta***	
	Kirjeidentifikaator	----------
	Juhi perekonnanimi	Perekonnanimi_____
	Juhi eesnimi (eesnimed)	Eesnimi_____
	Juhikaardi identimisandmed	Kaardi_identimisandmed__
11.4	*Sissekanne tööpäeva algus- ja/või lõpukoha kohta*	
	pi = algus-/lõpukoha piktogramm, aeg, riik, piirkond	pitt:mm Rii Prk
	Läbisõidumõõdik	x xxx xxx **km**
11.5	*Sissekanne tööpäeva algus- ja/või lõpukoha kohta*	
	ja kolme järjestikuse sõidutunni täitumisel	tt:mm
	Läbisõidumõõdik	x xxx xxx **km**
11.6	*Tegevused kokku (kaardilt)*	
	Kogu juhtimisaeg, läbitud vahemaa	tttmm x xxx **km**
	Kogu töö- ja valmisolekuaeg	tttmm tttmm
	Kogu puhke- ja teadmata aeg	tttmm ? tttmm
	Meeskonnategevuste kogukestus	tttmm
11.7	*Tegevused kokku (ajad ilma kaardita juhikaardi pesas)*	
	Kogu juhtimisaeg, läbitud vahemaa	tttmm x xxx **km**
	Kogu töö- ja valmisolekuaeg	tttmm tttmm
	Kogu puhkeaeg	tttmm

11.8	*Tegevused kokku (ajad ilma kaardita kaasjuhikaardi pesas)*	
	Kogu töö- ja valmisolekuaeg	tttmm tttmm
	Kogu puhkeaeg	tttmm
11.9	*Tegevused kokku (juhi kohta, võttes arvesse mõlemat pesa)*	
	Kogu juhtimisaeg, läbitud vahemaa	tttmm x xxx **km**
	Kogu töö- ja valmisolekuaeg	tttmm tttmm
	Kogu puhkeaeg	tttmm
	Meeskonnategevuste kogukestus	tttmm

Kui nõutakse päevast väljatrükki jooksva päeva kohta, arvutatakse päeva kokkuvõtte trükkimise ajal olemasolevate andmete alusel.

12	***Kaardile salvestatud sündmused ja/või vead***	
12.1	Plokiidentifikaator viimased 5 sündmust ja viga kaardilt	----------!×----------
12.2	Plokiidentifikaator kõik registreeritud sündmused kaardil	----------!----------
12.3	Plokiidentifikaator kõik registreeritud vead kaardil	----------×----------
12.4	*Sündmuse- ja/või veakirje*	
	Kirjeidentifikaator	
	Sündmuse/vea piktogramm, kirje eesmärk, alguse kuupäev ja kellaaeg	Pik (p) pp/kk/aaaa tt:mm
	Sündmuse/vea lisakood (kui see on olemas), kestus	!xx tttmm
	Sõiduki, milles sündmus või viga toimus, registreerinud liikmesriik ja VRN	Riik/VRN_____

13	***Sõidukiseadmesse salvestatud või seal kestvad sündmused ja/või vead***	
13.1	Plokiidentifikaator viimased 5 sündmust ja viga VUst	----------!×----------
13.2	Plokiidentifikaator kõik VUs registreeritud või kestvad sündmused	----------!----------
13.3	Plokiidentifikaator kõik VUs registreeritud või kestvad sündmused	----------×----------
13.4	*Sündmuse- ja/või veakirje*	
	Kirjeidentifikaator	
	Sündmuse/vea piktogramm, kirje eesmärk, alguse kuupäev ja kellaaeg	Pik (p) pp/kk/aaaa tt:mm
	Sündmuse/vea lisakood (kui see on olemas), sarnaste sündmuste arv sellel päeval, kestus	!xx (xxx) tttmm
	Sündmuse või vea alguses või lõpus sisestatud kaartide identimisandmed (kuni 4 rida, kordamata samu kaardinumbreid)	Kaardi_identimisandmed__ Kaardi_identimisandmed__ Kaardi_identimisandmed__ Kaardi_identimisandmed__
	Olukord, kus ühtki kaarti polnud sisestatud	---
	Tootjaomased andmed	**<Literal><ErrorCode>**

Kirje eesmärk (p) on numbrikood, mis selgitab, miks sündmus või viga registreeriti, ning see on kodeeritud vastavalt andmeelemendile `EventFaultRecordPurpose`.

`Literal` on sõidumeeriku tootja literaal, mis võib sisaldada kuni 12 märki.

`ErrorCode` on sõidumeeriku tootja veakood, mis võib sisaldada kuni 12 märki.

14 ***Sõidukiseadme (VU) identimisandmed***

Plokiidentifikaator	----------⊟----------
VU tootja nimi	⊟ Nimi_____
VU tootja aadress	Aadress_____
VU osa number	Osa_number_____
VU tüübikinnitusnumber	Tüübikinnitusnr_
VU seerianumber	Seerianr_____
VU tootmisaasta	aaaa
VU tarkvaraversioon ja selle installeerimise kuupäev	V xxxx pp/kk/aaaa

15 ***Anduri identimisandmed***

Plokiidentifikaator	----------⍼----------
15.1 *Ühendamise kirje*	
Anduri seerianumber	⍼ Seerianr_____
Anduri tüübikinnitusnumber	Tüübikinnitusnr_
Anduri ühendamise kuupäev	pp/kk/aaaa tt:mm

16 ***GNSSi identimisandmed***

Plokiidentifikaator	----------▚----------
16.1 *Ühendamise kirje*	
GNSSi välisseadme seerianumber	▚ Seerianr_____
GNSSi välisseadme tüübikinnitusnumber	Tüübikinnitusnr_
GNSSi välisseadme ühendamise kuupäev	pp/kk/aaaa tt:mm

17 ***Kalibreerimisandmed***

Plokiidentifikaator	----------⍑----------
17.1 *Kalibreerimiskirje*	
Kirjeidentifikaator	----------
Kalibreerimise teostanud töökoda	⍑ Töökoja_nimi_____
Töökoja aadress	Töökoja_aadress_____
Töökojakaardi identimisandmed	Kaardi_identimisandmed__
Töökojakaardi kehtivuse lõppkuupäev	pp/kk/aaaa
Tühi rida	
Kalibreerimise kuupäev + kalibreerimise eesmärk	⍑ pp/kk/aaaa (p)
VIN	⍝ VIN_____
Registreerinud liikmesriik ja VRN	Riik/VRN_____
Sõidukit iseloomustav koefitsient	w xx xxx imp/km
Sõidumeeriku konstant	k xx xxx imp/km
Effective circumference of wheel tyres	l xx xxx mm
Paigaldatud rehvide rehvimõõt	● _____
Kiiruspiiriku seadistus	› xxx km/h
Läbisõidumõõdiku vana ja uus näit	x xxx xxx – x xxx xxx km

Kalibreerimise eesmärk (p) märgitakse numbrikoodiga, mis selgitab, miks need kalibreerimisparameetrid registreeriti, ning see on kodeeritud vastavalt andmeelemendile `CalibrationPurpose`.

18 ***Aja korrigeerimine***

Plokiidentifikaator

```
----------◷----------
```

18.1 *Aja korrigeerimise kirje*

Kirjeidentifikaator
Eelmine kuupäev ja kellaaeg
Uus kuupäev ja kellaaeg
Aja korrigeerimise teostanud töökoda
Töökoja aadress
Töökojakaardi identimisandmed
Töökojakaardi kehtivuse lõppkuupäev

```
  --------------------
!◷ pp/kk/aaaa tt:mm
 ◷ pp/kk/aaaa tt:mm
T Töökoja_nimi__________
  Töökoja_aadress_______
Kaardi_identimisandmed__
  pp/kk/aaaa
```

19 ***Sõidukiseadmes registreeritud viimane sündmus ja viga***

Plokiidentifikaator
Viimase sündmuse kuupäev, kellaaeg
Viimase vea kuupäev, kellaaeg

```
----------!×🖩----------
! pp/kk/aaaa tt:mm
× pp/kk/aaaa tt:mm
```

20 ***Teave kiiruse ületamise kontrolli kohta***

Plokiidentifikaator
Viimase KIIRUSE ÜKLETAMISE KONTROLLI kuupäev ja kellaaeg
Esimese kiiruseületamise kuupäev/kellaaeg ja pärast seda toimunud kiiruse ületamise sündmuste arv

```
----------»»----------
»▯pp/kk/aaaa tt:mm
»»pp/kk/aaaa tt:mm (nnn)
```

21 ***Kiiruse ületamise kirje***

21.1 Plokiidentifikaator „Esimene kiiruse ületamine pärast viimast kalibreerimist”

```
--------»»T---------
```

21.2 Plokiidentifikaator „Viis kõige tõsisemat sündmust viimase 365 päeva jooksul”

```
-------»»(365)------
```

21.3 Plokiidentifikaator „Viimase kümne päeva jooksul toimunud iga päeva kõige tõsisem kiiruse ületamine”

```
-------»»(10)-------
```

21.4 Kirjeidentifikaator
Kuupäev, kellaaeg ja kestus
Maks. ja keskmine kiirus, sarnaste sündmuste arv samal päeval
Juhi perekonnanimi
Juhi eesnimi (eesnimed)
Juhikaardi identimisandmed

```
  --------------------
»»pp/kk/aaaa tt:mm tttmm
  xxx km/h xxx km/h(xxx)
◙ Perekonnanimi_________
  Eesnimi_______________
Kaardi_identimisandmed__
```

21.5 Kui plokis ei ole kiiruse ületamise kirjeid

```
»»---
```

22 ***Käsitsi kirjutatud teave***

Plokiidentifikaator

```
------------------------
```

22.1 Kontrolli koht
22.2 Kontrollija allkiri
22.3 Algusaeg
22.4 Lõpuaeg
22.5 Juhi allkiri

```
▯• ..................
▯  ..................
◷+ ..................
+◷ ..................
◙  ..................
```

„Käsitsi kirjutatud teave”: lisage käsitsi kirjutatava punkti kohale piisavalt tühje ridu, et sinna oleks ka tegelikult võimalik kirjutada nõutav teave või allkiri.

23 ***Viimased sõidukiseadmesse sisestatud kaardid***
Plokiidentifikaator
23.1 Sisestatud kaart
Kirjeidentifikaator
Kaardi tüüp, põlvkond, versioon, tootja (*)
Kaardi identimisandmed
Kaardi seerianumber
Kaardi viimase sisestamise kuupäev ja kellaaeg

```
-------- ⊟◨⊙ --------

----
⍑ <gen> <versioon> <MC>
Kaardi_identimisandmed__
Kaardi_seerianr__________
pp/kk/aaaa tt:mm
```

(*) Kõik ühel real:

kaardi tüüp: piktogramm, üks märk + tühik
gen: GEN1 või GEN2, 4 märki + tühik
versioon: kuni 10 märki
MC: tootja kood, 3 märki

3. VÄLJATRÜKKIDE SPETSIFIKATSIOON

Käesolevas peatükis on kasutatud järgmisi märkimistavasid.

N	Trükiploki või kirje number N
N	Trükiploki või kirje number N, seda korratakse nii palju kui vaja
X/Y	Trükiplokid või kirjed X ja/või Y vastavalt vajadusele, neid korratakse nii palju kui vaja

3.1. **Juhi ühe päeva tegevuse väljatrükk kaardilt**

PRT_008 Juhi ühe päeva tegevuse väljatrükk kaardilt vastab järgmisele vormingule.

1	Dokumendi trükkimise kuupäev ja kellaaeg
2	Väljatrüki tüüp
3	Kontrollija identimisandmed (VUsse on sisestatud kontrollikaart)
3	Juhi identimisandmed (kaardilt, millelt tehakse väljatrükk + GEN)
4	Sõiduki identimisandmed (sõiduk, millelt tehakse väljatrükk)
5	VU identimisandmed (VU, millest tehakse väljatrükk + GEN)
6	Selle VU viimane kalibreerimine
7	Kontrollitava juhi eelmine kontrollimine
8	Juhi tegevuste eraldaja
8a	Tingimus „Sõidumeerik mittevajalik“ päeva alguses
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Juhi tegevused toimumise järjekorras
11	Päevase kokkuvõtte eraldaja

11.4	Sisestatud kohad kronoloogilises järjestuses
11.5	GNSSi andmed
11.6	Tegevused kokku
12.1	Kaardil olevate sündmuste ja vigade eraldaja
12.4	Sündmuse-/veakirjed (kaardile salvestatud 5 viimast sündmust või viga)
13.1	VUs olevate sündmuste ja vigade eraldaja
13.4	Sündmuse-/veakirjed (VUsse salvestatud või seal kestvad 5 viimast sündmust või viga)
22.1	Kontrolli koht
22.2	Kontrollija allkiri
22.5	Juhi allkiri

3.2. **Juhi ühe päeva tegevuse väljatrükk sõidukiseadmest**

PRT_009 Juhi ühe päeva tegevuse väljatrükk sõidukiseadmest vastab järgmisele vormingule.

1	Dokumendi trükkimise kuupäev ja kellaaeg
2	Väljatrüki tüüp
3	Kaardiomaniku identimisandmed (kõigi VUsse sisestatud kaartide kohta + GEN)
4	Sõiduki identimisandmed (sõiduk, millelt tehakse väljatrükk)
5	VU identimisandmed (VU, millest tehakse väljatrükk + GEN)
6	Selle VU viimane kalibreerimine
7	Selle sõidumeeriku viimane kontrollimine
9	Juhi tegevuste eraldaja
10	Juhikaardi pesa eraldaja (pesa 1)
10a	Tingimus „Sõidumeerik mittevajalik“ päeva alguses
10.1 / 10.2 / 10.3 /10.3a / 10.4	Tegevused kronoloogilises järjestuses (juhikaardi pesa)
10	Kaasjuhikaardi pesa eraldaja (pesa 2)
10a	Tingimus „Sõidumeerik mittevajalik“ päeva alguses
10.1 / 10.2 / 10.3 /10.3a / 10.4	Tegevused kronoloogilises järjestuses (kaasjuhikaardi pesa)
11	Päevase kokkuvõtte eraldaja
11.1	Kokkuvõte aegadest, mil juhikaardi pesas kaarti ei olnud
11.4	Sisestatud kohad kronoloogilises järjestuses
11.5	GNSSi andmed
11.6	Tegevused kokku
11.2	Kokkuvõte aegadest, mil kaasjuhikaardi pesas kaarti ei olnud
11.4	Sisestatud kohad kronoloogilises järjestuses
11.5	GNSSi andmed

11.7	Tegevused kokku
11.3	Juhi tegevused kokku, võttes arvesse mõlemat pesa
11.4	Selle juhi sisestatud kohad kronoloogilises järjestuses
11.5	GNSSi andmed
11.8	Selle juhi tegevused kokku
13.1	Sündmuste ja vigade eraldaja
12.4	Sündmuse-/veakirjed (VUsse salvestatud või seal kestvad 5 viimast sündmust või viga)
13.1	Kontrolli koht
22.2	Kontrollija allkiri
22.3	Alates (koht juhi jaoks, kellel ei ole kaarti, et ta saaks ära näidata temaga seotud ajad)
22.4	kuni
22.5	Juhi allkiri

3.3. **Sündmuste ja vigade väljatrükk kaardilt**

PRT_010 Sündmuste ja vigade väljatrükk kaardilt vastab järgmisele vormingule.

1	Dokumendi trükkimise kuupäev ja kellaaeg
2	Väljatrüki tüüp
3	Kontrollija identimisandmed (kui VUsse on sisestatud kontrollikaart + GEN)
3	Juhi identimisandmed (kaardilt, millelt tehakse väljatrükk)
4	Sõiduki identimisandmed (sõiduk, millelt tehakse väljatrükk)
12.2	Sündmuste eraldaja
12.4	Sündmusekirjed (kõik kaardile salvestatud sündmused)
12.3	Vigade eraldaja
12.4	Veakirjed (kõik kaardile salvestatud vead)
22.1	Kontrolli koht
22.2	Kontrollija allkiri
22.5	Juhi allkiri

3.4. **Sündmuste ja vigade väljatrükk sõidukiseadmest**

PRT_011 Sündmuste ja vigade väljatrükk sõidukiseadmest vastab järgmisele vormingule.

1	Dokumendi trükkimise kuupäev ja kellaaeg
2	Väljatrüki tüüp
3	Kaardiomaniku identimisandmed (kõigi VUsse sisestatud kaartide kohta + GEN)
4	Sõiduki identimisandmed (sõiduk, millelt tehakse väljatrükk)

13.2	Sündmuste eraldaja
13.4	Sündmusekirjed (kõik sõidukiseadmesse salvestatud või seal kestvad sündmused)
13.3	Vigade eraldaja
13.4	Veakirjed (kõik sõidukiseadmesse salvestatud või seal kestvad vead)
22.1	Kontrolli koht
22.2	Kontrollija allkiri
22.5	Juhi allkiri

3.5. **Tehniliste andmete väljatrükk**

PRT_012 Tehniliste andmete väljatrükk vastab järgmisele vormingule.

1	Dokumendi trükkimise kuupäev ja kellaaeg
2	Väljatrüki tüüp
3	Kaardiomaniku identimisandmed (kõigi VUsse sisestatud kaartide kohta + GEN)
4	Sõiduki identimisandmed (sõiduk, millelt tehakse väljatrükk)
14	Sõidukiseadme (VU) identimisandmed
15	Anduri identimisandmed
15.1	Anduri ühendamise andmed (kõik olemasolevad andmed kronoloogilises järjestuses)
16	GNSSi identimisandmed
16.1	GNSSi välisseadme ühendamise andmed (kõik olemasolevad andmed kronoloogilises järjestuses)
17	Kalibreerimisandmete eraldaja
17.1	Kalibreerimiskirjed (kõik olemasolevad kirjed kronoloogilises järjestuses)
18	Aja korrigeerimise eraldaja
18.1	Aja korrigeerimise kirjed (kõik olemasolevad kirjed aja korrigeerimise ja kalibreerimisandmete kirjetest)
19	Sõidukiseadmes registreeritud viimane sündmus ja viga

3.6. **Kiiruse ületamiste väljatrükk**

PRT_013 Kiiruse ületamiste väljatrükk vastab järgmisele vormingule.

1	Dokumendi trükkimise kuupäev ja kellaaeg
2	Väljatrüki tüüp
3	Kaardiomaniku identimisandmed (kõigi VUsse sisestatud kaartide kohta + GEN)
4	Sõiduki identimisandmed (sõiduk, millelt tehakse väljatrükk)
20	Teave kiiruse ületamise kontrolli kohta
21.1	Kiiruse ületamise andmete identifikaator
21.4 / 21.5	Esimene kiiruse ületamine pärast viimast kalibreerimist

21.2	Kiiruse ületamise andmete identifikaator
21.4 / 21.5	5 kõige tõsisemat kiiruse ületamise sündmust viimase 365 päeva jooksul
21.3	Kiiruse ületamise andmete identifikaator
21.4 / 21.5	Viimase kümne päeva jooksul toimunud iga päeva kõige tõsisem kiiruse ületamine
22.1	Kontrolli koht
22.2	Kontrollija allkiri
22.5	Juhi allkiri

3.7. **Sisestatud kaarte käsitlev teave**

PRT_014 Sisestatud kaarte käsitleva teabe väljatrükk vastab järgmisele vormingule.

1	Dokumendi trükkimise kuupäev ja kellaaeg
2	Väljatrüki tüüp
3	Kaardiomaniku identimisandmed (kõigi VUsse sisestatud kaartide kohta)
23	Viimane VUsse sisestatud kaart
23.1	Sisestatud kaardid (kuni 88 kirjet)
12.3	Vigade eraldaja

5. liide

EKRAAN

Käesolevas liites on kasutatud järgmisi vormingu märkimistavasid:

— **poolpaksu** kirjaga tähistatakse kuvatavat lihtteksti (ekraanil kasutatakse tavalist kirja);

— tavalise kirjaga tähistatakse muutujaid (piktogrammid või andmed), mis kuvamisel asendatakse nende väärtusega:

  — pp kk aaaa: päev, kuu, aasta,

  — tt: tunnid,

  — mm: minutid,

  — D: kestust tähistav piktogramm,

  — EF: sündmust või riket tähistavate piktogrammide kombinatsioon,

  — O: kasutusrežiimi piktogramm.

DIS_001 Sõidumeerikus kasutatakse andmete kuvamiseks järgmisi vorminguid.

Andmed	Vorming
Vaikekuva	
Kohalik aeg	tt:mm
Kasutusrežiim	O
Juhiga seotud teave	1Ptttmm ⏸tttmm
Kaasjuhiga seotud teave	2Ptttmm
Tingimus „sõidumeerik mittevajalik“ kehtiv	OUT
Hoiatuskuva	
Katkematu juhtimisaja ületamine	1⊙tttmm ⏸tttmm
Sündmus või rike	EF
Muud kuvad	
UTC-kuupäev Kellaaeg	UTC⏱pp/kk/aaaa või UTC⏱pp.kk.aaaa tt:mm
Juhi katkematu juhtimisaeg ja kumulatiivne puhkepauside aeg	1⊙tttmm ⏸tttmm
Kaasjuhi katkematu juhtimisaeg ja kumulatiivne puhkepauside aeg	2⊙tttmm ⏸tttmm
Juhi kumulatiivne juhtimisaeg eelmisel ja jooksval nädalal	1⊙‖ ttttmm
Kaasjuhi kumulatiivne juhtimisaeg eelmisel ja jooksval nädalal	2⊙‖ ttttmm

6. liide

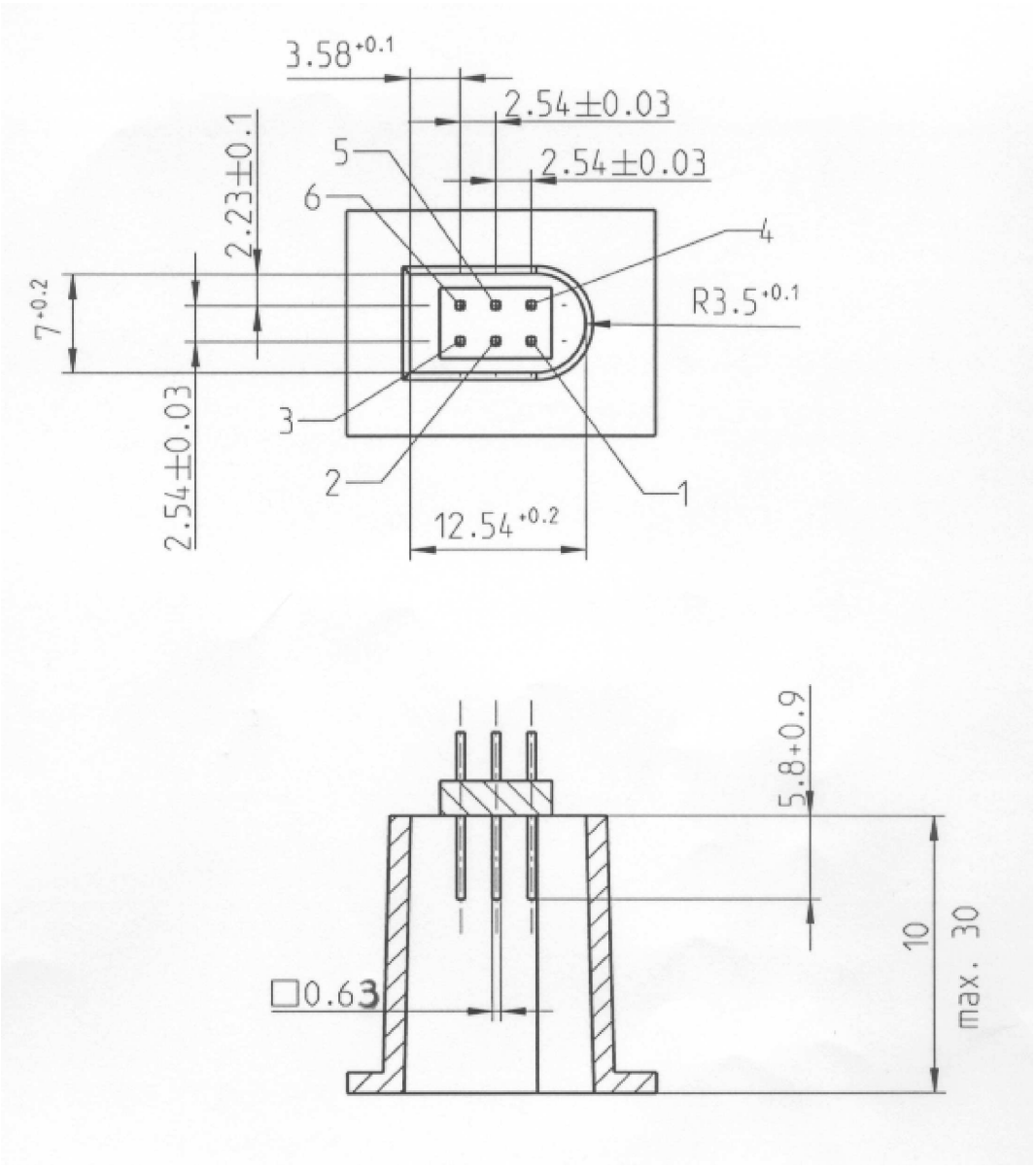
ESIPISTMIK KALIBREERIMISEKS JA ALLALAADIMISEKS

SISUKORD

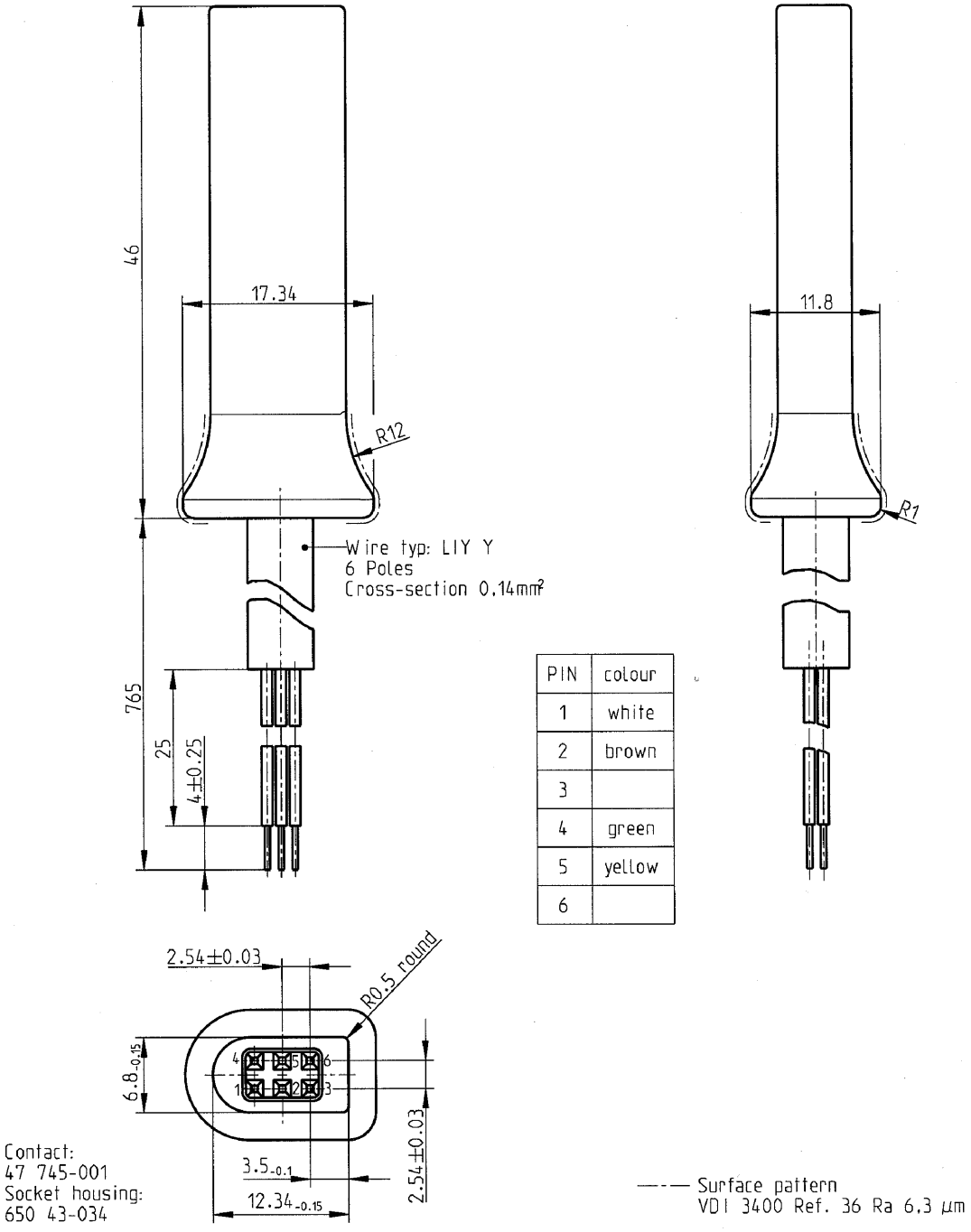
1. RIISTVARA

1.1. **Pistmik**

INT_001 Allalaadimis-/kalibreerimispistikupesa on esipaneelil paiknev kuue kontaktiga pesa, millele juurdepääsuks ei tule ühtki sõidumeeriku osa lahti ühendada ning mis vastab järgmisele joonisele (kõik mõõtmed on millimeetrites).



Järgmisel skeemil on tüüpiline kuue kontaktiga pistik.



1.2. **Kontaktide paigutus**

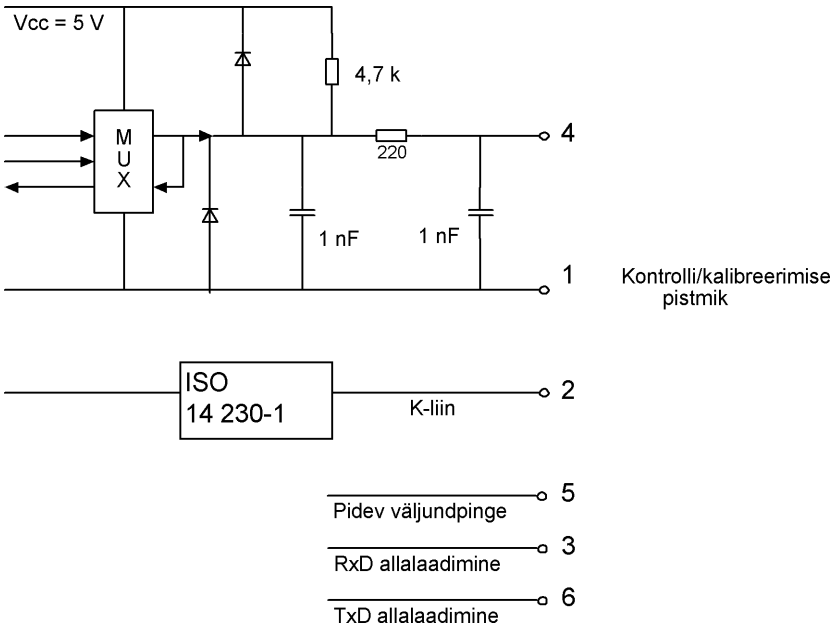
INT_002 Kontaktid paigutatakse vastavalt järgmisele tabelile.

Kontakt	Kirjeldus	Märkus
1	Aku miinuspoolus	Ühendatud sõiduki aku miinuspoolusega
2	Andmeside	K-liin (ISO 14230-1)

Kontakt	Kirjeldus	Märkus
3	RxD – Allalaadimine	Andmesisestus sõidumeerikusse
4	Sisend-/väljundsignaal	Kalibreerimine
5	Pidev väljundpinge	Pinge väärtuseks on ette nähtud sõiduki pinge miinus 3 V, et võtta arvesse kaitseelektroonikast tulenevat pingelangust Väljundvool 40 mA
6	TxD – Allalaadimine	Andmeväljastus sõidumeerikust

1.3. **Plokkskeem**

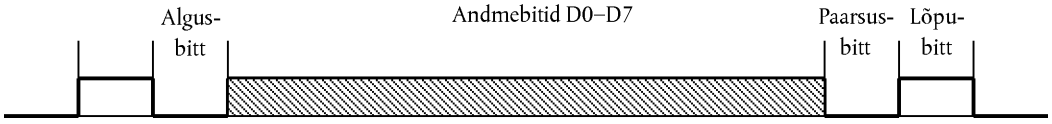
INT_003 Plokkskeem peab olema järgmine.



2. ALLALAADIMISLIIDES

INT_004 Allalaadimisliides vastab standardi RS232 spetsifikatsioonidele.

INT_005 Allalaadimisliideses kasutatakse ühte algusbitti, kaheksat andmebitti (kõige vähem tähtis bitt esimesena), ühte paarisuse paarsusbitti ja ühte lõpubitti.



Andmebaidi ülesehitus

Algusbitt: üks bitt, mille loogikatase on 0

Andmebitid: kõige vähem tähtis bitt edastatakse esimesena

Paarsusbitt: paarisus

Lõpubitt: üks bitt, mille loogikatase on 1

Kui edastatakse rohkem kui ühest baidist koosnevaid arvandmeid, 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 algne edastamiskiirus pärast ühenduse loomist seatakse 9 600 bitile sekundis.

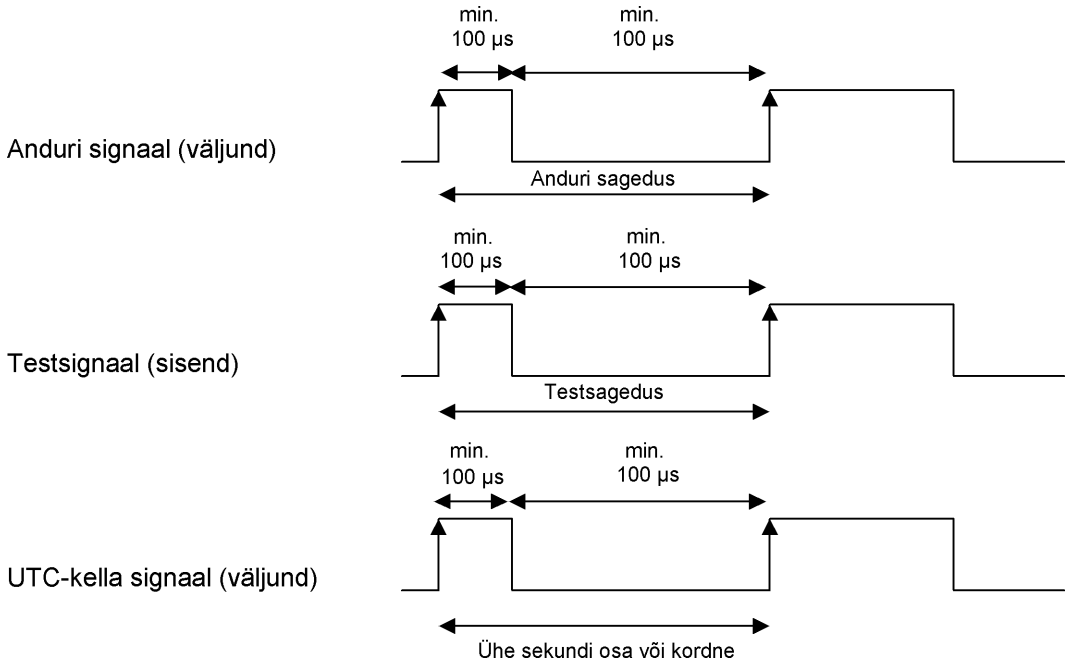
3. KALIBREERIMISLIIDES

INT_007 Andmeside vastab standardi ISO 14230-1 esimesele väljaandele „Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 1: Physical layer“ („Maanteesõidukid. Diagnostikasüsteemid. Võtmesõna-protokoll 2000. Osa 1: Füüsiline kiht“) (1999).

INT_008 Sisend-/väljundsignaal vastab järgmisele elektrilisele spetsifikatsioonile.

Näitaja	Minimaalne	Tüüpiline	Maksimaalne	Märkus
U_{madal} (sisend)			1,0 V	I = 750 µA
$U_{kõrge}$ (sisend)	4 V			I = 200 µA
Sagedus			4 kHz	
U_{madal} (väljund)			1,0 V	I = 1 mA
$U_{kõrge}$ (väljund)	4 V			I = 1 mA

INT_009 Sisend-/väljundsignaal vastab järgmistele ajastusskeemidele.



7. liide

ANDMETE ALLALAADIMISE PROTOKOLLID

SISUKORD

1. SISSEJUHATUS

Käesolevas liites on määratletud kord, mida tuleb järgida eri tüüpi andmete allalaadimiseks välisandmekandjale, ja protokollid, mida tuleb rakendada, et tagada andmete nõuetekohane edastus ja allalaaditud andmete vormingu täielik ühilduvus, mis võimaldab mis tahes kontrollijal neid andmeid uurida ning kontrollida enne andmete analüüsimist nende autentsust ja terviklust.

1.1. **Reguleerimisala**

Andmeid võib alla laadida välisandmekandjale:

— sõidukiseadmest sõidukiseadmega ühendatud eriotstarbelise seadme (IDE) abil,

— sõidumeerikukaardilt eriotstarbelise seadme abil, millel on kaardiliidese seade (IFD),

— sõidumeerikukaardilt sõidukiseadme kaudu sõidukiseadmega ühendatud eriotstarbelise seadme abil.

Et võimaldada välisandmekandjale salvestatud allalaaditud andmete autentsuse ja tervikluse tõendamist, laaditakse andmed alla koos neile lisatud allkirjaga kooskõlas 11. liitega „Ühised turbemehhanismid“. Samuti laaditakse alla allikseadme (sõidukiseade või kaart) identimisandmed ja turbesertifikaadid (liikmesriik ja seade). Andmete tõendaja peab sõltumatult omama usaldusväärset Euroopa avalikku võtit.

DDP_001 Ühe allalaadimisseansi ajal alla laaditud andmed tuleb salvestada välisandmekandjal 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. Seade (nt personaalarvuti), mida kasutatakse andmete allalaadimiseks välisandmekandjale

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*) turbetoimingu tegemine

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*) sõidukiseade

2. SÕIDUKISEADMES OLEVATE ANDMETE ALLALAADIMINE

2.1. **Allalaadimise kord**

Sõidukiseadmes olevate andmete allalaadimiseks peab kasutaja tegema järgmised toimingud:

— sisestama sõidumeerikukaardi sõidukiseadme kaardipesasse (*);

— ühendama eriotstarbelise seadme sõidukiseadme allalaadimispistmiku kaudu;

— looma ühenduse eriotstarbelise seadme ja sõidukiseadme vahel;

— valima eriotstarbelises seadmes allalaaditavad andmed ja saatma nõude sõidukiseadmele;

— sulgema allalaadimisseansi.

2.2. **Andmete allalaadimise protokoll**

Protokoll on struktureeritud ülem-alluv-põhimõttel, kus eriotstarbelisel seadmel on ülema ja sõidukiseadmel alluva roll.

Sõnumite struktuur, tüübid ja voog põhinevad võtmesõnaprotokollil 2000 (KWP) (ISO 14230-2: *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part2: Data link layer* („Maanteesõidukid. Diagnostikasüsteemid. Võtmesõnaprotokoll 2000. Osa 2: Andmelülikiht“)).

Rakenduskiht põhineb standardi ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1: Diagnostic services* („Maanteesõidukid. Diagnostikasüsteemid. Osa 1: Diagnostikateenused“), versioon 6, 22. veebruar 2001) kehtival versioonil.

2.2.1. *Sõnumi struktuur*

DDP_002 Kõigi eriotstarbelise seadme ja sõidukiseadme vahel liikuvate sõnumite vormingustruktuur koosneb kolmest osast:

— vormingubaidist (FMT), sihtbaidist (TGT), lähtebaidist (SRC) ja mõnikord pikkusbaidist (LEN) koosnev päis,

— andmeväli, mis koosneb teenuse identifikaatorbaidist (SID) ja muutuvast arvust andmebaitidest, mis võivad sisaldada valitavat diagnostilise seansi baiti (DS_) või valitavat edastusparameetribaiti (TRTP või TREP),

— kontrollsummabaidist (CS) koosnev kontrollsumma.

Päis				Andmeväli					Kontroll-summa
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 baiti				Maksimaalselt 255 baiti					1 bait

(*) Sisestatud kaart avab sobival tasemel juurdepääsu allalaadimisfunktsioonile ja andmetele. Sõidukiseadme ühte pesasse sisestatud juhikaardil olevaid andmeid peab siiski olema võimalik alla laadida ka juhul, kui teise pesasse ei ole sisestatud ühtki muud tüüpi kaarti.

Baidid TGT ja SRC väljendavad sõnumi saaja ja lähetaja füüsilist aadressi. Kuueteistkümnendsüsteemis on selle väärtus eriotstarbelise seadme puhul F0 ja sõidukiseadme puhul EE.

Bait LEN on andmevälja osa pikkus.

Kontrollsummabait (CS) on 8-bitistes rühmades kõigi sõnumi baitide, välja arvatud CS ise, summa moodul 256.

Baidid FMT, SID, DS_, TRTP ja TREP määratletakse käesolevas dokumendis allpool.

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 loendur, mis näitab allsõnumi numbrit terviksõnumis. Vigade kontrollimise ja katkestamise võimaldamiseks saadab eriotstarbeline seade iga allsõnumi kohta kinnitussõnumi. Eriotstarbeline seade võib allsõnumi aktsepteerida, paluda selle uuesti saata, nõuda sõidukiseadmelt edastamise uuesti alustamist või edastamise katkestada.

DDP_004 Kui viimase allsõnumi andmeväli sisaldab täpselt 255 baiti, tuleb sellele lisada tühja andmeväljaga (välja arvatud SID, TREP ja allsõnumi loendur) viimane allsõnum, mis näitab sõnumi lõppu.

Näide:

Päis	SID	TREP	Sõnum	CS
4 baiti	Pikem kui 255 baiti			

Edastatakse kujul:

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	Lühem kui 255 baiti					

või kujul:

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*

Sõidukiseadme ja eriotstarbelise seadme vahel andmete allalaadimiseks kasutatav sideprotokoll eeldab kaheksa erineva sõnumitüübi kasutamist andmevahetuses.

Järgmises tabelis on esitatud ülevaade nende sõnumite kohta.

Sõnumi struktuur	Maksimaalselt 4 baiti Päis				Maksimaalselt 255 baiti Andmed			1 bait Kontroll-summa
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Side alustamise nõue	81	EE	F0		81			E0
Side alustamisega nõustumist kinnitav vastus	80	F0	EE	03	C1		EA, 8F	9B
Diagnostilise seansi alustamise nõue	80	EE	F0	02	10	81		F1
Diagnostika alustamisega nõustumist kinnitav vastus	80	F0	EE	02	50	81		31
Sidelüli kontrolli teenus Boodikiiruse kontroll (1. etapp)								
9 600 Bd	80	EE	F0	04	87		01,01, 01	EC
19 200 Bd	80	EE	F0	04	87		01,01, 02	ED
38 400 Bd	80	EE	F0	04	87		01,01, 03	EE
57 600 Bd	80	EE	F0	04	87		01,01, 04	EF
115 200 Bd	80	EE	F0	04	87		01,01, 05	F0
Boodikiiruse kontrolli läbimist kinnitav vastus	80	F0	EE	02	C7		01	28
Ülekandmise boodikiirus (2. etapp)	80	EE	F0	03	87		02,03	ED
Üleslaadimise nõue	80	EE	F0	0A	35		00,00, 00,00, 00,FF,FF, FF,FF	99
Üleslaadimisega nõustumist kinnitav vastus	80	F0	EE	03	75		00,FF	D5

Sõnumi struktuur	Maksimaalselt 4 baiti Päis				Maksimaalselt 255 baiti Andmed			1 bait Kontroll-summa
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Andmete ülekandmise nõue								
Ülevaade	80	EE	F0	02	36	01		97
Tegevused	80	EE	F0	06	36	02	Kuupäev	CS
Sündmused ja vead	80	EE	F0	02	36	03		99
Üksikasjalikud andmed kiiruse kohta	80	EE	F0	02	36	04		9A
Tehnilised andmed	80	EE	F0	02	36	05		9B
Kaardilt alla laadimine	80	EE	F0	02	36	06	Pesa	CS
Andmete ülekandmisega nõustumist kinnitav vastus	80	F0	EE	LEN	76	TREP	Andmed	CS
Ülekande lõpetamise nõue	80	EE	F0	01	37			96
Ülekande lõpetamisega nõustumist kinnitav vastus	80	F0	EE	01	77			D6
Side lõpetamise nõue	80	EE	F0	01	82			E1
Side lõpetamisega nõustumist kinnitav vastus	80	F0	EE	01	C2			21
Allsõnumi saamise kinnitus	80	EE	F0	Len	83		Andmed	CS
Eitavad vastused								
Üldine keeldumine	80	F0	EE	03	7F	Sid Req	10	CS
Teenusel puudub tugi	80	F0	EE	03	7F	Sid Req	11	CS
Allfunktsioonil puudub tugi	80	F0	EE	03	7F	Sid Req	12	CS
Sõnumi pikkus vale	80	F0	EE	03	7F	Sid Req	13	CS
Tingimused pole õiged või nõudejada viga	80	F0	EE	03	7F	Sid Req	22	CS
Nõue väljaspool ulatust	80	F0	EE	03	7F	Sid Req	31	CS
Üleslaadimist ei aktsepteerita	80	F0	EE	03	7F	Sid Req	50	CS
Vastus ootel	80	F0	EE	03	7F	Sid Req	78	CS
Andmed puuduvad	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 midagi ei edastata.

— Terminit „üleslaadimine“ (eriotstarbelise seadme poolt vaadatuna) kasutatakse standardile ISO 14229 vastavuse tagamiseks. See tähendab sama mis „allalaadimine“ (sõidukiseadme poolt vaadatuna).

— Võimalikke kahebaidilisi allsõnumiloendureid ei ole tabelis näidatud.

— Pesa väljal osutatakse pesa numbrile, mis võib olla 1 (kaart on juhikaardi pesas) või 2 (kaart on kaasjuhikaardi pesas).

— Kui pesa numbrit ei ole täpsustatud, valib sõidukiseade pesa nr 1, kui selles pesas on kaart. Seade valib pesa nr 2 üksnes juhul, kui kasutaja on selle eraldi valinud.

2.2.2.1. Side alustamise nõue (SID 81)

DDP_005 Eriotstarbeline seade saadab selle sõnumi sidelüli loomiseks sõidukiseadmega. Algühendus luuakse alati kiirusega 9 600 boodi (kuni boodikiiruse võimaliku muutmiseni vastavate sidelüli kontrolli teenustega).

2.2.2.2. Side alustamisega nõustumist kinnitav vastus (SID C1)

DDP_006 Sõidukiseade saadab selle sõnumi nõustuva vastusena side alustamise nõudele. Sõnum sisaldab mõlemat võtmebaiti 'EA' ja '8F', mis näitavad, et seade toetab protokolli, millel on siht-, lähte- ja pikkusbaidiga päis.

2.2.2.3. Diagnostilise seansi alustamise nõue (SID 10)

DDP_007 Eriotstarbeline seade saadab diagnostilise seansi alustamise nõude, et taotleda sõidukiseadmelt uut diagnostilist seanssi. Allfunktsioon „default session" (81h) näitab, et tuleb avada standardne diagnostiline seanss.

2.2.2.4. Diagnostika alustamisega nõustumist kinnitav vastus (SID 50)

DDP_008 Sõidukiseade saadab diagnostika alustamisega nõustumist kinnitava vastuse, et nõustuda diagnostilise seansi alustamise nõudega.

2.2.2.5. Sidelüli kontrolli teenus (SID 87)

DDP_052 Eriotstarbeline seade kasutab sidelüli kontrolli teenust (*Link Control Service*) boodikiiruse muutmise algatamiseks. See toimub kahes etapis. Esimeses etapis teeb eriotstarbeline seade ettepaneku boodikiiruse muutmiseks, näidates ära uue kiiruse. Saades sõidukiseadmelt nõustuva vastuse, saadab eriotstarbeline seade sõidukiseadmele boodikiiruse muutuse kinnituse (teine etapp). Seejärel lülitub eriotstarbeline seade uuele boodikiirusele. Pärast kinnituse saamist lülitub sõidukiseade uuele boodikiirusele.

2.2.2.6. Sidelüli kontrolliga nõustumist kinnitav vastus (SID C7)

DDP_053 Sõidukiseade saadab sidelüli kontrolliga nõustumist kinnitava vastuse, et nõustuda sidelüli kontrolli teenuse nõudega (esimene etapp). Kinnitusnõudele (teine etapp) ei vastata.

2.2.2.7. Üleslaadimise nõue (SID 35)

DDP_009 Eriotstarbeline seade saadab üleslaadimise nõude sõnumi, et taotleda sõidukiseadmelt allalaadimistoimingut. Standardi ISO 14229 nõuete täitmiseks esitatakse sõnumis üksikasjad soovitud andmete aadressi, mahu ja vormingu kohta. Kuna eriotstarbeline seade neid enne allalaadimist ei tea, pannakse mäluaadressi väärtuseks null, vorming on krüpteerimata ja tihendamata ning valitakse maksimaalne mälu maht.

2.2.2.8. Üleslaadimisega nõustumist kinnitav vastus (SID 75)

DDP_010 Sõidukiseade saadab üleslaadimisega nõustumist kinnitava vastuse näitamaks eriotstarbelisele seadmele, et sõidukiseade on valmis andmeid alla laadima. Standardi ISO 14229 nõuete täitmiseks lisatakse nõustumissõnumisse andmed, mis näitavad eriotstarbelisele seadmele, et edaspidised andmete ülekandmisega nõustumist kinnitavad vastused sisaldavad maksimaalselt 00FFh baiti.

2.2.2.9. Andmete ülekandmise nõue (SID 36)

DDP_011 Eriotstarbeline seade saadab andmete ülekandmise nõude, et anda sõidukiseadmele teada, mis tüüpi andmeid hakatakse alla laadima. Ühebaidiline nõude edastusparameeter (TRTP) näitab edastuse tüüpi.

Andmeedastuse tüüpe on kuus:

— ülevaade (TRTP 01),

— tegevused konkreetsel kuupäeval (TRTP 02),

— sündmused ja vead (TRTP 03),

— üksikasjalikud andmed kiiruse kohta (TRTP 04),

— tehnilised andmed (TRTP 05),

— kaardilt alla laadimine (TRTP 06).

DDP_054 Eriotstarbeline seade peab nõudma ülevaate andmete edastamist (TRTP 01) allalaadimisseansi ajal, sest ainult see tagab sõidukiseadme sertifikaatide registreerimise allalaaditud failis (ning võimaldab tõendada digitaalallkirja).

Teisel juhul (TRTP 02) sisaldab andmete ülekandmise nõude sõnum viidet allalaaditavale kuupäevale (`TimeReal`-vormingus).

2.2.2.10. Andmete ülekandmisega nõustumist kinnitav vastus (SID 76)

DDP_012 Sõidukiseade saadab andmete ülekandmisega nõustumist kinnitava vastuse pärast andmete ülekandmise nõude saamist. Sõnum sisaldab nõutud andmeid koos nõude edastusparameetrile (TRTP) vastava vastuse edastusparameetriga (TREP).

DDP_055 Esimesel juhul (TREP 01) saadab sõidukiseade andmed, mis aitavad eriotstarbelise seadme kasutajal valida, milliseid andmeid ta edaspidi soovib alla laadida. Selles sõnumis sisaldub järgmine teave:

— turbesertifikaadid,

— sõiduki identimistunnus,

— sõidukiseadme hetkekuupäev ja -kellaaeg,

— varaseim ja hilisem kuupäev, mille andmeid saab alla laadida (sõidukiseadme andmed),

— märge selle kohta, kas sõidukiseadmes on kaarte,

— eelmine allalaadimine ettevõttele,

— ettevõttelukud,

— eelmised kontrollimised.

2.2.2.11. Ülekande lõpetamise nõue (SID 37)

DDP_013 Eriotstarbeline seade annab ülekande lõpetamise nõudega sõidukiseadmele teada, et allalaadimisseanss lõpetatakse.

2.2.2.12. Ülekande lõpetamisega nõustumist kinnitav vastus (SID 77)

DDP_014 Sõidukiseade saadab ülekande lõpetamisega nõustumist kinnitava vastuse, et nõustuda ülekande lõpetamise nõudega.

2.2.2.13. Side lõpetamise nõue (SID 82)

DDP_015 Eriotstarbeline seade saadab side lõpetamise nõude, et katkestada sidelüli sõidukiseadmega.

2.2.2.14. Side lõpetamisega nõustumist kinnitav vastus (SID C2)

DDP_016 Sõidukiseade saadab side lõpetamisega nõustumist kinnitava vastuse, et nõustuda side lõpetamise nõudega.

2.2.2.15. Allsõnumi saamise kinnitus (SID 83)

DDP_017 Eriotstarbeline seade saadab allsõnumi saamise kinnitus, et kinnitada mitme allsõnumina edastatud sõnumi iga osa kättesaamist. Andmeväli sisaldab sõidukiseadmelt saadud teenuseidentifikaatorit ja kahebaidilist koodi järgmiselt:

— MsgC +1 kinnitab allsõnumi nr MsgC korrektset kättesaamist.

Eriotstarbeline seade nõuab sõidukiseadmelt järgmist allsõnumit.

— MsgC näitab probleemi allsõnumi nr MsgC kättesaamisel.

Eriotstarbeline seade nõuab sõidukiseadmelt allsõnumi uuesti saatmist.

— FFFF nõuab sõnumi lõpetamist.

Eriotstarbeline seade saab seda kasutada selleks, et mis tahes põhjusel lõpetada sõidukiseadmest saabuva sõnumi edastamine.

Sõnumi viimase allsõnumi (LEN < 255) jaatamiseks võib kasutada ükskõik millist nendest koodidest või selle võib jätta jaatamata.

Sõidukiseadme vastuste puhul kasutatakse mitut allsõnumit järgmise vastuse saatmiseks:

— andmete ülekandmisega nõustumist kinnitav vastus (SID 76).

2.2.2.16. Eitav vastus (SID 7F)

DDP_018 Sõidukiseade saadab eespool osutatud nõudesõnumitele eitava vastuse, kui sõidukiseade ei saa nõuet täita. Sõnumi andmeväljad sisaldavad vastuse teenuseidentifikaatorit (7F), nõude teenuseidentifikaatorit ja eitava vastuse põhjuse koodi. Kasutada saab järgmisi koode:

— 10 üldine keeldumine

Toimingut ei saa teha mõnel allpool nimetamata põhjusel.

— 11 teenusel puudub tugi

Nõude teenuseidentifikaator 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 nõudesõnumite järjekord ei ole õige.

— 31 nõue väljaspool ulatust

Nõude kirjeparameeter (andmeväli) ei ole kehtiv.

— 50 üleslaadimist ei aktsepteerita

Nõuet ei saa täita (sõidukiseade ei ole selleks sobivas kasutusrežiimis või sõidukiseadmes on tekkinud sisemine viga).

— 78 vastus ootel

Nõutud toimingut ei ole võimalik õigeaegselt teha ja sõidukiseade ei ole valmis uut nõuet vastu võtma.

— FA andmed puuduvad

Sõidukiseadmes ei ole andmete ülekandmise nõudes soovitud andmeid (nt kaart ei ole sisestatud jne).

2.2.3. *Sõnumivoog*

Tüüpiline sõnumivoog tavalise andmete allalaadimise käigus on järgmine:

Eriotstarbeline seade		Sõidukiseade
Side alustamise nõue	⇨ ⇦	Kinnitav vastus
Diagnostilise teenuse alustamise nõue	⇨ ⇦	Kinnitav vastus
Üleslaadimise nõue	⇨ ⇦	Kinnitav vastus

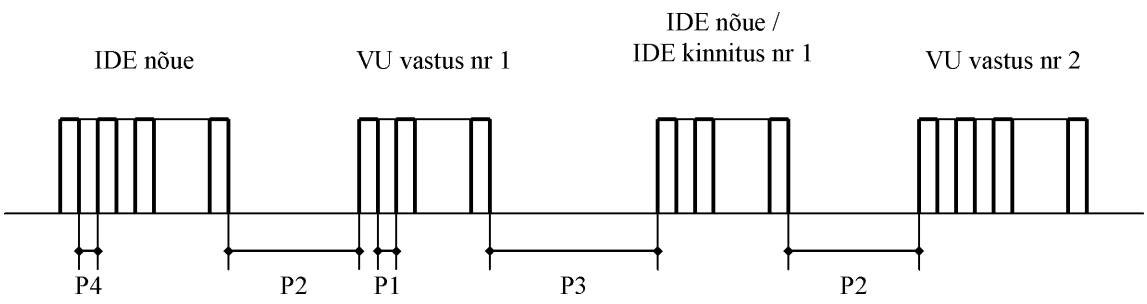
Eriotstarbeline seade		Sõidukiseade
Ülevaate andmete ülekandmise nõue	⇨	
	⇦	Kinnitav vastus
Andmete ülekandmise nõue nr 2	⇨	
	⇦	Kinnitav vastus nr 1
Allsõnumi saamise kinnitus nr 1	⇨	
	⇦	Kinnitav vastus nr 2
Allsõnumi saamise kinnitus nr 2	⇨	
	⇦	Kinnitav vastus nr m
Allsõnumi saamise kinnitus nr m	⇨	
	⇦	Kinnitav vastus (andmeväli < 255 baiti)
Allsõnumi saamise kinnitus (valitav)	⇨	
…		
Andmete ülekandmise nõue nr n	⇨	
	⇦	Kinnitav vastus
Ülekande lõpetamise nõue	⇨	
	⇦	Kinnitav vastus
Side lõpetamise nõue	⇨	
	⇦	Kinnitav vastus

2.2.4. *Ajastus*

DDP_019 Tavatöötamise ajal on asjakohased järgmisel joonisel näidatud ajastusparameetrid:

Joonis 1.

Sõnumivoog, ajastus



kus

P1 = baitidevaheline aeg sõidukiseadme vastuses;

P2 = aeg eriotstarbelise seadme nõude lõpu ja sõidukiseadme vastuse alguse vahel või eriotstarbelise seadme kinnituse lõpu ja sõidukiseadme järgmise vastuse alguse vahel;

P3 = aeg sõidukiseadme vastuse lõpu ja eriotstarbelise seadme uue nõude alguse vahel või sõidukiseadme vastuse lõpu ja eriotstarbelise seadme kinnituse alguse vahel või eriotstarbelise seadme nõude lõpu ja eriotstarbelise seadme uue nõude alguse vahel, kui sõidukiseade ei vasta;

P4 = baitidevaheline aeg eriotstarbelise seadme nõudes;

P5 = P3 laiendatud väärtus kaardilt alla laadimiseks.

Ajastusparameetrite lubatud väärtused on näidatud järgmises tabelis (võtmesõnaprotokolli laiendatud ajastusparameetrite kogum, kasutatakse kiiremaks edastuseks füüsilisel adresseerimisel).

Ajastusparameeter	Väikseim lubatud väärtus (ms)	Suurim lubatud väärtus (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minutit

(*) Kui sõidukiseade annab eitava vastuse, mis sisaldab koodi „nõue korrektselt vastu võetud, vastus ootel“, laiendatakse seda väärtust samale suurimale lubatud väärtusele kui P3 puhul.

2.2.5. *Vigade käitlemine*

Kui sõnumivahetuse käigus tekib viga, muudetakse sõnumivoo skeemi sõltuvalt sellest, milline seade on vea tuvastanud ja milline sõnum on vea genereerinud.

Joonistel 2 ja 3 on näidatud vastavalt sõidukiseadme ja eriotstarbelise seadme vigade käitlemiskorda.

2.2.5.1. Side alustamise etapp

DDP_020 Kui eriotstarbeline seade tuvastab side alustamise etapis ajastuse või bitivooga seotud vea, ootab see enne nõude taasesitamist vähemalt aja P3 jooksul.

DDP_021 Kui sõidukiseade tuvastab vea eriotstarbelisest seadmest tulevas jadas, ei saada see vastust ja ootab uut side alustamise nõuet maksimaalselt aja P3 jooksul.

2.2.5.2. Side etapp

Võib määratleda kaks erinevat veatöötluse valdkonda.

1. **Sõidukiseade tuvastab eriotstarbelise seadme edastusvea.**

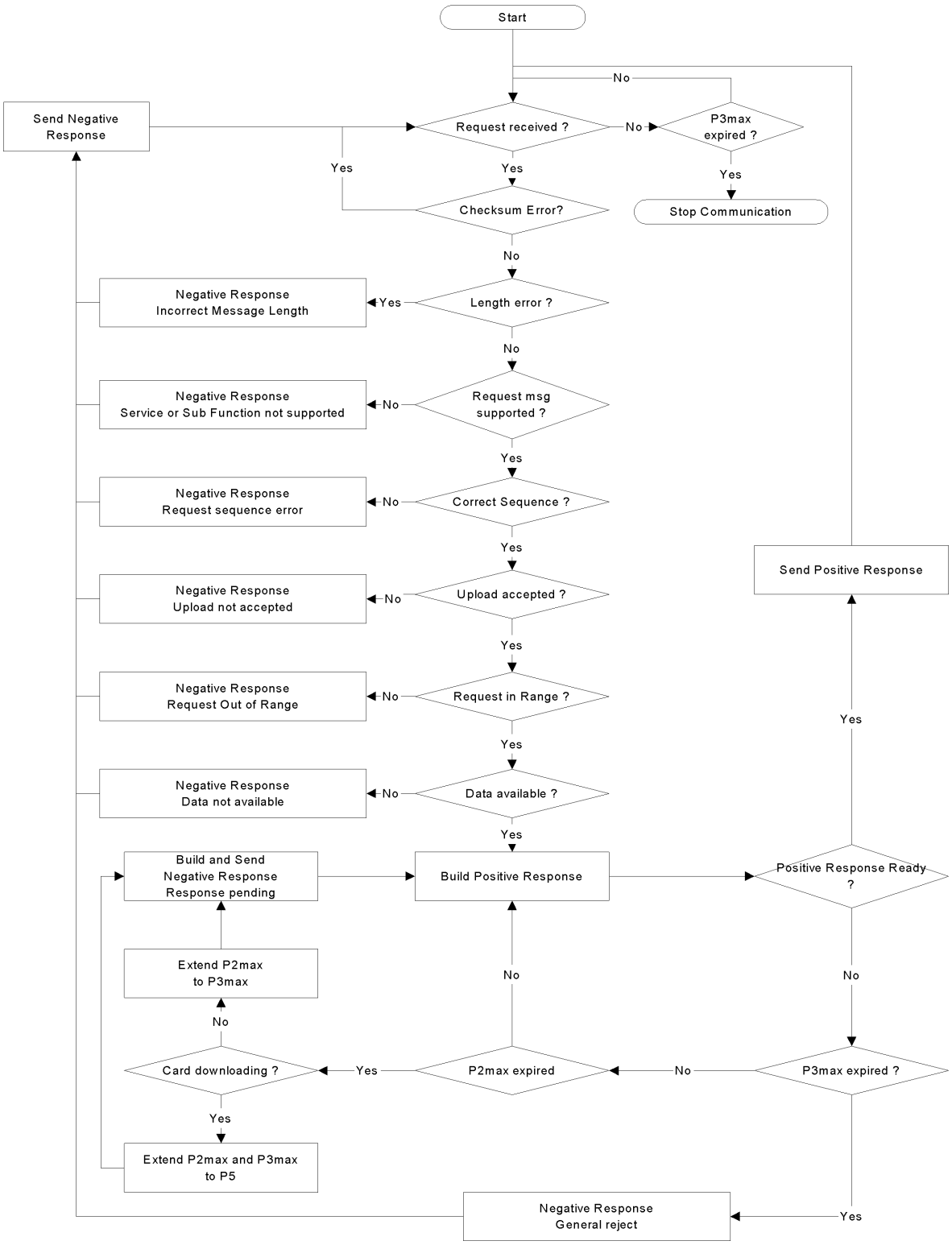
DDP_022 Iga saadud sõnumi puhul tuvastab sõidukiseade ajastusvead, baidivormingu vead (nt algus- ja lõpubiti rikkumised) ja kaadrivead (saadud vale arv baite, vale kontrollsummabait).

DDP_023 Kui sõidukiseade tuvastab ühe eespool nimetatud vigadest, ei saada see vastust ja eirab saadud sõnumit.

DDP_024 Sõidukiseade võib tuvastada saadud sõnumi vormingus või sisus muid vigu (nt sõnumil puudub tugi) isegi siis, kui sõnum vastab pikkus- ja kontrollsummanõuetele; sellisel juhul saadab sõidukiseade eriotstarbelisele seadmele eitava vastuse ja märgib vea laadi.

Joonis 2.

Vigade käitlemine sõidukiseadmes



2. **ERIOTSTARBELINE SEADE TUVASTAB SÕIDUKISEADME 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).

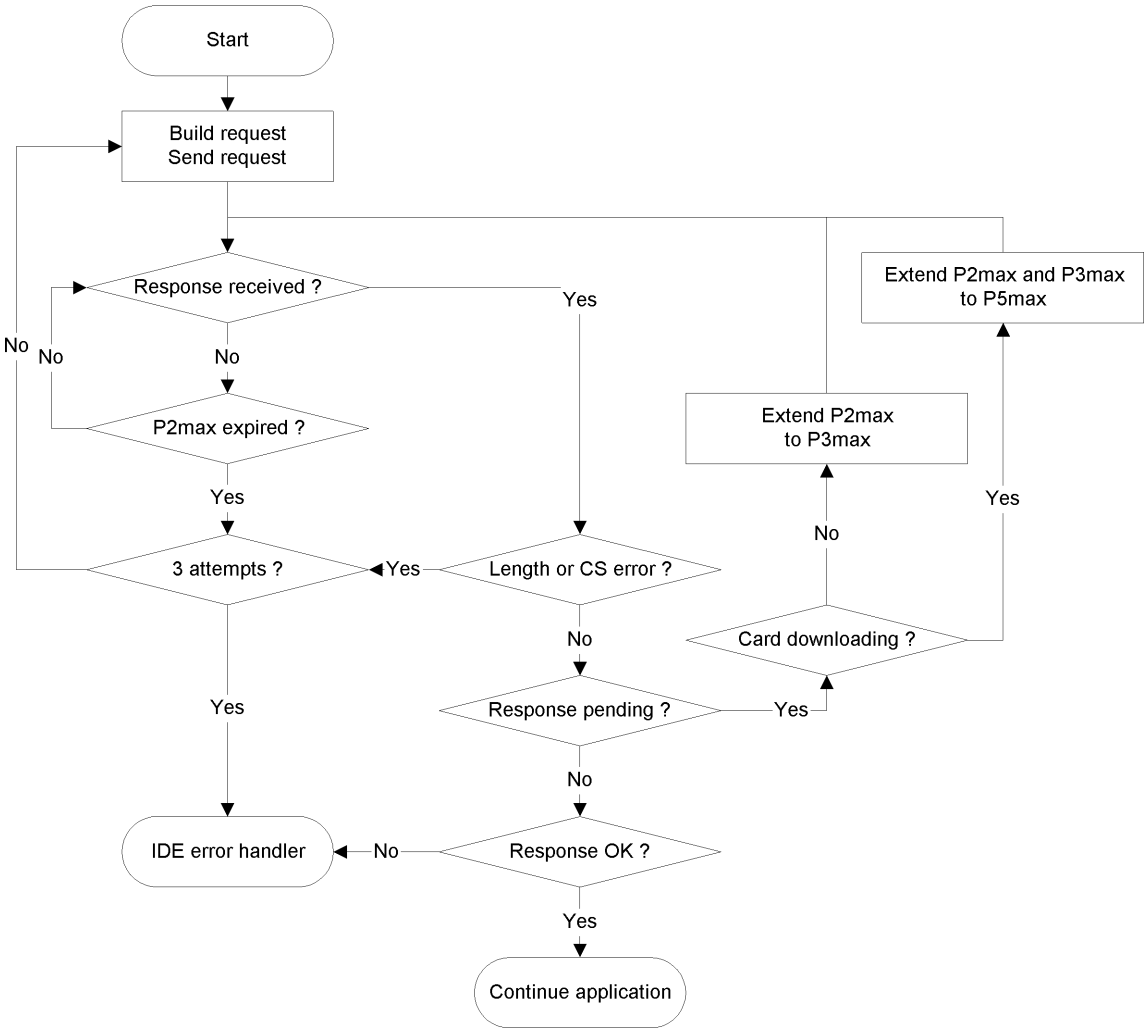
DDP_026 Eriotstarbeline seade tuvastab jadavead, nt allsõnumite loenduri vale suurenemine järjestikku saadud sõnumites.

DDP_027 Kui eriotstarbeline seade tuvastab vea või kui sõidukiseade ei vasta maksimaalse aja P2 jooksul, saadetakse nõudesõnum uuesti kokku kuni kolm korda. Selle vea tuvastamise eesmärgil käsitletakse allsõnumi saamise kinnitust sõidukiseadmele 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.

Vigade käitlemine eriotstarbelises seadmes



2.2.6. *Vastusesõnumi sisu*

Käesolevas punktis määratletakse erinevate kinnitavate vastusesõnumite andmeväljade sisu.

Andmeelemendid on määratletud 1. liite andmesõnastikus.

Märkus: 2. põlvkonna seadmetes vastab allalaadimiste korral igale kõrgema taseme andmeelemendile üks kirjemaatriks, isegi kui see sisaldab ainult ühte kirjet. Kirjemaatriks algab päisega; see päis sisaldab teavet kirje tüübi, kirje mahu ja kirjete arvu kohta. Järgmistes tabelites kasutatakse kirjemaatriksite nimetamisel kuju „… RecordArray“ (koos päisega).

2.2.6.1. Ülevaateandmete ülekandmisega nõustumist kinnitav vastus

DDP_029 Ülevaate andmete ülekandmisega nõustumist kinnitava vastussõnumi andmeväli sisaldab järgmisi andmeid järgmises järjestuses, kus teenuseidentifikaator (SID) on 76h ja vastuse edastusparameeter (TREP) on 01h ning rakendatakse kohast jagamist allsõnumiteks ja nende loendamist.

1. põlvkonna andmestruktuur

Andmeelement	Selgitus
MemberStateCertificate VUCertificate	Sõidukiseadme turbesertifikaadid
VehicleIdentificationNumber VehicleRegistrationIdentification	Sõiduki identimistunnus
CurrentDateTime	Sõidukiseadme hetkekuupäev ja -kellaaeg
VuDownloadablePeriod	Allalaaditav ajavahemik
CardSlotsStatus	Sõidukiseadmesse sisestatud kaartide tüüp
VuDownloadActivityData	Eelmine sõidukiseadmest alla laadimine
VuCompanyLocksData	Kõik salvestatud ettevõttelukud. Kui see osa on tühi, saadetakse ainult noOfLocks = 0.
VuControlActivityData	Kõik sõidukiseadmesse salvestatud kontrollikirjed. Kui see osa on tühi, saadetakse ainult noOfControls = 0.
Signature	Kõigi andmete (välja arvatud sertifikaadid) RSA allkiri alates kirjest VehicleIdentificationNumber kuni viimase VuControlActivityData kirje viimase baidini.

2. põlvkonna andmestruktuur

Andmeelement	Selgitus
MemberStateCertificateRecordArray	Liikmesriigi sertifikaat
VUCertificateRecordArray	Sõidukiseadme sertifikaat
VehicleIdentificationNumberRecordArray	Sõiduki identimistunnus
VehicleRegistrationNumberRecordArray	Sõiduki registreerimisnumber
CurrentDateTimeRecordArray	Sõidukiseadme hetkekuupäev ja -kellaaeg
VuDownloadablePeriodRecordArray	Allalaaditav ajavahemik
CardSlotsStatusRecordArray	Sõidukiseadmesse sisestatud kaartide tüüp
VuDownloadActivityDataRecordArray	Eelmine sõidukiseadmest alla laadimine
VuCompanyLocksRecordArray	Kõik salvestatud ettevõttelukud. Kui see osa on tühi, saadetakse maatriksi päis kirjega noOfLocks = 0.
VuControlActivityRecordArray	Kõik sõidukiseadmesse salvestatud kontrollikirjed. Kui see osa on tühi, saadetakse maatriksi päis kirjega noOfRecords = 0.
SignatureRecordArray	Kõigi eespool nimetatud andmete (välja arvatud sertifikaadid) ECC allkiri

2.2.6.2. Tegevusandmete ülekandmisega nõustumist kinnitav vastus

DDP_030 Tegevuste andmete ülekandmisega nõustumist kinnitava vastussõnumi andmeväli sisaldab järgmisi andmeid järgmises järjestuses, kus teenuseidentifikaator (SID) on 76h ja vastuse edastusparameeter (TREP) on 02h ning rakendatakse kohast jagamist allsõnumiteks ja nende loendamist.

1. põlvkonna andmestruktuur

Andmeelement	Selgitus
TimeReal	Allalaaditud andmetele vastava päeva kuupäev
OdometerValueMidnight	Läbisõidumõõdiku näit allalaaditud andmetele vastava päeva lõpus
VuCardIWData	Andmed kaartide sisestus- ja väljavõtmistsüklite kohta. — Kui selles osas andmeid ei ole, saadetakse ainult noOfVuCardIWRecords = 0. — Kui kirje VuCardIWRecord väärtus on üle kella 00.00 (kaart sisestati eelmisel päeval) või üle kella 24.00 (kaart võeti välja järgmisel päeval), esitatakse mõlema päeva täielikud andmed.
VuActivityDailyData	Pesade olek allalaaditud andmetele vastaval päeval kell 00.00 ja selle päeva kohta registreeritud tegevusmuutused.
VuPlaceDailyWorkPeriodData	Allalaaditud andmetele vastaval päeval registreeritud kohtadega seotud andmed. Kui see osa on tühi, saadetakse ainult noOfPlaceRecords = 0.
VuSpecificConditionData	Allalaaditud andmetele vastaval päeval registreeritud eritingimuste andmed. Kui see osa on tühi, saadetakse ainult noOfSpecificConditionRecords = 0.
Signature	Kõigi andmete RSA allkiri, mis hõlmab kõiki kirjeid alates kirjest TimeReal kuni viimase eritingimuse kirje viimase baidini.

2. põlvkonna andmestruktuur

Andmeelement	Selgitus
DateOfDayDownloadedRecordArray	Allalaaditud andmetele vastava päeva kuupäev
OdometerValueMidnightRecordArray	Läbisõidumõõdiku näit allalaaditud andmetele vastava päeva lõpus
VuCardIWRecordArray	Andmed kaartide sisestus- ja väljavõtmistsüklite kohta. — Kui see osa andmeid ei sisalda, saadetakse maatriksi päis kirjega noOfRecords = 0. — Kui kirje VuCardIWRecord väärtus on üle kella 00.00 (kaart sisestati eelmisel päeval) või üle kella 24.00 (kaart võeti välja järgmisel päeval), esitatakse mõlema päeva täielikud andmed.
VuActivityDailyRecordArray	Pesade olek allalaaditud andmetele vastaval päeval kell 00.00 ja selle päeva kohta registreeritud tegevusmuutused.
VuPlaceDailyWorkPeriodRecordArray	Allalaaditud andmetele vastaval päeval registreeritud kohtadega seotud andmed. Kui see osa on tühi, saadetakse maatriksi päis kirjega noOfRecords = 0.
VuGNSSCDRecordArray	Sõiduki asukoht GNSSi järgi igal korral, kui juhil täitub kolm järjestikust sõidutundi. Kui see osa on tühi, saadetakse maatriksi päis kirjega noOfRecords = 0.
VuSpecificConditionRecordArray	Allalaaditud andmetele vastaval päeval registreeritud eritingimuste andmed. Kui see osa on tühi, saadetakse maatriksi päis kirjega noOfRecords = 0.
SignatureRecordArray	Kõigi eespool nimetatud andmete ECC allkiri.

2.2.6.3. Sündmuste ja vigade andmete ülekandmisega nõustumist kinnitav vastus

DDP_031 Sündmuste ja vigade andmete ülekandmisega nõustumist kinnitava vastussõnumi andmeväli sisaldab järgmisi andmeid järgmises järjestuses, kus teenuseidentifikaator (SID) on 76h ja vastuse edastusparameeter (TREP) on 03h ning rakendatakse kohast jagamist allsõnumiteks ja nende loendamist.

1. põlvkonna andmestruktuur

Andmeelement	Selgitus
VuFaultData	Kõik sõidukiseadmesse salvestatud või seal kestvad vead. Kui see osa on tühi, saadetakse ainult noOfVuFaults = 0.
VuEventData	Kõik sõidukiseadmesse salvestatud või seal kestvad sündmused (välja arvatud kiiruse ületamine). Kui see osa on tühi, saadetakse ainult noOfVuEvents = 0.
VuOverSpeedingControlData	Viimase kiiruse ületamise kontrolliga seotud andmed (andmete puudumisel vaikeväärtus).
VuOverSpeedingEventData	Kõik sõidukiseadmesse salvestatud kiiruse ületamise sündmused. Kui see osa on tühi, saadetakse ainult noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Kõik sõidukiseadmesse salvestatud aja korrigeerimise sündmused (mis ei toimunud täieliku kalibreerimise ajal). Kui see osa on tühi, saadetakse ainult noOfVuTimeAdjRecords = 0.
Signature	Kõigi andmete RSA allkiri, mis hõlmab kõiki kirjeid alates kirjest noOfVuFaults kuni viimase aja korrigeerimise kirje viimase baidini.

2. põlvkonna andmestruktuur

Andmeelement	Selgitus
VuFaultRecordArray	Kõik sõidukiseadmesse salvestatud või seal kestvad vead. Kui see osa on tühi, saadetakse maatriksi päis kirjega noOfRecords = 0.
VuEventRecordArray	Kõik sõidukiseadmesse salvestatud või seal kestvad sündmused (välja arvatud kiiruse ületamine). Kui see osa on tühi, saadetakse maatriksi päis kirjega noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Viimase kiiruse ületamise kontrolliga seotud andmed (andmete puudumisel vaikeväärtus).
VuOverSpeedingEventRecordArray	Kõik sõidukiseadmesse salvestatud kiiruse ületamise sündmused. Kui see osa on tühi, saadetakse maatriksi päis kirjega noOfRecords = 0.
VuTimeAdjustmentRecordArray	Kõik sõidukiseadmesse salvestatud aja korrigeerimise sündmused (mis ei toimunud täieliku kalibreerimise ajal). Kui see osa on tühi, saadetakse maatriksi päis kirjega noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Kõigi eespool nimetatud andmete ECC allkiri.

2.2.6.4. Üksikasjalike kiiruseandmete ülekandmisega nõustumist kinnitav vastus

DDP_032 Üksikasjalike kiiruseandmete ülekandmisega nõustumist kinnitava vastussõnumi andmeväli sisaldab järgmisi andmeid järgmises järjestuses, kus teenuseidentifikaator (SID) on 76h ja vastuse edastusparameeter (TREP) on 04h ning rakendatakse kohast jagamist allsõnumiteks ja nende loendamist.

1. põlvkonna andmestruktuur

Andmeelement	Selgitus
VuDetailedSpeedData	Kõik sõidukiseadmesse salvestatud üksikasjalikud andmed kiiruse kohta (üks kiiruseplokk iga minuti kohta, mil sõiduk on liikunud). 60 kiiruseväärtust minuti kohta (üks sekundis).
Signature	Kõigi andmete RSA allkiri, mis hõlmab kõiki kirjeid alates kirjest noOfSpeedBlocks kuni viimase kiiruseploki viimase baidini.

2. põlvkonna andmestruktuur

Andmeelement	Selgitus
VuDetailedSpeedBlockRecordArray	Kõik sõidukiseadmesse salvestatud üksikasjalikud andmed kiiruse kohta (üks kiiruseplokk iga minuti kohta, mil sõiduk on liikunud). 60 kiiruseväärtust minuti kohta (üks sekundis).
SignatureRecordArray	Kõigi eespool nimetatud andmete ECC allkiri.

2.2.6.5. Tehniliste andmete ülekandmisega nõustumist kinnitav vastus

DDP_033 Tehniliste andmete ülekandmisega nõustumist kinnitava vastussõnumi andmeväli sisaldab järgmisi andmeid järgmises järjestuses, kus teenuseidentifikaator (SID) on 76h ja vastuse edastusparameeter (TREP) on 05h ning rakendatakse kohast jagamist allsõnumiteks ja nende loendamist.

1. põlvkonna andmestruktuur

Andmeelement	Selgitus
VuIdentification	
SensorPaired	
VuCalibrationData	Kõik sõidukiseadmesse salvestatud kalibreerimiskirjed.
Signature	Kõigi andmete RSA allkiri, mis hõlmab kõiki kirjeid alates kirjest vuManufacturerName kuni viimase VuCalibrationRecord-kirje viimase baidini.

2. põlvkonna andmestruktuur

Andmeelement	Selgitus
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Kõik sõidukiseadmesse salvestatud liikmesriikide paariühendamised.
VuSensorExternalGNSSCoupledRecordArray	Kõik sõidukiseadmesse salvestatud välise GNSS-seadme ühendamise andmed.
VuCalibrationRecordArray	Kõik sõidukiseadmesse salvestatud kalibreerimiskirjed.
VuCardRecordArray	Kõik sõidukiseadmesse salvestatud andmed kaardi sisestamise kohta.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Kõigi eespool nimetatud andmete ECC allkiri.

2.3. **Välisandmekandja faili salvestamine**

DDP_034 Kui allalaadimisseanss sisaldas sõidukiseadme andmete edastamist, salvestab eriotstarbeline seade kõik sõidukiseadmest alla laadimisseansi käigus saadud andmed, mis sisaldusid andmete ülekandmisega nõustumist kinnitavates vastussõnumites, ühte füüsilisse faili. Salvestavate andmete hulgast jäetakse välja sõnumipäised, allsõnumite loendurid, tühjad allsõnumid ja kontrollsummad, kuid salvestatakse SID ja TREP (mitme allsõnumi korral ainult esimese allsõnumi omad).

3. SÕIDUMEERIKUKAARDILT ALLA LAADIMISE PROTOKOLL

3.1. **Reguleerimisala**

Käesolevas peatükis kirjeldatakse sõidumeerikukaardi andmete otsest allalaadimist eriotstarbelisse seadmesse. Eriotstarbeline seade ei ole turbekeskkonna osa ning seetõttu ei toimu kaardi ja eriotstarbelise seadme vahel autentimist.

3.2. **Mõisted**

Allalaadimisseanss – igasugune kiipkaardiandmete allalaadimine. Seanss hõlmab kogu protseduuri alates liideseseadme tehtavast kiipkaardi nullimisest kuni kiipkaardi deaktiveerimiseni (kaardi väljavõtmine või uus lähtestus).

Allkirjastatud andmefail – kiipkaardilt saadav fail. Fail edastatakse liideseseadmesse lihttekstina. Kiipkaardil antakse failile räsiväärtus ja allkiri ning allkiri edastatakse liideseseadmesse.

3.3. **Kaardilt alla laadimine**

DDP_035 Sõidumeerikukaardilt alla laadimine hõlmab järgmisi etappe:

— kaardi elementaarfailides (ICC ja IC) oleva üldteabe allalaadimine. See on vabatahtlik teave ning seda ei turvata digitaalallkirjaga;

— elementaarfailide Card_Certificate (või CardSignCertificate) ja CA_Certificate allalaadimine. See teave ei ole turvatud digitaalallkirjaga.

Nende failide allalaadimine on iga allalaadimisseansi puhul kohustuslik;

— muude rakendusandmeid sisaldavate elementaarfailide (mis asuvad failis Tachograph DF ja Tachograph_G2 DF, kui see on olemas) allalaadimine, välja arvatud elementaarfail Card_Download. See teave on turvatud digitaalallkirjaga;

— iga allalaadimisseansi ajal on kohustuslik alla laadida vähemalt elementaarfailid Application_Identification ja ID;

— juhikaardilt alla laadimisel on kohustuslik alla laadida ka järgmised elementaarfailid:

- `Events_Data`,
- `Faults_Data`,
- `Driver_Activity_Data`,
- `Vehicles_Used`,
- `Places`,
- `GNSS_Places` (kui kasutatakse),
- `Control_Activity_Data`,
- `Specific_Conditions`;

— juhikaardilt alla laadimisel ajakohastatakse elementaarfailis `Card_Download` kuupäev `LastCardDownload`;

— töökojakaardilt alla laadimisel lähtestatakse elementaarfailis `Card_Download` kalibreerimisloendur;

— töökojakaardilt alla laadimisel ei laadita alla elementaarfaili `Sensor_Installation_Data`.

3.3.1. *Initsialiseerimisjada*

DDP_036 Eriotstarbeline seade initsialiseerib jada järgmiselt:

Kaart	Suund	IDE/IFD	Tähendus/märkused
	⇦	Riistvara lähtestus	
ATR	⇨		

Soovi korral võib suuremale boodikiirusele üleminekuks kasutada käsku PPS, kui kiipkaart seda toetab.

3.3.2. *Allkirjastamata andmefaili allalaadimise jada*

DDP_037 Elementaarfailide ICC, IC, Card_Certificate (või CardSignCertificate) ja CA_Certificate allalaadimisjada on järgmine:

Kaart	Suund	IDE/IFD	Tähendus/märkused
	⇦	**Select File**	Faili valimine failiidentifikaatorite alusel
OK	⇨		
	⇦	**Read Binary**	Kui fail sisaldab rohkem andmeid, kui mahub kaardilugeja või kaardi puhvrisse, tuleb käsku korrata kuni kogu faili lugemiseni.
File Data **OK**	⇨	Andmed salvestatakse välisandmekandjale	Vastavalt punktile **3.4** „Andmete salvestusvorming“

Märkus 1. Enne elementaarfaili Card_Certificate (või CardSignCertificate) valimist peab olema valitud sõidumeerikurakendus (valitakse rakenduse identifikaatori kaudu).

Märkus 2. Faili valimine ja lugemine võib toimuda ka ühes etapis, kui kasutatakse käsku „Read Binary“ koos elementaarfaili lühikese identifikaatoriga.

3.3.3. *Allkirjastatud andmefaili allalaadimise 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 räsialgoritmi vastavalt 11. liitele. See ei ole ISO standardile vastav käsk.
Faili räsiväärtuse arvutamine ja selle ajutine salvestamine			
OK	⇨		
	⇦	**Read Binary**	Kui fail sisaldab rohkem andmeid, kui mahub kaardilugeja või kaardi puhvrisse, tuleb käsku korrata kuni kogu faili lugemiseni.
File Data OK	⇨	Andmed salvestatakse välisandmekandjale	Vastavalt punktile **3.4** „Andmete salvestusvorming“
	⇦	**PSO: Compute Digital Signature**	
Tehakse turbetoiming „Compute Digital Signature“, kasutades ajutiselt salvestatud räsiväärtust			
Signature OK	⇨	Andmed lisatakse varem välisandmekandjale salvestatud andmetele	Vastavalt punktile **3.4** „Andmete salvestusvorming“

Märkus. Faili valimine ja lugemine võib toimuda ka ühes etapis, kui kasutatakse käsku „Read Binary“ koos elementaarfaili lühikese identifikaatoriga. Sellisel juhul võib elementaarfaili valimine ja lugemine toimuda enne käsu „Perform Hash of File“ andmist.

3.3.4. *Kalibreerimisloenduri lähtestamise jada*

DDP_039 Töökojakaardi elementaarfailis `Card_Download` asuva loenduri `NoOfCalibrationsSinceDownload` lähtestamiseks kasutatav jada on järgmine:

Kaart	Suund	IDE/IFD	Tähendus/märkused
	⇦	**Select File** EF Card_Download	Faili valimine failiidentifikaatorite alusel
OK	⇨		

Kaart	Suund	IDE/IFD	Tähendus/märkused
	⇦	**Update Binary** NoOfCalibrationsSince-Download = '00 00'	
Lähtestab kaardi allalaa-dimisnumbri			
OK	⇨		

Märkus. Faili valimine ja ajakohastamine võib toimuda ka ühes etapis, kui kasutatakse käsku „Read Binary" koos elementaarfaili lühikese identifikaatoriga.

3.4. Andmete salvestusvorming

3.4.1. *Sissejuhatus*

DDP_040 Allalaaditud andmed tuleb salvestada vastavalt järgmistele tingimustele:

— andmed salvestatakse transparentsena. See tähendab, et kaardilt edastatav baitide järjestus ning bittide järjestus baidis peavad salvestamisel säilima;

— kõik ühe allalaadimisseansi ajal kaardilt alla laaditud failid salvestatakse välisandmekandjal ühte faili.

3.4.2. *Failivorming*

DDP_041 Failivorming on mitmete TLV-objektide konkatenatsioon.

DDP_042 Elementaarfaili silt on faili 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. Pikkuse väljal olev väärtus „FF FF" on reserveeritud tulevikus kasutamiseks.

DDP_045 Kui faili ei laadita alla, ei salvestata seoses failiga mitte midagi (ei silti ega nullpikkust).

DDP_046 Allkiri salvestatakse vahetult järgmise TLV-objektina pärast faili andmeid sisaldavat TLV-objekti.

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

Välisandmekandjale salvestatud allalaadimisfaili andmete näidis:

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 andmed `Vehicles_Used`
`05 05 01`	`00 80`	Elementaarfaili allkiri `Vehicles_Used`

4. SÕIDUMEERIKUKAARDILT ALLA LAADIMINE SÕIDUKISEADME KAUDU

DDP_047 Sõidukiseade peab võimaldama alla laadida ühendatud liideseseadmesse sisestatud juhikaardi sisu.

DDP_048 Selle režiimi käivitamiseks saadab liideseseade sõidukiseadmele kaardi andmete allalaadimise nõude (vt punkt 2.2.2.9).

DDP_049 Seejärel laadib sõidukiseade kogu kaardi failide kaupa alla vastavalt 3. osas määratletud kaardi allalaadimisprotokollile ning edastab kaardilt saadud andmed eriotstarbelisse seadmesse, kasutades sobivat TLV-failivormingut (vt punkt 3.4.2), mis paigutatakse andmete ülekandmisega nõustumist kinnitavasse vastussõnumisse.

DDP_050 Eriotstarbeline seade võtab kaardi andmed ülekandmisega nõustumist kinnitavast vastussõnumist välja (eemaldades kõik päised, SIDid, TREPid, allsõnumite loendurid ja kontrollsummad) ning salvestab need ühte füüsilisse faili, nagu on kirjeldatud punktis 2.3.

DDP_051 Seejärel ajakohastab sõidukiseade vastavalt vajadusele juhikaardil faili `Control_Activity_Data` või `Card_Download`.

8. liide

KALIBREERIMISPROTOKOLL

SISUKORD

1. SISSEJUHATUS

Käesolevas liites kirjeldatakse, kuidas toimub andmevahetus sõidukiseadme ja testimisseadme vahel K-liini kaudu, mis moodustab 6. liites kirjeldatud kalibreerimisliidese osa. Selles kirjeldatakse ka sisend-/väljundsignaaliliini kontrollimist kalibreerimispistmikul.

K-liiniga side loomist kirjeldatakse 4. peatükis „Sideteenused".

Käesolevas liites kasutatakse K-liini eri tingimustel kontrollimise ulatuse määratlemiseks mõistet „diagnostilised seansid". Vaikeseanss on „StandardDiagnosticSession", mille käigus saab sõidukiseadmest lugeda kõiki andmeid, kuid sinna ei saa andmeid kirjutada.

Diagnostilise seansi valikut on kirjeldatud 5. peatükis „Haldusteenused".

Käesolevat liidet tuleb pidada kehtivaks sõidukiseadmete ja töökojakaartide mõlema põlvkonna suhtes vastavalt käesolevas määruses koostalitlusvõime kohta esitatud nõuetele.

CPR_001 „ECUProgrammingSession" võimaldab andmeid sõidukiseadmesse sisestada. Kalibreerimisandmete sisestamiseks peab sõidukiseade lisaks olema kalibreerimisrežiimis.

K-liini kaudu andmete edastamist on kirjeldatud 6. peatükis „Andmeedastusteenused". Andmeedastusvorminguid on üksikasjalikult kirjeldatud 8. peatükis „Andmekirjete vormingud".

CPR_002 „ECUAdjustmentSession" võimaldab valida K-liini liidese kaudu kalibreerimise sisend-/väljundsignaaliliini sisend-/väljundrežiimi. Kalibreerimise sisend-/väljundsignaaliliini juhtimist on kirjeldatud 7. peatükis „Testimpulsside juhtimine – sisend-/väljundsignaali juhtimise funktsionaalne üksus".

CPR_003 Käesolevas dokumendis on testimisseadme aadressiks märgitud 'tt'. Ehkki testimisseadmel võib olla eelistatud aadresse, peab sõidukiseade vastama korrektselt mis tahes testimisseadme aadressile. Sõidukiseadme füüsiline aadress on 0xEE.

2. MÕISTED, MÄÄRATLUSED JA VIITED

Protokollid, sõnumid ja veakoodid põhinevad peamiselt standardi ISO 14229-1 ühel versioonil (*Road vehicles – Diagnostic systems – Part 1: Diagnostic services* („Maanteesõidukid. Diagnostikasüsteemid. Osa 1: Diagnostikateenused"), versioon 6, 22. veebruar 2001).

Teenuse identifikaatorite, teenusenõuete ja -vastuste ning standardparameetrite jaoks kasutatakse baitkodeerimist ja kuueteistkümnendväärtusi.

„Testimisseade" on seade, mida kasutatakse programmeerimis-/kalibreerimisandmete sisestamiseks sõidukiseadmesse.

„Klient" ja „server" tähendavad vastavalt testimisseadet ja sõidukiseadet.

„ECU" tähendab elektroonilist juhtseadet ja selle all peetakse silmas sõidukiseadet.

Viited

ISO 14230-2

Road Vehicles – Diagnostic Systems – Keyword Protocol 2000 – Part 2: Data Link Layer („Maanteesõidukid. Diagnostikasüsteemid. Võtmesõnaprotokoll 2000. Osa 2: Andmelülikiht"). Esimene väljaanne, 1999.

3. TEENUSTE ÜLEVAADE

3.1. **Võimalikud teenused**

Järgmises tabelis esitatakse ülevaade teenustest, mis on sõidumeerikus kasutatavad ja on määratletud käesolevas dokumendis.

CPR_004 Tabelis on teenused, mida on võimalik kasutada käivitatud diagnostilise seansi ajal.

— **Esimeses veerus** on võimalikud teenused.

— **Teises veerus** on käesoleva liite selle punkti number, kus see teenus on täpsemalt määratletud.

— **Kolmandas veerus** määratakse nõudesõnumite teenuseidentifikaatori (SID) väärtused.

— **Neljandas veerus** määratletakse seansi **„StandardDiagnosticSession" (SD)** teenused, mis peavad olema kasutatavad igas sõidukiseadmes.

— **Viiendas veerus** määratletakse seansi **„ECUAdjustmentSession" (ECUAS)** teenused, mis peavad olema kasutatavad, et oleks võimalik juhtida sõidukiseadme esipaneelil asuva kalibreerimispistmiku sisend-/väljundsignaaliliini.

— **Kuuendas veerus** määratletakse seansi **„ECUProgrammingSession" (ECUPS)** teenused, mis peavad olema kasutatavad, et sõidukiseadmes oleks võimalik programmeerida parameetreid.

Tabel 1

Ülevaade teenuse identifikaatori väärtustest

			Diagnostiline seanss		
Diagnostilise teenuse nimetus	Punkt	Nõude SID väärtus	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. Kasutatavad teenused on esitatud järgmises tabelis.

Tabel 2

Sideteenused

Teenuse nimetus	Kirjeldus
StartCommunication	Klient nõuab sideseansi alustamist serveri(te)ga.
StopCommunication	Klient nõuab käimasoleva sideseansi lõpetamist.
TesterPresent	Klient annab serverile teada, et ta on veel aktiivne.

CPR_005 Teenust StartCommunication kasutatakse side alustamiseks. Mis tahes teenuse kasutamiseks tuleb algatada side ja sideparameetrid peavad olema soovitud režiimi jaoks sobivad.

4.1. **Teenus StartCommunication**

CPR_006 Indikatsiooniprimitiivi StartCommunication saamise korral kontrollib sõidukiseade, kas nõutud sidelüli saab olemasolevatel tingimustel luua. Sidelüli loomiseks kehtivaid tingimusi on kirjeldatud dokumendis ISO 14230-2.

CPR_007 Seejärel teeb sõidukiseade kõik toimingud, mis on vajalikud sidelüli loomiseks, ja saadab vastuseprimitiivi StartCommunication, milles on valitud kinnitava vastuse parameetrid.

CPR_008 Kui sõidukiseade, mis on juba initsialiseeritud (ja on alustanud diagnostilist seanssi), saab uue nõude StartCommunication (nt testimisseadme veast taastumise tõttu), see nõue aktsepteeritakse ja sõidukiseade initsialiseeritakse uuesti.

CPR_009 Kui mis tahes põhjusel ei saa sidelüli luua, jätkab sõidukiseade sama tööd, mida see tegi vahetult enne katset luua sidelüli.

CPR_010 Nõudesõnum StartCommunication peab olema füüsiliselt adresseeritud.

CPR_011 Sõidukiseadme initsialiseerimine teenuste kasutamiseks toimub „kiirinitsialiseerimise“ meetodil:

— mis tahes tegevusele eelneb siini jõudeaeg;

— seejärel saadab testimisseade initsialiseerimisjada;

— kogu vajalik teave sidelüli loomiseks sisaldub sõidukiseadme vastuses.

CPR_012 Pärast initsialiseerimise lõpetamist

— reguleeritakse kõik sideparameetrid tabelis 4 määratletud väärtustele vastavalt võtmebaitidele;

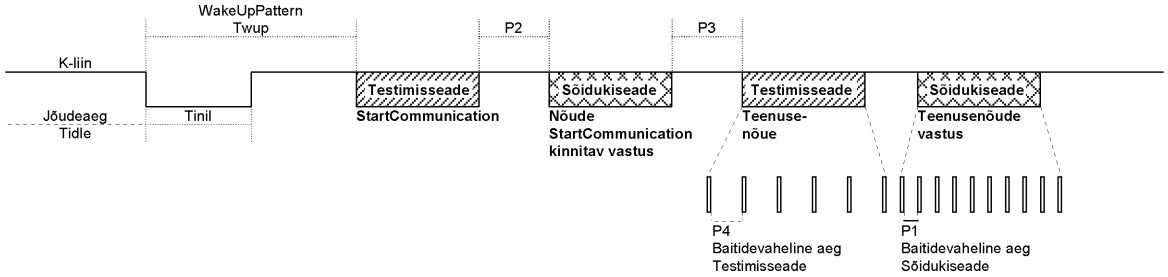
— sõidukiseade ootab testimisseadme esimest nõuet;

— sõidukiseade on diagnoosimise vaikerežiimis, milleks on StandardDiagnosticSession;

— kalibreerimise sisend-/väljundsignaaliliin on vaikeolekus, s.o välja lülitatud.

CPR_014 K-liini andmeedastuskiirus on 10 400 boodi.

CPR_016 Kiirinitsialiseerimine algab sellega, et testimisseade edastab K-liinil WakeUp-jada (Wup). Jada algab Tinil-ajaga madalal väärtusel pärast K-liini jõudeaega. Testimisseade edastab teenuse StartCommunication esimese biti pärast seda, kui signaali esimesest laskuvast servast on kulunud aeg Twup.



CPR_017 Kiirinitsialiseerimise ja üldise edastamise ajastusväärtused on esitatud allpool olevates tabelites. Jõudeaja puhul on erinevad võimalused:

— esimene edastus pärast sisselülitamist: Tidle = 300 ms;

— pärast teenuse StopCommunication lõpetamist: Tidle = P3 min;

— pärast edastamise lõpetamist P3 maksimaalväärtusele vastava ooteaja möödumisel: Tidle = 0.

Tabel 3

Kiirinitsialiseerimise ajastusväärtused

Parameeter		Minimaalväärtus	Maksimaalväärtus
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabel 4

Edastuse ajastusväärtused

Ajastusparameeter	Parameetri kirjeldus	Väikseim lubatud väärtus [ms]	Suurim lubatud väärtus [ms]
		Minimaalne	Maksimaalne
P1	Sõidukiseadme vastuse baitidevaheline aeg	0	20
P2	Testimisseadme nõude ja sõidukiseadme vastuse või sõidukiseadme kahe vastuse vaheline aeg	25	250
P3	Sõidukiseadme vastuste ja testimisseadme uue nõude vaheline aeg	55	5 000
P4	Testimisseadme nõude baitidevaheline aeg	5	20

CPR_018 Kiirinitsialiseerimise sõnumivorming on esitatud järgmistes tabelites. (MÄRKUS: Hex tähistab kuueteist-kümnendväärtusi.)

Tabel 5

Nõudesõnum StartCommunication

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	81	FMT
#2	Sihtaadressibait	EE	TGT
#3	Lähteaadressibait	tt	SRC
#4	**Nõude StartCommunication teenuseidentifikaator**	**81**	**SCR**
#5	Kontrollsumma	00-FF	CS

Tabel 6

Nõudega StartCommunication nõustumist kinnitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	**Nõude StartCommunication kinnitava vastuse teenuseidentifikaator**	**C1**	**SCRPR**
#6	1. võtmebait	EA	KB1
#7	2. võtmebait	8F	KB2
#8	Kontrollsumma	00-FF	CS

CPR_019 Nõudesõnumile StartCommunication ei saa anda eitavat vastust; kui ei ole võimalik kinnitavat vastust saata, siis sõidukiseadet ei initsialiseerita, midagi ei edastata ja seade jääb tavalisse töörežiimi.

4.2. **Teenus StopCommunication**

4.2.1. *Sõnumi kirjeldus*

Selle sidekihi teenuse eesmärk on lõpetada sideseanss.

CPR_020 Indikatsiooniprimitiivi StopCommunication saamise korral kontrollib sõidukiseade, kas hetketingimused võimaldavad sidet lõpetada. Sellisel juhul teeb sõidukiseade kõik toimingud, mis on vajalikud side lõpetamiseks.

CPR_021 Kui sidet on võimalik lõpetada, saadab sõidukiseade enne side lõpetamist vastuseprimitiivi StopCommunication, milles on valitud kinnitava vastuse parameetrid.

CPR_022 Kui side lõpetamine ei ole mingil põhjusel võimalik, saadab sõidukiseade vastuseprimitiivi StopCommunication, milles on valitud eitava vastuse parameeter.

CPR_023 Kui sõidukiseade tuvastab aja P3max lõppemise, lõpetatakse side ilma vastuseprimitiivi saatmata.

4.2.2. *Sõnumivorming*

CPR_024 Primitiivide StopCommunication sõnumivormingud on esitatud järgmistes tabelites.

Tabel 7

Nõudesõnum StopCommunication

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Lähteaadressibait	tt	SRC
#4	Lisapikkusebait	01	LEN
#5	**Nõude StopCommunication teenuseidentifikaator**	**82**	**SPR**
#6	Kontrollsumma	00-FF	CS

Tabel 8

Nõudega StopCommunication nõustumist kinnitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	01	LEN
#5	**Nõude StopCommunication kinnitava vastuse teenuseidentifikaator**	**C2**	**SPRPR**
#6	Kontrollsumma	00-FF	CS

Tabel 9

Nõudele StopCommunication saadetav eitav vastusesõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	**Eitava 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*

Teenus ei nõua ühegi parameetri määratlemist.

4.3. **Teenus TesterPresent**

4.3.1. *Sõnumi kirjeldus*

Testimisseade kasutab teenust TesterPresent näitamaks serverile, et ta on veel aktiivne ning et server ei läheks automaatselt tagasi tavalisse töörežiimi ega lõpetaks sidet. See perioodiliselt saadetav teenus hoiab diagnostilise seansi / side aktiivsena, lähtestades P3 taimeri iga kord, kui see teenusenõue saadakse.

4.3.2. *Sõnumivorming*

CPR_079 Primitiivide TesterPresent sõnumivormingud on esitatud järgmistes tabelites.

Tabel 10

Nõudesõnum TesterPresent

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Lähteaadressibait	tt	SRC
#4	Lisapikkusebait	02	LEN
#5	**Nõude TesterPresent teenuseidentifikaator**	**3E**	**TP**

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#6	Sub Function = responseRequired = [yes	01	RESPREQ_Y
	no]	02	RESPREQ_NO
#7	Kontrollsumma	00-FF	CS

CPR_080 Kui parameetrile responseRequired on seadistatud jaatav väärtus, vastab server järgmise kinnitava vastussõnumiga. Kui seadistus on eitav, siis server vastust ei saada.

Tabel 11

Nõudega TesterPresent nõustumist kinnitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	01	LEN
#5	**Nõude TesterPresent kinnitava vastuse teenuseidentifikaator**	**7E**	**TPPR**
#6	Kontrollsumma	00-FF	CS

CPR_081 Teenus toetab järgmisi eitavate vastuste koode:

Tabel 12

Nõudele TesterPresent saadetav eitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	**Eitava vastuse teenuseidentifikaator**	**7F**	**NR**
#6	Nõude TesterPresent teenuseidentifikaator	3E	TP

Baidi nr	Parameetri nimetus		Hex-väärtus	Mnemooniline nimi
#7	responseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Kontrollsumma		00-FF	CS

5. HALDUSTEENUSED

Kasutatavad teenused on esitatud järgmises tabelis.

Tabel 13

Haldusteenused

Teenuse nimetus	Kirjeldus
StartDiagnosticSession	Klient nõuab sõidukiseadmega diagnostilise seansi alustamist.
SecurityAccess	Klient nõuab juurdepääsu 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 peavad vastama järgmistele nõuetele:

— sõidukiseadmes on alati aktiivne täpselt üks diagnostiline seanss;

— sõidukiseade käivitab toite sisselülitamisel alati seansi StandardDiagnosticSession. Kui ühtki muud diagnostilist seanssi ei käivitata, töötab StandardDiagnosticSession, kuni sõidukiseade on toitega ühendatud;

— kui testimisseade nõuab diagnostilist seanssi, mis on juba käivitatud, saadab sõidukiseades kinnitava vastussõnumi;

— alati kui testimisseade nõuab uut diagnostilist seanssi, saadab sõidukiseade enne uue seansi aktiveerumist sõidukiseadmes kinnitava vastussõnumi StartDiagnosticSession. Kui sõidukiseade ei saa uut nõutud diagnostilist seanssi käivitada, vastab see eitava vastussõnumiga StartDiagnosticSession ning senine seanss jätkub.

CPR_026 Diagnostiline seanss käivitatakse ainult siis, kui on loodud side kliendi ja sõidukiseadme vahel.

CPR_027 Tabelis 4 määratletud ajastusparameetrid aktiveeritakse pärast edukat käsku StartDiagnosticSession, mille diagnosticSession-i parameetriks on nõudesõnumis valitud StandardDiagnosticSession, kui enne oli aktiivne mõni muu diagnostiline seanss.

5.1.2. *Sõnumivorming*

CPR_028 Primitiivide StartDiagnosticSession sõnumivormingud on esitatud järgmistes tabelites.

Tabel 14

Nõudesõnum StartDiagnosticSession

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Lähteaadressibait	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

Nõudega StartDiagnosticSession nõustumist kinnitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	02	LEN
#5	**Nõude StartDiagnosticSession kinnitava vastuse teenuseidentifikaator**	**50**	**STDSPR**
#6	diagnosticSession = [sama väärtus kui tabeli 14 baidis nr 6]	xx	DS_…
#7	Kontrollsumma	00-FF	CS

Tabel 16

Nõudele StartDiagnosticSession saadetav eitav vastusesõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	**Eitava 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 tingimused 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

Seansi diagnosticSession väärtuste määratlus

Hex	Kirjeldus	Mnemooniline nimi
81	**StandardDiagnosticSession** See diagnostiline seanss võimaldab kõiki teenuseid, mis on määratletud tabeli 1 neljandas veerus „SD“. Need teenused võimaldavad lugeda andmeid serverist (sõidukiseadmest). See diagnostiline seanss on aktiveeritud pärast side loomise edukat lõpetamist kliendi (testimisseade) ja serveri (sõidukiseade) vahel. Käesolevas punktis määratletud muude diagnostiliste seansside käigus võib selle diagnostilise seansi andmed üle kirjutada.	**SD**
85	**ECUProgrammingSession** See diagnostiline seanss võimaldab kõiki teenuseid, mis on määratletud tabeli 1 kuuendas veerus „ECUPS“. Need teenused toetavad serveri (sõidukiseadme) mälu programmeerimist. Käesolevas punktis määratletud muude diagnostiliste seansside käigus võib selle diagnostilise seansi andmed üle kirjutada.	**ECUPS**
87	**ECUAdjustmentSession** See diagnostiline seanss võimaldab kõiki teenuseid, mis on määratletud tabeli 1 viiendas veerus „ECUAS“. Need teenused toetavad serveri (sõidukiseadme) sisend-/väljundsignaali juhtimist. Käesolevas punktis määratletud muude diagnostiliste seansside käigus võib selle diagnostilise seansi andmed üle kirjutada.	**ECUAS**

5.2. **Teenus SecurityAccess**

Kalibreerimisandmete kirjutamine on võimalik ainult siis, kui sõidukiseade on režiimis CALIBRATION. Enne režiimi CALIBRATION kasutamise lubamist tuleb lisaks kehtiva töökojakaardi sisestamisele sisestada sõidukiseadmesse ka õige PIN-kood.

Kui sõidukiseade on režiimis CALIBRATION või CONTROL, on võimalik kasutada ka kalibreerimise sisend-/väljundliini.

Teenuse SecurityAccess abil saab sisestada PIN-koodi ja näidata testimisseadmele, kas sõidukiseade on režiimis CALIBRATION või mitte.

PIN-koodi sisestamine alternatiivsete meetodite abil on lubatud.

5.2.1. *Sõnumi kirjeldus*

Teenus SecurityAccess koosneb teenusesõnumist requestSeed, millele järgneb võimalik teenusesõnum sendKey. Teenus SecurityAccess tuleb käivitada pärast teenust StartDiagnosticSession.

CPR_033 Testimisseade kasutab teenuse SecurityAccess sõnumit „requestSeed“, et kontrollida, kas sõidukiseade on valmis PIN-koodi vastu võtma.

CPR_034 Kui sõidukiseade on juba režiimis CALIBRATION, saadab see nõudele vastamiseks „seemnejada“ 0x0000, kasutades teenuse SecurityAccess kinnitavat vastust.

CPR_035 Kui sõidukiseade on valmis töökojakaardi abil PIN-koodi kontrollimiseks, saadab see nõudele vastamiseks „seemnejada“, mis on suurem kui 0x0000, kasutades teenuse SecurityAccess kinnitavat vastust.

CPR_036 Kui sõidukiseade ei ole valmis testimisseadmelt PIN-koodi vastuvõtmiseks, sest sisestatud töökojakaart ei ole kehtiv, töökojakaarti ei ole sisestatud või sõidukiseade ootab PIN-koodi sisestamist muu meetodi abil, vastab see nõudele eitava vastusega, mille vastusekoodis on valitud conditionsNotCorrectOrRequestSequenceError.

CPR_037 Seejärel kasutab testimisseade valikulist teenuse SecurityAccess sõnumit „sendKey“, et saata PIN-kood sõidukiseadmesse. Et jätta aega kaardi autentimisprotsessi jaoks, kasutab sõidukiseade eitava vastuse koodi requestCorrectlyReceived-ResponsePending, et pikendada vastamiseks kuluvat aega. Vastamiseks kuluv maksimaalne aeg ei või siiski ületada viit minutit. Kohe pärast nõutud teenuse lõpetamist saadab sõidukiseade kinnitava vastussõnumi või eitava vastussõnumi, mille vastusekood on sellest erinev. Sõidukiseade võib eitavat vastusekoodi requestCorrectlyReceived-ResponsePending korrata kuni nõutud teenuse lõpetamiseni ja lõpliku vastussõnumi saatmiseni.

CPR_038 Sõidukiseade vastab sellele nõudele teenuse SecurityAccess kinnitava vastusega ainult juhul kui seade on režiimis CALIBRATION.

CPR_039 Järgmistel juhtudel saadab sõidukiseade sellele nõudele eitava vastuse, mille vastusekoodis on valitud:

— subFunctionNot supported: allfunktsiooni parameetri (accessType) kehtetu vorming,

— conditionsNotCorrectOrRequestSequenceError: sõidukiseade ei ole valmis sisestatud PIN-koodi vastu võtma,

— invalidKey: PIN-kood ei ole kehtiv, kuid PIN-koodi lubatud sisestuste arv ei ole ületatud,

— exceededNumberOfAttempts: PIN-kood ei ole kehtiv ja PIN-koodi lubatud sisestuste arv on ületatud,

— generalReject: PIN-kood on õige, kuid vastastikune autentimine töökojakaardiga ebaõnnestus.

5.2.2. *Sõnumivorming – SecurityAccess – requestSeed*

CPR_040 Teenuse SecurityAccess primitiivide „requestSeed“ sõnumivormingud on esitatud järgmistes tabelites.

Tabel 18

Teenuse SecurityAccess nõudesõnum requestSeed

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Lähteaadressibait	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

Teenuse SecurityAccess nõudega requestSeed nõustumist kinnitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	04	LEN
#5	**Nõude SecurityAccess kinnitava 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 saadetav eitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#4	Lisapikkusebait	03	LEN
#5	**Eitava vastuse teenuseidentifikaator**	**7F**	**NR**
#6	Nõude SecurityAccess teenuseidentifikaator	27	SA
#7	ResponseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Kontrollsumma	00-FF	CS

5.2.3. *Sõnumivorming – SecurityAccess – sendKey*

CPR_041 Teenuse SecurityAccess primitiivide „sendKey“ sõnumivormingud on esitatud järgmistes tabelites.

Tabel 21

Teenuse SecurityAccess nõudesõnum sendKey

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Lähteaadressibait	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) … Võti nr „m“ (kõige vähem tähtis bait, m peab olema vähemalt 4 ja kuni 8)	xx … xx	KEY
#m+7	Kontrollsumma	00-FF	CS

Tabel 22

Teenuse SecurityAccess nõudega sendKey nõustumist kinnitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#4	Lisapikkusebait	02	LEN
#5	**Nõude SecurityAccess kinnitava vastuse teenuseidentifikaator**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Kontrollsumma	00-FF	CS

Tabel 23

Nõudele SecurityAccess saadetav eitav vastussõnum

Baidi nr	Parameetri nimetus		Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine		80	FMT
#2	Sihtaadressibait		tt	TGT
#3	Lähteaadressibait		EE	SRC
#4	Lisapikkusebait		03	LEN
#5	**Eitava 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 nimetus	Kirjeldus
ReadDataByIdentifier	Klient nõuab identifikaatorile recordDataIdentifier juurdepääsu abil kirje hetkeväärtuse edastamist.
WriteDataByIdentifier	Klient nõuab identifikaatorile recordDataIdentifier juurdepääsu abil kirje kirjutamist.

6.1. **Teenus ReadDataByIdentifier**

6.1.1. *Sõnumi kirjeldus*

CPR_050 Klient kasutab teenust ReadDataByIdentifier andmekirjete väärtuste nõudmiseks serverilt. Andmed identitakse identifikaatori recordDataIdentifier järgi. Sõidukiseadme tootja ülesanne on tagada, et serveri tingimused oleksid selle teenuse kasutamise ajal täidetud.

6.1.2. *Sõnumivorming*

CPR_051 Primitiivide ReadDataByIdentifier sõnumivormingud on esitatud järgmistes tabelites.

Tabel 25

Nõudesõnum ReadDataByIdentifier

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Lähteaadressibait	tt	SRC
#4	Lisapikkusebait	03	LEN
#5	**Nõude ReadDataByIdentifier teenuseidentifikaator**	**22**	**RDBI**
#6 kuni #7	recordDataIdentifier = [väärtus tabelist 28]	xxxx	RDI_…
#8	Kontrollsumma	00-FF	CS

Tabel 26

Nõudega ReadDataByIdentifier nõustumist kinnitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	m+3	LEN
#5	**Nõude ReadDataByIdentifier kinnitava vastuse teenuseidentifikaator**	**62**	**RDBIPR**
#6 ja #7	recordDataIdentifier = [sama väärtus kui tabeli 25 baitides nr 6 ja nr 7]	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 saadetav eitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	**Eitava vastuse teenuseidentifikaator**	**7F**	**NR**
#6	Nõude ReadDataByIdentifier teenuseidentifikaator	22	RDBI
#7	ResponseCode= [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Kontrollsumma	00-FF	CS

6.1.3. *Parameetri määratlus*

CPR_052 Nõudesõnumis ReadDataByIdentifier identitakse andmekirje parameetri ***recordDataIdentifier (RDI_)*** järgi.

CPR_053 Käesolevas dokumendis määratletud parameetri recordDataIdentifier väärtused on esitatud järgmises tabelis.

Parameetri recordDataIdentifier tabel koosneb neljast veerust ja mitmest reast.

— **Esimene veerg (Hex)** sisaldab kolmandas veerus määratletud identifikaatorile recordDataIdentifier omistatud kuueteistkümnendsüsteemis väärtust.

— **Teises veerus (andmeelement)** määratletakse 1. liite andmeelement, millel recordDataIdentifier põhineb (mõnikord on vaja transkodeerida).

— **Kolmandas veerus (kirjeldus)** esitatakse vastava identifikaatori recordDataIdentifier nimetus.

— **Neljandas veerus (mnemooniline nimi)** esitatakse selle identifikaatori recordDataIdentifier mnemooniline nimi.

Tabel 28

Parameetri recordDataIdentifier väärtuste määratlus

Hex	Andmeelement	Identifikaatori recordDataIdentifier nimetus (vt vorming punkt 8.2)	Mnemooniline nimi
F90B	`CurrentDateTime`	TimeDate	RDI_TD
F912	`HighResOdometer`	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	`K-ConstantOfRecordingEquipment`	Kfactor	RDI_KF

Hex	Andmeelement	Identifikaatori recordDataIdentifier nimetus (vt vorming punkt 8.2)	Mnemooniline nimi
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 Identifikaatori ReadDataByIdentifier kinnitav vastussõnum kasutab parameetrit ***dataRecord (DREC_)*** identifikaatori recordDataIdentifier järgi identitud andmekirje väärtuse esitamiseks kliendile (testimisseadmele). Andmevormingud on määratletud 8. peatükis. Lisaks võib rakendada kasutaja valitavaid sõidukiseadmeomaseid 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 Klient kasutab teenust WriteDataByIdentifier andmekirjete väärtuste kirjutamiseks serverisse. Andmed identitakse identifikaatori recordDataIdentifier järgi. Sõidukiseadme tootja ülesanne on tagada, et serveri tingimused oleksid selle teenuse kasutamise ajal täidetud. Tabelis 28 loetletud parameetrite ajakohastamiseks peab sõidukiseade olema režiimis CALIBRATION.

6.2.2. *Sõnumivorming*

CPR_057 Primitiivide WriteDataByIdentifier sõnumivormingud on esitatud järgmistes tabelites.

Tabel 29

Nõudesõnum WriteDataByIdentifier

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Lähteaadressibait	tt	SRC
#4	Lisapikkusebait	m+3	LEN
#5	**Nõude WriteDataByIdentifier teenuseidentifikaator**	**2E**	**WDBI**
#6 kuni #7	recordDataIdentifier = [väärtus tabelist 28]	xxxx	RDI_…

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#8 kuni m +7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrollsumma	00-FF	CS

Tabel 30

Nõudega WriteDataByIdentifier nõustumist kinnitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	**Nõude WriteDataByIdentifier kinnitava vastuse teenuseidentifikaator**	**6E**	**WDBIPR**
#6 kuni #7	recordDataIdentifier = [sama väärtus kui tabeli 29 baitides nr 6 ja nr 7]	xxxx	RDI_…
#8	Kontrollsumma	00-FF	CS

Tabel 31

Nõudele WriteDataByIdentifier saadetav eitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	**Eitava vastuse teenuseidentifikaator**	**7F**	**NR**
#6	Nõude WriteDataByIdentifier teenuseidentifikaator	2E	WDBI

Baidi nr	Parameetri nimetus		Hex-väärtus	Mnemooniline nimi
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrollsumma		00-FF	CS

6.2.3. *Parameetri määratlus*

Parameeter ***recordDataIdentifier (RDI_)*** on määratletud tabelis 28.

Nõudesõnum WriteDataByIdentifier kasutab parameetrit ***dataRecord (DREC_)*** identifikaatori recordDataIdentifier järgi idenditud andmekirje väärtuste esitamiseks serverile (sõidukiseadmele). Andmevormingud on määratletud 8. peatükis.

7. TESTIMPULSSIDE JUHTIMINE – SISEND-/VÄLJUNDSIGNAALI JUHTIMISE FUNKTSIONAALNE ÜKSUS

Kasutatavad teenused on esitatud järgmises tabelis.

Tabel 32

Sisend-/väljundsignaali juhtimise funktsionaalne üksus

Teenuse nimetus	Kirjeldus
InputOutputControlByIdentifier	Klient nõuab serveriomase sisend-/väljundsignaali juhtimist.

7.1. **Teenus InputOutputControlByIdentifier**

7.1.1. *Sõnumi kirjeldus*

Esipistmiku kaudu saab luua ühenduse, mis võimaldab sobiva testimisseadme abil juhtida või kontrollida testimpulsse.

CPR_058 Kalibreerimise sisend-/väljundsignaaliliini saab konfigureerida K-liini käsuga, kasutades liini tarvis nõutava sisend- või väljundfunktsiooni valimiseks teenust InputOutputControlByIdentifier. Kasutatavad liini olekud on:

— välja lülitatud;

— speedSignalInput, kus kalibreerimise sisend-/väljundsignaaliliini kasutatakse liikumisanduri kiirusesignaali asendava kiirusesignaali (testsignaal) sisestamiseks. See funktsioon ei ole kasutatav režiimis CONTROL;

— realTimeSpeedSignalOutputSensor, kus kalibreerimise sisend-/väljundsignaaliliini kasutatakse liikumisanduri kiirusesignaali väljastamiseks;

— RTCOutput, kus kalibreerimise sisend-/väljundsignaaliliini kasutatakse koordineeritud maailmaaja kellasignaali väljastamiseks. See funktsioon ei ole kasutatav režiimis CONTROL.

CPR_059 Liini oleku konfigureerimiseks peab sõidukiseade olema käivitanud reguleerimisseansi ning olema režiimis CALIBRATION või CONTROL. Kui sõidukiseade on režiimis CALIBRATION, saab valida liini nelja oleku vahel (välja lülitatud, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Kui sõidukiseade on režiimis CONTROL, saab valida ainult liini kahe oleku vahel (välja lülitatud, realTimeSpeedOutputSensor). Reguleerimisseansist või režiimist CALIBRATION või CONTROL väljumisel peab sõidukiseade tagama, et kalibreerimise sisend-/väljundsignaaliliin läheb tagasi (vaike-) olekusse „välja lülitatud“.

CPR_060 Kui sõidukiseadme reaalaja kiirusesignaali sisendliinis võetakse vastu kiiruseimpulsse ning samal ajal on kalibreerimise sisend-/väljundsignaaliliin reguleeritud sisendile, reguleeritakse kalibreerimise sisend-/väljundsignaaliliin väljundile või lülitatakse uuesti välja.

CPR_061 Järjestus on järgmine:

— teenuse StartCommunication abil side loomine,

— teenuse StartDiagnosticSession abil reguleerimisseansi käivitamine ning režiimi CALIBRATION või CONTROL kasutamine (nende kahe toimingu järjestus ei ole oluline),

— teenuse InputOutputControlByIdentifier abil sisendsignaali muutmine väljundsignaaliks.

7.1.2. *Sõnumivorming*

CPR_062 Primitiivide InputOutputControlByIdentifier sõnumivormingud on esitatud järgmistes tabelites.

Tabel 33

Nõudesõnum InputOutputControlByIdentifier

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	EE	TGT
#3	Lähteaadressibait	tt	SRC
#4	Lisapikkusebait	xx	LEN
#5	**Nõude InputOutputControlByIdentifier teenuseidentifikaator**	**2F**	**IOCBI**
#6 ja #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 või	ControlOptionRecord = [		COR_…
#8 kuni #9	inputOutputControlParameter – üks väärtus tabelist 36	xx	IOCP_…
	controlState – üks väärtus tabelist 37 (vt allpool olev märkus)]	xx	CS_…
#9 või #10	Kontrollsumma	00-FF	CS

Märkus. Parameeter controlState on olemas ainult mõnedel juhtudel (vt 7.1.3).

Tabel 34

Nõudega InputOutputControlByIdentifier nõustumist kinnitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	xx	LEN
#5	**Nõude inputOutputControlByIdentifier kinnitava vastuse teenuseidentifikaator**	**6F**	**IOCBIPR**
#6 ja #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 või	controlStatusRecord = [		CSR_
#8 kuni #9	inputOutputControlParameter (sama väärtus kui tabeli 33 baidis nr 8)	xx	IOCP_…
	controlState (sama väärtus kui tabeli 33 baidis nr 9)] (kui on olemas)	xx	CS_…
#9 või #10	Kontrollsumma	00-FF	CS

Tabel 35

Nõudele InputOutputControlByIdentifier saadetav eitav vastussõnum

Baidi nr	Parameetri nimetus	Hex-väärtus	Mnemooniline nimi
#1	Vormingubait – füüsiline adresseerimine	80	FMT
#2	Sihtaadressibait	tt	TGT
#3	Lähteaadressibait	EE	SRC
#4	Lisapikkusebait	03	LEN
#5	**Eitava vastuse teenuseidentifikaator**	**7F**	**NR**
#6	Nõude InputOutputControlByIdentifier teenuseidentifikaator	2F	IOCBI
#7	responseCode = [		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	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 määratlus

Hex	Kirjeldus	Mnemooniline nimi
00	**ReturnControlToECU** Väärtus näitab serverile (sõidukiseade), et testimisseade ei juhi enam kalibreerimise sisend-/väljundsignaaliliini.	RCTECU
01	**ResetToDefault** Väärtus näitab serverile (sõidukiseade), et sellele on esitatud nõue viia kalibreerimise sisend-/väljundsignaaliliin tagasi vaikeolekusse.	RTD
03	**ShortTermAdjustment** Väärtus näitab serverile (sõidukiseade), et sellele on esitatud nõue reguleerida kalibreerimise sisend-/väljundsignaaliliin väärtusele, mis sisaldub parameetris controlState.	STA

CPR_065 Järgmises tabelis määratletud parameeter ***controlState*** on olemas ainult siis, kui parameetris inputOutputControlParameter on valitud ShortTermAdjustment.

Tabel 37

Parameetri controlState väärtuste määratlus

Režiim	Hex-väärtus	Kirjeldus
Välja lülitatud	00	Sisend-/väljundliin on välja lülitatud (vaikeolek)
Sisse lülitatud	01	Kalibreerimise sisend-/väljundliin on sisse lülitatud sisendina speedSignalInput
Sisse lülitatud	02	Kalibreerimise sisend-/väljundliin sisse lülitatud andurina realTimeSpeedSignalOutputSensor
Sisse lülitatud	03	Kalibreerimise sisend-/väljundliin sisse lülitatud väljundina RTCOutput

8. ANDMEKIRJETE VORMINGUD

Käesolev peatükk sisaldab järgmist teavet:

— üldeeskirjad, mida kohaldatakse erinevate parameetrite suhtes, mida sõidukiseade edastab testimisseadmele,

— vormingud, mida kasutatakse andmete edastamiseks 6. peatükis kirjeldatud andmeedastusteenuste kaudu.

CPR_067 Sõidukiseade peab toetama kõiki identitud parameetreid.

CPR_068 Sõidukiseadmest testimisseadme nõudesõnumile vastuseks edastatud andmed peavad olema mõõdetavad (st sõidukiseade on mõõtnud või täheldanud nõutud parameetri hetkeväärtuse).

8.1. **Edastatavad parameetriväärtused**

CPR_069 Tabelis 38 on määratletud vahemikud, mida kasutatakse edastatud parameetri kehtivuse kindlakstegemiseks.

CPR_070 Vahemikku „error indicator“ jäävate väärtuste puhul näitab sõidukiseade kohe, et kehtivaid parameetreid hetkel ei ole seoses mingi veaga sõidumeerikus.

CPR_071 Vahemikku „not available“ jäävate väärtuste puhul edastab sõidukiseade sõnumi, mis sisaldab parameetrit, mis ei ole kasutatav või mida see moodul ei toeta. Vahemikku „not requested“ jäävate väärtuste puhul edastab seade käsusõnumi ja identib 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

Andmekirjete (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 FAFFFFFF	1 kuni 254
Parameetriomane indikaator	FB	FB00 kuni FBFF	FB000000 kuni FBFFFFFF	puudub
Tulevaste indikaatorbittide kasutamiseks reserveeritud vahemik	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 piiraja jaoks on reserveeritud ASCII märk „*“.

8.2. **Andmekirjete vormingud**

Järgnevates tabelites 39 kuni 42 kirjeldatakse vorminguid, mida kasutatakse teenustes ReadDataByIdentifier ja WriteDataByIdentifier.

CPR_074 Tabelis 39 on esitatud identifikaatori recordDataIdentifier järgi identitud iga paremeetri kohta selle pikkus, eristusvõime ja toimeulatus.

Tabel 39

Andmekirjete (dataRecords) vorming

Parameetri nimetus	Andme-pikkus (baitides)	Eristusvõime	Toimeulatus
TimeDate	8	Üksikasjad tabelis 40	
HighResolutionTotalVehicleDistance	4	5 m/bitt, nihe 0 m	0 kuni + 21 055 406 km
Kfactor	2	0,001 impulssi/m /bitt, nihe 0	0 kuni 64,255 impulssi/m
LfactorTyreCircumference	2	0,125 10^{-3} m /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

Parameetri nimetus	Andme-pikkus (baitides)	Eristusvõime	Toimeulatus
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 42	
VIN	17	ASCII	ASCII

CPR_075 Tabelis 40 kirjeldatakse parameetri TimeDate erinevate baitide vorminguid.

Tabel 40

Kirje TimeDate üksikasjalik vorming (parameetri recordDataIdentifier väärtus # F90B)

Bait	Parameetri määratlus	Eristusvõime	Toimeulatus
1	Sekundid	0,25 s/bitt, nihe 0 s	0 kuni 59,75 s
2	Minutid	1 min/bitt, nihe 0 min	0 kuni 59 min
3	Tunnid	1 h/bitt, nihe 0 h	0 kuni 23 tundi
4	Kuu	1 kuu/bitt, nihe 0 kuud	1 kuni 12 kuud
5	Päev	0,25 päeva/bitt, nihe 0 päeva (vt tabeli 41 all olev märkus)	0,25 kuni 31,75 päeva
6	Aasta	1 aasta/bitt, nihe +1985. aasta (vt tabeli 41 all olev märkus)	1985. kuni 2235. aasta
7	Kohalik minutinihe	1 min/bitt, nihe – 125 min	– 59 kuni + 59 min
8	Kohalik tunninihe	1 h/bitt, nihe – 125 h	– 23 kuni + 23 h

CPR_076 Tabelis 41 on kirjeldatud parameetri NextCalibrationDate erinevate baitide vormingut.

Tabel 41

Kirje NextCalibrationDate üksikasjalik vorming (parameetri recordDataIdentifier väärtus # F922)

Bait	Parameetri määratlus	Eristusvõime	Toimeulatus
1	Kuu	1 kuu/bitt, nihe 0 kuud	1 kuni 12 kuud
2	Päev	0,25 päeva/bitt, nihe 0 päeva (vt märkus allpool)	0,25 kuni 31,75 päeva
3	Aasta	1 aasta/bitt, nihe +1985. aasta (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; väärtustega 5, 6, 7 ja 8 identitakse kuu teine päev jne.

2) See parameeter ei mõjuta ega muuda 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 kirjeldatud parameetri VehicleRegistrationNumber erinevate baitide vormingut.

Tabel 42

Kirje VehicleRegistrationNumber üksikasjalik vorming (parameetri recordDataIdentifier väärtus # F97E)

Bait	Parameetri määratlus	Eristusvõime	Toimeulatus
1	Koodilehekülg (vastavalt 1. liitele)	ASCII	01 kuni 0A
2–14	Sõiduki registreerimisnumber (vastavalt 1. liitele)	ASCII	ASCII

9. liide

TÜÜBIKINNITUS: MINIMAALSELT NÕUTAVATE KATSETE NIMEKIRI

SISUKORD

1. SISSEJUHATUS

1.1. **Tüübikinnitus**

Sõidumeeriku (või selle osa) või sõidumeerikukaardi ELi tüübikinnitus põhineb järgmisel:

— **turvalisuse sertifitseerimine**, mis põhineb ühiste kriteeriumide spetsifikaadil ning mille puhul turvalisust võrreldakse käesoleva lisa 10. liitele täielikult vastava turbe-eesmärgiga;

— **funktsionaalsuse sertifitseerimine**, mille viib läbi liikmesriigi asutus, kes tõendab, et katsetatud seadme funktsioonid, mõõtmistäpsus ja keskkonnaomadused vastavad täielikult käesolevale lisale;

— **koostalitlusvõime sertifitseerimine**, mille viib läbi pädev asutus, kes tõendab, et sõidumeerik (või sõidumeerikukaart) on täielikult koostalitlev vajalike sõidumeerikukaardi (või sõidumeeriku) mudelitega (vt käesoleva lisa 8. peatükk).

Käesolevas liites on määratletud, millised katsed peab liikmesriigi asutus minimaalselt läbi viima funktsionaalsete katsete puhul ja millised katsed peab pädev asutus minimaalselt läbi viima koostalitlusvõime katsete puhul. Nende katsete läbiviimise kord ja katsete liik 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 asjaomaste turvakatsete tulemusi. Nõuded, millele vastavuse kontrollimist turvalisuse tõendamise käigus eeldatakse (või mis on eeldatavalt läbi viidavate katsetega lähedalt seotud), on käesolevas liites tähistatud tärniga („*“).

Nummerdatud nõuete puhul viidatakse lisa tekstile ning muude nõuete puhul viidatakse teistele liidetele (nt PIC_001 viitab 3. liite „Piktogrammid“ nõudele PIC_001).

Käesolevas liites käsitletakse sõidumeeriku koosseisus oleva liikumisanduri, sõidukiseadme ja GNSSi välisseadme tüübikinnitust eraldi. Iga osa kohta antakse eraldi tüübikinnitustunnistus, kuhu märgitakse ülejäänud ühilduvad osad. Liikumisanduri (või GNSSi välisseadme) funktsionaalne katse tehakse koos sõidukiseadmega ja vastupidi.

Liikumisanduri (või GNSSi välisseadme) iga mudeli ja sõidukiseadme iga mudeli vahelist koostalitlusvõimet ei nõuta. Sel juhul võib liikumisanduri (või GNSSi välisseadme) kohta tüübikinnituse anda ainult seoses kasutatava sõidukiseadme tüübikinnitusega ja vastupidi.

1.2. **Viited**

Käesolevas liites kasutatakse järgmisi viiteid.

IEC 60068-2-1 *Environmental testing – Part 2-1: Tests – Test A: Cold* („Keskkonnakatsed. Osa 2-1: Katsed. Katse A: külm“)

IEC 60068-2-2 *Basic environmental testing procedures – Part 2: Tests – Tests B: Dry heat (sinusoidal)* („Põhilised keskkonnaalased katsemenetlused. Osa 2: Katsed. Katsed B: kuiv kuumus (siinuseline)“)

IEC 60068-2-6 *Environmental testing –- Part 2: Tests – Test Fc: Vibration* („Keskkonnakatsed. Osa 2: Katsed. Katse Fc: vibratsioon“)

IEC 60068-2-14 *Environmental testing – Part 2-14: Tests – Test N: Change of temperature* („Keskkonnakatsed. Osa 2-14: Katsed. Katse N: temperatuuri muutus“)

IEC 60068-2-27 *Environmental testing – Part 2: Tests – Test Ea and guidance: Shock* („Keskkonnakatsed. Osa 2: Katsed. Katse Ea ja juhised: löögid“)

IEC 60068-2-30 *Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)* („Keskkonnakatsed. Osa 2-30: Katsed. Katse Db: tsükliline niiske kuumus (12 + 12 tunni pikkune tsükkel)“)

IEC 60068-2-64 *Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance* („Keskkonnakatsed. Osa 2-64: Katsed. Katse Fh: lairibas toimuv juhuslik vibratsioon ja juhised“)

IEC 60068-2-78 *Environmental testing – Part 2-78: Tests – Test Cab: Damp heat, steady state* („Keskkonnakatsed. Osa 2-78: Katsed. Katse Cab: kuiv kuumus, püsiv“)

ISO 16750-3 *Mechanical loads* („Mehaanilised koormused“) (2012–12)

ISO 16750-4 *Climatic loads* („Klimaatilised koormused“) (2010–04)

ISO 20653 *Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access* („Maanteesõidukid. Kaitseaste (IP-kood). Elektriseadmete kaitse võõrkehade, vee ja juurdepääsu eest“)

ISO 10605:2008 + tehniline parandus: 2010 + 1. muudatus: 2014 *Road vehicles – Test methods for electrical disturbances from electrostatic discharge* („Maanteesõidukid. Elektrostaatilisest lahendusest tingitud elektriliste häiretega seotud katsemeetodid“)

ISO 7637-1: 2002 + 1. muudatus: 2008 *Road vehicles – Electrical disturbances from conduction and coupling – Part 1: Definitions and general considerations* („Maanteesõidukid. Juhtivusest ja ühendamisest tingitud elektrilised häired. Osa 1: Mõisted ja üldised kaalutlused“)

ISO 7637-2 *Road vehicles – Electrical disturbances from conduction and coupling – Part 2: Electrical transient conduction along supply lines only* („Maanteesõidukid. Juhtivusest ja ühendamisest tingitud elektrilised häired. Osa 2: Ainult toiteliinide siirdeelektrijuhtivus“)

ISO 7637-3 *Road vehicles – Electrical disturbances from conduction and coupling – Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines* („Maanteesõidukid. Juhtivusest ja ühendamisest tingitud elektrilised häired. Osa 3: Siirdeelektriedastus mahtuvusliku või induktiivse sidestusega muude liinide kui toiteliinide kaudu“)

ISO/IEC 7816-1 *Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics* („Identimiskaardid. Kontaktidega kiipkaardid. Osa 1: Füüsikalised omadused“)

ISO/IEC 7816-2 *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts* („Infotehnoloogia. Identimiskaardid. Kontaktidega kiipkaardid. Osa 2: Kontaktide mõõtmed ja asukoht“)

ISO/IEC 7816-3 *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol* („Infotehnoloogia. Identimiskaardid. Kontaktidega kiipkaardid. Osa 3: Elektroonilised signaalid ja edastusprotokoll“)

ISO/IEC 10373-1: 2006 + 1. muudatus: 2012 *Identification cards – Test methods – Part 1: General characteristics* („Identimiskaardid. Katsemeetodid. Osa 1: Üldised omadused“)

ISO/IEC 10373-3: 2010 + tehniline parandus: 2013 *Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices* („Identimiskaardid. Katsemeetodid. Osa 3: Kontaktidega kiipkaardid ja seotud liideseseadmed“)

ISO 16844-3:2004 + 1. parandus: 2006 *Road vehicles – Tachograph systems – Part 3: Motion sensor interface (with vehicle units)* („Maanteesõidukid. Sõidumeerikusüsteemid. Osa 3: Liikumisanduri liides (sõidukiseadmega)“)

ISO 16844-4 *Road vehicles – Tachograph systems – Part 4: CAN interface* („Maanteesõidukid. Sõidumeerikusüsteemid. Osa 4: CAN-liides“)

ISO 16844-6 *Road vehicles – Tachograph systems – Part 6: Diagnostics* („Maanteesõidukid. Sõidumeerikusüsteemid. Osa 6: Diagnostika“)

ISO 16844-7 *Road vehicles – Tachograph systems – Part 7: Parameters* („Maanteesõidukid. Sõidumeerikusüsteemid. Osa 7: Parameetrid“)

ISO 534 *Paper and board – Determination of thickness, density and specific volume* („Paber ja papp. Paksuse, tiheduse ja erimahu kindlaksmääramine“)

UN ECE R10 Ühtsed sätted, mis käsitlevad sõidukite tüübikinnitust seoses elektromagnetilise ühilduvusega (Ühinenud Rahvaste Organisatsiooni Euroopa Majanduskomisjon)

2. SÕIDUKISEADME FUNKTSIONAALSED KATSED

Nr	Katse	Kirjeldus	Seotud nõuded
1	**Halduskontroll**		
1.1	Dokumendid	Dokumentide õigsus	
1.2	Tootja katsetulemused	Kokkupaneku ajal tootja tehtud katsete tulemused. Kirjalikud tõendid.	88, 89, 91
2	**Visuaalne kontroll**		
2.1	Vastavus dokumentidele		
2.2	Identimisandmed/märgistus		224 kuni 226
2.3	Materjalid		219 kuni 223
2.4	Plommid		398, 401 kuni 405
2.5	Välisliidesed		
3	**Funktsionaalsed katsed**		
3.1	Olemasolevad funktsioonid		03, 04, 05, 07, 382,
3.2	Kasutusrežiimid		09 kuni 11*, 132, 133
3.3	Funktsioonid ja andmetele juurdepääsu õigused		12*, 13*, 382, 383, 386 kuni 389
3.4	Kaartide sisestamise ja väljavõtmise seire		15, 16, 17, 18, 19*, 20*, 132
3.5	Kiiruse ja vahemaa mõõtmine		21 kuni 31
3.6	Aja mõõtmine (katse 20 °C juures)		38 kuni 43
3.7	Juhi tegevuse seire		44 kuni 53, 132
3.8	Juhtimisstaatuse seire		54, 55, 132

Nr	Katse	Kirjeldus	Seotud nõuded
3.9	Käsitsi tehtavad sissekanded		56 kuni 62
3.10	Ettevõttelukkude haldamine		63 kuni 68
3.11	Kontrollitegevuse seire		69, 70
3.12	Sündmuste ja/või vigade avastamine		71 kuni 88, 132
3.13	Seadme identimisandmed		93*, 94*, 97, 100
3.14	Juhikaardi sisestamise ja väljavõtmise andmed		102* kuni 104*
3.15	Andmed juhi tegevuse kohta		105* kuni 107*
3.16	Koha- ja asukohaandmed		108* kuni 112*
3.17	Läbisõidumõõdiku andmed		113* kuni 115*
3.18	Üksikasjalikud andmed kiiruse kohta		116*
3.19	Andmed sündmuste kohta		117*
3.20	Andmed vigade kohta		118*
3.21	Kalibreerimisandmed		119* kuni 121*
3.22	Andmed aja korrigeerimise kohta		124*, 125*
3.23	Andmed kontrollitegevuse kohta		126*, 127*
3.24	Andmed ettevõttelukkude kohta		128*
3.25	Andmed allalaadimistegevuse kohta		129*
3.26	Andmed eritingimuste kohta		130*, 131*
3.27	Registreerimine ja salvestamine sõidumeerikukaartidele		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Kuvamine		90, 132, 149 kuni 166, PIC_001, DIS_001
3.29	Trükkimine		90, 132, 167 kuni 179, PIC_001, PRT_001 kuni PRT_014
3.30	Hoiatused		132, 180 kuni 189, PIC_001

Nr	Katse	Kirjeldus	Seotud nõuded
3.31	Andmete allalaadimine välisandmekandjale		90, 132, 190 kuni 194
3.32	Sihipärastes teeäärsetes kontrollides kasutatav kaugside		195 kuni 197
3.33	Andmete väljastamine lisavälisseadmetele		198, 199
3.34	Kalibreerimine		202 kuni 206*, 383, 384, 386 kuni 391
3.35	Teeäärne kalibreerimiskontroll		207 kuni 209
3.36	Aja korrigeerimine		210 kuni 212*
3.37	Lisafunktsioonide põhjustatud häired		06, 425
3.38	Liikumisanduri liides		02, 122
3.39	GNSSi välisseade		03, 123
3.40	Kontrollida, et sõidukiseade avastab, registreerib ja salvestab sõidukiseadme tootja kindlaks määratud sündmuse(d) ja/või vea(d), kui ühendatud liikumisandur reageerib sõiduki liikumise jälgimist segavatele magnetväljadele.		217
3.41	Šifrikomplekt ja domeeni standardparameetrid		CSM_48, CSM_50
4	**Keskkonnakatsed**		
4.1	Temperatuur	Funktsionaalsuse tõendamine järgmisel alusel: Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.1.1.2: talitluskatse madalal temperatuuril (72 h temperatuuril – 20 °C). Katse aluseks on standard IEC 60068-2-1: „Keskkonnakatsed. Osa 2-1: Katsed. Katse A: külm“. Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.1.2.2: talitluskatse kõrgel temperatuuril (72 h temperatuuril 70 °C). Katse aluseks on standard IEC 60068-2-2: „Põhilised keskkonnaalased katsemenetlused. Osa 2: Katsed. Katsed B: kuiv kuumus“. Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.3.2: kindla üleminekuajaga kiire temperatuurimuutus (– 20 °C/70 °C, 20 tsüklit, igal temperatuuril hoidmise aeg 2 tundi). Madalal temperatuuril, kõrgel temperatuuril ja temperatuuritsüklite ajal võib läbi viia vähendatud katsete kogumi (nende katsete puhul, mis on määratletud käesoleva tabeli 3. osas).	213

Nr	Katse	Kirjeldus	Seotud nõuded
4.2	Niiskus	Tõendada standardi IEC 60068-2-30 katse Db alusel, et sõidukiseade suudab taluda tsüklilist niiskust (kuumuskatse) kuue 24-tunnise tsükli jooksul; igas tsüklis kõigub temperatuur vahemikus + 25 °C kuni + 55 ° C ning suhteline niiskus on + 25 °C juures 97 % ja + 55 °C juures 93 %.	214
4.3	Mehaanilised omadused	1. Siinusvibratsioon: tõendada, et sõidukiseade suudab taluda järgmiste omadustega siinusvibratsiooni: püsinihe sagedusalas 5 kuni 11 Hz: maksimaalne 10 mm; püsikiirendus sagedusalas 11 kuni 300 Hz: 5 g. Seda nõuet tõendatakse standardi IEC 60068-2-6 katse Fc alusel; minimaalne katseaeg 3 × 12 tundi (12 tundi telje kohta). Standardi ISO 16750-3 kohaselt ei ole siinusvibratsiooni katse nõutav lahti haagitud sõidukikabiinis asuvate seadmete puhul. 2. Juhuslik vibratsioon: Katse viiakse läbi vastavalt standardi ISO 16750-3 punktile 4.1.2.8: VIII katse: tarbesõiduk, lahti haagitud sõidukikabiin. Juhusliku vibratsiooni katse, 10…2 000 Hz, vertikaalsuuna ruutkeskmine 21,3 m/s², pikisuuna ruutkeskmine 11,8 m/s², külgsuuna ruutkeskmine 13,1 m/s², 3 telge, 32 h telje kohta, temperatuuritsükliga – 20…70 °C. Katse aluseks on standard IEC 60068-2-64: „Keskkonnakatsed. Osa 2-64: Katsed. Katse Fh: lairibas toimuv juhuslik vibratsioon ja juhised“. 3. Löögid: mehaaniline löök 3 g poolsiinusega vastavalt standardile ISO 16750. Eespool kirjeldatud katsed tehakse katsetatava seadmetüübi kahe erineva näidisega.	219
4.4	Kaitse vee ja võõrkehade eest	Katse viiakse läbi vastavalt standardile ISO 20653: „Maanteesõidukid. Kaitseaste (IP-kood). Elektriseadmete kaitse võõrkehade, vee ja juurdepääsu eest“ (parameetrite muutusteta); miinimumväärtus IP 40.	220, 221
4.5	Kaitse ülepinge eest	Tõendada, et sõidukiseade suudab taluda järgmist toitepinget: 24 V versioonid: 1 tund 34 V temperatuuril + 40 °C 12 V versioonid: 1 tund 17 V temperatuuril + 40 °C (ISO 16750-2)	216
4.6	Kaitse polaarsuse vahetuse eest	Tõendada, et sõidukiseade suudab taluda toiteallika polaarsuse vahetust. (ISO 16750-2)	216

Nr	Katse	Kirjeldus	Seotud nõuded
4.7	Kaitse lühiste eest	Tõendada, et sisend-/väljundsignaalid on kaitstud lühiste eest toiteallikaga ja maaga. (ISO 16750-2)	216
5	**Elektromagnetilise ühilduvuse katsed**		
5.1	Kiirgusemissioon ja vastuvõtlikkus	Vastavus eeskirjale ECE R10	218
5.2	Elektrostaatiline lahendus	Vastavus standardile ISO 10605:2008 + tehniline parandus: 2010 + 1. muudatus: 2014: +/– 4 kV kontakti ja +/– 8 kV õhklahenduse korral	218
5.3	Juhtivuslike siirete vastuvõtlikkus vooluallikast	24 V versioonid: vastavus standardile ISO 7637-2 + ECE eeskirjale nr 10, red. 3: impulss 1a: Vs = – 450 V, Ri = 50 oomi impulss 2a: Vs = + 37 V, Ri = 2 oomi impulss 2a: Vs = + 20 V, Ri = 0,05 oomi impulss 3a: Vs = – 150 V, Ri = 50 oomi impulss 3a: Vs = + 150 V, Ri = 50 oomi impulss 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms impulss 5: Vs = + 120 V, Ri = 2,2 oomi, td = 250 ms 12 V versioonid: vastavus standardile ISO 7637-1 + ECE eeskirjale nr 10, red. 3: impulss 1: Vs = – 75 V, Ri = 10 oomi impulss 2a: Vs = + 37 V, Ri = 2 oomi impulss 2a: Vs = + 10 V, Ri = 0,05 oomi impulss 3a: Vs = – 112 V, Ri = 50 oomi impulss 3a: Vs = + 75 V, Ri = 50 oomi impulss 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms impulss 5: Vs = + 65 V, Ri = 3 oomi, td = 100 ms Impulssi 5 katsetatakse ainult nendel sõidukiseadmetel, mis on ette nähtud paigaldamiseks sõidukitele, millel puudub ühine väliskaitse koormuse avariilise vähenemise eest. Koormuse avariilise vähenemise ettepaneku kohta vt ISO 16750-2, 4. väljaanne, punkt 4.6.4.	218

3. LIIKUMISANDURI FUNKTSIONAALSED KATSED

Nr	Katse	Kirjeldus	Seotud nõuded
1.	**Halduskontroll**		
1.1	Dokumendid	Dokumentide õigsus	

Nr	Katse	Kirjeldus	Seotud nõuded
2.	**Visuaalne kontroll**		
2.1.	Vastavus dokumentidele		
2.2.	Tunnusmärgid/tähistused		225, 226
2.3	Materjalid		219 kuni 223
2.4.	Plommid		398, 401 kuni 405
3.	**Funktsionaalsed katsed**		
3.1	Anduri identimisandmed		95 kuni 97*
3.2	Liikumisanduri ja sõidukiseadme kokkuühendamine		122*, 204
3.3	Liikumise tuvastamine Liikumise mõõtmistäpsus		30 kuni 35
3.4	Sõidukiseadme liides		02
3.5	Kontrollida, et liikumisandur oleks püsimagnetväljade suhtes immuunne. Teine võimalus on kontrollida, et liikumisandur reageeriks sõiduki liikumise jälgimist segavatele püsimagnetväljadele nii, et ühendatud sõidukiseade suudab avastada, registreerida ja salvestada anduri rikkeid.		217
4.	**Keskkonnakatsed**		
4.1	Töötemperatuur	Tõendada funktsionaalsust (nagu on määratletud katses nr 3.3) temperatuurivahemikus [– 40 °C; + 135 °C] järgmistel alustel: IEC 60068-2-1, katse Ad, katse kestus 96 tundi madalaimal temperatuuril To_{min}, IEC 60068-2-2, katse Ad, katse kestus 96 tundi kõrgeimal temperatuuril To_{max}. Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.1.1.2: talitluskatse madalal temperatuuril (24 h temperatuuril – 40 °C). Katse aluseks on standard IEC 60068-2-1: „Keskkonnakatsed. Osa 2-1: Katsed. Katse A: külm“. IEC 68-2-2, katse Bd, katse kestus 96 tundi madalaimal temperatuuril – 40 °C. Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.1.2.2: talitluskatse kõrgel temperatuuril (96 h temperatuuril 135 °C). Katse aluseks on standard IEC 60068-2-2: „Põhilised keskkonnaalased katsemenetlused. Osa 2: Katsed. Katsed B: kuiv kuumus“.	213

Nr	Katse	Kirjeldus	Seotud nõuded
4.2	Temperatuuritsüklid	Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.3.2: kindla üleminekuajaga kiire temperatuurimuutus (– 40 °C/135 °C, 20 tsüklit, igal temperatuuril hoidmise aeg 30 min). IEC 60068-2-14 „Keskkonnakatsed. Osa 2-14: Katsed. Katse N: temperatuuri muutus“.	213
4.3	Niiskustsüklid	Tõendada funktsionaalsust (nagu on määratletud katses nr 3.3) standardi IEC 68-2-30 katse Db alusel, kuus 24-tunnist tsüklit, igas tsüklis kõigub temperatuur vahemikus + 25 °C kuni + 55 °C ning suhteline niiskus on + 25 °C juures 97 % ja + 55 °C juures 93 %.	214
4.4	Vibratsioon	ISO 16750-3 punkt 4.1.2.6: VI katse: tarbesõiduk, mootor, käigukast. Segarežiimil vibratsioonikatse, mis hõlmab järgmist: a) siinusvibratsiooni katse, 20…520 Hz, 11,4 … 120 m/s², <= 0,5 oktaavi/min; b) juhusliku vibratsiooni katse, 10…2 000 Hz, ruutkeskmine 177 … 94 h telje kohta, temperatuuritsükliga – 20…70 °C). Katse aluseks on standard IEC 60068-2-80: *Environmental testing – Part 2-80: Tests – Test Fi: Vibration – Mixed mode* („Keskkonnakatsed. Osa 2-80: Katsed. Katse Fi: vibratsioon – segarežiim“).	219
4.5	Mehaaniline löök	ISO 16750-3 punkt 4.2.3: VI katse: käigukastis või selle peal olevate seadmete katse. Poolsiinuslöök, kiirendus vastavalt kokkuleppele vahemikus 3 000…15 000 m/s², impulsi kestus vastavalt kokkuleppele, kuid igal juhul < 1 ms, löökide arv: vastavalt kokkuleppele. Katse aluseks on standard IEC 60068-2-27: „Keskkonnakatsed. Osa 2: Katsed. Katse Ea ja juhised: löögid“.	219
4.6	Kaitse vee ja võõrkehade eest	Katse viiakse läbi vastavalt standardile ISO 20653: „Maanteesõidukid. Kaitseaste (IP-kood). Elektriseadmete kaitse võõrkehade, vee ja juurdepääsu eest“ (sihtväärtus IP 64).	220, 221
4.7	Kaitse polaarsuse vahetuse eest	Tõendada, et liikumisandur suudab taluda toiteallika polaarsuse vahetust.	216
4.8	Kaitse lühiste eest	Tõendada, et sisend-/väljundsignaalid on kaitstud lühiste eest toiteallikaga ja maaga.	216

Nr	Katse	Kirjeldus	Seotud nõuded
5.	**Elektromagnetiline ühilduvus**		
5.1	Kiirgusemissioon ja vastuvõtlikkus	Tõendada vastavust eeskirjale ECE R10.	218
5.2	Elektrostaatiline lahendus	Vastavus standardile ISO 10605:2008 + tehniline parandus: 2010 + 1. muudatus: 2014: +/– 4 kV kontakti ja +/– 8 kV õhklahenduse korral	218
5.3	Vastuvõtlikkus juhtivuslikele siiretele andmeliinidest	24 V versioonid: vastavus standardile ISO 7637-2 + ECE eeskirjale nr 10, red. 3: impulss 1a: Vs = – 450 V, Ri = 50 oomi impulss 2a: Vs = + 37 V, Ri = 2 oomi impulss 2a: Vs = + 20 V, Ri = 0,05 oomi impulss 3a: Vs = – 150 V, Ri = 50 oomi impulss 3a: Vs = + 150 V, Ri = 50 oomi impulss 4: Vs = – 16 V, Va = – 12 V, t6 = 100ms impulss 5: Vs = + 120 V, Ri = 2,2 oomi, td = 250 ms 12 V versioonid: vastavus standardile ISO 7637-1 + ECE eeskirjale nr 10, red. 3: impulss 1: Vs = – 75 V, Ri = 10 oomi impulss 2a: Vs = + 37 V, Ri = 2 oomi impulss 2a: Vs = + 10 V, Ri = 0,05 oomi impulss 3a: Vs = – 112 V, Ri = 50 oomi impulss 3a: Vs = + 75 V, Ri = 50 oomi impulss 4: Vs = – 16 V, Va = – 5 V, t6 = 15 ms impulss 5: Vs = + 65 V, Ri = 3 oomi, td = 100 ms Impulssi 5 katsetatakse ainult nendel sõidukiseadmetel, mis on ette nähtud paigaldamiseks sõidukitele, millel puudub ühine väliskaitse koormuse avariilise vähenemise eest. Koormuse avariilise vähenemise ettepaneku kohta vt ISO 16750-2, 4. väljaanne, punkt 4.6.4.	218

4. SÕIDUMEERIKUKAARTIDE FUNKTSIONAALSED KATSED

Hindaja või sertifitseerija võib teha 4. peatükis nimetatud katsed

nr 5 „Protokolli katsed“,

nr 6 „Kaardi struktuur“ ja

nr 7 „Funktsionaalsed katsed“

ühistele kriteeriumidele vastava kiibimooduli turvalisuse sertifitseerimise protsessi käigus.

Katsed nr 2.3 ja 4.2 on kattuvad. Need on ühendatud kaardi ja kiibimooduli mehaanilised katsed. Need katsed on nõutavad ühe nimetatud osa (kaart, kiibimoodul) vahetamise korral.

Nr	Katse	Kirjeldus	Seotud nõuded
1.	**Halduskontroll**		
1.1	Dokumendid	Dokumentide õigsus	
2	**Kaart**		
2.1	Trükitud kujundus	Teha kindlaks, et kõik turvaelemendid ja nähtavad andmed on kaardile korrektselt trükitud ja nõuetekohased. [Tunnus] IC lisa punkt 4.1 „Nähtavad andmed“, 227) Esipoolel on: vastavalt kaardi tüübile kaardi väljaandnud liikmesriigi ametlikus keeles või ametlikes keeltes suurelt trükitult sõna „juhikaart“ või „kontrollikaart“ või „töökojakaart“ või „ettevõttekaart“. [Liikmesriigi nimi] IC lisa punkt 4.1 „Nähtavad andmed“, 228) Esipoolel on: kaardi välja andnud liikmesriigi nimi (vabatahtlik). [Märk] IC lisa punkt 4.1 „Nähtavad andmed“, 229) Esipoolel on: kaardi väljaandnud liikmesriigi rahvusvaheline tähis negatiivina sinises ristkülikus, mida ümbritseb kaksteist kollast tähte. [Nummerdus] IC lisa punkt 4.1 „Nähtavad andmed“, 232) Tagumisel küljel on: selgitus kaardi esiküljel olevate nummerdatud punktide kohta. [Värv] IC lisa punkt 4.1 „Nähtavad andmed“, 234) Sõidumeerikukaartidele trükitakse järgmine taustavärv: — juhikaart: valge, — töökojakaart: punane, — kontrollikaart: sinine, — ettevõttekaart: kollane.	227 kuni 229, 232, 234 kuni 236

Nr	Katse	Kirjeldus	Seotud nõuded
		[Turvalisus] IC lisa punkt 4.1 „Nähtavad andmed“, 235) Sõidumeerikukaartidel on vähemalt järgmised omadused, kaitsmaks neid võltsimise ja rikkumise eest: — peente giljoššmustrite ja vikerkaaretrükiga taustaturvamärk, — vähemalt üks kahevärviline mikrokirjas rida.	
		[Märgistus] IC lisa punkt 4.1 „Nähtavad andmed“, 236) Liikmesriigid võivad lisada värve või märgistusi, näiteks riiklikke sümboleid ja turvaelemente.	
		[Tüübikinnitusmärk] Sõidumeerikukaartidel peab olema tüübikinnitusmärk. Tüübikinnitusmärgi moodustavad: — e-tähte ümbritsev ristkülik, millele järgneb tüübikinnituse andnud riigi eraldusnumber või -täht, — tüübikinnitusnumber, mis vastab sõidumeerikukaardi tüübinäidise tüübikinnitustunnistuse numbrile ja asub mis tahes kohas ristküliku vahetus läheduses.	
2.2	Mehaanilised katsed	[Kaardi suurus] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identification cards – Physical characteristics“ („Identimiskaardid. Füüsikalised omadused“): [5] Kaardi mõõdud, [5.1] Kaardi suurus, [5.1.1] Kaardi mõõdud ja lubatud hälbed, kaardi tüüp ID-1, kasutamata kaart.	240, 243, ISO/IEC 7810
		[Kaardi servad] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [5] Kaardi mõõdud, [5.1] Kaardi suurus, [5.1.2] Kaardi servad.	

Nr	Katse	Kirjeldus	Seotud nõuded
		[Kaardi konstruktsioon] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [6] Kaardi konstruktsioon.	
		[Kaardi materjalid] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [7] Kaardi materjalid.	
		[Paindejäikus] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [8.1] Paindejäikus.	
		[Toksilisus] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [8.3] Toksilisus.	
		[Vastupidavus kemikaalidele] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [8.4] Vastupidavus kemikaalidele.	
		[Kaardi stabiilsus] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [8.5] Kaardi mõõtmete stabiilsus ja kõverdumine temperatuuri ja niiskuse mõjul	

Nr	Katse	Kirjeldus	Seotud nõuded
		[Valgustundlikkus] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [8.6] Valgustundlikkus.	
		[Vastupidavus] IC lisa punkt 4.4 „Keskkonnaalased ja elektrilised spetsifikatsioonid“, 241) Sõidumeerikukaardid toimivad nõuetekohaselt viis aastat, kui neid kasutatakse vastavalt keskkonnaalastele ja elektrilistele spetsifikatsioonidele.	
		[Koorumiskindlus] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [8.8] Koorumiskindlus.	
		[Kleepumine või blokeerumine] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [8.9] Kleepumine või blokeerumine.	
		[Kõverdumine] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [Vastupidavus kuumusele]	
		[8.11] Kaardi üldine kõverdumine. Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [8.12] Vastupidavus kuumusele.	

Nr	Katse	Kirjeldus	Seotud nõuded
		[Pinnamoonutused] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [8.13] Pinnamoonutused. [Saastumine] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810 „Identimiskaardid. Füüsikalised omadused“: [8] Kaardi omadused, [8.14] Kaardi osade saastumine ja vastastikune mõju.	
2.3	Mehaanilised katsed koos paigaldatud kiibimooduliga	[Painutamine] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810:2003/Amd. 1: 2009 „Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits“ („Identimiskaardid. Füüsikalised omadused. 1. muudatus: Kiipe sisaldavate kaartide suhtes kohaldatavad kriteeriumid“): [9.2] Dünaamiline paindepinge. Painutustsüklite koguarv: 4 000. [Väänamine] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810:2003/Amd. 1: 2009 „Identimiskaardid. Füüsikalised omadused. 1. muudatus: Kiipe sisaldavate kaartide suhtes kohaldatavad kriteeriumid“: [9.3] Dünaamiline väändepinge. Väänamistsüklite koguarv: 4 000.	ISO/IEC 7810
3	**Moodul**		
3.1	Moodul	Moodul koosneb kiibiümbrisest ja kontaktplaadist. [Pinnaprofiil] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7816-1:2011 „Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics“ („Identimiskaardid. Kiipkaardid. Osa 1: Kontaktidega kaardid. Füüsikalised omadused“): [4.2] Kontaktide pinna profiil.	ISO/IEC 7816

Nr	Katse	Kirjeldus	Seotud nõuded
		[Mehaaniline tugevus] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7816-1:2011 „Identimiskaardid. Kiipkaardid. Osa 1: Kontaktidega kaardid. Füüsikalised omadused“: [4.3] Mehaaniline tugevus (kaart ja kontaktid).	
		[Elektritakistus] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7816-1:2011 „Identimiskaardid. Kiipkaardid. Osa 1: Kontaktidega kaardid. Füüsikalised omadused“: [4.4] Elektritakistus (kontaktid)	
		[Mõõtmed] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7816-2:2007 „Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts“ („Identimiskaardid. Kiipkaardid. Osa 2: Kontaktidega kaardid. Kontaktide mõõtmed ja asukoht“): [3] Kontaktide mõõtmed.	
		[Asukoht] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7816-2:2007 „Identimiskaardid. Kiipkaardid. Osa 2: Kontaktidega kaardid. Kontaktide mõõtmed ja asukoht“: [4] Kontaktide arv ja asukoht. Kuue kontaktiga moodulite korral ei kohaldata seda katsenõuet kontaktide C4 ja C8 suhtes.	
4	**Kiip**		
4.1	Kiip	[Töötemperatuur] Sõidumeerikukaardi kiip peab toimima ümbritseva keskkonna temperatuuride vahemikus – 25 °C kuni + 85 °C.	241 kuni 244, ECE R10, ISO/IEC 7810, ISO/IEC 10373

Nr	Katse	Kirjeldus	Seotud nõuded
		[Temperatuur ja niiskus] IC lisa punkt 4.4 „Keskkonnaalased ja elektrilised spetsifikatsioonid“, 241) Sõidumeerikukaardid suudavad nõuetekohaselt toimida kõigis ühenduse territooriumil tavaliselt esinevates kliimatingimustes ning vähemalt temperatuurivahemikus – 25 °C kuni + 70 °C aeg-ajalt esineva maksimumtemperatuuriga kuni + 85 °C, kusjuures „aeg-ajalt“ tähendab kuni neli tundi korraga ja kuni sada korda kaardi kasutusea jooksul. Sõidumeerikukaarte mõjutatakse järjestikustes etappides kindlaksmääratud aja jooksul järgmiste temperatuuride ja niiskustega. Pärast igat etappi kontrollitakse sõidumeerikukaartide elektriliste funktsioonide toimivust. 1. 2 tundi temperatuuril – 20 °C. 2. 2 tundi temperatuuril +/– 0 °C. 3. 2 tundi temperatuuril + 20 °C suhtelise õhuniiskusega 50 %. 4. 2 tundi temperatuuril + 50 °C suhtelise õhuniiskusega 50 %. 5. 2 tundi temperatuuril + 70 °C suhtelise õhuniiskusega 50 %. Temperatuur tõstetakse 60 minuti jooksul aeg-ajalt tasemele + 85 °C suhtelise õhuniiskusega 50 %. 6. 2 tundi temperatuuril + 70 °C suhtelise õhuniiskusega 85 %. Temperatuur tõstetakse 30 minuti jooksul aeg-ajalt tasemele + 85 °C suhtelise õhuniiskusega 85 %.	
		[Niiskus] IC lisa punkt 4.4 „Keskkonnaalased ja elektrilised spetsifikatsioonid“, 242) Sõidumeerikukaardid toimivad nõuetekohaselt õhuniiskuse vahemikus 10–90 %.	
		[Elektromagnetiline ühilduvus] IC lisa punkt 4.4 „Keskkonnaalased ja elektrilised spetsifikatsioonid“, 244) Toimimise ajal vastavad sõidumeerikukaardid Euroopa Majanduskomisjoni eeskirjale R10, mis käsitleb elektromagnetilist ühilduvust.	

Nr	Katse	Kirjeldus	Seotud nõuded
		[Staatiline elekter] IC lisa punkt 4.4 „Keskkonnaalased ja elektrilised spetsifikatsioonid“, 244) Toimimise ajal kaitstakse sõidumeerikukaarte elektrostaatiliste lahenduste eest. Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810:2003/Amd. 1: 2009 „Identimiskaardid. Füüsikalised omadused. 1. muudatus: Kiipe sisaldavate kaartide suhtes kohaldatavad kriteeriumid“: [9.4] Staatiline elekter [9.4.1] Kontaktkiipkaardid Katsepinge: 4 000 V.	
		[Röntgenkiirgus] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810:2003/Amd. 1: 2009 „Identimiskaardid. Füüsikalised omadused. 1. muudatus: Kiipe sisaldavate kaartide suhtes kohaldatavad kriteeriumid“: [9.1] Röntgenkiirgus.	
		[Ultraviolettkiirgus] ISO/IEC 10373-1:2006 „Identimiskaardid. Katsemeetodid. Osa 1: Üldised omadused“: [5.11] Ultraviolettkiirgus.	
		[Kolme ratta katse] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 10373-1:2006/Amd. 1: 2012 „Identimiskaardid. Katsemeetodid. Osa 1: Üldised omadused. 1. muudatus“: [5.22] Kiipkaardid – mehaaniline tugevus: kontaktidega kiipkaartide kolme ratta katse.	
		[Pakkimine] Sõidumeerikukaardid peavad vastama standardile MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: pakkimiskatse, tugevus [13.2.1.32] TM-422: mehaaniline töökindlus: pakkimiskatse	

Nr	Katse	Kirjeldus	Seotud nõuded
4.2	Mehaanilised katsed koos kaardile paigaldatud kiibimooduliga -> sama mis 2.3	[Painutamine] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810:2003/Amd. 1: 2009 „Identimiskaardid. Füüsikalised omadused. 1. muudatus: Kiipe sisaldavate kaartide suhtes kohaldatavad kriteeriumid“: [9.2] Dünaamiline paindepinge. Painutustsüklite koguarv: 4 000. [Väänamine] Sõidumeerikukaardid peavad vastama standardile ISO/IEC 7810:2003/Amd. 1: 2009 „Identimiskaardid. Füüsikalised omadused. 1. muudatus: Kiipe sisaldavate kaartide suhtes kohaldatavad kriteeriumid“: [9.3] Dünaamiline väändepinge. Väänamistsüklite koguarv: 4 000.	ISO/IEC 7810
5	**Protokolli katsed**		
5.1	ATR	Kontrollida, et ATR-signaal on nõuetekohane	ISO/IEC 7816-3, TCS_14, TCS_17, TCS_18
5.2	T=0	Kontrollida, et protokoll T=0 on nõuetekohane	ISO/IEC 7816-3, TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Kontrollida, et käsk PTS on nõuetekohane, vahetades protokolli T=0 protokolli T=1 vastu.	ISO/IEC 7816-3, TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Kontrollida, et protokoll T=1 on nõuetekohane	ISO/IEC 7816-3, TCS_11, TCS_13, TCS_16
6	**Kaardi struktuur**		
6.1		Katsetada, kas kaardi failistruktuur on nõuetekohane, kontrollides kohustuslike failide olemasolu kaardil ja nendele juurdepääsu tingimusi	TCS_22 kuni TCS_28, TCS_140 kuni TCS_179
7	**Funktsionaalsed katsed**		
7.1	Tavaline andmetöötlus	Katsetada vähemalt kord iga käsu lubatud 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 käsuga mõjutati).	TCS_29 kuni TCS_139

Nr	Katse	Kirjeldus	Seotud nõuded
7.2	Veasõnumid	Katsetada vähemalt kord iga käsu iga veasõnumit (vastavalt 2. liitele). Katsetada vähemalt kord iga üldviga (v.a '**6400**' terviklusvead, mida kontrollitakse turvalisuse sertifitseerimise ajal).	
7.3	Šifrikomplekt ja domeeni standardparameetrid		CSM_48, CSM_50
8	**Isikustamine**		
8.1	Optiline isikustamine	IC lisa punkt 4.1 „Nähtavad andmed“, 230) Esipoolel on: teave väljaantud kaardi kohta. IC lisa punkt 4.1 „Nähtavad andmed“, 231) Esipoolel on: kuupäev vormingus „pp/kk/aaaa“ või „pp.kk.aaaa“ (päev, kuu, aasta). IC lisa punkt 4.1 „Nähtavad andmed“, 235) Sõidumeerikukaartidel on vähemalt järgmised omadused, kaitsmaks neid võltsimise ja rikkumise eest: — foto piirkonnas kattuvad taustaturvamärk ja foto.	230, 231, 235

5. GNSSi VÄLISSEADME KATSED

Nr	Katse	Kirjeldus	Seotud nõuded
1.	**Halduskontroll**		
1.1	Dokumendid	Dokumentide õigsus	
2.	**GNSSi välisseadme visuaalne kontroll**		
2.1.	Vastavus dokumentidele		
2.2.	Tunnusmärgid/tähistused		224 kuni 226
2.3	Materjalid		219 kuni 223
3.	**Funktsionaalsed katsed**		
3.1	Anduri identimisandmed		98, 99
3.2	GNSSi välisseadme ja sõidukiseadme ühendamine		123, 205

Nr	Katse	Kirjeldus	Seotud nõuded
3.3	Asukoht GNSSi järgi		36, 37
3.4	Sõidukiseadme liides, kui GNSSi vastuvõtja asub väljaspool sõidukiseadet		03
3.5	Šifrikomplekt ja domeeni standardparameetrid		CSM_48, CSM_50
4.	**Keskkonnakatsed**		
4.1	Temperatuur	Funktsionaalsuse tõendamine järgmisel alusel: Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.1.1.2: talitluskatse madalal temperatuuril (72 h temperatuuril – 20 °C). Katse aluseks on standard IEC 60068-2-1: „Keskkonnakatsed. Osa 2-1: Katsed. Katse A: külm“. Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.1.2.2: talitluskatse kõrgel temperatuuril (72 h temperatuuril 70 °C). Katse aluseks on standard IEC 60068-2-2: „Põhilised keskkonnaalased katsemenetlused. Osa 2: Katsed. Katsed B: kuiv kuumus“. Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.3.2: kindla üleminekuajaga kiire temperatuurimuutus (– 20 °C/70 °C, 20 tsüklit, igal temperatuuril hoidmise aeg 1 h). Madalal temperatuuril, kõrgel temperatuuril ja temperatuuritsüklite ajal võib läbi viia vähendatud katsete kogumi (nende katsete puhul, mis on määratletud käesoleva tabeli 3. osas).	213
4.2	Niiskus	Tõendada standardi IEC 60068-2-30 katse Db alusel, et sõidukiseade suudab taluda tsüklilist niiskust (kuumuskatse) kuue 24-tunnise tsükli jooksul; igas tsüklis kõigub temperatuur vahemikus + 25 °C kuni + 55 °C ning suhteline niiskus on + 25 °C juures 97 % ja + 55 °C juures 93 %.	214
4.3	Mehaanilised omadused	1. Siinusvibratsioon: tõendada, et sõidukiseade suudab taluda järgmiste omadustega siinusvibratsiooni: püsinihe sagedusalas 5 kuni 11 Hz: maksimaalne 10 mm; püsikiirendus sagedusalas 11 kuni 300 Hz: 5 g. Seda nõuet tõendatakse standardi IEC 60068-2-6 katse Fc alusel; minimaalne katseaeg 3 × 12 tundi (12 tundi telje kohta). Standardi ISO 16750-3 kohaselt ei ole siinusvibratsiooni katse nõutav lahti haagitud sõiduki kabiinis asuvate seadmete puhul.	219

Nr	Katse	Kirjeldus	Seotud nõuded
		2. Juhuslik vibratsioon: Katse viiakse läbi vastavalt standardi ISO 16750-3 punktile 4.1.2.8: VIII katse: tarbesõiduk, lahti haagitud sõidukikabiin. Juhusliku vibratsiooni katse, 10…2 000 Hz, vertikaalsuuna ruutkeskmine 21,3 m/s², pikisuuna ruutkeskmine 11,8 m/s², külgsuuna ruutkeskmine 13,1 m/s², 3 telge, 32 h telje kohta, temperatuuritsükliga – 20…70 °C. Katse aluseks on standard IEC 60068-2-64: „Keskkonnakatsed. Osa 2-64: Katsed. Katse Fh: lairibas toimuv juhuslik vibratsioon ja juhised“. 3. Löögid: mehaaniline löök 3 g poolsiinusega vastavalt standardile ISO 16750. Eespool kirjeldatud katsed tehakse katsetatava seadmetüübi kahe erineva näidisega.	
4.4	Kaitse vee ja võõrkehade eest	Katse viiakse läbi vastavalt standardile ISO 20653: „Maanteesõidukid. Kaitseaste (IP-kood). Elektriseadmete kaitse võõrkehade, vee ja juurdepääsu eest“ (parameetrite muutusteta).	220, 221
4.5	Kaitse ülepinge eest	Tõendada, et sõidukiseade suudab taluda järgmist toitepinget: 24 V versioonid: 1 tund 34 V temperatuuril + 40 °C 12 V versioonid: 1 tund 17 V temperatuuril + 40 °C (ISO 16750-2 jaotis 4.3)	216
4.6	Kaitse polaarsuse vahetuse eest	Tõendada, et sõidukiseade suudab taluda toiteallika polaarsuse vahetust. (ISO 16750-2 jaotis 4.7)	216
4.7	Kaitse lühiste eest	Tõendada, et sisend-/väljundsignaalid on kaitstud lühiste eest toiteallikaga ja maaga. (ISO 16750-2 jaotis 4.10)	216
5	**Elektromagnetilise ühilduvuse katsed**		
5.1	Kiirgusemissioon ja vastuvõtlikkus	Vastavus eeskirjale ECE R10	218

Nr	Katse	Kirjeldus	Seotud nõuded
5.2	Elektrostaatiline lahendus	Vastavus standardile ISO 10605:2008 + tehniline parandus: 2010 + 1. muudatus: 2014: +/– 4 kV kontakti ja +/– 8 kV õhklahenduse korral	218
5.3	Juhtivuslike siirete vastuvõtlikkus vooluallikast	24 V versioonid: vastavus standardile ISO 7637-2 + ECE eeskirjale nr 10, red. 3: impulss 1a: Vs = – 450 V, Ri = 50 oomi impulss 2a: Vs = + 37 V, Ri = 2 oomi impulss 2a: Vs = + 20 V, Ri = 0,05 oomi impulss 3a: Vs = – 150 V, Ri = 50 oomi impulss 3a: Vs = + 150 V, Ri = 50 oomi impulss 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms impulss 5: Vs = + 120 V, Ri = 2,2 oomi, td = 250 ms 12 V versioonid: vastavus standardile ISO 7637-1 + ECE eeskirjale nr 10, red. 3: impulss 1: Vs = – 75 V, Ri = 10 oomi impulss 2a: Vs = + 37 V, Ri = 2 oomi impulss 2a: Vs = + 10 V, Ri = 0,05 oomi impulss 3a: Vs = – 112 V, Ri = 50 oomi impulss 3a: Vs = + 75 V, Ri = 50 oomi impulss 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms impulss 5: Vs = + 65 V, Ri = 3 oomi, td = 100 ms Impulssi 5 katsetatakse ainult nendel sõidukiseadmetel, mis on ette nähtud paigaldamiseks sõidukitele, millel puudub ühine väliskaitse koormuse avariilise vähenemise eest. Koormuse avariilise vähenemise ettepaneku kohta vt ISO 16750-2, 4. väljaanne, punkt 4.6.4.	218

6. KAUGSIDESEADME KATSED

Nr	Katse	Kirjeldus	Seotud nõuded
1.	**Halduskontroll**		
1.1	Dokumendid	Dokumentide õigsus	
2.	**Visuaalne kontroll**		
2.1.	Vastavus dokumentidele		
2.2.	Tunnusmärgid/tähistused		225, 226
2.3	Materjalid		219 kuni 223

Nr	Katse	Kirjeldus	Seotud nõuded
4.	**Keskkonnakatsed**		
4.1	Temperatuur	Funktsionaalsuse tõendamine järgmisel alusel: Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.1.1.2: talitluskatse madalal temperatuuril (72 h temperatuuril – 20 °C). Katse aluseks on standard IEC 60068-2-1: „Keskkonnakatsed. Osa 2-1: Katsed. Katse A: külm“. Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.1.2.2: talitluskatse kõrgel temperatuuril (72 h temperatuuril 70 °C). Katse aluseks on standard IEC 60068-2-2: „Põhilised keskkonnaalased katsemenetlused. Osa 2: Katsed. Katsed B: kuiv kuumus“. Katse viiakse läbi vastavalt standardi ISO 16750-4 punktile 5.3.2: kindla üleminekuajaga kiire temperatuurimuutus (– 20 °C/70 °C, 20 tsüklit, igal temperatuuril hoidmise aeg 1 h). Madalal temperatuuril, kõrgel temperatuuril ja temperatuuritsüklite ajal võib läbi viia vähendatud katsete kogumi (nende katsete puhul, mis on määratletud käesoleva tabeli 3. osas).	213
4.4	Kaitse vee ja võõrkehade eest	Katse viiakse läbi vastavalt standardile ISO 20653: „Maanteesõidukid. Kaitseaste (IP-kood). Elektriseadmete kaitse võõrkehade, vee ja juurdepääsu eest“ (sihtväärtus IP 40).	220, 221
5	**Elektromagnetilise ühilduvuse katsed**		
5.1	Kiirgusemissioon ja vastuvõtlikkus	Vastavus eeskirjale ECE R10	218
5.2	Elektrostaatiline lahendus	Vastavus standardile ISO 10605:2008 + tehniline parandus: 2010 + 1. muudatus: 2014: +/– 4 kV kontakti ja +/– 8 kV õhklahenduse korral	218
5.3	Juhtivuslike siirete vastuvõtlikkus vooluallikast	24 V versioonid: vastavus standardile ISO 7637-2 + ECE eeskirjale nr 10, red. 3: impulss 1a: Vs = – 450 V, Ri = 50 oomi impulss 2a: Vs = + 37 V, Ri = 2 oomi impulss 2a: Vs = + 20 V, Ri = 0,05 oomi impulss 3a: Vs = – 150 V, Ri = 50 oomi impulss 3a: Vs = + 150 V, Ri = 50 oomi impulss 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms impulss 5: Vs = + 120 V, Ri = 2,2 oomi, td = 250 ms	218

Nr	Katse	Kirjeldus	Seotud nõuded
		12 V versioonid: vastavus standardile ISO 7637-1 + ECE eeskirjale nr 10, red. 3: impulss 1: Vs = – 75 V, Ri = 10 oomi impulss 2a: Vs = + 37 V, Ri = 2 oomi impulss 2a: Vs = + 10 V, Ri = 0,05 oomi impulss 3a: Vs = – 112 V, Ri = 50 oomi impulss 3a: Vs = + 75 V, Ri = 50 oomi impulss 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms impulss 5: Vs = + 65 V, Ri = 3 oomi, td = 100 ms Impulssi 5 katsetatakse ainult nendel sõidukiseadmetel, mis on ette nähtud paigaldamiseks sõidukitele, millel puudub ühine väliskaitse koormuse avariilise vähenemise eest. Koormuse avariilise vähenemise ettepaneku kohta vt ISO 16750-2, 4. väljaanne, punkt 4.6.4.	

7. PABERI FUNKTSIONAALSED KATSED

Nr	Katse	Kirjeldus	Seotud nõuded
1.	**Halduskontroll**		
1.1	Dokumendid	Dokumentide õigsus	
2	**Üldised katsed**		
2.1	Märkide arv rea kohta	Väljatrükkide visuaalne kontroll	172
2.2	Märgi minimaalne suurus	Väljatrüki visuaalne kontroll ja märkide kontroll	173
2.3	Toetatud märgistikud	Printer peab toetama 1. liite 4. peatükis „Märgistikud“ kirjeldatud märgistikke.	174
2.4	Väljatrükkide selgus	Sõidumeeriku tüübikinnituse kontrollimine ja väljatrükkide visuaalne kontroll	174
2.5	Väljatrükkide loetavus ja identimistunnused	Väljatrükkide kontroll. Tõendatakse tootja katsearuannete ja katseprotokollidega. Printeripaberiga kasutamiseks lubatud sõidumeerikute loanumbrid prinditakse paberile.	175, 177, 178
2.6	Käsitsi kirjutatud märkuste lisamine	Visuaalne kontroll: juhi allkirja väli on kasutatav. Muude käsitsi kirjutatud kannete väljad on kasutatavad.	180

Nr	Katse	Kirjeldus	Seotud nõuded
2.7	Täiendavad üksikasjad paberi esikülje kohta	Paberi esi- ja tagakülg võivad sisaldada täiendavaid üksikasju ja lisateavet. Sellised täiendavad üksikasjad ja teave ei tohi halvendada väljatrükkide loetavust. Visuaalne kontroll.	177, 178
3	**Säilitamiskatsed**		
3.1	Kuiv kuumus	Ettevalmistus: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %. Katsekeskkond: 72 tundi temperatuuril + 70 °C ± 2 °C. Taastumine: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %.	176, 178, IEC 60068-2-2-Bb
2.2	Niiske kuumus	Ettevalmistus: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %. Katsekeskkond: 144 tundi temperatuuril + 55 °C ± 2 °C/ suhtelisel õhuniiskusel 93 % ± 3 %. Taastumine: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %.	176, 178, IEC 60068-2-78-Cab
4	**Paberi kasutuskatsed**		
4.1	Üldine vastupidavus niiskusele (trükikirjata paber)	Ettevalmistus: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %. Katsekeskkond: 144 tundi temperatuuril + 55 °C ± 2 °C/ suhtelisel õhuniiskusel 93 % ± 3 %. Taastumine: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %.	176, 178, IEC 60068-2-78-Cab
4.2	Trükitavus	Ettevalmistus: 24 tundi temperatuuril + 40 °C ± 2 °C/suhtelisel õhuniiskusel 93 % ± 3 %. Katsekeskkond: väljatrükk tehakse temperatuuril + 23 °C ± 2 °C. Taastumine: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %.	176, 178
4.3	Vastupidavus kuumusele	Ettevalmistus: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %. Katsekeskkond: 2 tundi temperatuuril + 70 °C ± 2 °C, kuiv kuumus. Taastumine: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %.	176, 178, IEC 60068-2-2-Bb
4.4	Vastupidavus madalale temperatuurile	Ettevalmistus: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %. Katsekeskkond: 24 tundi temperatuuril – 20 °C ± 3 °C, kuiv külm temperatuur. Taastumine: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %.	176, 178, ISO 60068-2-1-Ab

Nr	Katse	Kirjeldus	Seotud nõuded
4.5	Valguskindlus	Ettevalmistus: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %. Katsekeskkond: 100 tundi valgustugevusel 5 000 lx temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %. Taastumine: 16 tundi temperatuuril + 23 °C ± 2 °C/suhtelisel õhuniiskusel 55 % ± 3 %.	176, 178

Katsete 3.x ja 4.x loetavuse kriteeriumid:

Väljatrüki loetavus on tagatud, kui optiline tihedus vastab järgmistele piirnormidele:

Trükitud märgid: vähemalt 1,0.

Taust (trükikirjata paber): maksimaalselt 0,2.

Väljatrükkide optilist tihedust mõõdetakse vastavalt standardile DIN EN ISO 534.

Väljatrükkide mõõtmed ei tohi muutuda ja need peavad jääma selgelt loetavaks.

8. KOOSTALITLUSVÕIME KATSED

Nr	Katse	Kirjeldus
9.1 Sõidukiseadmete ja sõidumeerikukaartide koostalitlusvõime katsed		
1	Vastastikune autentimine	Kontrollida, et sõidukiseadme ja sõidumeerikukaardi vaheline vastastikune autentimine toimiks normaalselt.
2	Kirjutamise/lugemise katsed	Sooritada sõidukiseadmega tüüpiline tegevuste jada. Tegevusjada kohandatakse katsetatava kaarditüübiga ning see hõlmab kirjutamist võimalikult paljudesse kaardi elementaarfailidesse. Kontrollida sõidukiseadmest allalaadimise teel, et kõik vastavad kirjed on nõuetekohaselt tehtud. Kontrollida kaardilt allalaadimise teel, et kõik vastavad kirjed on nõuetekohaselt tehtud. Kontrollida kaardi igapäevaste väljatrükkide alusel, et kõiki vastavaid kirjeid saab nõuetekohaselt lugeda.
9.2 Sõidukiseadmete ja liikumisandurite koostalitlusvõime katsed		
1	Ühendamine	Kontrollida, et sõidukiseadme ja liikumisanduri ühendamine toimiks normaalselt.
2	Tegevuskatsed	Sooritada liikumisanduriga tüüpiline tegevuste jada. Tegevusjadas kasutatakse tavapäraseid tegevusi ning luuakse võimalikult palju sündmusi või vigu. Kontrollida sõidukiseadmest allalaadimise teel, et kõik vastavad kirjed on nõuetekohaselt tehtud. Kontrollida kaardilt allalaadimise teel, et kõik vastavad kirjed on nõuetekohaselt tehtud. Kontrollida päeva väljatrüki alusel, et kõiki vastavaid kirjeid saab nõuetekohaselt lugeda.

Nr	Katse	Kirjeldus
9.3 Sõidukiseadme ja GNSSi välisseadme (kui see on olemas) koostalitlusvõime katsed		
1	Vastastikune autentimine	Kontrollida, et sõidukiseadme ja GNSSi välisseadme vaheline vastastikune autentimine (ühendamine) toimiks normaalselt.
2	Tegevuskatsed	Sooritada GNSSi välisseadmega tüüpiline tegevuste jada. Tegevusjadas kasutatakse tavapäraseid tegevusi ning luuakse võimalikult palju sündmusi või vigu. Kontrollida sõidukiseadmest allalaadimise teel, et kõik vastavad kirjed on nõuetekohaselt tehtud. Kontrollida kaardilt allalaadimise teel, et kõik vastavad kirjed on nõuetekohaselt tehtud. Kontrollida päeva väljatrüki alusel, et kõiki vastavaid kirjeid saab nõuetekohaselt lugeda.

10. liide

TURVANÕUDED

Käesolevas liites on määratletud aruka sõidumeeriku süsteemi (teise põlvkonna sõidumeeriku) komponentide IT-turvalisuse nõuded.

SEC_001 Vastavalt ühiste kriteeriumide kavale sertifitseeritakse aruka sõidumeeriku süsteemi järgmiste komponentide turvalisus:

— sõidukiseade,

— sõidumeerikukaart,

— liikumisandur,

— GNSSi välisseade.

SEC_002 Vastavalt ühiste kriteeriumide kavale määratletakse iga turvalisuse sertifitseerimist vajava komponendi suhtes kohaldatavad IT-turvalisuse miinimumnõuded asjaomase komponendi kaitseprofiilis.

SEC_003 Euroopa Komisjon tagab käesoleva lisa kohase nelja kaitseprofiili rahastamise, väljatöötamise, nende heakskiitmise Euroopa SOGIS-MRA (infotehnoloogia valdkonnas turvalisuse hindamise sertifikaatide vastastikuse tunnustamise kokkulepe) raames sertifikaatide vastastikust tunnustamist toetavasse ühise tõlgendamise töörühma (*Joint Interpretation Working Group*, JIWG) koondunud valitsusasutustes, kes vastutavad IT-turvalisuse sertifitseerimise eest, ning nende profiilide registreerimise:

— sõidukiseadme kaitseprofiil,

— sõidumeerikukaardi kaitseprofiil,

— liikumisanduri kaitseprofiil,

— GNSSi välisseadme kaitseprofiil.

Sõidukiseadme kaitseprofiil peab olema kohaldatav nii koos GNSSi välisseadmega kasutamiseks ette nähtud kui ka ilma selleta kasutatava sõidukiseadme puhul. Esimesel juhul nähakse GNSSi välisseadme turvanõuded ette eraldi kaitseprofiilis.

SEC_004 Komponendi tootja täpsustab vajaduse korral asjaomase komponendi kaitseprofiili ja koostab lõpliku profiili, muutmata või kustutamata seejuures spetsifikatsioone olemasolevate ohtude, eesmärkide, menetluskorra ja turvalisuse tagamise funktsioonide kohta, et püstitada turbe-eesmärk, mille jaoks ta soovib taotleda komponendi turvalisuse sertifitseerimist.

SEC_005 Hindamisprotsessi käigus tuleb kinnitada sellise konkreetse turbe-eesmärgi ranget vastavust asjaomasele kaitseprofiilile.

SEC_006 Iga kaitseprofiili usaldusväärsus on tasemel EAL4 ning seda võimendavad usaldusväärsuse komponendid ATE_DPT.2 ja AVA_VAN.5.

11. liide

ÜHISED TURBEMEHHANISMID

SISUKORD

PREAMBUL

Käesolevas liites on määratletud turbemehhanismid, millega tagatakse:

— sõidumeerikusüsteemi eri osade vastastikune autentimine;

— sõidumeerikusüsteemi eri osade vahel edastatud või välisandmekandjale alla laaditud andmete konfidentsiaalsus, terviklus, autentsus ja/või ümberlükkamatus.

Liide koosneb kahest osas. A osas määratletakse esimese põlvkonna sõidumeerikusüsteemi (digitaalne sõidumeerik) turbemehhanismid. B osas määratletakse teise põlvkonna sõidumeerikusüsteemi (arukas sõidumeerik) turbemehhanismid.

Liite A osas määratletud mehhanisme kohaldatakse juhul, kui vähemalt üks vastastikuse autentimise ja/või andmeedastuse protsessis osalev sõidumeerikusüsteemi osa kuulub esimesse põlvkonda.

Liite B osas määratletud mehhanisme kohaldatakse juhul, kui mõlemad vastastikuse autentimise ja/või andmeedastuse protsessis osalevad sõidumeerikusüsteemi osad kuuluvad teise põlvkonda.

15. liites on esitatud lisateave esimese põlvkonna osade kasutamise kohta koos teise põlvkonna osadega.

A OSA

ESIMESE PÕLVKONNA SÕIDUMEERIKUSÜSTEEM

1. SISSEJUHATUS

1.1. **Viited**

Käesolevas liites kasutatakse järgmisi viiteid.

SHA-1	National Institute of Standards and Technology (NIST). *FIPS Publication 180-1: Secure Hash Standard*, aprill 1995
PKCS1	RSA Laboratories. PKCS # 1: *RSA Encryption Standard*. Versioon 2.0, oktoober 1998.
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3: Data Encryption Standard*, projekt 1999
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation, 1998
ISO/IEC 7816-4	*Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interexchange* („Infotehnoloogia. Identimiskaardid. Kontaktidega kiipkaardid. Osa 4: Valdkondadevahelised andmevahetuskäsud“). 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* („Infotehnoloogia. Identimiskaardid. Kontaktidega kiipkaardid. Osa 6: Valdkondadevahelised andmeelemendid“). 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* („Infotehnoloogia. Identimiskaardid. Kontaktidega kiipkaardid. Osa 8: 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* („Infotehnoloogia. Turvameetodid. Digitaalallkirjad, mille abil saab taastada sõnumeid. Osa 2: Räsifunktsiooni kasutavad mehhanismid“). Esimene väljaanne, 1997
ISO/IEC 9798-3	*Information Technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm* („Infotehnoloogia. Turvameetodid. Üksuse autentimise mehhanismid. Osa 3: Üksuse autentimine avaliku võtme algoritmiga“). Teine väljaanne, 1998
ISO 16844-3	*Road vehicles – Tachograph systems – Part 3: Motion sensor interface* („Maanteesõidukid. Sõidumeerikusüsteemid. Osa 3: Liikumisanduri liides“).

1.2. **Märkused ja lühendid**

Käesolevas liites kasutatakse järgmisi märkusi ja lühendeid.

(Ka, Kb, Kc)	võtmekimp, mida kasutab kolmekordse krüpteerimise algoritm
CA	(*certification authority*) sertifitseerimisasutus
CAR	(*certification authority reference*) sertifitseerimisasutuse viide
CC	(*cryptographic checksum*) krüptograafiline kontrollsumma
CG	(*cryptogram*) krüptogramm
CH	(*command header*) käsu päis
CHA	(*certificate holder authorisation*) sertifikaadi omaniku luba
CHR	(*certificate holder reference*) sertifikaadi omaniku viide
D()	dekrüpteerimine algoritmiga DES

DE	(*data element*) andmeelement
DO	(*data object*) andmeobjekt
d	RSA privaatvõti, isiklik astendaja
e	RSA avalik võti, avalik astendaja
E()	krüpteerimine algoritmiga DES
EQT	(*equipment*) seade
Hash()	räsiväärtus, räsifunktsiooni väljund
Hash	räsifunktsioon
KID	(*key identifier*) võtme identifikaator
Km	TDES-võti. Standardis ISO 16844-3 määratletud peavõti
Km_{VU}	sõidukiseadmesse sisestatud TDES-võti
Km_{WC}	töökojakaarti sisestatud TDES-võti
m	sõnumit esindav täisarv vahemikus 0 kuni *n*– 1
n	RSA võtmed, moodul
PB	(*padding bytes*) täidisbaidid
PI	(*padding indicator byte*) täidise indikaatorbait (krüptogrammis kasutamiseks seoses andmeobjektide konfidentsiaalsusega)
PV	(*plain value*) lihtväärtus
s	allkirja esindav täisarv vahemikus 0 kuni *n* – 1
SSC	(*send sequence counter*) saatejada loendur
SM	(*secure messaging*) turvaline sõnumivahetus
TCBC	kolmekordse krüpteerimise algoritmi šifriplokki aheldav toimimisrežiim
TDEA	(*triple data encryption algorithm*) kolmekordse krüpteerimise algoritm
TLV	(*tag length value*) sildi pikkuse väärtus
VU	(*vehicle unit*) sõidukiseade
X.C	sertifitseerimisasutuse välja antud sertifikaat kasutajale X
X.CA	kasutaja X sertifitseerimisasutus
$X.CA.PK \circ X.C$	sertifikaadi lahtipakkimise toiming avaliku võtme eraldamiseks. See on infiksoperaator, mille vasakpoolne operand on sertifitseerimisasutuse avalik võti ja parempoolne operand selle sertifitseerimisasutuse välja antud sertifikaat. Tulemuseks on selle kasutaja X avalik võti, kelle sertifikaat on parempoolne operand
X.PK	kasutaja X RSA avalik võti
X.PK[I]	info I RSA krüpteerimine kasutaja X avaliku võtme abil
X.SK	kasutaja X RSA privaatvõti
X.SK[I]	info I RSA krüpteerimine kasutaja X privaatvõtme abil
‘xx’	väärtus kuueteistkümnendsüsteemis
||	konkatenatsioonioperaator

2. KRÜPTOGRAAFILISED SÜSTEEMID JA ALGORITMID

2.1. **Krüptograafilised süsteemid**

CSM_001 Sõidukiseadmed ja sõidumeerikukaardid kasutavad klassikalist RSA avaliku võtme krüptograafilist süsteemi järgmiste turbemehhanismide jaoks:

— autentimine sõidukiseadme ja kaardi vahel,

— kolmekordsete DES seansivõtmete transport sõidukiseadme ja sõidumeerikukaardi vahel,

— sõidukiseadmest või sõidumeerikukaardilt välisandmekandjale alla laaditud andmete digitaalallkirjastamine.

CSM_002 Sõidukiseadmed ja sõidumeerikukaardid kasutavad kolmekordset DES sümmeetrilist krüptograafilist süsteemi andmete terviklusmehhanismi rakendamiseks sõidukiseadme ja sõidumeerikukaardi vahelise andmevahetuse ajal ning vajaduse korral sõidukiseadme ja sõidumeerikukaardi vahelise andmevahetuse konfidentsiaalsuse tagamiseks.

2.2. **Krüptograafilised algoritmid**

2.2.1. *RSA algoritm*

CSM_003 RSA algoritm on täielikult määratletud järgmiste suhetega:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

RSA põhjalikum kirjeldus on esitatud viites PKCS1. Avalik astendaja e on RSA arvutuste puhul täisarv vahemikus 3 kuni n-1, mis vastab tingimusele gcd(e, lcm(p-1, q-1)) = 1.

2.2.2. *Räsialgoritm*

CSM_004 Digitaalallkirja mehhanismide puhul kasutatakse SHA-1 räsialgoritmi, mida on kirjeldatud viites SHA-1.

2.2.3. *Andmete krüpteerimise algoritm*

CSM_005 DES-il põhinevaid algoritme kasutatakse šifriplokki aheldavas toimimisrežiimis.

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.

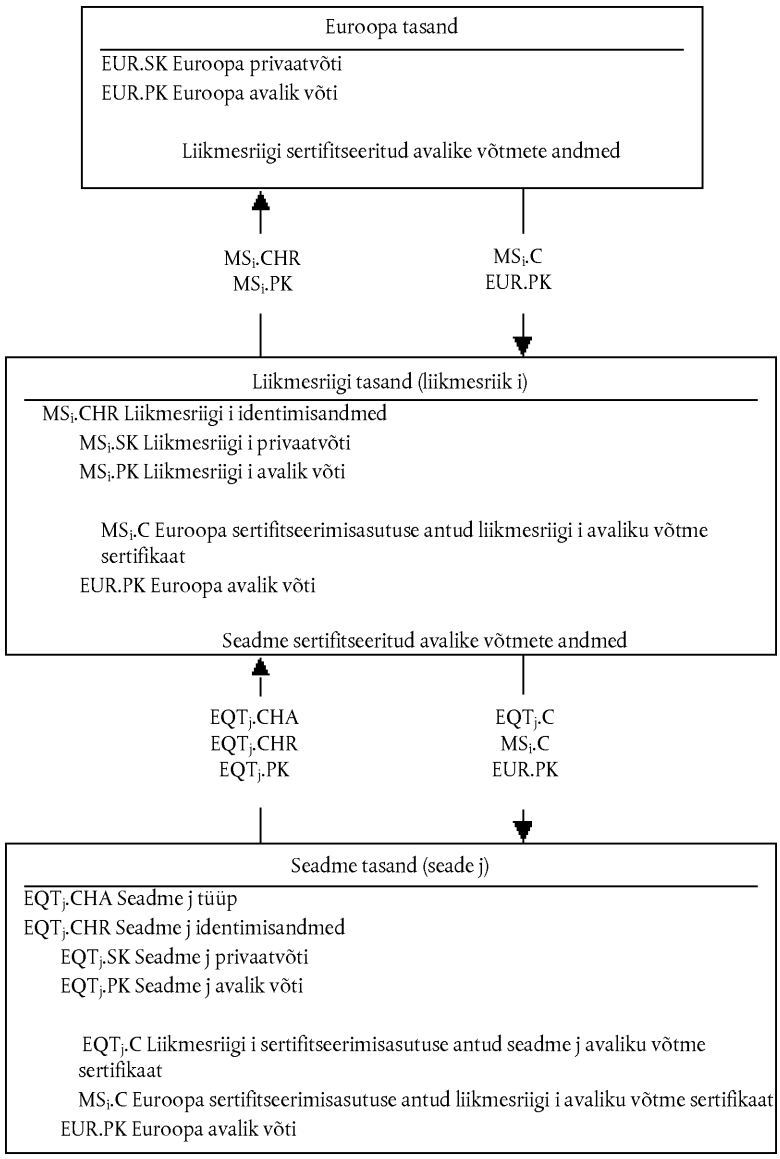
CSM_007 Euroopa tasandil luuakse ühtne Euroopa võtmepaar (EUR.SK ja EUR.PK). Euroopa privaatvõtit kasutatakse liikmesriikide avalike võtmete muutmiseks. Säilitatakse andmed kõigi sertifitseeritud võtmete kohta. Sellega tegeleb Euroopa Komisjoni volitusel ja vastutusel Euroopa sertifitseerimisasutus.

CSM_008 Liikmesriigi tasandil luuakse liikmesriigi võtmepaar (MS.SK ja MS.PK). Liikmesriikide avalikud võtmed sertifitseerib Euroopa sertifitseerimisasutus. Liikmesriigi avalikku võtit kasutatakse seadmesse (sõidukiseade või sõidumeerikukaart) sisestatavate avalike võtmete sertifitseerimiseks. Säilitatakse andmed kõigi sertifitseeritud avalike võtmete kohta koos selle seadme identimisandmetega, mille jaoks võti on ette nähtud. 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 võib tegelda seadme tootja, seadme isikustaja või liikmesriigi sertifitseerimisasutus. Seda võtmepaari kasutatakse autentimiseks, digitaalallkirjastamiseks ja krüpteerimisteenuste jaoks.

CSM_010 Privaatvõtmete loomise, transpordi (kui see toimub) ja salvestamise ajal säilitatakse nende konfidentsiaalsus.

Järgmisel joonisel on kokkuvõtlikult esitatud selle protsessi andmevoog.



3.1.2. *RSA katsevõtmed*

CSM_011 Seadme katsetamise eesmärgil (sealhulgas koostalitlusvõime katsed) loob Euroopa sertifitseerimisasutus erineva ühtse Euroopa katsevõtmepaari ja vähemalt kaks liikmesriigi katsevõtmepaari, mille avalikud võtmed sertifitseeritakse Euroopa privaatkatsevõtmega. Tootja sisestab tüübikinnituskatseid läbivasse seadmesse liikmesriigi ühe nimetatud katsevõtme abil sertifitseeritud katsevõtmed.

3.1.3. *Liikumisanduri võtmed*

Allpool kirjeldatud kolme TDES võtme loomise, transpordi (kui see toimub) ja salvestamise ajal säilitatakse nende konfidentsiaalsus.

Toetamaks standardile ISO 16844 vastavaid sõidumeerikuosi, tagavad Euroopa sertifitseerimisasutus ja liikmesriigi sertifitseerimisasutused muu hulgas järgmise.

CSM_036 Euroopa sertifitseerimisasutus loob kaks iseseisvat ja kordumatut kolmekordset DES võtit KmVU ja KmWC ja loob Km: $Km = Km_{VU}$ XOR Km_{WC} . Euroopa sertifitseerimisasutus edastab need võtmed kohases turvalises korras liikmesriikide sertifitseerimisasutustele nende taotlusel.

CSM_037 Liikmesriikide sertifitseerimisasutused:

— kasutavad liikumisanduri tootja taotluse kohaseks liikumisanduri andmete krüpteerimiseks Km (Km-ga krüpteeritavad andmed on määratletud standardis ISO 16844-3),

— edastavad kohases turvalises korras sõidukiseadme tootjale Km_{VU} selle sisestamiseks sõidukiseadmesse,

— tagavad Km_{WC} sisestamise kõigile töökojakaartidele (elementaarfaili `Sensor_Installation_Data` andmeväljale `SensorInstallationSecData`) kaardi isikustamise käigus.

3.1.4. *T-DES seansivõtmete loomine ja jagamine*

CSM_012 Sõidukiseadmed 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, kus kasutatakse turvalist sõnumivahetust. Selle kehtivus lõpeb seansi lõpus (kaardi väljavõtmine või kaardi lähtestus) ja/või pärast 240 kasutuskorda (võtme üks kasutus = üks turvalist sõnumivahetust kasutav kaardile saadetud käsk ja vastus sellele).

3.2. **Võtmed**

CSM_014 RSA võtmetel on (tasandist olenemata) järgmised pikkused: moodul *n* 1 024 bitti, avalik astendaja *e* maksimaalselt 64 bitti, isiklik astendaja *d* 1 024 bitti.

CSM_015 Kolmekordsete DES võtmete kuju on (K_a, K_b, K_a), kus K_a ja K_b on sõltumatud 64-bitise pikkusega võtmed. Paarsusbitte ei lisata.

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 väärtusega „FF“.
CHR	OCTET STRING	8	Sertifikaadi omaniku viide
n	OCTET STRING	128	Avalik võti (moodul)
e	OCTET STRING	8	Avalik võti (avalik astendaja)
		164	

Märkused

1. Sertifikaadi profiili identifikaator (CPI) sätestab autentimissertifikaadi täpse struktuuri. Seda võib kasutada seadmesiseselt 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)	Järgnevate andmeobjektide pikkus	Mooduli silt	Mooduli pikkus	Avaliku astendaja silt	Avaliku astendaja pikkus

2. Sertifitseerimisasutuse viite (CAR) eesmärk on identida sertifikaadi välja andnud sertifitseerimisasutus nii, et seda andmeelementi saab kasutada asutuse võtmeidentifikaatoriga samaaegselt, et viidata sertifitseerimisasutuse avalikule võtmele (kodeerimiseks vt allpool „Võtme identifikaator“).

3. Sertifikaadi omaniku volitusi (CHA) kasutatakse sertifikaadi omaniku õiguste identimiseks. See koosneb sõidumeerikurakenduse identimisandmetest ja seadme tüübist, mille jaoks sertifikaat on ette nähtud (vastavalt andmeelemendile `EquipmentType`, liikmesriigi jaoks '00').

4. Sertifikaadi omaniku viite (CHR) eesmärk on identida üheselt sertifikaadi omanik nii, et seda andmeelementi saab kasutada subjekti võtmeidentifikaatoriga samaaegselt, et viidata sertifikaadi omaniku avalikule võtmele.

5. Võtmeidentifikaatorid identivad üheselt sertifikaadi omaniku või sertifitseerimisasutuse. Need kodeeritakse järgmiselt.

5.1 Seade (sõidukiseade või kaart):

Andmed	Seadme seerianumber	Kuupäev	Tüüp	Tootja
Pikkus	4 baiti	2 baiti	1 bait	1 bait
Väärtus	Täisarv	kk aa kahend-kümnendkoodis	Tootjaomane	Tootja kood

Sõidukiseadme puhul võib tootja sertifikaatide taotlemisel teada või mitte teada selle seadme identimisandmeid, millesse võtmed sisestatakse.

Esimesel juhul saadab tootja seadme identimisandmed koos avaliku võtmega oma liikmesriigi asutusele sertifitseerimiseks. Sertifikaat sisaldab sel juhul seadme identimisandmeid ja tootja peab tagama, et võtmed ja sertifikaat sisestatakse selleks ette nähtud seadmesse. Võtmeidentifikaatoril on eespool näidatud kuju.

Teisel juhul peab tootja üheselt identima iga sertifikaadi taotluse ja saatma selle identimisandmed koos avaliku võtmega oma liikmesriigi asutusele sertifitseerimiseks. Sertifikaat sisaldab taotluse identimisandmeid. Pärast võtme paigaldamist seadmesse peab tootja andma oma liikmesriigi asutusele tagasisidet võtme määramise kohta seadmele (st sertifikaadi taotluse identimisandmed, seadme identimisandmed). Võtmeidentifikaatoril on järgmine kuju:

Andmed	Sertifitseerimistaotluse seerianumber	Kuupäev	Tüüp	Tootja
Pikkus	4 baiti	2 baiti	1 bait	1 bait
Väärtus	Täisarv	kk aa kahend-kümnendkoodis	'FF'	Tootja kood

5.2 Sertifitseerimisasutus:

Andmed	Asutuse identimistunnus	Võtme seerianumber	Lisainfo	Identifikaator
Pikkus	4 baiti	1 bait	2 baiti	1 bait

Väärtus	1 bait: riigi numbriline kood 3 baiti: riigi tähtnumbriline kood	Täisarv	Lisakood (CA-omane) 'FF', kui ei kasutata	'01'

Võtme seerianumbrit kasutatakse liikmesriigi eri 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 määratlemiseks objekti identifikaatorit).

3.3.2. *Väljaantud sertifikaadid*

CSM_018 Väljaantud sertifikaat on vastavalt standardile ISO/IEC 9796-2 (välja arvatud selle lisa A.4) digitaalallkiri koos osaliselt korratud sertifikaadi sisuga, millele on liidetud sertifitseerimisasutuse viide.

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

$$\text{Sertifikaadi sisu} = Cc = \underset{106\text{ baiti}}{C_r} \,||\, \underset{58\text{ baiti}}{C_n}$$

Märkused

1. See sertifikaat on 194 baiti pikk.

2. Allkirja peidetud CAR on ühtlasi allkirjale liidetud, 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 silt (konstrueeritud)	Järgnevate andmeobjektide pikkus	Allkirja silt	Allkirja pikkus	Jäägi silt	Jäägi pikkus	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 $_{o}$ X.C, ning sertifikaadi kehtivuse tõendamisest.

CSM_019 See hõlmab järgmisi samme.

Allkirja tõendamine ja sisu väljaotsimine:

— X.C-st välja otsida allkiri, Cn' ja CAR': X.C = Allkiri || C_n' || 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 [Sign],

— kontrollida, et Sr' alguses oleks '6A' ja lõpus 'BC',

— arvutada C_r' ja H' avaldisest: Sr' = '6A' || C_r' || H' || 'BC'

106 baiti 20 baiti

— taastada sertifikaadi sisu C' = C_r' || C_n',

— kontrollida, et *Hash*(C') = H'.

Kui kontroll läbitakse edukalt, 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* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV.

4. VASTASTIKUSE AUTENTIMISE MEHHANISM

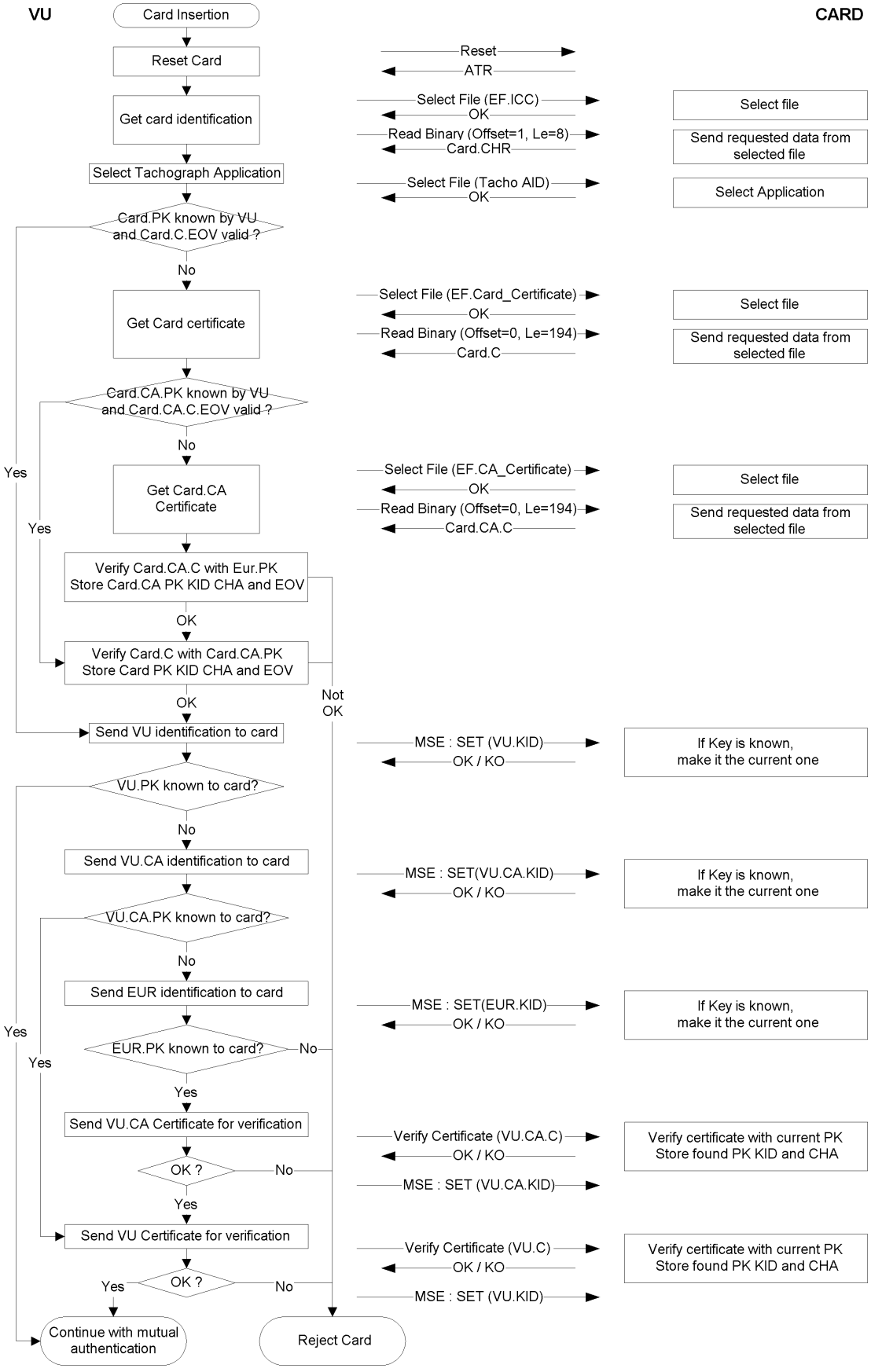
Kaartide ja sõidukiseadmete vaheline vastastikune autentimine põhineb järgmisel põhimõttel.

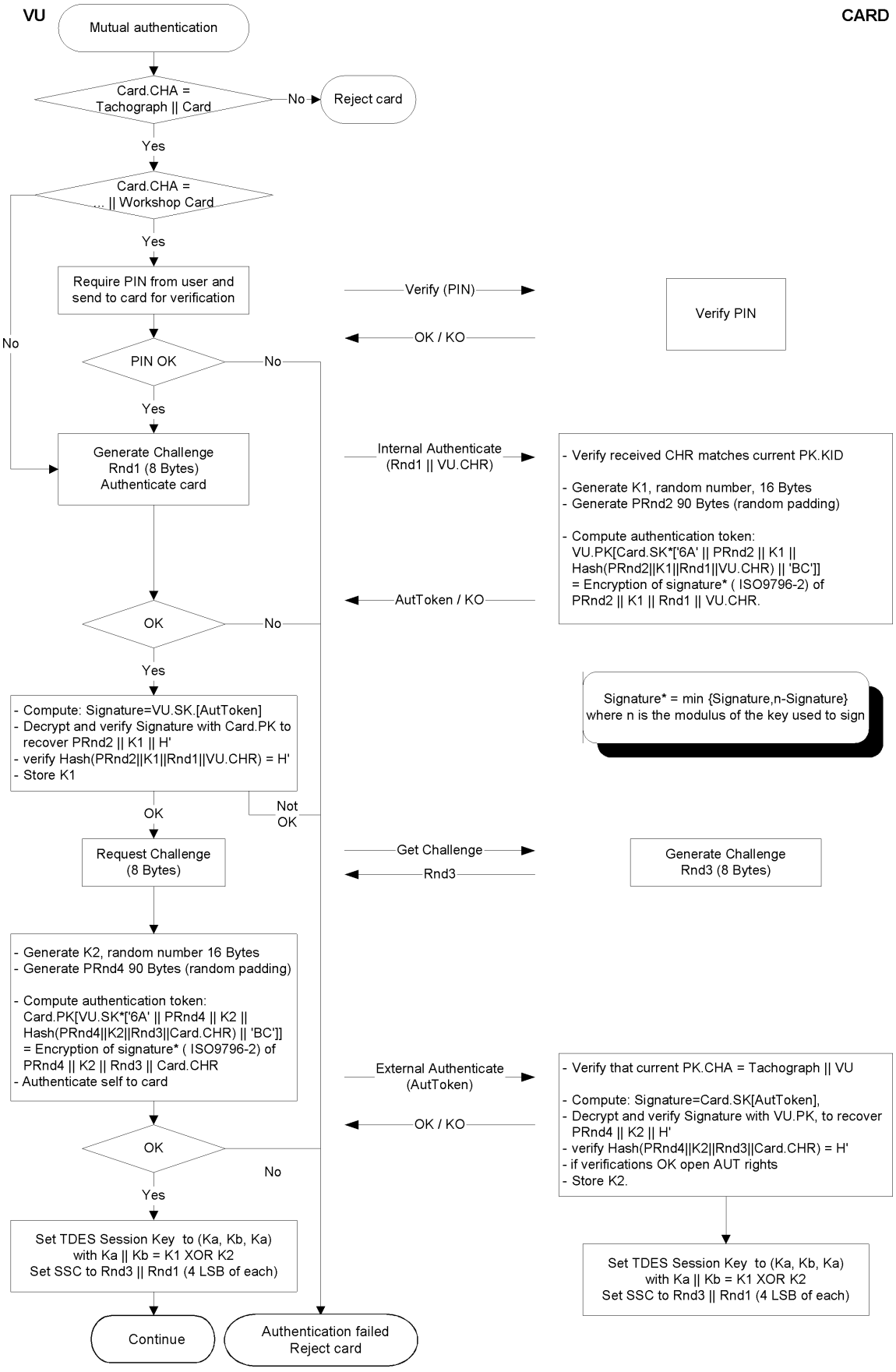
Kumbki pool tõendab teisele, et sel on kehtiv võtmepaar, millest avaliku võtme on sertifitseerinud liikmesriigi sertifitseerimisasutus, mille omakorda on sertifitseerinud Euroopa sertifitseerimisasutus.

Tõendamiseks allkirjastatakse isikliku võtmega juhuslik number, mille on saatnud teine pool, mis peab saadetud juhusliku numbri allkirja kontrollimisel taastama.

Mehhanism käivitub kaardi sisestamisel sõidukiseadmesse. See algab sertifikaatide vahetamise ja avalike võtmete lahtipakkimisega ning lõpeb seansivõtme loomisega.

CSM_020 Kasutatakse järgmist protokolli (nooled näitavad käske ja vahetatavaid andmeid (vt 2. liide)).




VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
No
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. SÕIDUKISEADME JA KAARTIDE VAHELISES ANDMEEDASTUSES KASUTATAVAD KONFIDENTSIAALSUSE, TERVIKLUSE JA AUTENTIMISE MEHHANISMID

5.1. **Turvaline sõnumivahetus**

CSM_021 Sõidukiseadme ja kaartide vahelises andmeedastuses kaitstakse andmete terviklust turvalise sõnumivahetusega vastavalt standarditele 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 kontrollib krüptograafilist kontrollsummat.

CSM_023 Käsuga saadetud andmete krüptograafiline kontrollsumma hõlmab käsu päist ja kõiki saadetud andmeelemente (= > CLA = '0C', ning kõik andmeobjektid ümbritsetakse 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 turvalise sõnumivahetuse kasutamise korral järgmine.

Kasutatud andmeobjektid on standardis ISO/IEC 7816-4 kirjeldatud turvalise sõnumivahetuse andmeobjektide osa:

Silt	Mnemooniline nimi	Tähendus
'81'	T_{PV}	Lihtväärtus, mida ei ole kodeeritud BER-TLV-s (kaitstakse CCga)
'97'	$\mathbf{T_{LE}}$	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 (BER-TLV-s kodeerimata lihtväärtus)

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 B1 kuni BL		

Vastuse sisu	Vastuse saba	
[Andmeväli]	SW1	SW2
L_r andmebaidid	kaks baiti	

Vastav turvatud käsu-vastuse paar on:

Turvatud käsk:

Käsu päis (CH)				Käsu sisu										
CLA	INS	P1	P2	(Uus L_c-väli)	[Uus andmeväli]									[Uus L_e-väli]
'OC'				Uue andmevälja pikkus	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
					'81'	L_c	And-meväli	'97'	'01'	L_e	'8E'	'04'	CC	

Kontrollsummasse lisatavad andmed = 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 2. meetodile.

Andmeobjektid PV ja LE on olemas ainult siis, kui turvamata käsus on mõned vastavad andmed.

Turvatud 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	Andmeväli	'8E'	'04'	CC	

Kontrollsummasse lisatavad andmed = 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-s kodeerimata andmed ja täidisbaidid.

Kontrollsummasse lisatavad andmed = $T_{PI\ CG}$ || $L_{PI\ CG}$ || 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	

Kontrollsummasse lisatavad andmed = T_{SW} || L_{SW} || SW || PB

5.2. **Turvalise sõnumivahetuse vigade töötlemine**

CSM_026 Kui sõidumeerikukaart tuvastab käsu tõlgendamise ajal ära turvalise sõnumivahetuse vea, tuleb olekubaidid tagasi saata ilma turvalise sõnumivahetuseta. 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 sõidukiseade seansi lõpetama.

5.3. **Krüptograafiliste kontrollsummade arvutusalgoritm**

CSM_028 Krüptograafiliste kontrollsummade koostamisel kasutatakse *retail* MAC tüüpi sõnumi tõendamise kontrollsummasid vastavalt standardile ANSI X9.19 koos DES koodiga:

— esimene etapp: esimese kontrollploki y0 on E(Ka, SSC),

— järgmised etapid: kontrollplokkide y1, .., yn arvutamiseks kasutatakse Ka,

— lõppetapp: krüptograafiline kontrollsumma arvutatakse viimasest kontrollplokist yn järgmiselt: E(Ka, D(Kb, yn)),

kus E() tähendab krüpteerimist DES koodiga ja D() tähendab dekrüpteerimist DES koodiga.

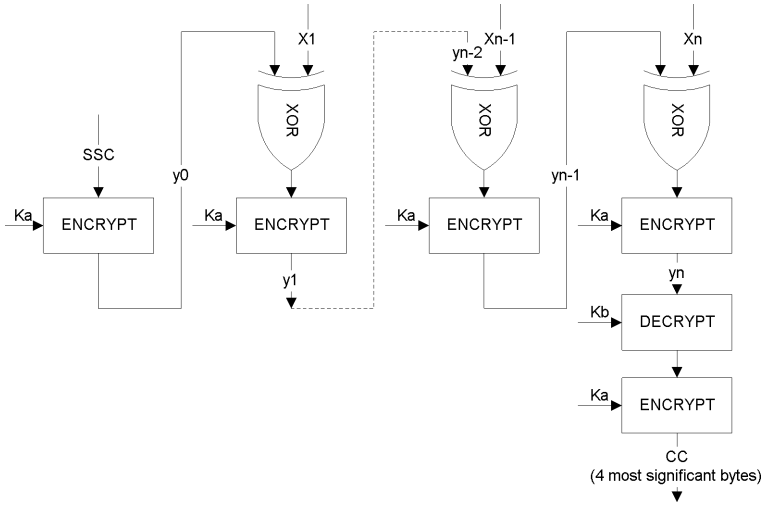
Edastatakse krüptograafilise kontrollsumma neli kõige tähtsamat baiti.

CSM_029 Saatejada lugeja (SSC) häälestatakse võtmete kooskõlastamise ajal järgmiselt:

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 algne SSC + 2).

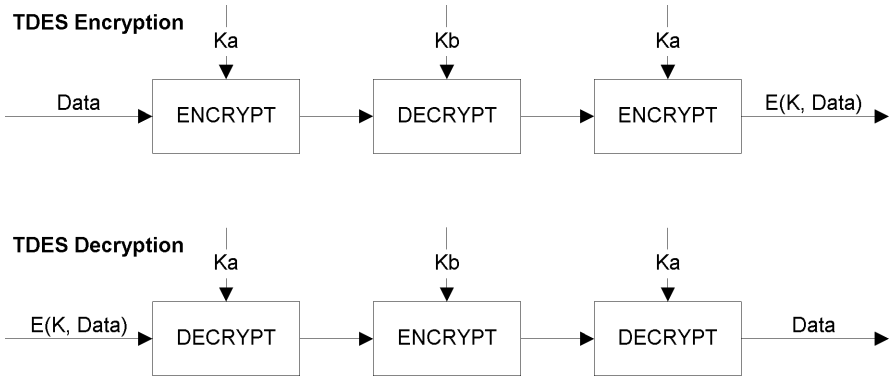
Järgmisel joonisel on näidatud *retail* MACi arvutamist.



5.4. Krüptogrammide arvutusalgoritm konfidentsiaalsuse andmeobjektide jaoks

CSM_031 Krüptogrammide arvutamisel kasutatakse TDEA-d TCBC toimimisrežiimis vastavalt viidetele TDES ja TDES-OP ning nii, et nullvektor on esimene väärtusplokk.

Järgmisel joonisel on näidatud võtmete rakendus TDES-is.



6. DIGITAALALLKIRJAMEHHANISMID ANDMETE ALLALAADIMISEL

CSM_032 Programmeeritav eriotstarbeline seade (IDE) salvestab seadmelt (sõidukiseadmest või kaardilt) ühe allalaadimisseansi käigus saadud andmed ühte füüsilisse andmefaili. See fail peab sisaldama sertifikaate MSi.C ja EQT.C. Fail sisaldab andmeplokkide digitaalallkirju vastavalt 7. liitele „Andmete allalaadimise protokollid“.

CSM_033 Allalaaditud andmete digitaalallkirjades kasutatakse sellise liitega digitaalallkirju, et allalaaditud andmeid saaks soovi korral lugeda igasuguse dešifreerimiseta.

6.1. Allkirja loomine

CSM_034 Seadme andmeallkirja loomisel kasutatakse viites (PKCS1) määratletud liitega allkirja koos SHA-1 räsifunktsiooniga:

Allkiri = EQT.SK[‘00’ || ‘01’ PS || ‘00’ || DER(SHA-1(Data))]

PS = 'FF' väärtusega baitidest moodustatud oktetistring, mille pikkus on 128.

DER(SHA-1(*M*)) on algoritmi identimiskood räsifunktsiooni tarvis ja räsiväärtuse kodeerimine standardi ASN.1 andmetüübi DigestInfo kohaseks (tunnustatud kodeerimiseeskirjad):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||räsiväärtus.

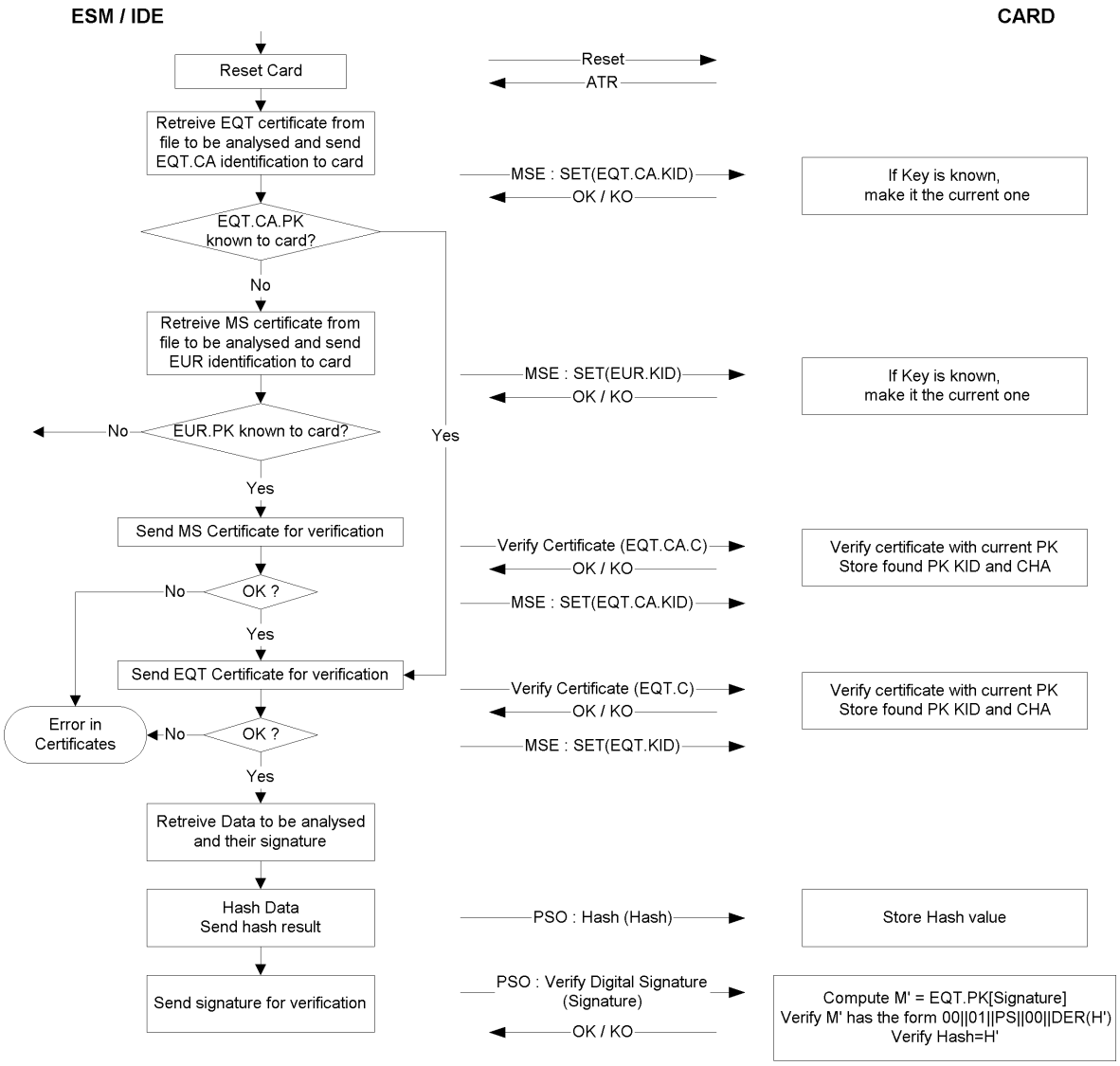
6.2. **Allkirja kontrollimine**

CSM_035 Allalaaditud andmete allkirja kontrollimiseks kasutatakse viites (PKCS1) määratletud liitega allkirjaskeemi koos SHA-1 räsifunktsiooniga.

Kontrollijale peab sõltumatult (ja usaldusväärselt) teada olema Euroopa avalik võti EUR.PK.

Järgmises tabelis on esitatud protokoll, mida võib täita kontrollikaarti omav eriotstarbeline seade, et kontrollida välisandmekandjale allalaaditud ja salvestatud andmete terviklust. Kontrollikaarti kasutatakse digitaalallkirjade dešifreerimiseks. Antud juhul ei tohi seda funktsiooni rakendada eriotstarbelises seadmes.

Seade, mis on analüüsitavad andmed alla laadinud ja need allkirjastanud, on tähistatud lühendiga EQT.



B OSA

TEISE PÕLVKONNA SÕIDUMEERIKUSÜSTEEM

7. SISSEJUHATUS

7.1. **Viited**

Liite käesolevas osas kasutatakse järgmisi viiteid.

AES	National Institute of Standards and Technology (NIST). *FIPS Publication 197: Advanced Encryption Standard (AES)*. 26. november 2001
DSS	National Institute of Standards and Technology (NIST). *FIPS Publication 186-4: Digital Signature Standard (DSS)*. Juuli 2013
ISO 7816-4	*Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange* („Identimiskaardid. Kiipkaardid. Osa 4: Andmevahetuse ülesehitus, turvalisus ja käsud“). Kolmas väljaanne, 15.04.2013
ISO 7816-8	*Identification cards – Integrated circuit cards – Part 8: Commands for security operations* („Identimiskaardid. Kiipkaardid. Osa 8: Turvatoimingute käsud“). Teine väljaanne, 01.06.2004
ISO 8825-1	*Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)* („Infotehnoloogia. ASN.1 kodeerimisreeglid: esmaste kodeerimisreeglite (BER), kanooniliste kodeerimisreeglite (CER) ja eristuvate kodeerimisreeglite (DER) spetsifikaat“). Neljas väljaanne, 15.12.2008
ISO 9797-1	Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher („Infotehnoloogia. Turvameetodid. Sõnumiautentimiskoodid (MAC-id). Osa 1: Plokišifrit kasutavad mehhanismid“). Teine väljaanne, 01.03.2011
ISO/IEC 10116	*Information technology – Security techniques – Modes of operation of an n-bit block cipher* („Infotehnoloogia. Turvameetodid. *n*-bitise plokišifri toimimisrežiimid“). Kolmas väljaanne, 01.02.2006
ISO 16844-3	*Road vehicles – Tachograph systems – Part 3: Motion sensor interface* („Maanteesõidukid. Sõidumeerikusüsteemid. Osa 3: Liikumisanduri liides“). Esimene väljaanne, 2004 + 1. tehniline parandus: 2006
RFC 5480	*Elliptic Curve Cryptography Subject Public Key Information*. Märts 2009
RFC 5639	*Elliptic Curve Cryptography (ECC) – Brainpool Standard Curves and Curve Generation*. 2010
RFC 5869	*HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*. Mai 2010
SHS	National Institute of Standards and Technology (NIST). *FIPS Publication 180-4: Secure Hash Standard*. Märts 2012
SP 800-38B	National Institute of Standards and Technology (NIST). *Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*. 2005
TR-03111	*BSI Technical Guideline TR-03111, Elliptic Curve Cryptography*. Versioon 2.00, 28.06.2012

7.2. **Märkused ja lühendid**

Käesolevas liites kasutatakse järgmisi märkusi ja lühendeid.

AES	(*advanced encryption standard*) täiustatud krüpteerimisstandard
CA	(*certificate authority*) sertifitseerimisasutus
CAR	(*certificate authority reference*) sertifitseerimisasutuse viide
CBC	šifriploki aheldamine (toimimisrežiim)

CH	(*command header*) käsu päis
CHA	(*certificate holder authorisation*) sertifikaadi omaniku luba
CHR	(*certificate holder reference*) sertifikaadi omaniku viide
CV	(*constant vector*) konstantne vektor
DER	(*distinguished encoding rules*) eristuvad kodeerimisreeglid
DO	(*data object*) andmeobjekt
DSRC	(*dedicated short range communication*) sihtotstarbeline lähitoimeside
ECC	(*elliptic curve cryptography*) elliptiliste kõverate krüptograafia
ECDSA	(*elliptic curve digital signature algorithm*) elliptiliste kõverate digitaalallkirja algoritm
ECDH	elliptiliste kõverate Diffie-Hellman (võtmete kooskõlastamise algoritm)
EGF	(*external GNSS facility*) GNSSi välisseade
EQT	(*equipment*) seade
IDE	(*intelligent dedicated equipment*) eriotstarbeline seade
K_M	liikumisanduri peavõti, mis võimaldab sõidukiseadet liikumisanduriga ühendada
K_{M-VU}	sõidukiseadmesse sisestatud võti, mis võimaldab sõidukiseadmel tuletada liikumisanduri peavõtme, kui töökojakaart on sõidukiseadmesse sisestatud
K_{M-WC}	töökojakaardile sisestatud võti, mis võimaldab sõidukiseadmel tuletada liikumisanduri peavõtme, kui töökojakaart on sõidukiseadmesse sisestatud
MAC	(*message authentication code*) sõnumiautentimiskood
MoS	(*motion sensor*) liikumisandur
MSB	(*most significant bit*) kõige tähtsam bitt
PKI	(*public key infrastructure*) avaliku võtme infrastruktuur
RCF	(*remote communication facility*) kaugsideseade
SSC	(*send sequence counter*) saatejada loendur
SM	(*secure messaging*) turvaline sõnumivahetus
TDES	(*triple data encryption standard*) kolmekordse andmekrüpteerimise standard
TLV	(*tag length value*) sildi pikkuse väärtus
VU	(*vehicle unit*) sõidukiseade
X.C	kasutaja X avaliku võtme sertifikaat
X.CA	kasutajale X sertifikaadi väljastanud asutuse sertifikaat
X.CAR	kasutaja X sertifikaadis sisalduv sertifikaadi väljastanud asutuse viide
X.CHR	kasutaja X sertifikaadis sisalduv sertifikaadi omaniku viide
X.PK	kasutaja X avalik võti
X.SK	kasutaja X privaatvõti
$X.PK_{eph}$	kasutaja X lühiajaline avalik võti
$X.SK_{eph}$	kasutaja X lühiajaline privaatvõti
‘xx’	väärtus kuueteistkümnendsüsteemis
||	konkatenatsioonioperaator

7.3. **Mõisted**

Käesolevas liites kasutatud mõistete määratlused on esitatud IC lisa 1. peatükis.

8. KRÜPTOGRAAFILISED SÜSTEEMID JA ALGORITMID

8.1. **Krüptograafilised süsteemid**

CSM_38 Sõidukiseadmed ja sõidumeerikukaardid kasutavad elliptilistel kõveratel põhinevat avaliku võtme krüptograafilist süsteemi järgmiste turbeteenuste osutamiseks:

— sõidukiseadme ja kaardi vastastikune autentimine,

— AES-i seansivõtmete kokkuleppimine sõidukiseadme ja kaardi vahel,

— sõidukiseadmest või sõidumeerikukaardilt välisandmekandjatele allalaaditud andmete autentsuse, tervikluse ja ümberlükkamatuse tagamine.

CSM_39 Sõidukiseadmed ja GNSSi välisseadmed kasutavad elliptilistel kõveratel põhinevat avaliku võtme krüptograafilist süsteemi järgmiste turbeteenuste osutamiseks:

— sõidukiseadme ja GNSSi välisseadme ühendamine,

— sõidukiseadme ja GNSSi välisseadme vastastikune autentimine,

— AES-i seansivõtme kokkuleppimine sõidukiseadme ja GNSSi välisseadme vahel.

CSM_40 Sõidukiseadmed ja sõidumeerikukaardid kasutavad AES-il põhinevat sümmeetrilist krüptograafilist süsteemi järgmiste turbeteenuste osutamiseks:

— sõidukiseadme ja sõidumeerikukaardi vahel vahetatavate andmete autentsuse ja tervikluse tagamine,

— vajaduse korral sõidukiseadme ja sõidumeerikukaardi vahel vahetatavate andmete konfidentsiaalsuse tagamine.

CSM_41 Sõidukiseadmed ja GNSSi välisseadmed kasutavad AES-il põhinevat sümmeetrilist krüptograafilist süsteemi järgmiste turbeteenuste osutamiseks:

— sõidukiseadme ja GNSSi välisseadme vahel vahetatavate andmete autentsuse ja tervikluse tagamine.

CSM_42 Sõidukiseadmed ja liikumisandurid kasutavad AES-il põhinevat sümmeetrilist krüptograafilist süsteemi järgmiste turbeteenuste osutamiseks:

— sõidukiseadme ja liikumisanduri ühendamine,

— sõidukiseadme ja liikumisanduri vastastikune autentimine,

— sõidukiseadme ja liikumisanduri vahel vahetatavate andmete konfidentsiaalsuse tagamine.

CSM_43 Sõidukiseadmed ja kontrollikaardid kasutavad AES-il põhinevat sümmeetrilist krüptograafilist süsteemi järgmiste turbeteenuste osutamiseks kaugsideliideses:

— sõidukiseadme ja kontrollikaardi vahel vahetatavate andmete konfidentsiaalsuse, autentsuse ja tervikluse tagamine.

Märkused

— Otseselt võttes edastatakse andmed sõidukiseadmest kontrolliametniku juhitavasse kaugpäringusaatjasse, kasutades sõidukiseadmes või sellest väljaspool paiknevat kaugsideseadet (vt 14. liide), kuid kaugpäringusaatja edastab saadud andmed dekrüpteerimiseks ja autentsuse kontrollimiseks kontrollikaardile. Turvalisuse seisukohalt on nii kaugsideseade kui ka kaugpäringusaatja täiesti läbipaistvad.

— Töökojakaart võimaldab kasutada DSRC-liidesega samu turbeteenuseid nagu kontrollikaart. See võimaldab töökojal tõendada sõidukiseadme kaugsideseadme nõuetekohast toimimist, sealhulgas turbefunktsioone. Lisateave punktis 9.2.2.

8.2. **Krüptograafilised algoritmid**

8.2.1. *Sümmeetrilised algoritmid*

CSM_44 Sõidukiseadmed sõidumeerikukaardid, liikumisandurid ja GNSSi välisseadmed peavad toetama AES-i algoritmi, mis on määratletud standardis AES, 128, 192 ja 256 biti pikkuste võtmetega.

8.2.2. *Asümmeetrilised algoritmid ja standardsed domeeniparameetrid*

CSM_45 Sõidukiseadmed sõidumeerikukaardid ja GNSSi välisseadmed peavad toetama elliptilistel kõveratel põhinevat krüptograafiat võtmesuurustega 256, 384 ja 512/521 bitti.

CSM_46 Sõidukiseadmed, sõidumeerikukaardid ja GNSSi välisseadmed peavad toetama ECSDA allkirjaalgoritmi, mis on määratletud süsteemis DSS.

CSM_47 Sõidukiseadmed, sõidumeerikukaardid ja GNSSi välisseadmed peavad toetama ECKA-EG võtmete kooskõlastamise algoritmi, mis on määratletud tehnilises eeskirjas TR 03111.

CSM_48 Sõidukiseadmed, sõidumeerikukaardid ja GNSSi välisseadmed peavad elliptiliste kõverate krüptograafias toetama kõiki standardseid domeeniparameetreid, mis on määratletud tabelis 1.

Tabel 1.

Standardsed domeeniparameetrid

Nimi	Suurus (bitti)	Viide	Objekti identifikaator
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

Märkus: tabeli 1 viimases veerus nimetatud objekti identifikaatorite spetsifikatsioon on Brainpooli kõverate kohta esitatud dokumendis RFC 5639 ja NIST-kõverate kohta dokumendis RFC 5480.

Näide 1: BrainpoolP256r1 kõvera objekti identifikaator on `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

Punktesituses: `1.3.36.3.3.2.8.1.1.7`.

Näide 2: NIST P-384 kõvera objekti identifikaator on

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

Punktesituses: `1.3.132.0.34`.

8.2.3. *Räsialgoritmid*

CSM_49 Sõidukiseadmed ja sõidumeerikukaardid peavad toetama algoritme SHA-256, SHA-384 ja SHA 512, mis on määratletud standardis SHS.

8.2.4. *Šifrikomplektid*

CSM_50 Sümmeetrilise algoritmi korral kasutatakse asümmeetrilist algoritmi ja/või räsialgoritmi koos, et moodustada turbeprotokoll. Nende vastavad võtmepikkused ja räsiväärtuste suurused peavad olema (ligikaudu) võrdse tugevusega. Tabelis 2 on näidatud lubatud šifrikomplektid.

Tabel 2.

Lubatud šifrikomplektid

Šifrikomplekti tunnus	ECC võtme suurus (bitti)	AES-i võtme pikkus (bitti)	Räsialgoritm	MAC-i pikkus (baiti)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Märkus: ECC võtmesuurusi 512 ja 521 peetakse kõigil käesolevas liites käsitletud juhtudel tugevuselt võrdseteks.

9. VÕTMED JA SERTIFIKAADID

9.1. **Asümmeetrilised võtmepaarid ja avaliku võtme sertifikaadid**

9.1.1. *Üldist*

Märkus: käesolevas punktis kirjeldatud võtmeid kasutatakse sõidukiseadmete ja sõidumeerikukaartide ning sõidukiseadmete ja GNSSi välisseadmete vastastikuseks autentimiseks ja turvaliseks sõnumivahetuseks. Nimetatud protsesse on üksikasjalikult kirjeldatud käesoleva liite 10. ja 11. peatükis.

CSM_51 Euroopa arukate sõidumeerikute süsteemis toimub ECC võtmepaaride ja neile vastavate sertifikaatide loomine ja haldamine kolme funktsionaalse hierarhilise tasandi kaudu:

— Euroopa tasand,

— liikmesriigi tasand,

— seadme tasand.

CSM_52 Kõikjal Euroopa arukate sõidumeerikute süsteemis toimub avalike ja privaatvõtmete ja sertifikaatide loomine, haldamine ja edastamine standardsete ja turvaliste meetoditega.

9.1.2. *Euroopa tasand*

CSM_53 Euroopa tasandil luuakse üks kordumatu ECC võtmepaar tähistusega EUR. See koosneb privaatvõtmest (EUR.SK) ja avalikust võtmest (EUR.PK). See võtmepaar moodustab kogu Euroopa arukate sõidumeerikute PKI juurvõtmepaari. Sellega tegeleb Euroopa Komisjoni volitustega ja vastutusel Euroopa juursertifikaatide asutus (*European Root Certificate Authority*, ERCA).

CSM_54 ERCA kasutab Euroopa privaatvõtit Euroopa avaliku võtme (ise allkirjastatud) juursertifikaadi allkirjastamiseks ning edastab selle juursertifikaadi kõigile liikmesriikidele.

CSM_55 ERCA kasutab Euroopa privaatvõtit nõudmisel liikmesriikide avalike võtmete sertifikaatide allkirjastamiseks. ERCA peab arvestust kõigi allkirjastatud liikmesriikide avaliku võtme sertifikaatide kohta.

CSM_56 Vastavalt punktis 9.1.7 esitatud joonisele 1 loob ERCA iga 17 aasta järel uue Euroopa juurvõtmepaari. Iga kord, kui ERCA loob uue Euroopa juurvõtmepaari, loob ta Euroopa uue avaliku võtme jaoks uue ise allkirjastatud juursertifikaadi. Euroopa juursertifikaadi kehtivusaeg on 34 aastat ja kolm kuud.

Märkus: uue juurvõtmepaari kasutusele võtmine eeldab ka seda, et ERCA loob liikumisanduri uue peavõtme ja DSRC uue peavõtme, vt punktid 9.2.1.2 ja 9.2.2.2.

CSM_57 Enne Euroopa uue juurvõtmepaari loomist analüüsib ERCA uue võtmepaari jaoks vajalikku krüptograafilist tugevust, võttes arvesse, et see peab püsima turvalisena järgmised 34 aastat. Kui see osutub vajalikuks, läheb ERCA üle senisest tugevamale šifrikomplektile vastavalt nõudele CSM_50.

CSM_58 Iga kord, kui ERCA loob Euroopa uue juurvõtmepaari, loob ta Euroopa uue avaliku võtme jaoks lülisertifikaadi ning allkirjastab selle Euroopa eelmise privaatvõtmega. Lülisertifikaadi kehtivusaeg on 17 aastat. Ka seda on kujutatud punktis 9.1.7 esitatud joonisel 1.

Märkus: kuna lülisertifikaat sisaldab ERCA *X*. põlvkonna avalikku võtit ja on allkirjastatud ERCA põlvkonna $X - 1$ privaatvõtmega, võimaldab lülisertifikaat põlvkonna $X - 1$ seadmetel kasutada meetodit *X*. põlvkonna seadmete usaldamiseks.

CSM_59 ERCA ei kasuta juurvõtmepaari privaatvõtit pärast uue juurvõtme sertifikaadi kehtivaks muutumist ühelgi muul otstarbel.

CSM_60 ERCA võib igal ajal käsutada järgmisi krüptograafilisi võtmeid ja sertifikaate:

— kehtiv Euroopa võtmepaar ja sellele vastav sertifikaat;

— kõik varasemad Euroopa sertifikaadid, mida kasutatakse veel kehtivate MSCA sertifikaatide kontrollimiseks;

— kõigi Euroopa sertifikaatide põlvkondade (välja arvatud esimene põlvkond) lülisertifikaadid.

9.1.3. *Liikmesriigi tasand*

CSM_61 Liikmesriigi tasandil loovad kõik liikmesriigid, kes peavad allkirjastama sõidumeerikukaartide sertifikaate, ühe või mitu kordumatut ECC võtmepaari tähistusega MSCA_Card. Kõik liikmesriigid, kes peavad allkirjastama sõidukiseadmete või GNSSi välisseadmete sertifikaate, loovad lisaks ühe või mitu kordumatut ECC võtmepaari tähistusega MSCA_VU-EGF.

CSM_62 Liikmesriigi võtmepaaride loomine tehakse ülesandeks liikmesriigi sertifitseerimisasutusele (*Member State Certificate Authority*, MSCA). Iga kord, kui liikmesriigi sertifitseerimisasutus loob liikmesriigi võtmepaari, saadab ta ERCA-le avaliku võtme, et saada vastav ERCA allkirjastatud liikmesriigi sertifikaat.

CSM_63 Liikmesriigi sertifitseerimisasutus valib liikmesriigi võtmepaari tugevuse nii, et see oleks võrdne liikmesriigi vastava sertifikaadi allkirjastamiseks kasutatud Euroopa juurvõtmepaari tugevusega.

CSM_64 Kui kasutatakse võtmepaari MSCA_VU-EGF, koosneb see privaatvõtmest MSCA_VU-EGF.SK ja avalikust võtmest MSCA_VU-EGF.PK. Liikmesriigi sertifitseerimisasutus kasutab privaatvõtit MSCA_VU-EGF.SK ainult sõidukiseadmete ja GNSSi välisseadmete avaliku võtme sertifikaatide allkirjastamiseks.

CSM_65 Võtmepaar MSCA_Card koosneb privaatvõtmest MSCA_Card.SK ja avalikust võtmest MSCA_Card.PK. Liikmesriigi sertifitseerimisasutus kasutab privaatvõtit MSCA_Card.SK ainult sõidumeerikukaartide avaliku võtme sertifikaatide allkirjastamiseks.

CSM_66 Liikmesriigi sertifitseerimisasutus säilitab andmed kõigi allkirjastatud sõidukiseadme sertifikaatide, GNSSi välisseadme sertifikaatide ja kaardisertifikaatide kohta koos nende seadmete identimisandmetega, millega kavatsetakse sertifikaati kasutada.

CSM_67 Sertifikaadi MSCA_VU-EGF kehtivusaeg on 17 aastat ja kolm kuud. Sertifikaadi MSCA_Card kehtivusaeg on seitse aastat ja üks kuu.

CSM_68 Nagu on näidatud punktis 9.1.7 esitatud joonisel 1, peab võtmepaari MSCA_VU-EGF privaatvõtme ja võtmepaari MSCA_Card privaatvõtme kasutusaeg olema kaks aastat.

CSM_69 Liikmesriigi sertifitseerimisasutus ei kasuta võtmepaari MSCA_VU-EGF privaatvõtit pärast selle kasutusaja lõppemist ühelgi otstarbel. Samuti ei kasuta liikmesriigi sertifitseerimisasutus võtmepaari MSCA_Card privaatvõtit ühelgi otstarbel alates selle kasutusaja lõppemisest.

CSM_70 Liikmesriigi sertifitseerimisasutus võib igal ajal käsutada järgmisi krüptograafilisi võtmeid ja sertifikaate:

— kehtiv võtmepaar MSCA_Card ja sellele vastav sertifikaat;

— kõik varasemad MSCA_Card-i sertifikaadid, mida kasutatakse veel kehtivate sõidumeerikukaardi sertifikaatide kontrollimiseks;

— kehtiv Euroopa sertifikaat, mis on vajalik liikmesriigi sertifitseerimisasutuse kehtiva sertifikaadi kontrollimiseks;

— kõik varasemad Euroopa sertifikaadid, mida kasutatakse liikmesriigi sertifitseerimisasutuse veel kehtivate sertifikaatide kontrollimiseks.

CSM_71 Kui liikmesriigi sertifitseerimisasutus peab allkirjastama sõidukiseadme või GNSSi välisseadme sertifikaate, käsutab ta lisaks järgmisi võtmeid ja sertifikaate:

— kehtiv võtmepaar MSCA_VU-EGF ja sellele vastav sertifikaat;

— kõik varasemad avalikud võtmed MSCA_VU-EGF, mida kasutatakse veel kehtivate sõidukiseadme või GNSSi välisseadme sertifikaatide kontrollimiseks.

9.1.4. *Seadme tasand: sõidukiseadmed*

CSM_72 Iga sõidukiseadme jaoks luuakse kaks kordumatut ECC võtmepaari tähistusega VU_MA ja VU_Sign. Seda ülesannet täidavad sõidukiseadmete tootjad. Iga kord, kui luuakse sõidukiseadme võtmepaar, saadab selle looja oma asukohariigi sertifitseerimisasutusele avaliku võtme, et saada liikmesriigi sertifitseerimisasutuse allkirjastatud vastav sõidukiseadme sertifikaat. Privaatvõtit kasutab ainult sõidukiseade.

CSM_73 Ühe sõidukiseadme sertifikaatidel VU_MA ja VU_Sign peab olema sama jõustumiskuupäev.

CSM_74 Sõidukiseadme tootja valib sõidukiseadme võtmepaari tugevuse nii, et see oleks võrdne sõidukiseadme vastava sertifikaadi allkirjastamiseks kasutatud liikmesriigi sertifitseerimisasutuse võtmepaari tugevusega.

CSM_75 Sõidukiseade kasutab võtmepaari VU_MA, mis koosneb privaatvõtmest VU_MA.SK ja avalikust võtmest VU_MA.PK ainult selleks, et autentida sõidukiseadmes sõidumeerikukaarte ja GNSSi välisseadmeid, nagu on määratletud käesoleva liite punktides 10.3 ja 11.4.

CSM_76 Sõidukiseade peab suutma luua lühiajalisi ECC võtmepaare ning kasutama lühiajalist võtmepaari ainult selleks, et kooskõlastada sõidumeerikukaardi või GNSSi välisseadmega seansivõti, nagu on määratletud käesoleva liite punktides 10.4 ja 11.4.

CSM_77 Sõidukiseade kasutab oma võtmepaari VU_Sign privaatvõtit VU_Sign.SK ainult selleks, et allkirjastada allalaaditud andmefaile, nagu on määratletud käesoleva liite 14. peatükis. Vastavat avalikku võtit VU_Sign.PK kasutatakse ainult sõidukiseadme loodud allkirjade kontrollimiseks.

CSM_78 Vastavalt punktis 9.1.7 esitatud joonisele 1 on sertifikaadi VU_MA kehtivusaeg 17 aastat ja kolm kuud. Sertifikaadi VU_Sign kehtivusaeg on samuti 15 aastat ja kolm kuud.

Märkused

— Sertifikaadi VU_Sign pikendatud kehtivusaeg võimaldab sõidukiseadmel luua allalaaditud andmetele kehtivaid allkirju veel kolme kuu jooksul pärast sertifikaadi aegumist, nagu nõutakse määruses (EL) 581/2010.

— Sertifikaadi VU_MA pikendatud kehtivusaeg on vajalik selleks, et sõidukiseade saaks autentida kontrollikaarti või ettevõttekaarti veel kolme kuu jooksul pärast sertifikaadi aegumist; see võimaldab näiteks andmeid alla laadida.

CSM_79 Sõidukiseade ei kasuta sõidukiseadme võtmepaari privaatvõtit pärast vastava sertifikaadi aegumist ühelgi otstarbel.

CSM_80 Pärast sõidukiseadme kasutusele võtmist ei ole lubatud selle sõidukiseadme võtmepaare (välja arvatud lühiajalised võtmepaarid) ja neile vastavaid sertifikaate välitöö korras vahetada ega uuendada.

Märkused

— Nõue ei kehti lühiajaliste võtmepaaride kohta, kuna sõidukiseade loob uue lühiajalise võtmepaari iga kord, kui toimub kiibi autentimine ja seansivõtme kooskõlastamine (vt punkt 10.4). Lühiajalisel võtmepaaril ei ole sellele vastavat sertifikaati.

— Kõnealune nõue ei välista võimalust, et sõidukiseadme tootja vahetab sõidukiseadme püsiva võtmepaari välja taastamise või remondi käigus turvalises keskkonnas.

CSM_81 Kasutusele võtmise ajal peab sõidukiseade sisaldama järgmisi krüptograafilisi võtmeid ja sertifikaate:

— privaatvõti VU_MA ja sellele vastav sertifikaat;

— privaatvõti VU_Sign ja sellele vastav sertifikaat;

— sertifikaat MSCA_VU-EGF, mis sisaldab avalikku võtit MSCA_VU-EGF.PK, mida kasutatakse sertifikaatide VU_MA ja VU_Sign kontrollimiseks;

— sertifikaat EUR, mis sisaldab avalikku võtit EUR.PK, mida kasutatakse sertifikaadi MSCA_VU-EGF kontrollimiseks;

— sertifikaat EUR (kui see on olemas), mille kehtivusaeg eelneb vahetult selle EUR-sertifikaadi kehtivusajale, mida kasutatakse sertifikaadi MSCA_VU-EGF kontrollimiseks;

— nimetatud kahte EUR-sertifikaati siduv lülisertifikaat, kui see on olemas.

CSM_82 Lisaks nõudes CSM_81 loetletud krüptograafilistele võtmetele ja sertifikaatidele peab sõidukiseade sisaldama ka käesoleva liite A osas nimetatud võtmeid ja sertifikaate, mis võimaldavad sõidukiseadmel andmeid vahetada esimese põlvkonna sõidumeerikukaartidega.

9.1.5. *Seadme tasand: sõidumeerikukaardid*

CSM_83 Iga sõidumeerikukaardi jaoks luuakse üks kordumatu ECC võtmepaar tähistusega Card_MA. Lisaks luuakse iga juhikaardi ja iga töökojakaardi jaoks teine kordumatu ECC võtmepaar tähistusega Card_Sign. Seda ülesannet võib täita kaardi tootja või kaardi isikustaja. Iga kord, kui luuakse kaardi võtmepaar, saadab selle looja oma asukohariigi sertifitseerimisasutusele avaliku võtme, et saada liikmesriigi sertifitseerimisasutuse allkirjastatud vastav kaardi sertifikaat. Privaatvõtit kasutab ainult sõidumeerikukaart.

CSM_84 Ühe juhikaardi või ühe töökojakaardi sertifikaatidel Card_MA ja Card_Sign peab olema sama jõustumiskuupäev.

CSM_85 Kaardi tootja või isikustaja valib kaardi võtmepaari tugevuse nii, et see oleks võrdne kaardi vastava sertifikaadi allkirjastamiseks kasutatud liikmesriigi sertifitseerimisasutuse võtmepaari tugevusega.

CSM_86 Sõidumeerikukaart kasutab võtmepaari Card_MA, mis koosneb privaatvõtmest Card_MA.SK ja avalikust võtmest Card_MA.PK, ainult vastastikuseks autentimiseks ja seansivõtme kooskõlastamiseks sõidukiseadmetega, nagu on määratletud käesoleva liite punktides 10.3 ja 10.4.

CSM_87 Juhikaart või töökojakaart kasutab oma võtmepaari Card_Sign privaatvõtit Card_Sign.SK ainult selleks, et allkirjastada allalaaditud andmefaile, nagu on määratletud käesoleva liite 14. peatükis. Vastavat avalikku võtit Card_Sign.PK kasutatakse ainult kaardi loodud allkirjade kontrollimiseks.

CSM_88 Sertifikaadi Card_MA kehtivusajad on järgmised:

— juhikaardid: 5 aastat

— ettevõttekaardid: 2 aastat

— kontrollikaardid 2 aastat

— töökojakaardid: 1 aasta

CSM_89 Sertifikaadi Card_Sign kehtivusajad on järgmised:

— juhikaardid: 5 aastat ja 1 kuu

— töökojakaardid: 1 aasta ja 1 kuu

Märkus: sertifikaadi Card_Sign pikendatud kehtivusaeg võimaldab juhikaardil luua allalaaditud andmetele kehtivaid allkirju veel ühe kuu jooksul pärast sertifikaadi aegumist. See on vajalik vastavalt määrusele (EL) nr 581/2010, milles nõutakse, et juhikaardilt peab olema võimalik andmeid alla laadida kuni 28 päeva pärast viimast andmete salvestamist.

CSM_90 Pärast kaardi väljaandmist ei ole lubatud selle sõidumeerikukaardi võtmepaare ja neile vastavaid sertifikaate vahetada ega uuendada.

CSM_91 Välja antud sõidumeerikukaart peab sisaldama järgmisi krüptograafilisi võtmeid ja sertifikaate:

— privaatvõti Card_MA ja sellele vastav sertifikaat;

— juhi- ja töökojakaartidel lisaks: privaatvõti Card_Sign ja sellele vastav sertifikaat;

— sertifikaat MSCA_Card, mis sisaldab avalikku võtit MSCA_Card.PK, mida kasutatakse sertifikaatide Card_MA ja Card_Sign kontrollimiseks;

— sertifikaat EUR, mis sisaldab avalikku võtit EUR.PK, mida kasutatakse sertifikaadi MSCA_Card kontrollimiseks;

— sertifikaat EUR (kui see on olemas), mille kehtivusaeg eelneb vahetult selle EUR-sertifikaadi kehtivusajale, mida kasutatakse sertifikaadi MSCA_Card kontrollimiseks;

— nimetatud kahte EUR-sertifikaati siduv lülisertifikaat, kui see on olemas.

CSM_92 Lisaks nõudes CSM_98 loetletud krüptograafilistele võtmetele ja sertifikaatidele peab sõidumeerikukaart sisaldama ka käesoleva liite A osas nimetatud võtmeid ja sertifikaate, mis võimaldavad kaardil andmeid vahetada esimese põlvkonna sõidukiseadmetega.

9.1.6. *Seadme tasand: GNSSi välisseadmed*

CSM_93 Iga GNSSi välisseadme jaoks luuakse üks kordumatu ECC võtmepaar tähistusega EGF_MA. Seda ülesannet täidavad GNSSi välisseadmete tootjad. Iga kord, kui luuakse võtmepaar EGF_MA, saadab selle looja oma asukohariigi sertifitseerimisasutusele avaliku võtme, et saada liikmesriigi sertifitseerimisasutuse allkirjastatud vastav EGF_MA sertifikaat. Privaatvõtit kasutab ainult GNSSi välisseade.

CSM_94 GNSSi välisseadme tootja valib võtmepaari EGF_MA tugevuse nii, et see oleks võrdne vastava EGF-MA sertifikaadi allkirjastamiseks kasutatud liikmesriigi sertifitseerimisasutuse võtmepaari tugevusega.

CSM_95 GNSSi välisseade kasutab võtmepaari EGF_MA, mis koosneb privaatvõtmest EGF_MA.SK ja avalikust võtmest EGF_MA.PK, ainult vastastikuseks autentimiseks ja seansivõtme kooskõlastamiseks sõidukiseadmetega, nagu on määratletud käesoleva liite punktis 11.4.

CSM_96 Sertifikaadi EGF-MA kehtivusaeg on 15 aastat.

CSM_97 GNSSi välisseade ei kasuta oma võtmepaari EGF_MA privaatvõtit sõidukiseadmega ühendumiseks pärast seda, kui vastav sertifikaat on aegunud.

Märkus: vastavalt punktis 11.3.3 esitatud selgitusele võib GNSSi välisseade põhimõtteliselt kasutada oma privaatvõtit vastastikuseks autentimiseks sõidukiseadmega ka pärast vastava sertifikaadi aegumist juhul, kui see on juba sõidukiseadmega ühendatud.

CSM_98 Pärast GNSSi välisseadme kasutusele võtmist ei ole lubatud selle võtmepaari EGF-MA ja sellele vastavat sertifikaati välitöö korras vahetada ega uuendada.

Märkus: kõnealune nõue ei välista võimalust, et GNSSi välisseadme võtmepaar vahetatakse välja taastamise või remondi käigus turvalises keskkonnas, mida kontrollib GNSSi välisseadme tootja.

CSM_99 Kasutusele võtmise ajal peab GNSSi välisseade sisaldama järgmisi krüptograafilisi võtmeid ja sertifikaate:

— privaatvõti EGF_MA ja sellele vastav sertifikaat;

— sertifikaat MSCA_VU-EGF, mis sisaldab avalikku võtit MSCA_VU-EGF.PK, mida kasutatakse sertifikaadi EGF_MA kontrollimiseks;

— sertifikaat EUR, mis sisaldab avalikku võtit EUR.PK, mida kasutatakse sertifikaadi MSCA_VU-EGF kontrollimiseks;

— sertifikaat EUR (kui see on olemas), mille kehtivusaeg eelneb vahetult selle EUR-sertifikaadi kehtivusajale, mida kasutatakse sertifikaadi MSCA-VU-EGF kontrollimiseks;

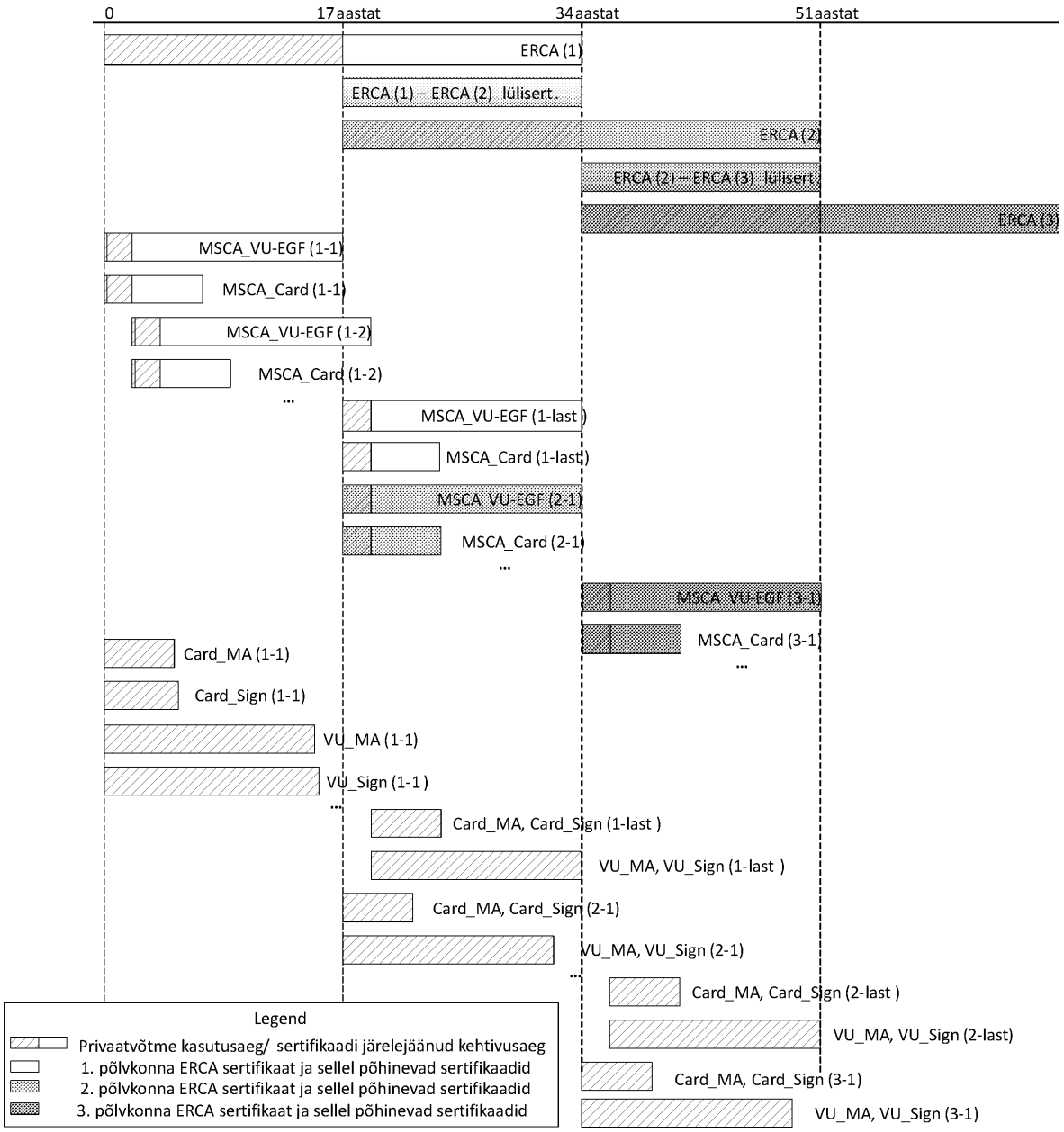
— nimetatud kahte EUR-sertifikaati siduv lülisertifikaat, kui see on olemas.

9.1.7. *Ülevaade: sertifikaadi vahetamine*

Allpool esitatud joonisel 1 on kujutatud, kuidas toimub aja jooksul erineva põlvkonna ERCA juursertifikaatide, ERCA lülisertifikaatide, liikmesriigi sertifitseerimisasutuse sertifikaatide ja seadmete (sõidukiseade ja kaart) sertifikaatide väljaandmine ja kasutamine.

Joonis 1.

Eri põlvkonna ERCA juursertifikaatide, ERCA lülisertifikaatide, liikmesriigi sertifitseerimisasutuse sertifikaatide ja seadmete sertifikaatide väljaandmine ja kasutamine



Märkused joonise 1 kohta.

1. Sulgudes olevad numbrid näitavad juursertifikaadi eri põlvkondi näitavad. Näiteks ERCA (1) on ERCA esimese põlvkonna juursertifikaat; ERCA (2) kuulub teise põlvkonda jne.

2. Ülejäänud sertifikaatide juures on sulgudes kaks numbrit, millest esimene näitab nende väljaandmise ajal kehtiva juursertifikaadi põlvkonda ning teine sertifikaadi enda põlvkonda. Näiteks MSCA_Card (1-1) on esimene sertifikaat MSCA_Card, mis on välja antud ERCA (1) kehtivuse ajal; MSCA_Card (2-1) on esimene sertifikaat MSCA_Card, mis on välja antud ERCA (2) kehtivuse ajal; MSCA_Card (2-last) on viimane sertifikaat MSCA_Card, mis on välja antud ERCA (2) kehtivuse ajal; Card_MA(2-1) on esimene vastastikuseks autentimiseks kasutatav kaardisertifikaat, mis on välja antud ERCA (2) kehtivuse ajal jne.

3. Sertifikaadid MSCA_Card (2-1) ja MSCA_Card (1-last) antakse välja peaaegu, aga mitte täpselt samal kuupäeval. MSCA_Card (2-1) on esimene sertifikaat MSCA_Card, mis antakse välja ERCA (2) kehtivusajal, ning see antakse välja natuke hiljem kui MSCA_Card (1-last), mis on viimane ERCA (1) kehtivusajal välja antud sertifikaat MSCA_Card.

4. Jooniselt on näha, et esimesed ERCA (2) kehtivusajal välja antavad sõidukiseadme ja kaardi sertifikaadid tulevad välja peaaegu kaks aastat enne seda kui viimased ERCA (1) kehtivusajal välja antavad sõidukiseadme ja kaardi sertifikaadid. Põhjuseks on asjaolu, et sõidukiseadme ja kaardi sertifikaate antakse välja liikmesriigi sertifitseerimisasutuse (MSCA) sertifikaadi alusel, mitte otse ERCA sertifikaadi alusel. Sertifikaat MSCA (2-1) antakse välja kohe pärast ERCA (2) kehtima hakkamist, kuid sertifikaat MSCA (1-last) antakse välja ainult veidi aega enne seda ehk sertifikaadi ERCA (1) kehtivuse viimasel hetkel. Seega on neil kahel liikmesriigi sertifitseerimisasutuse sertifikaadil peaaegu sama kehtivusaeg, kuigi nad kuuluvad eri põlvkondadesse.

5. Kaartide puhul on joonisel kujutatud juhikaartide kehtivusaega (5 aastat).

6. Ruumi kokkuhoiu huvides on sertifikaatide Card_MA ja Card_Sign ning VU_MA ja VU_Sign kehtivusaegade erinevused näidatud ainult esimeses põlvkonnas.

9.2. **Sümmeetrilised võtmed**

9.2.1. *Sõidukiseadme ja liikumisanduri vahelise andmevahetuse turbevõtmed*

9.2.1.1. *Üldist*

Märkus: käesoleva punkti lugejad peaksid olema tutvunud standardi ISO 16844-3 sisuga, milles kirjeldatakse sõidukiseadme ja liikumisanduri vahelist liidest. Sõidukiseadme ja liikumisanduri ühendamist on üksikasjalikult kirjeldatud käesoleva liite 12. peatükis.

CSM_100 Sõidukiseadmete ja liikumisandurite ühendamiseks, vastastikuseks autentimiseks ning nendevahelise side krüpteerimiseks on vaja mitmeid sümmeetrilisi võtmeid, nagu on näidatud tabelis 3. Kõik need võtmed peavad olema AES-i võtmed, mille pikkus on võrdne liikumisanduri peavõtme pikkusega, mis on omakorda seotud nõudes CSM_50 kirjeldatud (tulevase) Euroopa juurvõtmepaari pikkusega.

Tabel 3.

Sõidukiseadme ja liikumisanduri andmevahetuse turbevõtmed

Võti	Sümbol	Looja	Loomismeetod	Säilitaja
Liikumisanduri peavõti – sõidukiseadme osa	$K_{M\text{-}VU}$	ERCA	Juhuslik	ERCA, sõidukiseadmete sertifikaate välja andvad liikmesriikide sertifitseerimisasutused, sõidukiseadmete tootjad, sõidukiseadmed

Võti	Sümbol	Looja	Loomismeetod	Säilitaja
Liikumisanduri peavõti – töökoja osa	K_{M-WC}	ERCA	Juhuslik	ERCA, liikmesriikide sertifitseerimisasutused, kaartide tootjad, töökojakaardid
Liikumisanduri peavõti	K_M	Sõltumatut loomist ei toimu	Arvutatakse kujul $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, liikumisandurite võtmeid välja andvad liikmesriikide sertifitseerimisasutused (vabatahtlik) (*)
Identimisvõti	K_{ID}	Sõltumatut loomist ei toimu	Arvutatakse kujul $K_{ID} = K_M$ XOR CV, kus CV vastab nõudes CSM_106 esitatud spetsifikatsioonile	ERCA, liikumisandurite võtmeid välja andvad liikmesriikide sertifitseerimisasutused (vabatahtlik) (*)
Ühendamisvõti	K_P	Liikumisanduri tootja	Juhuslik	Üks liikumisandur
Seansivõti	K_S	Sõidukiseade (sõidukiseadme ja liikumisanduri ühendamise ajal)	Juhuslik	Üks sõidukiseade ja üks liikumisandur

(*) Võtmete K_M ja K_{ID} säilitamine on vabatahtlik, kuna neid võtmeid saab tuletada võtmetest K_{M-VU}, K_{M-WC} ja konstantsest vektorist.

CSM_101 Euroopa juursertifikaatide asutus (ERCA) loob võtmed K_{M-VU} ja K_{M-WC} – kaks juhuslikku ja kordumatud AES-i võtit, millest saab arvutada liikumisanduri peavõtme K_M kujul K_{M-VU} XOR K_{M-WC}. Liikmesriikide sertifitseerimisasutuste nõudmisel edastab ERCA võtmed K_M, K_{M-VU} ja K_{M-WC} neile asutustele.

CSM_102 ERCA annab igale liikumisanduri peavõtmele K_M kordumatu versiooninumbri, mis kehtib ka selle aluseks olevate võtmete K_{M-VU} ja K_{M-WC} ning seotud identimisvõtme K_{ID} kohta. Kui ERCA saadab liikmesriikide sertifitseerimisasutustele võtmed K_{M-VU} ja K_{M-WC}, teatab ta neile ka versiooninumbri.

Märkus: versiooninumbrit kasutatakse võtmete põlvkondade eristamiseks, nagu on põhjalikumalt selgitatud punktis 9.2.1.2.

CSM_103 Liikmesriigi sertifitseerimisasutus saadab võtme K_{M-VU} koos selle versiooninumbriga sõidukiseadmete tootjatele, kui need seda soovivad. Sõidukiseadmete tootjad sisestavad võtme K_{M-VU} ja selle versiooninumbri kõigisse toodetavatesse sõidukiseadmetesse.

CSM_104 Liikmesriigi sertifitseerimisasutus tagab, et võti K_{M-WC} ja selle versiooninumber sisestatakse kõigile asutuse haldusalas välja antavatele töökojakaartidele.

Märkused

— Vt 2. liites esitatud andmetüübi `SensorInstallationSecData` kirjeldust.

— Vastavalt punktis 9.2.1.2 esitatud selgitusele võib praktikas tekkida vajadus sisestada ühele töökojakaardile mitme põlvkonna võtmeid K_{M-WC}.

CSM_105 Liikmesriigi sertifitseerimisasutus tagab, et lisaks nõudes CSM_104 määratletud AES-i võtmele sisestatakse kõigile tema haldusalas välja antavatele töökojakaartidele ka käesoleva liite A osa nõudes CSM_037 määratletud TDES-võti Km_{WC}.

Märkused

— See võimaldab kasutada teise põlvkonna töökojakaarti esimese põlvkonna sõidukiseadme ühendamiseks.

— Teise põlvkonna töökojakaart sisaldab kahte eri rakendust, millest üks vastab käesoleva liite B osale ja teine vastab A osale. Viimane sisaldab TDES-võtit Km_{WC}.

CSM_106 Liikumisandurite võtmeid välja andev liikmesriigi sertifitseerimisasutus tuletab liikumisanduri peavõtmest selle identimisvõtme, sooritades sellel konstantse vektoriga (CV) XOR-tehte. CV väärtused on järgmised:

— 128-bitised liikumisanduri peavõtmed: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83'

— 192-bitised liikumisanduri peavõtmed: CV = '72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25'

— 256-bitised liikumisanduri peavõtmed: CV = '1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60'

Märkus: konstantsed vektorid on genereeritud järgmiselt:

Pi_10 = matemaatilise konstandi π = '24 3F 6A 88 85 A3 08 D3 13 19' kümnendkohtade esimesed 10 baiti

CV_128-bits = SHA-256(Pi_10) esimesed 16 baiti

CV_192-bits = SHA-384(Pi_10) esimesed 24 baiti

CV_256-bits = SHA-512(Pi_10) esimesed 32 baiti

CSM_107 Liikumisandurite tootjad loovad iga liikumisanduri jaoks juhusliku ja kordumatu ühendamisvõtme K_P ning saadavad kõik ühendamisvõtmed liikmesriigi sertifitseerimisasutusele. Liikmesriigi sertifitseerimisasutus krüpteerib iga ühendamisvõtme eraldi liikumisanduri peavõtmega K_M ning saadab krüpteeritud võtme liikumisanduri tootjale tagasi. Koos iga krüpteeritud võtmega teatab liikmesriigi sertifitseerimisasutus liikumisanduri tootjale vastava võtme K_M versiooninumbri.

Märkus: vastavalt punktis 9.2.1.2 esitatud selgitusele võib liikumisandurite tootjal praktikas tekkida vajadus luua ühe liikumisanduri jaoks mitu kordumatut ühendamisvõtit.

CSM_108 Liikumisandurite tootjad loovad iga liikumisanduri jaoks kordumatu seerianumbri ning saadavad kõik seerianumbrid liikmesriigi sertifitseerimisasutusele. Liikmesriigi sertifitseerimisasutus krüpteerib iga seerianumbri eraldi identimisvõtmega K_{ID} ning saadab krüpteeritud seerianumbri liikumisanduri tootjale tagasi. Koos iga krüpteeritud seerianumbriga teatab liikmesriigi sertifitseerimisasutus liikumisanduri tootjale vastava identimisvõtme K_{ID} versiooninumbri.

CSM_109 Nõuete CSM_107 ja CSM_108 täitmiseks rakendab liikmesriigi sertifitseerimisasutus AES-i algoritmi šifriplokki aheldavas toimimisrežiimis, nagu on määratletud standardis ISO 10116, kasutades vaheldamisparameetrit m = 1 ja initsialiseerimisvektorit SV = '00' {16}, st kuusteist baiti binaarväärtusega 0. Vajadusel kasutab liikmesriigi sertifitseerimisasutus standardis ISO 9797-1 määratletud täidistamismeetodit nr 2.

CSM_110 Liikumisanduri tootja salvestab krüpteeritud ühendamisvõtme ja krüpteeritud seerianumbri neile ette nähtud liikumisandurisse koos võtmete lihtteksti ning krüpteerimiseks kasutatud võtmete K_M ja K_{ID} versiooninumbriga.

Märkus: vastavalt punktis 9.2.1.2 esitatud selgitusele võib liikumisandurite tootja sisestada ühte liikumisandurisse mitu krüpteeritud ühendamisvõtit ja mitu krüpteeritud seerianumbrit.

CSM_111 Lisaks nõudes CSM_110 nimetatud krüptograafilisele materjalile, mis põhineb standardil AES, võib liikumisandurite tootja salvestada igasse liikumisandurisse ka standardil TDES põhinevat krüptograafilist materjali, mis on määratletud käesolevaliite A osa nõudes CSM_037.

Märkus: see võimaldab ühendada teise põlvkonna liikumisandurit esimese põlvkonna sõidukiseadmega.

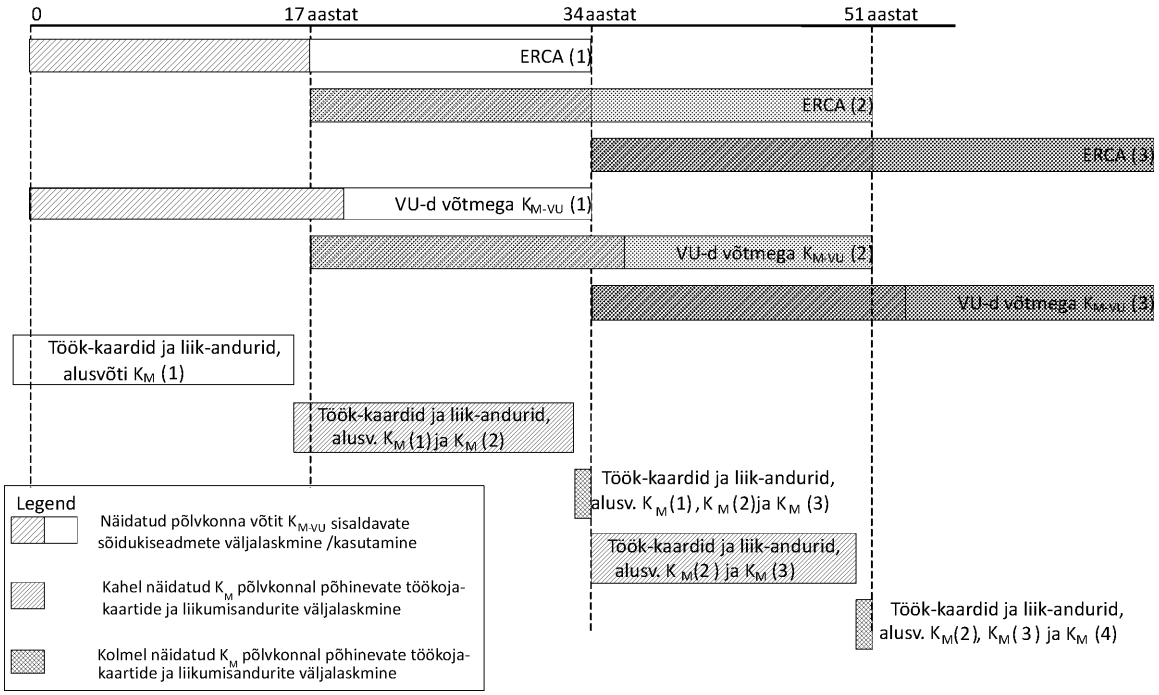
CSM_112 Liikumisanduri ühendamise ajal sõidukiseadmes loodava seansivõtme K_S pikkus peab olema seotud võtme K_{M-VU} pikkusega nii, nagu on kirjeldatud nõudes CSM_50.

9.2.1.2. *Liikumisanduri peavõtme vahetamine teise põlvkonna seadmetes*

CSM_113 Liikumisanduri iga peavõti ja kõik sellega seotud võtmed (vt tabel 3) kuuluvad ERCA juurvõtmepaari kindla põlvkonna juurde. Seega tuleb neid võtmeid iga 17 aasta järel vahetada. Liikumisanduri peavõtme iga põlvkonna kehtivusaeg algab üks aasta enne sellega seotud ERCA juurvõtmepaari kehtima hakkamist ning see lõpeb koos seotud ERCA juurvõtmepaari aegumisega. Seda on kujutatud joonisel 2.

Joonis 2.

Liikumisandurite eri põlvkonna peavõtmete väljaandmine ja kasutamine sõidukiseadmetes, liikumisandurites ja töökojakaartides



CSM_114 Vähemalt üks aasta enne Euroopa uue juurvõtmepaari loomist, nagu on kirjeldatud nõudes CSM_56, loob ERCA uute võtmete K_{M-VU} ja K_{M-WC} abil liikumisanduri uue peavõtme K_M. Liikumisanduri peavõtme pikkus peab olema seotud Euroopa uue juurvõtmepaari kavandatud pikkusega vastavalt nõudele CSM_50. Liikmesriikide sertifitseerimisasutuste nõudmisel saadab ERCA uued võtmed K_M, K_{M-VU} ja K_{M-WC} koos versiooninumbriga neile asutustele.

CSM_115 Liikmesriigi sertifitseerimisasutus tagab, et võtme K_{M-WC} kõik kehtivad põlvkonnad salvestatakse koos versiooninumbriga kõigile asutuse haldusalas välja antavatesse töökojakaartidele, nagu on kujutatud joonisel 2.

Märkus: see eeldab, et ERCA sertifikaadi kehtivuse viimasel aastal välja antavad töökojakaardid sisaldavad võtme K_{M-WC} kolme põlvkonda, nagu on kujutatud joonisel 2.

CSM_116 Nõuetes CSM_107 ja CSM_108 kirjeldatud protsessis kehtivad järgmised nõuded: liikmesriigi sertifitseerimisasutus krüpteerib liikumisandurite tootjalt saadud iga ühendamisvõtme K_P eraldi iga kehtiva põlvkonna liikumisanduri peavõtmega K_M. Liikmesriigi sertifitseerimisasutus krüpteerib ka liikumisandurite tootjalt saadud iga seerianumbri eraldi iga kehtiva põlvkonna liikumisanduri identimisvõtmega K_{ID}. Liikumisanduri tootja salvestab kõik krüpteeritud ühendamisvõtmed ja krüpteeritud seerianumbrid neile ette nähtud liikumisandurisse koos vastava võtmete lihtteksti ning krüpteerimiseks kasutatud võtmete K_M ja K_{ID} versiooninumbriga.

Märkus: see eeldab, et ERCA sertifikaadi kehtivuse viimasel aastal välja lastavad liikumisandurid sisaldavad võtme K_M kolme põlvkonna krüpteeritud andmeid, nagu on kujutatud joonisel 2.

CSM_117 Nõudes CSM_107 kirjeldatud protsessis kehtivad järgmised nõuded: kuna ühendamisvõtme K_P pikkus on seotud võtme K_M pikkusega (vt nõue CSM_100), võib liikumisandurite tootjal tekkida vajadus luua ühe liikumisanduri jaoks kuni kolm erinevat (erineva pikkusega) ühendamisvõtit juhul, kui hilisemate põlvkondade võtmed K_M on erineva pikkusega. Sellisel juhul saadab tootja liikmesriigi sertifitseerimisasutusele kõik ühendamisvõtmed. Liikmesriigi sertifitseerimisasutus tagab, et iga ühendamisvõti krüpteeritakse õigesse põlvkonda kuuluva (sama pikkusega) liikumisanduri peavõtmega.

Märkus: kui liikumisandurite tootja otsustab luua teise põlvkonna liikumisanduri jaoks standardil TDES põhineva ühendamisvõtme (vt nõue CSM_111), peab tootja liikmesriigi sertifitseerimisasutusele teatama, et selle ühendamisvõtme krüpteerimiseks tuleb kasutada standardil TDES põhinevat liikumisanduri peavõtit. Põhjuseks on asjaolu, et TDES-võti ja AES-võti võivad olla sama pikkusega, mistõttu liikmesriigi sertifitseerimisasutus ei saa lähtuda üksnes võtme pikkusest.

CSM_118 Sõidukiseadmete tootjad sisestavad igasse sõidukiseadmesse ainult ühe põlvkonna võtme K_{M-VU} ja selle versiooninumbri. Võtme K_{M-VU} loomine on seotud selle ERCA sertifikaadiga, millel põhinevad sõidukiseadme sertifikaadid.

Märkused

— *X*. põlvkonna ERCA sertifikaadil põhinev sõidukiseade võib sisaldada ainult *X*. põlvkonna võtit K_{M-VU}, isegi kui see lastakse välja pärast põlvkonna *X+1* ERCA sertifikaadi kehtivusaja algust. Seda on kujutatud joonisel 2.

— *X*. põlvkonna sõidukiseadet ei saa ühendada põlvkonda $X - 1$ kuuluva liikumisanduriga.

— Kuna töökojakaartide kehtivusaeg on üks aasta, tekib nõuete CSM_113–CSM_118 tulemusena olukord, kus esimese uut võtit K_{M-VU} sisaldava sõidukiseadme väljalaskmise hetkel sisaldavad kõik töökojakaardid juba uut võtit K_{M-WC}. Seega on sellisel sõidukiseadmel alati võimalik arvutada uus K_M. Lisaks sisaldab enamik uusi liikumisandureid selleks ajaks samuti uuel võtmel K_M põhinevaid krüpteeritud andmeid.

9.2.2. *Sihtotstarbelise lähitoimeside (DSRC) turbevõtmed*

9.2.2.1. *Üldist*

CSM_119 DSRC-kaugsidekanali kaudu sõidukiseadmest kontrolliasutusele edastatavate andmete autentsus ja konfidentsiaalsus tagatakse sõidukiseadmeomaste AES-võtmete kogumiga, mis tuletatakse ühest DSRC peavõtmest KM_{DSRC}.

CSM_120 DSRC peavõti KM_{DSRC} on AES-võti, mille turvalise loomise, säilitamise ja levitamisega tegeleb ERCA. Võtme pikkus võib olla 128, 192 või 256 bitti ning see peab olema seotud Euroopa juurvõtmepaari pikkusega, nagu on kirjeldatud nõudes CSM_50.

CSM_121 Liikmesriikide sertifitseerimisasutuste nõudel edastab ERCA DSRC peavõtme turvaliselt neile asutustele, et võimaldada neil tuletada sõidukiseadmeomaseid DSRC-võtmeid ja tagada DSRC peavõtme sisestamine kõigile nende haldusalas välja antavatele kontrolli- ja töökojakaartidele.

CSM_122 ERCA annab igale DSRC peavõtmele kordumatu versiooninumbri. Kui ERCA saadab liikmesriikide sertifitseerimisasutustele DSRC peavõtme, teatab ta neile ka versiooninumbri.

Märkus: versiooninumbrit kasutatakse DSRC peavõtme põlvkondade eristamiseks, nagu on põhjalikumalt selgitatud punktis 9.2.2.2.

CSM_123 Sõidukiseadmete tootja loob iga sõidukiseadme jaoks kordumatu seerianumbri ning saadab selle liikmesriigi sertifitseerimisasutusele, et taotleda kahte sõidukiseadmeomast DSRC-võtit. Sõidukiseadme seerianumbri andmetüüp on `VuSerialNumber`ning kodeerimiseks kasutatakse kodeeringut DER (*Distinguished Encoding Rules*) vastavalt standardile ISO 8825-1.

CSM_124 Sõidukiseadmeomaste DSRC-võtmete taotluse saamise korral tuletab liikmesriigi sertifitseerimisasutus sõidukiseadme jaoks kaks AES-võtit tähistustega K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC. Need sõidukiseadmeomased võtmed on sama pikkusega kui DSRC peavõti. Liikmesriigi sertifitseerimisasutus kasutab dokumendis RFC 5869 määratletud võtmetuletusfunktsiooni. HMAC-i räsifunktsiooni konkretiseerimiseks vajalik räsifunktsioon on seotud DSRC peavõtme pikkusega, nagu on kirjeldatud nõudes CSM_50. Dokumendis RFC 5869 määratletud võtmetuletusfunktsiooni kasutatakse järgmiselt:

1. samm (*Extract*):

— *PRK* = HMAC-Hash (*salt, IKM*), kus *salt* on tühi string '' ja *IKM* on KM_{DSRC}.

2. samm (*Expand*):

— *OKM* = *T(1)*, kus

T(1) = HMAC-Hash (*PRK, T(0)* || *info* || '01') ja

— *T(0)* = tühi string ('')

— *info* = nõudele CSM_123 vastav sõidukiseadme seerianumber

— K_VU_{DSRC}_ENC = *OKM*-i esimesed *L*-oktetid ja

K_VU_{DSRC}_MAC = *OKM*-i viimased *L*-oktetid,

kus *L* on võtmete K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC nõutav pikkus oktettides.

CSM_125 Liikmesriigi sertifitseerimisasutus saadab võtmed K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC turvaliselt sõidukiseadmete tootjale, kes sisestab need vastavasse sõidukiseadmesse.

CSM_126 Väljalaskmise ajal peavad sõidukiseadme turvatud mällu olema salvestatud võtmed K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC, mis võimaldavad tagada kaugsidekanali kaudu saadetud andmete tervikluse, autentsuse ja konfidentsiaalsuse. Sõidukiseadmesse peab olema salvestatud ka nende sõidukiseadmeomaste võtmete tuletamiseks kasutatud DSRC peavõti.

CSM_127 Väljaandmise ajal peab kontrollikaartide ja töökojakaartide turvatud mällu olema salvestatud võti KM_{DSRC}, mis võimaldab sõidukiseadmest kaugsidekanali kaudu saadetud andmete terviklust ja autentsust kontrollida ning neid andmed dekrüpteerida. Kontrolli- ja töökojakaartidele peab olema salvestatud ka DSRC peavõtme versiooninumber.

Märkus: vastavalt punktis 9.2.2.2 esitatud selgitusele võib praktikas tekkida vajadus sisestada ühele töökoja- või kontrollikaardile mitme põlvkonna võtmeid KM_{DSRC}.

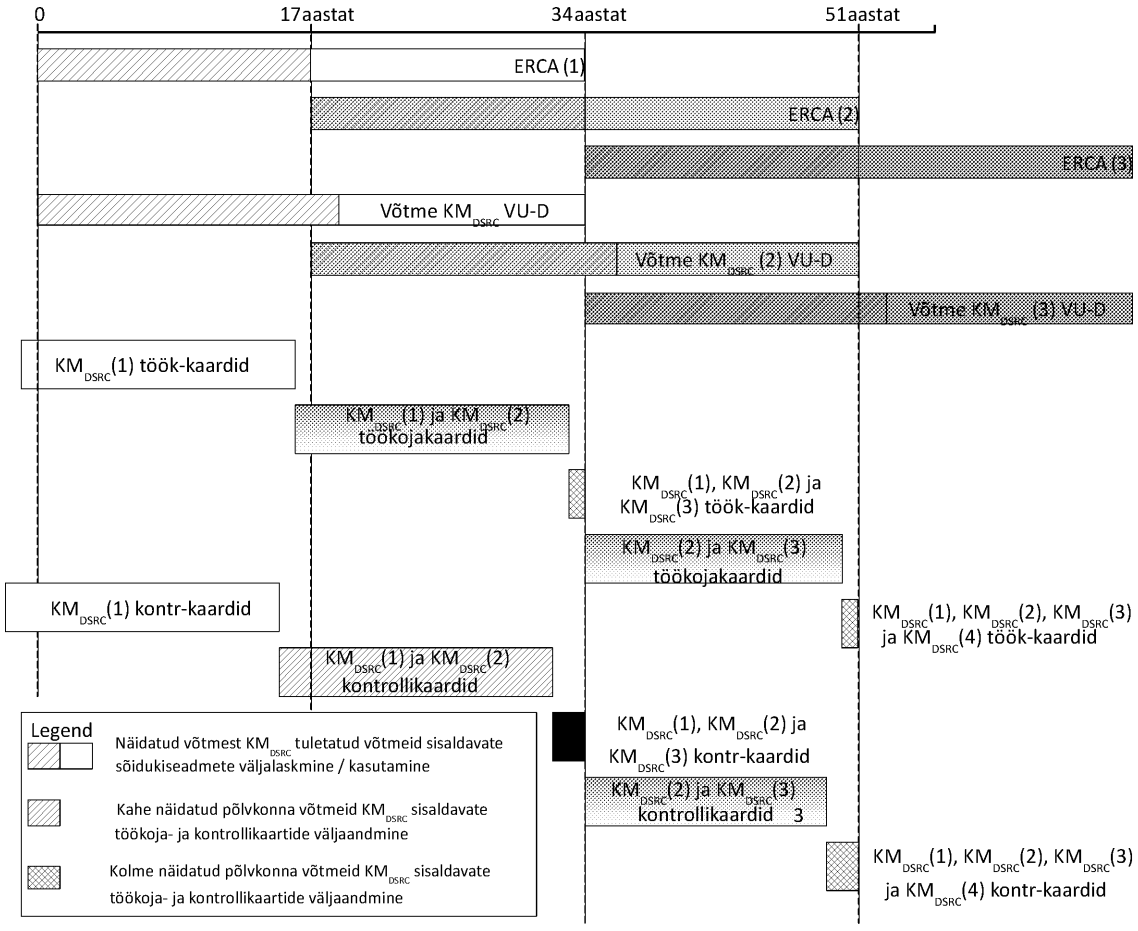
CSM_128 Liikmesriigi sertifitseerimisasutus peab arvestust kõigi loodud sõidukiseadmeomaste DSRC võtmete, nende versiooninumbri ja iga võtmekomplektiga kasutatava sõidukiseadme identimisandmete kohta.

9.2.2.2. *DSRC peavõtme vahetamine*

CSM_129 Iga DSRC peavõti kuulub ERCA juurvõtmepaari kindla põlvkonna juurde. Seega peab ERCA DSRC peavõtmeid iga 17 aasta järel vahetama. DSRC peavõtme põlvkonna kehtivusaeg algab kaks aastat enne sellega seotud ERCA juurvõtmepaari kehtima hakkamist ning see lõpeb koos seotud ERCA juurvõtmepaari aegumisega. Seda on kujutatud joonisel 3.

Joonis 3.

Eri põlvkonna DSERC peavõtmete väljaandmine ja kasutamine sõidukiseadmetes, töökoja- ja kontrollikaartides



CSM_130 Vähemalt kaks aastat enne Euroopa uue juurvõtmepaari loomist, nagu on kirjeldatud nõudes CSM_56, loob ERCA uue DSRC peavõtme. DSRC-võtme pikkus on seotud Euroopa uue juurvõtmepaari kavandatud pikkusega vastavalt nõudele CSM_50. Liikmesriikide sertifitseerimisasutuste nõudmisel saadab ERCA uue DSRC peavõtme koos versiooninumbriga neile asutustele.

CSM_131 Liikmesriigi sertifitseerimisasutus tagab, et võtme KM_{DSRC} kõik kehtivad põlvkonnad salvestatakse koos versiooninumbriga kõigile asutuse haldusalas välja antavatele kontrollikaartidele, nagu on kujutatud joonisel 3.

Märkus: see eeldab, et ERCA sertifikaadi kehtivuse kahel viimasel aastal välja antavad kontrollikaardid sisaldavad võtme KM_{DSRC} kolme eri põlvkonda, nagu on kujutatud joonisel 3.

CSM_132 Liikmesriigi sertifitseerimisasutus tagab, et võtme KM_{DSRC} kõik põlvkonnad, mis on kehtinud vähemalt ühe aasta ja on endiselt kehtivad, salvestatakse koos versiooninumbriga kõigile asutuse haldusalas välja antavatele töökojakaartidele, nagu on kujutatud joonisel 3.

Märkus: see eeldab, et ERCA sertifikaadi kehtivuse viimasel aastal välja antavad töökojakaardid sisaldavad võtme KM_{DSRC} kolme eri põlvkonda, nagu on kujutatud joonisel 3.

CSM_133 Sõidukiseadmete tootjad sisestavad igasse sõidukiseadmesse ainult ühe sõidukiseadmeomaste DSRC-võtmete komplekti ja selle versiooninumbri. See võtmekomplekt tuletatakse võtmest KM_{DSRC}, mis kuulub sõidukiseadme sertifikaatide aluseks oleva ERCA sertifikaadiga samasse põlvkonda.

Märkused

— See eeldab, et *X*. põlvkonna ERCA sertifikaadil põhinev sõidukiseade võib sisaldada ainult *X*. põlvkonna võtmeid K-VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC, isegi kui sõidukiseade lastakse välja pärast põlvkonna *X+1* ERCA sertifikaadi kehtivusaja algust. Seda on kujutatud joonisel 3.

— Kuna töökojakaardid kehtivad ühe aasta ja kontrollikaardid kaks aastat, tekib nõuete CSM_131–CSM_133 tulemusena olukord, kus vastaval peavõtmel põhinevaid sõidukiseadmeomaseid võtmeid sisaldavate esimeste sõidukiseadmete väljalaskmise hetkel sisaldavad kõik töökoja- ja kontrollikaardid juba uut DSRC peavõtit.

9.3. **Sertifikaadid**

9.3.1. *Üldist*

CSM_134 Kõik Euroopa arukate sõidumeerikute süsteemis kasutatavad sertifikaadid peavad olema standardite ISO 7816-4 ja ISO 7816-8 kohaselt ennast kirjeldavad (*self-descriptive*) ja kaardiga tõendatavad (*card-verifiable*).

CSM_135 Sertifikaatides sisalduva mõlema ASN.1 andmestruktuuri ja (rakendusspetsiifiliste) andmeobjektide kodeerimiseks kasutatakse kodeeringut DER vastavalt standardile ISO 8825-1.

Märkus: nimetatud kodeerimise tulemuseks on järgmine sildi-pikkuse-väärtuse (*Tag-Length-Value*, TLV) struktuur:

Silt: silt kodeeritakse ühes või kahes oktetis ja see osutab sisule.

Pikkus: pikkus kodeeritakse märgita täisarvuna ühes, kahes või kolmes oktetis, mis annab maksimaalseks pikkuseks 65 535 oktetti. Kasutatakse minimaalset oktettide arvu.

Väärtus: väärtus kodeeritakse nullis või enamas oktettides.

9.3.2. *Sertifikaatide sisu*

CSM_136 Kõigil sertifikaatidel peab olema tabelis 4 näidatud sertifikaadiprofiili struktuur.

Tabel 4.

Sertifikaadiprofiili versioon 1

Väli	Välja ID	Silt	Pikkus (baiti)	ASN.1 andmetüüp (vt 1. liide)
ECC sertifikaat	C	‘7F 21’	var	
ECC sertifikaadi keha	B	‘7F 4E’	var	

Väli	Välja ID	Silt	Pikkus (baiti)	ASN.1 andmetüüp (vt 1. liide)
Sertifikaadiprofiili identifikaator	CPI	'5F 29'	'01'	`INTEGER(0..255)`
Sertifitseerimisasutuse viide	CAR	'42'	'08'	`KeyIdentifier`
Sertifikaadi omaniku luba	CHA	'5F 4C'	'07'	`CertificateHolder Authorisation`
Avalik võti	PK	'7F 49'	var	
Domeeniparameetrid	DP	'06'	var	`OBJECT IDENTIFIER`
Avalik punkt	PP	'86'	var	`OCTET STRING`
Sertifikaadi omaniku viide	CHR	'5F 20'	'08'	`KeyIdentifier`
Sertifikaadi jõustumiskuupäev	CEfD	'5F 25'	'04'	`TimeReal`
Sertifikaadi aegumiskuupäev	CExD	'5F 24'	'04'	`TimeReal`
ECC sertifikaadi allkiri	S	'5F 37'	var	`OCTET STRING`

Märkus: Välja ID-d kasutatakse käesoleva liite järgnevates punktides sertifikaadi üksikute väljade tähistamiseks; näiteks X.CAR on kasutaja X sertifikaadis nimetatud sertifitseerimisasutuse viide.

9.3.2.1. Sertifikaadiprofiili identifikaator

CSM_137 Sertifikaatides kasutatav sertifikaadiprofiili identifikaator näitab, millist sertifikaadiprofiili kasutatakse. Tabelis 4 esitatud versioonile 1 vastab identifikaatori väärtus '00'.

9.3.2.2. Sertifitseerimisasutuse viide

CSM_138 Sertifitseerimisasutuse viide näitab, millist avalikku võtit tuleb sertifikaadi allkirja kontrollimiseks kasutada. Seega peab sertifitseerimisasutuse viide olema võrdne vastava sertifitseerimisasutuse sertifikaadis oleva sertifikaadi omaniku viitega.

CSM_139 ERCA juursertifikaat peab olema isesigneeritud (*self-signed*), st sertifikaadis sisalduv sertifitseerimisasutuse viide ja sertifikaadi omaniku viide peavad olema võrdsed.

CSM_140 ERCA lülisertifikaadi puhul peab sertifikaadi omaniku viide olema võrdne ERCA uue juursertifikaadi sertifikaadi omaniku viitega. Lülisertifikaadis sisalduv sertifitseerimisasutuse viide peab olema võrdne ERCA eelmise juursertifikaadi sertifikaadi omaniku viitega.

9.3.2.3. Sertifikaadi omaniku luba

CSM_141 Sertifikaadi omaniku luba kasutatakse sertifikaadi tüübi tuvastamiseks. See koosneb sõidumeerikurakenduse identifikaatori kuuest kõige tähtsamast baidist, mis on ühendatud seadme tüübiga, mille jaoks sertifikaat on antud.

9.3.2.4. Avalik võti

Avalik võti sisaldab kahte andmeelementi: standardsed domeeniparameetrid, mida kasutatakse sertifikaadis oleva avaliku võtmega, ja avaliku punkti väärtus.

CSM_142 Domeeniparameetrite (*Domain Parameters*) andmeelement peab sisaldama ühte tabelis 1 määratletud objekti identifikaatorit, mis viitab ühele standardsete domeeniparameetrite kogumile.

CSM_143 Avaliku punkti (*Public Point*) andmeelement peab sisaldama avalikku punkti. Elliptiliste kõverate avalikud punktid teisendatakse oktetistringideks vastavalt tehnilisele eeskirjale TR-03111. Kasutatakse tihendamata kodeerimisvormingut. Elliptilise kõvera punkti taastamisel kodeeritud vormingust tehakse alati tehnilises eeskirjas TR-03111 kirjeldatud kontrollid.

9.3.2.5. Sertifikaadi omaniku viide

CSM_144 Sertifikaadi omaniku viide on sertifikaadis oleva avaliku võtme identifikaator. Seda kasutatakse teistes sertifikaatides sellele avalikule võtmele viitamiseks.

CSM_145 Kaartide ja GNSSi välisseadmete sertifikaatides kasutatakse sertifikaadi omaniku viite jaoks 1. liites määratletud andmetüüpi `ExtendedSerialNumber`.

CSM_146 Sõidukiseadmete puhul võib, aga ei pruugi sertifikaati taotlev tootja teada sõidukiseadme toojaomast seerianumbrit, mille jaoks vastav sertifikaat ja sellega seotud privaatvõti on ette nähtud. Esimesel juhul kasutatakse sertifikaadi omaniku viite jaoks 1. liites määratletud andmetüüpi `ExtendedSerialNumber`. Teisel juhul kasutatakse sertifikaadi omaniku viite jaoks 1. liites määratletud andmetüüpi `CertificateRequestID`.

CSM_147 ERCA ja liikmesriigi sertifitseerimisasutuse sertifikaatides kasutatakse sertifikaadi omaniku viite jaoks 1. liites määratletud andmetüüpi `CertificationAuthorityKID`.

9.3.2.6. Sertifikaadi jõustumiskuupäev

CSM_148 Sertifikaadi jõustumiskuupäev näitab, sertifikaadi kehtivusaja alguse kuupäeva ja kellaaega. Sertifikaadi jõustumiskuupäev vastab sertifikaadi põlvkonna kuupäevale.

9.3.2.7. Sertifikaadi aegumiskuupäev

CSM_149 Sertifikaadi aegumiskuupäev näitab, sertifikaadi kehtivusaja lõppemise kuupäeva ja kellaaega.

9.3.2.8. Sertifikaadi allkiri

CSM_150 Sertifikaadi allkiri luuakse sertifikaadi kodeeritud keha peale, mis hõlmab ka sertifikaadi keha silti ja pikkust. Allkirja algoritm on standardis DSS kirjeldatud ECDSA ning vastavalt nõudele CSM_50 kasutatakse allkirjastava asutuse võtmesuurusega seotud räsialgoritmi. Allkirja vorming on tehnilises eeskirjas TR-03111 kirjeldatud lihtvorming.

9.3.3. *Sertifikaatide taotlemine*

CSM_151 Sertifikaadi taotlemisel saadab taotleja oma sertifitseerimisasutusele järgmised andmed:

— taotletava sertifikaadi sertifikaadiprofiili identifikaator;

— sertifitseerimisasutuse viide, mida eeldatavasti sertifikaadi allkirjastamiseks kasutatakse;

— allkirjastatav avalik võti.

CSM_152 Liikmesriigi sertifitseerimisasutus saadab ERCA-le esitatavas sertifikaaditaotluses lisaks nõudes CSM_151 nimetatud andmetele järgmised andmed, mis võimaldavad ERCA-l luua liikmesriigi sertifitseerimisasutuse uue sertifikaadi jaoks sertifikaadi omaniku viite:

— sertifitseerimisasutuse numbriline riigikood (1. liites määratletud andmetüüp `NationNumeric`);

— sertifitseerimisasutuse tähtnumbriline riigikood (1. liites määratletud andmetüüp `NationAlpha`);

— ühebaidine seerianumber, mille järgi eristatakse võtmete vahetamise korral sertifitseerimisasutuse erinevaid võtmeid;

— kahebaidine väli, mis sisaldab sertifitseerimisasutuse eriomast lisateavet.

CSM_153 Seadmetootja saadab liikmesriigi sertifitseerimisasutusele esitatavas sertifikaaditaotluses lisaks nõudes CSM_151 nimetatud andmetele järgmised andmed, mis võimaldavad liikmesriigi sertifitseerimisasutusel luua uue seadmesertifikaadi jaoks sertifikaadi omaniku viite:

— tootjaomane seadmetüübi identifikaator;

— tootja, seadmetüübi, ja tootmiskuu piires kordumatu seadme seerianumber, kui see on teada (vt nõue CSM_154); muul juhul sertifikaaditaotluse kordumatu identifikaator;

— seadme tootmise või sertifikaadi taotlemise kuu ja aasta.

Tootja tagab, et nimetatud andmed on õiged ning liikmesriigi sertifitseerimisasutuselt saadud sertifikaat sisestatakse seadmesse, mille jaoks see on ette nähtud.

CSM_154 Sõidukiseadmete puhul võib, aga ei pruugi sertifikaati taotlev tootja teada sõidukiseadme toojaomast seerianumbrit, mille jaoks vastav sertifikaat ja sellega seotud privaatvõti on ette nähtud. Kui seerianumber on teada, saadab sõidukiseadme tootja selle liikmesriigi sertifitseerimisasutusele. Kui seerianumber ei ole teada, kasutab tootja igal sertifikaaditaotlusel kordumatut identifikaatorit ning saadab selle sertifikaaditaotluse seerianumbri liikmesriigi sertifitseerimisasutusele. Saadav sertifikaat sisaldab sel juhul sertifikaaditaotluse seerianumbrit. Pärast sertifikaadi sisestamist konkreetsesse sõidukiseadmesse edastab tootja liikmesriigi sertifitseerimisasutusele andmed, mis võimaldavad seostada sertifikaaditaotluse seerianumbrit sõidukiseadme identimisandmetega.

10. SÕIDUKISEADME JA KAARDI VASTASTIKUNE AUTENTIMINE JA TURVALINE SÕNUMIVAHETUS

10.1. **Üldist**

CSM_155 Üldiselt kirjeldades peab sõidukiseadme ja sõidumeerikukaardi vaheline turvaline side põhinema järgmistel etappidel:

— Esiteks tõendab kumbki pool teisele, et tal on kehtiv avaliku võtme sertifikaat, mille on allkirjastanud liikmesriigi sertifitseerimisasutus. Liikmesriigi sertifitseerimisasutuse avaliku võtme sertifikaadi peab omakorda olema allkirjastanud Euroopa juursertifikaatide asutus. Seda etappi nimetatakse sertifikaadiahela kontrollimiseks ja seda on üksikasjalikult kirjeldatud punktis 10.2.

— Teiseks tõendab sõidukiseade kaardile, et sel on olemas privaatvõti, mis vastab esitatud sertifikaadis olevale avalikule võtmele. Selleks allkirjastab sõidukiseade kaardi saadetud juhusliku numbri. Kaart kontrollib juhuslikule numbrile antud allkirja. Kui kontroll õnnestub, siis on sõidukiseade autenditud. Seda etappi nimetatakse sõidukiseadme autentimiseks ja seda on üksikasjalikult kirjeldatud punktis 10.3.

— Kolmandaks arvutavad mõlemad pooled sõltumatult kaks AES-i seansivõtit, kasutades asümmeetrilist võtmete kooskõlastamise algoritmi. Kaart kasutab ühte nendest seansivõtmetest, et luua sõidukiseadme saadetud andmetele sõnumiautentimiskood (MAC). Sõidukiseade kontrollib MAC-i. Kui kontroll õnnestub, siis on kaart autenditud. Seda etappi nimetatakse kaardi autentimiseks ja seda on üksikasjalikult kirjeldatud punktis 10.4.

— Neljandaks kasutavad sõidukiseade ja kaart kooskõlastatud seansivõtmeid kõigi vahetatud sõnumite konfidentsiaalsuse, tervikluse ja autentsuse tagamiseks. Seda nimetatakse turvaliseks sõnumivahetuseks ja seda on üksikasjalikult kirjeldatud punktis 10.5.

CSM_156 Sõidukiseade käivitab nõudes CSM_155 kirjeldatud mehhanismi iga kord, kui selle kaardiavasse sisestatakse kaart.

10.2. **Vastastikune sertifikaadiahela kontrollimine**

10.2.1. *Kaardi sertifikaadiahela kontrollimine sõidukiseadmega*

CSM_157 Sõidukiseadmed kasutavad sõidumeerikukaardi sertifikaadiahela kontrollimiseks joonisel 4 kujutatud protokolli.

Märkused joonise 4 kohta

— Joonisel on kujutatud neid kaardisertifikaate ja avalikke võtmeid, mida kasutatakse vastastikuseks autentimiseks. Punktis 9.1.5 kasutatakse nende kohta tähistust Card_MA.

— Joonisel on kujutatud neid Card.CA sertifikaate ja avalikke võtmeid, mida kasutatakse kaardisertifikaatide allkirjastamiseks ja millele osutab kaardisertifikaadis olev sertifitseerimisasutuse viide. Punktis 9.1.3 kasutatakse nende kohta tähistust MSCA_Card.

— Joonisel kujutatud sertifikaat Card.CA.EUR on Euroopa juursertifikaat, millele osutatakse sertifikaadis Card.CA sisalduvas sertifitseerimisasutuse viites.

— Joonisel kujutatud sertifikaat Card.Link tähistab kaardi lülisertifikaati, kui see on olemas. Vastavalt punktile 9.1.2 on tegemist Euroopa uue juurvõtmepaari lülisertifikaadiga, mille loob ERCA ja mis allkirjastatakse Euroopa eelmise privaatvõtmega.

— Sertifikaat Card.Link.EUR on Euroopa juursertifikaat, millele osutatakse sertifikaadis Card.Link sisalduvas sertifitseerimisasutuse viites.

CSM_158 Nagu on näha jooniselt 4, algab kaardi sertifikaadiahela kontrollimine kaardi sisestamise hetkel. Sõidukiseade loeb failist EF ICC kaardi omaniku viite (`cardExtendedSerialNumber`). Sõidukiseade kontrollib, kas tegemist on tuttava kaardiga ehk kas ta on kaardi sertifikaadiahelat varem juba kontrollinud ja selle edaspidiseks kasutamiseks salvestanud. Kui see on nii ja kaardi sertifikaat on veel kehtiv, jätkub protsess sõidukiseadme sertifikaadiahela kontrollimisega. Muul juhul loeb sõidukiseade kaardilt järjest sertifikaadi MSCA_Card, mida kasutatakse kaardisertifikaadi kontrollimiseks, sertifikaadi Card.CA.EUR, mida kasutatakse sertifikaadi MSCA_Card kontrollimiseks, ning vajaduse korral lülisertifikaadi. Lugemist jätkatakse seni, kuni sõidukiseade leiab tuttava sertifikaadi või sellise sertifikaadi, mida ta saab kontrollida. Sellise sertifikaadi leidmise korral kasutab sõidukiseade seda kaardilt leitud kaardisertifikaatide kontrollimiseks. Kui see õnnestub, jätkub protsess sõidukiseadme sertifikaadiahela kontrollimisega. Kui see ebaõnnestub, siis sõidukiseade ignoreerib kaarti.

Märkus. On kolm võimalust, kuidas sertifikaat Card.CA.EUR võib sõidukiseadmele tuttavaks saada:

— sertifikaat Card.CA.EUR langeb kokku sõidukiseadme enda EUR-sertifikaadiga;

— sertifikaat Card.CA.EUR on varasem kui sõidukiseadme enda EUR-sertifikaat, mistõttu see oli sõidukiseadmesse sisestatud juba sõidukiseadme väljalaskmise ajal (vt nõue CSM_81);

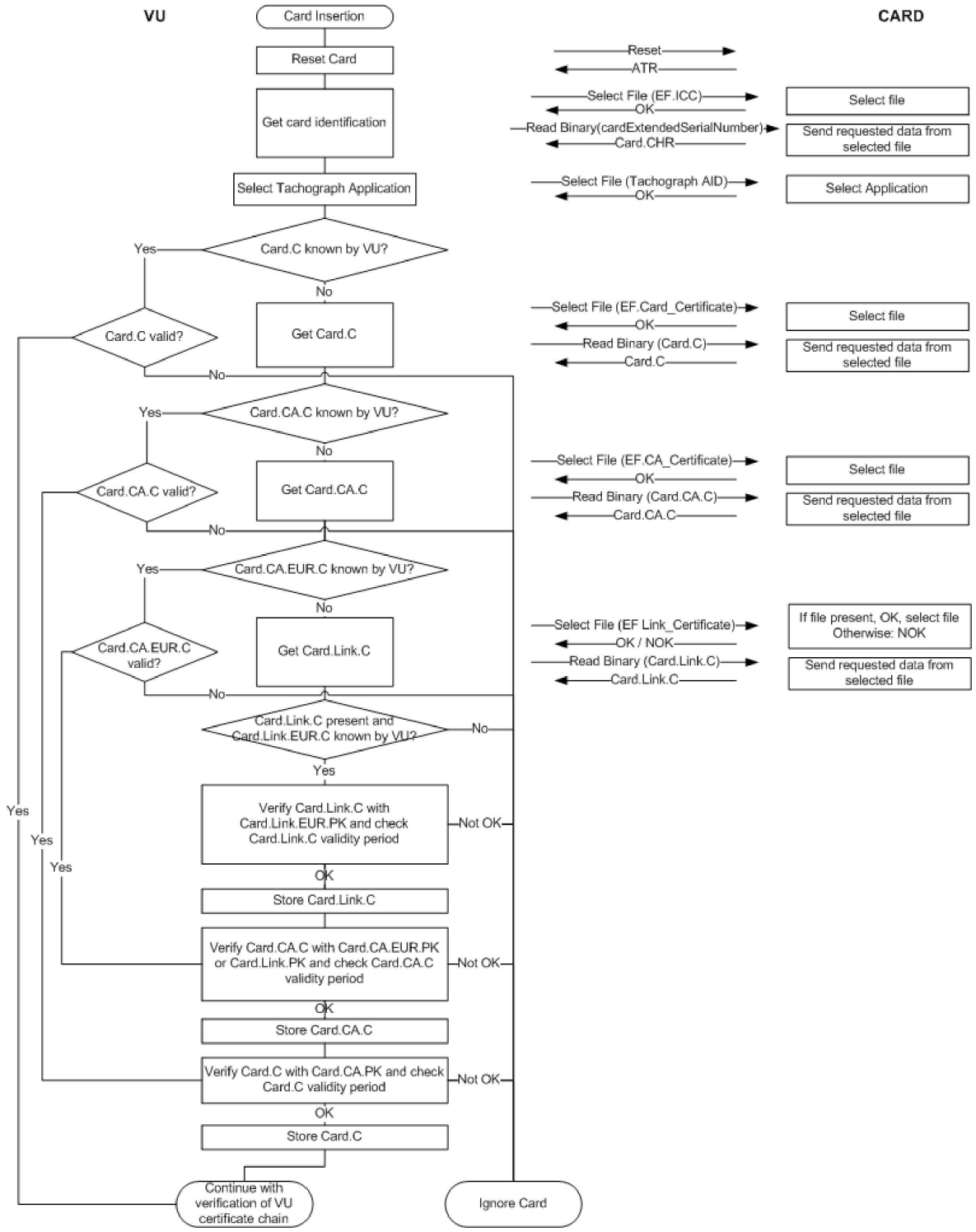
— sertifikaat Card.CA.EUR on hilisem kui sõidukiseadme enda EUR-sertifikaat ning sõidukiseade on saanud varem mõnelt muult sõidumeerikukaardilt lülisertifikaadi, on seda kontrollinud ja selle edaspidiseks kasutamiseks salvestanud.

CSM_159 Jooniselt 4 nähtub, et kui sõidukiseade on varem tundmatu sertifikaadi autentsust ja kehtivust kontrollinud, võib ta salvestada selle sertifikaadi edaspidiseks kasutamiseks, nii et ta ei pea järgmisel korral enam selle sertifikaadi autentsust kontrollima. Kogu sertifikaadi salvestamise asemel võib sõidukiseade salvestada ka ainult sertifikaadi keha sisu, mida on kirjeldatud punktis 9.3.2.

CSM_160 Sõidukiseade kontrollib kõigi kaardilt loetud või oma mällu salvestatud sertifikaatide ajalist kehtivust ja lükkab tagasi aegunud sertifikaadid. Kaardi esitatud sertifikaadi ajalise kehtivuse kontrollimiseks kasutab sõidukiseade oma sisemist kella.

Joonis 4.

Kaardi sertifikaadiahela sõidukiseadmega kontrollimise protokoll

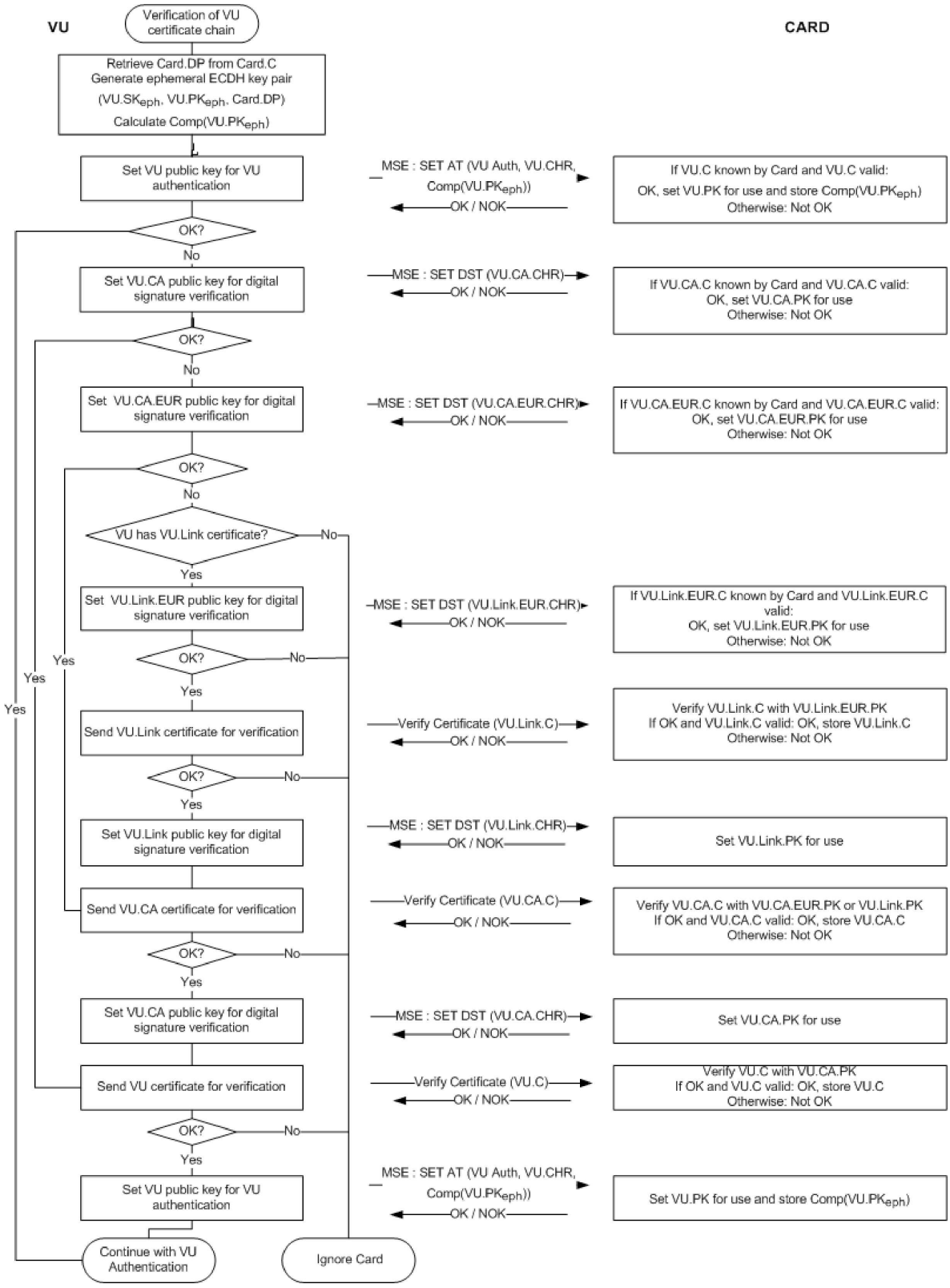


10.2.2. *Sõidukiseadme sertifikaadiahela kontrollimine kaardiga*

CSM_161 Sõidumeerikukaardid kasutavad sõidukiseadme sertifikaadiahela kontrollimiseks joonisel 5 kujutatud protokolli.

Joonis 5.

Sõidukiseadme sertifikaadiahela kaardiga kontrollimise protokoll



Märkused joonise 5 kohta

— Joonisel on kujutatud neid sõidukiseadme sertifikaate ja avalikke võtmeid, mida kasutatakse vastastikuseks autentimiseks. Punktis 9.1.4 kasutatakse nende kohta tähistust VU_MA.

— Joonisel on kujutatud neid VU.CA sertifikaate ja avalikke võtmeid, mida kasutatakse sõidukiseadme ja GNSSi välisseadme sertifikaatide allkirjastamiseks. Punktis 9.1.3 kasutatakse nende kohta tähistust MSCA_VU-EGF.

— Joonisel kujutatud sertifikaat Card.CA.EUR on Euroopa juursertifikaat, millele osutatakse sertifikaadis VU.CA sisalduvas sertifitseerimisasutuse viites.

— Joonisel kujutatud sertifikaat VU.Link tähistab sõidukiseadme lülisertifikaati, kui see on olemas. Vastavalt punktile 9.1.2 on tegemist Euroopa uue juurvõtmepaari lülisertifikaadiga, mille loob ERCA ja mis allkirjastatakse Euroopa eelmise privaatvõtmega.

— Sertifikaat VU.Link.EUR on Euroopa juursertifikaat, millele osutatakse sertifikaadis VU.Link sisalduvas sertifitseerimisasutuse viites.

CSM_162 Nagu on näha jooniselt 5, algab sõidukiseadme sertifikaadiahela kontrollimine sellega, et sõidukiseade püüab määrata oma avalikku võtit sõidumeerikukaardil kasutamiseks. Kui see õnnestub, siis on kaart sõidukiseadme sertifikaadiahelat varem juba kontrollinud ja on sõidukiseadme sertifikaadi edaspidiseks kasutamiseks salvestanud. Sellisel juhul on sõidukiseadme sertifikaat kasutamiseks valmis ja protsess jätkub sõidukiseadme autentimisega. Kui sõidukiseadme sertifikaat ei ole kaardile tuttav, esitab sõidukiseade kaardile järjest sertifikaadi VU.CA, mida kasutatakse sõidukiseadme sertifikaadi kontrollimiseks, sertifikaadi VU.CA.EUR, mida kasutatakse sertifikaadi VU.CA kontrollimiseks, ning vajaduse korral lülisertifikaadi, et leida mõni selline sertifikaat, mis on kaardile tuttav või mida kaart saab kontrollida. Sellise sertifikaadi leidmise korral kasutab kaart seda talle esitatud sõidukiseadme sertifikaatide kontrollimiseks. Kui see õnnestub, määrab sõidukiseade oma avaliku võtme sõidumeerikukaardil kasutamiseks. Kui see ebaõnnestub, siis sõidukiseade ignoreerib kaarti.

Märkus. On kolm võimalust, kuidas sertifikaat VU.CA.EUR võib kaardile tuttavaks saada:

— sertifikaat VU.CA.EUR langeb kokku kaardi enda EUR-sertifikaadiga;

— sertifikaat VU.CA.EUR on varasem kui kaardi enda EUR-sertifikaat, mistõttu see oli kaardile sisestatud juba kaardi väljaandmise ajal (vt nõue CSM_91);

— sertifikaat VU.CA.EUR on hilisem kui kaardi enda EUR-sertifikaat ning kaart on saanud varem mõnelt muult sõidukiseadmelt lülisertifikaadi, on seda kontrollinud ja selle edaspidiseks kasutamiseks salvestanud.

CSM_163 Sõidukiseade kasuta käsku MSE: Set AT, et määrata oma avalik võti sõidumeerikukaardil kasutamiseks. Vastavalt 2. liitele sisaldab see käsk viidet krüptograafilisele mehhanismile, mida kasutatakse koos määratud võtmega. Kasutatakse mehhanismi „sõidukiseadme autentimine ECSDA algoritmi ja räsialgoritmiga, mis on seotud sõidukiseadme võtmepaari VU_MA suurusega vastavalt nõudele CSM_50“.

CSM_164 Käsk MSE: Set AT sisaldab ka viidet lühiajalisele võtmepaarile, mida sõidukiseade kasutab seansivõtme kooskõlastamise ajal (vt punkt 10.4). Seega loob sõidukiseade enne käsu MSE: Set AT saatmist lühiajalise ECC võtmepaari. Sõidukiseade kasutab lühiajalise võtmepaari loomiseks kaardi sertifikaadis märgitud standardseid domeeniparameetreid. Lühiajalise võtmepaari kohta kasutatakse tähistust $VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP. Sõidukiseade võtab võtme identimise aluseks ECDH lühiajalise avaliku punkti; seda nimetatakse avaliku võtme tihendatud esituseks, mille kohta kasutatakse tähistust $Comp(VU.PK_{eph})$.

CSM_165 Kui käsk MSE: Set AT täidetakse, määrab kaart osutatud võtme VU.PK edasiseks kasutamiseks sõidukiseadme autentimise käigus ja salvestab ajutiselt väärtuse $Comp(VU.PK_{eph})$. Kui enne seansivõtme kooskõlastamist saadetakse järjest kaks või rohkem käsku MSE: Set AT, salvestab kaart ainult viimase saabunud väärtuse $Comp(VU.PK_{eph})$.

CSM_166 Kaart kontrollib kõigi sõidukiseadme esitatud või kaardi mällu salvestatud ja sõidukiseadme viidatud sertifikaatide ajalist kehtivust ja lükkab tagasi aegunud sertifikaadid.

CSM_167 Sõidukiseadme esitatud sertifikaadi ajalise kehtivuse kontrollimiseks peab igasse sõidumeerikukaarti olema salvestatud hetkeajale vastavaid andmeid. Need andmed ei tohi olla sõidukiseadmega otseselt uuendatavad. Kaardi väljaandmisel seadistatakse kaardi hetkeaeg võrdseks kaardi sertifikaadi Card_MA jõustumiskuupäevaga. Kaart uuendab oma hetkeaega siis, kui sõidukiseadme esitatud autentse „kehtiva ajaallika" sertifikaadi jõustumiskuupäev on hilisem kui kaardi hetkeaeg. Sellisel juhul määrab kaart oma hetkeajaks nimetatud sertifikaadi jõustumiskuupäeva. Kaart aktsepteerib kehtiva ajaallikana ainult järgmisi sertifikaate:

— ERCA teise põlvkonna lülisertifikaadid;

— liikmesriigi sertifitseerimisasutuse teise põlvkonna sertifikaadid;

— sõidumeeriku teise põlvkonna sertifikaadid, mille välja andnud riik on ka kaardi sertifikaadi (sertifikaatide) väljaandja.

Märkus: viimane nõue eeldab, et kaart suudab ära tunda sõidukiseadme sertifikaadi sertifitseerimisasutuse viite ehk sertifikaadi MSCA_VU-EGF. See ei ole sama mis kaardi enda sertifikaadi sertifitseerimisasutuse viide, milleks on sertifikaat MSCA_Card.

CSM_168 Jooniselt 5 nähtub, et kui kaart on varem tundmatu sertifikaadi autentsust ja kehtivust kontrollinud, võib ta salvestada selle sertifikaadi edaspidiseks kasutamiseks, nii et ta ei pea järgmisel korral enam selle sertifikaadi autentsust kontrollima. Kogu sertifikaadi salvestamise asemel võib kaart salvestada ka ainult sertifikaadi keha sisu, mida on kirjeldatud punktis 9.3.2.

10.3. **Sõidukiseadme autentimine**

CSM_169 Sõidukiseadmed ja kaardid peavad kasutama sõidukiseadme kaardi suhtes autentimiseks joonisel 6 kujutatud protokolli. Sõidukiseadme autentimine võimaldab sõidumeerikukaardil otseselt kontrollida sõidukiseadme autentsust. Selleks allkirjastab sõidukiseade oma privaatvõtmega kaardi genereeritud väljakutse.

CSM_170 Lisaks kaardi väljakutsele lisab sõidukiseade allkirjale kaardi omaniku viite, mis on võetud kaardi sertifikaadist.

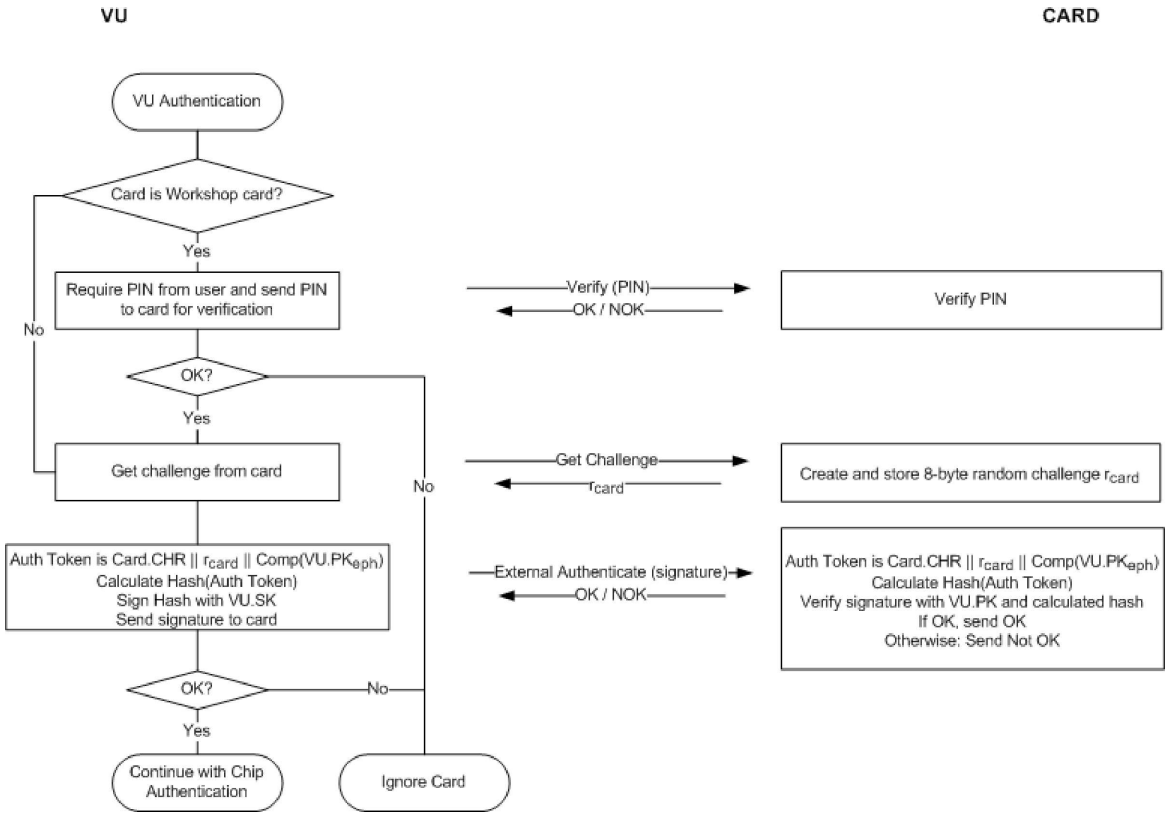
Märkus: see tagab, et kaart, mille suhtes sõidukiseade ennast autendib, on sama kaart, mille sertifikaadiahelat sõidukiseade varem kontrollis.

CSM_171 Sõidukiseade lisab allkirjale ka lühiajalise avaliku võtme Comp(VU.PK_{eph}) identifikaatori. Sõidukiseade kasutab seda avalikku võtit punktis 10.4 kirjeldatud kiibi autentimise ajal turvalise sõnumivahetuse seadistamiseks.

Märkus: sellega tagatakse, et sõidukiseade, millega kaart turvalise sõnumivahetuse ajal andmeid vahetab, on sama sõidukiseade, mille kaart on autentinud.

Joonis 6.

Sõidukiseadme autentimisprotokoll



CSM_172 Kui sõidukiseade saadab sõidukiseadme autentimise ajal mitu käsku GET CHALLENGE, saadab kaart iga kord tagasi 8-baidise juhusliku väljakutse, kuid salvestab neist ainult viimase.

CSM_173 Sõidukiseadme autentimiseks kasutatav allkirjastamisalgoritm on standardis DSS kirjeldatud ECSDA, milles kasutatakse räsialgoritmi, mis on seotud sõidukiseadme võtmepaari VU_MA võtmesuurusega vastavalt nõudele CSM_50. Allkirja vorming on tehnilises eeskirjas TR-03111 kirjeldatud lihtvorming. Sõidukiseade saadab loodud allkirja kaardile.

CSM_174 Pärast sõidukiseadme allkirja kättesaamist käsuga EXTERNAL AUTHENTICATE teeb kaart järgmised toimingud:

— arvutab autentimistõendi, ühendades sertifikaadi omaniku viite Card.CHR, kaardi väljakutse r_{card} ja sõidukiseadme lühiajalise avaliku võtme identifikaatori Comp($VU.PK_{eph}$);

— arvutab autentimistõendi kohta räsiväärtuse, kasutades räsialgoritmi, mis on seotud sõidukiseadme võtmepaari VU_MA võtmesuurusega vastavalt nõudele CSM_50;

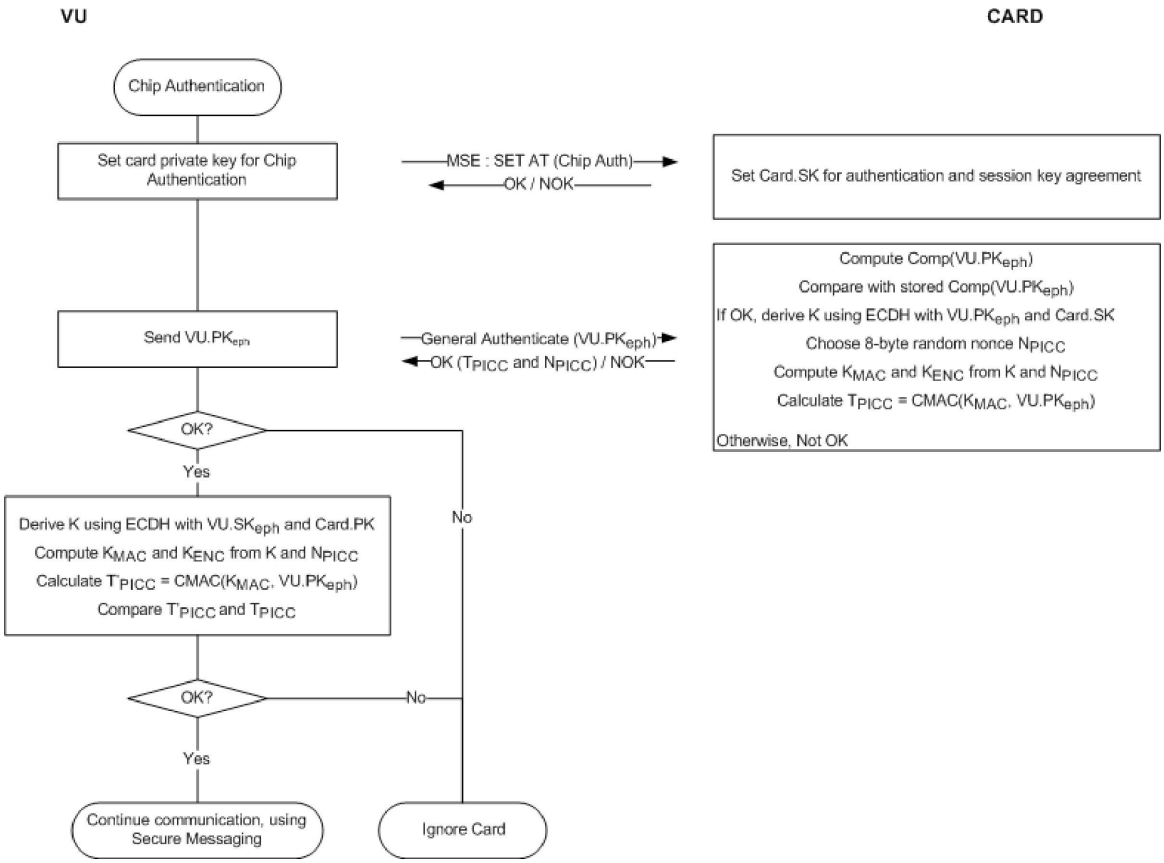
— kontrollib sõidukiseadme allkirja, kasutades ECDSA algoritmi koos võtmega VU.PK ja arvutatud räsiväärtusega.

10.4. Kiibi autentimine ja seansivõtme kooskõlastamine

CSM_175 Sõidukiseadmed ja kaardid peavad kasutama kaardi sõidukiseadme suhtes autentimiseks joonisel 7 kujutatud protokolli. Kiibi autentimine võimaldab sõidukiseadmel otseselt kontrollida kaardi autentsust.

Joonis 7.

Kiibi autentimine ja seansivõtme kooskõlastamine



CSM_176 Sõidukiseade ja kaart teevad järgmised toimingud:

1. Kiibi autentimise protsessi alustamiseks saadab sõidukiseade käsu MSE: Set AT, milles soovitakse „kiibi autentimist ECDH-algoritmiga, mille tulemuseks saadava AES-i seansivõtme pikkus on seotud kaardi võtmepaari Card_MA võtmesuurusega vastavalt nõudele CSM_50“. Sõidukiseade teeb kaardi võtmepaari võtmesuuruse kindlaks kaardi sertifikaadi põhjal.

2. Sõidukiseade saadab kaardile oma lühiajalise võtme avaliku punkti $VU.PK_{eph}$. Vastavalt nõudesCSM_164 esitatud selgitusele lõi sõidukiseade selle lühiajalise võtmepaari enne sõidukiseadme sertifikaadiahela kontrolli. Sõidukiseade saatis lühiajalise avaliku võtme Comp ($VU.PK_{eph}$) identifikaatori kaardile ja kaart salvestas selle.

3. Kaart arvutab $VU.PK_{eph}$ põhjal Comp($VU.PK_{eph}$) väärtuse ja võrdleb seda Comp($VU.PK_{eph}$) salvestatud väärtusega.

4. Kaart kasutab ECDH-algoritmi koos kaardi püsiva privaatvõtme ja sõidukiseadme lühiajalise avaliku võtmega ning arvutab salajase võtme K.

5. Kaart valib juhusliku 8-baidise nonsi N_{PICC} ning kasutab seda K-st kahe AES-i seansivõtme K_{MAC} ja K_{ENC} tuletamiseks K. Vt nõue CSM_179.

6. Kasutades võtit K_{MAC}, arvutab kaart sõidukiseadme lühiajalise avaliku võtme identifikaatorile autentimistõendi: T_{PICC} = CMAC(K_{MAC}, $VU.PK_{eph}$). Kaart saadab nonsi N_{PICC} ja tõendi T_{PICC} sõidukiseadmesse.

7. Sõidukiseade kasutab ECDH-algoritmi koos kaardi püsiva avaliku võtme ja sõidukiseadme lühiajalise privaatvõtmega ning arvutab sama salajase võtme K, mille kaart arvutas 4. toiminguga.

8. Sõidukiseade tuletab K-st seansivõtmed K_{MAC} ja K_{ENC} ning nonsi N_{PICC}; vt nõue CSM_179.

9. Sõidukiseade kontrollib autentimistõendit T_{PICC}.

CSM_177 Eespool nimetatud 3. toimingus arvutab kaart Comp(VU.PKeph) väärtuse kui võtmes $VU.PK_{eph}$ sisalduva x-koordinaadi.

CSM_178 Eespool nimetatud 4. ja 7. toimingus kasutavad kaart ja sõidukiseade tehnilises eeskirjas TR-03111 määratletud algoritmi ECKA-EG.

CSM_179 Eespool nimetatud 5. ja 8. toimingus kasutavad kaart ja sõidukiseade AES-i seansivõtmete võtmetuletusfunktsiooni, mis on määratletud tehnilises eeskirjas TR-03111, milles tehakse järgmised täpsustused ja muudatused:

— loenduri väärtus on K_{ENC} puhul '00 00 00 01' ja K_{MAC} puhul '00 00 00 02';

— kasutatakse vabatahtlikku nonssi *r*, mis võrdub nonsiga N_{PICC};

— 128-bitiste AES-võtmete tuletamiseks kasutatakse räsialgoritmi SHA-256;

— 192-bitiste AES-võtmete tuletamiseks kasutatakse räsialgoritmi SHA-384;

— 256-bitiste AES-võtmete tuletamiseks kasutatakse räsialgoritmi SHA-512.

Seansivõtmete pikkus (st pikkus, millest alates räsiväärtus kärbitakse), peab olema seotud võtmepaari Card_MA suurusega vastavalt nõudele CSM_50.

CSM_180 Eespool nimetatud 6. ja 9. toimingus kasutavad kaart ja sõidukiseade AES-i algoritmi CMAC-režiimis vastavalt dokumendile SP 800-38B. Tõendi T_{PICC} pikkus peab olema seotud AES-i seansivõtmete pikkusega vastavalt nõudele CSM_50.

10.5. **Turvaline sõnumivahetus**

10.5.1. *Üldist*

CSM_181 Pärast kiibi autentimise õnnestumist sõidukiseadme ja sõidumeerikukaardi vahel vahetatavad kõik käsud ja vastused kaitstakse kuni seansi lõpuni turvalise sõnumivahetusega.

CSM_182 Turvalist sõnumivahetust kasutatakse režiimis „ainult autentimine", välja arvatud juhul, kui loetakse faili, millele juurdepääsu tingimus on SM-R-ENC-MAC-G2 (vt 2. liite 4. osa). Selles režiimis lisatakse kõigile käskudele ja vastustele sõnumi autentsuse ja tervikluse tagamiseks krüptograafiline kontrollsumma (ehk MAC).

CSM_183 Kui andmeid loetakse failist, millele juurdepääsu tingimus on SM-R-ENC-MAC-G2, kasutatakse turvalist sõnumivahetust režiimis „krüpteerimine ja autentimine", st konfidentsiaalsuse tagamiseks krüpteeritakse vastuse andmed enne saatmist. Seejärel arvutatakse vormindatud krüpteeritud andmete kohta MAC, et tagada autentsust ja terviklust.

CSM_184 Turvalises sõnumivahetuses kasutatakse dokumendis AES määratletud standardit AES koos seansivõtmetega K_{MAC} ja K_{ENC}, mis kooskõlastati kiibi autentimise ajal.

CSM_185 Kordusrünnete vältimiseks kasutatakse saatejada loendurina (SSC) märgita täisarvu. SSC suurus peab võrduma AES-i plokisuurusega, st 128 bitti. SSC vorming on „kõige tähtsam bitt esimesena" (*MSB-first*). Turvalise sõnumivahetuse käivitamisel saatejada loendur nullitakse (st '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'). SSC suureneb iga kord enne käsu või vastuse rakendusprotokolli andmeühiku (*application protocol data unit*, APDU) loomist – kuna turvalise sõnumivahetuse seansi SSC algväärtus on 0, on SSC väärtus esimeses käsus 1. Esimeses vastuses on SSC väärtus 2.

CSM_186 Sõnumite krüpteerimiseks kasutatakse võtit K_{ENC} koos standardiga AES šifriploki aheldamise (CBC) režiimis vastavalt standardile ISO 10116; vaheldamise parameeter m = 1 ja initsialiseerimisvektor SV = E(K_{ENC}, SSC), st saatejada loenduri hetkeväärtus krüpteeritakse võtmega K_{ENC}.

CSM_187 Sõnumite autentimiseks kasutatakse võtit K_{MAC} koos standardiga AES CMAC-režiimis vastavalt dokumendile SP 800-38B. MAC-i pikkus peab olema seotud AES-i seansivõtmete pikkusega vastavalt nõudele CSM_50. Saatejada loendur lisatakse MAC-i ja paigutatakse seal autenditava datagrammi ette.

10.5.2. *Turvalise sõnumi struktuur*

CSM_188 Turvalises sõnumivahetuses kasutatakse ainult tabelis 5 loetletud turvalise sõnumivahetuse andmeobjekte (vt ISO 7816-4). Kõigis sõnumites kasutatakse andmeobjekte ainult selles tabelis esitatud järjekorras.

Tabel 5.

Turvalise sõnumivahetuse andmeobjektid

Andmeobjekti nimetus	Silt	Kasutamine kohustuslik (M), tingimuslik (C) või keelatud (F)	
		Käsud	Vastused
BER-TLV-s kodeerimata lihtväärtus	'81'	C	C
BER-TLV-s kodeeritud lihtväärtus, mis ei sisalda turvalise sõnumivahetuse andmeobjekte	'B3'	C	C
Täidise indikaator, millele järgneb krüptogramm, BER-TLV-s kodeerimata lihtväärtus	'87'	C	C
Kaitstud Le	'97'	C	F
Töötlusvastus	'99'	F	M
Krüptograafiline kontrollsumma	'8E'	M	M

Märkus: vastavalt 2. liitele võivad sõidumeerikukaardid toetada paaritu INS-baidiga ('B1' või 'D7') käske READ BINARY ja UPDATE BINARY. Need käsuvariandid on vajalikud vähemalt 32 768 baidi suuruste failide lugemiseks ja ajakohastamiseks. Sellise variandi kasutamise korral kasutatakse sildiga '81' andmeobjekti asemel andmeobjekti sildiga 'B3'. Lisateave on esitatud 2. liites.

CSM_189 Kõik turvalise sõnumivahetuse andmeobjektid kodeeritakse DER-TLV-s vastavalt standardile ISO 8825-1. Nimetatud kodeerimise tulemuseks on järgmine sildi-pikkuse-väärtuse (*Tag-Length-Value*, TLV) struktuur:

Silt: silt kodeeritakse ühes või kahes oktetis ja see osutab sisule.

Pikkus: pikkus kodeeritakse märgita täisarvuna ühes, kahes või kolmes oktetis, mis annab maksimaalseks pikkuseks 65 535 oktetti. Kasutatakse minimaalset oktettide arvu.

Väärtus: väärtus kodeeritakse nullis või enamas oktettides.

CSM_190 Turvalise sõnumivahetusega kaitstavad APDU-d luuakse järgmiselt:

— MAC-i arvutamisel võetakse arvesse käsu päis ja seega kasutatakse klassibaidi CLA jaoks väärtust '0C'.

— Vastavalt 2.liitele peavad kõik INS-baidid olema paaris, välja arvatud käskude READ BINARY ja UPDATE BINARY võimalikud paaritud INS-baidid.

— Pärast turvalise sõnumivahetuse rakendamist teisendatakse Lc tegelik väärtus kujule Lc'.

— Andmeväli peab koosnema turvalise sõnumivahetuse andmeobjektidest.

— Kaitstud käsu APDU-s määratakse Le baidi väärtuseks '00'. Vajaduse korral lisatakse Le algse väärtuse edastamiseks andmeväljale andmeobjekt '97'.

CSM_191 Kõik krüpteeritavad andmeobjektid täidistatakse vastavalt standardile ISO 7816-4, kasutades täidise indikaatorit '01'. MAC-i arvutamiseks täidistatakse vastavalt standardile ISO 7816-4 eraldi ka iga APDU-s olev andmeobjekt.

Märkus: turvalises sõnumivahetuses tehakse täidistamine alati turvalise sõnumivahetuse kihiga, mitte CMAC- või CBC-algoritmiga.

Kokkuvõte ja näited

Kui rakendatakse turvalist sõnumivahetust, siis olenevalt vastava turvamata käsu asjaoludest on käsu APDU struktuur järgmine („DO" on andmeobjekt):

Juhtum 1:	CLA INS P1 P2 || Lc'|| DO '8E' || Le
Juhtum 2:	CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le
Juhtum 3 (paaris INS-bait):	CLA INS P1 P2 || Lc'|| DO '81' || DO'8E' || Le
Juhtum 3 (paaritu INS-bait):	CLA INS P1 P2 || Lc'|| DO 'B3' || DO'8E' || Le
Juhtum 4 (paaris INS-bait):	CLA INS P1 P2 || Lc'|| DO '81' || DO'97' || DO'8E' || Le
Juhtum 4 (paaritu INS-bait):	CLA INS P1 P2 || Lc'|| DO 'B3' || DO'97' || DO'8E' || Le

kus Le = '00' või '00 00' olenevalt sellest, kas kasutatakse lühikesi või pikendatud välju; vt ISO 7816-4.

Kui rakendatakse turvalist sõnumivahetust, siis olenevalt vastava turvamata vastuse asjaoludest on vastuse APDU struktuur järgmine:

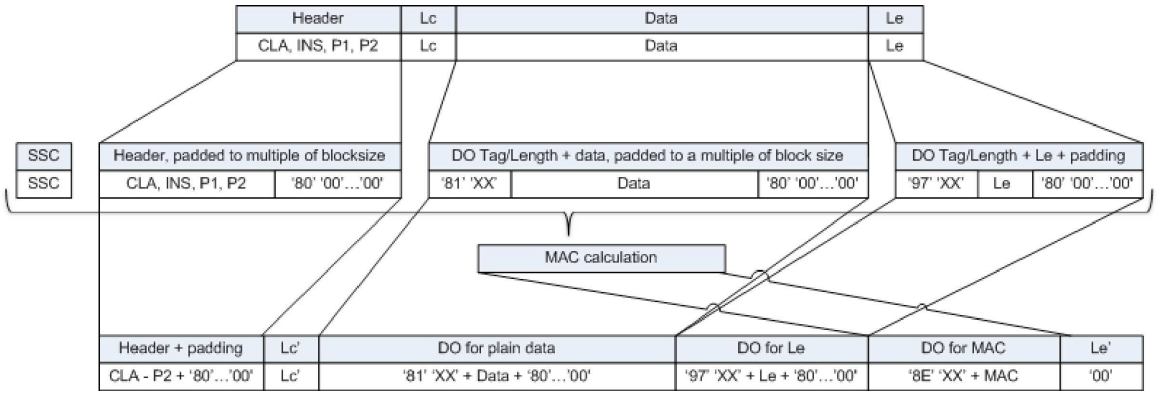
Juhtum 1 või 3:	DO '99' || DO '8E' || SW1SW2
Juhtum 2 või 4 (paaris INS-bait) krüpteerimisega:	DO '81' || DO '99' || DO '8E' || SW1SW2
Juhtum 2 või 4 (paaris INS-bait) krüpteerimiseta:	DO '87' || DO '99' || DO '8E' || SW1SW2
Juhtum 2 või 4 (paaritu INS-bait) krüpteerimiseta:	DO 'B3' || DO '99' || DO '8E' || SW1SW2

Märkus: krüpteerimisega juhtumeid 2 ja 4 (paaritu INS-bait) ei kasutada sõidukiseadme ja kaardi andmevahetuses kunagi.

Allpool on esitatud kolm näidet APDU teisendustest paaris INS-koodiga käskude puhul. Joonisel 8 on kujutatud juhtumi 4 autenditud käsu APDU-d; joonisel 9 on kujutatud juhtumi 1/3 autenditud vastuse APDU-d; joonisel 10 on kujutatud juhtumi 2/4 krüpteeritud ja autenditud vastuse APDU-d.

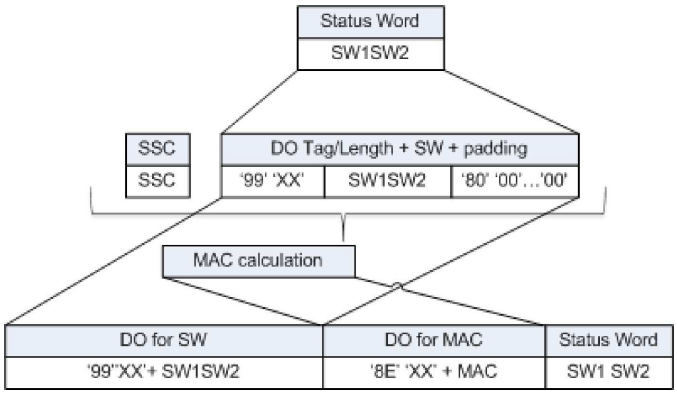
Joonis 8.

Juhtumi 4 autenditud käsu APDU teisendus



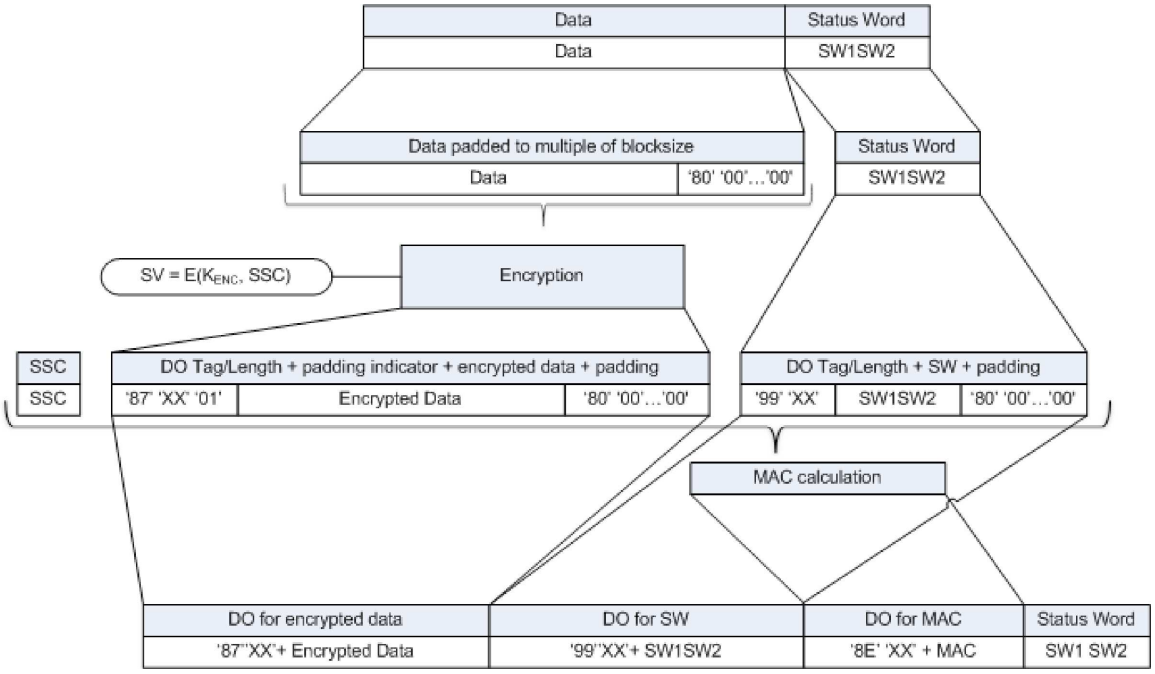
Joonis 9.

Juhtumi 1/3 autenditud vastuse APDU teisendus



Joonis 10.

Juhtumi 2/4 krüpteeritud ja autenditud vastuse APDU teisendus



10.5.3. *Turvalise sõnumivahetuse seansi abortimine*

CSM_192 Sõidukiseade abordib käimasoleva turvalise sõnumivahetuse seansi siis ja ainult siis, kui ilmneb mõni järgmine tingimus:

— ta saab vastuse APDU lihttekstina;

— ta tuvastab vastuse APDU-s turvalise sõnumivahetuse vea:

— oodatud turvalise sõnumivahetuse andmeobjekt puudub, andmeobjektide järjestus on vale või lisatud on tundmatu andmeobjekt,

— mõni turvalise sõnumivahetuse andmeobjekt on vale, nt MAC-i väärtus on vale, TLV struktuur on vale või sildi '87' täidistamise indikaatori väärtus ei ole '01';

— kaart saadab olekubaidi, mis näitab, et ta on avastanud turvalise sõnumivahetuse vea (vt nõud CSM_194);

— käimasoleva seansi käskude ja nendega seotud vastuse limiit on saavutatud. Iga sõidukiseadme limiidi määrab kindlaks selle tootja, võttes arvesse kasutatava riistvara turbenõudeid; maksimaalne väärtus on 240 turvalise sõnumivahetuse käsku ja seotud vastust seansi kohta.

CSM_193 Sõidumeerikukaart abordib käimasoleva turvalise sõnumivahetuse seansi siis ja ainult siis, kui ilmneb mõni järgmine tingimus:

— ta saab käsu APDU lihttekstina;

— ta tuvastab käsu APDU-s turvalise sõnumivahetuse vea:

— oodatud turvalise sõnumivahetuse andmeobjekt puudub, andmeobjektide järjestus on vale või lisatud on tundmatu andmeobjekt,

— mõni turvalise sõnumivahetuse andmeobjekt on vale, nt MAC-i väärtus on vale, TLV struktuur on vale;

— toimub voolukatkestus või lähtestamine;

— sõidukiseade valib kaardil rakenduse;

— sõidukiseade alustab sõidukiseadme autentimise protsessi;

— käimasoleva seansi käskude ja nendega seotud vastuse limiit on saavutatud. Iga kaardi limiidi määrab kindlaks selle tootja, võttes arvesse kasutatava riistvara turbenõudeid; maksimaalne väärtus on 240 turvalise sõnumivahetuse käsku ja seotud vastust seansi kohta.

CSM_194 Turvalise sõnumivahetuse vigade töötlemine sõidumeerikukaardiga:

— Kui käsu APDU-s puuduvad mõned oodatud turvalise sõnumivahetuse andmeobjektid, andmeobjektide järjestus on vale või lisatud on tundmatuid andmeobjekte, saadab sõidumeerikukaart vastuseks olekubaidid '69 87'.

— Kui mõni käsu APDU-s sisalduv turvalise sõnumivahetuse andmeobjekt on vale, saadab sõidumeerikukaart vastuseks olekubaidid '69 88'.

Sellisel juhul saadetakse olekubaidid ilma turvalist sõnumivahetust kasutamata.

CSM_195 Sõidukiseadme ja sõidumeerikukaardi turvalise sõnumivahetuse seansi abortimise korral teevad sõidukiseade ja sõidumeerikukaart järgmised toimingud:

— hävitavad salvestatud seansivõtmed turvaliselt;

— alustavad viivitamatult uut turvalise sõnumivahetuse seanssi vastavalt punktides 10.2–10.5 esitatud kirjeldusele.

CSM_196 Kui sõidukiseade otsustab vastastikust autentimist sisestatud kaardiga mingil põhjusel uuesti alustada, taaskäivitatakse protsess kaardi sertifikaadiahela kontrollimisega, nagu on kirjeldatud punktis 10.2, ning jätkub vastavalt punktides 10.2–10.5 esitatud kirjeldusele.

11. SÕIDUKISEADME JA GNSSI VÄLISSEADME ÜHENDAMINE, VASTASTIKUNE AUTENTIMINE JA TURVALINE SÕNUMIVAHETUS

11.1. **Üldist**

CSM_197 GNSSi seade, mida sõidukiseade oma asukoha kindlakstegemiseks kasutab, võib olla sisemine seade (st sõidukiseadme korpusesse lahutamatult sisse ehitatud) või väline moodul. Esimesel juhul puudub vajadus GNSSi seadme ja sõidukiseadme sisemise andmevahetuse standardimise järele ning käesoleva peatüki nõudeid ei kohaldata. Teisel juhul tuleb sõidukiseadme ja GNSSi välisseadme andmevahetus standardida ja kaitsta vastavalt käesolevas peatükis esitatud kirjeldusele.

CSM_198 Turvaline side sõidukiseadme ja GNSSi välisseadme vahel toimub samuti nagu turvaline side sõidukiseadme ja sõidumeerikukaardi vahel, kusjuures GNSSi välisseade täidab selles samasugust rolli nagu kaart. GNSSi välisseade peab vastama kõigile 10. peatükis sõidumeerikukaartide kohta esitatud nõuetele, võttes arvesse käesolevas peatükis nimetatud kõrvalekaldeid, selgitusi ja täiendusi. Täpsemalt toimub sertifikaadiahela vastastikune kontrollimine, sõidukiseadme autentimine ja kiibi autentimine vastavalt punktidele 11.3 ja 11.4.

CSM_199 Sõidukiseadme ja GNSSi välisseadme vaheline andmevahetus erineb sõidukiseadme ja kaardi andmevahetusest selle poolest, et enne GNSSil põhinevate andmete vahetamist sõidukiseadme ja GNSSi välisseadme vahel tuleb sõidukiseade ja GNSSi välisseade töökojas üks kord ühendada. Ühendamise protsessi on kirjeldatud punktis 11.2.

CSM_200 Sõidukiseadme ja GNSSi välisseadme andmevahetuses kasutatakse standarditel ISO 7816-4 ja ISO 7816-8 põhinevaid APDU-käske ja -vastuseid. APDU-de täpne struktuur on määratletud käesoleva lisa 2. liites.

11.2. **Sõidukiseadme ja GNSSi välisseadme ühendamine**

CSM_201 Sõidukiseade ja sõidukis asuv GNSSi välisseade ühendatakse töökojas. Ainult ühendatud sõidukiseade ja GNSSi välisseade suudavad tavapärase töö ajal üksteisega andmeid vahetada.

CSM_202 Sõidukiseadme ja GNSSi välisseadme ühendamine on võimalik ainult siis, kui sõidukiseade on kalibreerimisrežiimis. Ühendamise algatab sõidukiseade.

CSM_203 Töökoda võib igal ajal ühendada sõidukiseadme uuesti mõne muu või sama GNSSi välisseadmega. Uuesti ühendamise ajal peab sõidukiseade hävitama oma mälus oleva senise sertifikaadi EGF_MA ning salvestama selle asemele ühendatava GNSSi välisseadme sertifikaadi EGF_MA.

CSM_204 Töökoda võib igal ajal ühendada GNSSi välisseadme mõne muu või sama sõidukiseadmega. Uuesti ühendamise ajal peab GNSSi välisseade hävitama oma mälus oleva senise sertifikaadi VU_MA ning salvestama selle asemele ühendatava välise sõidukiseadme sertifikaadi VU_MA.

11.3. **Vastastikune sertifikaadiahela kontrollimine**

11.3.1. *Üldist*

CSM_205 Sõidukiseadme ja GNSSi välisseadme vastastikune sertifikaadiahela kontrollimine toimub ainult töökojas sõidukiseadme ja GNSSi välisseadme ühendamise ajal. Ühendatud sõidukiseadme ja GNSSi välisseadme tavapärase töö ajal sertifikaate ei kontrollita. Selle asemel usaldavad sõidukiseade ja GNSSi välisseade ühendamise ajal neisse salvestatud sertifikaate automaatselt pärast seda, kui nad on kontrollinud sertifikaatide ajalist kehtivust. Sõidukiseade ja GNSSi välisseade ei tohi tavapärase töö ajal omavahelise andmevahetuse kaitsmiseks usaldada ühtegi muud sertifikaati.

11.3.2. *Toimingud sõidukiseadme ja GNSSi välisseadme ühendamise ajal*

CSM_206 Sõidukiseade kasutab GNSSi välisseadmega ühendamise ajal GNSSi välisseadme sertifikaadiahela kontrollimiseks joonisel 4 (punkt 10.2.1) kujutatud protokolli.

Märkused joonise 4 kohta seoses käsitletava kontekstiga

— Käesolevas lisas ei käsitleta andmeside juhtimist. Tuleb siiski arvestada, et GNSSi välisseade ei ole kiipkaart ning seega ei saada sõidukiseade side alustamiseks tõenäoliselt *Reset*-käsku ja ei saa vastuseks ATR-i.

— Joonisel kujutatud kaardisertifikaate ja avalikke võtmeid tõlgendatakse vastastikuseks autentimiseks kasutatavate GNSSi välisseadme sertifikaatide ja avalike võtmetena. Punktis 9.1.6 kasutatakse nende kohta tähistust EGF_MA.

— Joonisel kujutatud sertifikaate Card.CA ja avalikke võtmeid tõlgendatakse GNSSi välisseadme sertifikaatide allkirjastamiseks kasutatavate liikmesriigi sertifitseerimisasutuse sertifikaatide ja avalike võtmetena. Punktis 9.1.3 kasutatakse nende kohta tähistust MSCA_VU-EGF.

— Joonisel kujutatud sertifikaati Card.CA.EUR tõlgendatakse Euroopa juursertifikaadina, millele osutatakse sertifikaadis MSCA_VU-EGF sisalduvas sertifitseerimisasutuse viites.

— Joonisel kujutatud sertifikaati Card.Link tõlgendatakse GNSSi välisseadme lülisertifikaadina, kui see on olemas. Vastavalt punktile 9.1.2 on tegemist Euroopa uue juurvõtmepaari lülisertifikaadiga, mille loob ERCA ja mis allkirjastatakse Euroopa eelmise privaatvõtmega.

— Sertifikaat Card.Link.EUR on Euroopa juursertifikaat, millele osutatakse sertifikaadis Card.Link sisalduvas sertifitseerimisasutuse viites.

— Andmetüübi `cardExtendedSerialNumber` asemel loeb sõidukiseade failist EF ICC andmetüübi `sensorGNSSserialNumber`.

— Sõidumeeriku rakendusidentifikaatori (Tachograph AID) asemel valib sõidukiseade GNSSi välisseadme rakendusidentifikaatori (EGF AID).

— Väljendit „kaardi ignoreerimine“ tõlgendatakse GNSSi välisseadme ignoreerimisena.

CSM_207 Pärast sertifikaadi EGF_MA kontrollimist salvestab sõidukiseade selle sertifikaadi tavapärase töö ajal kasutamiseks; vt punkt 11.3.3.

CSM_208 GNSSi välisseade kasutab sõidukiseadmega ühendamise ajal välise sõidukiseadme sertifikaadiahela kontrollimiseks joonisel 5 (punkt 10.2.2) kujutatud protokolli.

Märkused joonise 5 kohta seoses käsitletava kontekstiga

— Sõidukiseade kasutab uue lühiajalise võtmepaari loomiseks GNSSi välisseadme sertifikaadis märgitud standardseid domeeniparameetreid.

— Joonisel on kujutatud neid sõidukiseadme sertifikaate ja avalikke võtmeid, mida kasutatakse vastastikuseks autentimiseks. Punktis 9.1.4 kasutatakse nende kohta tähistust VU_MA.

— Joonisel on kujutatud neid VU.CA sertifikaate ja avalikke võtmeid, mida kasutatakse sõidukiseadme ja GNSSi välisseadme sertifikaatide allkirjastamiseks. Punktis 9.1.3 kasutatakse nende kohta tähistust MSCA_VU-EGF.

— Joonisel kujutatud sertifikaat Card.CA.EUR on Euroopa juursertifikaat, millele osutatakse sertifikaadis VU.CA sisalduvas sertifitseerimisasutuse viites.

— Joonisel kujutatud sertifikaat VU.Link tähistab sõidukiseadme lülisertifikaati, kui see on olemas. Vastavalt punktile 9.1.2 on tegemist Euroopa uue juurvõtmepaari lülisertifikaadiga, mille loob ERCA ja mis allkirjastatakse Euroopa eelmise privaatvõtmega.

— Sertifikaat VU.Link.EUR on Euroopa juursertifikaat, millele osutatakse sertifikaadis VU.Link sisalduvas sertifitseerimisasutuse viites.

CSM_209 Erinevalt nõudest CSM_167 kasutab GNSSi välisseade talle esitatud sertifikaatide ajalise kehtivuse kontrollimiseks GNSSi aega.

CSM_210 Pärast sertifikaadi VU_MA kontrollimist salvestab GNSSi välisseade selle sertifikaadi tavapärase töö ajal kasutamiseks; vt punkt 11.3.3.

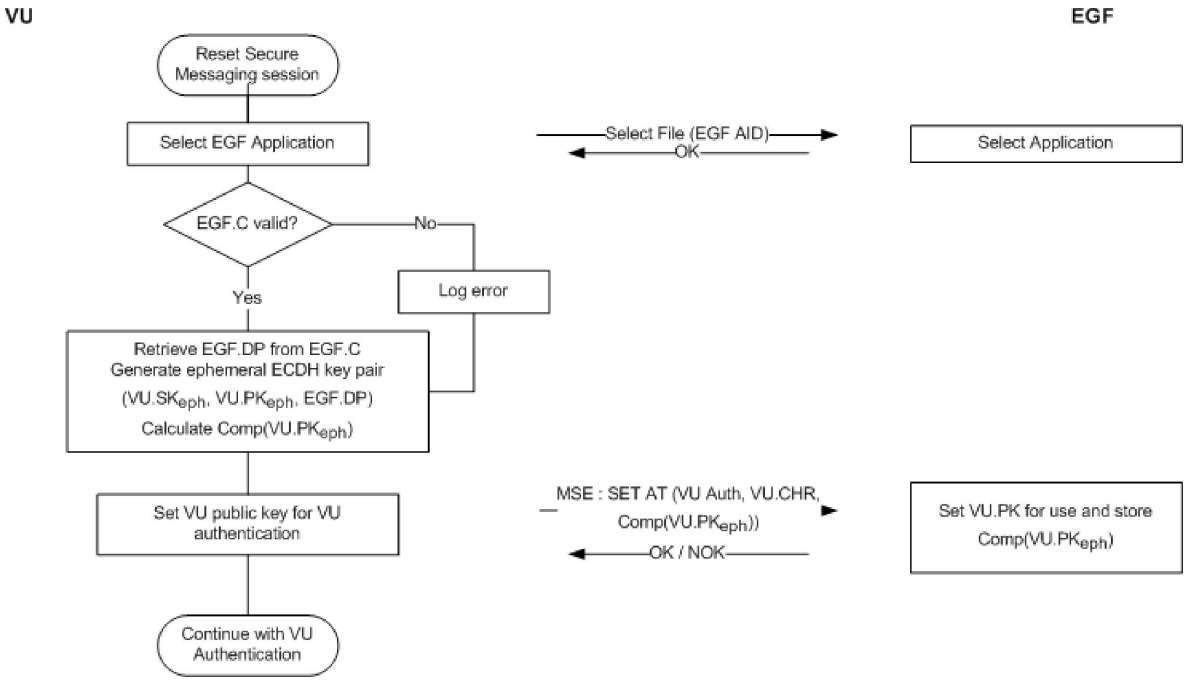
11.3.3. *Toimingud tavapärase töö ajal*

CSM_211 Tavapärase töö ajal kasutavad sõidukiseade ja GNSSi välisseade salvestatud sertifikaatide EGF_MA ja VU_MA ajalise kehtivuse kontrollimiseks ning sõidukiseadme autentimises kasutatava avaliku võtme VU_MA seadistamiseks joonisel 11 kujutatud protokolli. Mingeid muid vastastikuseid sertifikaadiahelate kontrolle tavapärase töö ajal ei toimu.

Pange tähele, et joonis 11 sisaldab sisuliselt joonistel 4 ja 5 kujutatud esimesi etappe. Samuti tuleb arvestada, et kuna GNSSi välisseade ei ole kiipkaart, siis ei saada sõidukiseade side alustamiseks tõenäoliselt *Reset*-käsku ja ei saa vastuseks ATR-i. Igal juhul ei kuulu need küsimused käesoleva liite reguleerimisalasse.

Joonis 11.

Sertifikaadi ajalise kehtivuse vastastikune kontroll sõidukiseadme ja GNSSi välisseadme tavapärase töö ajal



CSM_212 Nagu nähtub jooniselt 11, registreerib sõidukiseade vea juhul, kui sertifikaat EGF_MA enam ei kehti. Sellele vaatamata toimub vastastikune autentimine, võtmete kooskõlastamine ja järgnev andmevahetus tavapäraselt.

11.4. Sõidukiseadme autentimine, kiibi autentimine ja seansivõtme kooskõlastamine

CSM_213 Sõidukiseadme ja GNSSi välisseadme vaheline sõidukiseadme autentimine, kiibi autentimine ja seansivõtme kooskõlastamine peab toimuma ühendamise ajal ning alati, kui tavapärase töö käigus alustatakse uut turvalise sõnumivahetuse seanssi. Sõidukiseade ja GNSSi välisseade teostavad punktides 10.3 ja 10.4 kirjeldatud protsessid. Kõik nimetatud punktides esitatud nõuded kehtivad.

11.5. Turvaline sõnumivahetus

CSM_214 Pärast kiibi autentimise õnnestumist sõiduki ja GNSSi välisseadme vahel vahetatavad kõik käsud ja vastused kaitstakse kuni seansi lõpuni turvalise sõnumivahetusega režiimis „ainult autentimine“. Kõik punktis 10.5 esitatud nõuded kehtivad.

CSM_215 Sõidukiseadme ja GNSSi välisseadme turvalise sõnumivahetuse abortimise korral alustab sõidukiseade viivitamatult uut turvalise sõnumivahetuse seanssi, nagu on kirjeldatud punktides 11.3.3 ja 11.4.

12. SÕIDUKISEADME JA LIIKUMISANDURI ÜHENDAMINE JA ANDMEVAHETUS

12.1. **Üldist**

CSM_216 Sõidukiseade ja liikumisandur kasutavad ühendamise ja tavapärase töö ajal andmevahetuseks standardis ISO 16844-3 määratletud liideseprotokolli, milles on tehtud käesolevas peatükis ja punktis 9.2.1 kirjeldatud muudatused.

Märkus: käesoleva peatüki lugejad peaksid olema tutvunud standardi ISO 16844-3 sisuga.

12.2. **Sõidukiseadme ja liikumisanduri ühendamine eri võtmepõlvkondade puhul**

Vastavalt punktis 9.2.1 esitatud selgitusele vahetatakse liikumisanduri peavõtit ja kõiki sellega seotud võtmeid regulaarselt. Selle tagajärjel võib töökojakaardil olla kuni kolm liikumisanduriga seotud (järjestikuste põlvkondade) AES-võtit K_{M-WC}. Samuti võib liikumisanduris olla kuni kolm erinevat AES-il põhinevat andmekrüpteeringut (mis põhinevad liikumisanduri peavõtme K_M järjestikustel põlvkondadel). Sõidukiseade sisaldab ainult ühte liikumisanduriga seotud võtit K_{M-VU}.

CSM_217 Teise põlvkonna sõidukiseade ja teise põlvkonna liikumisandur ühendatakse järgmiselt (vrd tabel 6 standardis ISO 16844-3):

1. Sõidukiseadmesse sisestatakse teise põlvkonna töökojakaart ning sõidukiseadme ja liikumisanduri vahele luuakse ühendus.

2. Sõidukiseade loeb töökojakaardilt kõik seal olevad võtmed K_{M-WC}, kontrollib nende versiooninumbreid ning valib selle, mille versiooninumber vastab sõidukiseadme võtme K_{M-VU} versiooninumbrile. Kui töökojakaardil ei ole sobivat võtit K_{M-WC}, abordib sõidukiseade ühendamisprotsessi ja näitab töökojakaardi omanikule sellekohast veateadet.

3. Sõidukiseade arvutab K_{M-VU} ja K_{M-WC} põhjal liikumisanduri peavõtme K_M ning seejärel võtme K_M põhjal võtme K_{ID} vastavalt punktis 9.2.1 esitatud kirjeldusele.

4. Sõidukiseade saadab liikumisandurisse käsu ühendamisprotsessi alustamiseks vastavalt standardile ISO 16844-3 ning krüpteerib liikumisandurilt saadud seerianumbri identimisvõtmega K_{ID}. Sõidukiseade saadab krüpteeritud seerianumbri tagasi liikumisandurisse.

5. Liikumisandur kõrvutab krüpteeritud seerianumbrit järjest kõigi oma mällu salvestatud krüpteeritud seerianumbritega. Kokkulangevuse leidmise korral on sõidukiseade autenditud. Liikumisandur registreerib sõidukiseadme kasutatud võtme K_{ID} põlvkonna ning saadab vastuseks ühilduva krüpteeringuga ühendamisvõtme, st kasutab krüpteerimiseks sama põlvkonna võtit K_M.

6. Sõidukiseade dekrüpteerib ühendamisvõtme võtme K_M abil, loob seansivõtme K_S, krüpteerib selle ühendamisvõtmega ja saadab tulemuse liikumisandurile. Liikumisandur dekrüpteerib võtme K_S.

7. Sõidukiseade koostab standardis ISO 16844-3 määratletud ühendamisinfo, krüpteerib selle ühendamisvõtmega ja saadab tulemuse liikumisandurile. Liikumisandur dekrüpteerib ühendamisinfo.

8. Liikumisandur krüpteerib saadud ühendamisinfo saadud võtmega K_S ja saadab selle tagasi sõidukiseadmele. Sõidukiseade kontrollib, kas ühendamisinfo kattub eelmisel etapil sõidukiseadmest liikumisandurisse saadetud infoga. Kui see kattub, siis on tõendatud, et liikumisandur ja sõidukiseade kasutasid sama võtit K_S ning järelikult krüpteeris sõidukiseade 5. etapil saadetud ühendamisvõtme õige põlvkonna võtmega K_M. Seega on liikumisandur autenditud.

Pange tähele, et 2. ja 5. etapp erinevad standardis ISO 16844-3 kirjeldatud standardprotsessist; ülejäänud etapid on standardsed.

Näide: Oletame, et ühendamine toimub ERCA (3) sertifikaadi esimesel kehtivusaastal; vt punkti 9.2.1.2 joonis 2. Lisaks

— oletame, et liikumisandur lasti välja ERCA (1) sertifikaadi viimasel kehtivusaastal. Järelikult sisaldab see järgmisi võtmeid ja andmeid:

  — $N_s[1]$: anduri seerianumber, mis on krüpteeritud 1. põlvkonna võtmega K_{ID},

  — $N_s[2]$: anduri seerianumber, mis on krüpteeritud 2. põlvkonna võtmega K_{ID},

  — $N_s[3]$: anduri seerianumber, mis on krüpteeritud 3. põlvkonna võtmega K_{ID},

  — $K_P[1]$: 1. põlvkonna ühendamisvõti, ([1]) mis on krüpteeritud 1. põlvkonna võtmega K_M,

  — $K_P[2]$: 2. põlvkonna ühendamisvõti, mis on krüpteeritud 2. põlvkonna võtmega K_M,

  — $K_P[3]$: 3. põlvkonna ühendamisvõti, mis on krüpteeritud 3. põlvkonna võtmega K_M.

— Oletame, et töökojakaart anti välja ERCA (3) sertifikaadi esimesel kehtivusaastal. Seega sisaldab see 2. ja 3. põlvkonna võtit $K_{M\text{-}WC}$.

— Oletame, et sõidukiseade on 2. põlvkonna seade, mis sisaldab 2. põlvkonna võtit $K_{M\text{-}VU}$.

Sellisel juhul kulgevad etapid 2–5 järgmiselt:

— 2. etapp: sõidukiseade loeb töökojakaardilt 2. ja 3. põlvkonna võtme $K_{M\text{-}WC}$ ning kontrollib nende versiooninumbreid.

— 3. etapp: sõidukiseade kombineerib 2. põlvkonna võtme $K_{M\text{-}WC}$ oma võtmega $K_{M\text{-}VU}$ ning arvutab nende põhjal võtmed K_M ja K_{ID}.

— 4. etapp: sõidukiseade krüpteerib liikumisandurilt saadud seerianumbri identimisvõtmega K_{ID}.

— 5. etapp: liikumisandur võrdleb saadud andmeid seerianumbriga $N_s[1]$ ja ei leia vastavust. Siis võrdleb ta andmeid seerianumbriga $N_s[2]$ ja leiab vastavuse. Liikumisandur järeldab, et sõidukiseade on 2. põlvkonna seade ning saadab seetõttu vastuseks võtme $K_P[2]$.

12.3. **Sõidukiseadme ja liikumisanduri ühendamine ja andmevahetus standardi AES abil**

CSM_218 Vastavalt punktis 9.2.1 esitatud tabelile 3 peavad kõik (teise põlvkonna) sõidukiseadme ja liikumisanduri ühendamiseks ja järgnevas andmevahetuses kasutatavad võtmed olema AES-võtmed, mitte kahekordse pikkusega TDES-võtmed, nagu on määratletud standardis ISO 16844-3. Nende AES-võtmete pikkus võib olla 128, 192 või 256 bitti. Kuna AES-i plokisuurus on 16 baiti, peab krüpteeritud sõnumi pikkus olema 16 baidi kordarv (standardis TDES on vastav väärtus 8 baiti). Lisaks kasutatakse osa nendest sõnumitest 128, 192 või 256 biti pikkuste AES-võtmete edastamiseks. Seega tuleb standardi ISO 16844-3 tabelis 5 esitatud andmebaitide arvu käsu kohta muuta vastavalt tabelile 6:

Tabel 6.

Lihtteksti ja krüpteeritud andmebaitide arv käsu kohta vastavalt standardile ISO 16844-3

Käsk	Nõue / vastus	Andmete kirjeldus	Lihtteksti andmebaitide arv vastavalt standardile ISO 16844-3	Lihtteksti andmebaitide arv AES-võtmetega	Krüpteeritud andmebaitide arv AES-i bitipikkuse võtmetega		
					128	192	256
10	nõue	Autentimisanded + failinumber	8	8	16	16	16

([1]) Pange tähele, et 1., 2. ja 3. põlvkonnal võib olla sama ühendamisvõti või kolm eri pikkusega võtit, nagu on selgitatud nõudes CSM_117.

Käsk	Nõue / vastus	Andmete kirjeldus	Lihtteksti andmebaitide arv vastavalt standardile ISO 16844-3	Lihtteksti andmebaitide arv AES-võtmetega	Krüpteeritud andmebaitide arv AES-i bitipikkuse võtmetega		
					128	192	256
11	vastus	Autentimisanded + faili sisu	16 või 32, olenevalt failist	16 või 32, olenevalt failist	16 / 32	16 / 32	16 / 32
41	nõue	Liikumisanduri seerianumber	8	8	16	16	16
41	vastus	Ühendamisvõti	16	16 / 24 / 32	16	32	32
42	nõue	Seansivõti	16	16 / 24 / 32	16	32	32
43	nõue	Ühendamisinfo	24	24	32	32	32
50	vastus	Ühendamisinfo	24	24	32	32	32
70	nõue	Autentimisanded	8	8	16	16	16
80	vastus	Liikumisanduri loenduri väärtus + autentimisandmed	8	8	16	16	16

CSM_219 Käskudes 43 (sõidukiseadme nõue) ja 50 (liikumisanduri vastus) saadetav ühendamisinfo koostatakse vastavalt standardi ISO 16844-3 punktile 7.6.10, kuid ühendamisandmete krüpteerimisskeemis kasutatakse TDES-algoritmi asemel AES-algoritmi, mille tulemuseks on kaks AES-krüpteeringut, ning rakendatakse nõudes CSM_220 kirjeldatud täidistamist, et sobitada see AES-i plokisuurusega. Krüpteerimiseks kasutatav võti K'_P luuakse järgmiselt:

— kui ühendamisvõtme K_P pikkus on 16 baiti: $K'_P = K_P \text{ XOR } (N_s||N_s)$,

— kui ühendamisvõtme K_P pikkus on 24 baiti: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s)$,

— kui ühendamisvõtme K_P pikkus on 32 baiti: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s||N_s)$,

kus N_s on liikumisanduri 8-baidine seerianumber.

CSM_220 Kui lihtteksti andmepikkus (AES-võtmeid kasutades) ei ole 16 baidi kordarv, tuleb kasutada standardis ISO 9797-1 määratletud täidistamismeetodit nr 2.

Märkus: standardi ISO 16844-3 kohaselt jagub lihtteksti andmebaitide arv alati 8-ga, mistõttu standardi TDES kasutamisel ei ole täidistamine vajalik. Standardis ISO 16844-3 esitatud andmete ja sõnumite määratlust ei ole käesoleva liite selles osas muudetud, mistõttu tuleb rakendada täidistamist.

CSM_221 Käsu 11 kasutamise korral ning juhul, kui krüpteerimist vajab rohkem kui üks andmeplokk, kasutatakse standardis ISO 10116 määratletud šifriplokki aheldavat toimimisrežiimi vaheldamise parameetriga $m = 1$. Kasutatav initsialiseerimisvektor (IV) on

— käsu 11 puhul: standardi ISO 16844-3 punktis 7.6.3.3 määratletud 8-baidine autentimisplokk, mis on täidistatud vastavalt standardis ISO 9797-1 määratletud täidistamismeetodile nr 2; vt ka standardi ISO 16844-3 punktid 7.6.5 ja 7.6.6;

— kõigi ülejäänud käskude puhul, milles edastatakse rohkem kui 16 baiti, vastavalt tabelile 6: '00' {16}, st kuusteist baiti binaarväärtusega 0.

Märkus: standardi ISO 16844-3 punktidest 7.6.5 ja 7.6.6 nähtub, et kui liikumisandur krüpteerib andmefaile käsule 11 lisamiseks, tehakse autentimisplokiga mõlemad järgmised toimingud:

— seda kasutatakse andmefailide CBC-režiimis krüpteerimise initsialiseerimisvektorina;

— see krüpteeritakse ja lisatakse sõidukiseadmesse saadetavate andmete esimesse plokki.

12.4. **Sõidukiseadme ja liikumisanduri ühendamine eri seadmepõlvkondade puhul**

CSM_222 Punktis 9.2.1 esitatud selgituse kohaselt võib teise põlvkonna liikumisandur sisaldada standardil TDES põhinevat ühendamisandmete krüpteeringut (määratletud käesoleva liite A osas), mis võimaldab ühendada liikumisanduri esimese põlvkonna sõidukiseadmega. Sellisel juhul ühendatakse esimese põlvkonna sõidukiseade ja teise põlvkonna liikumisandur vastavalt käesoleva liite A osale ja standardile ISO 16844-3. Ühendamiseks võib kasutada esimese või teise põlvkonna töökojakaarti.

Märkused

— Teise põlvkonna sõidukiseadet ei saa ühendada esimese põlvkonna liikumisanduriga.

— Esimese põlvkonna töökojakaarti ei saa kasutada teise põlvkonna sõidukiseadme ühendamiseks liikumisanduriga.

13. DSRC KAUDU TOIMUVA KAUGSIDE TURVALISUS

13.1. **Üldist**

Vastavalt 14. liitele loob sõidukiseade regulaarselt sõidumeeriku kaugseire (*remote tachograph monitoring*, RTM) andmeid ja saadab need andmed (sisemisele või välisele) kaugsideseadmele (*remote communication facility*, RCF). Kaugsideseadme ülesanne on saata need andmed 14. liideses kirjeldatud DSRC-liidese kaudu kaugpäringusaatjasse. 1. liite kohaselt koosnevad sõidumeeriku kaugseire andmed järgmistest osadest:

krüpteeritud sõidumeerikuandmete sisu sõidumeerikuandmete lihtteksti krüpteering;

DSRC turbeandmed kirjeldatakse allpool.

Sõidumeerikuandmete lihtteksti vormingu spetsifikatsioon on esitatud 1. liites ja seda on täpsemalt kirjeldatud 14. liites. Käesolevas peatükis kirjeldatakse DSRC turbeandmete struktuuri; nende ametlik spetsifikatsioon on esitatud 1. liites.

CSM_223 Lihtteksti andmetüübi `tachographPayload` andmed, mille sõidukiseade edastab kaugsideseadmele (kui kaugsideseade asub väljaspool sõidukiseadet) või DSRC-liidese kaudu kaugpäringusaatjasse (kui kaugsideseade asub sõidukiseadmes), kaitstakse režiimis „krüpteerimine ja autentimine", st esmalt sõidumeerikuandmed krüpteeritakse sõnumi konfidentsiaalsuse tagamiseks ning seejärel arvutatakse MAC andmete autentsuse ja tervikluse tagamiseks.

CSM_224 DSRC turbeandmed koosnevad järgmistest ühendatud andmeelementides järgmises järjekorras (vt ka joonis 12):

hetkekuupäev ja -aeg	sõidukiseadme hetkekuupäev ja -aeg (andmetüüp `TimeReal`);
loendur	3-baidine loendur, vt nõue CSM_224;

VU seerianumber	sõidukiseadme seerianumber (andmetüüp `VuSerialNumber`);
DSRC peavõtme versiooninumber	DSRC peavõtme 1-baidine versiooninumber, millest on tuletatud konkreetse sõidukiseadme DSRC võtmed, vt punkt 9.2.2;
MAC	kõigile eelnevatele sõidumeeriku kaugseire andmetele arvutatud sõnumiautentimiskood.

CSM_225 DSRC turbeandmetes sisalduv 3-baidine loendur peab olema vormingus *MSB-first*. Kui tootmisse võetud sõidukiseade arvutab esimest korda sõidumeeriku kaugseire andmete kogumi, määrab ta loenduri väärtuseks 0. Seejärel suurendab sõidukiseade loenduri väärtust ühe võrra iga kord enne järgmise sõidumeeriku kaugseire andmete kogumi arvutamist.

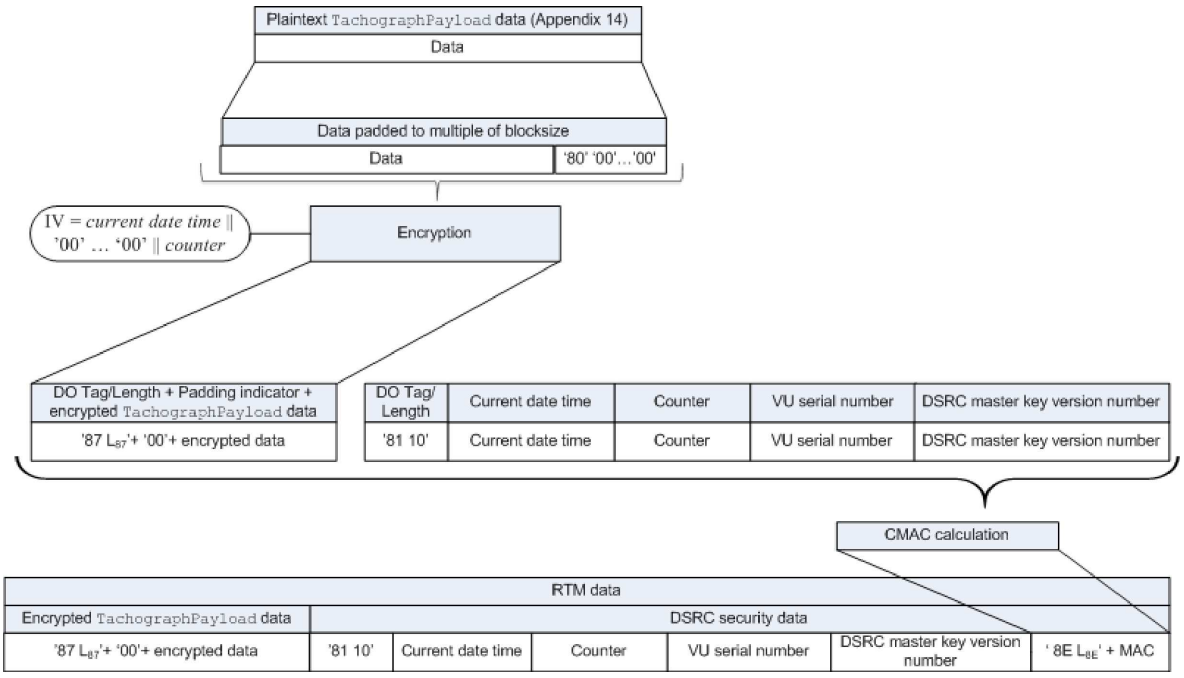
13.2. Sõidumeerikuandmete krüpteerimine ja MAC-i loomine

CSM_226 Kui kasutatakse 14. liite kohaselt andmetüübi `TachographPayload` alla kuuluvat lihttekstiga andmeelementi, krüpteerib sõidukiseade need andmed nii, nagu on kujutatud joonisel 12: sõidukiseadme DSRC-võtit võtme $K\_VU_{DSRC}\_ENC$ (vt punkt 9.2.2) krüpteerimiseks kasutatakse standardiga AES šifriploki aheldamise (CBC) toimimisrežiimis vastavalt standardile ISO 10116 koos vaheldamise parameetriga *m* = 1. Initsialiseerimisvektori väärtus *IV = hetkekuupäev/-aeg || '00 00 00 00 00 00 00 00' || hetkeaja ja -kuupäeva loenduri* määratlus on esitatud nõudes CMS_223. Krüpteeritavad andmed täidistatakse vastavalt standardis ISO 9797-1 määratletud meetodile nr 2.

CSM_227 Sõidukiseade arvutab DSRC turbeandmetes MAC-i, nagu on kujutatud joonisel 12: MAC arvutatakse kõigi eelnevate RTM-andmete baitide kohta kuni DSRC peavõtme versiooninumbrini (kaasa arvatud) ning see hõlmab ka andmeobjektide silte ja pikkusi. Sõidukiseade kasutab autentsuse tagamise DSRC-võtit $K\_VU_{DSRC}\_MAC$ (vt punkt 9.2.2) standardiga AES CMAC-režiimis vastavalt dokumendile SP 800-38B. MAC-i pikkus peab olema seotud sõidukiseadmeomaste DSRC-võtmete pikkusega vastavalt nõudele CSM_50.

Joonis 12.

Sõidumeerikuandmete krüpteerimine ja MAC-i loomine



13.3. **Sõidumeerikuandmete kontrollimine ja dekrüpteerimine**

CSM_228 Kui kaugpäringusaatja saab sõidukiseadmelt RTM-andmed, saadab ta kõik RTM-andmed käsu PROCESS DSRC MESSAGE andmeväljal kontrollikaardile, nagu on kirjeldatud 2.liites. Seejärel:

1. Kontrollikaart kontrollib DSRC turbeandmetes sisalduvat DSRC peavõtme versiooninumbrit. Kui vastav DSRC peavõti ei ole kontrollikaardile tuttav, saadab ta tagasi 2. liites kirjeldatud veateate ja abordib protsessi.

2. Kontrollikaart kasutab osutatud DSRC peavõtit koos DSRC turbeandmetes sisalduva sõidukiseadme seerianumbriga, et tuletada sõidukiseadmeomased DSRC-võtmed K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC vastavalt nõudele CSM_124.

3. Kontrollikaart kasutab koodi K_VU_{DSRC}_MAC selleks, et kontrollida DSRC turbeandmetes sisalduvat MAC-i vastavalt nõudele CSM_227. Kui MAC on vale, saadab kontrollikaart tagasi 2. liites kirjeldatud veateate ja abordib protsessi.

4. Kontrollikaart kasutab koodi K_VU_{DSRC}_ENC selleks, et dekrüpteerida krüpteeritud sõidumeerikuandmed vastavalt nõudele CSM_226. Kontrollikaart eemaldab täidise ja tagastab dekrüpteeritud sõidumeerikuandmed kaugpäringusaatjale.

CSM_229 Kordusrünnete vältimiseks kontrollib kaugpäringusaatja RTM-andmete värskust, et DSRC turbeandmetes sisalduv *hetkekuupäev/-aeg* ei erineks liiga palju kaugpäringusaatja hetkeajast.

Märkused

— See eeldab, et kaugpäringusaatja käsutuses on täpne ja usaldusväärne ajaallikas.

— Kuna 14. liite kohaselt peab sõidukiseade arvutama uue RTM-andmete kogumi iga 60 sekundi järel ning sõidukiseadme kellal on lubatud tegelikust ajast ühe minuti võrra erineda, on RTM-andmete värskuse alumine piirmäär kaks minutit. Nõutav tegelik värskus sõltub ka kaugpäringusaatja kella täpsusest.

CSM_230 Kui töökoda kontrollib sõidukiseadme DSRC-funktsiooni nõuetekohast toimimist, saadab ta kõik sõidukiseadmelt saadud RTM-andmed käsu PROCESS DSRC MESSAGE andmeväljal töökojakaardile, nagu on kirjeldatud 2.liites. Töökojakaart teeb kõik nõudes CSM_227 määratletud kontrollid ja toimingud.

14. ALLALAADITUD ANDMETE ALLKIRJASTAMINE JA ALLKIRJADE KONTROLLIMINE

14.1. **Üldist**

CSM_231 Programmeeritav eriotstarbeline seade (IDE) salvestab sõidukiseadmest või kaardilt ühe allalaadimisseansi käigus saadud andmed ühte füüsilisse andmefaili. Andmed võidakse salvestada välisandmekandjale. Kõnealune fail sisaldab andmeplokkidele antud digitaalallkirju vastavalt 7. liitele. Samuti peab faili sisaldama järgmisi sertifikaate (vt punkt 9.1.):

— Sõidukiseadmest allalaadimise korral:

— sertifikaat VU_Sign,

— sertifikaat MSCA_VU-EGF, mis sisaldab avalikku võtit, mida kasutatakse sertifikaadi VU_Sign kontrollimiseks;

— Kaardi allalaadimise korral:

— sertifikaat Card_Sign,

— sertifikaat MSCA_Card, mis sisaldab avalikku võtit, mida kasutatakse sertifikaadi Card_Sign kontrollimiseks.

CSM_232 Lisaks käsutab eriotstarbeline seade järgmisis sertifikaate:

— kui ta kasutab allkirja kontrollimiseks kontrollikaarti, nagu on näidatud joonisel 13: lülisertifikaat, mis seostab omavahel uusima EUR-sertifikaadi ja sellele vahetult eelnenud kehtivusajaga EUR-sertifikaadi, kui see on olemas;

— kui ta kontrollib allkirja ise: kõik kehtivad Euroopa juursertifikaadid.

Märkus: käesolevas liites ei ole kirjeldatud meetodit, mida eriotstarbeline seade kasutab nende sertifikaatide saamiseks.

14.2. **Allkirja loomine**

CSM_233 Allalaaditud andmetele digitaalallkirja loomise algoritm on standardis DSS kirjeldatud ECDSA ning vastavalt nõudele CSM_50 kasutatakse sõidukiseadme või kaardi võtme suurusega seotud räsialgoritmi. Allkirja vorming on tehnilises eeskirjas TR-03111 kirjeldatud lihtvorming.

14.3. **Allkirja kontrollimine**

CSM_234 Eriotstarbeline seade võib kontrollida allalaaditud andmete allkirja ise või kasutada selleks kontrollikaarti. Kontrollikaardi kasutamise korral toimub allkirja kontrollimine vastavalt joonisele 13. Kui eriotstarbeline seade kontrollib allkirja ise, kontrollib ta kõigi andmefaili sertifikaadiahelasse kuuluvate sertifikaatide autentsust ja kehtivust ning kontrollib andmete allkirja vastavalt standardis DSS määratletud allkirjaskeemile.

Märkused joonise 13 kohta

— Seade, mis on analüüsitavad andmed allkirjastanud, on tähistatud lühendiga EQT.

— Joonisel on kujutatud neid EQT sertifikaate ja avalikke võtmeid, mida kasutatakse allkirjastamiseks, st VU_Sign või Card_Sign.

— Joonisel on kujutatud neid EQT.CA sertifikaate ja avalikke võtmeid, mida kasutatakse vastavalt vajadusele sõidukiseadme või kaardi sertifikaatide allkirjastamiseks.

— Joonisel kujutatud sertifikaat EQT.CA.EUR on Euroopa juursertifikaat, millele osutatakse sertifikaadis EQT.CA sisalduvas sertifitseerimisasutuse viites.

— Joonisel kujutatud sertifikaat EQT.Link tähistab EQT lülisertifikaati, kui see on olemas. Vastavalt punktile 9.1.2 on tegemist Euroopa uue juurvõtmepaari lülisertifikaadiga, mille loob ERCA ja mis allkirjastatakse Euroopa eelmise privaatvõtmega.

— Sertifikaat EQT.Link.EUR on Euroopa juursertifikaat, millele osutatakse sertifikaadis EQT.Link sisalduvas sertifitseerimisasutuse viites.

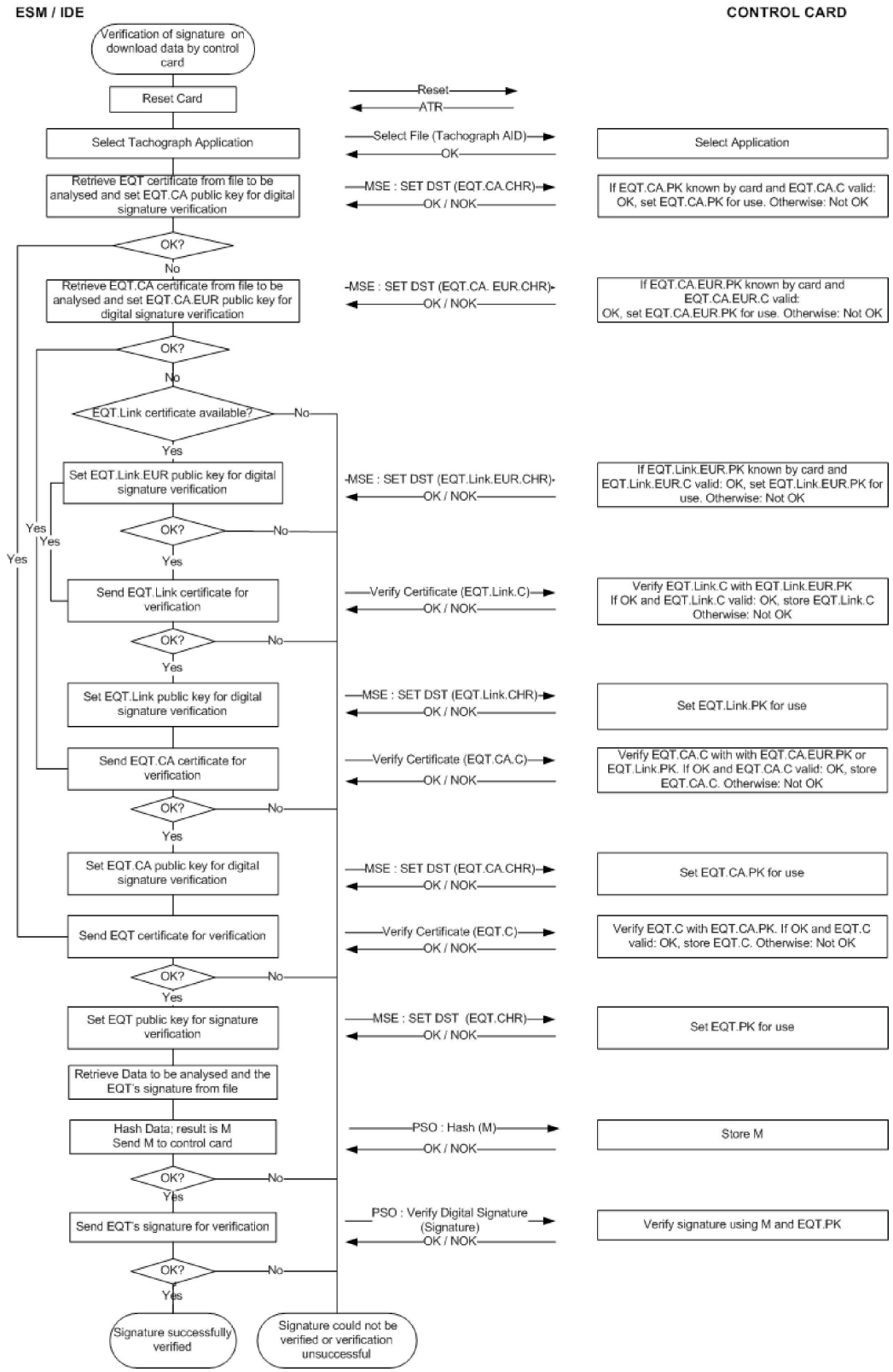
CSM_235 Eriotstarbeline seade kasutab käsuga PSO:Hash kontrollikaardile saadetud räsiväärtuse M arvutamiseks räsialgoritmi, mis on seotud selle sõidukiseadme või kaardi, kust andmed alla laaditi, võtme suurusega vastavalt nõudele CSM_50.

CSM_236 Kontrollikaart järgib EQT allkirja kontrollimiseks standardis DSS määratletud allkirjaskeemi.

Märkus: käesolevas dokumendis ei kirjeldata, mida tehakse juhul, kui allalaaditud andmete faili allkirja ei ole võimalik kontrollida või kui kontrollimine ebaõnnestub.

Joonis 13.

Allalaaditud andmete faili allkirja kontrollimise protokoll



12. liide

ÜLEMAAILMSEL SATELLIITNAVIGATSIOONISÜSTEEMIL (GNSS) PÕHINEV POSITSIONEERIMINE

SISUKORD

1. SISSEJUHATUS

Käesolevas liites sätestatakse tehnilised nõuded sõiduki seadmes kasutatavatele GNSSi andmetele, sealhulgas protokollidele, mida rakendatakse eesmärgiga tagada positsioneerimisandmete turvaline ja vigadeta edastamine.

Need nõuded tulenevad peamiselt järgmistest määruse (EL) nr 165/2014 artiklitest: artikkel 8 „Sõiduki asukoha salvestamine igapäevase tööaja konkreetsetes punktides“, artikkel 10 „Intelligentsete transpordisüsteemide liides“ ja artikkel 11 „Üksikasjalikud sätted aruka sõidumeeriku“.

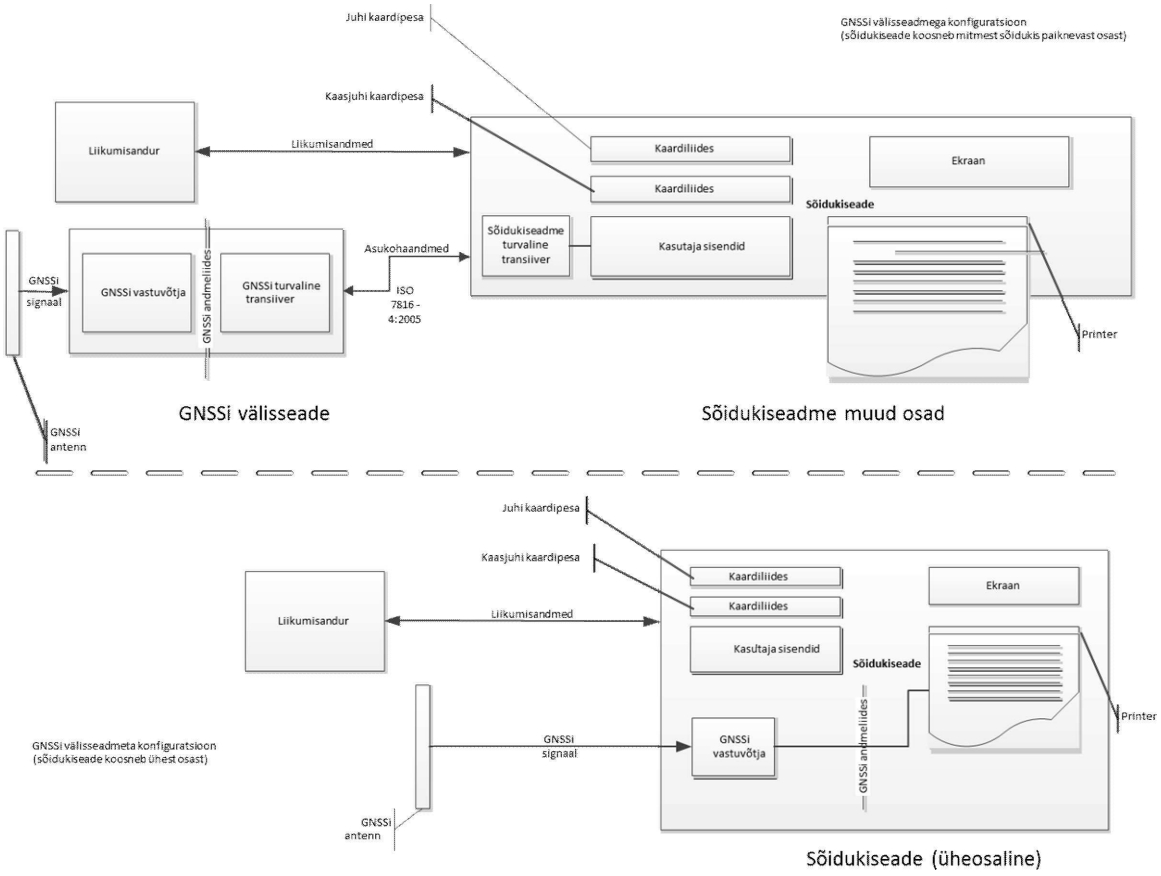
1.1. **Reguleerimisala**

GNS_1 Artikli 8 rakendamise toetamiseks kogutakse sõidukiseadmega asukohaandmeid vähemalt ühe GNSSi kaudu.

Sõidukiseade võib olla koos GNSSi välisseadmega või ilma selleta, nagu on kirjeldatud joonisel 1.

Joonis 1

GNSSi vastuvõtja eri konfiguratsioonid



1.2. **Lühendid ja tähised**

Käesolevas liites kasutatakse järgmisi lühendeid.

DOP täpsuse kadu (*Dilution of Precision*)

EGF elementaarfail GNSSi seadmes

EGNOS Euroopa Geostatsionaarne Navigatsioonilisasüsteem (*European Geostationary Navigation Overlay Service*)

GNSS ülemaailmne satelliitnavigatsioonisüsteem (*Global Navigation Satellite System*)

GSA GPSi DOP ja aktiivsed satelliidid

HDOP horisontaalse täpsuse kadu (*Horizontal Dilution of Precision*)

ICD liidese juhenddokument (*Interface Control Document*)

NMEA USA Riiklik Mereelektroonika Ühing (*National Marine Electronics Association*)

PDOP asukoha täpsuse kadu (*Position Dilution of Precision*)

RMC minimaalne soovitatav teave (*Recommended Minimum Specific*)

SIS signaal õhuruumis (*Signal in Space*)

VDOP vertikaalse täpsuse kadu (*Vertical Dilution of Precision*)

VU sõidukiseade (*Vehicle Unit*)

2. GNSSI VASTUVÕTJA SPETSIFIKATSIOON

Olenemata sellest, kas aruka sõidumeeriku konfiguratsiooniga on ette nähtud GNSSi välisseade või mitte, on täpse ja usaldusväärse positsioneerimisteabe edastamine aruka sõidumeeriku tõhusa töö tagamiseks hädavajalik. Seepärast on asjakohane nõuda meeriku ühilduvust Galileo programmi ja Euroopa Geostatsionaarse Navigatsioonilisasüsteemi (*European Geostationary Navigation Overlay Service*, EGNOS) programmi kaudu pakutavate teenustega, nagu on sätestatud Euroopa Parlamendi ja nõukogu määruses (EL) nr 1285/2013 ([1]). Galileo programmi raames loodud süsteem on sõltumatu ülemaailmne satelliitnavigatsioonisüsteem ning programmi EGNOS alusel loodud süsteem on piirkondlik satelliitnavigatsioonisüsteem, mis parandab globaalse positsioneerimissüsteemi signaali kvaliteeti.

GNS_2 Tootjad tagavad, et aruka sõidumeeriku GNSSi vastuvõtja ühildub Galileo ja EGNOSe positsioneerimisteenustega. Tootjad võivad lisaks tagada ühilduvuse ka muude satelliitnavigatsioonisüsteemidega.

GNS_3 GNSSi vastuvõtja peab olema võimeline toetama autentimist Galileo avatud teenuse raames, kui Galileo süsteemis hakatakse sellist teenust pakkuma ja GNSSi vastuvõtja tootjad seda toetavad. Sellise aruka sõidumeeriku puhul, mis lastakse turule enne, kui eespool nimetatud tingimused on täidetud, ja mis ei ole võimeline toetama autentimist Galileo avatud teenuse raames, ei ole moderniseerimine siiski nõutav.

3. NMEA LAUSENDID

Käesolevas peatükis kirjeldatakse aruka sõidumeeriku töös kasutatavaid NMEA lausendeid. Käesolevas peatükis sätestatu kehtib nii GNSSi välisseadmega kui ka ilma selleta aruka sõidumeeriku konfiguratsiooni puhul.

GNS_4 Asukohaandmed põhinevad GNSSi andmeid sisaldaval NMEA lausendil *Recommended Minimum Specific* (RMC, minimaalne soovitatav teave), mis hõlmab asukohateavet (laius- ja pikkuskraad), kellaaega UTC vormingus (ttmmss.ss) ja kiirust maapinna suhtes sõlmedes ning täiendavaid andmeid.

RMC-lausendi vorming (vastavalt NMEA standardile V4.1) on järgmine:

([1]) Euroopa Parlamendi ja nõukogu 11. detsembri 2013. aasta määrus (EL) nr 1285/2013 Euroopa satelliitnavigatsioonisüsteemide rajamise ja kasutamise kohta, millega tunnistatakse kehtetuks nõukogu määrus (EÜ) nr 876/2002 ning Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 683/2008 (ELT L 347, 20.12.2013, lk 1).

Joonis 2

RMC-lausendi struktuur

1) Kellaaeg (UTC)
2) Staatus: A = asukoht määratud nõuetekohaselt, V = hoiatus
3) Laiuskraad
4) N või S
5) Pikkuskraad
6) E või W
7) Kiirus maapinna suhtes sõlmedes
8) Tegelik teekonnanurk kraadides geograafilise põhjasuuna suhtes
9) Kuupäev, ppkkaa
10) Magnetiline varieeruvus kraadides
11) E või W
12) Kontrollsumma

Staatusest nähtub, kas GNSSi signaal on kättesaadav. Niikaua kui staatuseks ei ole märgitud „A“, ei saa vastuvõetud andmeid (nt aeg või pikkuskraad/laiuskraad) kasutada sõiduki asukoha salvestamiseks sõidukiseadmes.

Asukoha määramise täpsus põhineb eespool kirjeldatud RMC-lausendi vormingul. Väljade 3 ja 5 esimest osa kasutatakse kraadide väljendamiseks. Ülejäänud numbritega väljendatakse minuteid kolme kümnendkohaga. Seega on määramise täpsus 1/1000 minutit ehk 1/60000 kraadi (sest üks minut on 1/60 kraadi).

GNS_5 Sõidukiseadme andmebaasis salvestatakse asukohateave laius- ja pikkuskraadides täpsusega 1/10 minutit ehk 1/600 kraadi, nagu on kirjeldatud 1. liites andmetüübi „GeoCoordinates“ puhul.

Sõidukiseadmes võib signaali kättesaadavuse ja täpsuse kindlakstegemiseks ning selle teabe salvestamiseks kasutada käsku GSA (GPS DOP ja aktiivsed satelliidid). Eelkõige kasutatakse salvestatud asukohaandmete täpsuse hindamiseks näitajat HDOP (vt punkt 4.2.2). Sõidukiseadmes salvestatakse horisontaalse täpsuse kao (HDOP) see väärtus, mis vastab kättesaadavate GNSSide puhul saadud HDOP väärtustest väikseimale.

GNSSi identimistunnusest nähtub, kas tegemist on GPSi, Glonassi, Galileo, Beidou või satelliidipõhise võimendussüsteemiga (SBAS).

Joonis 3

GSA-lausendi struktuur

1) Valikurežiim
2) Režiim
3) Lukustamisel kasutatud 1. satelliidi identimistunnus
4) Lukustamisel kasutatud 2. satelliidi identimistunnus
...
14) Lukustamisel kasutatud 12. satelliidi identimistunnus
15) PDOP meetrites
16) HDOP meetrites
17) VDOP meetrites
18) GNSS identimistunnus
19) Kontrollsumma

Režiimi väljal (2) näidatakse ära, kas lukustus puudub (väärtus „1“) või on kättesaadav 2D-režiimis (väärtus „2“) või 3D-režiimis (väärtus „3“).

GNS_6 GSA-lausend salvestatakse numbri „06“ all.

GNS_7 NMEA lausendite (nt RMC, GSA või muu) maksimumsuurus, mida saab kasutada salvestatud andmete lugemise käsu puhul mahu määratlemisel, on 85 baiti (vt tabel 1).

4. GNSSI VÄLISSEADMEGA SÕIDUKISEADE

4.1. **Konfiguratsioon**

4.1.1. *Põhikomponendid ja liidesed*

Selle konfiguratsiooni puhul on GNSSi vastuvõtja GNSSi välisseadme osa.

GNS_8 GNSSi välisseade peab saama toidet spetsiaalse sõidukiliidese kaudu.

GNS_9 GNSSi välisseade koosneb järgmistest komponentidest (vt joonis 4):

a) kaubanduslik GNSSi vastuvõtja asukohaandmete edastamiseks GNSSi andmeliidese kaudu. GNSSi andmeliides võib vastata näiteks NMEA standardile V4.10, mille puhul GNSSi vastuvõtja toimib rääkiva seadmena ja edastab eelnevalt kindlaksmääratud tüüpi NMEA lausendid, mis peavad hõlmama vähemalt RMC- ja GSA-lausendeid, sagedusel 1 Hz GNSSi turvalisse transiiverisse. GNSSi andmeliidese töötab omal valikul välja GNSSi välisseadme tootja;

b) transiiverseade (GNSSi turvaline tansiiver), mis on võimeline toetama standardit ISO/IEC 7816-4:2013 (vt punkt 4.2.1), et pidada sidet sõidukiseadmega ja toetada GNSSi vastuvõtjaga ühendatud GNSSi andmeliidest. Transiiverseadmel on mälu, kuhu saab salvestada GNSSi vastuvõtja ja GNSSi välisseadme identimisandmed;

c) rikkumist tuvastada võimaldav süsteem kaitsekestaga, mis ümbritseb nii GNSSi vastuvõtjat kui ka GNSSi turvalist transiiverit. Rikkumise tuvastamise funktsiooni puhul rakendatakse turvalisuse kaitse meetmeid, mis on ette nähtud aruka sõidumeeriku kaitseprofiilis;

d) sõidukile paigaldatud GNSSi antenn, mis on ühendatud läbi kaitsekesta GNSSi vastuvõtjaga.

GNS_10 GNSSi välisseadmel on vähemalt järgmised välisliidesed:

a) liides sõidukile paigaldatud GNSSi antenniga, kui välisantenn on kasutusel;

b) liides sõidukiseadmega.

GNS_11 Sõidukiseadmes paikneb turvaline transiiver, mille abil peetakse turvalist sidet GNSSi turvalise transiiveriga ja mis peab GNSSi välisseadmega ühenduses olemiseks toetama standardit ISO/IEC 7816-4:2013.

GNS_12 Sõidukiseade peab GNSSi välisseadmega füüsilisel tasandil side pidamiseks toetama standardit ISO/IEC 7816-12:2005 või mõnda muud standardit, mis võimaldab toetada standardit ISO/IEC 7816-4:2013 (vt punkt 4.2.1).

4.1.2. *GNSSi välisseadme staatus toote valmimisel*

GNS_13 GNSSi välisseadmes peavad tehasest väljumisel olema GNSSi turvalise transiiveri säilmälus salvestatud järgmised näitajad:

— EGF_MA võtmepaar ja vastav sertifikaat,

— MSCA_VU-EGFi sertifikaat, mis sisaldab EGF_MA sertifikaadi kontrollimiseks kasutatavat avalikku võtit MSCA_VU-EGF.PK,

— EURi sertifikaat, mis sisaldab MSCA_VU-EGFi sertifikaadi kontrollimiseks kasutatavat avalikku võtit EUR.PK,

— olemasolu korral EURi sertifikaat, mille kehtivusperiood eelneb vahetult selle EURi sertifikaadi omale, mida kasutatakse MSCA_VU-EGFi sertifikaadi kontrollimiseks,

— olemasolu korral neid kahte EURi sertifikaati ühendav üleminekusertifikaat,

— GNSSi välisseadme laiendatud seerianumber,

— GNSSi seadme operatsioonisüsteemi identimistunnus,

— GNSSi välisseadme tüübikinnitusnumber,

— GNSSi välisseadme turvakomponendi identimistunnus.

4.2. **Sidepidamine GNSSi välisseadme ja sõidukiseadme vahel**

4.2.1. *Sideprotokoll*

GNS_14 GNSSi välisseadme ja sõidukiseadme vaheliseks sidepidamiseks kasutatav sideprotokoll peab toetama kolme funktsiooni:

1. GNSSi andmete (nt asukoht, aeg, kiirus) kogumine ja edastamine,

2. GNSSi välisseadme seadistusandmete kogumine,

3. haldusprotokolli kasutamine GNSSi välisseadme ja sõidukiseadme vahelise ühenduse loomiseks, vastastikuseks autentimiseks ja seansivõtmes kokku leppimiseks.

GNS_15 Sideprotokoll peab põhinema standardil ISO/IEC 7816-4:2013, kusjuures sõidukiseadme turvaline transiiver peab olema ülema ja GNSSi turvaline transiiver alluva rollis. Füüsiline ühendus GNSSi välisseadme ja sõidukiseadme vahel põhineb standardil ISO/IEC 7816-12:2005 või mõnel muul standardil, mis võimaldab toetada standardit ISO/IEC 7816-4:2013.

GNS_16 Sideprotokollis ei toetata laiendatud väljade kasutamist.

GNS_17 Standardite ISO 7816-4:2013 ja 7816-12:2005 kohases GNSSi välisseadme ja sõidukiseadme vahelises sides kasutatakse protokolli T = 1.

GNS_18 GNSSi turvaline transiiver simuleerib funktsioonide 1) „GNSSi andmete kogumine ja edastamine“, 2) „GNSSi välisseadme seadistusandmete kogumine“ ja 3) „haldusprotokolli kasutamine“ rakendamisel kiipkaarti, kasutades sellise ülesehitusega failisüsteemi, mis koosneb põhifailist (MF) ja 1. liite punktis 6.2 määratletud rakenduse identimistunnusega „FF 44 54 45 47 4D“ ning sertifikaate sisaldava kolme elementaarfaili (EF) ja ühe identimistunnusele „2F2F“ vastava elementaarfailiga (EF.EGF) erifailist (DF), nagu on kirjeldatud tabelis 1.

GNS_19 GNSSi turvalises transiiveris salvestatakse GNSSi vastuvõtjast saabunud andmed ja seadistusandmed failis EF.EGF. Tegemist on varieeruva pikkusega lineaarse andmefailiga, mille identimistunnus kuuekümnendsüsteemis on „2F2F“.

GNS_20 GNSSi turvalises transiiveris kasutatakse andmete salvestamiseks mälu, mis võimaldab läbi viia vähemalt 20 miljonit kirjutamise/lugemise tsüklit. Kui see aspekt välja arvata, jäävad GNSSi turvalise transiiveri siseehituse ja väljatöötamise üksikasjad tootja otsustada.

Kannete numbrite ja andmete kaardistus on esitatud tabelis 1. Pange tähele, et tabelis on neli GSA-lausendit nelja satelliidisüsteemi jaoks ja üks satelliidipõhise võimendussüsteemi (SBAS) jaoks.

GNS_21 Failistruktuur on esitatud tabelis 1. Juurdepääsutingimusi (ALW, NEV, SM-MAC) on selgitatud 2. liite punktis 3.5.

Tabel 1

Failistruktuur

		Juurdepääsutingimused		
Fail	Faili identimis-tunnus	Lugemine	Ajakohasta-mine	Kodeeritud
MF	3F00			
EF.ICC	0002	ALW	NEV (sõidukisead-mes)	Ei
DF GNSSi seadmes	0501	ALW	NEV	Ei
EF EGF_MACertificate	C100	ALW	NEV	Ei
EF CA_Certificate	C108	ALW	NEV	Ei
EF Link_Certificate	C109	ALW	NEV	Ei
EF.EGF	2F2F	SM-MAC	NEV (sõidukisead-mes)	Ei

Fail/andmeelement	Kande number	Suurus (baitides)		Vaikimisi väär-tused
		Min.	Maks.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSSi seadmes		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
NMEA RMC-lausend	„01“	85	85	
Esimene NMEA GSA-lausend	„02“	85	85	
Teine NMEA GSA-lausend	„03“	85	85	

Fail/andmeelement	Kande number	Suurus (baitides)		Vaikimisi väärtused
		Min.	Maks.	
Kolmas NMEA GSA-lausend	„04“	85	85	
Neljas NMEA GSA-lausend	„05“	85	85	
Viies NMEA GSA-lausend	„06“	85	85	
GNSSi välisseadme laiendatud seerianumber, mis on määratletud 1. liites kui sensorGNSSSerialNumber	„07“	8	8	
GNSSi turvalise transiiveri operatsioonisüsteemi identimistunnus, mis on määratletud 1. liites kui SensorOSIdentifier	„08“	2	2	
GNSSi välisseadme tüübikinnitusnumber, mis on määratletud 1. liites kui SensorExternalGNSSApprovalNumber	„09“	16	16	
GNSSi välisseadme turvakomponendi identimistunnus, mis on määratletud 1. liites kui SensorExternalGNSSSCIdentifier	„10“	8	8	
Jäetud kasutamiseks tulevikus	„11“ kuni „FD“			

4.2.2. *GNSSi andmete turvaline edastamine*

GNS_22 GNSSi asukohaandmete turvaline edastamine on lubatud üksnes järgmistel tingimustel:

1. ühendamisprotsess on lõpule viidud, nagu on kirjeldatud 11. liites „Ühised turbemehhanismid“;

2. sõidukiseadme ja GNSSi välisseadme vaheline regulaarne vastastikune autentimine ja seansivõtmes kokku leppimine, mida on samuti kirjeldatud 11. liites „Ühised turbemehhanismid“, peab olema ettenähtud sagedusega läbi viidud.

GNS_23 Sõidukiseade taotleb GNSSi välisseadmelt iga T sekundi järel (T väärtus on 10 või väiksem), välja arvatud vastastikuse autentimise ja seansivõtmes kokku leppimise ajal asukohateavet vastavalt järgmisele teabevoole.

1. Sõidukiseade taotleb GNSSi välisseadmelt asukohaandmeid koos täpsuse kao andmetega (NMEA GSA-lausendist). Sõidukiseadme turvalises transiiveris kasutatakse standardi ISO/IEC 7816-4:2013 käske SELECT ja READ RECORD(S) autentimist nõudvas turvalise sõnumivahetuse režiimis, nagu on kirjeldatud 11. liite punktis 11.5, kusjuures faili identimistunnus on „2F2F“ ning kande (RECORD) number on NMEA RMC-lausendi puhul „01“ ja NMEA GSA-lausendi puhul „02“, „03“, „04“, „05“ või „06“.

2. GNSSi turvalises transiiveris, kuhu saabuvad GNSSi vastuvõtjast GNSSi andmeliidese kaudu sagedusega vähemalt 1 Hz NMEA vormingus andmed, salvestatakse viimased asukohaandmed tabelis 1 kirjeldatud kannete kujul EFs identimistunnusega „2F2F“.

3. GNSSi turvaline transiiver saadab sõidukiseadme turvalisse transiiverisse 11. liite punkti 11.5 kirjeldusele vastavas autentimist nõudvas turvalise sõnumivahetuse režiimis APDU-vastussõnumi.

4. Sõidukiseadme turvalises transiiveris kontrollitakse saadud vastuse autentsust ja terviklikkust. Positiivse tulemuse korral saadetakse asukohaandmed GNSSi andmeliidese kaudu sõidukiseadme protsessorisse.

5. Sõidukiseadme protsessoris kontrollitakse saabunud andmeid ja võetakse NMEA RMC-lausendist asjakohane teave (nt pikkuskraad, laiuskraad, kellaaeg). NMEA RMC-lausend sisaldab teavet selle kohta, kas asukoht on määratud nõuetekohaselt. Kui asukoht ei ole määratud nõuetekohaselt, ei ole asukohaandmed veel kättesaadavad ja neid ei saa kasutada sõiduki asukoha salvestamiseks. Kui asukoht on määratud nõuetekohaselt, võtab sõidukiseadme protsessor NMEA GSA-lausenditest ka HDOP väärtused ja arvutab kättesaadavate (st asjaomasel hetkel lukustamist võimaldavate) satelliidisüsteemidega saadud väärtuste keskmise.

6. Sõidukiseadme protsessor salvestab saadud ja töödeldud andmed, näiteks pikkus- ja laiuskraadi, kellaaja ja kiiruse sõidukiseadmes vormingus, mis on määratletud 1. liites „Andmesõnastik" andmetüübi „GeoCoordinates" puhul; samuti salvestatakse HDOP see väärtus, mis vastab kättesaadavate GNSSide puhul saadud HDOP väärtustest väikseimale.

4.2.3. *Käsu „Read Record" struktuur*

Käesolevas punktis kirjeldatakse üksikasjalikult käsu „Read Record" struktuuri. Lisandub turvaline sõnumivahetus autentimist nõudvas režiimis, nagu on kirjeldatud 11. liites „Ühised turbemehhanismid".

GNS_24 Kõnealune käsk peab toetama turvalist sõnumivahetust autentimist nõudvas režiimis – vt 11. liide.

GNS_25 Käsusõnum

Bait	Pikkus	Väärtus	Kirjeldus
CLA	1	„0Ch"	Nõutakse turvalist sõnumivahetust
INS	1	„B2h"	Loe kannet
P1	1	„XXh"	Kande number („00" tähistab olemasolevat kannet)
P2	1	„04h"	Loe kannet, mille number on märgitud P1-s
Le	1	„XXh"	Oodatava andmerea pikkus; loetavate baitide arv

GNS_26 P1-s osutatud kanne muutub olemasolevaks kandeks.

Bait	Pikkus	Väärtus	Kirjeldus
#1-#X	X	„XX..XXh"	Loetud andmed
SW	2	„XXXXh"	Olekubaidid (SW1, SW2)

— Kui käsk on edukas, saadab GNSSi turvaline transiiver vastuse „**9000**".

— Kui olemasolev fail ei ole kannetele orienteeritud, saadab GNSSi turvaline transiiver vastuse „**6981**".

— Kui kasutatud käsu puhul P1 = „00", kuid olemasolev EF puudub, saadab GNSSi turvaline transiiver vastuse „**6986**" (käsk ei ole lubatud).

— Kui kannet ei leitud, saadab GNSSi turvaline transiiver vastuse „**6A83**".

— Kui GNSSi välisseadmel on tuvastatud rikkumine, saadetakse vastuseks olekubaidid „**6690**".

GNS_27 GNSSi turvaline transiiver peab toetama järgmisi sõidumeerikus kasutatavaid 2. liites määratletud 2. põlvkonna käske:

Käsk	Viide
Select	2. liite punkt 3.5.1
Read Binary	2. liite punkt 3.5.2
Get Challenge	2. liite punkt 3.5.4
PSO: Verify Certificate	2. liite punkt 3.5.7
External Authenticate	2. liite punkt 3.5.9
General Authenticate	2. liite punkt 3.5.10
MSE:SET	2. liite punkt 3.5.11

4.3. **GNSSi välisseadme ja sõidukiseadme vaheline ühenduse loomine, vastastikune autentimine ja seansivõtmes kokku leppimine**

GNSSi välisseadme ja sõidukiseadme vahelise ühenduse loomist, vastastikust autentimist ja seansivõtmes kokku leppimist kirjeldatakse 11. liite „Ühised turbemehhanismid“ 11. peatükis.

4.4. **Vigade käsitlemine**

Käesolevas punktis kirjeldatakse, kuidas GNSSi välisseadmega seotud võimalikke veaolukordi sõidukiseadmes käsitletakse ja salvestatakse.

4.4.1. *GNSSi välisseadmega side pidamise viga*

GNS_28 Kui sõidukiseade ei suuda ühendatud GNSSi välisseadmega enam kui 20 järjestikuse minuti jooksul sidet saada, luuakse ja salvestatakse sõidukiseadmes liiki EventFaultType kuuluv sündmus „GNSSi välisseadmega side pidamise viga“ enumeraatori väärtusega „53“H ja hetke kellaaega kajastava ajatempliga. Sündmus luuakse üksnes juhul, kui on täidetud järgmised kaks tingimust: a) arukas sõidumeerik ei ole kalibreerimisrežiimis ja b) sõiduk liigub. Selles kontekstis registreeritakse sidepidamise viga juhul, kui sõidukiseadme turvaline transiiver ei saa punktis 4.2 kirjeldatud nõudesõnumi saatmise järel vastussõnumit.

4.4.2. *GNSSi välisseadme füüsilise terviklikkuse rikkumine*

GNS_29 Kui GNSSi välisseadet on rikutud, kustutatakse GNSSi turvalise transiiveri kogu mälu, sealhulgas krüptitud materjal. Sõidukiseade tuvastab rikkumise, kui vastuse staatus on „6690“, nagu on kirjeldatud punktides GNS_25 ja GNS_26. Seejärel luuakse sõidukiseadmes liiki EventFaultType kuuluv sündmus „GNSSi seadmega manipuleerimise tuvastamine“ enumeraatori väärtusega „55“H.

4.4.3. *Asukohateabe mittelaekumine GNSSi vastuvõtjast*

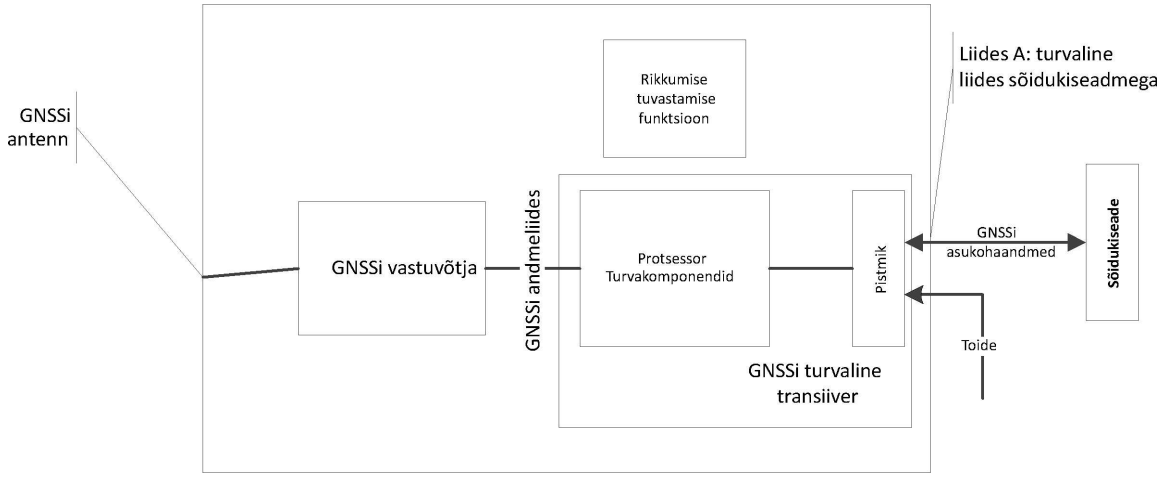
GNS_30 Kui GNSSi vastuvõtjast ei saabu GNSSi turvalisse transiiverisse enam kui 3 järjestikuse tunni jooksul andmeid, saadetakse GNSSi turvalisest transiiverist käsu READ RECORD peale vastussõnum, kus kande (RECORD) number on „01“ ja andmeväljal on kõik 12 baiti seatud väärtusele „0xFF“. Sellise andmeväljal oleva väärtusega vastussõnumi saabumisel luuakse ja salvestatakse sõidukiseadmes liiki EventFaultType kuuluv sündmus „GNSSi välisvastuvõtja viga“ enumeraatori väärtusega „52“H ja hetke kellaaega kajastava ajatempliga, kuid üksnes juhul, kui on täidetud järgmised kaks tingimust: a) arukas sõidumeerik ei ole kalibreerimisrežiimis ja b) sõiduk liigub.

4.4.4. *GNSSi välisseadme sertifikaadi aegumine*

GNS_31 Kui sõidukiseadmes tuvastatakse, et vastastikuseks autentimiseks kasutatav EGFi sertifikaat enam ei kehti, luuakse ja salvestatakse sõidukiseadmes liiki EventFaultType kuuluv salvestusseadme viga kirjeldav sündmus „GNSSi välisseadme sertifikaat aegunud“ enumeraatori väärtusega „56“H ja hetke kellaaega kajastava ajatempliga. Saabunud GNSSi asukohaandmeid kasutatakse sõidukiseadmes edasi.

Joonis 4

GNSSi välisseadme skeem



5. GNSSI VÄLISSEADMETA SÕIDUKISEADE

5.1. Konfiguratsioon

Selle konfiguratsiooni puhul paikneb GNSSi vastuvõtja sõidukiseadmes, nagu on kirjeldatud joonisel 1.

GNS_32 GNSSi vastuvõtja toimib rääkiva seadmena ja edastab eelnevalt kindlaks määratud tüüpi NMEA lausendid, mis peavad hõlmama vähemalt RMC- ja GSA-lausendeid, sagedusel vähemalt 1/10 Hz sõidukiseadme protsessorisse, mis toimib kuulava seadmena.

GNS_33 Sõidukile paigaldatud GNSSi välisantenn või GNSSi siseantenn peab olema ühendatud sõidukiseadmega.

5.2. Vigade käsitlemine

5.2.1. *Asukohateabe mittelaekumine GNSSi vastuvõtjast*

GNS_34 Kui GNSSi vastuvõtjast ei saabu sõidukiseadmesse enam kui 3 järjestikuse tunni jooksul andmeid, luuakse ja salvestatakse sõidukiseadmes liiki EventFaultType kuuluv sündmus „GNSSi sisemise vastuvõtja viga“ enumeraatori väärtusega „51“H ja hetke kellaaega kajastava ajatempliga, kuid üksnes juhul, kui on täidetud järgmised kaks tingimust: a) arukas sõidumeerik ei ole kalibreerimisrežiimis ja b) sõiduk liigub.

6. VASTUOLU GNSSI KELLAAJA ANDMETES

Kui sõidukiseadmes tuvastatakse enam kui 1 minuti suurune erinevus sõidukiseadme ajamõõtmisfunktsiooni kohase kellaaja ja GNSSi vastuvõtjast pärineva kellaaja vahel, salvestatakse sõidukiseadmes liiki EventFaultType kuuluv sündmus „ajakonflikt (GNSSi kellaaja ja sõidukiseadme sisekella võrdlus)“ enumeraatori väärtusega „0B“H. See sündmus salvestatakse koos sõidukiseadme sisekella näiduga ja sellega kaasneb automaatne kellaaja korrigeerimine. Pärast kellaaja andmete vastuoluga seotud sündmuse esinemist ei kontrollita sõidukiseadmes järgmise 12 tunni jooksul kellaaja erinevust. See sündmus ei käivitu juhul, kui GNSSi vastuvõtjasse ei ole viimase 30 päeva jooksul saabunud nõuetekohast GNSSi signaali. Kui aga asukohateave muutub GNSSi vastuvõtjast taas kättesaadavaks, toimub automaatne kellaaja korrigeerimine.

7. VASTUOLU SÕIDUKI LIIKUMISANDMETES

GNS_35 Kui liikumisanduri abil saadud liikumisandmed erinevad GNSSi sisemise vastuvõtja või GNSSi välisseadme abil saadud liikumisandmetest, luuakse ja salvestatakse sõidukiseadmes sündmus „vastuolu sõiduki liikumisandmetes“ (vt käesoleva lisa nõue 84) hetke kellaaega kajastava ajatempliga. Sellise vastuolu kindlakstegemiseks kasutatakse nimetatud allikatest saadud kiiruseandmete erinevuste mediaanväärtust, mis arvutatakse järgmiselt:

— vähemalt iga 10 sekundi järel arvutatakse sõiduki GNSSi andmete põhjal saadud kiiruse ja liikumisanduri andmete põhjal saadud kiiruse erinevuse absoluutväärtus;

— mediaanväärtuse arvutamiseks kasutatakse kõiki viimase viie sõiduminuti kestel saadud kõnealuseid absoluutväärtusi;

— pärast suurimate absoluutväärtuste kõrvalejätmist arvutatakse mediaanväärtus ülejäänud 80 % absoluutväärtuste põhjal.

Sündmus „vastuolu sõiduki liikumisandmetes“ luuakse juhul, kui kõnealune mediaanväärtus viie katkematu sõiduminuti kohta on suurem kui 10 km/h. Sõidumeerikuga manipuleerimise usaldusväärsemaks kindlakstegemiseks võib lisaks kasutada muid sõltumatuid sõiduki liikumise tuvastamist võimaldavaid andmeid. (I viimase viie minuti andmete mediaanväärtust kasutatakse selleks, et vähendada võõrväärtuste ja ajutiste väärtuste mõju.) See sündmus ei käivitu järgmistel juhtudel: a) parvlaeva-/rongisõidu ajal, b) kui asukohateave ei ole GNSSi vastuvõtjast kättesaadav ja c) kalibreerimisrežiimis.

13. liide

INTELLIGENTSE TRANSPORDISÜSTEEMI LIIDES

SISUKORD

1. SISSEJUHATUS

Käesolevas liites kirjeldatakse intelligentse transpordisüsteemi (ITS) liidese ülesehitust ning selle kasutusele võtmise korda vastavalt määruse (EL) nr 165/2014 (edaspidi „määrus“) artikli 10 nõuetele.

Määrusega on sätestatud, et sõidumeerikud võivad olla varustatud standarditud liidesega, mis võimaldab välisel seadmel kasutada sõidumeerikuga salvestatud või genereeritud andmeid töörežiimis, kui on täidetud järgmised tingimused:

a) liides ei mõjuta sõidumeeriku andmete õigsust ja terviklust;

b) liides on kooskõlas määruse artikli 11 üksikasjalike sätetega;

c) liidesega ühendatud väline seade saab juurdepääsu isikuandmetele, sealhulgas positsioneerimisandmetele alles pärast seda, kui juht, kellega need andmed on seotud, annab selleks kontrollitava nõusoleku.

2. REGULEERIMISALA

Käesoleva liite reguleerimisala hõlmab kirjeldust, kuidas välises seadmes asuvad rakendused saavad Bluetooth®-ühenduse kaudu sõidumeerikust andmeid (edaspidi „andmed“) hankida.

Liidese kaudu kättesaadavaid andmeid on kirjeldatud käesoleva liite 1. lisas. Liides ei takista muude liideste (nt CAN-andmesiini) kasutamist sõidukiseadme andmete edastamiseks muudele sõiduki töötlussõlmedele.

Käesolevas liites on määratletud:

— ITSi liidese kaudu kättesaadavad andmed,

— andmete edastamiseks kasutatav Bluetooth®-i profiil,

— päringu- ja allalaadimisprotseduurid ning toimingute järjekord,

— sõidumeeriku ja välisseadme ühendamise mehhanism,

— nõusoleku andmise mehhanism, mida juht saab kasutada.

Selgituseks lisatakse, et käesolevas liites ei ole määratletud järgmised aspektid:

— andmete kogumine ja haldamine sõidukiseadmes (seda kirjeldatakse määruse teistes osades või see lahendatakse tootedisaini käigus);

— kogutud andmete välisseadmes asuvale rakendusele esitamise vorm;

— Bluetooth®-i andmeturbele lisanduvad andmeturbe nõuded (näiteks krüpteerimine) seoses andmete sisuga (neid kirjeldatakse määruse teistes osades (11. liide „Ühised turbemehhanismid“));

— ITSi liidese kasutatavad Bluetooth®-i protokollid.

2.1. **Lühendid, mõisted ja märkused**

Käesolevas liites kasutatakse järgmisi lühendeid ja mõisted:

andmeside teabe/andmete vahetamine põhiseadme (nt sõidumeerik) ja välisseadme vahel ITSi liidese kaudu Bluetooth®-i vahendusel;

andmed 1. lisas määratletud andmekogumid;

määrus Euroopa Parlamendi ja nõukogu määrus (EL) nr 165/2014, 4. veebruar 2014, autovedudel kasutatavate sõidumeerikute kohta, millega tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 3821/85 autovedudel kasutatavate sõidumeerikute kohta ning muudetakse Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 561/2006, mis käsitleb teatavate autovedusid käsitlevate sotsiaalõigusnormide ühtlustamist.

BR (*Basic Rate*) Bluetooth®-i põhikiiruse režiim

EDR (*Enhanced Data Rate*) Bluetooth®-i suurendatud kiiruse režiim

GNSS (*Global Navigation Satellite System*) globaalne satelliitnavigatsioonisüsteem

IRK (*identity resolution key*) identiteedi teisendusvõti

ITS (*Intelligent Transport System*) intelligentne transpordisüsteem

LE (*Low Energy*) Bluetooth®-i madala energiatarbega protokoll

PIN (*personal identification number*) PIN-kood

PUC (*personal unblocking code*) personaalne deblokeerimise kood, PUK-kood

SID (*service identifier*) teenuse identifikaator

SPP (*serial port profile*) jadapordi profiil

SSP (*Secure Simple Pairing*) Bluetooth®-i lihtsa turvalise ühenduse funktsioon

TRTP (*transfer request parameter*) nõude edastusparameeter

TREP (*transfer response parameter*) vastuse edastusparameeter

VU (*vehicle unit*) sõidukiseade

3. VIIDATUD MÄÄRUSED JA STANDARDID

Käesolevas liites määratletud spetsifikaat lähtub ja sõltub tervikuna või osaliselt järgmistest määrustest ja standarditest. Käesoleva liite punktides on täpsustatud vastavad olulised standardid või standardite olulised punktid. Võimaliku vastuolu korral on ülimuslikud käesoleva liite sätted.

Käesolevas liites on viidatud järgmistele määrustele ja standarditele:

— Euroopa Parlamendi ja nõukogu määrus (EL) nr 165/2014, 4. veebruar 2014, autovedudel kasutatavate sõidumeerikute kohta, millega tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 3821/85 autovedudel kasutatavate sõidumeerikute kohta ning muudetakse Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 561/2006, mis käsitleb teatavate autovedusid käsitlevate sotsiaalõigusnormide ühtlustamist;

— Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 561/2006, 15. märts 2006, mis käsitleb teatavate autovedusid käsitlevate sotsiaalõigusnormide ühtlustamist ja millega muudetakse nõukogu määrusi (EMÜ) nr 3821/85 ja (EÜ) nr 2135/98 ning tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 3820/85;

— ISO 16844-4: *Road vehicles – Tachograph systems – Part 4: CAN interface* („Maanteesõidukid. Sõidumeerikusüsteemid. Osa 4: CAN-liides“);

— ISO 16844-7: *Road vehicles – Tachograph systems – Part 7: Parameters* („Maanteesõidukid. Sõidumeerikusüsteemid. Osa 7: Parameetrid“);

— Bluetooth® – Serial Port Profile – V1.2;

— Bluetooth® – Core Version 4.2;

— protokoll NMEA 0183 V4.1.

4. LIIDESE TÖÖPÕHIMÕTTED

4.1. **ITSi liidese kaudu toimuva andmeedastuse eeltingimused**

Sõidukiseade peab hoidma ajakohasena ja säilitama sõidukiseadmesse salvestatavaid andmeid ilma ITSi liidese abita. Selleks kasutatavad vahendid määratakse kindlaks sõidukiseadmes, need on sätestatud määruse muudes osades ning neid ei käsitleta käesolevas liites.

4.1.1. *ITSi liidese kaudu edastatavad andmed*

Sõidukiseade peab ITSi liidese kaudu kättesaadavaid andmeid ajakohastama sagedusega, mis on kindlaks määratud sõidukiseadme protseduurides, ning ilma ITSi liidese abita. Sõidukiseadme andmeid kasutatakse kättesaadavate andmeväljade täitmiseks ja ajakohastamiseks. Selleks kasutatavaid vahendeid on kirjeldatud määruse muudes osades või vastava kirjelduse puudumise korral lahendatakse see tootedisaini käigus ja seda ei käsitleta käesolevas liites.

4.1.2. *Andmete sisu*

Andmete sisu peab vastama käesoleva liite 1. lisale.

4.1.3. *ITSi rakendused*

ITSi rakendused kasutavad ITSi liidese kaudu kättesaadavaks tehtud andmeid näiteks juhi tegevuse haldamise optimeerimiseks kooskõlas määrusega, võimalike sõidumeeriku vigade tuvastamiseks või GNSSi andmete kasutamiseks. Rakenduste kirjeldamine ei kuulu käesoleva liite reguleerimisalasse.

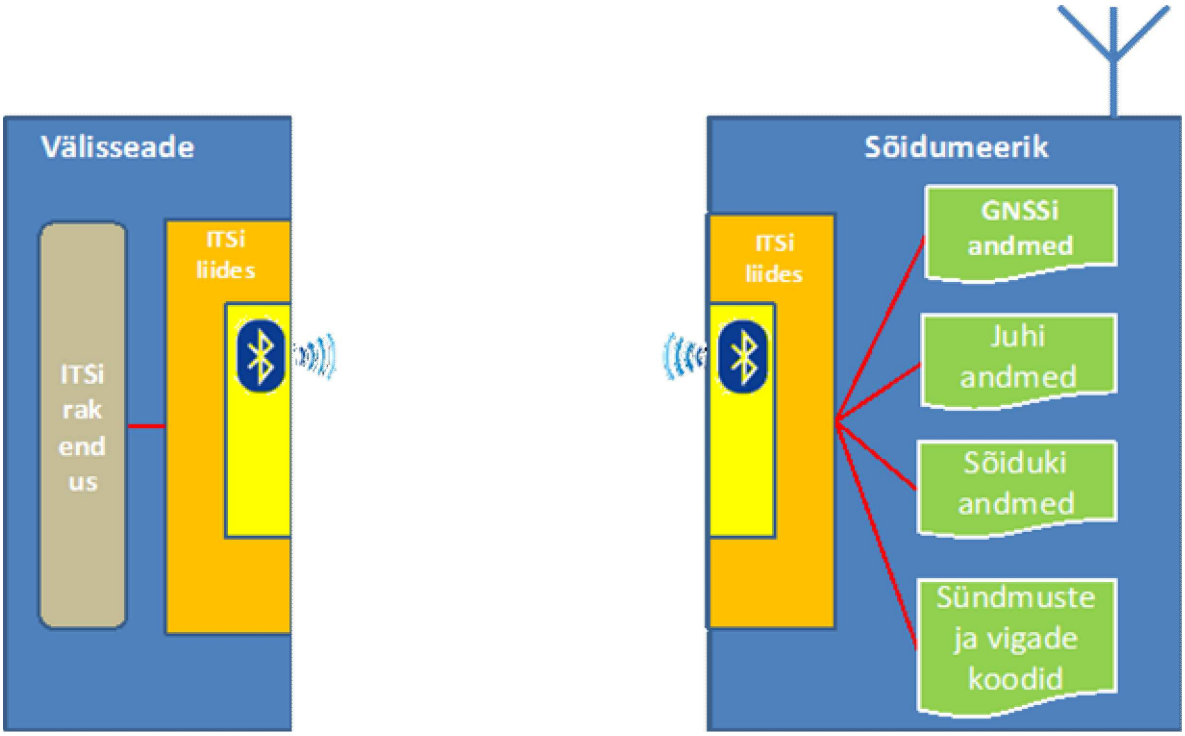
4.2. **Andmeside tehnoloogia**

ITSi liidese kaudu toimuv andmevahetus tuleb teostada Bluetooth®-i liidesega, mis ühildub versiooniga 4.2 või hilisema versiooniga. Bluetooth® toimib tööstus- teadus- ja meditsiiniseadmetele eraldatud litsentseerimata sagedusribas (ISM) 2,4–2,485 GHz. Bluetooth®-i versioon 4.2 sisaldab täiustatud privaatsus- ja turbemehhanisme ning suurendab andmeedastuse kiirust ja usaldusväärsust. Käesoleva spetsifikaadi kohaldamisel eeldatakse kuni 10 meetri kaugusele leviva Bluetooth®-i 2. klassi raadio kasutamist. Lisateavet Bluetooth® 4.2 kohta võib leida veebisaidilt www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Andmeside luuakse andmesideseadmetega pärast seda, kui volitatud seade on teostanud ühendamisprotsessi. Kuna Bluetooth® reguleerib seda, millal ja kuhu seadmed saavad andmeid saata, ülema-alluva mudeli abil, siis täidab sõidumeerik ülema ja välisseade alluva ülesandeid.

Kui välisseade siseneb esimest korda sõidukiseadme levialasse, võib alustada Bluetooth®-i ühendamisprotsessi (vt ka 2. lisa). Seadmed avaldavad üksteisele oma aadressi, nime, profiili ja ühise salajase võtme, mis võimaldab neil edaspidi kokku saades automaatselt ühenduse luua. Kui see etapp on lõppenud, tunnistatakse välisseade usaldusväärseks ning saab esitada sõidumeerikule andmete allalaadimise nõudeid. Täiendavate krüpteerimismehhanismide lisamist lisaks Bluetooth®-i pakutavatele mehhanismidele ei kavandata. Kui täiendavad turbmehhanismid osutuvad siiski vajalikuks, rakendatakse need vastavalt 11. liitele „Ühised turbemehhanismid“.

Andmeside üldpõhimõtet on kirjeldatud järgmisel joonisel.



Andmete edastamiseks sõidukiseadmest välisseadmesse kasutatakse Bluetooth®-i jadapordi profiili (*Serial Port Profile*, SPP).

4.3. **PIN-koodiga volitamine**

Turvakaalutlustel peab sõidukiseade kasutama PIN-koodiga volitamise süsteemi, mis toimib Bluetoothi seadmete ühendamise protsessist eraldi. Iga sõidukiseade peab suutma luua autentimiseks kasutatavaid PIN-koode, mis koosnevad vähemalt neljast numbrist. Sõidukiseadmega ühendudes peab välisseade iga kord esitama õige PIN-koodi, enne kui ta saab mis tahes andmeid vastu võtta.

Kui PIN-koodi sisestamine õnnestub, kantakse seade lubatud seadmete nimekirja. Lubatud seadmete nimekiri peab mahutama vähemalt 64 selle konkreetse sõidukiseadmega ühendatud seadet.

Kui õiget PIN-koodi ei esitata kolmel järjestikusel katsel, kantakse seade ajutiselt keelatud seadmete nimekirja. Keelatud seadmete nimekirjas oleku ajal lükatakse tagasi kõik järgmised seadme tehtavad ühenduse loomise katsed. Kõik järgmised korrad, kui õiget PIN-koodi ei esitata kolmel järjestikusel katsel, toovad kaasa järjest pikeneva keeluperioodi (vt tabel 1). Õige PIN-koodi esitamise korral keeluperioodi pikkuse ja tehtud sisestuskatsete arvestus nullitakse. 2. lisa joonisel 1 on kujutatud PIN-koodi tõendamiskatse skeemi.

Tabel 1

Keelu kestuse seos PIN-koodi esitamise järjestikuste ebaõnnestunud katsete arvuga

Järjestikuste ebaõnnestumiste arv	Keelu kestus
3	30 sekundit
6	5 minutit
9	1 tund
12	24 tundi
15	püsiv

Kui õiget PIN-koodi ei esitata viieteistkümnel järjestikusel katsel (5 × 3), kantakse ITSi seade püsivalt keelatud seadmete nimekirja. Selle püsiva keelu saab tühistada ainult õige PUK-koodi esitamisega.

PUK-kood koosneb kaheksast numbrist ning tootja paneb selle sõidukiseadmega kaasa. Kui õiget PUK-koodi ei esitata kümnel järjestikusel katsel, kantakse ITSi seade jäädavalt keelatud seadmete nimekirja.

Tootja võib soovi korral pakkuda võimalust PIN-koodi vahetamiseks otse sõidukiseadme kaudu, kuid PUK-kood peab olema muutumatu. Kui PIN-koodi muutmine on võimaldatud, tuleb nõuda kehtiva PIN-koodi sisestamist otse sõidukiseadmesse.

Seadmeid säilitatakse lubatud seadmete nimekirjas seni, kuni kasutaja need käsitsi eemaldab (nt sõidukiseadme kasutajaliidese kaudu või muude vahenditega). See võimaldab kadunud ja varastatud ITSi seadmeid lubatud seadmete nimekirjast kustutada. Samuti kustutatakse sõidukiseadme lubatud seadmete nimekirjast automaatselt kõik ITSi seadmed, mis väljuvad Bluetoothi levialast rohkem kui 24 tunniks. Ühenduse taasloomise korral peavad sellised seadmed esitama uuesti õige PIN-koodi.

Sõidukiseadme liidese ja sõidukiseadme vahel liikuvate sõnumite vormingut ei täpsustata; see jäetakse tootja otsustada. Tootja peab siiski tagama, et ITSi seadme ja sõidukiseadme liidese vahel liikuvate sõnumite puhul kasutatakse nõutavad vormingut (vt ASN.1 spetsifikaat).

Seega vastatakse igale andmenõudele enne selle mis tahes moel töötlemist kõigepealt saatja mandaadi nõuetekohase kontrollimisega. 2. lisa joonisel 2 on kujutatud kõnealuse protseduuri skeemi. Keelatud seadmete nimekirja kantud seadmele vastatakse automaatse keeldumisega. Kui seade ei ole keelatud ega lubatud seadmete nimekirjas, saadetakse sellele PIN-koodi nõue, mille see peab täitma enne oma andmenõude uuesti saatmist.

4.4. **Sõnumivorming**

Kõigi ITSi seadme ja sõidukiseadme liidese vahel liikuvate sõnumite vormingustruktuur koosneb kolmest osast: sihtbaidist (TGT), lähtebaidist (SRC) ja pikkusbaidist (LEN) koosnev päis;

andmeväli, mis koosneb teenuse identifikaatorbaidist (SID) ja muutuvast hulgast andmebaitidest (maksimaalselt 255);

kontrollsummabait (CS) on sõnumi kõigi baitide, välja arvatud CS ise, rühmade summa ühebaidine moodul 256.

Sõnum peab olema jämedaotsaline (*Big Endian*).

Tabel 2

Üldine sõnumivorming

Päis			Andmeväli					Kontroll-summa
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 baiti			Max 255 baiti					1 bait

Päis

TGT ja SRC: sõnumi sihtseadme (TGT) ja lähteseadme (SRC) identifikaatorid. Sõidukiseadme vaikeidentifikaator on „EE“. Seda identifikaatorit ei saa muuta. ITSi seade kasutab sideseansi esimeses sõnumis vaikeidentifikaatorit „A0“. Seejärel annab sõidukiseadme liides ITSi seadmele kordumatu identifikaatori ning teeb selle ITSi seadmele teatavaks, et kasutada seda seansi järgmistes sõnumites.

LEN-baidis võetakse arvesse ainult andmevälja andmete (DATA) osa (vt tabel 2); välja neli esimest baiti on varjatud.

Sõnumi saatja autentsuse kinnitamiseks võrdleb sõidukiseadme liides oma identifikaatorite loendit (IDList) Bluetoothi andmetega, kontrollides, kas esitatud identifikaatoriga nimekirja kantud ITSi seade on hetkel Bluetoothi ühenduse levialas.

Andmeväli

Lisaks teenuse identifikaatorile (SID) sisaldab andmeväli ka muid parameetreid: nõude edastusparameeter (TRTP) ja loendurbaidid.

Kui edastamist vajavaid andmeid on rohkem, kui mahub ühte sõnumisse, jagatakse need mitmeks allsõnumiks. Igal allsõnumil on sama päis ja SID, kuid see sisaldab kahte loendurbaiti – jooksev loendur (*Counter Current*, CC) ja maksimumi loendur (*Counter Max*, CM) –, mis näitavad allsõnumi numbrit. Vigade kontrollimise ja edastuse abortimise võimaldamiseks saadab vastuvõttev seade iga allsõnumi kohta jaatussõnumi. Vastuvõttev seade võib allsõnumi aktsepteerida, nõuda selle uuesti saatmist, nõuda saatvalt seadmelt saatmise otsast alustamist või edastamise abortida.

Kui baite CC ja CM ei kasutata, antakse neile väärtus 0xFF.

Näiteks sõnum

HEADER	SID	TRTP	CC	CM	DATA	CS
3 baiti	Pikem kui 255 baiti					1 bait

edastatakse kujul:

HEADER	SID	TRTP	01	n	DATA	CS
3 baiti	255 baiti					1 bait

HEADER	SID	TRTP	02	n	DATA	CS
3 baiti	255 baiti					1 bait

…

HEADER	SID	TRTP	N	N	DATA	CS
3 baiti	Max 255 baiti					1 bait

Tabelis 3 on loetletud sõnumid, mida sõidukiseade ja ITSi seade peavad suutma vahetada. Iga parameetri sisu on esitatud kuueteistkümnendsüsteemis. Selguse huvides on tabelist välja jäänud baidid CC ja CM; vormingu täielik kirjeldus on esitatud eespool.

Tabel 3

Sõnumi üksikasjalik sisu

Sõnum	Päis			ANDMED			Kontroll-summa
	TGT	SRC	LEN	SID	TRTP	DATA	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Aeg	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		

Sõnum	Päis			ANDMED			Kontroll-summa
	TGT	SRC	LEN	SID	TRTP	DATA	
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Andmed	
DataUnavailable							
Andmed puuduvad	*ITSID*	EE	02	0A	TREP	10	
Isikuandmeid ei jagata	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Üldine keeldumine	*ITSID*	EE	02	0B	SID Req	10	
Teenusel puudub tugi	*ITSID*	EE	02	0B	SID Req	11	
Allfunktsioonil puudub tugi	*ITSID*	EE	02	0B	SID Req	12	
Sõnumi pikkus vale	*ITSID*	EE	02	0B	SID Req	13	
Tingimused pole õiged või nõudejada viga	*ITSID*	EE	02	0B	SID Req	22	
Nõue väljaspool ulatust	*ITSID*	EE	02	0B	SID Req	31	
Vastus ootel	*ITSID*	EE	02	0B	SID Req	78	
ITSID sobimatus	*ITSID*	EE	02	0B	SID Req	FC	
ITSID-d ei leitud	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Sõidukiseadme liides saadab selle sõnumi juhul, kui ta saab mis tahes andmenõude nii keelatud kui ka lubatud seadmete nimekirja kandmata ITSi seadmelt.

SendITSID (SID 02)

Sõidukiseadme liides saadab selle sõnumi alati, kui ta saab nõude mõnelt uuelt seadmelt. Uus seade peab kasutama vaikeidentifikaatorit „A0“, enne kui sõidukiseade annab sellele sideseansi ajal kasutatava kordumatu identifikaatori.

SendPIN (SID 03)

Selle sõnumiga taotleb ITSi seade sõidukiseadme liideselt lubatud seadmete nimekirja kandmist. Sõnumi sisuks on kood, mis koosneb neljast täisarvust 0 ja 9 vahel.

PairingResult (SID 04)

Selle sõnumiga teatab sõidukiseadme liides ITSi seadmele, kas saadetud PIN-kood oli õige. Sõnumi sisuks on kahendmuutuja (BOOLEAN), mille väärtus on „True“, kui PIN-kood oli õige, või muul juhul „False“.

SendPUC (SID 05)

Selle sõnumiga taotleb ITSi seade sõidukiseadme liideselt keelatud seadmete nimekirjast kustutamist. Sõnumi sisuks on kood, mis koosneb kaheksast täisarvust 0 ja 9 vahel.

BanLiftingResult (SID 06)

Selle sõnumiga teatab sõidukiseadme liides ITSi seadmele, kas saadetud PUK-kood oli õige. Sõnumi sisuks on kahendmuutuja (BOOLEAN), mille väärtus on „True“, kui PUK-kood oli õige, või muul juhul „False“.

RequestRejected (SID 07)

Selle sõnumiga vastab sõidukiseadme liides kõigile keelatud seadmete nimekirja kantud ITSi seadmelt saadud sõnumitele, välja arvatud sõnum „SendPUC“. Sõnum sisaldab teavet järelejäänud aja kohta, mille jooksul ITSi seade on veel keelatud seadmete nimekirjas, vastavalt 3. lisas määratletud jada „Time“ vormingule.

RequestData (SID 08)

Selle andmetele juurdepääsu nõudva sõnumi saadab ITSi seade. Ühebaidiline nõude edastusparameeter (TRTP) näitab, millist tüüpi andmeid küsitakse. Kasutatakse mitut andmetüüpi:

— standardTachData (TRTP 01): sõidumeerikust saadaolevad andmed, mis ei kuulu isikuandmete kategooriasse;

— personalTachData (TRTP 02): sõidumeerikust saadaolevad andmed, mis kuuluvad isikuandmete kategooriasse;

— gnssData (TRTP 03): GNSSi andmed, alati isikuandmete kategoorias;

— standardEventData (TRTP 04): registreeritud sündmuste andmed, mis ei kuulu isikuandmete kategooriasse;

— personalEventData (TRTP 05): registreeritud sündmuste andmed, mis kuuluvad isikuandmete kategooriasse;

— standardFaultData (TRTP 06): registreeritud vead, mis ei kuulu isikuandmete kategooriasse;

— manufacturerData (TRTP 07): tootja avaldatud andmed.

Lisateave iga andmetüübi sisu kohta on esitatud käesoleva liite 3. lisas.

Lisateave GNSSi andmete vormingu ja sisu kohta on esitatud käesoleva liite 12. lisas.

Lisateave sündmuste ja vigade andmekoodide kohta on esitatud lisades IB ja IC.

ResquestAccepted (SID 09)

Selle sõnumiga kinnitab sõidukiseadme liides ITSi seadme andmenõudega „RequestData“ nõustumist. Sõnumi sisuks on ühebaidine parameeter TREP, mis kattub vastava nõudesõnumi „RequestData“ TRTP-baidiga, ning kõik nõutud tüüpi andmed.

DataUnavailable (SID 0A)

Sõidukiseadme liides saadab selle sõnumi juhul, kui mingil põhjusel ei ole võimalik nõutud andmeid lubatud seadmete nimekirjas olevale ITSi seadmele saata. Sõnumi sisuks on ühebaidine parameeter TREP, mis kattub andmenõude parameetriga TRTP, ning tabelile 3 vastav ühebaidine veakood. Võimalik on kasutada järgmisi koode:

— andmed puuduvad (10): sõidukiseadme liides ei pääse mingil põhjusel sõidukiseadme andmetele ligi;

— isikuandmeid ei jagata (11): ITSi seade püüab saada isikuandmeid olukorras, kus nende jagamiseks ei ole luba.

NegativeAnswer (SID 0B)

Sõidukiseadme liides saadab selle tüübi alla kuuluva sõnumi juhul, kui nõuet ei saa täita mõnel muul põhjusel peale andmete puudumise. Reeglina on need sõnumid tingitud nõude vigasest vormingust (pikkus, SID, ITSID jne), aga on ka muid põhjusi. Andmevälja parameeter TRTP sisaldab nõude identifikaatorit SID. Andmeväli sisaldab koodi, mis näitab eitava vastuse põhjust. Kasutada saab järgmisi koode.

— Üldine keeldumine (kood: 10)

— Toimingut ei saa teha põhjusel, mida ei ole nimetatud allpool ega punktis (sisestada punkti *DataUnavailable* number).

— Teenusel puudub tugi (kood: 11)

— Nõudes sisalduv SID on arusaamatu.

— Allfunktsioonil puudub tugi (kood: 12)

— Nõudes sisalduv TRTP on arusaamatu. Näiteks see puudub või ei ole vastuvõetavas väärtustevahemikus.

— Sõnumi pikkus vale (kood: 13)

— Saadud sõnum on vale pikkusega (LEN-baidi väärtus ei lange kokku sõnumi tegeliku pikkusega).

— Tingimused pole õiged või nõudejada viga (kood: 22)

— Nõutav teenus ei ole aktiivne või nõudesõnumi jada ei ole korrektne.

— Nõue väljaspool ulatust (kood: 33)

— Nõude kirjeparameeter (andmeväli) ei ole kehtiv.

— Vastus ootel (kood: 78)

— Nõutud toimingut ei ole võimalik õigeaegselt teha ja sõidukiseade ei ole valmis uut nõuet vastu võtma.

— *ITSID* sobimatus (kood: FB)

— Bluetoothi andmetega võrdlemisel selgub, et lähtebaidi (SRC) identifikaator *ITSID* ei vasta seotud seadmele.

— *ITSID*-d ei leitud (kood: FC)

— Lähtebaidi (SRC) identifikaator *ITSID* ei ole seotud ühegi seadmega.

3. lisas esitatud ASN.1 koodi ridadel 1–72 (**FormatMessageModule**) on kirjeldatud tabelis 3 esitatud sõnumite vormingut. Allpool on esitatud rohkem teavet sõnumite sisu kohta.

4.5. **Juhi nõusolek**

Kõik saadaolevad andmed liigitatakse standardsete või isikuandmete kategooriasse. Juurdepääs isikuandmetele lubatakse üksnes juhul, kui juht on andnud nõusoleku, et tema sõidumeerikus olevad isikuandmed võivad väljuda sõiduki võrgust kolmandate isikute rakendustes kasutamiseks.

Juhi nõusolek antakse siis, kui sõidukiseadme jaoks tundmatu juhikaardi või töökojakaardi esmakordsel sisestamisel küsitakse kaardi omanikult nõusolekut sõidumeerikuga seotud isikuandmete edastamiseks valikulise ITSi liidese kaudu (vt ka IC lisa punkt 3.6.2).

Nõusoleku staatus (lubatud/keelatud) salvestatakse sõidumeeriku mälus.

Mitme juhi korral jagatakse ITSi liidese kaudu ainult nende juhtide isikuandmeid, kes on oma nõusoleku andnud. Näiteks kui sõidukis on kaks juhti ja ainult esimene juht nõustus oma isikuandmete jagamisega, siis teise juhi isikuandmeid välja ei saadeta.

4.6. **Standardandmete väljavõtmine**

2. lisa joonisel 3 on skeemina kujutatud, kuidas töödeldakse ITSi seadme saadetud nõuet standardandmete saamiseks. Kui ITSi seade on nõuetekohaselt lubatud seadmete nimekirja kantud ja ei nõua isikuandmeid, siis ei ole vaja mingeid täiendavaid kontrolle. Skeemil eeldatakse, et 2. lisa joonisel 2 kujutatud volitamistoiming on nõuetekohaselt teostatud. Skeemi võib paigutada joonisel 2 kujutatud halli lahtri *REQUEST TREATMENT* kohale.

Järgmised saadaolevad andmed kuuluvad standardandmete kategooriasse:

— standardTachData (TRTP 01),

— StandardEventData (TRTP 04),

— standardFaultData (TRTP 06).

4.7. **Isikuandmete väljavõtmine**

2. lisa joonisel 4 on kujutatud isikuandmete nõude töötlemise skeemi. Nagu eespool öeldud, saadab sõidukiseadme liides isikuandmeid välja üksnes juhul, kui juht on selleks otseselt nõusoleku andnud (vt ka punkt 4.5). Vastasel korral tuleb nõue automaatselt tagasi lükata.

Järgmised saadaolevad andmed kuuluvad isikuandmete kategooriasse:

— personalTachData (TRTP 02),

— gnssData (TRTP 03),

— personalEventData (TRTP 05),

— manufacturerData (TRTP 07).

4.8. **Sündmuste ja vigade andmete väljavõtmine**

ITSi seadmetel peab olema võimalus nõuda sündmuste andmeid, mille sisuks on kõigi ootamatute sündmuste nimekiri. Need andmed kuuluvad standard- või isikuandmete kategooriasse, vt 3. lisa. Iga sündmuse sisu vastab käesoleva liite 1. lisas osutatud dokumenteerimisnõuetele.

1. LISA

ITSi LIIDESE KAUDU KÄTTESAADAVATE ANDMETE NIMEKIRI

Data	Source	Data classification (personal/ not personal)
VehicleIdentificationNumber	Vehicle Unit	**not personal**
CalibrationDate	Vehicle Unit	**not personal**
TachographVehicleSpeed speed instant t	Vehicle Unit	personal
Driver1WorkingState Selector driver	Vehicle Unit	personal
Driver2WorkingState	Vehicle Unit	personal
DriveRecognize Speed Threshold detected	Vehicle Unit	**not personal**
Driver1TimeRelatedStates Weekly day time	Driver Card	personal
Driver2TimeRelatedStates	Driver Card	personal
DriverCardDriver1	Vehicle Unit	**not personal**
DriverCardDriver2	Vehicle Unit	**not personal**
OverSpeed	Vehicle Unit	personal
TimeDate	Vehicle Unit	**not personal**
HighResolutionTotalVehicleDistance	Vehicle Unit	**not personal**
ServiceComponentIdentification	Vehicle Unit	**not personal**
ServiceDelayCalendarTimeBased	Vehicle Unit	**not personal**
Driver1Identification	Driver Card	personal
Driver2Identification	Driver Card	personal
NextCalibrationDate	Vehicle Unit	**not personal**
Driver1ContinuousDrivingTime	Driver Card	personal
Driver2ContinuousDrivingTime	Driver Card	personal
Driver1CumulativeBreakTime	Driver Card	personal
Driver2CumulativeBreakTime	Driver Card	personal
Driver1CurrentDurationOfSelectedActivity	Driver Card	personal
Driver2CurrentDurationOfSelectedActivity	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
SpeedAuthorised	Vehicle Unit	**not personal**
TachographCardSlot1	Driver Card	**not personal**
TachographCardSlot2	Driver Card	**not personal**
Driver1Name	Driver Card	personal
Driver2Name	Driver Card	personal
OutOfScopeCondition	Vehicle Unit	**not personal**
ModeOfOperation	Vehicle Unit	**not personal**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
EngineSpeed	Vehicle Unit	personal
RegisteringMemberState	Vehicle Unit	**not personal**
VehicleRegistrationNumber	Vehicle Unit	**not personal**
Driver1EndOfLastDailyRestPeriod	Driver Card	personal
Driver2EndOfLastDailyRestPeriod	Driver Card	personal
Driver1EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver1EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver1CurrentDailyDrivingTime	Driver Card	personal
Driver2CurrentDailyDrivingTime	Driver Card	personal
Driver1CurrentWeeklyDrivingTime	Driver Card	personal
Driver2CurrentWeeklyDrivingTime	Driver Card	personal
Driver1TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver1CardExpiryDate	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
Driver2CardExpiryDate	Driver Card	personal
Driver1CardNextMandatoryDownloadDate	Driver Card	personal
Driver2CardNextMandatoryDownloadDate	Driver Card	personal
TachographNextMandatoryDownloadDate	Vehicle Unit	**not personal**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Driver Card	personal
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Driver Card	personal
Driver1CumulativeUninterruptedRestTime	Driver Card	personal
Driver2CumulativeUninterruptedRestTime	Driver Card	personal
Driver1MinimumDailyRest	Driver Card	personal
Driver2MinimumDailyRest	Driver Card	personal
Driver1MinimumWeeklyRest	Driver Card	personal
Driver2MinimumWeeklyRest	Driver Card	personal
Driver1MaximumDailyPeriod	Driver Card	personal
Driver2MaximumDailyPeriod	Driver Card	personal
Driver1MaximumDailyDrivingTime	Driver Card	personal
Driver2MaximumDailyDrivingTime	Driver Card	personal
Driver1NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver2NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver1RemainingCurrentDrivingTime	Driver Card	personal
Driver2RemainingCurrentDrivingTime	Driver Card	personal
GNSS position	Vehicle Unit	personal

2) JUHI NÕUSOLEKU JÄREL PIDEVALT SAADAOLEVAD GNSSi ANDMED

Vt 12. liide „GNSS“.

3) ILMA JUHI NÕUSOLEKUTA SAADAOLEVAD SÜNDMUSEANDMED

Sündmus	Salvestusreegel	Sündmuse kohta registreeritavad andmed
Kehtetu kaardi sisestamine	— 10 viimast sündmust	— sündmuse kuupäev ja kellaaeg, — sündmuse tekitanud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Kaardikonflikt	— 10 viimast sündmust	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — kummagi konflikti tekitanud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond
Viimane kaardiseanss nõuetekohaselt sulgemata	— 10 viimast sündmust	— kaardi sisestamise kuupäev ja kellaaeg, — kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — kaardilt loetud andmed viimase seansi kohta: — kaardi sisestamise kuupäev ja kellaaeg, — sõiduki registreerimisnumber, registreerinud liikmesriik ja sõidukiseadme põlvkond
Voolukatkestus (2)	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Kaugsideseadmega side pidamise viga	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
GNSSi vastuvõtja asukohateabe puudumine	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Liikumisandmete viga	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval

Sündmus	Salvestusreegel	Sündmuse kohta registreeritavad andmed
Vastuolu sõiduki liikumisandmetes	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Turvalisuse rikkumise katse	10 viimast sündmust iga sündmuse tüübi kohta.	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg vajaduse korral, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — sündmuse tüüp
Ajakonflikt	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sõidumeeriku kuupäev ja kellaaeg, — GNSSi kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval

4) JUHI NÕUSOLEKUL SAADAOLEVAD SÜNDMUSEANDMED

Sündmus	Salvestusreegel	Sündmuse kohta registreeritavad andmed
Vajaliku kaardita juhtimine	— pikim sündmus iga kümne viimase päeva kohta, mil sündmus toimus, — viis kõige pikemat sündmust viimase 365 päeva jooksul	— sündmuse alguse kuupäev ja kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
Kaardi sisestamine juhtimise ajal	— viimane sündmus iga kümne viimase päeva kohta, mil sündmus toimus	— sündmuse kuupäev ja kellaaeg, — kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond, — samasuguste sündmuste arv sellel päeval
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 kellaaeg, — sündmuse lõpu kuupäev ja kellaaeg, — sündmuse ajal mõõdetud suurim kiirus, — sündmuse ajal mõõdetud kiiruste aritmeetiline keskmine, — juhikaardi tüüp, number, väljaandnud liikmesriik ja põlvkond (vajaduse korral), — samasuguste sündmuste arv sellel päeval

5) ILMA JUHI NÕUSOLEKUTA SAADAOLEVAD VEAANDMED

Viga	Salvestusreegel	Vea kohta registreeritavad andmed
Kaardi viga	— 10 viimast juhikaardi viga	— vea alguse kuupäev ja kellaaeg, — vea lõpu kuupäev ja kellaaeg, — kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond,
Sõidumeeriku vead	— 10 viimast viga iga veatüübi kohta, — esimene viga pärast viimast kalibreerimist	— vea alguse kuupäev ja kellaaeg, — vea lõpu kuupäev ja kellaaeg, — vea tüüp, — sündmuse alguses ja/või lõpus sisestatud kaardi tüüp, number, väljaandnud liikmesriik ja põlvkond

Viga käivitub iga järgneva tõrke puhul, välja arvatud kalibreerimisrežiimis:

— sõidukiseadme sisetõrge,

— printeri tõrge,

— kuvari tõrge,

— allalaadimise tõrge,

— anduri tõrge,

— GNSSi vastuvõtja või GNSSi välisseadme tõrge,

— kaugsideseadme tõrge.

6) JUHI NÕUSOLEKUT MITTEVAJAVAD TOOTJAOMASED SÜNDMUSED JA VEAD

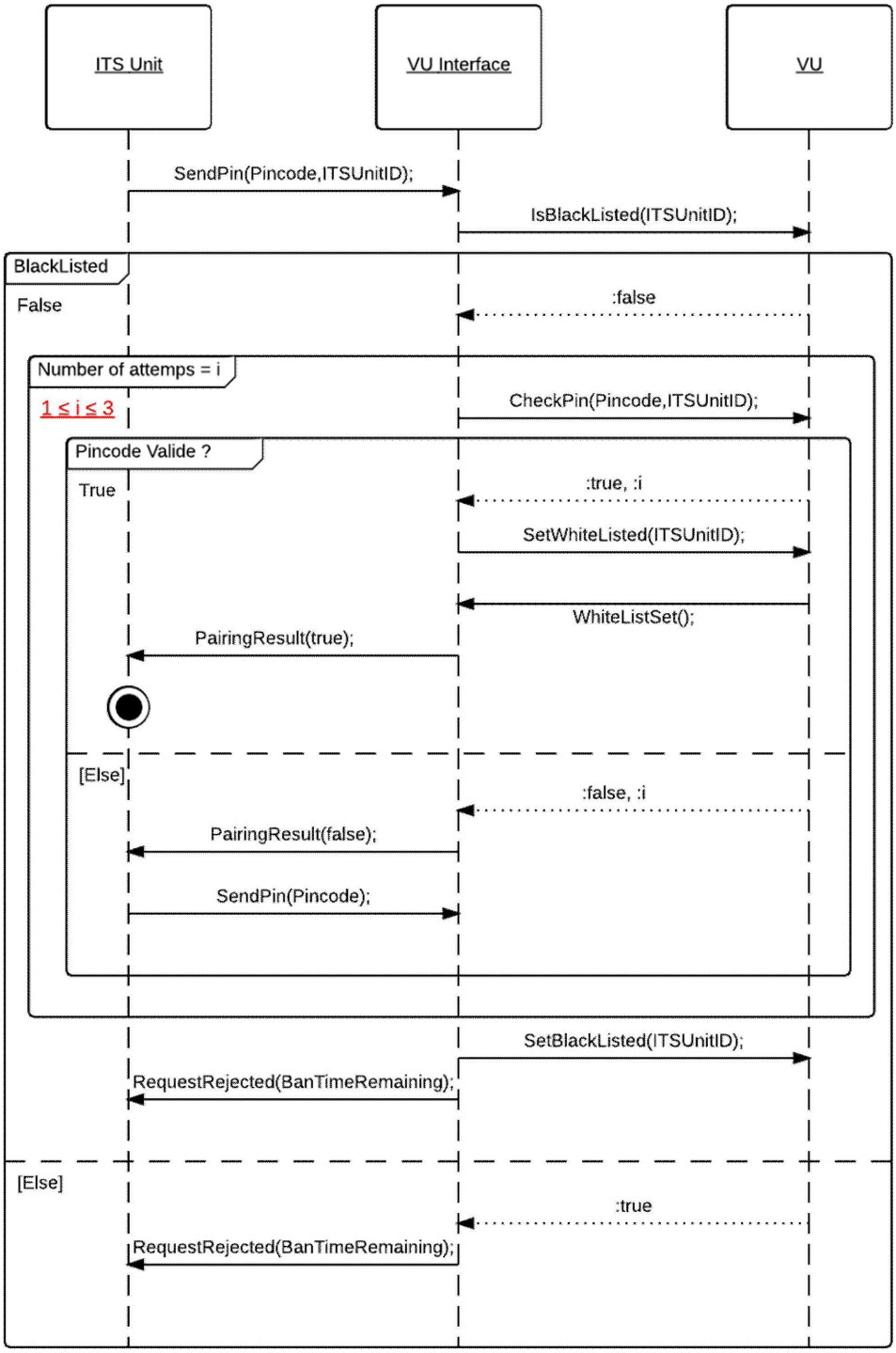
Sündmus või rike	Salvestusreegel	Sündmuse kohta registreeritavad andmed
Vastavalt tootja määratlusele	Vastavalt tootja määratlusele	Vastavalt tootja määratlusele

2. LISA

ITSi SEADMES TOIMUVA SÕNUMIVAHETUSE JÄRGNEVUSSKEEMID

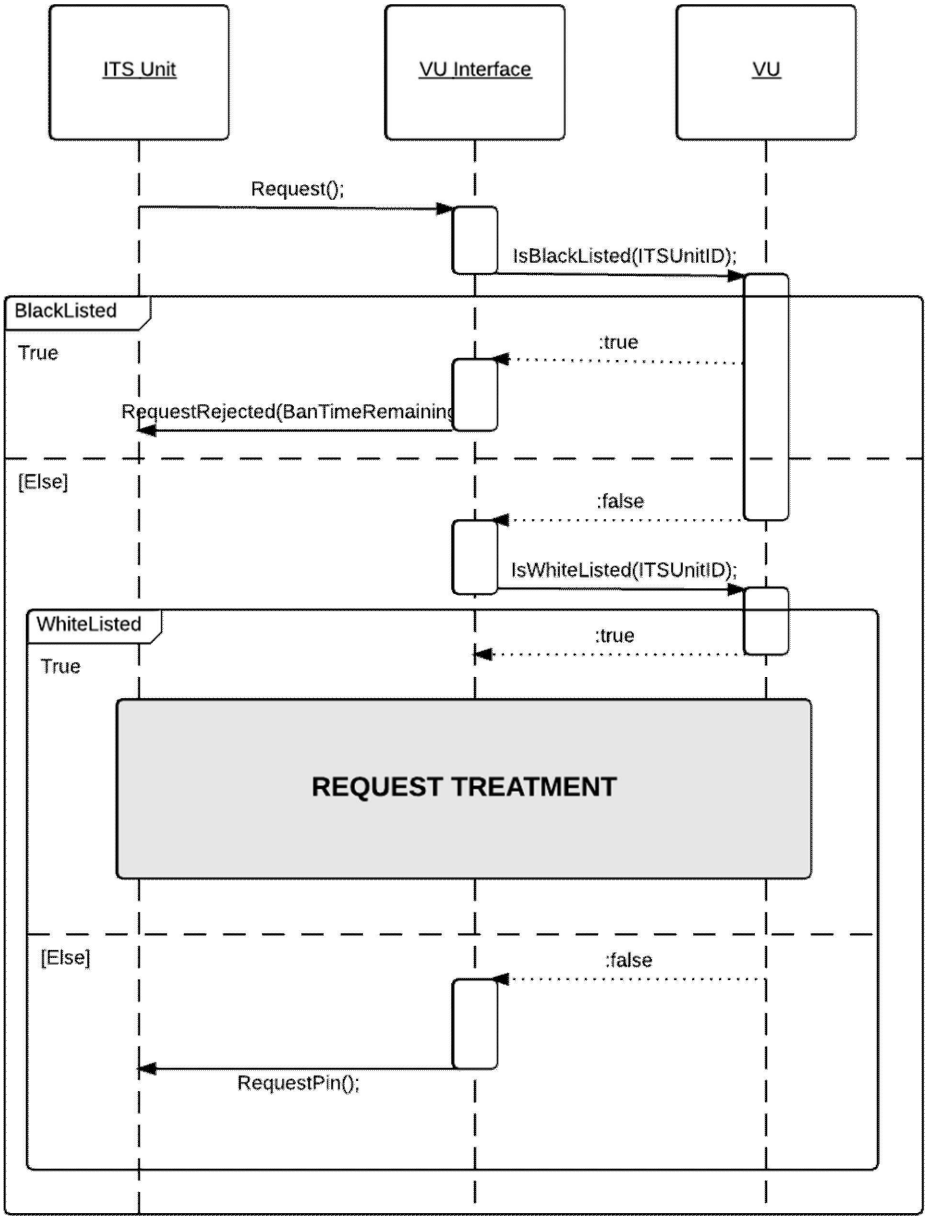
Joonis 1

PIN-koodi tõendamiskatse järgnevusskeem



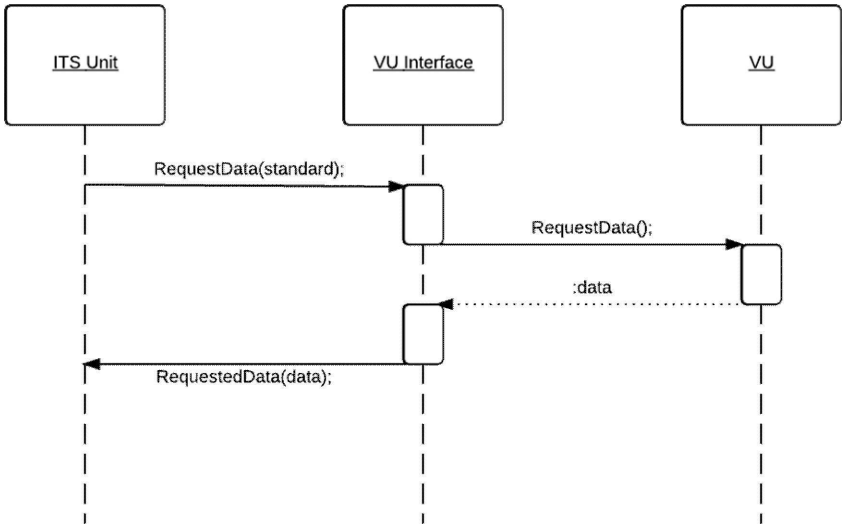
Joonis 2

ITSi seadme volituste kontrollimise järgnevusskeem



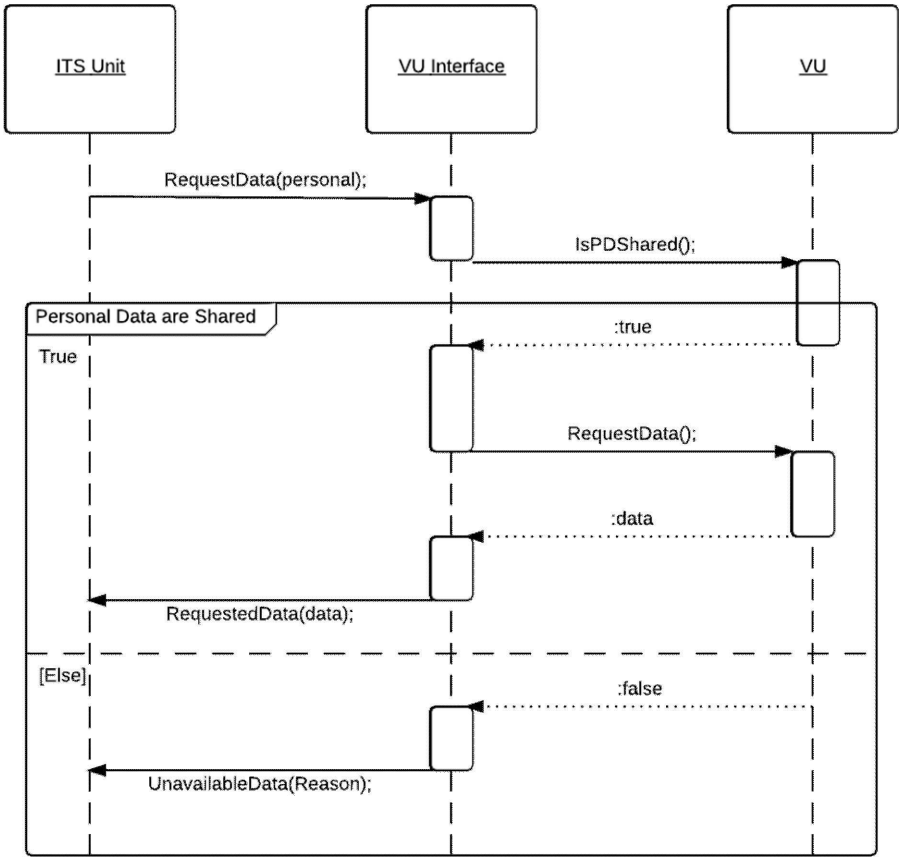
Joonis 3

Isikuandmete alla mittekuuluvate andmete nõude (pärast õige PIN-koodi esitamist) töötlemise järgnevusskeem



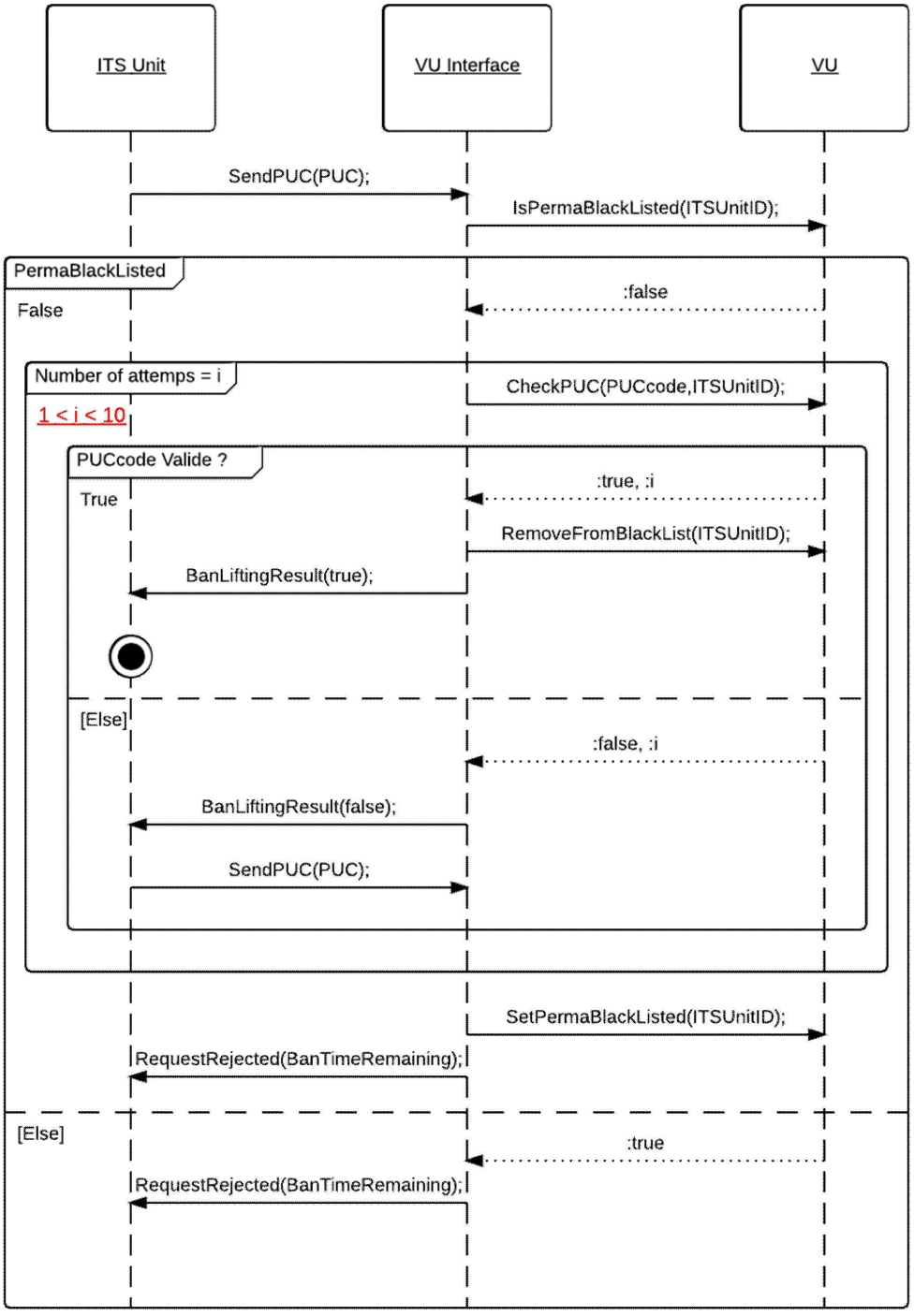
Joonis 4

Isikuandmete alla kuuluvate andmete nõude (pärast õige PIN-koodi esitamist) töötlemise järgnevusskeem



Joonis 5

PUK-koodi tõendamiskatse järgnevusskeem



3. LISA

ASN.1 SPETSIFIKAAT

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

      CompleteMessage ::=SEQUENCE{
            header Header,
            data DataField,
            checksum Checksum
      }

      ----------------
      --HEADER TYPES--
      ----------------


      Header::=SEQUENCE{
            tgt IDList,
            src IDList,
            len BIT STRING (1..255)
      }

      vuID BIT STRING ::= 'EE'H
      IDList ::=CHOICE{
            vu BIT STRING (vuID),
            itsUnits SEQUENCE OF BIT STRING,
                  --Default hex Value:A0, redefined after first message exchange--
                  --Each ID will be linked to the Bluetooth ID of the device--
            ...
      }

      --------------------
      --DATAFIELDS TYPES--
      --------------------
      DataField ::=SEQUENCE{
            sid BIT STRING,
            trtp BIT STRING,
            subMBytes SubMessageBytes,
            dataField Content,
            ...
      }

      SubMessageBytes ::= SEQUENCE{
            currentSubM BIT STRING,
            totalSubM BIT STRING
      }

      Content ::= CHOICE{
            requestPIN RequestPIN,
            sendITSID SendITSID,
            sendPin SendPIN,
```

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

	----------
	---Utils--
	----------

	PUC ::= SEQUENCE (SIZE(8)) OF
	INTEGER (SIZE(0..9))

	PIN ::=	SEQUENCE (SIZE(4)) OF
		INTEGER (SIZE(0..9))

	--------------------------
	--Messages From ITS Unit--
	--------------------------

	SendPIN {PIN:pin} ::= SEQUENCE {
		sid BIT STRING ('03'H),
		pin PIN (pin)
	}

	SendPUC {PUC:puc} ::= SEQUENCE {
		sid BIT STRING ('05'H),
		puc PUC (puc)
	}
	--------------------
	--Messages From VU--
	--------------------

	PairingResult ::= SEQUENCE{
		sid BIT STRING ('04'H),
		result BOOLEAN
	}

	RequestPIN {MType:receivedRequest}::= SEQUENCE{
		sid BIT STRING ('01'H)
	}

	RequestRejected ::= SEQUENCE{
		sid BIT STRING ('07'H),
		banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

	BanLiftingResult ::= SEQUENCE{
		sid BIT STRING ('06'H),
		result BOOLEAN
	}
END
```

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	----------------------------
	--Complete Tachograph Data--
	----------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document–

```

```
Time ::= SEQUENCE{
	seconds INTEGER (0..59.75), --increment: 0.25s--
	minutes INTEGER (0..59), --increment: 1min--
	hours INTEGER (0..23), --increment: 1h--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	month INTEGER (1..12), --increment: 1month--
	year INTEGER (1985..2235), --increment: 1year--
	locMinOffset INTEGER (-59..59), --increment: 1min--
	locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
	month INTEGER (1..12), --increment: 1month--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
	codePageSurname UTF8String, --See ISO/IEC 8859--
	surname UTF8String,
	codePageFirstname UTF8String, --See ISO/IEC 8859--
	firstname UTF8String,
}

--------------------
--Message Content--
--------------------

StandardTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardTachData),
	personal BOOLEAN (FALSE),
	data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalTachData),
	personal BOOLEAN (TRUE),
	data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&gnssData),
	personal BOOLEAN (TRUE),
	data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardEventData),
	personal BOOLEAN (FALSE),
	data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalEventData),
	personal BOOLEAN (TRUE),
	data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

```
243                 trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                 personal BOOLEAN (FALSE),
245                 data StandardFault
246           }
247
248           ManufacturerDataContent ::= SEQUENCE{
249                 trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                 personal BOOLEAN (TRUE),
251                 ...
252           }
253
254           ---------------
255           --DATA SHEETS--
256           ---------------
257
258           --Data sheet format follows ISO 16844-7.--
259           StandardTachyDataSheet ::= SEQUENCE{
260                 vin UTF8String (SIZE(17)),
261                 calibrationDate Date,
262                 driveRecognize INTEGER (2 UNION 12),
263                 driverCardDriver1 INTEGER (2 UNION 12),
264                 driverCardDriver2 INTEGER (2 UNION 12),
265                 timeDate Time,
266                 highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267     5m--
268                 serviceComponentIdentification INTEGER (0..255),
269                 serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270     -
271                 nextCalibrationDate Date,
272                 speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                 tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                 tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                 outOfScopeCondition INTEGER(2 UNION 12),
276                 modeOfOperation INTEGER (0..4...), --Maximum 250--
277                 registeringMemberState UTF8String,
278           vehicleRegistrationNumber SEQUENCE {
279                       codePageVRN INTEGER (0..255),
280                       vrn OCTET STRING (SIZE(13)),
281                 },
282                 tachographNextMandatoryDownloadDate Date,
283                 ...
284           }
285
286           PersonalTachyDataSheet ::= SEQUENCE{
287                 tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                 driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289     UNION 1012...),
290                 driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291     UNION 1012...),
292
293                 driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294     1002 UNION
295                                                   1012 UNION 1102 UNION 1112 UNION
296     10002 UNION 10012 UNION
297                                                   10102 UNION 10112 UNION 11002 UNION
298     11012...),
299                 driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300     1002 UNION
```

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

             overSpeed INTEGER (2 UNION 12),
             driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver1Name DriverName,
             driver2Name DriverName,
             driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
             driver1EndOfLastDailyRestPeriod Time,
             driver2EndOfLastDailyRestPeriod Time,
             driver1EndOfLastWeeklyRestPeriod Time,
             driver2EndOfLastWeeklyRestPeriod Time,
             driver1EndOfSecondLastWeeklyRestPeriod Time,
             driver2EndOfSecondLastWeeklyRestPeriod Time,
             driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1CardExpiryDate Date,
             driver2CardExpiryDate Date,
             driver1CardNextMandatoryDownloadDate Date,
             driver2CardNextMandatoryDownloadDate Date,
             driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
             driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
             driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367   1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369   1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385   END
386
387   EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390   about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408   CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410   AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

```
PersonalEvent ::= CHOICE{
	lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
	cardInsertionWhileDriving CardInsertionWhileDriving,
	overSpeeding OverSpeeding,
	...
}

StandardFault ::= CHOICE{
	cardFault CardFault,
	recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
	date GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
```

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

```
		numberOfSimilarEvent INTEGER
	}

	PositionDataError ::= SEQUENCE{
		beginDate GeneralizedTime,
		endDate GeneralizedTime,
		carsdType SEQUENCE OF UTF8String,
		cardsNumber SEQUENCE OF INTEGER,
		issuingMemberState SEQUENCE OF NationAlpha,
		cardsGeneration SEQUENCE OF INTEGER,
		numberOfSimilarEvent INTEGER
	}

	MotionDataError ::= SEQUENCE{
		beginDate GeneralizedTime,
		endDate GeneralizedTime,
		carsdType SEQUENCE OF UTF8String,
		cardsNumber SEQUENCE OF INTEGER,
		issuingMemberState SEQUENCE OF NationAlpha,
		cardsGeneration SEQUENCE OF INTEGER,
		numberOfSimilarEvent INTEGER
	}

	VehicleMotionConflict ::= SEQUENCE{
		beginDate GeneralizedTime,
		endDate GeneralizedTime,
		carsdType SEQUENCE OF UTF8String,
		cardsNumber SEQUENCE OF INTEGER,
		issuingMemberState SEQUENCE OF NationAlpha,
		cardsGeneration SEQUENCE OF INTEGER,
		numberOfSimilarEvent INTEGER
	}

	SecurityBreachAttempt ::= SEQUENCE{
		beginDate GeneralizedTime,
		endDate GeneralizedTime OPTIONAL,
		carsdType SEQUENCE OF UTF8String,
		cardsNumber SEQUENCE OF INTEGER,
		issuingMemberState SEQUENCE OF NationAlpha,
		numberOfSimilarEvent INTEGER,
		typeOfEvent SecurityBreachEvent
	}


	TimeConflict ::= SEQUENCE{
		beginDate GeneralizedTime,
		endDate GeneralizedTime,
		carsdType SEQUENCE OF UTF8String,
		cardsNumber SEQUENCE OF INTEGER,
		issuingMemberState SEQUENCE OF NationAlpha,
		cardsGeneration SEQUENCE OF INTEGER,
		numberOfSimilarEvent INTEGER
	}

	---------------
	--FAULTS LIST--
	---------------

	CardFault ::= SEQUENCE{
```

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

14. liide

KAUGSIDEFUNKTSIOON

SISUKORD

1. SISSEJUHATUS

Käesolevas liites kirjeldatakse kaugsidefunktsiooni lahendust ja selle kasutamise korda vastavalt määruse (EL) nr 165/2014 (edaspidi „määrus“) artikli 9 nõuetele.

DSC_1 Määruses (EL) nr 165/2014 nõutakse, et sõidumeerikul peab olema kaugsidefunktsioon, mis võimaldab pädevate kontrolliasutuste esindajatel lugeda mööduvatest sõidukitest sõidumeerikuinfot kaugpäringuseadme (varajase avastamise kaugsidelugeja (REDCR)) abil, täpsemalt päringuseadme abil, mis kasutab juhtmevaba ühenduse loomiseks CENi 5,8 GHz sihtotstarbelise lähitoimeside (DSRC) liideseid.

Oluline on mõista, et nimetatud funktsiooni eesmärk on toimida üksnes eelfiltrina, mis võimaldab valida sõidukeid põhjalikumaks kontrolliks, ning see ei asenda määrusega (EL) nr 165/2014 sätestatud ametlikku kontrolliprotsessi. Vt kõnealuse määruse põhjendust 9, milles öeldakse, et kaugside sõidumeerikute ja kontrolliasutuste vahel teeäärsete kontrollide eesmärgil lihtsustab sihipäraseid teeäärseid kontrolle.

DSC_2 Andmete vahetamiseks kasutatakse andmesidet, milleks on käesoleva liitega kooskõlas olev 5,8 GHz juhtmeta DSRC-sidesüsteem, mida on kontrollitud vastavalt asjakohastele parameetritele, mis on sätestatud standardis EN 300 674-1 *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)* („Elektromagnetilise ühilduvuse ja raadiospektri küsimused (ERM). Maanteetranspordi ja liikluse telemaatika (RTTT). Tööstus-, teadus- ja meditsiinirakenduste (TTM) sagedusalas raadiosagedusel 5,8 GHz töötavad sihtotstarbelise lähitoimeside (DSRC) edastusseadmed (500 kbit/s / 250 kbit/s). Osa 1: Teeäärsete seadmete (RSU) ja sõidukisiseste seadmete (OBU) üldised omadused ja katsemeetodid“).

DSC_3 Andmeside luuakse sidevahenditega üksnes juhul, kui pädeva kontrolliasutuse seade seda nõuetele vastavate raadioside vahenditega (varajase avastamise kaugsidelugeja, REDCR) nõuab.

DSC_4 Andmed turvatakse nende tervikluse tagamiseks.

DSC_5 Edastatud andmetele on juurdepääs vaid määruse (EÜ) nr 561/2006 ja määruse (EL) nr 165/2014 rikkumisi kontrollima volitatud kontrolliasutustel ning töökodadel, kui see on vajalik sõidumeerikute nõuetekohase toimimise kontrollimiseks.

DSC_6 Andmeside ajal vahetatavad andmed on piiratud andmetega, mis on vajalikud sihipäraste teeäärsete kontrollide tegemiseks sõidumeeriku manipuleerimise või väärkasutuse kahtlusega sõidukite puhul.

DSC_7 Andmete terviklus ja turvalisus saavutatakse sõidukiseadmes (VU) olevate andmete turvamisega ning sellega, et juhtmeta 5,8 GHz DSRC-kaugside vahendusel edastatakse ainult turvatud andmeid ja turbega seotud andmeid (vt punkt 5.4.4), mis tähendab, et andmeside kaudu edastatud andmete mõistmiseks ja nende autentsuse kontrollimiseks vajalikud vahendid on ainult pädevate kontrolliasutuste volitatud isikutel. Vt 11. liide „Ühised turbemehhanismid".

DSC_8 Andmed sisaldavad nende viimase ajakohastamise aega näitavat ajatemplit.

DSC_9 Turbeandmete sisu teavad ja käsutavad üksnes pädevad kontrolliasutused ja isikud, kellele kontrolliasutused kõnealuse teabe avaldavad, ning see ei kuulu käesolevas liites käsitletud andmeside alla, välja arvatud juhul, kui andmesides tuleb koos iga sisuandmete paketiga saata ka turbeandmete pakett.

DSC_10 Sama ülesehituse ja seadmetega peab olema võimalik saada ka muud liiki andmeid (nt sõidukisisese kaalumise andmed), millel puhul on kasutusel siin kirjeldatud ülesehitus.

DSC_11 Selgituseks lisatakse, et vastavalt määruse (EL) nr 165/2014 nõuetele (artikkel 7) ei edastata andmeside kaudu juhi isikut käsitlevaid andmeid.

2. REGULEERIMISALA

Käesolevas liites reguleeritakse seda, kuidas pädevate kontrolliasutuste esindajad kasutavad spetsifikaadile vastavat 5,8 GHz juhtmeta DSRC-andmesidet, et saada huvi pakkuvast sõidukist kaugside teel andmeid (edaspidi „andmed"), mis võimaldavad kindlaks teha, et huvi pakkuva sõiduki puhul võib esineda määruse (EL) nr 165/2014 nõuete rikkumine, ning kaaluda selle peatamist täiendava kontrolli eesmärgil.

Määruses (EL) nr 165/2014 nõutakse, et kogutavad andmed peavad piirduma ainult selliste andmetega, mis võimaldavad kindlaks teha võimaliku rikkumise vastavalt määruse (EL) nr 165/2014 artiklis 9 esitatud määratlusele, või käsitlema selliseid andmeid.

Kõnealusel juhul on andmesideks kasutatav aeg piiratud, sest andmeside on sihtotstarbeline ja lähitoimeline. Pädevad kontrolliasutused võivad sõidumeerikute kaugseireks (*remote tachograph monitoring*, RTM) kasutatavaid sidevahendeid kasutada lisaks ka muul eesmärgil (näiteks direktiivis (EL) 2015/719 määratletud raskeveokite suurima massi ja maksimaalmõõtmete kontrollimine) ning sellised toimingud võidakse pädeva kontrolliasutuse äranägemisel teha eraldi või üksteise järel.

Käesolevas liites on määratletud:

— andmesides kasutatavad sideseadmed, protseduurid ja protokollid;

— standardid ja määrused, millele raadioseadmed peavad vastama;

— andmete sideseadmetele esitamise viis;

— päringu- ja allalaadimisprotseduurid ning toimingute järjekord;

— edastatavad andmed;

— andmeside kaudu edastatud andmete võimalik tõlgendamine;

— nõuded andmesidega seotud turbeandmetele;

— andmete kättesaadavus pädevatele kontrolliasutustele;

— kuidas varajase avastamise kaugsidelugeja saab nõuda erinevaid andmeid lasti ja sõidukipargi kohta.

Selgituseks lisatakse, et käesolevas liites ei ole määratletud järgmised aspektid:

— andmete kogumine ja haldamine sõidukiseadmes (kui see ei ole määratletud määruse (EL) nr 165/2014 muudes osades, siis lahendatakse see tootedisaini käigus);

— kogutud andmete pädeva kontrolliasutuse esindajale esitamise vorm ning kriteeriumid, mille alusel pädevad kontrolliasutused valivad välja peatatavad sõidukid (kui see ei ole määratletud määruse (EL) nr 165/2014 muudes osades ega pädeva kontrolliasutuse poliitilise otsusega, siis lahendatakse see tootedisaini käigus). Selgituseks: andmeside teeb andmed pädevale kontrolliasutusele üksnes kättesaadavaks, et asutus saaks teha teadlikke otsuseid;

— andmete sisuga seotud andmeturbe nõuded (näiteks krüpteerimine) (neid kirjeldatakse määruse 11. liites „Ühised turbemehhanismid“);

— sama ülesehitusega ja samade seadmetega kogutavate RTM-andmetest erinevat liiki andmete üksikasjad;

— sõidukiseadmete ning sõiduki lähitoimesideseadmete toimingute ja haldamise üksikasjad ning sõiduki kaugsideseadme sisemised toimingud (peale REDCR-i nõudel andmete edastamise).

3. LÜHENDID, MÕISTED JA MÄRKUSED

Käesolevas liites kasutatakse järgmisi lühendeid ja mõisted:

antenn	koos raadiosaatja või raadiovastuvõtjaga kasutatav elektriseade, mis muundab elektrienergia raadiolaineteks ja vastupidi. Raadiosaatja saadab raadiosagedusel võnkuva elektrivoolu antenni kontaktidele ning antenn kiirgab voolust saadud energiat elektromagnetlainetena (raadiolained). Vastuvõtmisel püüab antenn kinni osa elektromagnetlaine energiast, et tekitada oma kontaktidel nõrk pinge, mis edastatakse võimendamiseks vastuvõtjasse;
andmeside	andmete saamise eesmärgil toimuv 5. peatüki kohane teabe/andmete vahetamine ülem-alluva suhtes oleva sihtotstarbelist lähitoimesidet kasutava varajase avastamise kaugsidelugeja (DSRC-REDCR) ja sõiduki lähitoimesideseadme (DSRC-VU) vahel;
andmed	kindlaksmääratud vormingus (vt punkt 5.4.4) olevad turvatud andmed, mida DSRC-REDCR nõuab ja mida DSRC-VU sellele edastab 5. peatükis määratletud 5,8 GHz DSRC-ühenduse kaudu;
määrus (EL) nr 165/2014	Euroopa Parlamendi ja nõukogu määrus (EL) nr 165/2014, 4. veebruar 2014, autovedudel kasutatavate sõidumeerikute kohta, millega tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 3821/85 autovedudel kasutatavate sõidumeerikute kohta ning muudetakse Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 561/2006, mis käsitleb teatavate autovedusid käsitlevate sotsiaalõigusnormide ühtlustamist.
AID	(*application identifier*) rakenduse identifikaator
BLE	(*Bluetooth Low Energy*) Bluetooth®-i madala energiatarbega protokoll
BST	(*Beacon Service Table*) majakateenuste tabel

CIWD	(*card insertion while driving*) kaardi sisestamine juhtimise ajal
CRC	(*cyclic redundancy check*) tsükkelkoodkontroll
DSC (n)	kindla DSRC-liite saamise nõude identifikaator
DSRC	(*Dedicated Short Range Communication*) sihtotstarbeline lähitoimeside
DSRC-REDCR	(DSRC – *Remote Early Detection Communication Reader*) sihtotstarbelist lähitoimesidet kasutav varajase avastamise kaugsidelugeja,
DSRC-VU	(*DSRC – Vehicle Unit*) sõiduki lähitoimesideseade, sõiduki DSRC-seade. See on IC lisas määratletud „kaugsideseade“.
DWVC	(*driving without valid card*) juhtimine ilma kehtiva kaardita
EID	(*element identifier*) elemendi identifikaator
LLC	(*Logical Link Control*) loogilise lüli juhtimiskiht
LPDU	(*LLC protocol data unit*) LLC protokolli andmeüksus
OWS	(*onboard weighing system*) sõidukisisene kaalumissüsteem
PDU	(*protocol data unit*) protokolli andmeüksus
REDCR	(*remote early detection communication reader*) varajase avastamise kaugsidelugeja. See on IC lisas määratletud „varajase avastamise kaugsidelugeja“.
RTM	(*remote tachograph monitoring*) sõidumeerikute kaugseire
SM-REDCR	(*security module – remote early detection communication reader*) varajase avastamise kaugsidelugeja turbemoodul
TARV	(*Telematics Applications for Regulated Vehicles*) reguleerimisalasse kuuluvate sõidukite telemaatikarakendused (standardiseeria ISO 15638)
VU	(*vehicle unit*) sõidukiseade
VUPM	(*vehicle unit payload memory*) sõidukiseadme andmemälu
VUSM	(*vehicle unit security module*) sõidukiseadme turbemoodul
VST	(*Vehicle Service Table*) sõidukiteenuste tabel
WIM	(*weigh in motion*) liikuva sõiduki kaalumine
WOB	(*weigh on board*) sõidukisisene kaalumine

Käesolevas liites määratletud spetsifikaat lähtub ja sõltub tervikuna või osaliselt järgmistest määrustest ja standarditest. Käesoleva liite punktides on täpsustatud vastavad olulised standardid või standardite olulised punktid. Võimaliku vastuolu korral on ülimuslikud käesoleva liite sätted. Võimaliku vastuolu korral, kui käesolevas liites ei ole selget määratlust esitatud, lähtutakse eelkõige dokumendist ERC 70-03 (mida on kontrollitud standardi EN 300 674-1 asjakohaste parameetrite suhtes) ning seejärel tähtsuse järjekorras standarditest EN 12795, EN 12253, EN 12834 ja standardi EN 13372 punktidest 6.2, 6.3, 6.4 ja 7.1.

Käesolevas liites on viidatud järgmistele määrustele ja standarditele.

[1] Euroopa Parlamendi ja nõukogu määrus (EL) nr 165/2014, 4. veebruar 2014, autovedudel kasutatavate sõidumeerikute kohta, millega tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 3821/85 autovedudel kasutatavate sõidumeerikute kohta ning muudetakse Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 561/2006, mis käsitleb teatavate autovedusid käsitlevate sotsiaalõigusnormide ühtlustamist

[2] Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 561/2006, 15. märts 2006, mis käsitleb teatavate autovedusid käsitlevate sotsiaalõigusnormide ühtlustamist ja millega muudetakse nõukogu määrusi (EMÜ) nr 3821/85 ja (EÜ) nr 2135/98 ning tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 3820/85

[3] ERC 70-03 CEPT: ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)

[4] ISO 15638 *Intelligent transport systems – Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV)* („Intelligentsed transpordisüsteemid. Reguleerimisalasse kuuluvate kaubaveosõidukite (TARV) koostoimivate telemaatikarakenduste raamistik“)

[5] EN 300 674-1 *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)* („Elektromagnetilise ühilduvuse ja raadiospektri küsimused (ERM). Maanteetranspordi ja liikluse temaatika (RTTT). Tööstus-, teadus- ja meditsiinirakenduste (TTM) sagedusalas raadiosagedusel 5,8 GHz töötavad sihtotstarbelise lähitoimeside (DSRC) edastusseadmed (500 kbit/s / 250 kbit/s). Osa 1: Teeäärsete seadmete (RSU) ja sõidukisiseste seadmete (OBU) üldised omadused ja katsemeetodid“)

[6] EN 12253 *Road transport and traffic telematics – Dedicated short-range communication – Physical layer using microwave at 5.8 GHz* („Maanteetranspordi ja liikluse telemaatika. Sihtotstarbeline lähitoimeside. Sagedusel 5,8 GHz mikrolaineid kasutav füüsiline kiht“)

[7] EN 12795 *Road transport and traffic telematics – Dedicated short-range communication – Data link layer: medium access and logical link control* („Maanteetranspordi ja liikluse telemaatika. Sihtotstarbeline lähitoimeside. Andmelülikiht: juurdepääs kandjale ja loogilise lüli juhtimiskiht“)

[8] EN 12834 *Road transport and traffic telematics – Dedicated short-range communication – Application layer* („Maanteetranspordi ja liikluse telemaatika. Sihtotstarbeline lähitoimeside. Rakenduskiht“)

[9] EN 13372 *Road transport and traffic telematics – Dedicated short-range communication – Profiles for RTTT applications* („Maanteetranspordi ja liikluse telemaatika. Sihtotstarbeline lähitoimeside. RTTT rakenduste profiilid“)

[10] ISO 14906 *Electronic fee collection – Application interface definition for dedicated short- range communication* („Elektrooniline tasu kogumine. Sihtotstarbelise lähitoimeside rakendusliidese määratlus“)

4. TALITLUSOLUKORRAD

4.1. **Ülevaade**

Määruses (EL) nr 165/2014 on esitatud konkreetsed kontrollitavad olukorrad, kus tuleb andmesidet kasutada.

Toetatud olukorrad on järgmised:

„Sideprofiil 1: teeäärne kontroll, milles kasutatakse juhtmeta lähitoimeside varajase avastamise kaugsidelugejat, mis algatab füüsilise teeäärse kontrolli (ülem:alluv).

Lugeja profiil 1a: käsitsi suunatava või ajutiselt tee äärde paigaldatud varajase avastamise kaugsidelugeja abil.

Lugeja profiil 1b: sõidukile paigaldatud ja suunatud varajase avastamise kaugsidelugeja abil.“

4.1.1. *5,8 GHz DSRC-liidese kaudu toimuva andmeedastuse eeltingimused*

MÄRKUS: eeltingimuste konteksti mõistmiseks tuleks lähtuda allpool esitatud joonisest 14.3.

4.1.1.1. Sõidukiseadmes hoitavad andmed

DSC_12 Sõidukiseade peab iga 60 sekundi järel ajakohastama ja säilitama sõidukiseadmesse salvestatavaid andmeid ilma DSRC sidefunktsiooni abita. Selleks kasutatavad vahendid määratakse kindlaks sõidukiseadmes, need on määratletud IC lisa punktis 3.19 („Sihipärastes teeäärsetes kontrollides kasutatav kaugside“) ning neid ei käsitleta käesolevas liites.

4.1.1.2. Sõiduki DSRC-seadme edastatavad andmed

DSC_13 Sõidukiseade peab ajakohastama DSRC sõidumeeriku andmeid (edaspidi „andmed“) alati, kui sõidukiseadmes salvestatud andmeid ajakohastatakse punktis 4.1.1.1 (nõue DSC_12) nimetatud ajavahemiku järel ilma DSRC sidefunktsiooni abita.

DSC_14 Sõidukiseadme andmeid kasutatakse edastatavate andmeväljade täitmiseks ja ajakohastamiseks. Selleks kasutatavaid vahendeid on kirjeldatud IC lisa punktis 3.19 „Sihipärastes teeäärsetes kontrollides kasutatav kaugside“ või vastava kirjelduse puudumise korral lahendatakse see tootedisaini käigus ja seda ei käsitleta käesolevas liites. Sõiduki DSRC-seadme ja sõidukiseadme ühenduse lahenduse kohta vt punkt 5.6.

4.1.1.3. Andmete sisu

DSC_15 Andmete sisu ja vorming peab olema selline, et see on pärast dekrüpteerimist liigendatud ja kättesaadav käesoleva liite punktis 5.4.4 (Andmestruktuurid) määratletud vormis ja vormingus.

4.1.1.4. Andmete esitamine

DSC_16 Punktis 4.1.1.1 osutatud korra kohaselt piisava sagedusega ajakohastatud andmed tuleb enne sõiduki DSRC-seadmele esitamist turvata ning esitada sõiduki DSRC-seadmele ajutiseks salvestamiseks andmete kehtiva turvatud versioonina. Kõnealused andmed edastatakse sõidukiseadme turbemoodulist (VUSM) sõidukiseadme andmemälu (VUPM) DSRC-funktsioonile. VUSM ja VUPM on funktsioonid, mitte tingimata füüsilised üksused. Nimetatud funktsioonide füüsiline vorm lahendatakse tootedisaini käigus, kui seda ei ole määratletud määruse (EL) nr 165/2014 muudes osades.

4.1.1.5. Turbeandmed

DSC_17 Turbeandmed (*securityData*), mis on REDCR-i jaoks vajalikud andmete dekrüpteerimiseks, edastatakse vastavalt 11. liitele („Ühised turbemehhanismid“) ning esitatakse sõiduki DSRC-seadmes ajutiselt salvestamiseks andmetüübina *securityData* käesoleva liite punktis 5.4.4 määratletud kujul.

4.1.1.6. DSRC-liidese kaudu edastatavad sõidukiseadme andmemälu andmed

DSC_18 Sõidukiseadme andmemälu DSRC-funktsioonis alati saadaolevad andmetüübid, mida REDCR-i nõudmisel saab kohe edastada, on määratletud punktis 5.4.4 kooskõlas täieliku ASN.1 mooduli spetsifikaadiga.

Sideprofiili 1 üldine ülevaade

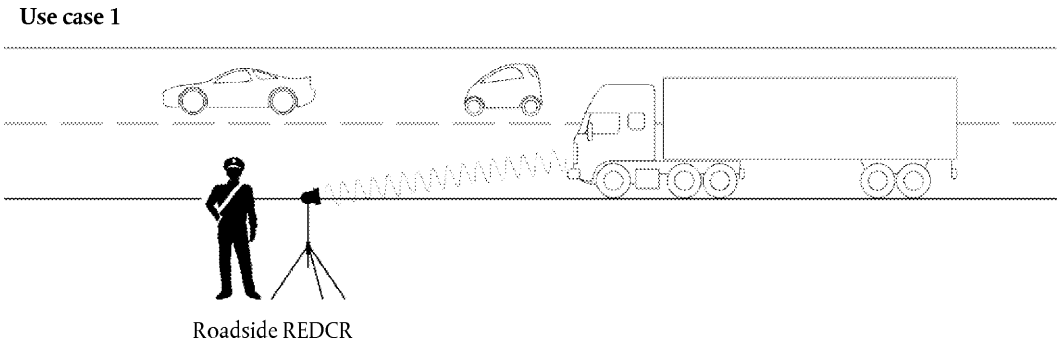
Profiil hõlmab kasutusolukorda, kus pädeva kontrolliasutuse esindaja kasutab lähitoimelist varajase avastamise kaugsidelugejat (5,8 GHz DSRC-liides, mis toimib vastavalt dokumendi ERC 70-03 nõuetele ning mida on katsetatud standardi EN 300 674-1 asjakohaste parameetrite suhtes, nagu on kirjeldatud 5. peatükis) selleks, et teha kaugside teel kindlaks sõiduk, mis võib rikkuda määruse (EL) 165/2014 nõudeid.

4.1.2. *Profiil 1a: käsitsi suunatav või ajutiselt tee äärde paigaldatud suunatav varajase avastamise kaugsidelugeja*

Selles kasutusolukorras asub pädeva kontrolliasutuse esindaja tee ääres ning suunab käes hoitava, statiivile paigaldatud või muul viisil teisaldatava varajase avastamise kaugsidelugeja (REDCR) huvi pakkuva sõiduki tuuleklaasi keskkohta. 5,8 GHz DSRC-liidese kaudu edastatav päring tehakse vastavalt dokumendile ERC 70-03 ning seda kontrollitakse standardis EN 300 674-1 nimetatud asjakohaste parameetrite suhtes, nagu on kirjeldatud 5. peatükis. Vt joonis 14.1 (kasutusolukord 1).

Joonis 14.1.

Teeäärse päringu saatmine 5,8 GHz DSRC kaudu

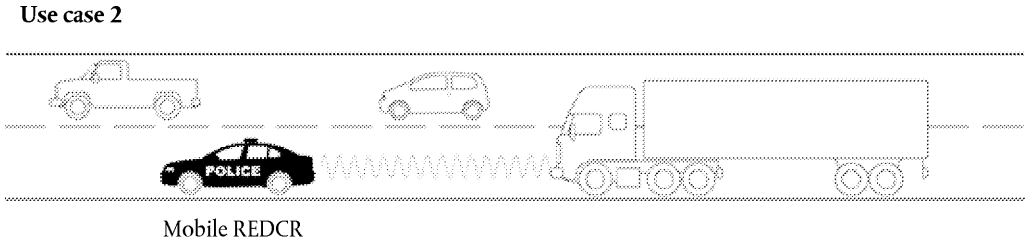


4.1.3. *Profiil 1b: sõidukile paigaldatud ja suunatud varajase avastamise kaugsidelugeja (REDCR) abil*

Selles kasutusolukorras asub pädeva kontrolliasutuse esindaja liikuvas sõidukis ning suunab käes hoitava teisaldatava REDCR-i huvi pakkuva sõiduki tuuleklaasi keskkohta või on REDCR paigaldatud sõiduki sisse või peale nii, et see on suunatud huvi pakkuva sõiduki tuuleklaasi keskkohta olukorras, kus varajase avastamise kaugsidelugejat kandev sõiduk on huvi pakkuva sõiduki suhtes teatud kindlas asukohas (näiteks liiklusvoos vahetult selle ees). 5,8 GHz DSRC-liidese kaudu edastatav päring tehakse vastavalt dokumendile ERC 70-03 ning seda kontrollitakse standardis EN 300 674-1 nimetatud asjakohaste parameetrite suhtes, nagu on kirjeldatud 5. peatükis. Vt joonis 14.2 (kasutusolukord 2).

Joonis 14.2.

Sõidukilt päringu saatmine 5,8 GHz DSRC kaudu



4.2. **Turvalisus/terviklus**

Et võimaldada kaugside kaudu allalaaditud andmete autentsuse ja tervikluse kontrollimist, toimub andmete kontrollimine ja dekrüpteerimine kooskõlas 11. liitega „Ühised turbemehhanismid“.

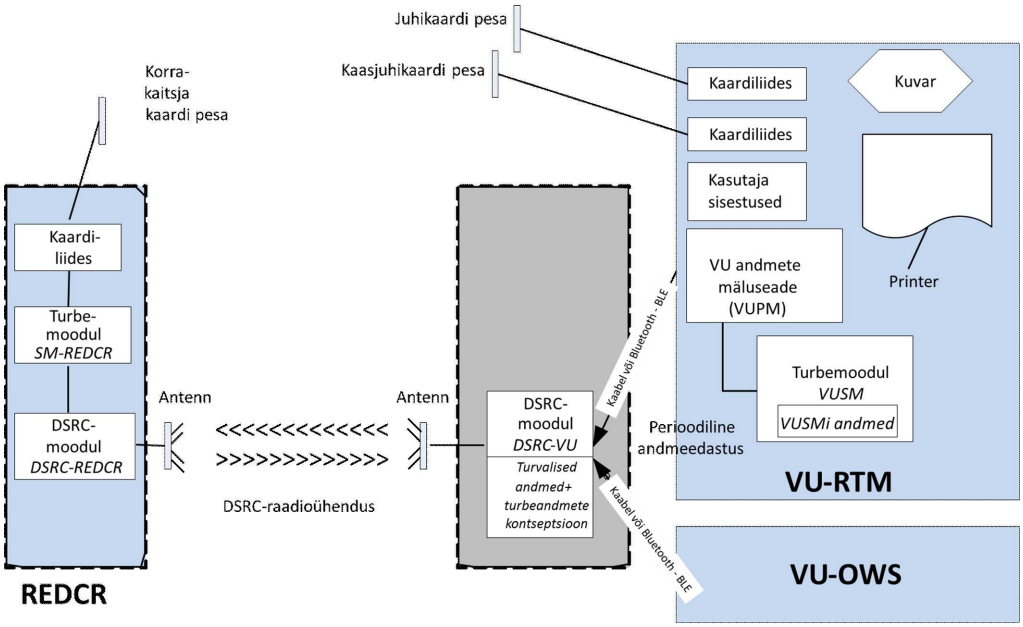
5. KAUGSIDE LAHENDUS JA PROTOKOLLID

5.1. **Lahendus**

Aruka sõidumeeriku kaugsidefunktsiooni lahendust on kirjeldatud joonisel 14.3.

Joonis 14.3.

Kaugsidefunktsiooni lahendus



DSC_19 Sõidukiseadmes asuvad järgmised funktsioonid.

— Turbemoodul (VUSM). See sõidukiseadme funktsioon tegeleb sõiduki DSRC-seadmest kaugside kaudu pädeva asutuse esindajale saadetavate andmete turvamisega.

— Turvatud andmed salvestatakse VUSM-i mälus. Punktis 4.1.1.1 (DSC_12) määratletud ajavahemike järel sõidukiseade krüpteerib ja täiendab sõiduki DSRC-seadme mälus hoitavaid RTM-andmeid (mis koosnevad sõidumeeriku andmetest ja käesolevas liites allpool määratletud turbeandmetest). Turbemooduli toimingud on määratletud 11. liites „Ühised turbemehhanismid“ ning ei kuulu käesoleva liite reguleerimisalasse, välja arvatud nõue, et turbemoodul peab saatma sõiduki kaugsideseadmele ajakohastatud andmed alati, kui VUSM-i andmed muutuvad.

— Sõidukiseadme ja sõiduki DSRC-seadme vaheline side võib olla lahendatud juhtmega või Bluetooth Low Energy (BLE) protokolliga ning sõiduki DSRC-seadme füüsiline asukoht võib olla sõiduki tuuleklaasil paiknevas antennis, sõidukiseadme sees või mujal.

— Sõiduki DSRC-seadmel peab olema alati kasutatav töökindel toiteallikas. Selle toitevooluga varustamise vahendid valitakse projekteerimise käigus.

— Sõiduki DSRC-seadme mälu peab olema säilmälu, mis säilitab andmeid sõiduki DSRC-seadmes ka pärast sõiduki süüte väljalülitamist.

— Kui sõidukiseadme ja sõiduki DSRC-seadme vaheline side põhineb BLE protokollil ning toiteallikas on mittelaetav patarei, vahetatakse sõiduki DSRC-seadme toiteallikas välja iga korralise ülevaatuse ajal ning sõiduki DSRC-seadme tootja peab tagama, et kasutatav toiteallikas kestab ühest korralisest ülevaatusest järgmiseni, hoides andmeid REDCR-i jaoks tavapärasel viisil kättesaadavana kogu selle perioodi vältel ilma tõrgete ja katkestusteta.

— Sõidukiseadme RTM-andmete mälu (VUPM). See sõidukiseadme funktsioon esitab ja ajakohastab andmeid. Andmete sisu („TachographPayload“) on määratletud allpool punktis 5.4.4/5.4.5 ning seda ajakohastatakse punktis 4.1.1.1 (DSC_12) nimetatud ajavahemike järel.

— Sõiduki DSRC-seade. See antenni sisse ehitatud või sellega ühendatud ning juhtmega või juhtmeta (BLE) side kaudu sõidukiseadmega ühenduses olev funktsioon hoiab aktuaalseid andmeid (VUPM-i andmed) ning haldab 5,8 GHz DSRC kaudu saadud päringute vastuseid. DSRC-seadme lahtiühendamine või selle talitluse häirimine sõiduki tavapärase töö ajal on määruse (EL) nr 165/2014 rikkumine.

— REDCR-i turbemoodul (SM-REDCR) on funktsioon, mida kasutatakse sõidukiseadmest pärit andmete dekrüpteerimiseks ja nende tervikluse kontrollimiseks. Selle saavutamiseks kasutatavad vahendid on määratletud 11. liites „Ühised turbemehhanismid“ ja mitte käesolevas liites.

— REDCR-i DSRC-seadme (DSRC-REDCR) funktsioon hõlmab 5,8 GHz transiiverit ning sellega seotud püsi- ja tarkvara, mis haldab sõiduki DSRC-seadmega toimuvat andmesidet vastavalt käesolevale liitele.

— DSRC-REDCR saadab huvi pakkuva sõiduki DSRC-seadmele päringu, võtab vastu DSRC-ühenduse kaudu saavad andmed (huvi pakkuva sõiduki kehtivad VUPM-i andmed), töötleb neid ning salvestab need oma turbemoodulisse SM-REDCR.

— Sõiduki DSRC-seadme antenn peab paiknema kohas, kus on tagatud sõiduki ja teeäärse antenni vaheline optimaalne DSRC-ühendus (üldjuhul sõiduki tuuleklaasi keskkohas või selle lähedal). Kergsõidukitel võib antenni paigaldada tuuleklaasi ülemisse ossa.

— Antenni ees või läheduses ei tohi olla metallist objekte (nt nimesildid, kleebised, peegeldumisvastased (toonivad) ribad, päikesesirmid, puhkeasendis klaasipuhastid.

— Antenn paigaldatakse nii, et selle telg on tee pinnaga ligikaudu paralleelne.

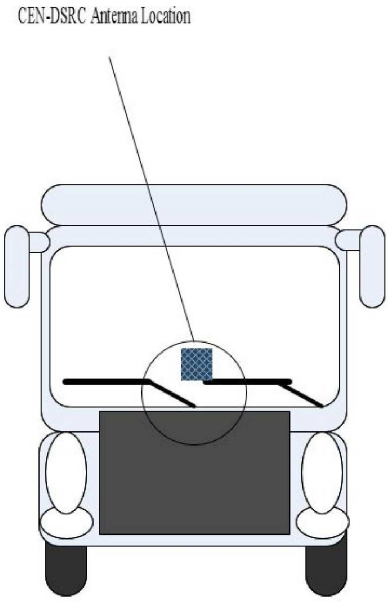
DSC_20 Antenn ja andmeside peavad toimima vastavalt dokumendile ERC 70-03 ning seda kontrollitakse standardis EN 300 674-1 nimetatud asjakohaste parameetrite suhtes, nagu on kirjeldatud 5. peatükis. Antenni ja andmeside puhul võib kasutada ECC aruandes nr 228 kirjeldatud raadiohäirete vähendamise meetodeid, näiteks CENi 5,8 GHz DSRC-ühenduse filtreid.

DSC_21 DSRC-antenn peab olema ühendatud sõiduki DSRC-seadmega otse tuuleklaasile või selle lähedusse paigaldatud moodulis või spetsiaalse kaabli kaudu, mille ehitus raskendab ebaseaduslikku lahtiühendamist. Antenni lahtiühendamine või selle töö häirimine on määruse (EL) nr 165/2014 rikkumine. Antenni tahtlik kinnikatmine või selle tööomaduste muul viisil halvendamine on määruse (EL) nr 165/2014 rikkumine.

DSC_22 Antenni kuju ei ole kindlaks määratud ning see määratletakse tootja otsusega, kuid paigaldatud sõiduki DSRC-seade peab vastama allpool 5. peatükis esitatud nõuetele. Antenn paigutatakse vastavalt nõudele DSC_19 ja joonisele 14.4 (ovaalne joon) ning see peab toetama punktides 4.1.2 ja 4.1.3 kirjeldatud kasutusolukordi.

Joonis 14.4.

Näide 5,8 GHz DSRC-antenni paigutusest reguleerimisalasse kuuluva sõiduki tuuleklaasil



REDCR-i ja selle antenni kuju võib olla erinev olenevalt lugeja kasutusviisist (statiivil, käeshoitav, sõidukile paigaldatud jne) ja pädeva kontrolliasutuse esindaja tegevusest.

Kaugsidefunktsiooni tulemuste edastamiseks pädeva kontrolliasutuse esindajale kasutatakse kuvamist ja/või teavitusfunktsiooni. Näit võidakse kuvada ekraanil, edastada prinditud väljatrükil, helisignaalina või selliste teavituste kombinatsioonina. Kõnealuse näidu ja/või teavituste esitamise vorm sõltub pädeva kontrolliasutuse esindaja nõuetest ja seadme tehnilisest lahendusest ning seda ei ole käesolevas liites määratletud.

DSC_23 REDCR-i tehniline lahendus ja kuju lahendatakse tootedisainiga kooskõlas dokumendiga ERC 70-03 ning käesolevas liites (punkt 5.3.2) esitatud tehnilise lahenduse ja töönäitajate määratlusega, et anda turule võimalikult suur paindlikkus pädeva kontrolliasutuse kindlates päringuolukordades kasutatavate seadmete väljatöötamiseks ja tarnimiseks.

DSC_24 Sõiduki DSRC-seadme tehniline lahendus, kuju ning paiknemine sõidukiseadmes või sellest väljaspool lahendatakse tootearendusega kooskõlas dokumendiga ERC 70-03, käesolevas liites (punkt 5.3.2) esitatud tehnilise lahenduse ja töönäitajate määratlusega ning käesoleva punktiga 5.1

DSC_25 Sõiduki DSRC-seade peab suutma muudelt intelligentsetelt sõidukiseadmetelt vastu võtta eri andmetüüpide väärtusi valdkonnas kasutatava standardse ühenduse ja standardsete protokollide abil (näiteks sõidukisisese kaalumise seadmetelt) tingimusel, et sellised andmetüübid on eristatud kordumatute ja teadaolevate rakendusidentifikaatorite/failinimedega, selliste protokollide kasutamise juhised esitatakse Euroopa Komisjonile ning tehakse tasuta kättesaadavaks vastavate seadmete tootjatele.

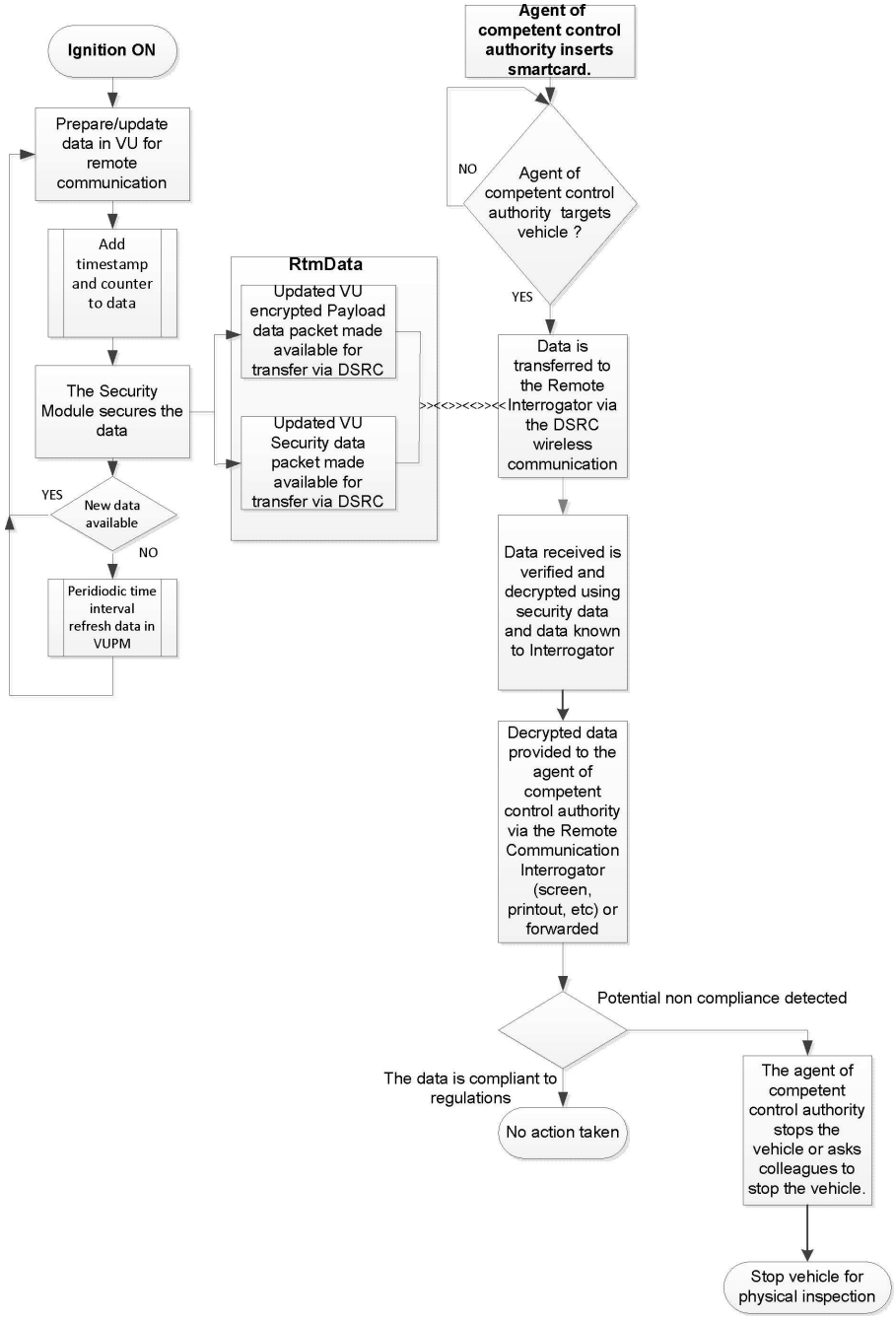
5.2. **Töövoog**

5.2.1. *Toimingud*

Toimingute voogu on kujutatud joonisel 14.5.

Joonis 14.5.

Kaugsidefunktsiooni töövoog



Etappe on kirjeldatud allpool.

a. Sõiduki töötamise ajal (süüde on sisse lülitatud) edastab sõidumeerik pidevalt andmeid sõidukiseadme funktsioonile. Sõidukiseadme funktsioon valmistab andmed ette kaugsidefunktsiooni jaoks (krüpteeritud) ning ajakohastab sõiduki DSRC-seadme mälu ja andmemälu (VUPM) sisu (vastavalt punktidele 4.1.1.1–4.1.1.2). Kogutud andmed vormindatakse vastavalt punktidele5.4.4–5.4.5.

b. Andmete iga ajakohastamise korral uuendatakse turbeandmetes määratletud ajatemplit.

c. VUSM-i funktsioon turvab andmeid vastavalt 11. liites kindlaks määratud korrale.

d. Andmete iga ajakohastamise korral (vt punktid 4.1.1.1–4.1.1.2) edastatakse andmed sõiduki DSRC-seadmele, kus need asendavad eelmised seal hoitud andmed, et REDCR-ilt päringu saamisel oleks alati võimalik edastada ajakohastatud kehtivaid andmeid („andmed"). Sõidukiseadmelt sõiduki DSRC-seadmele edastatavad andmed peavad olema tuvastatavad failinime *RTMData* või rakenduse ja atribuudi identifikaatorite järgi.

e. Kui pädeva kontrolliasutuse esindaja soovib sõidukit uurida ja huvi pakkuvalt sõidukilt andmeid koguda, sisestab pädeva kontrolliasutuse esindaja kõigepealt REDCR-i oma kiipkaardi, et lubada andmeside ning võimaldada SM-REDCR-il andmete autentsust kontrollida ja andmeid dekrüpteerida.

f. Seejärel valib pädeva kontrolliasutuse esindaja välja sõiduki ning nõuab sellele kaugside teel andmeid. REDCR avab huvi pakkuva sõiduki DSRC-seadmega 5,8 GHz liidese seansi ja nõuab sellelt andmeid. Andmed edastatakse REDCR-ile juhtmeta andmeside süsteemi kaudu DSRC-i atribuudina, kasutades rakendusteenust GET, mis on määratletud punktis 5.4. Atribuut sisaldab krüpteeritud andmeväärtusi ja DSRC-i turbeandmeid.

g. REDCR analüüsib andmeid ning edastab need pädeva kontrolliasutuse esindajale.

h. Pädeva kontrolliasutuse esindaja teeb andmetest lähtudes otsuse, kas peatada sõiduk põhjalikumaks kontrolliks või paluda mõnel teisel pädeva kontrolliasutusel sõiduk peatada.

5.2.2. *DSRC-andmeside kaudu saadud andmete tõlgendamine*

DSC_26 5,8 GHz liidese kaudu saadud andmetel on allpool punktides 5.4.4 ja 5.4.5 määratletud tähendus ja vorming ning käesolevas liites määratletud eesmärkide täitmiseks peab olema mõistetav ainult see tähendus ja vorming. Kooskõlas määruse (EL) nr 165/2014 sätetega kasutatakse andmeid üksnes olulise teabe andmiseks pädevale asutusele, et aidata otsustada, milline sõiduk tuleks peatada füüsiliseks kontrolliks. Seejärel andmed hävitatakse vastavalt määruse (EL) nr 165/2014 artiklile 9.

5.3. **Kaugsideks kasutatava DSRC füüsilise liidese parameetrid**

5.3.1. *Piirangud asukohale*

DSC_27 5,8 GHz liidesega kaugpäringusaatjat ei tohiks kasutada 200 meetri raadiuses toimivast 5,8 GHz DSRC-signaalsillast.

5.3.2. *Alla- ja üleslüli parameetrid*

DSC_28 Sõidumeerikute kaugseireks kasutatavad seadmed peavad vastama dokumendi ERC 70-03 nõuetele ning allpool tabelites 14.1 ja 14.2 määratletud parameetritele.

DSC_29 Lisaks peavad sõidumeerikute kaugseireks kasutatavad seadmed selleks, et tagada ühilduvust muude standardsete 5,8 GHz DSRC-süsteemidega, vastama standardites EN12253 ja EN 13372 esitatud ja allpool täpsustatud parameetritele.

Tabel 14.1.

Allalüli parameetrid

Nr	Parameeter	Väärtus(ed)	Märkus
D1	Allalüli kandesagedused	REDCR võib kasutada nelja sagedust: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	ERC 70-03 kohaselt Kandesageduse võib valida teeäärse süsteemi teostaja ning see ei pea olema teada sõiduki DSRC-seadmes. (kooskõlas standarditega EN 12253, EN 13372)
D1a (*)	Kandesageduste lubatud hälve	± 5 ppm	(kooskõlas standardiga EN 12253)
D2 (*)	RSU (REDCR) saatja spektrimask	ERC 70-03 kohaselt REDCR peab vastama standardis EN 12253 määratletud klassile B, C. Muid erinõudeid käesolevas lisas ei esitata.	Parameeter, mida kasutatakse läheduses asuvate päringuseadmete põhjustatud häirete kontrollimiseks (vastavalt standarditele EN 12253 ja EN 13372).
D3	OBU(DSRC-VU) minimaalne sagedusvahemik	5,795–5,815 GHz	(kooskõlas standardiga EN 12253)
D4 (*)	Maksimaalne E.I.R.P.	ERC 70-03 kohaselt (litsentseerimata) ja vastavalt riiklikele eeskirjadele Maksimaalselt + 33 dBm	(kooskõlas standardiga EN 12253)
D4a	E.I.R.P. nurkmask	Vastavalt päringuseadme väljatöötaja teatavaks tehtud ja avaldatud spetsifikaadile	(kooskõlas standardiga EN 12253)
D5	Polarisatsioon	Vasakpoolne ringpolarisatsioon	(kooskõlas standardiga EN 12253)
D5a	Ristpolarisatsioon	XPD: Teljel: (REDCR) RSU t ≥ 15 dB (DSRC-VU) OBU r ≥ 10 dB 3 dB alas: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(kooskõlas standardiga EN 12253)
D6 (*)	Modulatsioon	Kahetasemeline amplituudimodulatsioon	(kooskõlas standardiga EN 12253)
D6a (*)	Modulatsiooniindeks	0,5 ... 0,9	(kooskõlas standardiga EN 12253)

Nr	Parameeter	Väärtus(ed)	Märkus
D6b	Eye Pattern	≥ 90 % (aeg) / ≥ 85 % (amplituud)	
D7 (*)	Andmete kodeerimine	FM0 Bitil „1“ on üleminekud ainult bitiintervalli alguses ja lõpus. Bitil „0“ on võrreldes bitiga „1“ täiendav üleminek bitiintervalli keskel.	(kooskõlas standardiga EN 12253)
D8 (*)	Bitikiirus	500 kBit/s	(kooskõlas standardiga EN 12253)
D8a	Bitikella lubatud hälve	väiksem kui ± 100 ppm	(kooskõlas standardiga EN 12253)
D9 (*)	Bitiveategur (B.E.R.) andmesides	$\leq 10^{-6}$ kui OBU (DSRC-VU) otsene energia on punktidest nr D11a kuni D11b tulenevas vahemikus.	(kooskõlas standardiga EN 12253)
D10	OBU (DSRC-VU) äratustriger	OBU (DSRC-VU) ärkab juhul, kui ta saab 11 või enam oktetti sisaldava kaadri (koos eelsignaaliga)	Eraldi äratusmuster ei ole vajalik. DSRC-VU võib ärgata ka vähem kui 11 oktetti sisaldava kaadri saamisel (kooskõlas standardiga EN 12253)
D10a	Maksimaalne käivitusaeg	≤ 5 ms	(kooskõlas standardiga EN 12253)
D11	Sidetsoon	Ruumipiirkond, milles saavutatakse punktile D9a vastav B.E.R.	(kooskõlas standardiga EN 12253)
D11a (*)	Side energialimiit (ülemine)	– 24dBm	(kooskõlas standardiga EN 12253)
D11b (*)	Side energialimiit (alumine)	Otsene energia: – 43 dBm (telg) – 41 dBm (– 45° kuni + 45° vahemikus teepinnaga paralleelse tasapinna suhtes, kui DSRC-VU paigaldatakse hiljem sõidukisse (asimuut))	(kooskõlas standardiga EN 12253) Käesolevas lisas määratletud kasutusolukordade tõttu on horisontaalnurka suurendatud kuni ± 45°.
D12 (*)	DSRC-VU katkestusenergia tase	– 60 dBm	(kooskõlas standardiga EN 12253)
D13	Eelsignaal	Eelsignaal on kohustuslik.	(kooskõlas standardiga EN 12253)
D13a	Eelsignaali pikkus ja muster	16 bitti ± 1 bitt FM0 koodiga bittidest „1“	(kooskõlas standardiga EN 12253)

Nr	Parameeter	Väärtus(ed)	Märkus
D13b	Eelsignaali lainekuju	Vahelduva madala ja kõrge tasemega jada impulsi kestusega 2 µs. Lubatud hälve on esitatud punktis D8a.	(kooskõlas standardiga EN 12253)
D13c	Järelbitid	RSU (REDCR) võib edastada pärast lõpusilti kuni 8 bitti. OBU (DSRC-VU) ei pea neid täiendavaid bitte arvesse võtma.	(kooskõlas standardiga EN 12253)

(*) – allalüli parameetrite suhtes tehakse vastavuskatsed vastavalt standardis EN 300 674-1 kirjeldatud parameetrikatsetele

Tabel 14.2.

Üleslüli parameetrid

Nr	Parameeter	Väärtus(ed)	Märkus
U1 (*)	Abikandesagedused	OBU (DSRC-VU) toetab sagedusi 1,5 MHz ja 2,0 MHz. RSU (REDCR) toetab sagedust 1,5 MHz või 2,0 MHz või mõlemat. U1-0: 1.5 MHz U1-1: 2.0 MHz	Abikandesageduse valik (1,5 MHz või 2,0 MHz) sõltub standardi EN 13372 kohasest valitud profiilist.
U1a (*)	Abikandesageduste lubatud hälve	± 0,1 %	(kooskõlas standardiga EN 12253)
U1b	Külgribade kasutamine	Samad andmed mõlemal küljel	(kooskõlas standardiga EN 12253)
U2 (*)	OBU (DSRC-VU) saatja spektrimask	Vastavalt standardile EN12253 1) Ribaväline energia: vt ETSI EN 300674-1 2) Ribasisene energia: [U4a] dBm, 500 kHz 3) Emissioon muudes üleslüli kanalites: U2(3)-1 = – 35 dBm, 500 kHz	(kooskõlas standardiga EN 12253)
U4a (*)	Ühe külgriba maksimaalne E.I.R.P. (telg)	Kaks varianti: U4a-0: – 14 dBm U4a-1: – 21 dBm	Vastavalt seadme väljatöötaja teatavaks tehtud ja avaldatud spetsifikaadile
U4b (*)	Ühe külgriba maksimaalne E.I.R.P. (35°)	Kaks varianti: — ei kohaldata — – 17dBm	Vastavalt seadme väljatöötaja teatavaks tehtud ja avaldatud spetsifikaadile
U5	Polarisatsioon	Vasakpoolne ringpolarisatsioon	(kooskõlas standardiga EN 12253)

Nr	Parameeter	Väärtus(ed)	Märkus
U5a	Ristpolarisatsioon	XPD: Teljel: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB – 3 dB juures: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(kooskõlas standardiga EN 12253)
U6	Abikandesageduse modulatsioon	2-PSK Abikandesagedusega sünkroonitud andmed kodeeritud andmete üleminekud kattuvad abikandesageduse üleminekutega	(kooskõlas standardiga EN 12253)
U6b	Täitetegur	Täitetegur: 50 % ± α, α ≤ 5 %	(kooskõlas standardiga EN 12253)
U6c	Kandesageduse modulatsioon	Moduleeritud abikandesageduse korrutamine kandesagedusega.	(kooskõlas standardiga EN 12253)
U7 (*)	Andmete kodeerimine	NRZI (biti „1“ alguses üleminekut ei ole, biti „0“ alguses on üleminek, biti sees üleminekut ei ole)	(kooskõlas standardiga EN 12253)
U8 (*)	Bitikiirus	250 kBit/s	(kooskõlas standardiga EN 12253)
U8a	Bitikella lubatud hälve	± 1 000 ppm	(kooskõlas standardiga EN 12253)
U9	Bitiveategur (B.E.R.) andmesides	≤ 10^{-6}	(kooskõlas standardiga EN 12253)
U11	Sidetsoon	Ruumipiirkond, milles DSRC-VU asub, nii et REDCR saab edastuse kätte väiksema kui punktis U9a osutatud veateguriga B.E.R.	(kooskõlas standardiga EN 12253)
U12a (*)	Muundusvõimendus (alumine limiit)	1 dB iga külgriba kohta Nurgavahemik: teljesuuna ja nurga ± 35° vahel ringikujuliselt sümmeetriline	
		ning – 45° kuni + 45° vahemikus teepinnaga paralleelse tasapinna suhtes, kui DSRC-VU paigaldatakse hiljem sõidukisse (asimuut))	Käesolevas lisas määratletud kasutusolukordade tõttu on horisontaalnurka suurendatud kuni ± 45°.
U12b (*)	Muundusvõimendus (ülemine limiit)	10 dB iga külgriba kohta	Väiksem kui määratletud väärtusevahemik igas külgribas, mis asub telje ümber ümmarguses koonuses vahemikus ± 45° avanemisnurgast
U13	Eelsignaal	Eelsignaal on kohustuslik.	(kooskõlas standardiga EN 12253)

Nr	Parameeter	Väärtus(ed)	Märkus
U13a	Eelsignaali pikkus ja muster	Ainult abikandesagedusega moduleeritud 32 kuni 36 µs, seejärel 8 bitti NRZI koodiga bittidest „0“.	(kooskõlas standardiga EN 12253)
U13b	Järelbitid	DSRC-VU võib edastada pärast lõpusilti kuni 8 bitti. RSU (REDCR) ei pea neid täiendavaid bitte arvesse võtma.	(kooskõlas standardiga EN 12253)

(*) – üleslüli parameetrite suhtes tehakse vastavuskatsed vastavalt standardis EN 300 674-1 kirjeldatud parameetrikatsetele

5.3.3. *Antenni tehniline lahendus*

5.3.3.1. REDCR-i antenn

DSC_30 REDCR-i antenni tehniline lahendus määratakse kindlaks tootedisaini käigus ning see peab toimima punktis 5.3.2 määratletud piirides, mida on kohandatud, et optimeerida DSRC-REDCRi tööomadusi vastavalt konkreetsele eesmärgile ja lugemisolukorrale, milles töötamiseks REDCR on ette nähtud.

5.3.3.2. Sõidukiseadme antenn

DSC_31 Sõiduki DSRC-seadme antenni tehniline lahendus määratakse kindlaks tootedisaini käigus ning see peab toimima punktis 5.3.2 määratletud piirides, mida on kohandatud, et optimeerida DSRC-REDCRi tööomadusi vastavalt konkreetsele eesmärgile ja lugemisolukorrale, milles töötamiseks REDCR on ette nähtud.

DSC_32 Sõidukiseadme antenn kinnitatakse sõiduki eesmisele tuuleklaasile või selle lähedale vastavalt punktile 5.1.

DSC_33 Töökoja katsekeskkonnas (vt punkt 6.3) peab punkti 5.1 nõuete kohaselt paigaldatud sõiduki DSRC-seadme antenn suutma edukalt luua standardse katseandmesideühenduse ning edastama käesolevas liites määratletud RTM-andmeid kauguste vahemikus 2–10 meetrit suurema õnnestumiste protsendiga kui 99 %, mis on arvutatud 1 000 lugemispäringu keskmise väärtusena.

5.4. **DSRC-protokolli nõuded sõidumeerikute kaugseirele**

5.4.1. *Ülevaade*

DSC_34 5,8 GHz DSRC-liidese ühenduse kaudu andmete allalaadimiseks kasutatav andmesideprotokoll peab toimima vastavalt allpool loetletud etappidele. Käesolevas punktis kirjeldatakse andmesidevoogu ideaaltingimustel ilma kordusedastuste ja sidekatkestusteta.

MÄRKUS Initsialiseerimisetapi (etapp 1) eesmärk on luua side REDCR-i ja sõiduki DSRC-seadme vahel, mis on sisenenud 5,8 GHz DSRC (ülem-alluv) andmesidealasse, kuid ei ole veel REDCR-iga ühendust loonud, ning edastada teade rakendusprotsessidele.

— **Etapp 1** Initsialiseerimine. REDCR saadab välja kaadri, mis sisaldab „majakateenuste tabelit“ (BST), milles on toetatavate teenuste rakendusidentifikaatorid (AID). RTM-rakenduses on selleks lihtsalt teenus, mille AID väärtus = 2 (Freight&Fleet). Sõiduki DSRC-seade hindab saadud BST-d ning vastab (vt allpool) omapoolse domeenis Freight&Fleet toetatud rakenduste nimekirjaga või ei saada vastust, kui ühtegi teenust ei toetata. Kui REDCR ei paku identifikaatorit AID = 2, siis sõiduki DSRC-seade REDCR-ile ei vasta.

— **Etapp 2** Sõiduki DSRC-seade saadab välja kaadri, mis sisaldab nõuet privaatakna eraldamiseks.

— **Etapp 3** REDCR saadab välja kaardi, mis sisaldab privaatakna eraldamise kinnitust.

— **Etapp 4** Sõiduki DSRC-seade kasutab eraldatud privaatakent, et saata välja kaader, mis sisaldab sõidukiteenuste tabelit (VST). VST sisaldab loetelu kõigist rakenduste eksemplaridest, mida sõiduki DSRC-seade AID = 2 raamistikus toetab. Erinevate eksemplaride eristamiseks kasutatakse kordumatuid elemendi identifikaatoreid (EID), millest igaüks on seotud mõne rakenduse kontekstimärgi parameetri väärtusega, mis näitab toetatavat rakendust ja standardit.

— **Etapp 5** Seejärel analüüsib REDCR pakutud VST-d ning lõpetab ühenduse (käsk RELEASE), kui ta ei ole huvitatud VST-s pakutavast (st VST saatja on sõiduki DSRC-seade, mis ei toeta RTM-andmesidet), või sobiva VST saamise korral käivitab rakenduse eksemplari.

— **Etapp 6** Selleks saadab REDCR välja kaadri, mis sisaldab RTM-andmete väljavõtmise käsku ning täpsustab RTM-i rakenduse eksemplari sellele vastava identifikaatoriga (vastavalt sõiduki DSRC-seadme VST-le) ja eraldab privaatakna.

— **Etapp 7** Sõiduki DSRC-seade kasutab uut privaatakent selleks, et saata välja kaader, mis sisaldab RTM-i rakenduse eksemplarile vastavat identifikaatorit, mis on märgitud VST-s, ning seejärel atribuut *RtmData* (andmeelement + turbeelement).

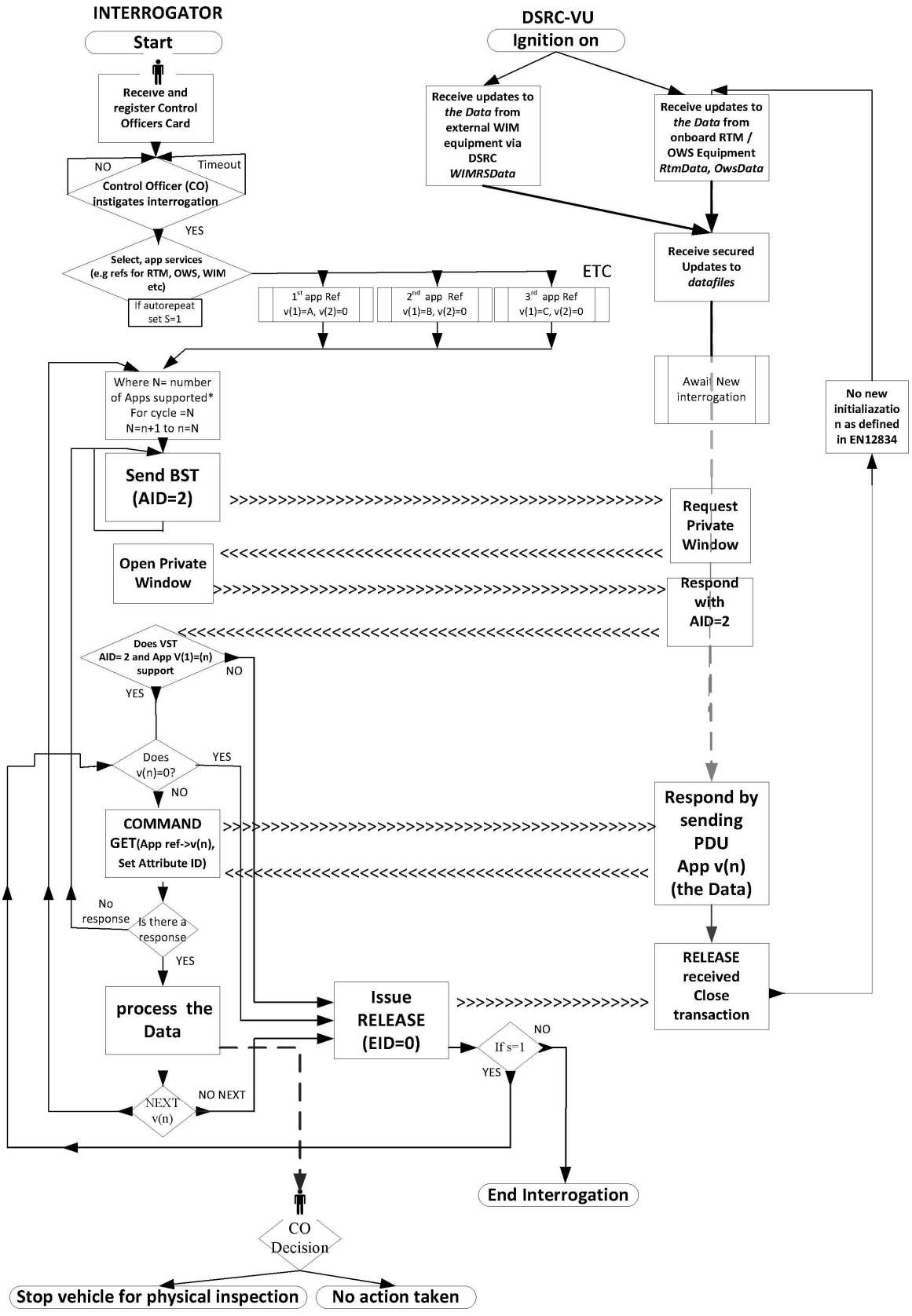
— **Etapp 8** Mitme teenuse nõudmise korral asendub väärtus n järgmise teenuse viitenumbriga ja protsessi korratakse.

— **Etapp 9** REDCR kinnitab andmete kättesaamist ja lõpetab seansi, saates sõiduki DSRC-seadmele kaadri, mis sisaldab käsku RELEASE, või alustab uuesti etappi 6, kui LDPU kättesaamise kontrollimine ebaõnnestus.

Andmesideprotokolli pildiline kujutis on esitatud joonisel 14.6.

Joonis 14.6.

5,8 GHz DSRC kaudu RTM-andmete saatmise protsessivoog



5.4.2. *Käsud*

DSC_35 Järgmised käsud on ainsad funktsioonid, mida RTM-andmeside etapis kasutatakse.

— **INITIALISATION.request**: REDCR-i saadetav levikäsk, mis sisaldab REDCR-i toetatud rakenduste määratlust.

— **INITIALISATION.response**: sõiduki DSRC-seadme vastus, mis kinnitab ühenduse loomist ning sisaldab toetatud rakenduste eksemplaride nimekirja koos nende karakteristikutega ja juhistega nende adresseerimiseks (EID).

— **GET.request**: REDCR-ist sõiduki DSRC-seadmesse saadetav käsk, milles täpsustatakse määratletud EID abil soovitud rakenduse eksemplar vastavalt saadud VST-le ning antakse sõiduki DSRC-seadmele korraldus saata väljastatavates andmetes valitud atribuudid. Käsu GET eesmärk on see, et REDCR saaks sõiduki DSRC-seadmest kätte andmed.

— **GET.response**: sõiduki DSRC-seadme vastus, mis sisaldab nõutud andmeid.

— **ACTION.request ECHO**: käsk, mis annab sõiduki DSRC-seadmele korralduse saata andmeid sõiduki DSRC-seadmest tagasi REDCR-i. Käsu ECHO eesmärk on võimaldada töökodadel või tüübikinnituskatsete tegijatel kontrollida, kas DSRC-ühendus toimib, ilma et neil oleks vaja juurdepääsu turbemandaatidele.

— **ACTION**.response ECHO: sõiduki DSRC-seadme vastus käsule ECHO.

— **EVENT_REPORT.request** RELEASE: käsk, mis teatab sõiduki DSRC-seadmele, et andmeside on lõppenud. Käsu RELEASE eesmärk on lõpetada seanss sõiduki DSRC-seadmega. Käsu RELEASE saamise järel ei vasta sõiduki DSRC-seade hetkel avatud ühenduse ajal enam edasistele päringutele. Pange tähele, et vastavalt standardile EN 12834 ei loo sõiduki DSRC-seade sama päringusaatjaga ühendust kaks korda, kui see ei ole olnud 255 sekundit väljaspool sidetsooni või kui päringusaatja majaka ID ei ole muutunud.

5.4.3. *Päringukäskude jada*

DSC_36 Käskude ja vastuste jadana saab ühendust kirjeldada järgmiselt:

Järjekorranr	Saatja		Vastuvõtja	Kirjeldus	Toiming
1	REDCR	>	DSRC-VU	Sideühenduse initsialiseerimine nõue	REDCR saadab BST
2	*DSRC-VU*	>	*REDCR*	*Sideühenduse initsialiseerimine vastus*	*Kui BST toetab AID = 2, siis nõuab DSRC-VU privaatakent*
3	REDCR	>	DSRC-VU	Eraldab privaatakna	Saadab privaatakna eraldamist kinnitava kaadri
4	*DSRC-VU*	>	*REDCR*	*Saadab VST*	*Saadab VST-d sisaldava kaadri*
5	REDCR	>	DSRC-VU	Saadab nõude GET.request, et saada kindla EID atribuudis olevaid andmeid	
6	*DSRC-VU*	>	*REDCR*	*Saadab vastuse GET.response soovitud EID atribuudiga*	*Saadab atribuudi (RTMData, OWSData….) koos soovitud EID andmetega*

Järjekorranr	Saatja		Vastuvõtja	Kirjeldus	Toiming
7	REDCR	>	DSRC-VU	Saadab nõude GET.request, et saada muu atribuudi andmeid (vajadusel)	
8	*DSRC-VU*	>	*REDCR*	*Saadab vastuse GET.response koos nõutud atribuudiga*	*Saadab atribuudi koos soovitud EID andmetega*
9	REDCR	>	DSRC-VU	Kinnitab andmete kättesaamise õnnestumist	Saadab käsu RELEASE, mis sulgeb ühenduse
10	*DSRC-VU*			*Sulgeb ühenduse*	

Punktides 5.4.7 ja 5.4.8 on esitatud andmesidejada ja vahetatud raamide näide.

5.4.4. *Andmestruktuurid*

DSC_37 5,8 GHz DSRC-liidese kaudu edastatavate andmete semantiline struktuur peab vastama käesolevas liites esitatud kirjeldusele. Andmete struktureerimist on kirjeldatud käesolevas punktis.

DSC_38 Sisuandmed (RTM-andmed) sisaldavad ühendatud kujul järgmisi andmeid:

1. andmed EncryptedTachographPayload, mis on andmete TachographPayload krüpteeritud vorm vastavalt standardi ASN.1 punktile 5.4.5. Krüpteerimismeetodit on kirjeldatud 11.liites.

2. 11. liites määratletud andmed DSRCSecurityData.

DSC_39 RTM-andmete aadress on RTM Attribute=1 ning need edastatakse andmeümbrises RTM container =10.

DSC_40 RTM Context Mark näitab TARV-standardiseeria toetatud standardi osa (RTM vastab osale 9).

RTM-i rakenduses sisalduvate DSRC andmete ASN.1 mooduli määratlus on järgmine:

```
    TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
    DEFINITIONS AUTOMATIC TAGS
    ::= BEGIN
    IMPORTS
    -- Imports data attributes and elements from EFC which are used for RTM
    LPN
    FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

    -- Imports function parameters from the EFC Application Interface Definition
    SetMMIRq
    FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

    -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
    Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
    Attributes,
    BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
    EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
    ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
    FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


    -- Definitions of the RTM functions:
    RTM-InitialiseComm-Request ::= BST
    RTM-InitialiseComm-Response::= VST
    RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
    ABSENT,  attrIdList})
    RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
    RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
    eventType (0)})

    RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
    (15), accessCredentials ABSENT, iid ABSENT})

    RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
    (0), iid ABSENT})

    -- Definitions of the RTM attributes:
    RtmData ::= SEQUENCE {
          encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
    TachographPayload as per Appendix 11 --}),
          DSRCSecurityData OCTET STRING
          }
    TachographPayload ::= SEQUENCE {
                tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
                tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
                tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
                tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
                tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
                tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
                tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
                tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
                tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                          -- 0= driving selected
                tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
                tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
                tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
    -- All subsequent time related types as defined in Annex 1C.
                tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
                tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
                tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
                tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
                tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
                tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
                tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
                }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                  C1 (1),
                                  C2 (2)
                                  } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                  Ok (1),
                  NoK (2)
                  } SIZE (1..255)
```

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                         [0]    INTEGER,
        bitstring                       [1]    BIT STRING,
        octetstring                     [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString                 [3]    UniversalString,
        beaconId                        [4]    BeaconID,
        t-apdu                          [5]    T-APDUs,
        dsrcApplicationEntityId         [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                     [7]    Dsrc-EID,
        attrIdList                      [8]    AttributeIdList,
        attrList                        [9]    AttributeList{RtmContainer},
        rtmData                         [10]   RtmData,
        rtmContextmark                  [11]   Rtm-ContextMark,
        reserved12                      [12]   NULL,
        reserved13                     [13]   NULL,
        reserved14                      [14]   NULL,
        time                            [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5. *RtmData elemendid, toimingud ja määratlused*

DSC_41 Sõidukiseadme arvutatavad andmeväärtused, mida kasutatakse sõiduki DSRC-seadmes olevate turvatud andmete ajakohastamiseks, arvutatakse vastavalt tabelis 14.3 määratletud reeglitele.

Tabel 14.3.

RtmData, elemendid, toimingud ja määratlused

(1) RTM-i andmeelement	(2) Sõidukiseadme toiming		(3) Andmete määratlus standardis ASN.1
RTM1 **sõiduki numbrimärk**	Sõidukiseade registreerib andmeelemendi *tp15638VehicleRegistrationPlate* väärtuse RTM1 andmeetüübi *VehicleRegistrationIdentification* salvestatud väärtusest vastavalt 1. liitele *VehicleRegistrationIdentification*	Sõiduki numbrimärk, esitatakse märkide stringina	`tp15638VehicleRegstrationPlate LPN, --Vehicle Registration Plate imported from ISO 14906 with the limitation specified in EN 15509 which is a SEQUENCE comprising Country Code followed by an alphabet indicator followed by the plate number itself, which is always 14 octets (padded with zero's) so the EN 15509 LPN type length is always 17 octets, of which 14 are the "real" plate number.`

(1) RTM-i andmeelement	(2) Sõidukiseadme toiming		(3) Andmete määratlus standardis ASN.1
RTM2 **kiiruse ületamise sündmus**	Sõidukiseade loob andmeelemendi RTM2 tp15638SpeedingEvent kohta kahendväärtuse. Sõidukiseade arvutab elemendi tp15638SpeedingEvent väärtuse sõidukiseadmesse salvestatud viimase 10 päeva jooksul esinenud kiiruseületamise sündmuste arvu põhjal vastavalt IC lisale. Kui viimase 10 päeva jooksul on vähemalt üks tp15638SpeedingEvent, määratakse andmeelemendi tp15638SpeedingEvent väärtuseks TRUE. MUUL JUHUL, kui viimase 10 päeva jooksul sündmusi olnud ei ole, määratakse elemendi tp15638SpeedingEvent väärtuseks FALSE.	1 (TRUE) – näitab kiiruse ületamist 10 päeva jooksul	`tp15638speedingEvent BOOLEAN,`
RTM3 **juhtimine ilma kehtiva kaardita**	Sõidukiseade loob andmeelemendi RTM3 tp15638DrivingWithoutValidCard kohta kahendväärtuse. Sõidukiseade määrab muutuja tp15638DrivingWithoutValidCard väärtuseks „True“, kui sõidukiseadmesse on viimase 10 päeva jooksul salvestatud sündmus „vajaliku kaardita juhtimine“, nagu on määratletud IC lisas. MUUL JUHUL, kui viimase 10 päeva jooksul toimunud sündmusi ei ole, määratakse muutuja tp15638DrivingWithoutValidCard väärtuseks FALSE.	1 (TRUE) = näitab vale kaardikasutust	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **kehtiv juhikaart**	Sõidukiseade loob andmeelemendi RTM4 tp15638DriverCard kohta kahendväärtuse vastavalt sõidukiseadmes salvestatud ja 1. liites määratletud andmetele. Kui sõidukiseadmes kehtivat juhikaarti ei ole, määrab sõidukiseade muutuja väärtuseks TRUE. MUUL JUHUL, kui sõidukiseadmes on kehtiv juhikaart, määrab sõidukiseade muutuja väärtuseks FALSE.	0 (FALSE) = näitab kehtiva juhikaardi olemasolu	`tp15638DriverCard BOOLEAN,`
RTM5 **kaardi sisestamine juhtimise ajal**	Sõidukiseade loob andmeelemendi RTM5 kohta kahendväärtuse. Sõidukiseade määrab muutuja tp15638CardInsertion väärtuseks „True“, kui sõidukiseade on viimase 10 päeva jooksul registreerinud vähemalt ühe sündmuse „kaardi sisestamine juhtimise ajal“, nagu on määratletud IC lisas. MUUL JUHUL, kui viimase 10 päeva jooksul selliseid sündmusi ei ole, määratakse muutuja tp15638CardInsertion väärtuseks FALSE.	1 (TRUE) = näitab juhtimise ajal toimunud kaardi sisestamist viimase 10 päeva jooksul	`tp15638CardInsertion BOOLEAN,`
RTM6 **liikumisandmete viga**	Sõidukiseade loob andmeelemendi RTM6 kohta kahendväärtuse. Sõidukiseade määrab muutuja tp15638MotionDataError väärtuseks TRUE, kui sõidukiseadmesse on viimase 10 päeva jooksul salvestatud sündmus „liikumisandmete viga“, nagu on määratletud IC lisas. MUUL JUHUL, kui viimase 10 päeva jooksul selliseid sündmusi ei ole, määratakse muutuja tp15638MotionDataError väärtuseks FALSE.	1 (TRUE) = näitab viimase 10 päeva jooksul esinenud juhtimisandmete viga	`tp15638motionDataError BOOLEAN,`

(1) RTM-i andmeelement	(2) Sõidukiseadme toiming		(3) Andmete määratlus standardis ASN.1
RTM7 **vastuolu sõiduki liikumisandmetes**	Sõidukiseade loob andmeelemendi RTM7 kohta kahendväärtuse. Sõidukiseade määrab muutuja tp15638vehicleMotionConflict väärtuseks TRUE, kui sõidukiseadmesse on viimase 10 päeva jooksul salvestatud vähemalt üks sündmus „vastuolu sõiduki liikumisandmetes“ (väärtusega ‘0A’H). MUUL JUHUL, kui viimase 10 päeva jooksul selliseid sündmusi ei ole, määratakse muutuja tp15638vehicleMotionConflict väärtuseks FALSE.	1 (TRUE) = näitab viimase 10 päeva jooksul esinenud vastuolu liikumisandmetes	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **kaasjuhikaart**	Sõidukiseade loob andmeelemendi RTM8 vastavalt IC lisale („andmed juhi tegevuse kohta“, MEESKOND ja KAASJUHT). Kui sõidukiseadmes on teine kehtiv juhikaart, määrab sõidukiseade muutuja väärtuseks TRUE. MUUL JUHUL, kui teist kehtivat juhikaarti ei ole, määrab sõidukiseade muutuja väärtuseks FALSE.	1 (TRUE) = näitab, et kaasjuhikaart on sisestatud	`tp156382ndDriverCard BOOLEAN,`
RTM9 **hetketegevus**	Sõidukiseade loob andmeelemendi RTM9 kohta kahendväärtuse. Kui sõidukiseadmes salvestatud hetketegevus ei ole „JUHTIMINE“ vastavalt IC lisa määratlusele, määrab sõidukiseade muutuja väärtuseks TRUE. MUUL JUHUL, kui sõidukiseadmes salvestatud hetketegevus on „JUHTIMINE“, määrab sõidukiseade muutuja väärtuseks FALSE.		`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **viimane seanss suletud**	Sõidukiseade loob andmeelemendi RTM10 kohta kahendväärtuse. Kui viimast kaardiseanssi ei suletud nõuetekohaselt vastavalt IC lisa määratlusele, määrab sõidukiseade selle muutuja väärtuseks TRUE. MUUL JUHUL, kui viimane kaardiseanss suleti nõuetekohaselt, määrab sõidukiseade selle muutuja väärtuseks FALSE.	1 (TRUE) = suleti mittenõuetekohaselt; 0 (FALSE) = suleti nõuetekohaselt	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **voolukatkestus**	Sõidukiseade loob andmeelemendi RTM11 kohta täisarvulise väärtuse. Sõidukiseade määrab muutujale tp15638PowerSupplyInterruption väärtuse, mis võrdub voolukatkestuste arvuga vastavalt määruse (EL) nr 165/2014 artiklile 9 ja IC lisas määratletud andmetüübile „voolukatkestus“. MUUL JUHUL, kui viimase 10 päeva jooksul voolukatkestuse sündmusi olnud ei ole, määratakse arvu väärtuseks 0.	— Voolukatkestuste arv viimase 10 päeva jooksul	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

(1) RTM-i andmeelement	(2) Sõidukiseadme toiming		(3) Andmete määratlus standardis ASN.1
RTM12 **anduri tõrge**	Sõidukiseade loob andmeelemendi RTM12 kohta täisarvulise väärtuse. Sõidukiseade määrab muutuja sensorFault väärtuseks: — 1, kui viimase 10 päeva jooksul on registreeritud anduri tõrke sündmus '35'H; — 2, kui viimase 10 päeva jooksul on registreeritud GNSSi vastuvõtja tõrke sündmus (sisemine või väline vastavalt numbriväärtusega '51'H või '52'H); — 3, kui viimase 10 päeva jooksul on registreeritud välise GNSSi side tõrge '53'H; — 4, kui viimase 10 päeva jooksul on registreeritud nii anduri tõrge kui ka GNSSi vastuvõtja tõrge; — 5, kui viimase 10 päeva jooksul on registreeritud nii anduri tõrge kui ka GNSSi välisseadmega side pidamise tõrge; — 6, kui viimase 10 päeva jooksul on registreeritud nii GNSSi vastuvõtja tõrge kui ka GNSSi välisseadmega side pidamise tõrge; — 7, kui viimase 10 päeva jooksul on registreeritud kõik kolm andurite tõrget. MUUL JUHUL, kui viimase 10 päeva jooksul sündmusi registreeritud ei ole, määratakse muutuja väärtuseks 0.	— anduri tõrge, üks oktett vastavalt andmesõnastikule	`tp15638SensorFault INTEGER (0..255),`
RTM13 **aja korrigeerimine**	Sõidukiseade loob andmeelemendi RTM13 kohta täisarvulise väärtuse (1. liite timeReal) sõltuvalt IC lisas määratletud aja korrigeerimise andmete olemasolust. Sõidukiseade määrab selle aja väärtuse, millel toimus viimane aja korrigeerimise sündmus. MUUL JUHUL, kui sõidukiseadme andmed ei sisalda IC lisas määratletud sündmust „aja korrigeerimine", määratakse väärtuseks 0.	Viimase aja korrigeerimise aeg	`tp15638TimeAdjustment INTEGER(0..4294967295),`
RTM14 **turvalisuse rikkumise katse**	Sõidukiseade loob andmeelemendi RTM14 kohta täisarvulise väärtuse (1. liite timeReal) sõltuvalt IC lisas määratletud turvalisuse rikkumise katse sündmuse olemasolust. Sõidukiseade määrab muutujale viimase sõidukiseadmes registreeritud turvalisuse rikkumise katse sündmuse aja. MUUL JUHUL, kui sõidukiseadme andmed ei sisalda IC lisas määratletud sündmust „turvalisuse rikkumise katse", määratakse väärtuseks 0x00FF.	Viimase turvalisuse rikkumise katse aeg — vaikeväärtus =0x00FF	`tp15638LatestBreachAttempt INTEGER(0..4294967295),`
RTM15 **viimane kalibreerimine**	Sõidukiseade loob andmeelemendi RTM15 kohta täisarvulise väärtuse (1. liite timeReal) sõltuvalt IC lisas määratletud viimase kalibreerimise andmete olemasolust. Sõidukiseade määrab muutja väärtuseks viimase kahe kalibreerimise (RTM15 ja RTM16) ajad, mis on määratud 1. liites määratletud andmetüübis VuCalibrationData. Sõidukiseade määrab elemendi RTM15 väärtuseks viimase kalibreerimiskirje andmevälja timeReal väärtuse.	Viimase kalibreerimise andmete aeg	`tp15638LastCalibrationData INTEGER(0..4294967295),`

(1) RTM-i andmeelement	(2) Sõidukiseadme toiming		(3) Andmete määratlus standardis ASN.1
RTM16 **eelmine kalibreerimine**	Sõidukiseade loob andmeelemendi RTM16 kohta täisarvulise väärtuse (1. liite timeReal) sõltuvalt IC lisas määratletud viimasele kalibreerimisele eelnenud kalibreerimise andmete olemasolust. MUUL JUHUL, kui eelmist kalibreerimist ei ole toimunud, määrab sõidukiseade elemendi RTM16 väärtuseks 0.	Eelmise kalibreerimise andmete aeg	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **sõidumeeriku ühendamise kuupäev**	Sõidukiseade loob andmeelemendi RTM17 kohta täisarvulise väärtuse (1. liite timeReal). Sõidukiseade määrab aja väärtuseks sõidukiseadme algse paigalduse aja. Sõidukiseade võtab vastavad andmed andmetüübist VuCalibrationData (1. liide), mis asub kirjes vuCalibrationRecords, mille välja CalibrationPurpose väärtus on: '03'H	Sõidumeeriku ühendamise kuupäev	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **hetkekiirus**	Sõidukiseade loob andmeelemendi RTM18 kohta täisarvulise väärtuse. Sõidukiseade määrab elemendi RTM16 väärtuseks RtmData viimase ajakohastamise ajal registreeritud hetkekiiruse väärtuse.	Viimane registreeritud hetkekiirus	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **ajatempel**	Sõidukiseade loob andmeelemendi RTM19 kohta täisarvulise väärtuse (1. liite timeReal). Sõidukiseade määrab elemendi RTM19 väärtuseks RtmData viimase ajakohastamise aja.	Viimase kirje TachographPayload ajatempel	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6. *Andmete edastamise mehhanism*

DSC_42 REDCR nõuab eespool määratletud andmeid pärast initsialiseerimise etappi ning sõiduki DSRC-seade edastab need seejärel eraldatud aknas. REDCR kasutab andmete saamiseks käsku GET.

DSC_43 Kõigis DSRC andmevahetustes kodeeritakse andmed reeglite PER (*Packed Encoding Rules*) kohaselt.

5.4.7. *DSRC-andmeside üksikasjalik kirjeldus*

DSC_44 Initsialiseerimine tehakse vastavalt nõuetele DSC_44–DSC_48 ja tabelitele 14.4–14.9. Initsialiseerimise etapis saadab REDCR kaadri, mis sisaldab majakateenuste tabelit BST vastavalt standardile EN 12834 ja standardi EN 13372 punktidele 6.2, 6.3, 6.4 ja 7.1, kasutades tabelis 14.4 määratletud seadistusi.

Tabel 14.4.

Initsialiseerimine – BST kaadri seadistused

Väli	Seadistus
Link Identifier	Leviaadress
BeaconId	Vastavalt standardile EN 12834
Time	Vastavalt standardile EN 12834
Profile	Ilma laiendite, kasutatakse 0 või 1
MandApplications	Ilma laiendita, EID puudub, parameeter puudub, AID = 2 Freight&Fleet
NonMandApplications	Puudub
ProfileList	Ilma laiendita, loendis olevate profiilide arv = 0
Fragmentation header	Fragmenteerimine puudub
Layer 2 settings	Käsu PDU, UI käsk

Tabelis 14.5 on esitatud tabelis 14.4 määratletud seadistuste praktiline näide koos bitikoodidega.

Tabel 14.5.

Initsialiseerimine – BST kaadri sisu näide

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
1	FLAG	0111 1110	Algussilt
2	Broadcast ID	1111 1111	Leviaadress
3	MAC Control Field	1010 0000	Käsu PDU
4	LLC Control field	0000 0011	UI käsk
5	Fragmentation header	1xxx x001	Fragmenteerimine puudub

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
6	BST	1000	Initsialiseerimisnõue
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	NonMand rakendusi ei ole
		xxx	Tootja identifikaator
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	Tootja kohta on saadaval 27-bitine ID
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32-bitine UNIX, reaalaeg
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,…)	0000 0000	Ilma laiendita. Näidisprofiil 0
17	MandApplications SEQUENCE (SIZE(0..127, …)) OF {	0000 0001	Ilma laiendita, mandApplications arv = 1
18	SEQUENCE {		
	OPTION indicator	0	EID puudub
	OPTION indicator	0	Parameeter puudub
	AID DSRCApplicationEntityID } }	00 0010	Ilma laiendita; AID = 2 Freight&Fleet

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
19	ProfileList SEQUENCE (0..127,…) OF Profile }	0000 0000	Ilma laiendita, loendis olevate profiilide arv = 0
20	FCS	xxxx xxxx	Kaadrikontrolli jada
21		xxxx xxxx	
22	Flag	0111 1110	Lõpusilt

DSC_45 Pärast BST saamist nõuab sõiduki DSRC-seade privaatakna eraldamist vastavalt standardile EN 12795 ja standardi EN 13372 punktile 7.1.1, ilma kindlate RTM-i seadistusteta. Tabelis 14.6 on esitatud bitikoodide näide.

Tabel 14.6.

Initsialiseerimine – privaatakna eraldamist nõudva kaadri sisu

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
1	FLAG	0111 1110	Algussilt
2	Private LID	xxxx xxxx	Konkreetse DSRC-VU ühendusaadress
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Privaatakna nõue
7	FCS	xxxx xxxx	Kaadrikontrolli jada
8		xxxx xxxx	
9	Flag	0111 1110	Lõpusilt

DSC_46 Seejärel vastab REDCR privaatakna eraldamisega vastavalt standardile EN 12795 ja standardi EN 13372 punktile 7.1.1, ilma kindlate RTM-i seadistusteta.

Tabelis 14.7 on esitatud bitikoodide näide.

Tabel 14.7.

Initsialiseerimine – privaatakna eraldamist kinnitava kaadri sisu

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
1	FLAG	0111 1110	Algussilt
2	Private LID	xxxx xxxx	Konkreetse DSRC-VU ühendusaadress
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Privaatakna eraldamine
7	FCS	xxxx xxxx	Kaadrikontrolli jada
8		xxxx xxxx	
9	Flag	0111 1110	Lõpusilt

DSC_47 Pärast privaatakna eraldamist saadab sõiduki DSRC-seade eraldatud edastusakna kaudu oma VST (sõidukiteenuste tabel) vastavalt standardile EN 12834 ja standardi EN 13372 punktidele 6.2, 6.3, 6.4 ja 7.1, koos tabelis 14.8 määratletud seadistusega.

Tabel 14.8.

Initsialiseerimine – VST kaadri seadistused

Väli	Seadistus
Private LID	Vastavalt standardile EN 12834
VST parameters	Täiteväärtus = 0, seejärel iga toetatud rakenduse kohta: olemasolev EID, olemasolev parameeter,AID=2, OBU poolt loodud EID
Parameter	Ilma laiendita, sisaldab kirjet RTM Context Mark
ObeConfiguration	Vabatahtlik väli ObeStatus võib olemas olla, aga REDCR seda ei kasuta
Fragmentation header	Fragmenteerimine puudub
Layer 2 settings	Käsu PDU, UI käsk

DSC_48 Sõiduki DSRC-seade toetab rakendust „Freight and Fleet“, mille rakendusidentifikaator on ‘2’. Muude rakendusidentifikaatorite toetus võib olla võimalik, kuid neid ei esitata selles VST-s, kuna BST nõuab ainult AID = 2. Väli „Applications“ sisaldab sõiduki DSRC-seadmes toetatud rakenduste eksemplaride nimekirja. Iga toetatud rakenduse eksemplari puhul esitatakse viide vastavale standardile, mis koosneb märgist RTM Context Mark, mille sisuks on seotud standardile vastav OBJECT IDENTIFIER, standardi osa number (RTM-i puhul 9) ja vajadusel selle versioon ning lisaks sõiduki DSRC-seadme loodud ja selle rakenduse eksemplariga seotud EID.

Tabelis 14.9 on esitatud tabelis 14.8 määratletud seadistuste praktiline näide koos bitikoodidega.

Tabel 14.9.

Initsialiseerimine – VST kaadri sisu näide

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
1	FLAG	0111 1110	Algussilt
2	Private LID	xxxx xxxx	Konkreetse DSRC-VU ühendusaadress
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	Käsu PDU
7	LLC Control field	0000 0011	UI käsk
8	Fragmentation header	1xxx x001	Fragmenteerimine puudub
9	VST SEQUENCE {	1001	Initsialiseerimise vastus
	Fill BIT STRING (SIZE(4))	0000	Kasutamata, väärtuseks on määratud 0
10	Profile INTEGER (0..127,…) Applications SEQUENCE OF {	0000 0000	Ilma laiendita. Näidisprofiil 0
11		0000 0001	Ilma laiendita, 1 rakendus
12	SEQUENCE {		
	OPTION indicator	1	Olemasolev EID
	OPTION indicator	1	Olemasolev parameeter
	AID DSRCApplicationEntityID	00 0010	Ilma laiendita. AID = 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Määratletakse OBU-s ja idendib rakenduse eksemplari

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
14	Parameter Container {	0000 0010	Ilma laiendita, ümbrise valik = 02, oktetistring
15		0000 1000	Ilma laiendita, kirje Rtm Context Mark pikkus = 8
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	Toetatud standardi osa ja versiooni objekti identifikaator: Näide: ISO (1) standard (0) TARV (15638) osa 9 (9) versioon 1 (1). Esimene oktett on 06H ehk objekti identifikaator; teine on 06H ehk pikkus. Järgmises kuues oktetis esitatakse näite objekti identifikaatori kood. Pange tähele, et olemas on ainult jada üks element (vabatahtlik element RtmCommProfile on välja jäetud)
17		0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence {		
	OPTION indicator	0	ObeStatus puudub
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	DSRC-VU tootja identifikaator vastavalt standardi ISO 14816 registris esitatud kirjeldusele
27		xxxx xxxx	
28	FCS	xxxx xxxx	Kaadrikontrolli jada
29		xxxx xxxx	
30	Flag	0111 1110	Lõpusilt

DCS_49 Seejärel loeb REDCR andmeid, saates käsu GET, mis vastab standardi EN 13372 punktides 6.2, 6.3, 6.4 ja standardis EN 12834 määratletud käsule GET, kasutades tabelis 14.10 määratletud seadistusi.

Tabel 14.10.

Esitamine – GET-nõude kaadri seadistused

Väli	Seadistus
Invoker Identifier (IID)	Puudub
Link Identifier (LID)	Konkreetse DSRC-VU ühendusaadress
Chaining	Pole

Väli	Seadistus
Element Identifier (EID)	Vastavalt VST-le. Ilma laiendita
Access Credentials	Pole
AttributeIdList	Ilma laiendita, 1 atribuut, AttributeID = 1 (RtmData)
Fragmentation	Pole
Layer2 settings	Käsu PDU, pollitud ACn käsk

Tabelis 14.11 on esitatud RTM-andmete lugemise näide.

Table 14.11.

Esitamine – GET-nõude kaadri näide

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
1	FLAG	0111 1110	Algussilt
2	Private LID	xxxx xxxx	Konkreetse DSRC-VU ühendusaadress
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Käsu PDU
7	LLC Control field	n111 0111	Pollitud ACn käsk, bitt n
8	Fragmentation header	1xxx x001	Fragmenteerimine puudub
9	Get.request SEQUENCE {	0110	GET-nõue
	OPTION indicator	0	Juurdepääsumandaadid puuduvad
	OPTION indicator	0	IID puudub
	OPTION indicator	1	Olemasolev AttributeIdList
	Fill BIT STRING(SIZE(1))	0	Väärtuseks on määratud 0
10	EID INTEGER(0..127,…)	xxxx xxxx	RTM-rakenduse eksemplari EID, vastavalt VST-le; ilma laiendita
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Ilma laiendita, atribuutide arv = 1
12		0000 0001	AttributeId=1, RtmData; ilma laiendita

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
13	FCS	xxxx xxxx	Kaadrikontrolli jada
14		xxxx xxxx	
15	Flag	0111 1110	Lõpusilt

DSC_50 Pärast GET-nõude saamist saadab sõiduki DSRC-seade nõutud andmetega GET-vastuse, standardi EN 13372 punktides 6.2, 6.3, 6.4 ja standardis EN 12834 määratletud GET-vastusele, kasutades tabelis 14.12 määratletud seadistusi.

Tabel 14.12.

Esitamine – GET-vastuse kaadri seadistused

Väli	Seadistus
Invoker Identifier (IID)	Puudub
Link Identifier (LID)	Vastavalt standardile EN 12834
Chaining	Pole
Element Identifier (EID)	Vastavalt VST-le.
Access Credentials	Pole
Fragmentation	Pole
Layer2 settings	Vastuse PDU, vastus on saadaval ja käsk on vastu võetud, ACn käsk

Tabelis 14.13 on esitatud RTM-andmete lugemise näide.

Table 14.13.

Esitamine – Vastuse kaadri sisu näide

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
1	FLAG	0111 1110	Algussilt
2	Private LID	xxxx xxxx	Konkreetse DSRC-VU ühendusaadress
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
6	MAC Control field	1101 0000	Vastuse PDU
7	LLC Control field	n111 0111	Vastus saadaval, ACn käsu bitt n
8	LLC Status field	0000 0000	Vastus on saadaval ja käsk on vastu võetud
9	Fragmentation header	1xxx x001	Fragmenteerimine puudub
10	Get.response SEQUENCE {	0111	Käsu GET vastus
	OPTION indicator	0	IID puudub
	OPTION indicator	1	Olemasolev atribuudinimekiri
	OPTION indicator	0	Tagastuse olek puudub
	Fill BIT STRING(SIZE(1))	0	Ei kasutata
11	EID INTEGER(0..127,…)	xxxx xxxx	RTM-rakenduse eksemplarist vastamine. Ilma laiendita
12	AttributeList SEQUENCE OF {	0000 0001	Ilma laiendita, atribuutide arv = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Ilma laiendita, AttributeId=1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Ilma laiendita, ümbrise valik = 10_{10}
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Kaadrikontrolli jada
n+2		xxxx xxxx	
n+3	Flag	0111 1110	Lõpusilt

DSC_51 Seejärel sulgeb REDCR ühenduse käsuga EVENT_REPORT, RELEASE, mis vastab standardi EN 13372 punktidele 6.2, 6.3, 6.4 ja standardi EN 12834 punktile 7.3.8, ilma kindlate RTM-i seadistusteta. Tabelis 14.14 on esitatud käsu RELEASE bitikoodide näide.

Tabel 14.14.

Lõpetamine. Kaadri EVENT_REPORT Release sisu

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
1	FLAG	0111 1110	Algussilt
2	Private LID	xxxx xxxx	Konkreetse DSRC-VU ühendusaadress
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1000 s000	Kaader sisaldab käsu LPDU-d
7	LLC Control field	0000 0011	UI käsk
8	Fragmentation header	1xxx x001	Fragmenteerimine puudub
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Juurdepääsumandaadid puuduvad
	OPTION indicator	0	Sündmuse parameeter puudub
	OPTION indicator	0	IID puudub
	Mode BOOLEAN	0	Vastust ei oodata
10	EID INTEGER (0..127,…)	0000 0000	Ilma laiendita, EID = 0 (System)
11	EventType INTEGER (0..127,…) }	0000 0000	Sündmuse tüüp 0 = Release
12	FCS	xxxx xxxx	Kaadrikontrolli jada
13		xxxx xxxx	
14	Flag	0111 1110	Lõpusilt

DSC_52 Sõiduki DSRC-seade ei pea Release-käsule vastama. Seejärel andmeside lõpetatakse.

5.4.8. *DSRC-katseseansi kirjeldus*

DSC_53 Volitatud isikud, kellel on õigus kasutada turbeprotseduure, peavad läbi viima täielikud, turbeandmeid hõlmavad katsed vastavalt 11. liitele „Ühised turbemehhanismid“, kasutades eespool määratletud tavapärast GET-käsku.

DSC_54 Kasutusele võtmise ja korraliste ülevaatuste ajal korraldatavad katsed, mis eeldavad dekrüpteerimist ja dekrüpteeritud andmete sisu mõistmist, tehakse vastavalt 11. liitele „Ühised turbemehhanismid“ ja 9. liitele „Tüübikinnitus: minimaalselt nõutavate katsete nimekiri“.

Lihtsat DSRC andmesidet saab katsetada ka ainult käsuga ECHO. Sellised katsed võivad olla nõutavad kasutusele võtmise või korraliste ülevaatuste ajal või muul juhul vastavalt pädeva kontrolliasutuse või määruse (EL) nr 165/2014 nõuetele (vt allpool 6. peatükk).

DSC_55 Lihtsa andmeside katse tegemiseks saadab REDCR seansi ajal, st pärast initsialiseerimise etapi edukat lõpetamist, käsu ECHO. Toimingute järjestus sarnaneb päringu saatmise olukorraga:

— Etapp 1 REDCR saadab välja „majakateenuste tabeli“ (BST), milles on toetatavate teenuste rakendusidentifikaatorid (AID). RTM-rakendustes on selleks lihtsalt teenus, mille AID väärtus = 2.

Sõiduki DSRC-seade hindab saadud BST-d ning kui BST-s nõutakse domeeni Freight&Fleet (AID = 2) andmeid, saadab sõiduki DSRC-seade vastuse. Kui REDCR ei paku identifikaatorit AID = 2, siis sõiduki DSRC-seade sulgeb ühenduse REDCR-iga.

— Etapp 2 sõiduki DSRC-seade saadab nõude privaatakna eraldamiseks.

— Etapp 3 REDCR saadab privaatakna eraldamise kinnituse.

— Etapp 4 sõiduki DSRC-seade kasutab eraldatud privaatakent, et saata välja oma sõidukiteenuste tabel (VST). VST sisaldab loetelu kõigist rakenduste eksemplaridest, mida sõiduki DSRC-seade AID = 2 raamistikus toetab. Erinevate eksemplaride eristamiseks kasutatakse kordumatuid elemendi identifikaatoreid (EID), millest igaüks on seotud mõne parameetri väärtusega, mis näitab toetatavat rakendust.

— Etapp 5 seejärel analüüsib REDCR pakutud VST-d ning lõpetab ühenduse (käsk RELEASE), kui ta ei ole huvitatud VST-s pakutavast (st VST saatja on sõiduki DSRC-seade, mis ei ole RTM-funktsiooniga sõidukiseade), või sobiva VST saamise korral käivitab rakenduse eksemplari.

— Etapp 6 REDCR saada konkreetsele sõiduki DSRC-seadmele käsu (ECHO) ning eraldab privaatakna.

— Etapp 7 sõiduki DSRC-seade kasutab uut privaatakent ECHO vastuse kaadri saatmiseks.

Järgmistes tabelites on esitatud käsuga ECHO seotud seansside praktiline näide.

DSC_56 Initsialiseerimine tehakse vastavalt punktile 5.4.7 (DSC_44–DSC_48) ja tabelitele 14.4–14.9.

DSC_57 Seejärel saadab REDCR standardile 14906 vastava käsu ACTION, ECHO, mis sisaldab 100 andmeoktetti ja ei sisalda kindlaid RTM-i seadistusi. Tabelis 14.15 on esitatud REDCR saadetud kaadri sisu.

Tabel 14.15.

Nõude ACTION, ECHO kaadri näide

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
1	FLAG	0111 1110	Algussilt
2	Private LID	xxxx xxxx	Konkreetse DSRC-VU ühendusaadress
3		xxxx xxxx	

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Käsu PDU
7	LLC Control field	n111 0111	Pollitud ACn käsk, bitt n
8	Fragmentation header	1xxx x001	Fragmenteerimine puudub
9	ACTION.request SEQUENCE {	0000	Toimingu nõue (ECHO)
	OPTION indicator	0	Juurdepääsumandaadid puuduvad
	OPTION indicator	1	Olemasolev toimingu parameeter
	OPTION indicator	0	IID puudub
	Mode BOOLEAN	1	Oodatakse vastust
10	EID INTEGER (0..127,…)	0000 0000	Ilma laiendita, EID = 0 (System)
11	ActionType INTEGER (0..127,…)	0000 1111	Ilma laiendita, toimingu tüüp: ECHO nõue
12	ActionParameter CONTAINER {	0000 0010	Ilma laiendita, ümbrise valik = 2
13		0110 0100	Ilma laiendita, stringi pikkus = 100 oktetti
14		xxxx xxxx	ECHO-käsuga edastatavad andmed
…		…	
113	}}	xxxx xxxx	
11-46-14	FCS	xxxx xxxx	Kaadrikontrolli jada
11-57-15		xxxx xxxx	
11-68-16	Flag	0111 1110	Lõpusilt

DSC_58 Pärast ECHO-nõude saamist saadab sõiduki DSRC-seade 100 andmeoktetist koosneva ECHO vastuse, peegeldades saadud käsu tagasi vastavalt standardile ISO 14906 ilma kindlate RTM-i seadistusteta. Tabelis 14.16 on esitatud käsu bitikoodide näide.

Tabel 14.16.

Vastuse ACTION, ECHO kaadri näide

Okteti nr	Atribuut/väli	Okteti bitid	Kirjeldus
1	FLAG	0111 1110	Algussilt
2	Private LID	xxxx xxxx	Konkreetse VU ühendusaadress
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	Vastuse PDU
7	LLC Control field	n111 0111	ACn käsk, bitt n
8	LLC status field	0000 0000	Vastus saadaval
9	Fragmentation header	1xxx x001	Fragmenteerimine puudub
10	ACTION.response SEQUENCE {	0001	Toimingu vastus (ECHO)
	OPTION indicator	0	IID puudub
	OPTION indicator	1	Olemasolev vastuse parameeter
	OPTION indicator	0	Tagastuse olek puudub
	Fill BIT STRING (SIZE (1))	0	Ei kasutata.
11	EID INTEGER (0..127,…)	0000 0000	Ilma laiendita, EID = 0 (System)
12	ResponseParameter CONTAINER {	0000 0010	Ilma laiendita, ümbrise valik = 2
13		0110 0100	Ilma laiendita, stringi pikkus = 100 oktetti
14		xxxx xxxx	Käsuga ECHO saadetud andmed
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Kaadrikontrolli jada
115		xxxx xxxx	
116	Flag	0111 1110	Lõpusilt

5.5. **Direktiivi 2015/719 tugi**

5.5.1. *Ülevaade*

DSC_59 Maanteesõidukite maksmaalmõõtmeid ja täismassi käsitleva direktiivi 2015/719 toetamiseks kasutatakse sõidukisisese kaalumissüsteemi andmete ja RTM-andmete (vt punkt 5.4.1) allalaadimiseks sama 5,8 GHz DSRC-liidese ühendust. Ainus erinevus seisneb selles, et TARV-standardiga seotud objekti identifikaator osutab standardi ISO 15638 (TARV) osale 20, milles käsitletakse sõidukisiseseid kaalumissüsteeme.

5.5.2. *Käsud*

DSC_60 Sõidukisisese kaalumissüsteemi andmete edastamise käsud on samad, mida kasutatakse RTM-andmesides.

5.5.3. *Päringukäskude jada*

DSC_61 Sõidukisisese kaalumissüsteemi andmete päringukäskude jada on sama, mida kasutatakse RTM-andmete puhul.

5.5.4. *Andmestruktuurid*

DSC_62 Sõidukisisese kaalumissüsteemi andmed (OwsData) sisaldavad ühendatud kujul järgmisi andmeid:

1. andmed EncryptedOwsPayload, mis on andmete OwsPayload krüpteeritud vorm vastavalt standardi ASN.1 punktile 5.5.5. Kasutatakse sama krüpteerimismeetodit mida RtmData puhul ja mis on määratletud 11. liites;

2. DSRCSecurityData, mis arvutatakse RtmData puhul kasutatavate algoritmidega, mis on määratletud 11. liites.

5.5.5. *Sõidukisisese kaalumissüsteemi DSRC-andmeside ASN.1 moodul*

DSC_63. RTM-i rakenduses sisalduvate DSRC andmete ASN.1 mooduli määratlus on järgmine:

```
   TarvOws {iso(1) standard(0) 15638 part20(20)
   version1(1)} DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for OWS
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

   -- Definitions of the OWS functions:
   OWS-InitialiseComm-Request ::= BST
   OWS-InitialiseComm-Response::= VST
   OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
   ABSENT, iid ABSENT, attrIdList})
   OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})
   OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})
   OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the OWS attributes:
   OwsData :: = SEQUENCE {
        encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
   OwsPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   OwsPayload :: = SEQUENCE {
              tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
              recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
   goods vehicle                                                          -- with 10 Kg
   resolution.
              axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                  -- of axles for 10 axles.
              axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                                -- with 10 Kg resolution.
              tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
        }

Ows-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
        }

StandardIdentifier ::= OBJECT IDENTIFIER
  OwsContainer ::= CHOICE {
        integer                       [0]    INTEGER,
        bitstring                     [1]    BIT STRING,
        octetstring                   [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString               [3]    UniversalString,
        beaconId                      [4]    BeaconID,
        t-apdu                        [5]    T-APDUs,
        dsrcApplicationEntityId       [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                   [7]    Dsrc-EID,
        attrIdList                    [8]    AttributeIdList,
        attrList                      [9]    AttributeList{RtmContainer},
        reserved10                    [10]   NULL,
        OwsContextmark                [11]   Ows-ContextMark,
        OwsData                       [12]   OwsData,
        reserved13                    [13]   NULL,
        reserved14                    [14]   NULL,
        time                          [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.5.6. *OwsData elemendid, toimingud ja määratlused*

OwsData elemendid on määratletud maanteesõidukite maksimaalmõõtmeid ja täismassi käsitleva direktiivi 2015/719 toetamise eesmärgil. Nende tähendus on järgmine:

— recordedWeight on raskeveoki mõõdetud kogumass eraldusvõimega 10 kg vastavalt standardile EN ISO 14906. Näiteks väärtus 2500 vastab massile 25 tonni.

— axlesConfiguration vastab raskeveoki konfiguratsioonile, mida näitab telgede arv. Konfiguratsiooni näidatakse 20-bitise bitimaski abil (tuletatud standardist EN ISO 14906).

2-bitine bitimask näitab telgede konfiguratsiooni järgmises vormingus:

— Väärtus 00B tähendab, et „väärtus puudub“, kuna sõidukil ei ole telgedele mõjuva massi andmete kogumiseks vajalikke seadmeid.

— Väärtus 01B tähendab, et telg puudub.

— Väärtus 10B tähendab, et telg on olemas ja sellele mõjuv mass on arvutatud, vastavad andmed on kogutud ja need esitatakse väljal axlesRecordedWeight.

— Väärtus 11B on reserveeritud tulevikus kasutamiseks.

Viimased neli bitti on reserveeritud tulevikus kasutamiseks.

Telgede arv										
Veduki telgede arv			Haagise telgede arv							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 bitti)

— axlesRecordedWeight näitab iga telje kohta registreeritud massi eraldusvõimega 10 kg. Iga telje kohta kasutatakse kahte oktetti. Näiteks väärtus 150 vastab massile 1 500 kg.

Muud andmetüübid on määratletud punktis 5.4.5.

5.5.7. *Andmete edastamise mehhanism*

DSC_64 Sõidukisisese kaalumissüsteemi andmete edastamise mehhanism päringusaatja ja sõiduki DSRC-seadme vahel on sama, mida kasutatakse RTM-andmete jaoks (vt punkt 5.4.6).

DSC_65 Täismassi andmeid koguva platvormi ja sõiduki DSRC-seadme vaheline andmeedastus peab põhinema füüsilistel ühendustel ja liidestel ning punktis 5.6 määratletud protokollil.

5.6. **Sõiduki DSRC-seadme ja sõidukiseadme vaheline andmeedastus**

5.6.1. *Füüsilised ühendused ja liidesed*

DSC_66 Sõidukiseadme ja sõiduki DSRC-seadme vaheline ühendus võidakse luua füüsilise kaabli või Bluetooth v4.0 BLE põhjal toimiva lähitoimelise raadioside abil.

DSC_67 Füüsilise ühenduse ja liidese valikust olenemata peavad olema täidetud järgmised nõuded:

DSC_68 a) et võimaldada sõidukiseadmete ja sõiduki DSRC-seadmete ja nende erinevate partiide tellimist erinevatelt tootjatelt, peab sõidukiseadme ja sõiduki DSRC-seadme ühendus vastama avatud standardile. Sõidukiseade kasutab sõiduki DSRC-seadmega ühenduse loomiseks:

i) vähemalt 2 meetri pikkust fikseeritud kaablit, millel on sõiduki DSRC-seadmest lähtuv sirge 11 kontaktiga DIN 41612 H11 pistik, mis sobib sõidukiseadmel oleva DIN/ISO standardi nõuetele vastava pistikupesaga;

ii) Bluetoothi Low Energy (BLE) protokolli;

iii) standardset ISO 11898 või SAE J1939 kohast ühendust;

DSC_69 b) sõidukiseadme ja sõiduki DSRC-seadme vaheliste liideste ja ühenduste määratlus peab toetama punktis 5.6.2 määratletud rakendusprotokolli käske;

DSC_70 c) sõidukiseade ja sõiduki DSRC-seadme töönäitajad ja energiavarustus peavad toetama andmeedastust valitud ühenduse kaudu.

5.6.2. *Rakendusprotokoll*

DSC_71 Sõidukiseadme ja sõiduki DSRC-seadme vahelise rakendusprotokolli ülesanne on edastada sõidukiseadme andmeid regulaarselt DSRC-seadmesse.

DSC_72 Määratletud on järgmised põhilised käsud:

1. Sideühenduse initsialiseerimine – nõue
2. Sideühenduse initsialiseerimine – vastus
3. RTM-rakenduse identifikaatoriga andmete ja RTM andmete sisu saatmine
4. Andmete kättesaamise jaatamine
5. Sideühenduse lõpetamine – nõue
6. Sideühenduse lõpetamine – vastus

DSC_73 Standardi ASN1.0 kohaselt võib eespool nimetatud käsud määratleda järgmiselt:

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 Käskude ja parameetrite kirjeldus on järgmine:

— RCDT-Communication Link Initialization – Request – kasutatakse sideühenduse initsialiseerimiseks. Käsu saadab sõidukiseade sõiduki DSRC-seadmesse. Sõidukiseade määrab identifikaatori LinkIdentifier ning edastab selle sõiduki DSRC-seadmele, et jälgida seda konkreetset sideühendust.

(Märkus: selle eesmärk on toetada tulevasi ühendusi ja muid rakendusi/mooduleid, nagu sõidukisisene kaalumine).

— RCDT-Communication Link Initialization – Response – sõiduki DSRC-seade saadab sellega vastuse sideühenduse initsialiseerimise nõudele. Käsu saadab sõiduki DSRC-seade sõidukiseadmesse. Käsk näitab initsialiseerimise tulemust vastusena = 1 (õnnestus) või =0 (ebaõnnestus).

DSC_75 Sideühendus initsialiseeritakse alles pärast sõidukiseadme paigaldamist ja kalibreerimist ning mootori/sõidukiseadme sisselülitamist.

— RCDT-Send Data – selle käsuga saadab sõidukiseade allkirjastatud RCDTData (kaugsideandmed) sõiduki DSRC-seadmesse. Andmed saadetakse iga 60 sekundi järel. Parameeter DataTransactionId võimaldab identida konkreetse andmeedastuse. Kasutatakse ka identifikaatorit LinkIdentifier, et veenduda ühenduse õigsuses.

— RCDT-Data Acknowledgment – selle saadab sõiduki DSRC-seade, et anda sõidukiseadmele tagasisidet käsuga RCDT-Send Data , mis identitakse parameetri DataTransactionId järgi, saadetud andmete kättesaamise kohta. Vastuse parameeter on 1 (õnnestus) või = 0 (ebaõnnestus). Kui sõidukiseade saab rohkem kui kolm 0-ga võrduvat vastust või kui sõidukiseade ei saa konkreetse DataTransactionId-ga RCDT-Send Data andmete kättesaamise kohta kinnitust, loob ja registreerib sõidukiseade uue sündmuse.

— RCDT-Communication Link Termination request – selle saadab sõidukiseade sõiduki DSRC-seadmele, et lõpetada kindla identifikaatoriga LinkIdentifier ühendus.

DSC_76 Sõiduki DSRC-seadme või sõidukiseadme taaskäivitamisel tuleb kõik olemasolevad sideühendused eemaldada, kuna sõidukiseadme ootamatu väljalülitumise korral võib sinna jääda „rippuvaid“ ühendusi.

— RCDT-Communication Link Termination – Response – selle saadab sõiduki DSRC-seade sõidukiseadmele, et kinnitada kindla identifikaatoriga LinkIdentifier ühenduse lõpetamine.

5.7. **Vigade töötlemine**

5.7.1. *Andmete registreerimine ja edastamine sõiduki DSRC-seadmes*

DSC_77 Andmed edastatakse sõiduki DSRC-seadmele juba VUSM-funktsiooniga turvatud kujul. VUSM kontrollib, kas sõiduki DSRC-seadmes registreeritud andmed on registreeritud õigesti. Andmete sõidukiseadmest sõiduki DSRC-seadme mällu edastamisel esinenud vigade registreerimisel ja neist teatamisel kasutatakse andmetüüpi EventFaultType, mille arvuliseks väärtuseks määratakse ‘62’H (kaugsidemooduliga side pidamise viga), ning lisatakase ajatempel.

DSC_78 Sõidukiseade säilitab sõidukiseadme sisemiste side tõrgete registreerimiseks kordumatu nimega faili, mida kontrollijatel oleks lihtne tuvastada.

DSC_79 Kui VUPM püüab saada sõidukiseadme andmeid turbemoodulist (et edastada need sõiduki DSRC-seadmele), kui see ei õnnestu, kasutab ta vea registreerimiseks andmetüüpi EventFaultType ja määrab arvuliseks väärtuseks ‘62’H (kaugsidemooduliga side pidamise viga) ning lisab ajatempli. Andmeside tõrge tuvastatakse juhul, kui sõnumit RCDT Data Acknowledgment ei saada seotud (st sõnumites Send Data ja Acknowledgment kattuva DataTransactionId-ga) andmete saatmise käsu RCDT Send Data vastuseks rohkem kui kolmel järjestikusel korral.

5.7.2. *Raadioside vead*

DSC_80 Sidevigade käsitlemine peab toimuma kooskõlas seotud DSRC standarditega: EN 300 674-1, EN 12253, EN 12795, EN 12834 ja standardi EN 13372 sobivad parameetrid.

5.7.2.1. *Krüpteerimis- ja allkirjavead*

DSC_81 Krüpteerimis- ja allkirjavigu töödeldakse vastavalt 11. liitele „Ühised turbemehhanismid“ ning neid ei lisata veateadetele, mis on seotud andmeedastusega DSRC kaudu.

5.7.2.2. *Vigade registreerimine*

DSRC on dünaamiline raadiosidevahend, mida kasutatakse muutuvate atmosfääri- ja häiretingimustega keskkonnas, eriti kui on tegemist kaasaskantava REDCR-i ja liikuva sõiduki kombinatsiooniga. Seetõttu tuleb teha kindlaks erinevus „lugemistõrke“ ja „vea“ vahel. Juhtmeta liidese kaudu toimuvas andmeedastuses on lugemistõrked sagedased ja nende korral tehakse tavaliselt uues katse, st saadetakse uuesti BST ning püütakse käsujada korrata. Enamikul juhtudel lõpeb see õnnestunud andmesideühenduse loomise ja andmete edastamisega, välja arvatud juhul, kui huvi pakkuv sõiduk liigub kordusedastuseks vajaliku aja jooksul levialast välja. (Üks õnnestunud lugemise juhtum võib hõlmata mitut katset ja korduskatset.)

Lugemistõrge võib tekkida seetõttu, et antennid ei ole korralikult ühendatud („sihtimisviga“), üks antennidest on varjestatud – see võib olla tahtlik või olla tingitud teise sõiduki füüsilisest lähedusest, esinevad raadiohäired, eriti sagedusala 5,8 GHz lähedasel alal töötavate WiFi-võrkude või muude avalike raadiosidevõrkude mõjul, esinevad radarihäired või rasked atmosfääritingimused (nt äike) või lihtsalt seepärast, et sõiduk liigub DSRC levialast välja. Üksikuid lugemistõrgete esinemisjuhte ei ole võimalik põhimõtteliselt registreerida, sest sel juhul andmesidet lihtsalt ei toimunud.

Kui aga pädeva kontrolliasutuse esitaja suunab antenni sõidukile ja püüab selle DSRC-seadmele päringut esitada, kuid õnnestunud andmeedastust ei järgne, võib tõrke põhjuseks olla tahtlik manipuleerimine seadmetega, mistõttu pädeva kontrolliasutuse esindaja vajab vahendeid tõrke registreerimiseks ning tagapool paiknevate kolleegide teavitamiseks võimalikust rikkumisest. Kolleegid saavad sel juhul sõiduki peatada ja seda füüsiliselt kontrollida. Kuna aga andmeside loomine ei õnnestunud, ei saa sõiduki DSRC-seade tõrke kohta andmeid esitada. Järelikult peab selline aruandlus olema REDCR-seadmete funktsioon.

„Lugemistõrge“ on tehniliselt erinev mõiste kui „viga“. Siinses kontekstis tähendab „viga“ vale väärtuse saamist.

Sõiduki DSRC-seadmele edastatakse andmed juba turvatud kujul, mistõttu neid peab kontrollima andmete esitaja (vt punkt 5.4).

Hiljem raadioliidese kaudu edastatud andmeid kontrollitakse tsükkelkoodkontrolliga (CRC) andmeside tasandil. Kui CRC kinnitab andmete terviklust, siis on andmed õiged. Kui CRC ei kinnita terviklust, edastatakse andmed uuesti. Võimalus, et andmed saaksid CRC eksikombel läbida, on statistiliselt sedavõrd vähetõenäoline, et selle võib arvestamata jätta.

Kui CRC andmete terviklust ei kinnita ning enam ei ole aega õigete andmete uuesti edastamiseks ja vastuvõtmiseks, siis ei ole tulemuseks viga, vaid kindlat tüüpi lugemistõrke juht.

Sellises olukorras saab tõrgete kohta sisuliselt registreerida ainult andmesideühenduse algatamiseks tehtud katsete arvu, mille tulemuseks ei olnud andmete edukas edastamine REDCR-ile.

DSC_82 Seetõttu registreerib REDCR ajatempliga varustatult nende juhtude arvu, mille korral sõiduki DSRC-seadmele päringu esitamise initsialiseerimise etapp õnnestus, kuid andmesideühendus lõpetati enne andmete vastuvõtmist REDCR-is. Need andmed peavad olema pädeva kontrolliasutuse esindajale kättesaadavad ning salvestatakse REDCR-seadme mälus. Selle saavutamiseks kasutatavad vahendid määratakse kindlaks tootedisaini käigus või pädeva kontrolliasutuse spetsifikaadiga.

Sisuliselt ainsad andmed, mida saab vigade kohta registreerida, on nende juhtumite arv, mille korral REDCR ei saa vastu võetud andmeid dekrüpteerida. Tuleb siiski märkida, et see on seotud ainult REDCR-i tarkvara tõhususega. Andmed võidakse tehniliselt dekrüpteerida, aga need ei pruugi olla semantiliselt arusaadavad.

DSC_83 Seetõttu registreerib REDCR ajatempliga varustatult nende juhtude arvu, mille korral ta püüdis DSRC-liidese kaudu saadud andmeid dešifreerida, aga see ei õnnestunud.

6. KAUGSIDESEADME KASUTUSELE VÕTMINE JA KORRALISTE ÜLEVAATUSTE KÄIGUS TEHTAVAD KATSED

6.1. **Üldist**

DSC_84 Kaugsidefunktsiooni jaoks on ette nähtud kahte liiki katsed:

1) ECHO katse, millega kontrollitakse raadiosidekanali *DSRC-REDCR* >>-:-<< *DSRC-VU* toimimist

2) otspunktide turbekatse, millega kontrollitakse, kas töökojakaardiga pääseb ligi sõidukiseadmes loodud krüpteeritud ja allkirjastatud andmetele, mis on edastatud raadiosidekanali kaudu.

6.2. **ECHO**

Käesolevas punktis käsitletakse katset, mille eesmärk on kontrollida ainult seda, kas raadiosidekanal *DSRC-REDCR* >>-:-<< *DSRC-VU* on funktsionaalselt toimiv.

Käsu ECHO eesmärk on võimaldada töökodadel või tüübikatseasutustel kontrollida, kas DSRC-ühendus toimib, ilma et neil oleks vaja juurdepääsu turbemandaatidele. Seetõttu on kontrollija seadmel vaja üksnes initsialiseerida DSRC-side (saates BST koos identifikaatoriga AID = 2) ning saata seejärel käsk ECHO. Kui DSRC toimib, siis saab ta seepeale ECHO vastuse. Täpsem teave punktis 5.4.8. Kui kõnealune vastus saadakse nõuetekohaselt, võib kinnitada, et DSRC-ühendus (*DSRC-REDCR* >>-:-<< *DSRC-VU*) toimib õigesti.

6.3. **Turvatud andmete sisu kontrollimise katsed**

DSC_85 See katse tehakse selleks, et kontrollida otspunktides turvalist andmevoogu. Katse tegemiseks on vaja DSRC-katselugejat. DSRC-katselugejal on samad funktsioonid ja see valmistatakse sama spetsifikaadi järgi nagu korrakaitsjate kasutatavad lugejad, kuid DSRC-katselugeja kasutaja autentimiseks kasutatakse kontrollikaardi asemel töökojakaarti. Katse võib läbi viia pärast aruka sõidumeeriku esimest aktiveerimist või kalibreerimise lõpus. Pärast aktiveerimist loob sõidukiseaade turvalised varajase tuvastamise andmed ning edastab need sõiduki DSRC-seadmele.

DSC_86 Töökoja töötaja peab paigutama DSRC-katselugeja sõiduki ette 2–10 meetri vahele jäävale kaugusele.

DSC_87 Seejärel sisestab töökoja töötaja DSRC-katselugejasse töökojakaardi, et esitada sõidukiseadmele varajase tuvastamise andmete päring. Kui päringu esitamine õnnestub, vaatab töökoja töötaja saadud andmeid, et veenduda, kas nende tervikluse kontrollimine ja dekrüpteerimine õnnestus.

15. Liide

ÜLEMINEK: ERI PÕLVKONNA SEADMETE ÜHEAEGNE KASUTAMINE

SISUKORD

1. MÕISTED

Käesolevas liites kasutatakse järgmisi mõisteid:

aruka sõidumeeriku süsteem – nagu on määratletud käesolevas lisas (1. peatükk, mõiste bbb);

esimese põlvkonna sõidumeeriku süsteem – nagu on määratletud käesolevas määruses (artikkel 2, mõiste 1);

teise põlvkonna sõidumeeriku süsteem – nagu on määratletud käesolevas määruses (artikkel 2, mõiste 7);

kasutuselevõtu kuupäev – nagu on määratletud käesolevas lisas (1. peatükk, mõiste ccc);

eriotstarbeline seade – andmete allalaadimiseks kasutatav seade, nagu on määratletud käesoleva lisa 7. liites.

2. ÜLDSÄTTED

2.1. Üleminekut käsitlev ülevaade

Käesoleva lisa sissejuhatuses on esitatud ülevaade esimese põlvkonna sõidumeeriku süsteemilt teise põlvkonna süsteemile ülemineku kohta.

Täiendav teave lisaks nimetatud sissejuhatuse sätetele:

— esimese põlvkonna liikumisandur ei tööta koos teise põlvkonna sõidukiseadmega;

— teise põlvkonna liikumisandureid hakatakse sõidukitele paigaldama samaaegselt teise põlvkonna sõidukiseadmetega;

— andmete allalaadimise ja kalibreerimise seadmeid tuleb täiustada, et toetada kummagi põlvkonna sõidumeerikute ja sõidumeerikukaartide kasutamist.

2.2. **Sõidukiseadme ja kaardi koostalitlusvõime**

Eeldatakse, et esimese põlvkonna sõidumeerikukaart on koostalitlusvõimeline esimese põlvkonna sõidukiseadmega (kooskõlas määruse (EMÜ) nr 3821/85 IB lisaga) ning teise põlvkonna sõidumeerikukaart on koostalitlusvõimeline teise põlvkonna sõidukiseadmega (kooskõlas käesoleva määruse IC lisaga). Peale selle kohaldatakse järgmisi nõudeid.

MIG_001 Esimese põlvkonna sõidumeerikukaarti võib kuni kaardi kehtivusaja lõpuni jätkuvalt kasutada teise põlvkonna sõidukiseadmes, kui nõuetes MIG_004 ja MIG_005 ei ole sätestatud teisiti. Sellise kaardi valdaja võib taotleda kaardi asendamist teise põlvkonna sõidumeerikukaardiga niipea, kui see kättesaadavaks muutub.

MIG_002 Teise põlvkonna sõidukiseade peab võimaldama kasutada seadmesse sisestatud mis tahes kehtivat esimese põlvkonna juhi-, kontrolli- või ettevõttekaarti.

MIG_003 Kõnealuse sõidukiseadme sellise koostalitlusvõime võib töökojas alatiseks tõkestada, nii et esimese põlvkonna sõidumeerikukaarti ei ole enam võimalik aktsepteerida. Seda on lubatud teha üksnes pärast seda, kui Euroopa Komisjon on algatanud menetluse, mille eesmärk on nõuda töökodadelt selle toimingu läbiviimist näiteks iga sõidumeeriku perioodilise kontrolli käigus.

MIG_004 Teise põlvkonna sõidukiseadmes peab olema võimalik kasutada üksnes teise põlvkonna töökojakaarti.

MIG_005 Teise põlvkonna sõidukiseadmes kasutatakse kasutusrežiimi kindlakstegemiseks üksnes sisestatud kehtiva kaardi liiki, olenemata selle põlvkonnast.

MIG_006 Iga kehtivat teise põlvkonna sõidumeerikukaarti peab saama kasutada esimese põlvkonna sõidukiseadmes täpselt samal viisil nagu esimese põlvkonna sama liiki sõidumeerikukaarti.

2.3. **Sõidukiseadme ja liikumisanduri koostalitlusvõime**

Eeldatakse, et esimese põlvkonna liikumisandur on koostalitlusvõimeline esimese põlvkonna sõidukiseadmega ning teise põlvkonna liikumisandur on koostalitlusvõimeline teise põlvkonna sõidukiseadmega. Peale selle kohaldatakse järgmisi nõudeid.

MIG_007 Teise põlvkonna sõidukiseade ei saa töötada koos esimese põlvkonna liikumisanduriga.

MIG_008 Teise põlvkonna liikumisandurit võib kasutada kas üksnes koos teise põlvkonna sõidukiseadmega või koos kummagi põlvkonna sõidukiseadmetega.

2.4. **Sõidukiseadme, sõidumeerikukaardi ja andmete allalaadimise seadme koostalitlusvõime**

MIG_009 Andmete allalaadimise seadet võib kasutada kas üksnes ühe põlvkonna või kummagi põlvkonna sõidukiseadmete ja sõidumeerikukaartidega.

2.4.1. *Eriotstarbelise seadmega otse kaardilt alla laadimine*

MIG_010 Andmete allalaadimiseks eriotstarbelise seadme kaardilugejasse sisestatud konkreetse põlvkonna sõidumeerikukaardilt kasutatakse asjaomase põlvkonna turbemehhanisme ja andmete allalaadimise protokolli ning allalaaditud andmed peavad olema selle põlvkonna jaoks kindlaks määratud vormingus.

MIG_011 Et võimaldada kontrolliasutustel väljaspool ELi sõidukijuhte kontrollida, peab allalaadimine teise põlvkonna juhi- või töökojakaardilt olema võimalik täpselt samal viisil nagu esimese põlvkonna juhi- või töökojakaardilt. Selline allalaadimine hõlmab:

— allkirjastamata elementaarfaile `IC` ja `ICC`,

— allkirjastamata elementaarfaile (esimene põlvkond) `Card_Certificate` ja `CA_Certificate`,

— muid esimese põlvkonna kaardilt allalaadimise protokollis nõutavaid rakendusandmete elementaarfaile (erifailis TACHO). Need andmed turvatakse digitaalallkirjaga vastavalt esimese põlvkonna turbemehhanismidele.

Kõnealune allalaadimine ei hõlma selliseid rakendusandmete elementaarfaile, mis on olemas üksnes teise põlvkonna juhi- ja töökojakaartides (rakendusandmete elementaarfailid erifailis TACHO_G2).

2.4.2. *Kaardilt alla laadimine sõidukiseadme kaudu*

MIG_012 Esimese põlvkonna sõidukiseadmesse sisestatud teise põlvkonna kaardilt andmete allalaadimiseks kasutatakse esimese põlvkonna allalaadimisprotokolli. Selline kaart vastab sõidukiseadme käskudele täpselt samal viisil nagu esimese põlvkonna kaart ning allalaaditud andmed on samas vormingus kui esimese põlvkonna kaardilt alla laaditud andmed.

MIG_013 Teise põlvkonna sõidukiseadmesse sisestatud esimese põlvkonna kaardilt andmete alla laadimiseks kasutatakse käesoleva lisa 7. liites määratletud allalaadimisprotokolli. Sõidukiseade saadab sellisele kaardile käske täpselt samal viisil nagu esimese põlvkonna sõidukiseade ning allalaaditud andmed on esimese põlvkonna kaardi jaoks kindlaks määratud vormingus.

2.4.3. *Sõidukiseadmest alla laadimine*

MIG_014 Teise põlvkonna sõidukiseadmest andmete alla laadimiseks kasutatakse teise põlvkonna turbemehhanisme ja käesoleva lisa 7. liites määratletud allalaadimisprotokolli.

MIG_015 Et võimaldada kontrolliasutustel väljaspool ELi sõidukijuhte kontrollida ja töökodadel väljaspool ELi sõidukiseadme andmeid alla laadida, võib soovi korral luua võimaluse kasutada teise põlvkonna sõidukiseadmest andmete alla laadimiseks esimese põlvkonna turbemehhanisme ja esimese põlvkonna allalaadimisprotokolli. Allalaaditud andmed peavad olema samas vormingus kui esimese põlvkonna sõidukiseadmest alla laaditud andmed. See võimalus võib olla valitav menüükäskude abil.

2.5. **Sõidukiseadme ja kalibreerimisseadme koostalitlusvõime**

MIG_016 Kalibreerimisseade peab võimaldama kasutada konkreetse põlvkonna sõidumeeriku kalibreerimisel asjaomase põlvkonna kalibreerimisprotokolli. Kalibreerimisseadet võib kasutada kas ühe või kummagi põlvkonna sõidumeerikute jaoks.

3. TÄHTSAMAD SAMMUD KASUTUSELEVÕTULE EELNEVAL PERIOODIL

MIG_017 Katsevõtmed ja sertifikaadid tehakse tootjale kättesaadavaks hiljemalt **30 kuud** enne kasutuselevõtu kuupäeva.

MIG_018 Koostalitlusvõime katsetega alustamiseks tootja nõudel tuleb olla valmis hiljemalt **15 kuud** enne kasutuselevõtu kuupäeva.

MIG_019 Ametlikud võtmed ja sertifikaadid tehakse tootjale kättesaadavaks hiljemalt **12 kuud** enne kasutuselevõtu kuupäeva.

MIG_020 Liikmesriigid peavad olema võimelised andma välja teise põlvkonna töökojakaarte hiljemalt **3 kuud** enne kasutuselevõtu kuupäeva.

MIG_021 Liikmesriigid peavad olema võimelised andma välja iga liiki teise põlvkonna sõidumeerikukaarte hiljemalt **1 kuu** enne kasutuselevõtu kuupäeva.

4. SÄTTED KASUTUSELEVÕTU JÄRGSEKS PERIOODIKS

MIG_022 Pärast kasutuselevõtu kuupäeva annavad liikmesriigid välja üksnes teise põlvkonna sõidumeerikukaarte.

MIG_023 Sõidukiseadme/liikumisanduri tootjal lubatakse toota esimese põlvkonna sõidukiseadet/liikumisandurit seni, kuni seda veel kasutatakse, et võimaldada rikkis komponentide asendamist.

MIG_024 Sõidukiseadme/liikumisanduri tootjal võimaldatakse juba tüübikinnituse saanud esimese põlvkonna sõidukiseadme/liikumisanduri puhul taotleda ja saada tüübikinnituse kehtivusaja pikendust.

16. Liide

M1- JA N1-KATEGOORIA SÕIDUKITE ADAPTER

SISUKORD

1. LÜHENDID JA VIITEDOKUMENDID

1.1. **Lühendid**

VU sõidukiseade (*Vehicle Unit*)

1.2. **Viidatud standard**

ISO 16844-3 „Road vehicles – Tachograph systems – Part 3: Motion sensor interface“ („Maanteesõidukid. Sõidumeerikusüsteemid. Osa 3: Liikumisanduri liides“)

2. ADAPTERI ÜLDOMADUSED JA FUNKTSIOONID

2.1. **Adapteri üldkirjeldus**

ADA_001 Adapter varustab sellega ühendatud VUd pidevalt turvatud andmetega sõiduki kiiruse ja läbitud vahemaa kohta.

Adapter on ette nähtud ainult sõidukitele, mis peavad vastavalt käesolevale määrusele olema varustatud sõidumeerikuga.

Adapter paigaldatakse ja seda kasutatakse ainult selliste IC lisa mõiste yy „adapter" all määratletud sõidukite puhul, millele ei ole tehniliselt võimalik paigaldada ühtki olemasolevat muud tüüpi liikumisandurit, mis vastab käesoleva lisa ja selle 1.–16. liite sätetele.

Adapterit ei tohi mehaaniliselt ühendada sõiduki liikuva osaga, vaid see ühendatakse kiiruse-/vahemaaimpulsse genereeriva sisseehitatud anduri või muu liidesega.

ADA_002 Adapteri kesta paigaldatakse käesoleva IC lisa 8. jao „Sõidumeeriku ja sõidumeerikukaartide tüübikinnitus" sätete alusel tüübikinnituse saanud liikumisandur; kestas paikneb ka konverter sisenevate impulsside suunamiseks adapterisse paigaldatud liikumisandurisse. Adapteris paiknev liikumisandur ühendatakse VUga nii, et oleks tagatud VU ja adapteri vahelise liidese vastavus standardi ISO 16844-3 nõuetele.

2.2. **Funktsioonid**

ADA_003 Adapter täidab järgmisi funktsioone:

— sisenevate kiiruseimpulsside vastuvõtmine ja kohandamine;

— sisenevate impulsside suunamine adapteris paiknevasse liikumisandurisse;

— kõik adapteris paikneva liikumisanduri funktsioonid, millega tagatakse turvatud liikumisandmete edastamine VUsse.

2.3. **Turvalisus**

ADA_004 Adapteri turvalisuse sertifitseerimisel ei lähtuta liikumisandurit käsitlevast käesoleva lisa 10. liites määratletud üldisest turbe-eesmärgist. Selle asemel kohaldatakse käesoleva liite punktis 4.4 sätestatud turvanõudeid.

3. NÕUDED SÕIDUMEERIKULE ADAPTERI KASUTAMISEL

Allpool sätestatud nõuetest ilmneb, kuidas tuleb mõista käesoleva lisa nõudeid adapteri kasutamise korral. IC lisa nõuete asjaomased numbrid on esitatud nurksulgudes.

ADA_005 Iga adapteriga varustatud sõiduki sõidumeerik peab vastama kõikidele käesoleva lisa sätetele, välja arvatud juhul, kui käesoleva liitega on ette nähtud teisiti.

ADA_006 Paigaldatud adapteriga sõiduki sõidumeerik koosneb juhtmetest, adapterist (sealhulgas liikumisandur) ja sõidukiseadmest [01].

ADA_007 Sõidumeeriku sündmuste ja/või rikete tuvastamise funktsioon seadistatakse ümber järgmiselt:

— sündmuse „voolukatkestus" käivitab sõidukiseade juhul, kui see ei ole kalibreerimisrežiimis ja adapteris paikneva liikumisanduri toitevoolu katkestus kestab kauem kui 200 millisekundit [79];

— sündmuse „liikumisandmete viga" käivitab sõidukiseade juhul, kui adapteris paikneva liikumisanduri ja sõidukiseadme vaheline tavapärane andmevahetus katkeb ja/või sellise andmevahetuse ajal tekib andmete tervikluse või andmete autentimisega seotud viga [83];

— sündmuse „turvalisuse rikkumise katse“ käivitab sõidukiseade juhul, kui see ei ole kalibreerimisrežiimis ja esineb mis tahes muu sündmus, mis mõjutab adapteris paikneva liikumisanduri turvalisust [85];

— vea „sõidumeerik“ käivitab sõidukiseade juhul, kui see ei ole kalibreerimisrežiimis ja adapteris paiknevas liikumisanduris tekib mis tahes tõrge [88].

ADA_008 Sõidumeeriku tuvastatavad adapteri tõrked on adapteris paikneva liikumisanduriga seotud tõrked [88].

ADA_009 Sõidukiseadme kalibreerimisfunktsioon võimaldab ühendada liikumisanduri automaatselt sõidukiseadmega [202, 204].

4. ADAPTERI EHITUST JA FUNKTSIOONE KÄSITLEVAD NÕUDED

4.1. **Sisenevate kiiruseimpulsside vastuvõtmine ja kohandamine**

ADA_011 Adapteri sisendliides võtab vastu sagedusimpulsse, mis kajastavad sõiduki kiirust ja läbitud vahemaad. Sisenevate impulsside elektrilised omadused määrab kindlaks tootja. Seadistus, mida saab muuta ainult tootja ja adapterit paigaldav tunnustatud töökoda, peab vajaduse korral võimaldama adapteri sisendi nõuetekohast liidestamist sõidukiga.

ADA_012 Adapteri sisendliides peab vajaduse korral võimaldama korrutada või jagada kiirust kajastavaid sisenevaid sagedusimpulsse kindla teguriga, et kohandada signaali nii, et see jääks käesolevas lisas määratletud teguri k väärtuste vahemikku (4 000–25 000 impulssi kilomeetri kohta). Seda kindlaksmääratud tegurit võivad programmeerida ainult adapteri tootja ja adapterit paigaldav tunnustatud töökoda.

4.2. **Sisenevate impulsside suunamine adapteris paiknevasse liikumisandurisse**

ADA_013 Sisenevad impulsid, mis võivad olla eespool kirjeldatud viisil kohandatud, suunatakse adapteris paiknevasse liikumisandurisse nii, et liikumisanduris tuvastatakse kõik sisenevad impulsid.

4.3. **Adapteris paiknev liikumisandur**

ADA_014 Adapteris paiknevasse liikumisandurisse suunatud impulsid mõjutavad andurit, võimaldades sellel genereerida liikumisandmeid, mis kirjeldavad sõiduki liikumist täpselt nii, nagu oleks andur mehaaniliselt ühendatud sõiduki liikuva osaga.

ADA_015 Sõidukiseadmes kasutatakse adapteri identimiseks adapteris paikneva liikumisanduri identimisandmeid [95].

ADA_016 Adapteri paigaldusandmetena käsitatakse adapteris paiknevasse liikumisandurisse salvestatud paigaldusandmeid [122].

4.4. **Turvanõuded**

ADA_017 Adapteri kest on ehitatud nii, et seda ei ole võimalik avada. Adapter plommitakse nii, et füüsilise avamise katsed on hõlpsalt tuvastatavad (näiteks visuaalsel vaatlusel, vt ADA_035). Kõnealused plommid vastavad samadele nõuetele kui liikumisanduri plommid [398–406].

ADA_018 Adapteris paiknev liikumisandur ei ole adapterist eemaldatav ilma adapteri kesta plommi(de) või anduri ja adapteri kesta vahelise plommi lõhkumiseta (vt ADA_034).

ADA_019 Adapteriga tagatakse, et vastu võtta ja töödelda saab ainult adapteri sisendi kaudu saabuvaid liikumisandmeid.

4.5. **Tööomadused**

ADA_020 Adapter on täielikult toimiv tootja kindlaks määratud temperatuurivahemikus.

ADA_021 Adapter on täielikult toimiv õhuniiskuse vahemikus 10–90 % [214].

ADA_022 Adapter on kaitstud ülepinge, toiteallika polaarsuse vahetuse ja lühiste eest [216].

ADA_023 Adapter kas:

— reageerib magnetväljale, mis häirib sõiduki liikumise jälgimist – sel juhul registreeritakse ja salvestatakse sõidukiseadmes anduri tõrge [88], või

— sisaldab tajurit, mis on magnetvälja vastu kaitstud või mida magnetväli ei mõjuta [217].

ADA_024 Adapter vastab elektromagnetilist ühilduvust käsitlevale ÜRO Euroopa Majanduskomisjoni rahvusvahelisele eeskirjale nr 10 ning on kaitstud elektrostaatiliste lahenduste ja siirdeprotsesside eest [218].

4.6. **Materjalid**

ADA_025 Adapter vastab kaitseklassile, mille määrab kindlaks tootja vastavalt paigalduskohale [220, 221].

ADA_026 Adapteri kest on kollane.

4.7. **Märgistus**

ADA_027 Adapterile kinnitatakse kirjeldav tahvel, millele on kantud järgmised üksikasjad:

— adapteri tootja nimi ja aadress;

— adapteri valmistamise aasta ja tootja osa number;

— adapteri või adapterit sisaldava sõidumeeriku tüübikinnitusmärk;

— adapteri paigaldamise kuupäev;

— selle sõiduki tehasetähis, millele adapter on paigaldatud.

ADA_028 Kirjeldavale tahvlile kantakse ka järgmised üksikasjad (kui need ei ole loetavad adapteris paikneva liikumisanduri välispinnal):

— adapteris paikneva liikumisanduri tootja nimi;

— adapteris paikneva liikumisanduri valmistamise aasta ja tootja osa number;

— adapteris paikneva liikumisanduri tüübikinnitusmärk.

5. SÕIDUMEERIKU PAIGALDAMINE ADAPTERI KASUTAMISEL

5.1. **Paigaldamine**

ADA_029 Adapteri paigaldab sõidukile üksnes sõiduki tootja või tunnustatud töökoda, kellel on luba paigaldada, aktiveerida ja kalibreerida digitaalseid ja arukaid sõidumeerikuid.

ADA_030 Adapterit paigaldav tunnustatud töökoda kohandab sisendliidese ja valib vajaduse korral siseneva impulsi jagamisteguri.

ADA_031 Adapterit paigaldav tunnustatud töökoda plommib adapteri kesta.

ADA_032 Adapter paigaldatakse võimalikult lähedale sellele sõidukiosale, millest sisenevad impulsid lähtuvad.

ADA_033 Adapteri toitejuhtmed on punast (positiivne toide) ja musta (maandus) värvi.

5.2. **Plommid**

ADA_034 Kohaldatakse järgmisi plommimisnõudeid:

— adapteri kest on plommitud (vt ADA_017);

— adapteris paikneva anduri kest on plommitud adapteri kesta külge, välja arvatud juhul, kui andurit ei ole võimalik eemaldada adapteri kesta plommi lõhkumata (vt ADA_018);

— adapteri kest on plommitud sõiduki külge;

— adapteri ja sisenevaid impulsse edastava seadme vaheline ühendus on mõlemas otsas plommitud (mõistlikus ulatuses).

6. KONTROLL, ÜLEVAATUS JA REMONT

6.1. **Perioodiline kontroll**

ADA_035 Adapteri kasutamisel kontrollitakse sõidumeeriku igal korralisel ülevaatusel (viiakse läbi vastavalt IC lisa nõuetele 409–413) järgmist:

— et adapteril on nõuetekohased tüübikinnitusmärgid;

— et adapteri ja selle ühenduste plommid on terved;

— et adapter on paigaldatud vastavalt paigaldustahvlil märgitule;

— et adapter on paigaldatud adapteri ja/või sõiduki tootja määratud viisil;

— et adapteri paigaldamine on kontrollitava sõiduki puhul lubatud.

ADA_036 Selline kontroll hõlmab ka kalibreerimist ja kõikide plommide asendamist, olenemata nende seisundist.

7. SÕIDUMEERIKU TÜÜBIKINNITUS ADAPTERI KASUTAMISEL

7.1. **Üldnõuded**

ADA_037 Sõidumeerik esitatakse tüübikinnituse saamiseks komplektsena, koos adapteriga [425].

ADA_038 Iga adapteri võib esitada tüübikinnituse saamiseks eraldi või sõidumeeriku osana.

ADA_039 Selline tüübikinnitus hõlmab funktsionaalseid katseid koos adapteriga. Iga sellise katse positiivseid tulemusi kinnitab asjakohane tunnistus [426].

7.2. **Funktsionaalsuse sertifikaat**

ADA_040 Adapteri või adapterit sisaldava sõidumeeriku funktsionaalsuse sertifikaat väljastatakse adapteri tootjale alles pärast kõikide allpool nimetatud funktsionaalsete miinimumkatsete edukat läbimist.

Nr	Katse	Kirjeldus	Seotud nõuded
1.	**Halduskontroll**		
1.1.	Dokumenteerimine	Adapteri dokumentide õigsus	
2.	**Visuaalne kontroll**		
2.1.	Adapteri vastavus dokumentidele		
2.2.	Adapteri identimisandmed/märgistus		ADA_027, ADA_028
2.3.	Adapteri materjalid		[219–223] ADA_026
2.4.	Plommid		ADA_017, ADA_018, ADA_034
3.	**Funktsionaalsed katsed**		
3.1.	Kiiruseimpulsside suunamine adapteris paiknevasse liikumisandurisse		ADA_013
3.2.	Sisenevate kiiruseimpulsside vastuvõtmine ja kohandamine		ADA_011, ADA_012
3.3.	Liikumise mõõtmise täpsus		[30–35, 217]
4.	**Keskkonnakatsed**		
4.1.	Tootja katsetulemused	Tootja keskkonnakatsete tulemused	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Elektromagnetiline ühilduvus**		
5.1.	Kiirgusemissioon ja vastuvõtlikkus	Direktiivile 2006/28/EÜ vastavuse kontroll	ADA_024
5.2.	Tootja katsetulemused	Tootja keskkonnakatsete tulemused	ADA_024

ISSN 1977-0650 (elektrooniline väljaanne)
ISSN 1725-5082 (paberväljaanne)

Euroopa Liidu Väljaannete Talitus
2985 Luxembourg
LUKSEMBURG

ET