Tämä asiakirja on ainoastaan dokumentoinnin apuväline eikä sillä ole oikeudellista vaikutusta. Unionin toimielimet eivät vastaa sen sisällöstä. Säädösten todistusvoimaiset versiot on johdanto-osineen julkaistu Euroopan unionin virallisessa lehdessä ja ne ovat saatavana EUR-Lexissä. Näihin virallisiin teksteihin pääsee suoraan tästä asiakirjasta siihen upotettujen linkkien kautta.

►B

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2016/799,

annettu 18 päivänä maaliskuuta 2016,

ajopiirturien ja niiden osien rakentamista, testaamista, asentamista, käyttöä ja korjaamista koskevan Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 165/2014 täytäntöönpanemisesta

(ETA:n kannalta merkityksellinen teksti)

(EUVL L 139, 26.5.2016, s. 1)

Oikaistu:

►C1 Oikaisu, EUVL L 146, 3.6.2016, s. 31 (2016/799)

►C2 Oikaisu, EUVL L 27, 1.2.2017, s. 169 (2016/799)

▼B

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2016/799,

annettu 18 päivänä maaliskuuta 2016,

ajopiirturien ja niiden osien rakentamista, testaamista, asentamista, käyttöä ja korjaamista koskevan Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 165/2014 täytäntöönpanemisesta

(ETA:n kannalta merkityksellinen teksti)

1 artikla

Kohde ja soveltamisala

1. Tässä asetuksessa annetaan säännökset seuraavien ajopiirturin ominaisuuksien yhdenmukaisen soveltamisen varmistamiseksi:

a) ajoneuvon sijainnin kirjaaminen tietyissä paikoissa kuljettajan vuorokautisen työjakson aikana;

b) etäyhteys älykkäiden ajopiirturien mahdollisten manipulointien tai väärinkäytösten varhaista havaitsemista varten;

c) ITS-rajapinta;

d) ajopiirturien tyyppihyväksyntämenettelyjen hallinnolliset ja tekniset vaatimukset, mukaan lukien turvallisuusmekanismit.

2. Älykkäiden ajopiirturien ja niiden osien rakentamisen, testaamisen, asentamisen, tarkastamisen, käytön ja korjaamisen on tapahduttava tämän asetuksen liitteessä 1C säädettyjä teknisiä vaatimuksia noudattaen.

3. Muiden ajopiirturien kuin älykkäiden ajopiirturien rakentamisen, testaamisen, asentamisen, tarkastamisen, käytön ja korjaamisen on edelleen tapahduttava soveltuvin osin joko neuvoston asetuksen (ETY) N:o 3821/85 ([1]) liitteen 1 tai liitteen 1B vaatimusten mukaisesti.

4. Direktiivin 96/53/EY 10 d artiklan nojalla varhaiseen havaitsemiseen tarkoitetun etäyhteyslaitteiston on lähetettävä myös ajoneuvoon asennetun punnitusjärjestelmän punnitustiedot petosten havaitsemiseksi varhaisessa vaiheessa.

2 artikla

Määritelmät

Tässä asetuksessa sovelletaan asetuksen (EU) N:o 165/2014 2 artiklassa säädettyjä määritelmiä.

Lisäksi tässä asetuksessa tarkoitetaan

1) ’digitaalisella ajopiirturilla’ tai ’ensimmäisen sukupolven ajopiirturilla’ muuta digitaalista ajopiirturia kuin älykästä ajopiirturia;

2) ’ulkoisella GNSS-laitteistolla’ laitteistoa, joka sisältää GNSS-vastaanottimen, kun ajoneuvoyksikkö ei ole yksi yksikkö, ja muita osia, jotka tarvitaan suojaamaan muualle ajoneuvoyksikköön tapahtuvaa sijaintitietojen siirtämistä;

([1]) Neuvoston asetus (ETY) N:o 3821/85, annettu 20 päivänä joulukuuta 1985, tieliikenteen valvontalaitteista (EYVL L 370, 31.12.1985, s. 8).

▼B

3) ’valmistusasiakirjoilla’ täydellistä sähköistä tai paperimuotoista asiakirja-aineistoa, jossa on kaikki tiedot, jotka valmistaja tai sen edustaja on toimittanut tyyppihyväksyntäviranomaiselle ajopiirturin tai sen osan tyyppihyväksyntää varten, mukaan lukien asetuksen (EU) N:o 165/2014 12 artiklan 3 kohdassa tarkoitetut todistukset, ja tämän asetuksen liitteessä 1C määriteltyjen testien tekemistä varten, sekä piirroksia, valokuvia ja muita asiaankuuluvia asiakirjoja;

4) ’hyväksyntäasiakirjoilla’ sähköisiä tai paperimuotoisia valmistusasiakirjoja, joiden mukana on mahdollisia muita tyyppihyväksyntäviranomaisen tehtäviensä suorittamisen aikana lisäämiä asiakirjoja, mukaan lukien typpihyväksyntäprosessin lopussa lisätty ajopiirturin tai sen osan EY-tyyyppihyväksyntätodistus;

5) ’hyväksyntäasiakirjojen hakemistolla’ asiakirjaa, jossa luetellaan hyväksyntäasiakirjojen numeroitu sisältö, josta kaikki näiden asiakirjojen asiaankuuluvat osat voidaan yksilöidä. Mainitun asiakirjan muodon on oltava sellainen, että siitä voidaan erottaa kaikki EY-tyyppihyväksyntäprosessin peräkkäiset vaiheet, mukaan lukien asiakirjojen mahdollisten tarkistusten ja päivitysten päivämäärät;

6) ’varhaiseen havaitsemiseen tarkoitetulla etäyhteyslaitteistolla’ ajoneuvoyksikön laitteita, joita käytetään kohdistettujen tienvarsitarkastusten tekemiseksi;

7) ’älykkäällä ajopiirturilla’ tai ’toisen sukupolven ajopiirturilla’ asetuksen (EU) N:o 165/2014 8, 9 ja 10 artiklan ja tämän asetuksen liitteen 1C mukaista digitaalista ajopiirturia;

8) ’ajopiirturin osalla’ tai ’osalla’ tarkoitetaan seuraavia: ajoneuvoyksikkö, liiketunnistin, ajopiirturikortti, piirturilevy, ulkoinen GNSS-laitteisto ja varhaiseen havaitsemiseen tarkoitettu etäyhteyslaitteisto;

9) ’tyyppihyväksyntäviranomaisella’ jäsenvaltion viranomaista, joka on toimivaltainen suorittamaan ajopiirturin tai sen osien tyyppihyväksynnän ja lupaprosessin sekä myöntämään ja tarvittaessa kumoamaan tyyppihyväksyntätodistukset ja joka toimii muiden jäsenvaltioiden tyyppihyväksyntäviranomaisten yhteyspisteenä ja varmistaa, että valmistajat täyttävät tämän asetuksen vaatimusten noudattamista koskevat velvoitteensa.

3 artikla

Paikannuspalvelut

1. Valmistajien on varmistettava, että älykkäät ajopiirturit ovat yhteensopivat Galileon ja Euroopan geostationaarisen navigointilisäjärjestelmän (EGNOS) tarjoamien paikannuspalvelujen kanssa.

2. Valmistajat voivat 1 kohdassa tarkoitettujen järjestelmien lisäksi halutessaan varmistaa yhdenmukaisuuden myös muiden satelliittinavigointijärjestelmien kanssa.

▼B

4 artikla

Ajopiirturin ja ajopiirturin osien tyyppihyväksyntämenettely

1. Valmistajan tai sen edustajan on toimitettava ajopiirturin taikka sen osan tai osakokonaisuuden tyyppihyväksyntähakemus kunkin jäsenvaltion nimeämille tyyppihyväksyntäviranomaisille. Hakemuksessa on oltava kutakin asianomaista osaa koskevat tiedot sisältävät valmistusasiakirjat, mukaan lukien, soveltuvin osin, kokonaisen ajopiirturin valmistamiseksi tarvittavien muiden osien tyyppihyväksyntätodistukset ja mahdolliset muut asiaankuuluvat asiakirjat.

2. Jäsenvaltion on myönnettävä tyyppihyväksyntä kaikille ajopiirtureille, osille ja osakokonaisuuksille, jotka täyttävät soveltuvin osin 1 artiklan 1, 2 tai 3 kohdassa tarkoitetut hallinnolliset ja tekniset vaatimukset, Tällaisessa tapauksessa tyyppihyväksyntäviranomaisen on annettava hakijalle tyyppihyväksyntätodistus, joka on tämän asetuksen liitteessä II olevan mallin mukainen.

3. Tyyppihyväksyntäviranomainen voi pyytää valmistajaa tai sen edustajaa toimittamaan lisätietoja.

4. Valmistajan tai sen edustajan on annettava tyyppihyväksyntäviranomaisten ja asetuksen (EU) N:o 165/2014 12 artiklan 3 kohdassa tarkoitettujen todistusten myöntämisestä vastaavien elinten saataville niin monta ajopiirturia tai ajopiirturin osaa kuin on tarpeen tyyppihyväksyntämenettelyn suorittamiseksi asianmukaisella tavalla.

5. Kun valmistaja tai sen edustaja hakee ajopiirturin tietyn osan tai osakokonaisuuden tyyppihyväksyntää, sen on annettava tyyppihyväksyntäviranomaisille jo tyyppihyväksytyt muut osat ja kokonaisen ajopiirturin rakentamiseksi tarvittavat muut osat, jotta kyseiset viranomaiset voivat tehdä tarvittavat testit.

5 artikla

Tyyppihyväksynnän muuttaminen

1. Valmistajan tai sen edustajan on viipymättä ilmoitettava alkuperäisen tyyppihyväksynnän myöntäneille tyyppihyväksyntäviranomaisille kaikista ajopiirturin ohjelmiston tai varusteiden taikka sen valmistuksessa käytettävien materiaalien muutoksista, jotka on kirjattu hyväksyntäasiakirjoihin, ja toimitettava hakemus tyyppihyväksynnän muuttamiseksi.

2. Tyyppihyväksyntäviranomaiset voivat tarkistaa tai laajentaa olemassa olevaa tyyppihyväksyntää tai myöntää uuden tyyppihyväksynnän muutosten luonteesta ja ominaisuuksista riippuen.

Tarkistus tehdään silloin, kun tyyppihyväksyntäviranomainen katsoo, että ajopiirturin ohjelmiston tai varusteiden taikka sen valmistuksessa käytettyjen materiaalien muutokset ovat vähäisiä. Tällaisissa tapauksissa tyyppihyväksyntäviranomainen myöntää tarkistetut hyväksyntäasiakirjat ja ilmoittaa tehtyjen muutosten luonteen ja hyväksyntäpäivämäärän. Tämän vaatimuksen täyttämiseksi riittää, että hyväksyntäasiakirjojen päivitetty toisinto annetaan kootussa muodossa yhdessä tehtyjä muutoksia koskevan yksityiskohtaisen kuvauksen kanssa.

▼B

Laajentaminen tehdään silloin, kun tyyppihyväksyntäviranomainen katsoo, että ajopiirturin ohjelmiston tai varusteiden taikka sen valmistuksessa käytettyjen materiaalien muutokset ovat huomattavia. Tällaisissa tapauksissa se voi pyytää tekemään uudet testit ja ilmoittaa tästä valmistajalle tai sen edustajalle. Jos kyseiset testit osoittautuvat tyydyttäviksi, tyyppihyväksyntäviranomaisen on annettava tarkistettu tyyppihyväksyntätodistus, jossa on myönnettyyn laajennukseen viittaava numero. Tyyppihyväksyntätodistuksessa on mainittava laajennuksen syy ja todistuksen myöntämispäivä.

3. Hyväksyntäasiakirjojen hakemistossa on oltava tyyppihyväksynnän viimeisimmän laajennuksen tai tarkistuksen päivämäärä tai tyyppihyväksynnän päivitetyn toisinnon viimeisimmän koonnoksen päivämäärä.

4. Uusi tyyppihyväksyntä on annettava silloin, kun tyyppihyväksyttyyn ajopiirturiin tai sen osiin pyydetyt muutokset johtaisivat uuden turvallisuus- tai yhteentoimivuustodistuksen myöntämiseen.

6 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Sitä sovelletaan 2 päivästä maaliskuuta 2016.

Liitteitä sovelletaan kuitenkin 2 päivästä maaliskuuta 2019, lukuun ottamaa lisäystä 16, jota sovelletaan 2 päivästä maaliskuuta 2016.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

▼B

LIITE I C

Rakennetta, testausta, asennusta ja tarkastusta koskevat vaatimukset

JOHDANTO

1. MÄÄRITELMÄT

2. VALVONTALAITTEIDEN YLEISET OMINAISUUDET JA TOIMINNOT

2.1 Yleiset ominaisuudet

2.2 Toiminnot

2.3 Toimintatilat

2.4 Turvallisuus

3. VALVONTALAITTEIDEN RAKENNETTA JA TOIMINTOJA KOSKEVAT VAATIMUKSET

3.1 Korttien paikoilleen asettamisen ja poistamisen seuranta

3.2 Nopeuden, sijainnin ja matkan mittaus

3.2.1 Kuljetun matkan mittaus

3.2.2 Nopeuden mittaus

3.2.3 Sijainnin mittaus

3.3 Ajanmittaus

3.4 Kuljettajan toiminnan seuranta

3.5 Ajoneuvon miehityksen seuranta

3.6 Kuljettajan syöttämät tiedot

3.6.1 Tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy

3.6.2 Kuljettajan toimintaa koskevien tietojen syöttö käsin ja ITS-rajapintaan liittyvä kuljettajan suostumus

3.6.3 Erityisolosuhteisiin liittyvien tietojen syöttö

3.7 Yritysten tekemien lukitusten hallinta

3.8 Tarkastustoimien seuranta

3.9 Tapahtumien ja/tai vikojen havaitseminen

3.9.1 ”Ei voimassa olevan kortin asettaminen laitteeseen”

3.9.2 ”Korttiristiriita” -tapahtuma

3.9.3 ”Aikojen päällekkäisyys” -tapahtuma

3.9.4 ”Ajo ilman asianmukaista korttia” -tapahtuma

3.9.5 ”Kortin paikoilleen asettaminen ajettaessa” -tapahtuma

3.9.6 ”Edellistä kortin käyttöjaksoa ei lopetettu oikein” -tapahtuma

3.9.7 ”Ylinopeus”-tapahtuma

3.9.8 ”Keskeytynyt virransyöttö” –tapahtuma

3.9.9 ”Virhe viestinnässä etäviestintälaitteiston kanssa” -tapahtuma

3.9.10 ”Sijaintitietojen puuttuminen GNSS-vastaanottimesta” -tapahtuma

▼B

3.9.11	”Virhe viestinnässä ulkoisen GNSS-laitteiston kanssa” -tapahtuma
3.9.12	”Virhe liikedatassa” –tapahtuma
3.9.13	”Ajoneuvon liikeristiriita” -tapahtuma
3.9.14	”Tietoturvan murtoyritys” –tapahtuma
3.9.15	”Aikojen päällekkäisyys” -tapahtuma
3.9.16	”Kortti” -vikatapahtuma
3.9.17	”Valvontalaite”-vikatapahtuma
3.10	Sisäänrakennetut ja laitteen itse suorittamat testit
3.11	Tietojen haku datamuistista
3.12	Tietojen kirjaaminen ja tallentaminen datamuistiin
3.12.1	Laitteen tunnistetiedot
3.12.1.1	Ajoneuvoyksikön tunnistetiedot
3.12.1.2	Liiketunnistimen tunnistetiedot
3.12.1.3	Maailmanlaajuisen satelliittinavigointijärjestelmän tunnistetiedot
3.12.2	Avaimet ja varmenteet
3.12.3	Kuljettaja- tai korjaamokortin paikoilleen asettamiseen ja poistamiseen liittyvät tiedot
3.12.4	Kuljettajan toimintaan liittyvät tiedot
3.12.5	Paikat ja sijainnit, joissa päivän työaika alkaa, loppuu, ja/tai jossa 3 tunnin jatkuva ajoaika saavutetaan
3.12.6	Matkamittariin liittyvät tiedot
3.12.7	Nopeuteen liittyvät yksityiskohtaiset tiedot
3.12.8	Tapahtumiin liittyvät tiedot
3.12.9	Vikoihin liittyvät tiedot
3.12.10	Kalibrointiin liittyvät tiedot
3.12.11	Ajan asetukseen liittyvät tiedot
3.12.12	Tarkastustoimiin liittyvät tiedot
3.12.13	Yritysten tekemiin lukituksiin liittyvät tiedot
3.12.14	Tietojen kopiointitapahtumiin liittyvät tiedot
3.12.15	Erityisolosuhteisiin liittyvät tiedot
3.12.16	Ajopiirturikortin tiedot
3.13	Tietojen haku ajopiirturikorteilta
3.14	Tietojen kirjaaminen ja tallentaminen ajopiirturikorteille
3.14.1	Tietojen kirjaaminen ja tallentaminen ensimmäisen sukupolven ajopiirturikorteille
3.14.2	Tietojen kirjaaminen ja tallentaminen toisen sukupolven ajopiirturikorteille
3.15	Tietojen näyttö
3.15.1	Oletusarvoinen näyttö
3.15.2	Varoitusnäyttö

▼B

3.15.3	Valikkojen käyttö
3.15.4	Muut näytöt
3.16	Tulostus
3.17	Varoitukset
3.18	Tietojen kopioiminen ulkoisille tietovälineille
3.19	Kohdistettuihin tienvarsitarkastuksiin liittyvä etäviestintä
3.20	Tietojen tulostus ulkoisille lisälaitteille
3.21	Kalibrointi
3.22	Kalibroinnin tarkastus tien varrella
3.23	Ajan asetus
3.24	Suorituskykyä koskevat tiedot
3.25	Materiaalit
3.26	Merkinnät
4.	AJOPIIRTURIKORTTIEN RAKENNETTA JA TOIMINTOJA KOSKEVAT VAATIMUKSET
4.1	Näkyvissä olevat tiedot
4.2	Turvallisuus
4.3	Standardit
4.4	Ympäristöön liittyvät ja sähkötekniset eritelmät
4.5	Tietojen säilyttäminen
4.5.1	Perustiedostot tunnistamiseen ja kortin hallinnointiin
4.5.2	Sirukorttien tunnistetiedot
4.5.2.1	Mikrosirujen tunnistetiedot
4.5.2.2	DIR-tiedostot (esiintyvät ainoastaan toisen sukupolven ajopiirturikorteissa)
4.5.2.3	ATR-tiedot (ehdolliset, esiintyvät ainoastaan toisen sukupolven ajopiirturikorteissa)
4.5.2.4	Laajennettua pituutta koskevat tiedot (ehdolliset, esiintyvät ainoastaan toisen sukupolven ajopiirturikorteissa.
4.5.3	Kuljettajakortti
4.5.3.1	Ajopiirturikortin sovellus (joka on ensimmäisen ja toisen sukupolven ajoneuvoyksikköjen käytettävissä)
4.5.3.1.1	Sovellusten tunnistetiedot
4.5.3.1.2	Avaimet ja varmenteet
4.5.3.1.3	Kortin tunniste
4.5.3.1.4	Kortin haltijan tunnistetiedot
4.5.3.1.5	Kortilla olevien tietojen kopiointi
4.5.3.1.6	Ajokorttiin liittyvät tiedot
4.5.3.1.7	Tapahtumiin liittyvät tiedot
4.5.3.1.8	Vikoihin liittyvät tiedot
4.5.3.1.9	Kuljettajan toimintaan liittyvät tiedot

▼B

4.5.3.1.10	Käytössä olleisiin ajoneuvoihin liittyvät tiedot
4.5.3.1.11	Tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy
4.5.3.1.12	Kortin käyttöjaksoon liittyvät tiedot
4.5.3.1.13	Tarkastustoimiin liittyvät tiedot
4.5.3.1.14	Erityisolosuhteisiin liittyvät tiedot
4.5.3.2	Ajopiirturin sukupolven 2 sovellus (ei voida käyttää ensimmäisen sukupolven ajoneuvoyksikössä)
4.5.3.2.1	Sovellusten tunnistetiedot
4.5.3.2.2	Avaimet ja varmenteet
4.5.3.2.3	Kortin tunniste
4.5.3.2.4	Kortin haltijan tunnistetiedot
4.5.3.2.5	Kortilla olevien tietojen kopiointi
4.5.3.2.6	Ajokorttiin liittyvät tiedot
4.5.3.2.7	Tapahtumiin liittyvät tiedot
4.5.3.2.8	Vikoihin liittyvät tiedot
4.5.3.2.9	Kuljettajan toimintaan liittyvät tiedot
4.5.3.2.10	Käytössä olleisiin ajoneuvoihin liittyvät tiedot
4.5.3.2.11	Tiedot paikasta ja sijainnit, jossa päivän työaika alkaa ja/tai päättyy
4.5.3.2.12	Kortin käyttöjaksoon liittyvät tiedot
4.5.3.2.13	Tarkastustoimiin liittyvät tiedot
4.5.3.2.14	Erityisolosuhteisiin liittyvät tiedot
4.5.3.2.15	Käytössä olleiden ajoneuvoyksikköjen tiedot
4.5.3.2.16	Kolmen tunnin keskeytymätöntä ajoa koskevat paikkatiedot.
4.5.4	Korjaamokortti
4.5.4.1	Ajopiirturikortin sovellus (joka on ensimmäisen ja toisen sukupolven ajoneuvoyksikköjen käytettävissä)
4.5.4.1.1	Sovellusten tunnistetiedot
4.5.4.1.2	Avaimet ja varmenteet
4.5.4.1.3	Kortin tunniste
4.5.4.1.4	Kortin haltijan tunnistetiedot
4.5.4.1.5	Kortilla olevien tietojen kopiointi
4.5.4.1.6	Kalibrointiin ja ajan asetukseen liittyvät tiedot
4.5.4.1.7	Tapahtumiin ja vikoihin liittyvät tiedot
4.5.4.1.8	Kuljettajan toimintaan liittyvät tiedot
4.5.4.1.9	Käytössä olleisiin ajoneuvoihin liittyvät tiedot
4.5.4.1.10	Päivän työajan alkamiseen ja/tai päättymiseen liittyvät tiedot
4.5.4.1.11	Kortin käyttöjaksoon liittyvät tiedot
4.5.4.1.12	Tarkastustoimiin liittyvät tiedot

▼B

4.5.4.1.13	Erityisolosuhteisiin liittyvät tiedot
4.5.4.2	Ajopiirturin sukupolven 2 sovellus (ei voida käyttää ensimmäisen sukupolven ajoneuvoyksikössä)
4.5.4.2.1	Sovellusten tunnistetiedot
4.5.4.2.2	Avaimet ja varmenteet
4.5.4.2.3	Kortin tunniste
4.5.4.2.4	Kortin haltijan tunnistetiedot
4.5.4.2.5	Kortilla olevien tietojen kopiointi
4.5.4.2.6	Kalibrointiin ja ajan asetukseen liittyvät tiedot
4.5.4.2.7	Tapahtumiin ja vikoihin liittyvät tiedot
4.5.4.2.8	Kuljettajan toimintaan liittyvät tiedot
4.5.4.2.9	Käytössä olleisiin ajoneuvoihin liittyvät tiedot
4.5.4.2.10	Päivän työajan alkamiseen ja/tai päättymiseen liittyvät tiedot
4.5.4.2.11	Kortin käyttöjaksoon liittyvät tiedot
4.5.4.2.12	Tarkastustoimiin liittyvät tiedot
4.5.4.2.13	Käytössä olleiden ajoneuvoyksikköjen tiedot
4.5.4.2.14	Kolmen tunnin keskeytymätöntä ajoa koskevat paikkatiedot.
4.5.4.2.15	Erityisolosuhteisiin liittyvät tiedot
4.5.5	Valvontakortti
4.5.5.1	Ajopiirturikortin sovellus (joka on ensimmäisen ja toisen sukupolven ajoneuvoyksikköjen käytettävissä)
4.5.5.1.1	Sovellusten tunnistetiedot
4.5.5.1.2	Avaimet ja varmenteet
4.5.5.1.3	Kortin tunniste
4.5.5.1.4	Kortin haltijan tunnistetiedot
4.5.5.1.5	Tarkastustoimiin liittyvät tiedot
4.5.5.2	Ajopiirturin sukupolven 2 sovellus (ei voida käyttää ensimmäisen sukupolven ajoneuvoyksikössä)
4.5.5.2.1	Sovellusten tunnistetiedot
4.5.5.2.2	Avaimet ja varmenteet
4.5.5.2.3	Kortin tunniste
4.5.5.2.4	Kortin haltijan tunnistetiedot
4.5.5.2.5	Tarkastustoimiin liittyvät tiedot
4.5.6	Yrityskortti
4.5.6.1	Ajopiirturikortin sovellus (joka on ensimmäisen ja toisen sukupolven ajoneuvoyksikköjen käytettävissä)
4.5.6.1.1	Sovellusten tunnistetiedot
4.5.6.1.2	Avaimet ja varmenteet
4.5.6.1.3	Kortin tunniste

▼B

4.5.6.1.4	Kortin haltijan tunnistetiedot
4.5.6.1.5	Yrityksen toimenpiteitä koskevat tiedot
4.5.6.2	Ajopiirturin sukupolven 2 sovellus (ei voida käyttää ensimmäisen sukupolven ajoneuvoyksikössä)
4.5.6.2.1	Sovellusten tunnistetiedot
4.5.6.2.2	Avaimet ja varmenteet
4.5.6.2.3	Kortin tunniste
4.5.6.2.4	Kortin haltijan tunnistetiedot
4.5.6.2.5	Yrityksen toimenpiteitä koskevat tiedot
5.	VALVONTALAITTEEN ASENNUS
5.1	Asennus
5.2	Asennuskilpi
5.3	Sinetöinti
6.	TARKASTUKSET, MÄÄRÄAIKAISTARKASTUKSET JA KORJAUKSET
6.1	Asentajien, korjaamoiden ja ajoneuvovalmistajien hyväksyntä
6.2	Uusien tai korjattujen laitteiden tarkastaminen
6.3	Asennustarkastus
6.4	Määräaikaistarkastukset
6.5	Virheiden mittaus
6.6	Korjaukset
7.	KORTTIEN MYÖNTÄMINEN
8.	VALVONTALAITTEIDEN JA AJOPIIRTURIKORTTIEN TYYPPIHYVÄKSYNTÄ
8.1	Yleistä
8.2	Tietoturvatodistus
8.3	Toiminnallisuustodistus
8.4	Yhteentoimivuustodistus
8.5	Tyyppihyväksyntätodistus
8.6	Poikkeusmenettely: ensimmäiset yhteentoimivuustodistukset toisen sukupolven valvontalaitteille ja ajopiirturikorteille

JOHDANTO

Ensimmäisen sukupolven digitaalinen ajopiirturijärjestelmä on ollut käytössä 1. toukokuuta 2006 lähtien. Sitä voidaan käyttää kansallisessa liikenteessä sen elinkaaren loppuun saakka. Kansainvälisessä liikenteessä 15 vuoden kuluttua tämän komission asetuksen voimaantulosta kaikissa ajoneuvoissa on oltava säännösten mukainen tällä asetuksella käyttöön otettava toisen sukupolven älykäs ajopiirturi.

Tähän liitteeseen sisältyvät toisen sukupolven valvontalaitteita ja ajopiirturikortteja koskevat vaatimukset. Järjestelmän käyttöönottopäivästä lähtien ensimmäisen kerran rekisteröitäviin ajoneuvoihin asennetaan toisen sukupolven valvontalaitteet ja käyttöön otetaan toisen sukupolven ajopiirturikortit.

Jotta toisen sukupolven ajopiirturijärjestelmä saadaan otettua sujuvasti käyttöön,

▼B

— toisen sukupolven ajopiirturikortit suunnitellaan käytettäviksi myös ensimmäisen sukupolven ajoneuvoyksiköissä,

— voimassa olevien ensimmäisen sukupolven ajopiirturikorttien korvaamista ei pyydetä käyttöönottopäivänä.

Kuljettajat voivat siten pitää yksilöllisen kuljettajakortin ja käyttää sen perusteella kumpaakin järjestelmää.

Toisen sukupolven valvontalaite kuitenkin kalibroidaan pelkästään toisen sukupolven korjaamokortteja käyttämällä.

Tähän liitteeseen sisältyvät ensimmäisen ja toisen sukupolven ajopiirturijärjestelmien yhteensopivuuteen liittyvät kaikki vaatimukset.

Lisäyksessä 15 on lisätietoja siitä, miten kahta rinnakkaista järjestelmää hallitaan.

Luettelo lisäyksistä

Lisäys 1: DATAHAKEMISTO

Lisäys 2: AJOPIIRTURIKORTTIEN ERITTELY

Lisäys 3: KUVAKKEET

Lisäys 4: TULOSTEET

Lisäys 5: NÄYTTÖ

Lisäys 6: ETULEVYSSÄ OLEVA KALIBROINTI-/KOPIOINTILIITIN

Lisäys 7: TIETOJEN KOPIOINTIPROTOKOLLAT

Lisäys 8: KALIBROINTIPROTOKOLLA

Lisäys 9: TYYPPIHYVÄKSYNTÄ JA LUETTELO VÄHINTÄÄN VAADITTAVISTA TESTEISTÄ

Lisäys 10: TURVALLISUUSVAATIMUKSET

Lisäys 11: YHTEISET TURVALLISUUSMEKANISMIT

Lisäys 12: MAAILMANLAAJUISEEN SATELLIITTINAVIGOINTIJÄRJESTELMÄÄN (GNSS) PERUSTUVA PAIKANTAMINEN

Lisäys 13: ITS-RAJAPINTA

Lisäys 14: ETÄYHTEYSTOIMINTO

Lisäys 15: SIIRTYMINEN: ERI SUKUPOLVIEN LAITTEIDEN RINNAKKAISEN KÄYTÖN HALLINTA

Lisäys 16: MUUNNIN M1- JA N1-LUOKAN AJONEUVOJA VARTEN

1. MÄÄRITELMÄT

Tässä liitteessä tarkoitetaan

a) ”aktivoinnilla”

vaihetta, jossa ajopiirturi on täysin toimintavalmis ja toteuttaa kaikki toiminnot, turvallisuustoiminnot mukaan luettuina, korjaamokortin avulla;

b) ”todentamisella”

toimea, jonka tarkoitus on selvittää ja varmentaa väitetty henkilöllisyys;

c) ”autenttisuudella”

tiedon ominaisuutta, jonka toteutuessa tieto on peräisin lähteestä, jonka henkilöllisyys voidaan varmentaa;

d) ”sisäänrakennetulla testillä”

testiä, joka suoritetaan tarvittaessa, käyttäjän tai ulkoisten laitteiden käynnistämänä;

▼B

e) ”kalenteripäivällä”

vuorokautta, joka alkaa klo 00.00 ja päättyy klo 24.00. Kaikki kalenterivuorokaudet lasketaan UTC-ajan (Greenwichin yleisajan) mukaan;

f) ”kalibroinnilla” älykkään ajopiirturin osalta

datamuistiin tallennettujen ajoneuvon parametrien päivittämistä tai vahvistamista. Ajoneuvon parametreja ovat ajoneuvon tunnistetiedot (tunnistenumero, rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity) sekä ajoneuvon ominaisuuksia koskevat tiedot (w-, k- ja l-kertoimien ja -vakioiden arvot, rengaskoko, nopeudenrajoittimen asetukset (jos sellainen on), oikea UTC-aika, matkamittarin lukema); valvontalaiteen kalibroinnin aikana tyyppihyväksynnän kannalta asiaankuuluvat sinetöinnit on myös tallennettava datamuistiin.

Pelkän UTC-ajan päivitys tai vahvistus on katsottava ajan asetukseksi eikä kalibroinniksi edellyttäen, ettei se ole ristiriidassa vaatimuksen 409 kanssa.

Valvontalaitteen kalibrointiin tarvitaan korjaamokortti;

g) ”kortin numerolla”

16 aakkosnumeerista merkkiä sisältävää tunnusta, joka yksilöi jäsenvaltiossa käytettävän ajopiirturikortin. Kortin numero sisältää kortin haltijakohtaisen sarjanumeron (jos sellainen on käytössä), kortin korvausnumeron sekä kortin uusintanumeron.

Näin ollen kortin myöntäneen jäsenvaltion tunnus ja kortin numero yksilöivät kortin täydellisesti;

h) ”kortin haltijakohtaisella sarjanumerolla”

kortin numeron neljättätoista aakkosnumeerista merkkiä, jolla erotetaan toisistaan yrityksen, korjaamon tai valvontaelimen eri kortit. Niille voidaan myöntää useampia ajopiirturikortteja. Korttitunnuksen 13 ensimmäistä merkkiä yksilöivät täysin kyseisen yrityksen, korjaamon tai valvontaelimen;

i) ”kortin uusintanumerolla”

kortin numeron kuudettatoista aakkosnumeerista merkkiä, jonka arvoa suurennetaan aina, kun ajopiirturikortti uusitaan;

j) ”kortin korvausnumerolla”

kortin numeron viidettätoista aakkosnumeerista merkkiä, jonka arvoa suurennetaan aina, kun ajopiirturikortti korvataan;

k) ”ajoneuvon ominaiskertoimella”

numeerista tunnuslukua, jolla ilmaistaan sen lähtösignaalin arvo, jonka ajoneuvon se osa lähettää, joka yhdistää ajoneuvon valvontalaitteeseen (vaihteiston ulostuloakseli) silloin, kun ajoneuvo kulkee yhden kilometrin matkan normaaleissa testausolosuhteissa, kuten vaatimuksessa 414 määritetään. Ominaiskerroin ilmaistaan impulsseina kilometriä kohden (w = … imp/km);

l) ”yrityskortilla”

ajopiirturikorttia, jonka jäsenvaltion viranomaiset myöntävät ajopiirturilla varustettuja ajoneuvoja käyttävälle kuljetusyritykselle ja joka yksilöi kuljetusyrityksen ja mahdollistaa ajopiirturiin tallennettujen tämän kuljetusyrityksen lukitsemien tietojen näyttämisen, lataamisen ja tulostamisen;

▼B

m) ”valvontalaitteen vakiolla”

numeerista tunnuslukua, jolla ilmaistaan sen tulosignaalin arvo, joka tarvitaan yhden kuljetun kilometrin matkan näyttämiseksi ja tallentamiseksi; tämä vakio on ilmoitettava impulsseina kilometriä kohti (k = … imp/km);

n) valvontalaitteen laskemalla ”keskeytymättömällä ajoajalla” ([1])

tietyn kuljettajan kokonaisajoaikaa hänen viimeisen vähintään 45 minuuttia kestäneen AVAILABILITY (varallaolo)- tai BREAK/REST (tauko/lepo)- tai UNKNOWN ([2]) (tuntemattomat) -jaksonsa jälkeen (tämä jakso saattaa olla useina osina Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 561/2006 ([3]) mukaisesti). Kyseisissä laskelmissa otetaan tarpeen mukaan huomioon kuljettajakortille tallennetut aiemmat tapahtumat. Jos kuljettaja ei ole asettanut korttiaan laitteeseen, laskelmat perustuvat niihin datamuistin tietoihin, jotka liittyvät kuluvaan jaksoon, jolloin korttia ei ollut asetettuna laitteen asianmukaiseen aukkoon;

o) ”valvontakortilla”

ajopiirturikorttia, jonka jäsenvaltion viranomaiset myöntävät kansalliselle toimivaltaiselle valvontaviranomaiselle ja joka yksilöi valvontaelimen sekä mahdollisesti tarkastajan ja mahdollistaa datamuistiin tai kuljettajakortteihin sekä mahdollisesti korjaamokortteihin tallennettujen tietojen lukemisen, tulostamisen ja/tai lataamisen.

Sen on myös tarjottava pääsy kalibroinnin tarkastukseen tien varrella ja annettava käyttöön varhaiseen havaitsemiseen tarkoitetun etäyhteyslukijan tiedot;

p) valvontalaitteen laskemalla ”yhteenlasketulla taukoajalla” ([1])

tietyn kuljettajan yhteenlaskettua taukoaikaa, joka lasketaan vähintään 15 minuuttia kestävistä AVAILABILITY- tai BREAK/REST- tai UNKNOWN -jaksoista ([2]), jotka on vietetty hänen viimeisimmän vähintään 45 minuuttia kestäneen AVAILABILITY- tai BREAK/REST- tai UNKNOWN -jaksonsa ([3]) jälkeen (tämä jakso saattaa olla useina osina asetuksen (EY) N:o 561/2006 mukaisesti).

Kyseisissä laskelmissa otetaan tarpeen mukaan huomioon kuljettajakortille tallennetut aiemmat tapahtumat. Tuntemattomia jaksoja, joiden kesto on negatiivinen (tuntemattoman jakson alku on myöhempi kuin tuntemattoman jakson loppu) eri valvontalaitteiden aikojen päällekkäisyyksien vuoksi, ei oteta laskelmissa huomioon.

([1]) Tämän keskeytymättömän ajoajan ja yhteenlasketun taukoajan laskutavan ansiosta valvontalaite kykenee laskemaan keskeytymättömän ajoajan ylityksestä annettavan varoituksen. Se ei kuitenkaan kumoa näiden aikojen lainmukaista tulkintaa. Nämä määritelmät voidaan korvata käyttämällä keskeytymättömän ajoajan ja yhteenlasketun taukoajan vaihtoehtoisia laskutapoja, jos määritelmät ovat vanhentuneet muun asiaa koskevan lainsäädännön päivitysten vuoksi.

([2]) UNKNOWN (tuntemattomat) -jaksot ovat jaksoja, jolloin kuljettajan kortti ei ole ollut asetettuna valvontalaitteeseen ja joita vastaavia kuljettajan toimintaa koskevia tietoja ei ole syötetty käsin.

([3]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 561/2006, annettu 15 päivänä maaliskuuta 2006, tieliikenteen sosiaalilainsäädännön yhdenmukaistamisesta ja neuvoston asetusten (ETY) N:o 3821/85 ja (EY) N:o 2135/98 muuttamisesta sekä neuvoston asetuksen (ETY) N:o 3820/85 kumoamisesta (EUVL L 102, 11.4.2006, s. 1).

▼B

Jos kuljettaja ei ole asettanut korttiaan laitteeseen, laskelmat perustuvat niihin datamuistin tietoihin, jotka liittyvät kuluvaan jaksoon, jolloin korttia ei ollut asetettuna laitteen asianmukaiseen aukkoon;

q) ”tietomuistilla”

elektronista tietojen tallennuslaitetta, joka on osa valvontalaitetta;

r) ”digitaalisella allekirjoituksella”

tietokenttään lisättyä dataa tai tietokentän salakirjoitukseksi muunnettua sisältöä, jonka avulla vastaanottaja voi varmistautua tietokentän sisällön muuttamattomuudesta ja eheydestä;

s) ”lataamisella”

digitaalisesta ajopiirturista ajoneuvoyksikön datamuistiin tai ajopiirturikortin muistiin tallennettujen tiedostojen osittaista tai täydellistä kopiointia digitaalisesti allekirjoitettuna edellyttäen, että prosessi ei muuta tai poista mitään tallennettua tietoa.

Älykkääseen ajopiirturiin perustuvien ajoneuvoyksikköjen valmistajien ja sellaisten laitteiden valmistajien, jotka on suunniteltu ja tarkoitettu tiedostojen kopioimiseen, on kaikkien kohtuullisten toimenpiteiden avulla varmistettava, että kuljetusyritykset tai kuljettajat voivat suorittaa tällaisten tietojen kopioinnin niin, että aiheutetaan mahdollisimman vähän viivästystä.

Yksityiskohtaisen nopeustiedoston kopiointi ei ole välttämättä tarpeen asetuksen (EY) N:o 561/2006 noudattamiseksi, mutta sitä voidaan käyttää muihin tarkoituksiin, kuten onnettomuustutkintaan;

t) ”kuljettajakortilla”

ajopiirturikorttia, jonka jäsenvaltion viranomaiset myöntävät tietylle kuljettajalle ja joka yksilöi kuljettajan ja mahdollistaa tietojen tallentamisen kuljettajan toiminnasta;

u) ”pyörän renkaiden tehollisella ympärysmitalla”

ajoneuvoa liikuttavien pyörien (vetävien pyörien) yhden täyden kierroksen aikana kulkemien matkojen keskiarvoa. Nämä matkat on mitattava tavanomaisissa testausolosuhteissa, kuten vaatimuksessa 414 määritetään, ja ne on ilmaistava muodossa: ”l = … mm”. Ajoneuvojen valmistajat voivat näiden matkojen mittaamisen sijaan tehdä teoreettisen laskelman, jossa otetaan huomioon painon jakautuminen akseleille ajoneuvon ollessa kuormaamaton ja normaalissa ajokunnossa ([1]). Jäsenvaltioiden toimivaltaiset viranomaiset hyväksyvät tällaisissa teoreettisissa laskelmissa käytettävät menetelmät, ja ne voidaan tehdä ainoastaan ennen kuin ajopiirturi on aktivoitu;

v) ”tapahtumalla”

älykkään ajopiirturin havaitsemaa epänormaalia toimintoa, joka saattaa johtua petosyrityksestä;

w) ”ulkoisella GNSS-laitteistolla”

laitteistoa, joka sisältää GNSS-vastaanottimen, kun ajoneuvoyksikkö ei ole yksi yksikkö, ja muita osia, joita tarvitaan suojaamaan muualle ajoneuvoyksikköön tapahtuvaa sijaintitietojen siirtämistä;

([1]) Komission asetus (EU) N:o 1230/2012, annettu 12 päivänä joulukuuta 2012, Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 661/2009 täytäntöönpanosta moottoriajoneuvojen ja niiden perävaunujen massojen ja mittojen tyyppihyväksyntävaatimusten osalta sekä Euroopan parlamentin ja neuvoston direktiivin 2007/46/EY muuttamisesta (EUVL L 353, 21.12.2012, s. 31), sellaisena kuin se on viimeksi muutettuna.

▼B

x) ”vikatapahtumalla”

älykkään ajopiirturin havaitsemaa epänormaalia toimintaa, joka saattaa olla seurausta laitteen virheellisestä toiminnasta tai rikkoutumisesta;

y) ”GNNS-vastaanottimella”

elektronista laitetta, joka vastaanottaa ja käsittelee digitaalisesti signaaleja yhdestä tai useammasta maailmanlaajuisesta satelliittinavigointijärjestelmästä (englanniksi GNSS) ja jolla annetaan sijaintia, nopeutta ja ajankohtaa koskevia tietoja;

z) ”asentamisella”

ajopiirturin asentamista ajoneuvoon;

aa) ”yhteentoimivuudella”

järjestelmien ja niiden osan muodostavien toimintaprosessien kykyä datanvaihtoon sekä tiedon jakamiseen;

bb) ”rajapinnalla”

järjestelmien välistä menetelmäkokonaisuutta, jonka avulla ne voivat liittyä toisiinsa ja olla keskenään vuorovaikutuksessa;

cc) ”sijainnilla”

ajoneuvon maantieteellisiä koordinaatteja tietyllä hetkellä;

dd) ”liiketunnistimella”

ajopiirturin osaa, joka tuottaa ajoneuvon nopeutta ja/tai sen kulkemaa matkaa kuvaavan signaalin;

ee) ”kortilla, joka ei ole voimassa”

korttia, joka on havaittu vialliseksi tai jonka alkuvarmennus epäonnistui, jonka voimassaoloaika ei ole vielä alkanut tai jonka voimassaoloaika on loppunut;

ff) ”avoimella standardilla”

standardieritelmässä esitettyä standardia, joka on saatavilla maksutta tai nimellistä maksua vastaan ja joka on kopioitavissa, jaettavissa tai käytettävissä maksutta tai nimellistä maksua vastaan;

gg) ”asetuksen piiriin kuulumattomalla”

tilannetta, jossa asetuksen (EY) N:o 561/2006 säännöksien mukaisesti ei edellytetä valvontalaitteen käyttöä;

hh) ”ylinopeudella”

ajoneuvolle sallitun nopeuden ylittäminen, joksi määritellään mikä hyvänsä 60 sekuntia ylittävä aika, jonka kuluessa ajoneuvon nopeus ylittää sellaisen nopeudenrajoittimen asetusrajat, josta on säädetty neuvoston direktiivissä 92/6/ETY ([1]), sellaisena kuin se on viimeksi muutettuna;

ii) ”määräaikaistarkastuksella”

toimintasarjoja, joilla tarkistetaan se, että ajopiirturi toimii asianmukaisesti, se, että sen asetukset vastaavat ajoneuvon parametreja, ja se, ettei ajopiirturiin ole liitetty minkäänlaisia manipulointilaitteita;

([1]) Neuvoston direktiivi 92/6/ETY, annettu 10 päivänä helmikuuta 1992, tiettyjen moottoriajoneuvoluokkien nopeudenrajoittimien asentamisesta ja käytöstä yhteisössä (EYVL L 57, 2.3.1992, s. 27).

▼B

jj) ”tulostimella”

valvontalaitteen osaa, jolla tulostetaan tallennettuja tietoja;

kk) ”varhaiseen havaitsemiseen tarkoitetulla etäyhteydellä”

varhaiseen havaitsemiseen tarkoitetun etäviestintäjärjestelmän ja varhaiseen havaitsemiseen tarkoitetun etäyhteyslukijan välistä yhteyttä kohdistetuissa tienvarsitarkastuksissa, jolla pyritään havaitsemaan etäältä valvontalaitteen mahdollinen manipulointi tai väärinkäyttö;

ll) ”etäviestintälaitteistolla”

ajoneuvoyksikön laitteita, joita käytetään kohdistettujen tienvarsitarkastuksien tekemiseksi;

mm) ”varhaiseen havaitsemiseen tarkoitetulla etäyhteyslukijalla”

kohdistettujen tienvarsitarkastusten tarkastajien käyttämää järjestelmää;

nn) ”uusimisella”

uuden ajopiirturikortin myöntämistä entisen vanhentuessa tai silloin, kun entinen toimii virheellisesti ja on palautettu sen myöntäneelle viranomaiselle. Uusimistapauksissa on aina oltava varmuus siitä, ettei samanaikaisesti ole olemassa kahta voimassa olevaa korttia;

oo) ”korjaamisella”

ajoneuvon liiketunnistimen tai ajoneuvoyksikön taikka liitäntäkaapelin korjaamista, joka vaatii sen voimalähteen irti kytkemistä tai sen irrottamista ajopiirturin muista osista tai liiketunnistimen tai ajoneuvoyksikön avaamista;

pp) ”kortin korvaamisella”

ajopiirturikortin myöntämistä korvaamaan entinen kortti, joka on ilmoitettu kadonneeksi, varastetuksi tai epäkuntoiseksi ja jota ei ole palautettu sen myöntäneelle viranomaiselle. Korvaustapauksissa on aina olemassa vaara, että samanaikaisesti on olemassa kaksi voimassa olevaa korttia;

qq) ”turvavarmennuksella”

yleisiä perusteita käsittelevän sertifiointielimen suorittamaa toimenpidettä sen varmentamiseksi, että tutkittava valvontalaite (tai sen osa) tai ajopiirturikortti täyttää ne tietoturvavaatimukset, jotka on määritelty asiaankuuluvissa suojausprofiileissa;

rr) ”laitteen itse suorittamalla testillä”

testiä, jonka valvontalaite suorittaa säännöllisesti ja automaattisesti vikojen havaitsemiseksi;

ss) ”ajanmittauksella”

UTC-päivämäärän ja -ajan jatkuvaa digitaalista kirjaamista;

tt) ”ajan asetuksella”

kuluvan ajan automaattista asetusta säännöllisin väliajoin yhden minuutin enimmäisvirheen puitteissa tai kalibroinnin yhteydessä suoritettua asetusta;

uu) ”rengaskoolla”

neuvoston direktiivin 92/23/ETY ([1]), sellaisena kuin se on viimeksi muutettuna, mukaista renkaiden (ulkorenkaiden) koon määritettä;

([1]) Neuvoston direktiivi 92/23/ETY, annettu 31 päivänä maaliskuuta 1992, moottoriajoneuvojen ja niiden perävaunujen renkaista ja renkaiden asentamisesta (EYVL L 129, 14.5.1992, s. 95).

▼B

vv) ”ajoneuvon tunnistuksella”

ajoneuvon yksilöivää tunnusta: ajoneuvon rekisteritunnusta siihen liittyvine tietoineen rekisteröintijäsenvaltiosta ja valmistenumeroa ([1]);

ww) valvontalaitteen ”viikolla” tietojenkäsittelytarkoituksessa

ajanjaksoa maanantaista klo 00.00 UTC-aikaa sunnuntaihin klo 24.00 UTC-aikaa;

xx) ”korjaamokortilla”

ajopiirturikorttia, jonka jäsenvaltion viranomaiset myöntävät kyseisen jäsenvaltion hyväksymien ajopiirturien valmistajan nimetylle henkilöstölle, asentajalle, ajoneuvovalmistajalle tai korjaamolle ja joka yksilöi kortin haltijan ja mahdollistaa ajopiirtureiden testaamisen, kalibroimisen, aktivoinnin ja/tai niissä olevien tietojen lataamisen;

yy) ”muuntimella”

valvontalaitteen osaa, joka tuottaa ajoneuvon nopeutta ja/tai sen kulkemaa matkaa jatkuvasti kuvaavan signaalin, joka on muu kuin se, jota käytetään riippumattomaan liikkeen havaitsemiseen, ja joka on

— asennettu M1- ja N1-luokan ajoneuvoon ja jota käytetään ainoastaan M1- ja N1-luokan ajoneuvoissa (siten kuin ne on määritelty Euroopan parlamentin ja direktiivin 2007/46/EY ([2]) liitteessä II, sellaisena kuin se on viimeksi muutettuna), jotka on otettu käyttöön 1 päivän toukokuuta 2006 jälkeen,

— joka on asennettu paikkaan, johon ei ole mekaanisesti mahdollista asentaa minkään muun tyyppistä olemassa olevaa liiketunnistinta, joka on muutoin tämän liitteen ja sen lisäysten 1–15 määräysten mukainen,

— joka on asennettu ajoneuvoyksikön ja sen pisteen väliin, jossa integroidut anturit tai vaihtoehtoiset rajapinnat tuottavat nopeus- ja etäisyysimpulsseja,

— ja ajoneuvoyksikön kannalta muunnin käyttäytyy samalla tavoin kuin jos ajoneuvoyksikköön olisi liitetty tämän liitteen ja sen lisäysten 1–16 määräysten mukainen liiketunnistin.

Tällaisen muuntimen käytön edellä kuvatuissa ajoneuvoissa on mahdollistettava tämän liitteen kaikkien vaatimusten mukaisen ajoneuvoyksikön asentaminen ja asianmukainen käyttö.

Mainittujen ajoneuvojen älykkääseen ajopiirturiin sisältyvät kaapelit, muunnin ja ajoneuvoyksikkö;

([1]) Neuvoston direktiivi 76/114/ETY, annettu 18 päivänä joulukuuta 1975, moottoriajoneuvojen ja niiden perävaunujen lakisääteisiä kilpiä ja merkintöjä sekä niiden sijaintia ja kiinnitysmenetelmää koskevan jäsenvaltioiden lainsäädännön lähentämisestä (EYVL L 24, 30.1.1976, s. 1).

([2]) Euroopan parlamentin ja neuvoston direktiivi 2007/46/EY, annettu 5 päivänä syyskuuta 2007, puitteiden luomisesta moottoriajoneuvojen ja niiden perävaunujen sekä tällaisiin ajoneuvoihin tarkoitettujen järjestelmien, osien ja erillisten teknisten yksiköiden hyväksymiselle (Puitedirektiivi) (EUVL L 263, 9.10.2007, s. 1).

▼B

zz) ”tietojen eheydellä”

tallennetun tiedon tarkkuutta ja johdonmukaisuutta, jonka osoittaa se, ettei tietoja ole muutettu tietyn tietueen kahden päivityksen välillä. Eheys merkitsee, että tiedot ovat tarkka kopio alkuperäisestä versiosta, eli ne eivät ole vaurioituneet silloin kuin niitä on kirjattu ajopiirturikortille tai erityislaitteistoon tai luettu niiltä taikka silloin, kuin niitä on siirretty viestintäkanavan kautta;

aaa) ”tietosuojalla”

yleisiä teknisiä toimenpiteitä, joita on toteutettu Euroopan parlamentin ja neuvoston direktiivin 95/46/EY ([1]) sekä Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY ([2]) periaatteiden panemiseksi asianmukaisesti täytäntöön;

bbb) ”älykkäällä ajopiirturijärjestelmällä”

valvontalaitetta, ajopiirturikortteja ja kaikkia suoraan tai epäsuorasti vuorovaikutuksessa olevia laitteita niiden rakentamisen, asennuksen, käytön, testauksen ja valvonnan aikana, kuten kortteja, etäyhteyslukijaa ja kaikkia muita laitteita, jotka koskevat esim. datan lataamista, data-analyysia, kalibrointia, turvatekijöiden luomista, hallinnointia tai käyttöönottoa;

ccc) ”käyttöönottopäivämäärällä”

36 kuukautta Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 165/2014 ([3]) 11 artiklassa viitattujen yksityiskohtaisten säännösten voimaantulosta.

Tämä on päivämäärä, jolloin ensimmäisen kerran rekisteröidyt ajoneuvot

— *varustetaan ajopiirturilla, joka on liitetty satelliittinavigointijärjestelmään perustuvaan paikannuspalveluun*

— *voivat välittää tietoja kohdistettuihin tienvarsitarkastuksiin toimivaltaisille valvontaviranomaisille, kun ajoneuvo on liikkeessä*

— *voidaan varustaa standardien mukaisilla rajapinnoilla, jotka mahdollistavat sen, että ulkoinen laite voi käyttää normaalitilassa ajopiirturin kirjaamia tai tuottamia tietoja.*

ddd) ”turvavarmenteella”

asiakirjaa, jota käytetään osana sertifiointimenettelyä yleisten perusteiden mukaisesti ja jolla pannaan täytäntöön riippumaton eritelmä tietoturvavaatimuksista;

([1]) Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 281, 23.11.1995, s. 31).

([2]) Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) (EYVL L 201, 31.7.2002, s. 37).

([3]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 165/2014, annettu 4 päivänä helmikuuta 2014, tieliikenteessä käytettävistä ajopiirtureista, tieliikenteen valvontalaitteista annetun neuvoston asetuksen (ETY) N:o 3821/85 kumoamisesta sekä tieliikenteen sosiaalilainsäädännön yhdenmukaistamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 561/2006 muuttamisesta (EUVL L 60, 28.2.2014, s. 1).

▼B

eee) ”GNSS-tietojen tarkkuudella”

kun kyse on maailmanlaajuisen satelliittinavigointijärjestelmän paikkatietojen tallentamisesta ajopiirtureilla, HDOP-arvoa (Horizontal Dilution of Precision), joka lasketaan vähimmäisarvona käytössä olevilla GNSS-järjestelmillä kerätyistä HDOP-arvoista.

2. VALVONTALAITTEIDEN YLEISET OMINAISUUDET JA TOIMINNOT

2.1 **Yleiset ominaisuudet**

Valvontalaitteen tarkoitus on kirjata, tallentaa, näyttää, tulostaa paperille ja muulla tavoin tulostaa kuljettajan toimintaan liittyviä tietoja.

Ajoneuvossa, johon on asennettu tämän liitteen määräysten mukainen valvontalaite, on oltava nopeus- ja matkamittari. Nämä toiminnot voivat kuulua osana valvontalaitteeseen.

1) Valvontalaite koostuu kaapeleista, liiketunnistimesta ja ajoneuvoyksiköstä.

2) Liiketunnistinten ja ajoneuvoyksikköjen välinen rajapinta on lisäyksen 11 vaatimusten mukainen.

3) Ajoneuvoyksikkö on liitettävä maailmanlaajuiseen satelliittinavigointijärjestelmään, kuten lisäyksessä 12 määritellään.

4) Ajoneuvoyksikkö on yhteydessä varhaiseen havaitsemiseen tarkoitettuun etäyhteysjärjestelmään, kuten lisäyksessä 14 määritellään.

5) Ajoneuvoyksikköön voi sisältyä ITS-rajapinta, joka määritellään lisäyksessä 13.

Valvontalaite voidaan liittää muihin järjestelmiin täydentävien rajapintojen ja/tai valinnaisen ITS-rajapinnan välityksellä.

6) Mikään valvontalaitteeseen lisätty tai liitetty toiminto, laite tai laitteisto, riippumatta siitä, onko sillä hyväksyntä tai ei, ei saa häiritä tai kyetä häiritsemään valvontalaitteen asianmukaista ja turvallista toimintaa tai olla ristiriidassa tämän asetuksen säännösten kanssa.

Valvontalaitteen käyttäjät antavat laitteelle tunnistetietonsa ajopiirturikorttien avulla.

7) Valvontalaite antaa valikoidut tietojen ja toimintojen käyttöoikeudet käyttäjätyypin ja/tai käyttäjän henkilöllisyyden perusteella.

Valvontalaite kirjaa ja tallentaa tietoja datamuistiinsa, etäviestintälaitteistoon ja ajopiirturikorteille.

Tämä tehdään yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun direktiivin 95/46/EY ([1]), henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12 päivänä heinäkuuta 2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY ([2]) sekä asetuksen (EU) N:o 165/2014 7 artiklan mukaisesti.

([1]) EYVL L 281, 23.11.1995, s. 31.
([2]) EYVL L 201, 31.7.2002, s. 37.

▼B

2.2 **Toiminnot**

8) Valvontalaitteen on huolehdittava seuraavista toiminnoista:

— korttien paikoilleen asetuksen ja poistamisen valvonta,

— nopeuden, matkan ja sijainnin mittaus,

— ajanmittaus,

— kuljettajan toiminnan valvonta,

— ajoneuvon miehityksen valvonta,

— kuljettajan käsin syöttämät tiedot:

— tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy

— kuljettajan toimintaa koskevien tietojen syöttö käsin

— erityisolosuhteita koskevien tietojen syöttö,

— yritysten tekemien lukitusten hallinta,

— tarkastustoimien hallinta,

— tapahtumien ja/tai vikojen havaitseminen,

— sisäänrakennetut ja laitteen itse suorittamat testit,

— tietojen haku datamuistista,

— tietojen kirjaaminen ja tallentaminen datamuistiin,

— tietojen haku ajopiirturikorteilta,

— tietojen kirjaaminen ja tallentaminen ajopiirturikorteille,

— tietojen näyttö,

— tietojen tulostus,

— varoitukset,

— tietojen kopiointi ulkoisille tietovälineille,

— etäyhteys kohdistetuille tienvarsitarkistuksille,

— tietojen tulostaminen muille järjestelmille,

— kalibrointi,

— kalibroinnin tarkastus tien varrella,

— ajan asetus.

2.3 **Toimintatilat**

9) Valvontalaitteella on oltava neljä toimintatilaa:

— normaalitila,

— tarkastustila,

— kalibrointitila,

— yritystila.

10) Valvontalaitteen on siirryttävä seuraaviin toimintatiloihin liitäntälaitteisiin asetettujen voimassa olevien ajopiirturikorttien mukaisesti. Ajopiirturikortin sukupolvella ei ole merkitystä toimintatilan määrittelyssä, jos sisään asetettu kortti on voimassa. Ensimmäisen sukupolven korjaamokorttia on pidettävä aina muuna kuin voimassa olevana korttina, kun se asennetaan toisen sukupolven ajoneuvoyksikköön.

▼B

Toimintatila		Kuljettajan korttiaukko				
		Ei korttia	Kuljettajakortti	Valvontakortti	Korjaamokortti	Yrityskortti
Apukuljettajan korttiaukko	Ei korttia	Toiminnallinen	Toiminnallinen	Tarkastustoimi	Kalibrointi	Yritys
	Kuljettajakortti	Toiminnallinen	Toiminnallinen	Tarkastustoimi	Kalibrointi	Yritys
	Valvontakortti	Tarkastustoimi	Tarkastustoimi	Tarkastustoimi (*)	Toiminnallinen	Toiminnallinen
	Korjaamokortti	Kalibrointi	Kalibrointi	Toiminnallinen	Kalibrointi (*)	Toiminnallinen
	Yrityskortti	Yritys	Yritys	Toiminnallinen	Toiminnallinen	Yritys (*)

(*) Tällaisissa tilanteissa valvontalaitteen on käytettävä ainoastaan kuljettajan korttiaukkoon asetettua ajopiirturikorttia.

11) Valvontalaite ei saa hyväksyä siihen asetettuja kortteja, jotka eivät ole voimassa, mutta vanhentuneella kortilla olevien tietojen näyttämisen, tulostamisen tai kopioinnin on oltava mahdollista.

12) Kaikkien 2.2 kohdassa lueteltujen toimintojen on oltava käytettävissä kaikissa toimintatiloissa seuraavin poikkeuksin:

— kalibrointitoiminto on käytettävissä vain kalibrointitilassa,

— kalibroinnin tarkastustoiminto tien varrella on käytettävissä vain tarkastustilassa,

— yritysten tekemien lukitusten hallintatoiminto on käytettävissä vain yritystilassa,

— tarkastustoimien hallintatoiminto on käytettävissä vain tarkastustilassa,

— kopiointitoiminto ei ole käytettävissä normaalitilassa (paitsi vaatimuksessa 193 kuvatuissa tapauksissa) lukuun ottamatta kuljettajakortin kopiointia, kun ajoneuvoyksikköön ei ole asetettu mitään muuta korttityyppiä.

13) Valvontalaite voi tulostaa kaikkia tietoja näyttöön, tulostimeen tai ulkoisiin liitäntälaitteisiin seuraavin poikkeuksin:

— normaalitilassa sellaiset henkilötiedot (sukunimi ja etunimi (-nimet)), jotka eivät vastaa laitteeseen asetettua ajopiirturikorttia, tulostetaan tyhjinä, ja sellaiset korttinumerot, jotka eivät vastaa laitteeseen asetettua ajopiirturikorttia, tulostetaan osittain tyhjinä (jokainen poikkeava merkki – vasemmalta oikealle – tulostetaan tyhjänä),

— yritystilassa voidaan kuljettajaan liittyviä tietoja (vaatimukset 102, 105 ja 108) tulostaa vain jaksoilta, joissa ei ole lukitusta tai joita mikään muu yritys (joka yksilöidään yrityskortin numeron 13 ensimmäisen numeron avulla) ei ole lukinnut,

— kun valvontalaitteeseen ei ole asetettu mitään korttia, kuljettajaan liittyvien tietojen tulostaminen on mahdollista vain kuluvan ja kahdeksan edellisen kalenterivuorokauden osalta,

— ajoneuvoyksiköstä peräisin olevia henkilötietoja ei tulosteta ajoneuvoyksikön ITS-järjestelmän kautta, ellei varmisteta, että kuljettaja, jota tiedot koskevat, antaa siihen suostumuksensa,

▼B

— ajoneuvoyksikköjen tavanomainen käyttöaika on 15 vuotta ajoneuvoyksikön todistusten myöntämispäivästä lähtien, mutta ajoneuvoyksikköjä voidaan käyttää vielä kolme kuukautta yksinomaan datan lataamiseen.

2.4 **Turvallisuus**

Järjestelmän tietoturvan tavoitteena on suojata datamuistia siten, että se ehkäisee tietojen luvattoman käytön ja muuttamisen sekä havaitsee näiden yritykset, suojaa liiketunnistimen ja ajoneuvoyksikön välillä siirrettävien tietojen eheyttä ja muuttamattomuutta, suojaa valvontalaitteen ja ajopiirturikorttien välillä siirrettävien tietojen eheyttä ja muuttamattomuutta, suojelee valvontalaitteen ja ulkoisen GNSS-laitteiston välillä siirrettävien tietojen eheyttä ja muuttumattomuutta, suojelee varhaiseen havaitsemiseen tarkoitetun etäyhteyslukijan välityksellä valvontatarkoituksessa siirrettävien tietojen luottamuksellisuutta, eheyttä ja muuttamattomuutta sekä varmistaa kopioitavien tietojen eheyden ja muuttamattomuuden.

14) Järjestelmän turvallisuuden saavuttamiseksi seuraavien osien on täytettävä tietoturvavaatimukset, jotka on määritelty niiden suojausprofiilissa, kuten lisäyksessä 10 edellytetään:

— ajoneuvoyksikkö,

— ajopiirturikortti,

— liiketunnistin,

— ulkoinen GNSS-laitteisto (tätä profiilia tarvitaan ja sovelletaan ainoastaan ulkoista GNSS-laitteistoa koskevaan vaihtoehtoon).

3. VALVONTALAITTEIDEN RAKENNETTA JA TOIMINTOJA KOSKEVAT VAATIMUKSET

3.1 **Korttien paikoilleen asettamisen ja poistamisen seuranta**

15) Valvontalaitteen on valvottava korttien liitäntälaitteita, jotta se havaitsee korttien paikoilleen asetuksen ja poistamisen.

16) Korttia sisään asetettaessa valvontalaitteen on tunnistettava, onko sisään asetettu kortti voimassa oleva ajopiirturikortti, ja jos on, tunnistaa sen tyyppi ja sen sukupolvi.

Jos kortti, jolla on sama korttinumero ja korkeampi uusintanumero on jo asetettu valvontalaitteeseen, korttia ei pidetä voimassa olevana.

Jos kortti, jolla on sama korttinumero ja uusintanumero, mutta jonka korvausnumero on suurempi, on jo asetettu valvontalaitteeseen, korttia ei pidetä voimassa olevana.

17) Valvontalaitteiden on pidettävä ensimmäisen sukupolven ajopiirturikortteja muina kuin voimassaolevina, kun korjaamo poistaa mahdollisuuden käyttää ensimmäisen sukupolven ajopiirturikortteja, lisäystä 15 noudattaen (vaatimus MIG003).

18) Ensimmäisen sukupolven korjaamokortteja, jotka asennetaan toisen sukupolven valvontalaitteeseen, ei pidetä voimassa olevina.

▼B

19) Valvontalaitteen on oltava suunniteltu siten, että ajopiirturikortit lukittuvat paikoilleen, kun ne on asetettu oikein korttien liitäntälaitteisiin.

20) Ajopiirturikorttien paikoilleen lukituksen avaus saa toimia vain ajoneuvon ollessa pysähtyneenä ja vasta silloin, kun kaikki asianmukaiset tiedot on tallennettu korteille. Korttien paikoilleen lukituksen avautuminen saa tapahtua vain avaajan nimenomaisesta toimenpiteestä.

3.2 **Nopeuden, sijainnin ja matkan mittaus**

21) Liiketunnistin (joka on mahdollisesti sulautettu muuntimeen) on nopeuden ja matkan mittauksen pääasiallinen lähde.

22) Tämän toiminnon on jatkuvasti mitattava matkamittarin lukemaa ja kyettävä antamaan lukema, joka vastaa ajoneuvon kulkemaa kokonaismatkaa käyttämällä liiketunnistimen tarjoamia pulsseja.

23) Tämän toiminnon on jatkuvasti mitattava ajoneuvon nopeutta ja kyettävä antamaan nopeuslukema käyttämällä liiketunnistimen tarjoamia pulsseja.

24) Nopeudenmittaustoiminnon on myös annettava tieto siitä, onko ajoneuvo liikkeessä vai pysähtyneenä. Ajoneuvon katsotaan olevan liikkeessä, kun toiminto havaitsee liiketunnistimelta useamman kuin yhden impulssin sekunnissa vähintään viiden sekunnin ajan; muussa tapauksessa ajoneuvon katsotaan olevan pysähtyneenä.

25) Tämän asetuksen mukaisella valvontalaitteella varustettuihin ajoneuvoihin asennettujen laitteiden, jotka osoittavat nopeutta (nopeusmittari) ja kokonaismatkaa (matkamittari), on oltava tässä liitteessä (ks. 3.2.1 ja 3.2.2 kohta) vahvistettujen suurimpia sallittuja toleransseja koskevien vaatimusten mukainen.

26) Jotta liikedatan käsittely voidaan havaita, liiketunnistimen tiedot on vahvistettava ajoneuvon liikettä koskevien tietojen avulla, jotka ovat peräisin GNSS-vastaanottimesta ja vaihtoehtoisesti muista liiketunnistimesta erillisistä lähteistä.

27) Tämän toiminnon on mitattava ajoneuvon sijaintia, jotta voidaan automaattisesti tallentaa:

— sijainnit, joissa kuljettajan ja/tai apukuljettajan päivän työaika alkaa,

— sijainnit, joissa kuljettajan keskeytymätön ajoaika on yli kolmen tunnin jakso,

— sijainnit, joissa kuljettajan ja/tai apukuljettajan päivän työaika päättyy.

3.2.1 *Kuljetun matkan mittaus*

28) Kuljettu matka voidaan mitata joko:

— eteen- ja taaksepäin kuljettujen matkojen summana, tai

— ainoastaan eteenpäin tapahtuneen liikkeen osalta.

29) Valvontalaitteen on mitattava matkaa välillä 0–9 999 999,9 km.

▼B

30) Mitatun matkan on oltava seuraavissa virherajoissa (koskee vähintään 1 000 metrin pituisia matkoja):

— ± 1 % ennen asennusta,

— ± 2 % asennettuna ja määräaikaistarkastusten aikana,

— ± 4 % normaalikäytössä.

31) Mitatun matkan lukematarkkuuden on oltava 0,1 km tai parempi.

3.2.2 *Nopeuden mittaus*

32) Valvontalaitteen on mitattava nopeutta välillä 0–220 km/t.

33) Jotta varmistetaan osoitetun nopeuden enimmäisvirheeksi ± 6 km/t normaalikäytössä ja kun otetaan huomioon:

— sisääntulosignaalin vaihtelusta (renkaiden eroista, …) aiheutuva virhe suuruudeltaan ± 2 km/t,

— asennuksen tai määräaikaistarkastusten yhteydessä tehtyjen mittauksien virhe suuruudeltaan ± 1 km/t,

valvontalaitteen on nopeusalueella 20–180 km/t ja ajoneuvon ominaiskertoimen ollessa välillä 4 000–25 000 imp/km kyettävä mittaamaan nopeus tarkkuudella ± 1 km/t (ajettaessa tasaista nopeutta).

Huomautus: tiedontallennuksen lukematarkkuus aiheuttaa valvontalaitteen tallentamaan nopeuslukemaan lisävirheen suuruudeltaan ± 0,5 km/t.

34) Nopeuden mittauksen on tapahduttava oikein ja normaaleissa virherajoissa kahden sekunnin kuluessa siitä, kun nopeuden muutos on päättynyt, kun nopeuden muutosnopeus on enintään 2 m/s^2.

35) Nopeuden mittauksen lukematarkkuuden on oltava 1 km/t tai parempi.

3.2.3 *Sijainnin mittaus*

36) Valvontalaitteen on mitattava ajoneuvon täydellinen sijainti GNSS-vastaanotinta käyttämällä.

37) Täydellinen sijainti mitataan maantieteellisinä koordinaatteina: leveys- ja pituusasteina, asteina ja minuutteina minuutin kymmenesosan tarkkuudella.

3.3 **Ajanmittaus**

38) Ajanmittaustoiminnon on mitattava jatkuvasti UTC-päivämäärä ja -aika ja annettava ne digitaalimuodossa.

39) UTC-päivämäärää ja -aikaa on käytettävä valvontalaitteen sisällä olevan tiedon päiväyksiin (tallenteet, tietojen siirto) ja kaikkiin lisäyksessä 4 ”Tulosteet” määritettyihin tulosteisiin.

40) Paikallisen ajan näyttämiseksi on näytettävän ajan ero UTC-aikaan nähden oltava aseteltavissa puolen tunnin välein. Muut ajan erot UTC-aikaan nähden kuin puolen tunnin negatiiviset tai positiiviset kerrannaiset eivät ole sallittuja.

41) Kellon käyntitarkkuuden on tyyppihyväksyntää vastaavissa olosuhteissa oltava rajoissa ± 2 sekuntia/päivä ajan asetusten puuttuessa.

▼B

42) Mitatun ajan lukematarkkuuden on oltava 1 sekunti tai parempi.

43) Ulkoisen virtalähteen kytkeminen pois lyhyemmäksi kuin 12 kuukauden ajaksi ei saa vaikuttaa ajanmittaukseen tyyppihyväksyntää vastaavissa olosuhteissa.

3.4 **Kuljettajan toiminnan seuranta**

44) Tämän toiminnon on jatkuvasti ja erikseen seurattava yhden kuljettajan ja yhden apukuljettajan toimintaa.

45) Kuljettajan toimintaa on DRIVING (ajo), WORK (työ), AVAILABILITY (varallaolo) tai BREAK/REST (tauko/lepo).

46) Kuljettajan ja/tai apukuljettajan on kyettävä käsin valitsemaan WORK, AVAILABILITY tai BREAK/REST.

47) Kun ajoneuvo on liikkeessä, laitteen on automaattisesti valittava kuljettajalle DRIVING ja apukuljettajalle AVAILABILITY.

48) Kun ajoneuvo pysähtyy, laitteen on automaattisesti valittava kuljettajalle WORK.

49) Ensimmäinen REST-toiminnan tai AVAILABILITY-toiminnan muutos, joka tapahtuu 120 sekunnin kuluessa siitä, kun ajoneuvon pysäyttäminen aiheutti WORK-toiminnan automaattisen valinnan, katsotaan tapahtuneeksi sillä hetkellä, kun ajoneuvo pysähtyi (ja sen vuoksi tämä toiminta mahdollisesti peruuttaa valinnan WORK).

50) Tämän toiminnon on tulostettava toiminnan muutokset tallennustoiminnoille yhden minuutin tarkkuudella.

51) Jos toiminnaksi on kirjattu DRIVING sekä tiettyä kalenteriminuuttia välittömästi edeltävän minuutin että sitä välittömästi seuraavan minuutin aikana, katsotaan koko minuutti kuluneeksi DRIVING-toiminnassa.

52) Jos tiettyä kalenteriminuuttia ei vaatimuksen 051 nojalla katsota kuluneeksi DRIVING-toiminnassa, katsotaan koko minuutin kuluneen siinä toiminnassa, joka edustaa pisintä yhtäjaksoista toimintaa kyseisen minuutin aikana (tai viimeisintä yhtä pitkistä pisimmistä jaksoista).

53) Tämän toiminnon on myös jatkuvasti valvottava keskeytymätöntä ajoaikaa ja kuljettajan yhteenlaskettua taukoaikaa.

3.5 **Ajoneuvon miehityksen seuranta**

54) Tämä toiminto valvoo jatkuvasti ja automaattisesti ajoneuvon miehitystä.

55) Valvontalaitteen on automaattisesti valittava asetus CREW (miehistö), kun siihen on asetettu kaksi voimassa olevaa kuljettajakorttia; muissa tapauksissa sen on valittava asetus SINGLE (yksin).

3.6 **Kuljettajan syöttämät tiedot**

3.6.1 *Tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy*

56) Tämän toiminnan avulla voidaan antaa tiedot paikasta, jossa kuljettajan/apukuljettajan mukaan päivän työaika alkaa ja/tai päättyy.

▼B

57) Paikat määritellään valtion ja tarvittaessa myös alueen tarkkuudella, ja ne syötetään tai vahvistetaan käsin.

58) Kun kuljettajakortti poistetaan, valvontalaitteen on kehotettava (apu)kuljettajaa syöttämään ”tiedot paikasta, jossa päivän työaika päättyy”.

59) Kuljettaja syöttää sen jälkeen ajoneuvon senhetkisen paikkatiedon, jota pidetään tilapäisenä tietona.

60) Päivän työajan alkamis- ja/tai päättymispaikkoja koskevien tietojen syöttämisen on oltava mahdollista valikkokomentojen avulla. Jos yhden kalenteriminuutin kuluessa syötetään enemmän kuin yhdet tiedot, vain kyseisen ajanjakson kuluessa syötetyt viimeisen alkamispaikan tiedot ja viimeisen päättymispaikan tiedot säilyvät tallennettuina.

3.6.2 *Kuljettajan toimintaa koskevien tietojen syöttö käsin ja ITS-rajapintaan liittyvä kuljettajan suostumus*

61) Asetettaessa paikoilleen kuljettajakorttia (tai korjaamokorttia), ja ainoastaan tällöin, valvontalaitteen on sallittava toimintaan liittyvien tietojen syöttö käsin. Toimintaan liittyvät tiedot syötetään käsin käyttäen ajoneuvoyksikölle kulloinkin määritetyn aikavyöhykkeen (aikaero UTC-aikaan nähden) paikallisia aika- ja päivämääräarvoja.

Asetettaessa paikoilleen kuljettaja- tai korjaamokorttia kortin haltijalle on kerrottava:

— päivämäärä ja aika, jolloin tämä edellisen kerran poisti korttinsa,

— valinnaisesti: ajoneuvoyksikölle kulloinkin asetettu paikallisen ajan ero UTC-aikaan nähden.

Ajoneuvoyksikölle tuntematonta kuljettajakorttia tai korjaamokorttia ensimmäistä kertaa asetettaessa kortin haltijalta pyydetään suostumusta ajopiirturiin liittyvään henkilötietojen tulostamiseen vaihtoehtoisen ITS-järjestelmän rajapinnan kautta.

Kuljettajan (tai korjaamon) suostumus voidaan milloin tahansa ottaa käyttöön tai poistaa käytöstä valikkokomennoilla, jos kuljettajakortti (tai korjaamokortti) on asetettu yksikköön.

Toimintaan liittyviä tietoja on voitava syöttää seuraavin rajoituksin:

— toiminnan tyyppi on WORK (työ), AVAILABILITY (varallaolo) tai BREAK/REST (tauko/lepo),

— kunkin toiminnan aloitus- ja päättymisaikojen on oltava ajanjaksolta kortin viimeisen poistamisen ja tällä hetkellä tapahtuneen paikoilleen asettamisen välillä,

— Toimintatietojen ajoissa ei saa olla päällekkäisyyksiä.

Tietojen syötön käsin on oltava tarvittaessa mahdollista, kun aikaisemmin käyttämätön kuljettajakortti (tai korjaamokortti) asetetaan paikalleen ensimmäisen kerran.

▼B

Toimintatietojen käsin syöttämistä koskevan menettelyn on sisällettävä niin monta peräkkäistä vaihetta kuin on tarpeen kunkin toiminnan tyypin, aloitusajan ja päättymisajan asettamiseksi. Kortin haltijalla on oltava mahdollisuus olla ilmoittamatta toiminnasta miltä tahansa sen aikavälin osalta, joka on kulunut kortin viimeisestä poistamisesta tähän paikoilleen asettamiseen.

Kortin paikoilleen asettamiseen liittyvän tietojen käsin syötön aikana ja siltä osin kuin se tulee kyseeseen, kortin haltijalla on oltava mahdollisuus syöttää:

— paikka, jossa edellinen päivän työaika päättyi, asiaankuuluvaan aikaan liittyvänä (eli viimeisimmän poiston yhteydessä syötettyjen tietojen päälle kirjoitetaan uusi tieto),

— paikka, jossa nykyinen päivän työaika alkaa, asiaankuuluvaan aikaan liittyvänä.

Jos kortin haltija ei syötä mitään paikkaa, missä päivän työaika alkaa tai päättyy kortin paikoilleen asettamiseen liittyvän tietojen käsin syötön aikana, tämän katsotaan merkitsevän, ettei hänen työaikansa ole muuttunut kortin viimeisimmän poiston jälkeen. Seuraavan paikan, jossa päivän työaika päättyy, syöttö korvaa kortin viimeisimmän poiston yhteydessä syötetyt tilapäiset tiedot.

Jos paikka syötetään, se on tallennettava asiaankuuluvalle ajopiirturikortille.

Tietojen syöttö käsin on keskeytettävä, jos:

— kortti poistetaan tai

— ajoneuvo liikkuu ja kortti on kuljettajan korttiaukossa.

Muitakin keskeytyksiä sallitaan, esim. aikakatkaisu, kun käyttäjä ei ole tehnyt mitään tietyn ajan kuluessa. Jos tietojen syöttö käsin keskeytetään, valvontalaitteen on vahvistettava kaikki siihen mennessä syötetyt täydelliset paikka- ja toimintatiedot (joko paikka ja aika tai toiminnan tyyppi, aloitusaika ja päättymisaika ovat yksiselitteiset).

Jos toinen kuljettaja- tai korjaamokortti asetetaan paikoilleen, kun aikaisemmin asetetun kortin toimintatietojen syöttäminen käsin on meneillään, tämän aikaisemman kortin tietojen syöttäminen käsin loppuun asti on sallittava, ennen kuin toisen kortin tietojen käsin syöttäminen aloitetaan.

Kortin haltijalla on oltava mahdollisuus lisätä käsin syötettäviä tietoja seuraavan vähimmäisvaatimukset täyttävän menettelyn mukaisesti:

— Toimintatietojen syöttäminen käsin aikajärjestyksessä kortin viimeisestä poistosta tähän paikoilleen asettamiseen

— Ensimmäisen toiminnan alkamisajaksi on asetettava kortin poistohetki. Kuidenkin seuraavien syötettyjen tietojen aloitusajaksi on asetettava edellisten tietojen päättymisaikaa välittömästi seuraava aika. Kullekin toiminnalle on valittava toiminnan tyyppi ja päättymisaika.

▼B

Toimenpiteen on päätyttävä, kun käsin syötetyn toimintatiedon päättymisaika on sama kuin aika, jolloin kortti asetettiin paikoilleen. Seuraavaksi valvontalaite voi haluttaessa sallia sen, että kortin haltija muokkaa käsin syötettyjä toimintatietoja, kunnes kortin haltija vahvistaa ne valitsemalla tietyn komennon. Tämän jälkeen kaikki tällainen muokkaaminen on estettävä.

3.6.3 *Erityisolosuhteisiin liittyvien tietojen syöttö*

62) Valvontalaitteen on sallittava se, että kuljettaja syöttää tosiaikaisesti seuraavia erityisolosuhteita koskevat tiedot:

— OUT OF SCOPE (pois julkisilta teiltä) (alkaminen, päättyminen)

— FERRY/TRAIN CROSSING (lautta-/junakuljetus) (alkaminen, päättyminen).

FERRY/TRAIN CROSSING -olosuhteita ei voi esiintyä, jos OUT OF SCOPE -olosuhteet ovat voimassa.

Valvontalaitteen on automaattisesti lopetettava OUT OF SCOPE -olosuhteiden voimassaolo, jos kuljettajakortti asetetaan paikoilleen tai poistetaan.

OUT OF SCOPE -olosuhteiden voimassaolon on estettävä seuraavat tapahtumat ja varoitukset:

— ajo ilman asianmukaista korttia,

— Keskeytymättömään ajoaikaan liittyvät varoitukset.

FERRY/TRAIN CROSSING -alkutunnus asetetaan ennen kuin moottori sammutetaan lautassa/junassa.

Avattu FERRY/TRAIN CROSSING -olosuhde on päätettävä jonkin seuraavan vaihtoehdon esiintyessä:

— kuljettaja päättää manuaalisesti FERRY/TRAIN CROSSING -olosuhteen,

— kuljettaja poistaa korttinsa yksiköstä,

avattu FERRY/TRAIN CROSSING -olosuhde päättyy, kun se ei ole enää voimassa asetuksessa (EY) N:o 561/2006 esitettyjen määräysten perusteella.

3.7 **Yritysten tekemien lukitusten hallinta**

63) Tämän toiminnon avulla on voitava hallita yrityksen tekemiä lukituksia, jotta vain sillä olisi mahdollisuus käyttää tietoja yritystilassa.

64) Yrityksen tekemät lukitukset sisältävät alkamispäivän ja -ajan (lukitseminen) ja päättymispäivän ja -ajan (lukituksen avaaminen), johon liittyy yrityksen tunnistus yrityskortin numeron perusteella (lukittaessa).

65) Lukituksia voi kytkeä ”päälle” tai ”pois” vain toisaikaisesti.

66) Lukituksen pois kytkemisen on oltava mahdollista vain yritykselle, jonka lukitus on ”päällä” (mikä tunnistetaan yrityskortin 13 ensimmäisen numeron perusteella), tai

67) lukituksen pois kytkemisen on tapahduttava automaattisesti, jos jokin toinen yritys tekee lukituksen.

▼B

68) Tapauksessa, jossa yritys tekee lukituksen ja aikaisempi lukitus on saman yrityksen, oletetaan, että aikaisempaa lukitusta ei ole kytketty ”pois”, vaan se on yhä ”päällä”.

3.8 **Tarkastustoimien seuranta**

69) Tämän toiminnon on valvottava DISPLAYING (näyttö)-, PRINTING (tulostus)-, VU (ajoneuvoyksikkö)- sekä DOWNLOADING (kortin tietojen kopiointi)- ja ROADSIDE CALIBRATION (kalibrointi tien varrella) -tarkastustoimenpiteitä laitteen ollessa tarkastustilassa.

70) Tämän toiminnon on myös valvottava OVER SPEEDING CONTROL (ylinopeuden valvonta) -toimenpiteitä laitteen ollessa tarkastustilassa. Ylinopeuden valvonta katsotaan tapahtuneeksi, kun ylinopeudesta kertova tuloste on lähetetty tulostimelle tai näytölle laitteen ollessa tarkastustilassa tai kun tapahtumiin ja vikoihin liittyvät tiedot on kopioitu ajoneuvoyksikön datamuistista.

3.9 **Tapahtumien ja/tai vikojen havaitseminen**

71) Tämän toiminnon on havaittava seuraavat tapahtumat ja/tai viat:

3.9.1 *”Ei voimassa olevan kortin asettaminen laitteeseen”*

72) Tämä tapahtuma syntyy, kun paikoilleen asetetaan jokin kortti, joka ei ole voimassa, kun paikoilleen asetetaan kuljettajakortti, joka on jo korvattu, ja/tai kun paikoilleen asetetun kortin voimassaoloaika umpeutuu.

3.9.2 *”Korttiristiriita”-tapahtuma*

73) Tämä tapahtuma syntyy, kun jokin seuraavassa taulukossa kirjaimella X merkityistä kahden voimassa olevan kortin yhdistelmistä on asetettu paikoilleen:

Korttiristiriita		Kuljettajan korttiaukko				
		Ei korttia	Kuljettajakortti	Valvontakortti	Korjaamokortti	Yrityskortti
Apukuljettajan korttiaukko	Ei korttia					
	Kuljettajakortti				X	
	Valvontakortti			X	X	X
	Korjaamokortti		X	X	X	X
	Yrityskortti			X	X	X

3.9.3 *”Aikojen päällekkäisyys” -tapahtuma*

74) Tämä tapahtuma syntyy, kun kortilta luettu viimeisin kuljettajakortin pois ottamisen päivämäärä/aika on myöhempi kuin se valvontalaitteen päivämäärä/aika, jolloin kortti asetetaan paikoilleen.

3.9.4 *”Ajo ilman asianmukaista korttia” -tapahtuma*

75) Tämä tapahtuma syntyy, kun jokin seuraavassa taulukossa kirjaimella X merkityistä voimassa olevista ajopiirturikorttiyhdistelmistä on asetettu paikoilleen ja kuljettajan toiminta muuttuu DRIVING-toiminnaksi tai laitteen toimintatila muuttuu kuljettajan toiminnan ollessa tyyppiä DRIVING:

▼B

Ajo ilman asianmukaista korttia		Kuljettajan korttiaukko				
		Ei korttia (tai kortti ei voimassa)	Kuljettajakortti	Valvontakortti	Korjaamokortti	Yrityskortti
Apukuljettajan korttiaukko	Ei korttia (tai kortti ei voimassa)	X		X		X
	Kuljettajakortti	X		X	X	X
	Valvontakortti	X	X	X	X	X
	Korjaamokortti	X	X	X		X
	Yrityskortti	X	X	X	X	X

3.9.5 *”Kortin paikoilleen asettaminen ajettaessa” -tapahtuma*

76) Tämä tapahtuma syntyy, kun ajopiirturikortti asetetaan johonkin korttiaukkoon kuljettajan toiminnan ollessa DRIVING.

3.9.6 *”Edellistä kortin käyttöjaksoa ei lopetettu oikein” -tapahtuma*

77) Tämä tapahtuma syntyy, kun valvontalaite havaitsee korttia paikoilleen asetettaessa, että 3.1 kohdan määräyksistä huolimatta kortin edellistä käyttöjaksoa ei ole lopetettu oikein (kortti on otettu pois ennen kuin kaikki asianmukaiset tiedot on tallennettu sille). Tämä tapahtuma koskee vain kuljettaja- ja korjaamokortteja.

3.9.7 *”Ylinopeus”-tapahtuma*

78) Tämä tapahtuma syntyy aina, kun ajetaan ylinopeutta.

3.9.8 *”Keskeytynyt virransyöttö” -tapahtuma*

79) Tämä tapahtuma syntyy, kun laite on muussa kuin kalibrointi- tai tarkastustilassa ja liiketunnistimen tai ajoneuvoyksikön virransyöttö keskeytyy yli 200 millisekunnin ajaksi. Laitteen valmistajan on määriteltävä keskeytymisen kynnysarvo. Jännitteen aleneminen ajoneuvoa käynnistettäessä ei saa aiheuttaa tätä tapahtumaa.

3.9.9 *”Virhe viestinnässä etäviestintälaitteiston kanssa” -tapahtuma*

80) Tämä tapahtuma esiintyy, **kun yksikkö ei ole kalibrointitilassa**, jos etäviestintälaitteisto ei ilmoita vastaanottaneensa ajoneuvoyksiköstä lähetettyjä etäviestintätietoja onnistuneesti yli kolmen yrityksen jälkeen.

3.9.10 *”Sijaintitietojen puuttuminen GNSS-vastaanottimesta” -tapahtuma*

81) Tämä tapahtuma esiintyy, **kun yksikkö ei ole kalibrointitilassa**, jos (sisäisestä tai ulkoisesta) GNSS-vastaanottimesta peräisin olevia sijaintitietoja ei saada yli kolmen tunnin kertyneellä yhteenlasketulla ajoajalla.

3.9.11 *”Virhe viestinnässä ulkoisen GNSS-laitteiston kanssa” -tapahtuma*

82) Tämä tapahtuma esiintyy, **kun yksikkö ei ole kalibrointitilassa**, jos ulkoisen GNSS-vastaanottimen ja ajoneuvoyksikön viestintä keskeytyy yli 20 peräkkäisen minuutin ajaksi, kun ajoneuvo liikkuu.

▼B

3.9.12 *”Virhe liikedatassa” -tapahtuma*

83) Tämä tapahtuma syntyy **laitteen ollessa muussa kuin kalibrointitilassa**, kun liiketunnistimen ja ajoneuvoyksikön välinen normaali datavirta keskeytyy ja/tai kun liiketunnistimen ja ajoneuvoyksikön välisen tiedonsiirron eheydessä tai autenttisuudessa ilmenee virhe.

3.9.13 *”Ajoneuvon liikeristiriita” -tapahtuma*

84) Tämä tapahtuma syntyy, **kun yksikkö ei ole kalibrointitilassa**, jos liiketunnistimesta lasketut liiketiedot ovat ristiriidassa sisäisestä GNSS-vastaanottimesta tai ulkoisesta GNSS-laitteesta taikka muista riippumattomista lähteistä laskettavien liiketietojen kanssa, kuten lisäyksessä 12 määritellään. Tämä tapahtuma ei saa syntyä lautta-/junakuljetuksen aikana, OUT OF SCOPE -olosuhteissa tai kun GNSS-vastaanottimen sijaintitietoja ei ole saatavilla.

3.9.14 *”Tietoturvan murtoyritys” -tapahtuma*

85) Tämä tapahtuma syntyy, kun ilmenee jokin muu tapahtuma, joka vaikuttaa liiketunnistimen ja/tai ajoneuvoyksikön ja/tai ulkoisen GNSS-laitteiston lisäyksessä 10 edellytettyyn tietoturvaan laitteen ollessa muussa kuin kalibrointitilassa.

3.9.15 *”Aikojen päällekkäisyys” -tapahtuma*

86) Tämä tapahtuma syntyy, **kun yksikkö ei ole kalibrointitilassa**, jos ajoneuvoyksikkö havaitsee yli minuutin kestoisen poikkeaman ajoneuvoyksikön ajanmittaustoiminnon ja GNSS-vastaanottimesta peräisin olevan ajan välillä. Tämä tapahtuma tallennetaan yhdessä ajoneuvoyksikön sisäisen kellon arvon kanssa ja yhdessä automaattisen ajansäädön kanssa. Kun aikojen päällekkäisyys -tapahtuma on syntynyt, ajoneuvoyksikkö ei tuota muita aikojen päällekkäisyys -tapahtumia seuraavaan 12 tuntiin. Tämä tapahtuma ei synny tapauksissa, joissa GNSS-vastaanotin ei havainnoinut mitään kelvollista GNSS-signaalia edellisen 30 päivän aikana. Kun GNSS-vastaanottimen sijaintitiedot ovat jälleen saatavilla, aika säädetään automaattisesti.

3.9.16 *”Kortti”-vikatapahtuma*

87) Tämä vikatapahtuma syntyy, kun ajopiirturikorttiin tulee vika käytön aikana.

3.9.17 *”Valvontalaite”-vikatapahtuma*

88) Tämä vikatapahtuma syntyy, kun jokin seuraavista vioista ilmenee laitteen ollessa muussa kuin kalibrointitilassa:

— vika ajoneuvoyksikön sisällä

— vika tulostimessa

— vika näytössä

— tietojen kopiointiin liittyvä vika

— vika tunnistimessa

— GNSS-vastaanottimeen tai ulkoiseen GNSS-laitteistoon liittyvä vika

— etäviestintälaitteistoon liittyvä vika.

▼B

3.10 **Sisäänrakennetut ja laitteen itse suorittamat testit**

89) Valvontalaitteen on itse havaittava viat itse suorittamiensa ja sisäänrakennettujen testien avulla seuraavan taulukon mukaisesti:

Testattava osakokoonpano	Laitteen itse suorittama testi	Sisäänrakennettu testi
Ohjelmisto		Eheys
Datamuisti	Käyttö	Käyttö, datan eheys
Kortin liitäntälaite	Käyttö	Käyttö
Näppäimistö		Tarkastus käsin
Tulostin	(riippuu valmistajasta)	Koetuloste
Näyttö		Silmämääräinen tarkastus
Tietojen kopiointi (suoritetaan vain kopioinnin yhteydessä)	Virheetön toiminta	
Tunnistin	Virheetön toiminta	Virheetön toiminta
Etäviestintälaitteisto	Virheetön toiminta	Virheetön toiminta
GNSS-laitteisto	Virheetön toiminta	Virheetön toiminta

3.11 **Tietojen haku datamuistista**

90) Valvontalaitteen on kyettävä lukemaan kaikkea dataa, jota on tallennettu sen datamuistiin.

3.12 **Tietojen kirjaaminen ja tallentaminen datamuistiin**

Tässä kohdassa:

— 365 vuorokaudella tarkoitetaan 365:tä keskimääräistä kuljettajan toimintaa sisältävää kalenterivuorokautta. Keskimääräisen päivittäisen toiminnan ajoneuvossa määritellään sisältävän vähintään kuusi kuljettajaa tai apukuljettajaa, kuusi kortin paikoilleen asettamis- ja poistotapahtumaa sekä 256 muutosta toiminnan tilassa. Näin ollen ”365 vuorokautta” sisältää vähintään 2 190 (apu)kuljettajaa, 2 190 kortin paikoilleen asettamis- ja poistotapahtumaa sekä 93 440 muutosta toiminnan tilassa,

— keskimääräinen sijaintitietojen määrä päivässä määritellään vähintään 6 sijaintiin, kun päivän työaika alkaa, 6 sijaintiin, kun kuljettajan keskeytymätön ajoaika saavuttaa yli kolmen tunnin jakson ja 6 sijaintiin, kun päivittäinen työaika päättyy, joten ”365 päivää” sisältää ainakin 6 570 sijaintitietoa,

— ajat kirjataan yhden minuutin tarkkuudella, ellei toisin määritellä,

— matkamittarin lukemat kirjataan yhden kilometrin tarkkuudella,

— nopeudet kirjataan tarkkuudella 1 km/t,

— sijainnit (leveys- ja pituusasteet) tallennetaan asteina ja minuutteina tarkkuudella 1/10 minuuttia, samoin kuin siihen liittyvä GNSS-laitteiston tarkkuus ja koontiaika.

▼B

91) Ulkoisen virransyötön katkeaminen lyhyemmäksi kuin 12 kuukauden ajaksi ei saa vaikuttaa datamuistiin tallennettuun dataan tyyppihyväksyntää vastaavissa olosuhteissa. Lisäksi ulkoiseen etäviestintälaitteeseen tallennettuihin tietoihin, kuten lisäyksessä 14 määritetään, ei vaikuta alle 28 päivän kestänyt virtalähteen katkeaminen.

92) Valvontalaitteen on kyettävä epäsuorasti tai suoraan kirjaamaan ja tallentamaan datamuistiinsa seuraavat tiedot:

3.12.1 *Laitteen tunnistetiedot*

3.12.1.1 Ajoneuvoyksikön tunnistetiedot

93) Valvontalaitteen on kyettävä tallentamaan datamuistiinsa seuraavat ajoneuvoyksikön tunnistetiedot:

— valmistajan nimi,

— valmistajan osoite,

— osanumero,

— sarjanumero,

— ajoneuvoyksikön sukupolvi

— kyky käyttää ensimmäisen sukupolven ajopiirturikortteja,

— ohjelmistoversion numero,

— ohjelmaversion asennuspäivämäärä,

— laitteen valmistusvuosi,

— hyväksyntänumero.

94) Ajoneuvoyksikön valmistaja kirjaa ja tallentaa yksikön tunnistetiedot yhdellä kertaa, lukuun ottamatta ohjelmistoon liittyviä tietoja ja hyväksyntänumeroa, joita voidaan muuttaa ohjelmistoa päivitettäessä, ja kyvyn käyttää ensimmäisen sukupolven ajopiirturikortteja.

3.12.1.2 Liiketunnistimen tunnistetiedot

95) Liiketunnistimen on kyettävä tallentamaan muistiinsa seuraavat tunnistetiedot:

— valmistajan nimi,

— sarjanumero,

— hyväksyntänumero,

— tunnistimeen sulautetun tietoturvakomponentin tunniste (esim. sirun/prosessorin osanumero),

— käyttöjärjestelmän tunniste (esim. ohjelmistoversion numero).

96) Liiketunnistimen valmistaja kirjaa ja tallentaa liiketunnistimen tunnistetiedot liiketunnistimeen yhdellä kertaa.

97) Ajoneuvoyksikön on kyettävä kirjaamaan ja tallentamaan datamuistiinsa liiketunnistimien 20 viimeisimpään liitäntään liittyvät seuraavat tiedot (jos yhtenä kalenterivuorokautena on useita liitäntöjä, ainoastaan kyseisen vuorokauden ensimmäinen ja viimeinen tallennetaan):

▼B

Kaikista näistä liitännöistä on tallennettava seuraavat tiedot:

— liiketunnistimen tunnistetiedot:

— sarjanumero

— hyväksyntänumero,

— liiketunnistimen liittämistiedot:

— päivämäärä, jolloin tunnistin ensi kerran liitettiin ajoneuvoyksikköön.

3.12.1.3 Maailmanlaajuisen satelliittinavigointijärjestelmän tunnistetiedot

98) Ulkoisen GNSS-laitteiston on kyettävä tallentamaan muistiinsa seuraavat tunnistetiedot:

— valmistajan nimi,

— sarjanumero

— hyväksyntänumero,

— tunnistimeen sulautetun tietoturvakomponentin tunniste (esim. sirun/prosessorin osanumero),

— käyttöjärjestelmän tunniste (esim. ohjelmistoversion numero).

99) Ulkoisen GNSS-laitteiston valmistaja kirjaa ja tallentaa tunnistetiedot ulkoiseen GNSS-laitteistoon yhdellä kertaa.

100) Ajoneuvoyksikön on kyettävä kirjaamaan ja tallentamaan datamuistiinsa ulkoisten GNSS-laitteistojen 20 viimeisimpään kytkentään liittyvät seuraavat tiedot (jos yhtenä kalenterivuorokautena on useita kytkentöjä, ainoastaan kyseisen vuorokauden ensimmäinen ja viimeinen tallennetaan):

Kaikista näistä kytkennöistä on tallennettava seuraavat tiedot:

— ulkoisen GNSS-laitteiston tunnistetiedot:

— sarjanumero,

— hyväksyntänumero,

— ulkoisen GNSS-laitteiston kytkentätiedot:

— kytkennän päivämäärä.

3.12.2 *Avaimet ja varmenteet*

101) Valvontalaitteen on kyettävä tallentamaan useita salausavaimia ja varmenteita, kuten lisäyksen 11 A ja B osassa määritetään.

3.12.3 *Kuljettaja- tai korjaamokortin paikoilleen asettamiseen ja poistamiseen liittyvät tiedot*

102) Aina kun kuljettaja- tai korjaamokortti asetetaan paikoilleen laitteeseen tai poistetaan siitä, valvontalaitteen on tallennettava ja säilytettävä datamuistissaan:

— kortin haltijan sukunimi ja etunimi (-nimet) siinä muodossa kuin ne on tallennettu kortille,

— kortin numero, kortin myöntänyt jäsenvaltio sekä viimeinen voimassaolopäivä siinä muodossa kuin ne on tallennettu kortille,

— kortin sukupolvi,

▼B

— päivämäärä ja aika, jolloin kortti asetettiin paikoilleen,

— ajoneuvon matkamittarin lukema hetkellä, jolloin kortti asetettiin paikoilleen,

— korttiaukko, johon kortti on asetettu,

— päivämäärä ja aika, jolloin kortti poistettiin,

— ajoneuvon matkamittarin lukema hetkellä, jolloin kortti poistettiin,

— seuraavat tiedot ajoneuvosta, jota kuljettaja käytti ennen tätä, siinä muodossa kuin ne on tallennettu kortille:

  — rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity,

  — ajoneuvoyksikön sukupolvi (jos saatavilla),

  — päivämäärä ja aika, jolloin kortti poistettiin,

— tunnus, josta ilmenee, onko kuljettaja korttia paikoilleen asettaessaan syöttänyt toimintatietoja käsin.

103) Datamuistin on kyettävä tallentamaan näitä tietoja vähintään 365 vuorokauden ajalta.

104) Kun tiedontallennuskapasiteetti loppuu, uusimpien tietojen on korvattava vanhimmat tiedot.

3.12.4 *Kuljettajan toimintaan liittyvät tiedot*

105) Aina kun kuljettajan ja/tai apukuljettajan toiminnan tyyppi muuttuu ja/tai ajoneuvon miehitys muuttuu ja/tai kuljettaja- tai korjaamokortti asetetaan paikoilleen tai poistetaan, valvontalaitteen on tallennettava ja säilytettävä datamuistissaan:

— ajoneuvon miehitys (CREW, SINGLE),

— korttiaukko (DRIVER, CO-DRIVER),

— kunkin korttiaukon tila (INSERTED, NOT INSERTED),

— toiminta (DRIVING, AVAILABILITY, WORK, BREAK/REST),

— päivämäärä ja aika, jolloin muutos tapahtui.

INSERTED tarkoittaa, että korttiaukkoon on asetettu voimassa oleva kuljettaja- tai korjaamokortti. NOT INSERTED tarkoittaa, että tilanne on päinvastainen, toisin sanoen korttiaukkoon ei ole asetettu voimassa olevaa kuljettaja- tai korjaamokorttia (esim. korttiaukkoon on asetettu yrityskortti tai siinä ei ole lainkaan korttia).

Kuljettajan käsin syöttämät toimintatiedot eivät tallennu datamuistiin.

106) Datamuistin on kyettävä tallentamaan kuljettajan toimintaan liittyviä tietoja vähintään 365 vuorokauden ajalta.

107) Kun tiedontallennuskapasiteetti loppuu, uusimpien tietojen on korvattava vanhimmat tiedot.

▼B

3.12.5 *Paikat ja sijainnit, joissa päivän työaika alkaa, loppuu, ja/tai jossa 3 tunnin jatkuva ajoaika saavutetaan*

108) Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan:

— paikat ja sijainnit, joissa kuljettajan ja/tai apukuljettajan päivän työaika alkaa;

— sijainnit, joissa kuljettajan keskeytymätön ajoaika on yli kolmen tunnin jakso;

— paikat ja sijainnit, joissa kuljettajan ja/tai apukuljettajan päivän työaika päättyy.

109) Kun ajoneuvon sijaintitieto ei ole saatavilla GNSS-vastaanottimesta näinä aikoina, valvontalaitteen on käytettävä viimeisintä saatavilla olevaa sijaintitietoa ja siihen liittyvää päivämäärää ja kellonaikaa.

110) Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan kunkin paikka- ja sijaintitiedon lisäksi:

— (apu)kuljettajan kortin numero ja kortin myöntänyt jäsenvaltio,

— kortin sukupolvi,

— päivämäärä, jolloin tieto syötettiin,

— syötetyn tiedon tyyppi (alkamis- tai päättymistieto tai kolmen tunnin keskeytymätön ajoaika),

— asiaankuuluva GNSS-laitteiston tarkkuus, päättymispäivä ja -aika (tarvittaessa),

— ajoneuvon matkamittarin lukema.

111) Datamuistin on voitava säilyttää 365 päivän ajan paikka- ja sijaintitiedot päivän työajan alkamisesta, päättymisestä ja/tai kun saavutetaan 3 tunnin keskeytymätön ajoaika.

112) Kun tiedontallennuskapasiteetti loppuu, uusimpien tietojen on korvattava vanhimmat tiedot.

3.12.6 *Matkamittariin liittyvät tiedot*

113) Valvontalaitteen on tallennettava datamuistiinsa ajoneuvon matkamittarin lukema ja sitä vastaava päivämäärä keskiyöllä jokaisena kalenterivuorokautena.

114) Datamuistin on kyettävä tallentamaan keskiyöllä otettuja matkamittarin lukemia vähintään 365 vuorokauden ajalta.

115) Kun tiedontallennuskapasiteetti loppuu, uusimpien tietojen on korvattava vanhimmat tiedot.

3.12.7 *Nopeuteen liittyvät yksityiskohtaiset tiedot*

116) Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan ajoneuvon hetkellinen nopeus ja sitä vastaava päivämäärä ja aika kerran sekunnissa vähintään viimeisen 24 sellaisen tunnin ajalta, jolloin ajoneuvoa on ajettu.

3.12.8 *Tapahtumiin liittyvät tiedot*

Tässä alakohdassa käsiteltäviin asioihin liittyvä aika on kirjattava yhden sekunnin tarkkuudella.

117) Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan seuraavat tiedot kustakin havaitusta tapahtumasta seuraavien tallennussääntöjen mukaisesti:

▼B

Tapahtuma	Tallennussäännöt	Kustakin tapahtumasta kirjattavat tiedot
Ei-voimassa olevan kortin asettaminen laitteeseen	— 10 viimeisintä tapahtumaa,	— päivämäärä ja aika, jolloin tapahtuma esiintyi, — kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja tapahtuman luoneen kortin sukupolvi, — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Korttiristiriita	— 10 viimeisintä tapahtumaa,	— tapahtuman alkamispäivämäärä ja -aika, — tapahtuman päättymispäivämäärä ja -aika, — kunkin kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja ristiriidan aiheuttaneiden kunkin kortin sukupolvi
Ajo ilman asianmukaista korttia	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui, — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika, — tapahtuman päättymispäivämäärä ja -aika, — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi, — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Kortin paikoilleen asettaminen ajon aikana	— viimeinen tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui	— päivämäärä ja aika, jolloin tapahtuma sattui, — kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi, — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Edellistä kortin käyttöjaksoa ei lopetettu oikein	— 10 viimeisintä tapahtumaa	— päivämäärä ja aika, jolloin kortti asetettiin paikoilleen, — kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi, — viimeisimmän käyttöjakson tiedot sellaisina kuin ne ovat luettavissa kortilta: — päivämäärä ja aika, jolloin kortti asetettiin paikoilleen, — rekisteritunnus, jäsenvaltio, jossa ajoneuvo on rekisteröity ja ajoneuvoyksikön sukupolvi
Ylinopeus (1)	— vakavin ylinopeustapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui (eli tapahtuma, johon liittyy korkein keskinopeus), — viisi vakavinta tapahtumaa viimeisten 365 vuorokauden ajalta, — ensimmäinen tapahtuma, joka sattui viimeksi suoritetun kalibroinnin jälkeen	— tapahtuman alkamispäivämäärä ja -aika, — tapahtuman päättymispäivämäärä ja -aika, — suurin tapahtuman kestäessä mitattu nopeus, — tapahtuman kestäessä mitattujen nopeuslukemien aritmeettinen keskiarvo, — kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja kuljettajakortin sukupolvi (tarvittaessa), — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä

▼B

Tapahtuma	Tallennussäännöt	Kustakin tapahtumasta kirjattavat tiedot
Keskeytynyt virransyöttö (2)	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui, — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika, — tapahtuman päättymispäivämäärä ja -aika, — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi, — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Virhe yhteydessä etäviestintälaitteistoon	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui, — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika, — tapahtuman päättymispäivämäärä ja -aika, — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi, — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Sijaintitietojen puuttuminen GNSS-vastaanottimesta	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui, — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika, — tapahtuman päättymispäivämäärä ja -aika, — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi, — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Virhe liikedatassa	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui, — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika, — tapahtuman päättymispäivämäärä ja -aika, — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi, — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Ajoneuvon liikeristiriita	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui, — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika, — tapahtuman päättymispäivämäärä ja -aika, — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi, — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Tietoturvan murtoyritys	— 10 viimeisintä kutakin tyyppiä edustavaa tapahtumaa	— tapahtuman alkamispäivämäärä ja -aika, — tapahtuman päättymispäivämäärä ja -aika (jos tieto on oleellinen), — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi, — tapahtuman tyyppi

▼B

Tapahtuma	Tallennussäännöt	Kustakin tapahtumasta kirjattavat tiedot
Aikojen päällekkäisyys	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui, — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— valvontalaitteen päivämäärä ja aika — GNSS-laitteiston päivämäärä ja aika, — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi, — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä.

(1) Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan:

— viimeisimmän OVER SPEEDING CONTROL -toimenpiteen päivämäärä ja aika,

— päivämäärä ja aika, jolloin ensimmäinen ylinopeustapahtuma sattui tämän OVER SPEEDING CONTROL -toimenpiteen jälkeen.

— viimeisen ylinopeustarkastuksen jälkeen sattuneiden OVER SPEEDING CONTROL -toimenpiteiden määrä.

(2) Nämä tiedot voidaan tallentaa ainoastaan, kun virtalähde liitetään uudelleen, ja ajat voidaan tietää minuutin tarkkuudella.

3.12.9 *Vikoihin liittyvät tiedot*

Tässä alakohdassa käsiteltäviin asioihin liittyvä aika on kirjattava yhden sekunnin tarkkuudella.

118) Valvontalaitteen on yritettävä tallentaa ja säilyttää datamuistissaan seuraavat, kutakin havaittua vikaa koskevat tiedot seuraavien tallennussääntöjen mukaisesti:

Vikatapahtumat	Tallennussäännöt	Kustakin viasta kirjattavat tiedot
Korttivika	— 10 viimeisintä kuljettajakortin vikatapahtumaa	— päivämäärä ja aika, jolloin vikatapahtuma alkoi, — päivämäärä ja aika, jolloin vikatapahtuma päättyi, — kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi,
Valvontalaiteviat	— 10 viimeisintä kutakin tyyppiä edustavaa vikatapahtumaa, — ensimmäinen vikatapahtuma, joka sattui viimeksi suoritetun kalibroinnin jälkeen	— päivämäärä ja aika, jolloin vikatapahtuma alkoi, — päivämäärä ja aika, jolloin vikatapahtuma päättyi, — vian tyyppi, — vikatapahtuman alkaessa ja/tai päättyessä paikoilleen asetettujen korttien tyyppi, numero ja ne myöntänyt jäsenvaltio sekä niiden sukupolvi.

3.12.10 *Kalibrointiin liittyvät tiedot*

119) Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan tiedot, jotka liittyvät:

— aktivointihetkellä tunnettuihin kalibrointiparametreihin,

▼B

— laitteen ensimmäiseen kalibrointiin sen aktivoinnin jälkeen,

— sen ensimmäiseen kalibrointiin nykyisessä ajoneuvossa (joka tunnistetaan rekisteritunnuksensa perusteella),

— sen 20 viimeiseen kalibrointiin (jos saman kalenterivuorokauden aikana suoritetaan useita kalibrointeja, ainoastaan ensimmäinen ja viimeinen niistä tallennetaan).

120) Kaikista näistä kalibroinneista on tallennettava seuraavat tiedot:

— kalibroinnin tarkoitus (aktivointi, ensiasennus, asennus, määräaikaistarkastus),

— korjaamon nimi ja osoite,

— korjaamokortin numero, kortin myöntänyt jäsenvaltio ja kortin viimeinen voimassaolopäivä,

— ajoneuvon tunnistetiedot,

— päivitetyt tai vahvistetut parametrit: w, k, l, rengaskoko, nopeudenrajoittimen asetukset, matkamittari (vanhat ja uudet lukemat), päivämäärä ja aika (vanhat ja uudet lukemat),

— kaikkien käytössä olevien sinetöintien tyypit ja tunnisteet.

121) Lisäksi valvontalaitteen on tallennettava ja säilytettävä datamuistissaan tieto siitä, pystyykö se käyttämään ensimmäisen sukupolven ajopiirturikortteja (edelleen käytössä olevia tai ei).

122) Liiketunnistimen on tallennettava ja säilytettävä muistissaan seuraavat liiketunnistimen asennustiedot:

— sen ensimmäinen liittäminen ajoneuvoyksikköön (päivämäärä, aika, ajoneuvoyksikön hyväksyntänumero, ajoneuvoyksikön sarjanumero),

— sen viimeisin liittäminen ajoneuvoyksikköön (päivämäärä, aika, ajoneuvoyksikön hyväksyntänumero, ajoneuvoyksikön sarjanumero).

123) Ulkoisen GNSS-laitteiston on tallennettava ja säilytettävä muistissaan seuraavat ulkoisen GNSS-laitteiston asennustiedot:

— sen ensimmäinen kytkeminen ajoneuvoyksikköön (päivämäärä, aika, ajoneuvoyksikön hyväksyntänumero, ajoneuvoyksikön sarjanumero),

— sen viimeinen kytkeminen ajoneuvoyksikköön (päivämäärä, aika, ajoneuvoyksikön hyväksyntänumero, ajoneuvoyksikön sarjanumero).

3.12.11 *Ajan asetukseen liittyvät tiedot*

124) Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan tiedot, jotka liittyvät ajan asettamistapahtumaan muulloin kuin tavanomaisen kalibroinnin yhteydessä (määritelmä f):

— viimeisimpään ajan asetukseen,

— viiteen suurimpaan ajan asetukseen.

125) Kaikista näistä ajan asetuksista on tallennettava seuraavat tiedot:

— päivämäärä ja aika, vanhat lukemat,

— päivämäärä ja aika, uudet lukemat,

— ajan asetuksen suorittaneen korjaamon nimi ja osoite,

— korjaamokortin numero, kortin myöntänyt jäsenvaltio sekä kortin sukupolvi ja sen viimeinen voimassaolopäivä.

▼B

3.12.12 *Tarkastustoimiin liittyvät tiedot*

126) Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan seuraavat tiedot, jotka liittyvät 20 viimeisimpään tarkastustoimeen:

— tarkastuksen päivämäärä ja aika,

— valvontakortin numero, kortin myöntänyt jäsenvaltio ja kortin sukupolvi,

— tarkastuksen tyyppi (tietojen näyttö ja/tai tulostus ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi ja/tai kalibroinnin tarkastus tien varrella).

127) Kun tietoja kopioidaan, myös tiedot ensimmäisestä ja viimeisestä päivästä, joita kopiointi koskee, on kirjattava.

3.12.13 *Yritysten tekemiin lukituksiin liittyvät tiedot*

128) Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan seuraavat tiedot, jotka liittyvät 255 viimeisimpään yrityksen tekemään lukitukseen:

— päivämäärä ja aika, jolloin lukitus tehtiin,

— päivämäärä ja aika, jolloin lukitus avattiin,

— yrityskortin numero, kortin myöntänyt jäsenvaltio ja kortin sukupolvi,

— yrityksen nimi ja osoite.

Lukituksella aikaisemmin lukittuja tietoja, jotka on poistettu muistista edellä mainitun rajan vuoksi, käsitellään tietoina, jotka eivät ole lukittuja.

3.12.14 *Tietojen kopiointitapahtumiin liittyvät tiedot*

129) Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan seuraavat tiedot, jotka liittyvät datamuistin viimeisimpään kopiointiin ulkoiselle tietovälineelle laitteen ollessa yritys- tai kalibrointitilassa:

— päivämäärä ja aika, jolloin kopiointi suoritettiin,

— yritys- tai korjaamokortin numero, kortin myöntänyt jäsenvaltio ja kortin sukupolvi,

— yrityksen tai korjaamon nimi.

3.12.15 *Erityisolosuhteisiin liittyvät tiedot*

130) Valvontalaitteen on tallennettava datamuistiinsa seuraavat tiedot, jotka liittyvät erityisolosuhteisiin:

— päivämäärä ja aika, jolloin tieto syötettiin,

— erityisolosuhteiden tyyppi.

131) Datamuistin on kyettävä tallentamaan erityisolosuhteisiin liittyviä tietoja vähintään 365 vuorokauden ajalta (olettaen, että päivittäin alkaa ja päättyy keskimäärin yksi erityisolosuhdetilanne). Kun tiedontallennuskapasiteetti loppuu, uusimpien tietojen on korvattava vanhimmat tiedot.

3.12.16 *Ajopiirturikortin tiedot*

132) Valvontalaitteen on kyettävä tallentamaan seuraavat tiedot, jotka liittyvät ajoneuvoyksikössä käytettyihin eri ajopiirturikortteihin:

— ajopiirturikortin numero ja sen sarjanumero,

— ajopiirturikortin valmistaja,

▼B

— ajopiirturikortin tyyppi,

— ajopiirturikortin versio.

133) Valvontalaitteen on kyettävä tallentamaan vähintään 88 tällaista tietuetta.

3.13 **Tietojen haku ajopiirturikorteilta**

134) Valvontalaitteen on kyettävä tarvittaessa lukemaan ensimmäisen ja toisen sukupolven ajopiirturikorteilta tiedot, jotta voidaan:

— tunnistaa kortin tyyppi, kortin haltija, aiemmin käytetty ajoneuvo, päivämäärä ja aika, jolloin kortti viimeksi poistettiin, sekä tuolloin valittu toiminnan tyyppi,

— tarkastaa, että viimeisin kortin käyttöjakso lopetettiin oikein,

— laskea kuljettajan keskeytymätön ajoaika, yhteenlaskettu taukoaika sekä edellisen ja kuluvan viikon yhteenlasketut ajoajat,

— tulostaa tarvittavia tulosteita, jotka liittyvät kuljettajakortille tallennettuihin tietoihin,

— kopioida kuljettajakortin tietoja ulkoiselle tietovälineelle.

Tätä vaatimusta sovelletaan ainoastaan ensimmäisen sukupolven ajopiirturikortteihin, jos korjaamo ei ole poistanut niitä käytöstä.

135) Jos tietojen lukemisessa tapahtuu virhe, valvontalaitteen on yritettävä enintään kolme kertaa uudelleen käyttää samaa lukukomentoa, ja mikäli tietojen lukeminen ei vieläkään onnistu, laitteen on katsottava, että kortti on viallinen eikä se ole voimassa.

3.14 **Tietojen kirjaaminen ja tallentaminen ajopiirturikorteille**

3.14.1 *Tietojen kirjaaminen ja tallentaminen ensimmäisen sukupolven ajopiirturikorteille*

136) Jos korjaamo ei ole poistanut ensimmäisen sukupolven ajopiirturikortteja käytöstä, valvontalaitteen on tallennettava ja säilytettävä tiedot täsmälleen samalla tavalla kuin ensimmäisen sukupolven valvontalaite tekisi.

137) Valvontalaitteen on kirjattava kortin tätä käyttöjaksoa koskevat tiedot kuljettaja- tai korjaamokortille heti, kun se on asetettu laitteeseen.

138) Valvontalaitteen on päivitettävä voimassa olevat kuljettaja-, korjaamo-, yritys- ja/tai valvontakortit kaikilla niillä tarvittavilla tiedoilla, jotka liittyvät aikaan, jolloin kortti on asetettuna laitteeseen, sekä tiedoilla, jotka liittyvät kortin haltijaan. Näille korteille tallennettavat tiedot on määritelty luvussa 4.

139) Valvontalaitteen on päivitettävä kuljettajan toimintaa ja olinpaikkaa koskevat tiedot (kuten 4.5.3.1.9 ja 4.5.3.1.11 kohdassa on määritelty), jotka on tallennettu voimassa oleville kuljettaja- ja/tai korjaamokorteille, kortin haltijan käsin syöttämillä toimintaa ja olinpaikkaa koskevilla tiedoilla.

140) Kaikkia tapahtumia, joita ei ole määritelty ensimmäisen sukupolven valvontalaitteille, ei säilytetä kuljettaja- ja korjaamokortissa.

▼B

141) Ajopiirturikorttien tietojen päivityksen on tapahduttava siten, että tarvittaessa ja tiedontallennuskapasiteetti huomioon ottaen uusimmat tiedot korvaavat vanhimmat tiedot.

142) Jos tietojen kirjoittamisessa kortille tapahtuu virhe, valvontalaitteen on yritettävä enintään kolme kertaa uudelleen käyttää samaa kirjoituskomentoa, ja mikäli tietojen kirjoittaminen ei vieläkään onnistu, laitteen on katsottava, että kortti on viallinen eikä se ole voimassa.

143) Ennen kuin valvontalaite sallii kuljettajakortin poistamisen ja sen jälkeen, kun kaikki oleelliset tiedot on tallennettu kortille, valvontalaitteen on saatettava nyt päättyvää kortin käyttöjaksoa koskevat tiedot ajan tasalle.

3.14.2 *Tietojen kirjaaminen ja tallentaminen toisen sukupolven ajopiirturikorteille*

144) Toisen sukupolven ajopiirturikortteihin on sisällyttävä kaksi eri korttisovellusta, joista ensimmäisen on oltava täsmälleen sama kuin ensimmäisen sukupolven ajopiirturikorttien TACHO-sovellus, ja toisen ”TACHO_G2”-sovellus, kuten 4 kohdassa ja lisäyksessä 2 määritellään.

145) Valvontalaitteen on kirjattava kortin tätä käyttöjaksoa koskevat tiedot kuljettaja- tai korjaamokortille heti, kun se on asetettu laitteeseen.

146) Valvontalaitteen on päivitettävä kahden kortin sovelluksiin tallennetut voimassa olevat kuljettaja-, korjaamo-, yritys- ja/tai valvontakortit kaikilla niillä tarvittavilla tiedoilla, jotka liittyvät aikaan, jolloin kortti on asetettuna laitteeseen, sekä tiedoilla, jotka liittyvät kortin haltijaan. Näille korteille tallennettavat tiedot on määritelty luvussa 4.

147) Valvontalaitteen on päivitettävä kuljettajan toimintaa ja olinpaikkaa koskevat tiedot (kuten 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 ja 4.5.3.2.11 kohdassa on määritelty), jotka on tallennettu voimassa oleville kuljettaja- ja/tai korjaamokorteille, kortin haltijan käsin syöttämillä toiminta- ja paikkatiedoilla.

148) Ajopiirturikorttien tietojen päivityksen on tapahduttava siten, että tarvittaessa ja tiedontallennuskapasiteetti huomioon ottaen uusimmat tiedot korvaavat vanhimmat tiedot.

149) Jos tietojen kirjoittamisessa kortille tapahtuu virhe, valvontalaitteen on yritettävä enintään kolme kertaa uudelleen käyttää samaa kirjoituskomentoa, ja mikäli tietojen kirjoittaminen ei vieläkään onnistu, laitteen on katsottava, että kortti on viallinen eikä se ole voimassa.

150) Ennen kuin valvontalaite sallii kuljettajakortin poistamisen ja sen jälkeen, kun kaikki oleelliset tiedot on tallennettu kortin toisen sukupolven sovellukseen, valvontalaitteen on saatettava nyt päättyvää kortin käyttöjaksoa koskevat tiedot ajan tasalle.

3.15 **Tietojen näyttö**

151) Näytön on oltava vähintään 20 merkin laajuinen.

152) Merkkien on oltava vähintään 5 mm korkeita ja 3,5 mm leveitä.

153) Näytön on tuettava lisäyksen 1 luvussa 4 ”Merkistöt” määritettyjä merkkejä. Näytössä voidaan käyttää yksinkertaistettuja merkkikuvioita (esim. merkit, joissa on korkomerkkejä, voidaan näyttää ilman niitä, tai pienet kirjaimet voidaan näyttää isoina kirjaimina).

▼B

154) Näytössä on oltava asianmukainen ja häikäisemätön valaistus.

155) Näytön on oltava nähtävissä avaamatta valvontalaitetta.

156) Valvontalaitteen on kyettävä näyttämään:

— oletusarvoiset tiedot,

— varoituksiin liittyvät tiedot,

— valikkojen käyttöön liittyvät tiedot,

— muut käyttäjän pyytämät tiedot.

Valvontalaite saa näyttää muitakin tietoja, edellyttäen, että ne ovat selvästi erotettavissa edellä mainituista tiedoista.

157) Valvontalaitteen näytössä on käytettävä lisäyksessä 3 lueteltuja kuvakkeita tai niiden yhdistelmiä. Näytössä voidaan lisäksi käyttää muita kuvakkeita tai niiden yhdistelmiä, mikäli ne ovat selvästi erotettavissa edellä mainituista kuvakkeista tai niiden yhdistelmistä.

158) Näytön on aina oltava ON (päällä) -tilassa ajoneuvon ollessa liikkeessä.

159) Valvontalaitteessa saa olla käsikäyttöinen tai automaattinen mahdollisuus kytkeä näyttö OFF (pois) -tilaan silloin, kun ajoneuvo ei ole liikkeessä.

Näytön esitysmuoto on määritelty lisäyksessä 5.

3.15.1 *Oletusarvoinen näyttö*

160) Kun ei ole tarvetta näyttää muita tietoja, valvontalaitteen on oletusarvoisesti näytettävä seuraavat tiedot:

— paikallinen aika (UTC-ajan ja kuljettajan asettaman aikaeron perusteella),

— laitteen toimintatila,

— kuljettajan ja apukuljettajan sen hetkisen toiminnan tyyppi,

— kuljettajaan liittyvät tiedot:

— jos kuljettajan sen hetkinen toiminta on tyyppiä DRIVING, näytetään kuljettajan sen hetkinen keskeytymätön ajoaika ja sen hetkinen yhteenlaskettu taukoaika

— jos kuljettajan sen hetkinen toiminta ei ole tyyppiä DRIVING, näytetään kyseisen toiminnan sen hetkinen kesto (alkaen hetkestä, jolloin se valittiin) ja kuljettajan sen hetkinen yhteenlaskettu taukoaika.

161) Kuhunkin kuljettajaan liittyvien tietojen näytön on oltava selkeä, pelkistetty ja yksiselitteinen. Jos kuljettajaan ja apukuljettajaan liittyviä tietoja ei voida näyttää samanaikaisesti, valvontalaitteen on oletusarvoisesti näytettävä kuljettajaan liittyvät tiedot ja sallittava se, että käyttäjä itse tuo näyttöön apukuljettajaan liittyvät tiedot.

162) Jos laitteen toimintatilaa ei voida oletusarvoisesti näyttää näytön leveyden asettamien rajoitusten vuoksi, on valvontalaitteen näytettävä uusi toimintatila hetken ajan tilan vaihtuessa.

▼B

163) Valvontalaitteen on näytettävä kortin haltijan nimi hetken ajan korttia paikoilleen asetettaessa.

164) Kun OUT OF SCOPE tai FERRY/TRAIN -olosuhteet ovat voimassa, näytössä on oletusarvoisesti oltava asianomainen kuvake, joka osoittaa, että tietyt olosuhteet ovat voimassa (kuljettajan sen hetkisen toiminnan tyyppiä ei tarvitse näyttää samaan aikaan).

3.15.2 *Varoitusnäyttö*

165) Valvontalaitteen on näytettävä varoitukset ensisijaisesti käyttäen lisäyksen 3 kuvakkeita täydennettynä tarvittaessa numerokoodein välitettävillä lisätiedoilla. Varoituksen selväkielinen kuvaus kuljettajan valitsemalla kielellä voidaan myös lisätä toimintoon.

3.15.3 *Valikkojen käyttö*

166) Valvontalaitteessa on oltava asianmukaisen valikkorakenteen avulla käytettävät tarvittavat komennot.

3.15.4 *Muut näytöt*

167) Haluttaessa on voitava valita seuraavien tietojen näyttö:

— UTC-päivämäärä ja -aika sekä paikallisen ajan ero UTC-aikaan nähden,

— kuuden eri vakiotulosteen sisältö samassa muodossa kuin itse tulosteet,

— kuljettajan keskeytymätön ajoaika ja yhteenlaskettu taukoaika,

— apukuljettajan keskeytymätön ajoaika ja yhteenlaskettu taukoaika,

— kuljettajan edellisen ja kuluvan viikon yhteenlasketut ajoajat,

— apukuljettajan edellisen ja kuluvan viikon yhteenlasketut ajoajat.

vapaaehtoisesti:

— apukuljettajan toiminnan nykyinen kesto (alkaen hetkestä, jolloin se valittiin),

— kuljettajan kuluvan viikon yhteenlasketut ajoajat,

— apukuljettajan kuluvan päivän työajan yhteenlaskettu ajoaika.

— kuljettajan kuluvan päivän työajan yhteenlaskettu ajoaika.

168) Tulosteen sisällön näyttämisen on tapahduttava jaksoittaisesti, rivi kerrallaan. Jos näytön leveys on alle 24 merkkiä, käyttäjän on saatava tiedot täydellisinä käyttäen sopivaa keinoa (tiedon näyttäminen useammalla rivillä, rivien vierittäminen…).

Käsin tehtäviä merkintöjä varten varattuja tulosteiden rivejä ei tarvitse näyttää.

▼B

3.16 **Tulostus**

169) Valvontalaitteen on kyettävä tulostamaan datamuistissaan ja/tai ajopiirturikorteilla olevia tietoja seuraavan seitsemän tulosteen muodossa:

— kuljettajan toiminta kortin tietojen mukaan päivittäin tulostettuna,

— kuljettajan toiminta ajoneuvoyksikön tietojen mukaan päivittäin tulostettuna,

— tapahtumat ja viat kortin tietojen mukaan tulostettuna,

— tapahtumat ja viat ajoneuvoyksikön tietojen mukaan tulostettuna,

— teknisten tietojen tuloste,

— ylinopeustuloste,

— tietyn ajopiirturikortin tietojen käyttöhistoria (ks. 3.12.16 kohta).

Näiden tulosteiden ulkoasu ja sisältö on määritelty lisäyksessä 4.

Tulosteiden lopussa voidaan antaa lisätietoja.

Valvontalaite voi tuottaa myös muita tulosteita, jos ne ovat selvästi erotettavissa seitsemästä edellä mainitusta tulosteesta.

170) Tulosteiden ”kuljettajan toiminta kortin tietojen mukaan päivittäin tulostettuna” ja ”tapahtumat ja viat kortin tietojen mukaan tulostettuina” on oltava saatavissa vain, kun valvontalaitteeseen on asetettu kuljettaja- tai korjaamokortti. Valvontalaitteen on päivitettävä kyseiselle kortille tallennetut tiedot ennen tulostusta.

171) Tulosteiden ”kuljettajan toiminta kortin tietojen mukaan päivittäin tulostettuna” ja ”tapahtumat ja viat kortin tietojen mukaan tulostettuina” tulostamiseksi valvontalaitteen on:

— joko automaattisesti valittava kuljettajakortti tai korjaamokortti, jos vain toinen näistä on asetettu laitteeseen,

— tai annettava käyttäjän käyttöön komento, jolla tämä voi valita kortin, jolta tiedot luetaan, tai kortin, joka on asetettu kuljettajan korttiaukkoon, jos laitteeseen on asetettu kaksi korttia.

172) Tulostimen on kyettävä tulostamaan 24 merkkiä riville.

173) Merkkien on oltava vähintään 2,1 mm korkeita ja 1,5 mm leveitä.

174) Tulostimen on tuettava lisäyksen 1 luvussa 4 ”Merkistöt” määritettyjä merkkejä.

175) Tulostimien on oltava suunniteltu siten, että ne kykenevät tuottamaan edellä mainitut tulosteet riittävän selvinä, jottei niitä luettaessa synny väärinkäsityksiä.

176) Tulosteiden koon ja niiden sisältämien tietojen on säilyttävä muuttumattomina normaaleissa kosteus- (10–90 prosenttia) ja lämpötilaolosuhteissa.

177) Valvontalaitteessa käytettävä tyyppihyväksytty tulostinpaperi on varustettava asianmukaisin tyyppihyväksyntämerkinnöin sekä merkinnöin siitä, minkä tyyppisessä (tyyppisissä) valvontalaitteessa (-laitteissa) sitä saadaan käyttää.

▼B

178) Tulosteiden on säilyttävä selvästi luettavina ja tunnistettavina ainakin kahden vuoden ajan valaistuksen, kosteuden ja lämpötilan osalta normaaleissa olosuhteissa.

179) Tulosteiden on oltava ainakin lisäyksessä 9 määriteltyjen testauseritelmien mukaiset.

180) Näihin asiakirjoihin on myös voitava tehdä käsin kirjoitettuja merkintöjä kuten kuljettajan allekirjoitus.

181) Valvontalaitteen on hallittava tilanteet, joissa tulostuspaperi loppuu, siten, että uuden paperin lisäämisen jälkeen laite joko aloittaa tulostuksen alusta tai jatkaa tulostusta antamalla yksiselitteisen viitteen ennen paperin loppumista tulostettuun osaan.

3.17 **Varoitukset**

182) Valvontalaitteen on varoitettava kuljettajaa, jos se havaitsee tapahtuman ja/tai vian.

183) Virransyötön keskeytymistapausta koskeva varoitus voidaan antaa virransyötön uudelleenkytkemisen jälkeen.

184) Valvontalaitteen on varoitettava kuljettajaa 15 minuuttia ennen suurimman sallitun keskeytymättömän ajoajan ylitystä sekä ylityksen tapahtumahetkellä.

185) Varoitusten on oltava näkyviä. Näkyvien varoitusten lisäksi voidaan antaa kuultavia varoituksia.

186) Käyttäjän on kyettävä selvästi tunnistamaan näkyvät varoitukset, niiden on oltava kuljettajan näkökentässä ja selvästi luettavissa sekä päivällä että yöllä.

187) Näkyviä varoituksia voidaan lisätä valvontalaitteeseen ja/tai järjestää erilleen siitä.

188) Jälkimmäisessä tapauksessa varoituksessa on oltava merkki ”T”.

189) Varoitusten on kestettävä vähintään 30 sekuntia, ellei käyttäjä kuittaa niitä painamalla yhtä tai useampaa valvontalaitteen erityisnäppäintä. Tämä pikakuittaus ei tyhjennä varoituksen syyn kertovaa näyttöä, johon viitataan seuraavassa kappaleessa.

190) Varoituksen syyn on näyttävä valvontalaitteen näytössä, kunnes käyttäjä kuittaa sen tietyllä valvontalaitteen näppäimellä tai komennolla.

191) Muita varoituksia voidaan antaa, jos ne eivät aiheuta kuljettajille sekaannusta edellä mainittujen varoitusten suhteen.

3.18 **Tietojen kopioiminen ulkoisille tietovälineille**

192) Valvontalaitteen on kyettävä tarvittaessa kopioimaan tietoja datamuististaan tai kuljettajakortilta ulkoisille tallennusvälineille kalibrointi-/kopiointiliittimen kautta. Valvontalaitteen on päivitettävä kyseiselle kortille tallennetut tiedot ennen tulostusta.

▼B

193) Lisäksi valvontalaitteessa voi olla lisäominaisuus, jonka avulla se voi missä hyvänsä toimintatilassa kopioida tietoja jollakin muulla keinolla yritykselle, jonka tunnistetiedot on varmennettu tämän väylän kautta. Tällaisessa tapauksessa kopioinnille pätevät yritystilaa vastaavat käyttöoikeudet.

194) Kopiointi ei saa muuttaa tai pyyhkiä tallennettuja tietoja.

195) Kalibrointi-/kopiointiliittimen sähköiset liityntätiedot on määritelty lisäyksessä 6.

196) Kopiointiprotokollat on määritelty lisäyksessä 7.

3.19 **Kohdistettuihin tienvarsitarkastuksiin liittyvä etäviestintä**

197) Kun virta on päällä, ajoneuvoyksikön on tallennettava 60 sekunnin välein etäviestintälaitteistolla viimeisimmät tarvittavat tiedot kohdistettuja tienvarsitarkastuksia varten. Tällaiset tiedot on salattava ja allekirjoitettava lisäyksen 11 ja 14 perusteella.

198) Etäältä tarkistettavien tietojen on oltava etäyhteyslukijoiden käytettävissä langattoman viestinnän avulla, kuten lisäyksessä 14 määritetään.

199) Tiedot, joita tarvitaan kohdistettuja tienvarsitarkastuksia varten koskevat seuraavaa:

— viimeisin tietoturvaloukkausyritys,

— pisin virtakatkos,

— sensorivika,

— virhe liikedatassa,

— ajoneuvon liikeristiriita,

— ajaminen ilman voimassa olevaa korttia,

— kortin syöttäminen ajon aikana,

— ajanasetustiedot,

— kalibrointitiedot ja kahden viimeisen tallennetun kalibrointitiedon ajankohdat,

— ajoneuvon rekisterinumero,

— ajopiirturin kirjaama nopeus.

3.20 **Tietojen tulostus ulkoisille lisälaitteille**

200) Valvontalaitteet voidaan varustaa standardien mukaisilla rajapinnoilla, jotka mahdollistavat sen, että ajopiirturin kirjaamia tai tuottamia tietoja voidaan käyttää kalibrointi- tai normaalitilassa ulkoisessa laitteistossa.

Lisäyksessä 13 määritellään ja standardoidaan vaihtoehtoinen ITS-rajapinta. Muita vastaavia rajapintoja voi esiintyä samaan aikaan, jos ne täyttävät täysin lisäyksen 13 vaatimukset tietoja, turvallisuutta ja kuljettajan suostumusta koskevasta vähimmäisluettelosta.

Seuraavia vaatimuksia sovelletaan ITS-tietoihin, jotka on asetettu saataville kyseisen rajapinnan kautta:

— nämä tiedot ovat sarja ajopiirtureiden tietohakemiston valittuja olemassa olevia tietoja (lisäys 1),

▼B

— näiden valittujen tietojen osajoukko merkitään henkilötiedoiksi,

— henkilötietoja koskeva osajoukko on saatavilla vain, jos voidaan todentaa kuljettajan suostumus siihen, että hänen henkilötietoja saadaan välittää ajoneuvoverkon ulkopuolelle,

— kuljettajan suostumus voidaan millä hetkellä tahansa ottaa käyttöön tai poistaa käytöstä valikkokomennoilla, jos kuljettajakortti on asetettu yksikköön,

— tietojoukko ja tietojen osajoukko lähetetään langattomalla Bluetooth-yhteyskäytännöllä ajoneuvon ohjaamon lähistössä, ja sen virkistystaajuus on 1 minuutti,

— ulkoisen laitteen liittämistä ITS-rajapintaan suojataan tiettyyn käyttöön varatulla ja sattumanvaraisella vähintään neljän numeron PIN-koodilla, joka tallennetaan kuhunkin ajoneuvoyksikköön ja on saatavilla sen näytöllä,

— ITS-rajapinnan olemassaolo ei saa missään tilanteessa häiritä ajoneuvoyksikön asianmukaista toimintaa ja turvallisuutta tai vaikuttaa siihen.

Valittujen olemassa olevien tietojoukkojen, jotka katsotaan vähimmäisluetteloksi, lisäksi voidaan tulostaa myös muita tietoja, mikäli niitä ei voida pitää henkilötietoina.

Valvontalaitteen on välitettävä muille ulkoisille laitteistoille tieto kuljettajan suostumuksesta.

Kun ajoneuvon sytytysvirtakytkin on ON-asennossa, laitteen on tulostettava näitä tietoja jatkuvasti sarjaliitäntäporttiin.

201) Sarjaliitännän rajapinta, joka määritetään asetuksen (ETY) N:o 3821/85 liitteessä 1 B, sellaisena kuin se on viimeksi muutettuna, voi edelleen olla ajopiirtureissa yhteensopivuuden takaamiseksi. Kuljettajan suostumusta tarvitaan kuitenkin edelleen, jos välitetään henkilötietoja.

3.21 **Kalibrointi**

202) Kalibrointitoiminnon avulla on voitava:

— automaattisesti liittää liiketunnistin ajoneuvoyksikköön,

— automaattisesti kytkeä ulkoinen GNSS-laitteisto ajoneuvoyksikköön tarvittaessa,

— digitaalisesti sovittaa valvontalaitteen vakio (k) ajoneuvon ominaiskertoimeen (w),

— asettaa kuluva aika korttiaukkoon asetetun korjaamokortin voimassaoloajan puitteisiin,

— asettaa matkamittarin kuluva lukema,

— päivittää datamuistiin tallennetut liiketunnistimen tunnistetiedot,

— päivittää tarvittaessa datamuistiin tallennetut ulkoisen GNSS-laitteiston tunnistetiedot,

▼B

— päivittää kaikkien käytössä olevien sinetöintien tyypit ja tunnisteet,

— päivittää tai vahvistaa muita valvontalaitteen tiedossa olevia parametreja, joita ovat: ajoneuvon tunnistetiedot, w-kerroin, l-mitta, rengaskoko ja nopeudenrajoittimen asetukset, jos sellainen on.

203) Lisäksi kalibrointitoiminnon perustella voidaan poistaa ensimmäisen sukupolven ajopiirturikorttien käyttö valvontalaitteessa, jos lisäyksessä 15 tarkoitetut olosuhteet täyttyvät.

204) Liiketunnistimen ajoneuvoyksikköön liittämiseen on sisällyttävä ainakin:

— liiketunnistimeen tallennettujen liiketunnistimen asennustietojen päivitys (tarvittaessa),

— tarvittavien liiketunnistimen tunnistetietojen kopiointi tunnistimelta ajoneuvoyksikön datamuistiin.

205) Ulkoisen GNSS-laitteiston ajoneuvoyksikköön liittämiseen on sisällyttävä ainakin:

— ulkoisen GNSS-laitteiston muistiin tallennettujen asennustietojen päivittäminen (tarvittaessa),

— tarvittavien ulkoisen GNSS-laitteiston tunnistetietojen kopiointi tunnistimelta ajoneuvoyksikön datamuistiin, mukaan lukien ulkoisen GNSS-laitteiston sarjanumero.

Kytkentää seuraa GNSS-sijaintitietojen todentaminen.

206) Kalibrointitoiminnon avulla on kyettävä automaattisesti syöttämään tarvittavat tiedot kalibrointi-/kopiointiliittimen kautta lisäyksessä 8 määriteltyä kalibrointiprotokollaa käyttäen. Kalibrointitoiminnon avulla voidaan syöttää myös muita tarvittavia tietoja muiden keinojen avulla.

3.22 **Kalibroinnin tarkastus tien varrella**

207) Kalibroinnin tarkastus tien varrella mahdollistaa liiketunnistimen (joka on mahdollisesti sulautettu muuntimeen) sarjanumeron ja ulkoisen GNSS-laitteiston sarjanumeron (kun tämä on tarpeen) lukemisen pyynnön esittämishetkellä.

208) Tämä voidaan suorittaa ainakin ajoneuvoyksikön näytöllä valikon komennoilla.

209) Kalibroinnin tarkastuksessa tien varrella on voitava valvoa myös kalibroinnin tulo-/lähtösignaalijohtimen tilan valintaa, kuten lisäyksessä 6 määritetään, K-johdinliitännän avulla. Tämä on tehtävä ECUAdjustmentSession-jakson kautta, kuten lisäyksessä 8 olevassa 7 kohdassa (Testipulssien ohjaus – tulo-/lähtösignaalien ohjauksen toimintayksikkö) määritetään.

3.23 **Ajan asetus**

210) Ajan asetustoiminnon avulla on kyettävä asettamaan kuluva aika automaattisesti. Valvontalaitteessa käytetään kahta aikalähdettä ajan säätämiseen: 1) ajoneuvoyksikön sisäistä kelloa, 2) GNSS-vastaanottajaa.

▼B

211) Ajoneuvoyksikön sisäistä kelloa säädetään automaattisesti uudelleen korkeintaan 12 tunnin välein. Kun tämä aika on kulunut ja GNSS-signaalia ei ole käytettävissä, ajan säätäminen suoritetaan heti, kun ajoneuvoyksikkö saa GNSS-vastaanottimesta oikean aikatiedon ajoneuvon sytytysvirtaa koskevien olosuhteiden perusteella. Ajoneuvoyksikön sisäisen kellon automaattisen ajan asetuksen aikaviite saadaan GNSS-vastaanottimesta. Aikojen päällekkäisyys -tapahtuma syntyy, jos kuluva aika poikkeaa yli minuutin GNSS-vastaanottimen antamista aikatiedoista.

212) Ajan asetustoiminnon perusteella kuluvaa aikaa mukautetaan laitteen ollessa kalibrointitilassa.

3.24 **Suorituskykyä koskevat tiedot**

213) Ajoneuvoyksikön on säilyttävä täysin toimintakuntoisena lämpötilan ollessa – 20 °C–70 °C, ulkoisen GNSS-laitteiston – 20 °C–70 °C, ja liiketunnistimen – 40 °C–135 °C. Datamuistin tietojen on säilyttävä alle – 40 °C lämpötilassa.

214) Ajopiirturin on säilyttävä täysin toimintakuntoisena kosteuden ollessa 10–90 %.

215) Älykkäässä ajopiirturissa käytettyjen sinetöintien on kestettävä samat vaatimukset, joita sovelletaan ajopiirturin osiin, joihin ne on kiinnitetty.

216) Valvontalaitteen on oltava suojattu ylijännitettä, väärää napaisuutta ja oikosulkuja vastaan.

217) Liiketunnistinten on:

— reagoitava magneettikenttään, joka häiritsee ajoneuvon liikkeen havaitsemista. Näissä tilanteissa ajoneuvoyksikön on tallennettava ja säilytettävä liiketunnistimen vika (vaatimus 88), tai

— sisällettävä tuntoelin, joka on suojattu magneettikentiltä tai joka ei reagoi magneettikenttiin.

218) Valvontalaitteen ja ulkoisen GNSS-laitteiston on oltava kansainvälisen säännön UN ECE R10 mukainen ja suojattu staattisen sähkön aiheuttamilta purkauksilta ja jännitepiikeiltä.

3.25 **Materiaalit**

219) Kaikkien valvontalaitteen osien on oltava valmistettuja materiaaleista, joilla on riittävä kestävyys ja mekaaninen lujuus sekä muuttumattomat sähköiset ja magneettiset ominaisuudet.

220) Normaalien käyttöolosuhteiden vuoksi kaikki laitteen sisäpuoliset osat on suojattava kosteudelta ja pölyltä.

221) Ajoneuvoyksikön ja ulkoisen GNSS-laitteiston on täytettävä IEC 60529:1989 -standardin mukaiset suojausluokan IP 40 vaatimukset ja liiketunnistimen on täytettävä suojausluokan IP 64 vaatimukset, mukaan lukien A1:1999 ja A2:2013.

222) Valvontalaitteen on täytettävä siihen soveltuvien ergonomiseen muotoiluun liittyvien määräysten vaatimukset.

▼B

223) Valvontalaite on suojattava mahdollisilta vahingoilta.

3.26 **Merkinnät**

224) Jos valvontalaite näyttää ajoneuvon matkamittarilukeman ja nopeuden, on sen näytössä oltava seuraavat merkinnät:

— matkan mittayksikkö, jota osoittaa km-lyhenne matkaa osoittavan lukeman lähellä,

— merkintä ”km/h” nopeutta osoittavan lukeman lähellä.

Valvontalaite voidaan myös kytkeä osoittamaan nopeutta maileina tunnissa, jolloin nopeuden mittayksikkö on näytettävä lyhenteellä ”mph”. Valvontalaite voidaan myös kytkeä osoittamaan etäisyyttä maileina, jolloin etäisyyden mittayksikkö on näytettävä lyhenteellä ”mi”.

225) Jokaiseen valvontalaitteen erilliseen osaan on kiinnitettävä tunnistekilpi, josta ilmenevät seuraavat tiedot:

— laitteen valmistajan nimi ja osoite,

— valmistajan osanumero sekä laitteen valmistusvuosi,

— laitteen sarjanumero,

— laitteen tyyppihyväksyntätunnus.

226) Jos tila ei riitä kaikkien edellä mainittujen tietojen näyttämiseen, tunnistekilvestä on ilmettävä ainakin valmistajan nimi tai liiketunnus sekä laitteen osanumero.

4. AJOPIIRTURIKORTTIEN RAKENNETTA JA TOIMINTOJA KOSKEVAT VAATIMUKSET

4.1 **Näkyvissä olevat tiedot**

Etupuolella on oltava

227) kortin tyypin mukaan sana ”kuljettajakortti” tai ”valvontakortti” tai ”korjaamokortti” tai ”yrityskortti” painettuna suurikokoisin kirjaimin kortin myöntävän jäsenvaltion virallisella kielellä tai kielillä,

228) kortin myöntävän jäsenvaltion nimi (vapaaehtoinen merkintä),

229) kortin myöntävän jäsenvaltion kansainvälinen tunnus negatiivina sinisessä suorakulmiossa ja kahdentoista keltaisen tähden ympäröimänä. Jäsenvaltioiden kansainväliset tunnukset ovat seuraavat:

B	Belgia	LV	Latvia
BG	Bulgaria	L	Luxemburg
CZ	Tšekki	LT	Liettua
CY	Kypros	M	Malta
EOS	Tanska	NL	Alankomaat
D	Saksa	A	Itävalta
EST	Viro	PL	Puola

▼B

GR	Kreikka	P RO SK SLO	Portugali Romania Slovakia Slovenia
E	Espanja	FIN	Suomi
F HR H	Ranska Kroatia Unkari	S	Ruotsi
IRL	Irlanti	UK	Yhdistynyt kuningaskunta
I	Italia		

230) myönnettyä korttia koskevat seuraavasti numeroidut tiedot:

	Kuljettajakortti	Valvontakortti	Yritys- tai korjaamokortti
1.	kuljettajan sukunimi	tarkastuselimen nimi,	yrityksen tai korjaamon nimi.
2.	kuljettajan etunimi (etunimet)	valvojan nimi: (jos myönnetty)	kortinhaltijan sukunimi (jos myönnetty)
3.	kuljettajan syntymäaika	kuljettajan etunimi (etunimet) (jos myönnetty)	haltijan etunimi (etunimet), (jos myönnetty)
4.a	kortin ensimmäinen voimassaolopäivä		
4.b	kortin viimeinen voimassaolopäivä		
4.c	kortin myöntänyt viranomainen (voidaan painaa kortin kääntöpuolelle)		
4.d	hallinnollinen numero, joka on muu kuin kohdassa 5 ilmoitettu numero (vapaaehtoinen)		
5. a	ajokortin numero: (kuljettajakortin myöntämispäivänä)	—	—
5. b	kortin numero		
6.	kuljettajan valokuva	valvojan valokuva (vapaaehtoinen)	asentajan valokuva (vapaaehtoinen)
7.	haltijan allekirjoitus (vapaaehtoinen)		
8.	haltijan vakinainen asuinpaikka tai postiosoite (vapaaehtoinen)	valvontaelimen postiosoite	yrityksen tai korjaamon postiosoite

231) Päivämäärät on kirjoitettava käyttäen muotoa ”pp/kk/vvvv” tai ”pp.kk.vvvv” (päivä, kuukausi, vuosi).

Kääntöpuolella on oltava

232) Kortin etupuolella olevien numeroitujen kohtien selitykset ja

▼B

233) haltijan nimenomaisella kirjallisella suostumuksella lisättyjä, muita kuin korttia koskevia hallinnollisia tietoja; tämänkaltaisten tietojen lisääminen ei millään tavoin vaikuta mallin käyttämiseen ajopiirturikorttina.

234) Ajopiirturikortit on painettava käyttäen seuraavia hallitsevia taustavärejä:

— kuljettajakortti: valkoinen,

— valvontakortti: sininen,

— korjaamokortti: punainen,

— yrityskortti: keltainen.

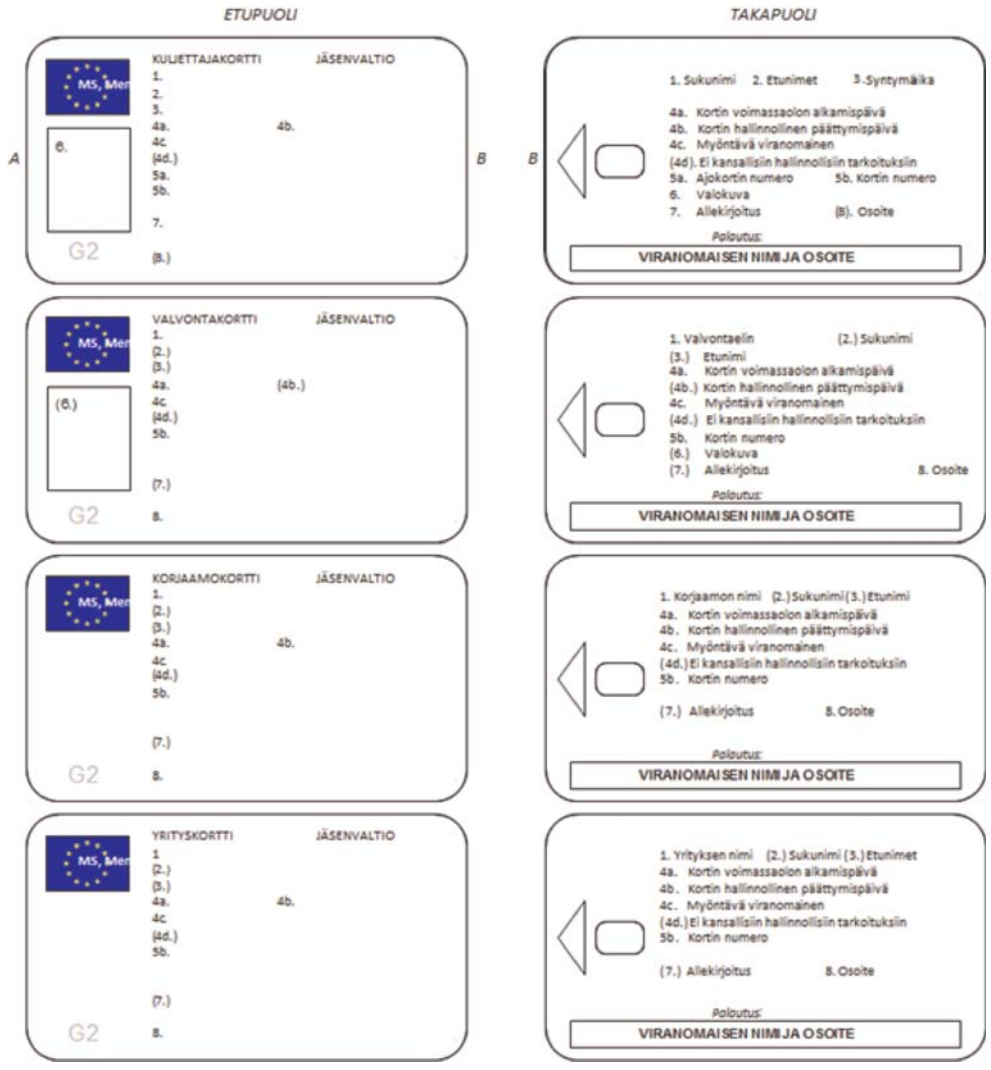
235) Ajopiirturikorteilla on oltava ainakin seuraavat ominaisuudet, jotka suojaavat niitä väärentämiseltä ja vilpilliseltä käsittelyltä:

— turvakuviointi, jossa on ohut aaltomainen viivakuvio ja iirispainatus,

— valokuvan kohdalla on taustan turvakuvioinnin ja valokuvan mentävä osittain päällekkäin,

— ainakin yksi kaksiväristä mikrokirjoitusta sisältävä rivi.

AJOPIIRTURIKORTTIEN YHTEISÖN MALLI



▼B

236) Jäsenvaltiot voivat komissiota kuultuaan lisätä korttiin värejä tai merkintöjä, kuten kansallisia tunnuksia ja turvallisuutta lisääviä ominaisuuksia, tämän kuitenkaan rajoittamatta tämän liitteen muita määräyksiä.

237) Asetuksen (EU) N:o 165/2014 26 artiklan 4 kohdassa tarkoitettujen tilapäisten korttien on oltava tämän liitteen säännösten mukaisia.

4.2 **Turvallisuus**

Järjestelmän turvallisuuden tavoitteena on suojata korttien ja valvontalaitteen välillä siirrettävien tietojen eheys ja autenttisuus, suojata korteilta kopioitavien tietojen eheys ja autenttisuus, sallia valvontalaitteiden siirtää vain tiettyjä tietoja korteille, salata tietyt tiedot, tehdä korteille tallennetun tiedon väärentäminen mahdottomaksi, estää vilpillinen käsittely sekä havaita kaikki sen tapaiset yritykset.

238) Järjestelmän turvallisuuden saavuttamiseksi ajopiirturikorttien on täytettävä tietoturvavaatimukset, jotka on määritelty lisäyksessä 10 ja 11.

239) Ajopiirturikorttien on oltava luettavissa muilla laitteilla, kuten henkilökohtaisilla tietokoneilla.

4.3 **Standardit**

240) Ajopiirturikorttien on oltava seuraavien standardien mukaisia:

— ISO/IEC 7810 Identification cards – Physical characteristics,

— ISO/IEC 7816 Identification cards – Integrated circuit cards:

  — Part 1: Physical characteristics (fyysiset ominaisuudet),

  — Part 2: Dimensions and position of the contacts (ISO/IEC 7816-2:2007),

  — Part 3: Electrical interface and transmission protocols (ISO/IEC 7816-3:2006),

  — Part 4: Organisation, security and commands for interchange (ISO/IEC 7816-4:2013 + Cor 1:2014),

  — Part 6: Interindustry data elements for interchange (ISO/IEC 7816-6:2004 + Cor 1:2006),

  — Part 8: Commands for security operations (ISO/IEC 7816-8:2004).

— Ajopiirturikortit on testattava seuraavan standardin mukaisesti: ISO/IEC 10373-3:2010 Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices.

4.4 **Ympäristöön liittyvät ja sähkötekniset eritelmät**

241) Ajopiirturikorttien on kyettävä toimimaan moitteettomasti kaikissa yhteisön alueella tavattavissa ilmasto-olosuhteissa sekä vähintään lämpötila-alueella – 25 °C–+ 70 °C, jolloin satunnaiset lämpötilahuiput voivat olla jopa + 85 °C, missä satunnainen tarkoittaa enintään neljän tunnin jaksoja kerrallaan enintään sata kertaa kortin käyttöiän aikana.

242) Ajopiirturikorttien on voitava toimia moitteettomasti kosteuden ollessa 10–90 %.

▼B

243) Ajopiirturikorttien on voitava toimia moitteettomasti viiden vuoden ajan, jos niitä käytetään ympäristöön liittyvien ja sähköteknisten eritelmien rajoissa.

244) Käytön aikana ajopiirturikortin on oltava sähkömagneettisesta yhteensopivuudesta annetun standardin ECE R10 mukainen sekä suojattu staattisen sähkön aiheuttamilta purkauksilta.

4.5 **Tietojen säilyttäminen**

Tässä kohdassa:

— ajat kirjataan yhden minuutin tarkkuudella, ellei toisin määritellä,

— matkamittarin lukemat kirjataan yhden kilometrin tarkkuudella,

— nopeudet kirjataan tarkkuudella 1 km/t,

— sijainnit (leveys- ja pituusasteet) tallennetaan asteina ja minuutteina tarkkuudella 1/10 minuuttia.

Tietojen tallennuksen vaatimukset täyttävät ajopiirturikorttien toiminnot, komennot ja loogiset rakenteet on määritelty lisäyksessä 2.

Jollei toisin mainita, tietojen säilyttäminen ajopiirturikorteilla on järjestettävä siten, että uudet tiedot korvaavat säilytetyt vanhimmat tiedot, jos tietyille tietueille varattu muisti on käytetty loppuun.

245) Tässä kohdassa määritellään erilaisia sovellustiedostoja koskevat tiedontallennuskapasiteetin vähimmäisvaatimukset. Ajopiirturikorttien on kyettävä antamaan valvontalaitteelle tieto näiden tiedostojen vaatimasta todellisesta tallennuskapasiteetista.

246) Muut ajopiirturikorteille mahdollisesti tallennettavat, muihin kortilla mahdollisesti oleviin sovelluksiin liittyvät tiedot on tallennettava direktiivin 95/46/EY, direktiivin 2002/58/EY sekä asetuksen (EU) N:o 165/2014 7 artiklan mukaisesti.

247) Jokaiseen ajopiirturikortin MF-tiedostoon on sisällyttävä enintään viisi EF-tiedostoa kortin hallinnointia, soveltamista ja sirujen tunnistetietoja varten sekä kaksi DF-tiedostoa (Dedicated File):

— DF Tachograph -tiedosto, johon sisältyy ensimmäisen sukupolven ajoneuvoyksikköihin soveltuva laite, sisältyy myös ensimmäisen sukupolven ajopiirturikortteihin,

— DF Tachograph_G2-tiedosto, johon sisältyy pelkästään toisen sukupolven ajoneuvoyksikköihin soveltuva laite, sisältyy ainoastaan toisen sukupolven ajopiirturikortteihin.

Täydelliset tiedot ajopiirturikorteista määritellään lisäyksessä 2.

4.5.1 *Perustiedostot tunnistamiseen ja kortin hallinnointiin*

4.5.2 *Sirukorttien tunnistetiedot*

248) Ajopiirturikorttien on kyettävä tallentamaan seuraavat älykorttien tunnistetiedot:

— kellon pysäytys,

▼B

— kortin sarjanumero (mukaan lukijan valmistajan viitetiedot),

— kortin tyyppihyväksyntänumero,

— kortin yksilöivä tunniste,

— kortin laminoijan tunniste,

— integroidun piirin tunniste.

4.5.2.1 Mikrosirujen tunnistetiedot

249) Ajopiirturikorttien on kyettävä tallentamaan seuraavat integroitujen piirien tunnistetiedot:

— integroidun piirin sarjanumero,

— integroidun piirin valmistajan viitetiedot.

4.5.2.2 DIR-tiedostot (esiintyvät ainoastaan toisen sukupolven ajopiirturikorteissa)

250) Ajopiirturikorttien on kyettävä säilyttämään sovellusten tunnistetiedot, jotka määritellään lisäyksessä 2.

4.5.2.3 ATR-tiedot (ehdolliset, esiintyvät ainoastaan toisen sukupolven ajopiirturikorteissa)

251) Ajopiirturikorttien on kyettävä tallentamaan seuraavat pituudeltaan laajennetut dataobjektin tiedot:

— jos ajopiirturikortit tukevat pidennettyjä kenttäpituuksia, lisäyksessä 2 määritetyt pituudeltaan laajennetut dataobjektin tiedot.

4.5.2.4 Laajennettua pituutta koskevat tiedot (ehdolliset, esiintyvät ainoastaan toisen sukupolven ajopiirturikorteissa)

252) Ajopiirturikorttien on kyettävä säilyttämään seuraavat pituudeltaan laajennetut dataobjektin tiedot:

— Jos ajopiirturikortti tukee laajennettuja kenttäpituuksia, lisäyksessä 2 määritetyt pituudeltaan laajennetut dataobjektin tiedot.

4.5.3 *Kuljettajakortti*

4.5.3.1 Ajopiirturikortin sovellus (joka on ensimmäisen ja toisen sukupolven ajoneuvoyksikköjen käytettävissä)

4.5.3.1.1 Sovellusten tunnistetiedot

253) Kuljettajakortin on kyettävä tallentamaan seuraavat sovellusten tunnistetiedot:

— ajopiirturisovelluksen tunniste,

— ajopiirturikortin tunnisteen tyyppi.

4.5.3.1.2 Avaimet ja varmenteet

254) Kuljettajakortin on kyettävä tallentamaan useita salausavaimia ja varmenteita, kuten lisäyksen 11 A osassa määritetään.

▼B

4.5.3.1.3 Kortin tunniste

255) Kuljettajakortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:

— kortin numero,

— kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,

— kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä.

4.5.3.1.4 Kortin haltijan tunnistetiedot

256) Kuljettajakortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:

— haltijan sukunimi,

— haltijan etunimi (etunimet),

— syntymäaika,

— haltijan ensisijaisesti käyttämä kieli.

4.5.3.1.5 Kortilla olevien tietojen kopiointi

257) Kuljettajakortin on kyettävä tallentamaan seuraavat kortilla olevien tietojen kopiointiin liittyvät tiedot:

— viimeisimmän (muussa kuin valvontatarkoituksessa tehdyn) kortin tietojen kopioinnin päivämäärä ja aika.

258) Kuljettajakortin on kyettävä tallentamaan yksi tällainen tietue.

4.5.3.1.6 Ajokorttiin liittyvät tiedot

259) Kuljettajakortin on kyettävä tallentamaan seuraavat ajokorttiin liittyvät tiedot:

— kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi,

— ajokortin numero (myöntämispäivänä).

4.5.3.1.7 Tapahtumiin liittyvät tiedot

Tässä alakohdassa käsiteltäviin asioihin liittyvä aika on kirjattava yhden sekunnin tarkkuudella.

260) Kuljettajakortin on kyettävä tallentamaan tiedot, jotka liittyvät seuraaviin tapahtumiin, jotka valvontalaite on havainnut kortin ollessa paikoilleen asetettuna:

— aikojen päällekkäisyys (jos tapahtuma on tämän kortin aiheuttama),

— kortin paikoilleen asettaminen ajettaessa (jos tämä kortti on tapahtuman kohteena),

— edellistä kortin käyttöjaksoa ei lopetettu oikein (jos tämä kortti on tapahtuman kohteena),

— keskeytynyt virransyöttö,

— virhe liikedatassa,

— tietoturvan murtoyritykset.

261) Kuljettajakortin on kyettävä tallentamaan seuraavat näihin tapahtumiin liittyvät tiedot:

— tapahtuman tunnuskoodi,

— päivämäärä ja aika, jolloin tapahtuma alkoi (tai päivämäärä ja aika, jolloin kortti asetettiin paikoilleen, jos tapahtuma oli tuolloin jo alkanut),

▼B

— päivämäärä ja aika, jolloin tapahtuma päättyi (tai päivämäärä ja aika, jolloin kortti poistettiin, jos tapahtuma oli tuolloin vielä käynnissä),

— tapahtumaan liittyvän ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

Huomautus: ”aikojen päällekkäisyys” -tapahtuman osalta:

— tapahtuman alkamispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti poistettiin edellisestä ajoneuvosta,

— tapahtuman päättymispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti asetettiin paikoilleen tällä hetkellä käytössä olevaan ajoneuvoon,

— ajoneuvoon liittyvien tietojen on vastattava tällä hetkellä käytössä olevaa, tapahtuman aiheuttanutta ajoneuvoa.

Huomautus: ”edellistä kortin käyttöjaksoa ei lopetettu oikein” -tapahtuman osalta:

— tapahtuman alkamispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti asetettiin paikoilleen sen käyttöjakson aluksi, jota ei lopetettu oikein,

— tapahtuman päättymispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti asetettiin paikoilleen sen käyttöjakson aluksi, jonka aikana tapahtuma havaittiin (kuluva käyttöjakso),

— ajoneuvoon liittyvien tietojen on vastattava sitä ajoneuvoa, jota käytettäessä kortin käyttöjaksoa ei lopetettu oikein.

262) Kuljettajakortin on kyettävä tallentamaan kuuteen viimeisimpään kutakin tapahtumatyyppiä edustavaan tapahtumaan liittyvät tiedot (eli 36 tapahtuman tiedot).

4.5.3.1.8 Vikoihin liittyvät tiedot

Tässä alakohdassa käsiteltäviin asioihin liittyvä aika on kirjattava yhden sekunnin tarkkuudella.

263) Kuljettajakortin on kyettävä tallentamaan tiedot, jotka liittyvät seuraaviin vikoihin, jotka valvontalaite on havainnut kortin ollessa paikoilleen asetettuna:

— korttivika (jos tämä kortti on tapahtuman kohteena),

— valvontalaitteen vika.

264) Kuljettajakortin on kyettävä tallentamaan seuraavat näihin vikoihin liittyvät tiedot:

— vikakoodi,

— päivämäärä ja aika, jolloin vikatapahtuma alkoi (tai päivämäärä ja aika, jolloin kortti asetettiin paikoilleen, jos vikatapahtuma oli tuolloin jo alkanut),

— päivämäärä ja aika, jolloin vikatapahtuma päättyi (tai päivämäärä ja aika, jolloin kortti poistettiin, jos vikatapahtuma oli tuolloin vielä käynnissä),

— vikatapahtumaan liittyvän ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

265) Kuljettajakortin on kyettävä tallentamaan kahteentoista viimeisimpään kutakin vikatyyppiä edustavaan vikatapahtumaan liittyvät tiedot (eli 24 vikatapahtuman tiedot).

▼B

4.5.3.1.9 Kuljettajan toimintaan liittyvät tiedot

266) Kuljettajakortin on kyettävä tallentamaan seuraavat tiedot erikseen jokaista sellaista kalenterivuorokautta kohti, jolloin korttia on käytetty tai joille kuljettaja on syöttänyt tietoja käsin:

— päivämäärä,

— käyttövuorokausien juokseva järjestysnumero (jota suurennetaan yhdellä jokaisena sellaisena kalenterivuorokautena, jolloin korttia käytetään),

— kuljettajan kyseisen vuorokauden aikana kulkema kokonaismatka,

— kuljettajatilanne klo 00.00,

— seuraavat tiedot aina, kun kuljettajan toiminnan tila muuttuu ja/tai ajoneuvon miehitys muuttuu ja/tai kuljettajakortti asetetaan paikoilleen tai poistetaan:

— ajoneuvon miehitys (CREW, SINGLE),

— korttiaukko (DRIVER, CO-DRIVER),

— kortin tila (INSERTED, NOT INSERTED),

— toiminta (DRIVING, AVAILABILITY, WORK, BREAK/REST),

— aika, jolloin muutos tapahtui.

267) Kuljettajakortin muistin on kyettävä tallentamaan kuljettajan toimintaan liittyviä tietoja vähintään 28 vuorokauden ajalta (kuljettajan keskimääräisen toiminnan määritellään sisältävän 93 toiminnan tilan muutosta vuorokaudessa).

268) Vaatimuksien 261, 264 ja 266 perusteella luetellut tiedot on tallennettava siten, että toimintaa koskevat tiedot voidaan hakea siinä järjestyksessä, jossa nämä toiminnat ovat tapahtuneet, vaikka aikatiedoissa olisikin päällekkäisyyttä.

4.5.3.1.10 Käytössä olleisiin ajoneuvoihin liittyvät tiedot

269) Kuljettajakortin on kyettävä tallentamaan seuraavat tiedot erikseen jokaista sellaista kalenterivuorokautta kohti, jolloin korttia on käytetty, ja erikseen jokaista tietyn ajoneuvon kyseisenä päivänä tapahtunutta käyttöjaksoa kohti (käyttöjaksoon sisältyvät kaikki peräkkäin tapahtuneet työjaksot kortin paikoilleen asettamisesta sen poistoon kyseisessä ajoneuvossa, kortin kannalta tarkasteltuna):

— päivämäärä ja aika, jolloin ajoneuvoa ensi kerran käytettiin (eli hetki, jolloin kortti ensimmäisen kerran asetettiin paikoilleen kyseisen ajoneuvon käyttöjakson aikana, tai klo 00.00, jos ajoneuvon käyttö tuolloin oli jatkuvaa),

— ajoneuvon matkamittarin lukema tuona ajanhetkenä,

— päivämäärä ja aika, jolloin ajoneuvoa viimeisen kerran käytettiin (eli hetki, jolloin kortti viimeisen kerran poistettiin kyseisen ajoneuvon käyttöjakson aikana, tai klo 23.59, jos ajoneuvon käyttö tuolloin oli jatkuvaa),

▼B

— ajoneuvon matkamittarin lukema tuona ajanhetkenä,

— ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

270) Kuljettajakortin on kyettävä tallentamaan vähintään 84 tällaista tietuetta.

4.5.3.1.11 Tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy

271) Kuljettajakortin on kyettävä tallentamaan seuraavat kuljettajan syöttämät tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy:

— päivämäärä ja aika, jolloin tiedot syötettiin (tai syötettyihin tietoihin liittyvä päivämäärä ja aika, jos tietojen syöttäminen tapahtui tietojen käsin syöttämistä koskevan menettelyn mukaisesti),

— syötetyn tiedon tyyppi (alkamis- tai päättymistieto, olosuhteet, joissa tieto on syötetty),

— valtio ja alue, jota syötetty tieto koskee,

— ajoneuvon matkamittarin lukema.

272) Kuljettajakortin muistin on kyettävä tallentamaan vähintään 42 paria tällaisia tietueita.

4.5.3.1.12 Kortin käyttöjaksoon liittyvät tiedot

273) Kuljettajakortin on kyettävä tallentamaan tiedot, jotka liittyvät ajoneuvoon, jota käytettäessä kuluva käyttöjakso alkoi:

— päivämäärä ja aika, jolloin käyttöjakso alkoi (eli kortti asetettiin paikoilleen) yhden sekunnin tarkkuudella,

— ajoneuvon rekisteritunnus, ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

4.5.3.1.13 Tarkastustoimiin liittyvät tiedot

274) Kuljettajakortin on kyettävä tallentamaan seuraavat tarkastustoimiin liittyvät tiedot:

— tarkastuksen päivämäärä ja aika,

— valvontakortin numero ja kortin myöntänyt jäsenvaltio,

— tarkastuksen tyyppi (tietojen näyttö ja/tai tulostus ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi (ks. huomautus)),

— jakso, jota koskevat tiedot kopioitiin, kun kyseessä on tietojen kopiointi,

— tarkastettavan ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

Huomautus: tietojen kopiointi kirjataan vain, jos se on suoritettu valvontalaitteen kautta.

275) Kuljettajakortin on kyettävä tallentamaan yksi tällainen tietue.

4.5.3.1.14 Erityisolosuhteisiin liittyvät tiedot

276) Kuljettajakortin on kyettävä tallentamaan seuraavat erityisolosuhteisiin liittyvät tiedot, jotka on syötetty kortin ollessa paikoilleen asetettuna (mihin hyvänsä korttiaukkoon):

— päivämäärä ja aika, jolloin tieto syötettiin,

— erityisolosuhteiden tyyppi.

▼B

277) Kuljettajakortin on kyettävä tallentamaan vähintään 56 tällaista tietuetta.

4.5.3.2 Ajopiirturin sukupolven 2 sovellus (ei voida käyttää ensimmäisen sukupolven ajoneuvoyksikössä)

4.5.3.2.1 Sovellusten tunnistetiedot

278) Kuljettajakortin on kyettävä tallentamaan seuraavat sovellusten tunnistetiedot:

— ajopiirturisovelluksen tunniste,

— ajopiirturikortin tunnisteen tyyppi.

4.5.3.2.2 Avaimet ja varmenteet

279) Kuljettajakortin on kyettävä tallentamaan useita salausavaimia ja varmenteita, kuten lisäyksessä 11 olevassa B osassa määritetään.

4.5.3.2.3 Kortin tunniste

280) Kuljettajakortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:

— kortin numero,

— kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,

— kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä.

4.5.3.2.4 Kortin haltijan tunnistetiedot

281) Kuljettajakortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:

— haltijan sukunimi,

— haltijan etunimi (etunimet),

— syntymäaika,

— haltijan ensisijaisesti käyttämä kieli.

4.5.3.2.5 Kortilla olevien tietojen kopiointi

282) Kuljettajakortin on kyettävä tallentamaan seuraavat kortilla olevien tietojen kopiointiin liittyvät tiedot:

— viimeisimmän (muussa kuin valvontatarkoituksessa tehdyn) kortin tietojen kopioinnin päivämäärä ja aika.

283) Kuljettajakortin on kyettävä tallentamaan yksi tällainen tietue.

4.5.3.2.6 Ajokorttiin liittyvät tiedot

284) Kuljettajakortin on kyettävä tallentamaan seuraavat ajokorttiin liittyvät tiedot:

— kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi,

— ajokortin numero (myöntämispäivänä).

4.5.3.2.7 Tapahtumiin liittyvät tiedot

Tässä alakohdassa käsiteltäviin asioihin liittyvä aika on kirjattava yhden sekunnin tarkkuudella.

▼B

285) Kuljettajakortin on kyettävä tallentamaan tiedot, jotka liittyvät seuraaviin tapahtumiin, jotka valvontalaite on havainnut kortin ollessa paikoilleen asetettuna:

— aikojen päällekkäisyys (jos tapahtuma on tämän kortin aiheuttama),

— kortin paikoilleen asettaminen ajettaessa (jos tämä kortti on tapahtuman kohteena),

— edellistä kortin käyttöjaksoa ei lopetettu oikein (jos tämä kortti on tapahtuman kohteena),

— keskeytynyt virransyöttö,

— virhe yhteydessä etäviestintälaitteistoon,

— sijaintitietojen puuttuminen GNSS-vastaanottimesta -tapahtuma,

— virhe viestinnässä ulkoisen GNSS-laitteiston kanssa,

— virhe liikedatassa,

— ajoneuvon liikeristiriita,

— tietoturvan murtoyritykset,

— aikojen päällekkäisyys.

286) Kuljettajakortin on kyettävä tallentamaan seuraavat näihin tapahtumiin liittyvät tiedot:

— tapahtuman tunnuskoodi,

— päivämäärä ja aika, jolloin tapahtuma alkoi (tai päivämäärä ja aika, jolloin kortti asetettiin paikoilleen, jos tapahtuma oli tuolloin jo alkanut),

— päivämäärä ja aika, jolloin tapahtuma päättyi (tai päivämäärä ja aika, jolloin kortti poistettiin, jos tapahtuma oli tuolloin vielä käynnissä),

— tapahtumaan liittyvän ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

Huomautus: ”aikojen päällekkäisyys” -tapahtuman osalta:

— tapahtuman alkamispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti poistettiin edellisestä ajoneuvosta,

— tapahtuman päättymispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti asetettiin paikoilleen tällä hetkellä käytössä olevaan ajoneuvoon,

— ajoneuvoon liittyvien tietojen on vastattava tällä hetkellä käytössä olevaa, tapahtuman aiheuttanutta ajoneuvoa.

Huomautus: ”edellistä kortin käyttöjaksoa ei lopetettu oikein” -tapahtuman osalta:

— tapahtuman alkamispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti asetettiin paikoilleen sen käyttöjakson aluksi, jota ei lopetettu oikein,

— tapahtuman päättymispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti asetettiin paikoilleen sen käyttöjakson aluksi, jonka aikana tapahtuma havaittiin (kuluva käyttöjakso),

▼B

— ajoneuvoon liittyvien tietojen on vastattava sitä ajoneuvoa, jota käytettäessä kortin käyttöjaksoa ei lopetettu oikein.

287) Kuljettajakortin on kyettävä tallentamaan kuuteen viimeisimpään kutakin tapahtumatyyppiä edustavaan tapahtumaan liittyvät tiedot (eli 66 tapahtuman tiedot).

4.5.3.2.8 Vikoihin liittyvät tiedot

Tässä alakohdassa käsiteltäviin asioihin liittyvä aika on kirjattava yhden sekunnin tarkkuudella.

288) Kuljettajakortin on kyettävä tallentamaan tiedot, jotka liittyvät seuraaviin vikoihin, jotka valvontalaite on havainnut kortin ollessa paikoilleen asetettuna:

— korttivika (jos tämä kortti on tapahtuman kohteena),

— valvontalaitteen vika.

289) Kuljettajakortin on kyettävä tallentamaan seuraavat näihin vikoihin liittyvät tiedot:

— vikakoodi,

— päivämäärä ja aika, jolloin vikatapahtuma alkoi (tai päivämäärä ja aika, jolloin kortti asetettiin paikoilleen, jos vikatapahtuma oli tuolloin jo alkanut),

— päivämäärä ja aika, jolloin vikatapahtuma päättyi (tai päivämäärä ja aika, jolloin kortti poistettiin, jos vikatapahtuma oli tuolloin vielä käynnissä),

— vikatapahtumaan liittyvän ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

290) Kuljettajakortin on kyettävä tallentamaan kahteentoista viimeisimpään kutakin vikatyyppiä edustavaan vikatapahtumaan liittyvät tiedot (eli 24 vikatapahtuman tiedot).

4.5.3.2.9 Kuljettajan toimintaan liittyvät tiedot

291) Kuljettajakortin on kyettävä tallentamaan seuraavat tiedot erikseen jokaista sellaista kalenterivuorokautta kohti, jolloin korttia on käytetty tai joille kuljettaja on syöttänyt tietoja käsin:

— päivämäärä,

— käyttövuorokausien juokseva järjestysnumero (jota suurennetaan yhdellä jokaisena sellaisena kalenterivuorokautena, jolloin korttia käytetään),

— kuljettajan kyseisen vuorokauden aikana kulkema kokonaismatka,

— kuljettajatilanne klo 00.00,

— seuraavat tiedot aina, kun kuljettajan toiminnan tila muuttuu ja/tai ajoneuvon miehitys muuttuu ja/tai kuljettajakortti asetetaan paikoilleen tai poistetaan:

— ajoneuvon miehitys (CREW, SINGLE),

— korttiaukko (DRIVER, CO-DRIVER),

— kortin tila (INSERTED, NOT INSERTED),

— toiminta (DRIVING, AVAILABILITY, WORK, BREAK/REST),

▼B

— aika, jolloin muutos tapahtui.

292) Kuljettajakortin muistin on kyettävä tallentamaan kuljettajan toimintaan liittyviä tietoja vähintään 28 vuorokauden ajalta (kuljettajan keskimääräisen toiminnan määritellään sisältävän 93 toiminnan tilan muutosta vuorokaudessa).

293) Vaatimuksien 286, 289 ja 291 perusteella luetellut tiedot on tallennettava siten, että toimintaa koskevat tiedot voidaan hakea siinä järjestyksessä, jossa nämä toiminnat ovat tapahtuneet, vaikka aikatiedoissa olisikin päällekkäisyyttä.

4.5.3.2.10 Käytössä olleisiin ajoneuvoihin liittyvät tiedot

294) Kuljettajakortin on kyettävä tallentamaan seuraavat tiedot erikseen jokaista sellaista kalenterivuorokautta kohti, jolloin korttia on käytetty, ja erikseen jokaista tietyn ajoneuvon kyseisenä päivänä tapahtunutta käyttöjaksoa kohti (käyttöjaksoon sisältyvät kaikki peräkkäin tapahtuneet työjaksot kortin paikoilleen asettamisesta sen poistoon kyseisessä ajoneuvossa, kortin kannalta tarkasteltuna):

— päivämäärä ja aika, jolloin ajoneuvoa ensi kerran käytettiin (eli hetki, jolloin kortti ensimmäisen kerran asetettiin paikoilleen kyseisen ajoneuvon käyttöjakson aikana, tai klo 00.00, jos ajoneuvon käyttö tuolloin oli jatkuvaa),

— ajoneuvon matkamittarin lukema ajanhetkenä, jolloin ajoneuvoa käytettiin ensi kerran,

— päivämäärä ja aika, jolloin ajoneuvoa viimeisen kerran käytettiin (eli hetki, jolloin kortti viimeisen kerran poistettiin kyseisen ajoneuvon käyttöjakson aikana, tai klo 23.59, jos ajoneuvon käyttö tuolloin oli jatkuvaa),

— ajoneuvon matkamittarin lukema ajanhetkenä, jolloin ajoneuvoa käytettiin viimeisen kerran,

— ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity,

— ajoneuvon valmistenumero.

295) Kuljettajakortin on kyettävä tallentamaan vähintään 84 tällaista tietuetta.

4.5.3.2.11 Tiedot paikasta ja sijainnit, jossa päivän työaika alkaa ja/tai päättyy

296) Kuljettajakortin on kyettävä tallentamaan seuraavat kuljettajan syöttämät tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy:

— päivämäärä ja aika, jolloin tiedot syötettiin (tai syötettyihin tietoihin liittyvä päivämäärä ja aika, jos tietojen syöttäminen tapahtui tietojen käsin syöttämistä koskevan menettelyn mukaisesti),

— syötetyn tiedon tyyppi (alkamis- tai päättymistieto, olosuhteet, joissa tieto on syötetty),

— valtio ja alue, jota syötetty tieto koskee,

— ajoneuvon matkamittarin lukema,

— ajoneuvon sijainti,

— GNSS-laitteiston tarkkuus, päivämäärä ja kellonaika, jolloin sijainti määritettiin.

297) Kuljettajakortin muistin on kyettävä tallentamaan vähintään 84 paria tällaisia tietueita.

▼B

4.5.3.2.12 Kortin käyttöjaksoon liittyvät tiedot

298) Kuljettajakortin on kyettävä tallentamaan tiedot, jotka liittyvät ajoneuvoon, jota käytettäessä kuluva käyttöjakso alkoi:

— päivämäärä ja aika, jolloin käyttöjakso alkoi (eli kortti asetettiin paikoilleen) yhden sekunnin tarkkuudella,

— ajoneuvon rekisteritunnus, ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

4.5.3.2.13 Tarkastustoimiin liittyvät tiedot

299) Kuljettajakortin on kyettävä tallentamaan seuraavat tarkastustoimiin liittyvät tiedot:

— tarkastuksen päivämäärä ja aika,

— valvontakortin numero ja kortin myöntänyt jäsenvaltio,

— tarkastuksen tyyppi (tietojen näyttö ja/tai tulostus ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi (ks. huomautus)),

— jakso, jota koskevat tiedot kopioitiin, kun kyseessä on tietojen kopiointi,

— tarkastettavan ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

Huom: tietoturvavaatimusten vuoksi tietojen kopiointi kirjataan vain, jos se on suoritettu valvontalaitteen kautta.

300) Kuljettajakortin on kyettävä tallentamaan yksi tällainen tietue.

4.5.3.2.14 Erityisolosuhteisiin liittyvät tiedot

301) Kuljettajakortin on kyettävä tallentamaan seuraavat erityisolosuhteisiin liittyvät tiedot, jotka on syötetty kortin ollessa paikoilleen asetettuna (mihin hyvänsä korttiaukkoon):

— päivämäärä ja aika, jolloin tieto syötettiin,

— erityisolosuhteiden tyyppi.

302) Kuljettajakortin on kyettävä tallentamaan vähintään 56 tällaista tietuetta.

4.5.3.2.15 Käytössä olleiden ajoneuvoyksikköjen tiedot

303) Kuljettajakortin on kyettävä tallentamaan seuraavat tiedot, jotka liittyvät eri ajoneuvoyksikköihin, joissa korttia käytettiin:

— ajoneuvoyksikön käyttöajan alun (eli hetki, jolloin kortti asetettiin ensimmäisen kerran paikoilleen ajoneuvoyksikköön käyttöajaksi) päivämäärä ja kellonaika,

— ajoneuvoyksikön valmistaja,

— ajoneuvoyksikön tyyppi,

— ajoneuvoyksikön ohjelmistoversion numero.

304) Kuljettajakortin on kyettävä tallentamaan vähintään 84 tällaista tietuetta.

▼B

4.5.3.2.16 Kolmen tunnin keskeytymätöntä ajoa koskevat paikkatiedot.

305) Kuljettajakortin on voitava tallentaa seuraavat tiedot, jotka liittyvät ajoneuvon sijaintiin, kun kuljettajan keskeytymätön ajoaika saavuttaa yli kolmen tunnin jakson:

— päivämäärä ja aika, jolloin kuljettajan keskeytymätön ajoaika saavuttaa yli kolmen tunnin jakson.

— ajoneuvon sijainti,

— GNSS-laitteiston tarkkuus, päivämäärä ja kellonaika, jolloin sijainti määritettiin.

306) Kuljettajakortin on kyettävä tallentamaan vähintään 252 tällaista tietuetta.

4.5.4 *Korjaamokortti*

4.5.4.1 Ajopiirturikortin sovellus (joka on ensimmäisen ja toisen sukupolven ajoneuvoyksikköjen käytettävissä)

4.5.4.1.1 Sovellusten tunnistetiedot

307) Korjaamokortin on kyettävä tallentamaan seuraavat sovellusten tunnistetiedot:

— ajopiirturisovelluksen tunniste,

— ajopiirturikortin tunnisteen tyyppi.

4.5.4.1.2 Avaimet ja varmenteet

308) Korjaamokortin on kyettävä tallentamaan useita salausavaimia ja varmenteita, kuten lisäyksen 11 A osassa määritetään.

309) Korjaamokortin on kyettävä tallentamaan henkilökohtainen tunnusluku (PIN-koodi).

4.5.4.1.3 Kortin tunniste

310) Korjaamokortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:

— kortin numero,

— kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,

— kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä.

4.5.4.1.4 Kortin haltijan tunnistetiedot

311) Korjaamokortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:

— korjaamon nimi,

— korjaamon osoite,

— haltijan sukunimi,

— haltijan etunimi (etunimet),

— haltijan ensisijaisesti käyttämä kieli.

4.5.4.1.5 Kortilla olevien tietojen kopiointi

312) Korjaamokortin on kyettävä tallentamaan kortin tietojen kopiointiin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

▼B

4.5.4.1.6 Kalibrointiin ja ajan asetukseen liittyvät tiedot

313) Korjaamokortin on kyettävä tallentamaan tiedot, jotka liittyvät kalibrointeihin ja/tai ajan asetuksiin, jotka on suoritettu kortin ollessa asetettuna valvontalaitteeseen.

314) Kunkin kalibrointiin liittyvän tietueen on kyettävä tallentamaan seuraavat tiedot:

— kalibroinnin tarkoitus (aktivointi, ensiasennus, asennus, määräaikaistarkastus)

— ajoneuvon tunnistetiedot

— päivitetyt tai vahvistetut parametrit (w, k, l, rengaskoko, nopeudenrajoittimen asetukset, matkamittari (uudet ja vanhat lukemat), päivämäärä ja aika (uudet ja vanhat lukemat))

— valvontalaitteen tunnistetiedot (ajoneuvoyksikön osanumero, ajoneuvoyksikön sarjanumero, liiketunnistimen sarjanumero).

315) Korjaamokortin on kyettävä tallentamaan vähintään 88 tällaista tietuetta.

316) Korjaamokortin on pidettävä muistissa sen avulla suoritettujen kalibrointien kokonaislukumäärä.

317) Korjaamokortin on pidettävä muistissa sen avulla suoritettujen kalibrointien lukumäärä kortin tietojen viimeksi tapahtuneen kopioinnin jälkeen.

4.5.4.1.7 Tapahtumiin ja vikoihin liittyvät tiedot

318) Korjaamokortin on kyettävä tallentamaan tapahtumiin ja vikoihin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

319) Korjaamokortin on kyettävä tallentamaan tiedot, jotka koskevat kolmea viimeisintä kutakin tapahtumatyyppiä edustavaa tapahtumaa (eli 18 tapahtumaa) ja kuutta viimeisintä kutakin vikatyyppiä edustavaa vikatapahtumaa (eli 12 vikatapahtumaa).

4.5.4.1.8 Kuljettajan toimintaan liittyvät tiedot

320) Korjaamokortin on kyettävä tallentamaan kuljettajan toimintaan liittyvät tiedot samalla tavoin kuin kuljettajakortin.

321) Korjaamokortin on kyettävä tallentamaan vähintään yhden kuljettajan keskimääräistä toimintaa vastaavan päivän tiedot.

4.5.4.1.9 Käytössä olleisiin ajoneuvoihin liittyvät tiedot

322) Korjaamokortin on kyettävä tallentamaan käytössä olleisiin ajoneuvoihin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

323) Korjaamokortin on kyettävä tallentamaan vähintään neljä tällaista tietuetta.

4.5.4.1.10 Päivän työajan alkamiseen ja/tai päättymiseen liittyvät tiedot

324) Korjaamokortin on kyettävä tallentamaan päivän työajan alkamiseen ja/tai päättymiseen liittyvät tiedot samalla tavoin kuin kuljettajakortin.

325) Korjaamokortin on kyettävä tallentamaan vähintään kolme paria tällaisia tietueita.

▼B

4.5.4.1.11 Kortin käyttöjaksoon liittyvät tiedot

326) Korjaamokortin on kyettävä tallentamaan kortin tietojen kopiointiin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

4.5.4.1.12 Tarkastustoimiin liittyvät tiedot

327) Korjaamokortin on kyettävä tallentamaan tarkastustoimiin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

4.5.4.1.13 Erityisolosuhteisiin liittyvät tiedot

328) Korjaamokortin on kyettävä tallentamaan erityisolosuhteisiin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

329) Korjaamokortin on kyettävä tallentamaan vähintään 2 tällaista tietuetta.

4.5.4.2 Ajopiirturin sukupolven 2 sovellus (ei voida käyttää ensimmäisen sukupolven ajoneuvoyksikössä)

4.5.4.2.1 Sovellusten tunnistetiedot

330) Korjaamokortin on kyettävä tallentamaan seuraavat sovellusten tunnistetiedot:

— ajopiirturisovelluksen tunniste,

— ajopiirturikortin tunnisteen tyyppi.

4.5.4.2.2 Avaimet ja varmenteet

331) Korjaamokortin on kyettävä tallentamaan useita salausavaimia ja varmenteita, kuten lisäyksessä 11 olevassa B osassa määritetään.

332) Korjaamokortin on kyettävä tallentamaan henkilökohtainen tunnusluku (PIN-koodi).

4.5.4.2.3 Kortin tunniste

333) Korjaamokortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:

— kortin numero,

— kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,

— kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä.

4.5.4.2.4 Kortin haltijan tunnistetiedot

334) Korjaamokortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:

— korjaamon nimi,

— korjaamon osoite,

— haltijan sukunimi,

— haltijan etunimi (etunimet),

— haltijan ensisijaisesti käyttämä kieli.

4.5.4.2.5 Kortilla olevien tietojen kopiointi

335) Korjaamokortin on kyettävä tallentamaan kortin tietojen kopiointiin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

▼B

4.5.4.2.6 Kalibrointiin ja ajan asetukseen liittyvät tiedot

336) Korjaamokortin on kyettävä tallentamaan tiedot, jotka liittyvät kalibrointeihin ja/tai ajan asetuksiin, jotka on suoritettu kortin ollessa asetettuna valvontalaitteeseen.

337) Kunkin kalibrointiin liittyvän tietueen on kyettävä tallentamaan seuraavat tiedot:

— kalibroinnin tarkoitus (aktivointi, ensiasennus, asennus, määräaikaistarkastus)

— ajoneuvon tunnistetiedot,

— päivitetyt tai vahvistetut parametrit (w, k, l, rengaskoko, nopeudenrajoittimen asetukset, matkamittari (uudet ja vanhat lukemat), päivämäärä ja aika (uudet ja vanhat lukemat)),

— valvontalaitteen tunnistetiedot (ajoneuvoyksikön osanumero, ajoneuvoyksikön sarjanumero, liiketunnistimen sarjanumero, etäviestintälaitteiston sarjanumero ja ulkoisen GNSS-laitteiston sarjanumero tarvittaessa),

— kaikkien käytössä olevien sinetöintien tyypit ja tunnisteet,

— ajoneuvoyksikön kyky käyttää ensimmäisen sukupolven ajopiirturikortteja (käytössä tai ei).

338) Korjaamokortin on kyettävä tallentamaan vähintään 88 tällaista tietuetta.

339) Korjaamokortin on pidettävä muistissa sen avulla suoritettujen kalibrointien kokonaislukumäärä.

340) Korjaamokortin on pidettävä muistissa sen avulla suoritettujen kalibrointien lukumäärä kortin tietojen viimeksi tapahtuneen kopioinnin jälkeen.

4.5.4.2.7 Tapahtumiin ja vikoihin liittyvät tiedot

341) Korjaamokortin on kyettävä tallentamaan tapahtumiin ja vikoihin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

342) Korjaamokortin on kyettävä tallentamaan tiedot, jotka koskevat kolmea viimeisintä kutakin tapahtumatyyppiä edustavaa tapahtumaa (eli 33 tapahtumaa) ja kuutta viimeisintä kutakin vikatyyppiä edustavaa vikatapahtumaa (eli 12 vikatapahtumaa).

4.5.4.2.8 Kuljettajan toimintaan liittyvät tiedot

343) Korjaamokortin on kyettävä tallentamaan kuljettajan toimintaan liittyvät tiedot samalla tavoin kuin kuljettajakortin.

344) Korjaamokortin on kyettävä tallentamaan vähintään yhden kuljettajan keskimääräistä toimintaa vastaavan päivän tiedot.

4.5.4.2.9 Käytössä olleisiin ajoneuvoihin liittyvät tiedot

345) Korjaamokortin on kyettävä tallentamaan käytössä olleisiin ajoneuvoihin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

346) Korjaamokortin on kyettävä tallentamaan vähintään neljä tällaista tietuetta.

▼B

4.5.4.2.10 Päivän työajan alkamiseen ja/tai päättymiseen liittyvät tiedot

347) Korjaamokortin on kyettävä tallentamaan päivän työajan alkamiseen ja/tai päättymiseen liittyvät tiedot samalla tavoin kuin kuljettajakortin.

348) Korjaamokortin on kyettävä tallentamaan vähintään kolme paria tällaisia tietueita.

4.5.4.2.11 Kortin käyttöjaksoon liittyvät tiedot

349) Korjaamokortin on kyettävä tallentamaan kortin tietojen kopiointiin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

4.5.4.2.12 Tarkastustoimiin liittyvät tiedot

350) Korjaamokortin on kyettävä tallentamaan tarkastustoimiin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

4.5.4.2.13 Käytössä olleiden ajoneuvoyksikköjen tiedot

351) Korjaamokortin on kyettävä tallentamaan seuraavat tiedot, jotka liittyvät eri ajoneuvoyksikköihin, joissa korttia käytettiin:

— ajoneuvoyksikön käyttöajan alun (eli hetki, jolloin kortti asetettiin ensimmäisen kerran paikoilleen ajoneuvoyksikköön käyttöajaksi) päivämäärä ja kellonaika,

— ajoneuvoyksikön valmistaja,

— ajoneuvoyksikön tyyppi,

— ajoneuvoyksikön ohjelmistoversion numero.

352) Korjaamokortin on kyettävä tallentamaan vähintään neljä tällaista tietuetta.

4.5.4.2.14 Kolmen tunnin keskeytymätöntä ajoa koskevat paikkatiedot.

353) Korjaamokortin on voitava tallentaa seuraavat tiedot, jotka liittyvät ajoneuvon sijaintiin, kun kuljettajan keskeytymätön ajoaika saavuttaa yli kolmen tunnin jakson:

— päivämäärä ja aika, jolloin kuljettajan keskeytymätön ajoaika saavuttaa yli kolmen tunnin jakson,

— ajoneuvon sijainti,

— GNSS-laitteiston tarkkuus, päivämäärä ja kellonaika, jolloin sijainti määritettiin.

354) Korjaamokortin on kyettävä tallentamaan vähintään 18 tällaista tietuetta.

4.5.4.2.15 Erityisolosuhteisiin liittyvät tiedot

355) Korjaamokortin on kyettävä tallentamaan erityisolosuhteisiin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

356) Korjaamokortin on kyettävä tallentamaan vähintään 2 tällaista tietuetta.

▼B

4.5.5 *Valvontakortti*

4.5.5.1 Ajopiirturikortin sovellus (joka on ensimmäisen ja toisen sukupolven ajoneuvoyksikköjen käytettävissä)

4.5.5.1.1 Sovellusten tunnistetiedot

357) Valvontakortin on kyettävä tallentamaan seuraavat sovellusten tunnistetiedot:

— ajopiirturisovelluksen tunniste,

— ajopiirturikortin tunnisteen tyyppi.

4.5.5.1.2 Avaimet ja varmenteet

358) Valvontakortin on kyettävä tallentamaan useita salausavaimia ja varmenteita, kuten lisäyksessä 11 olevassa A osassa määritetään.

4.5.5.1.3 Kortin tunniste

359) Valvontakortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:

— kortin numero,

— kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,

— kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä (jos sellainen on).

4.5.5.1.4 Kortin haltijan tunnistetiedot

360) Valvontakortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:

— tarkastuselimen nimi,

— tarkastuselimen osoite,

— haltijan sukunimi,

— haltijan etunimi (etunimet),

— haltijan ensisijaisesti käyttämä kieli.

4.5.5.1.5 Tarkastustoimiin liittyvät tiedot

361) Valvontakortin on kyettävä tallentamaan seuraavat tarkastustoimiin liittyvät tiedot:

— tarkastuksen päivämäärä ja aika,

— tarkastuksen tyyppi (tietojen näyttö ja/tai tulostus ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi ja/tai kalibroinnin tarkastus tien varrella),

— jakso, jota koskevat tiedot kopioitiin (jos niitä kopioitiin),

— tarkastettavan ajoneuvon rekisteritunnus ja jäsenvaltion viranomainen, joka on rekisteröinyt tarkastettavan ajoneuvon,

— tarkastettavan kuljettajakortin numero ja kortin myöntänyt jäsenvaltio.

362) Valvontakortin on kyettävä tallentamaan vähintään 230 tällaista tietuetta.

▼B

4.5.5.2 Ajopiirturin sukupolven 2 sovellus (ei voida käyttää ensimmäisen sukupolven ajoneuvoyksikössä)

4.5.5.2.1 Sovellusten tunnistetiedot

363) Valvontakortin on kyettävä tallentamaan seuraavat sovellusten tunnistetiedot:

— ajopiirturisovelluksen tunniste,

— ajopiirturikortin tunnisteen tyyppi.

4.5.5.2.2 Avaimet ja varmenteet

364) Valvontakortin on kyettävä tallentamaan useita salausavaimia ja varmenteita, kuten lisäyksessä 11 olevassa B osassa määritetään.

4.5.5.2.3 Kortin tunniste

365) Valvontakortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:

— kortin numero,

— kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,

— kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä (jos sellainen on).

4.5.5.2.4 Kortin haltijan tunnistetiedot

366) Valvontakortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:

— tarkastuselimen nimi,

— tarkastuselimen osoite,

— haltijan sukunimi,

— haltijan etunimi (etunimet),

— haltijan ensisijaisesti käyttämä kieli.

4.5.5.2.5 Tarkastustoimiin liittyvät tiedot

367) Valvontakortin on kyettävä tallentamaan seuraavat tarkastustoimiin liittyvät tiedot:

— tarkastuksen päivämäärä ja aika,

— tarkastuksen tyyppi (tietojen näyttö ja/tai tulostus ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi ja/tai kalibroinnin tarkastus tien varrella).

— jakso, jota koskevat tiedot kopioitiin (jos niitä kopioitiin),

— tarkastettavan ajoneuvon rekisteritunnus ja jäsenvaltion viranomainen, joka on rekisteröinyt tarkastettavan ajoneuvon,

— tarkastettavan kuljettajakortin numero ja kortin myöntänyt jäsenvaltio.

368) Valvontakortin on kyettävä tallentamaan vähintään 230 tällaista tietuetta.

▼B

4.5.6 *Yrityskortti*

4.5.6.1 Ajopiirturikortin sovellus (joka on ensimmäisen ja toisen sukupolven ajoneuvoyksikköjen käytettävissä)

4.5.6.1.1 Sovellusten tunnistetiedot

369) Yrityskortin on kyettävä tallentamaan seuraavat sovellusten tunnistetiedot:

— ajopiirturisovelluksen tunniste,

— ajopiirturikortin tunnisteen tyyppi.

4.5.6.1.2 Avaimet ja varmenteet

370) Yrityskortin on kyettävä tallentamaan useita salausavaimia ja varmenteita, kuten lisäyksen 11 A osassa määritetään.

4.5.6.1.3 Kortin tunniste

371) Yrityskortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:

— kortin numero,

— kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,

— kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä (jos sellainen on).

4.5.6.1.4 Kortin haltijan tunnistetiedot

372) Yrityskortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:

— yrityksen nimi,

— yrityksen osoite.

4.5.6.1.5 Yrityksen toimenpiteitä koskevat tiedot

373) Yrityskortin on kyettävä tallentamaan seuraavat yrityksen toimenpiteitä koskevat tiedot:

— päivämäärä ja aika, jolloin toimenpide suoritettiin,

— toimenpiteen tyyppi (ajoneuvoyksikön lukitseminen ja/tai lukituksen avaaminen ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi),

— jakso, jota koskevat tiedot kopioitiin (jos niitä kopioitiin),

— kyseisen ajoneuvon rekisteritunnus ja jäsenvaltion viranomainen, joka on rekisteröinyt kyseisen ajoneuvon,

— kortin numero ja kortin myöntänyt jäsenvaltio (jos kortin tietoja kopioitiin).

374) Yrityskortin on kyettävä tallentamaan vähintään 230 tällaista tietuetta.

▼B

4.5.6.2 Ajopiirturin sukupolven 2 sovellus (ei voida käyttää ensimmäisen sukupolven ajoneuvoyksikössä)

4.5.6.2.1 Sovellusten tunnistetiedot

375) Yrityskortin on kyettävä tallentamaan seuraavat sovellusten tunnistetiedot:

— ajopiirturisovelluksen tunniste,

— ajopiirturikortin tunnisteen tyyppi.

4.5.6.2.2 Avaimet ja varmenteet

376) Yrityskortin on kyettävä tallentamaan useita salausavaimia ja varmenteita, kuten lisäyksessä 11 olevassa B osassa määritetään.

4.5.6.2.3 Kortin tunniste

377) Yrityskortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:

— kortin numero,

— kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,

— kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä (jos sellainen on).

4.5.6.2.4 Kortin haltijan tunnistetiedot

378) Yrityskortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:

— yrityksen nimi,

— yrityksen osoite.

4.5.6.2.5 Yrityksen toimenpiteitä koskevat tiedot

379) Yrityskortin on kyettävä tallentamaan seuraavat yrityksen toimenpiteitä koskevat tiedot:

— päivämäärä ja aika, jolloin toimenpide suoritettiin,

— toimenpiteen tyyppi (ajoneuvoyksikön lukitseminen ja/tai lukituksen avaaminen ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi),

— jakso, jota koskevat tiedot kopioitiin (jos niitä kopioitiin),

— kyseisen ajoneuvon rekisteritunnus ja jäsenvaltion viranomainen, joka on rekisteröinyt kyseisen ajoneuvon,

— kortin numero ja kortin myöntänyt jäsenvaltio (jos kortin tietoja kopioitiin).

380) Yrityskortin on kyettävä tallentamaan vähintään 230 tällaista tietuetta.

5. VALVONTALAITTEEN ASENNUS

5.1 **Asennus**

381) Uudet valvontalaitteet on toimitettava asentajille tai ajoneuvovalmistajille aktivoimattomana ja siten, että kaikille 3.21 kohdassa luetelluille kalibrointiparametreille on asetettu asianmukaiset ja käyvät oletusarvot. Tapauksissa, joissa mikään oletusarvo ei ole asianmukainen, kirjaimin ilmaistavien parametrien arvo on asetettava kysymysmerkeistä muodostuviksi merkkijonoiksi ja numeeristen parametrien arvo nollaksi. Valvontalaitteen turvatekniikan kannalta merkityksellisten osien toimittamista voidaan rajoittaa, jos tätä edellytetään turvavarmennuksen aikana.

▼B

382) Valvontalaite on ennen sen aktivointia pystyttävä kalibroimaan, vaikka laite ei olisikaan kalibrointitilassa.

383) Valvontalaite ei saa ennen aktivoimistaan kirjata tai tallentaa tietoja, jotka on kuvattu 3.12.3, 3.12.9 ja 3.12.12–3.12.15 kohdassa (mainitut kohdat mukaan lukien).

384) Asennuksen aikana ajoneuvovalmistajien on asetettava valmiiksi kaikki tiedossa olevat parametrit.

385) Ajoneuvovalmistajien tai asentajien on aktivoitava asennettu valvontalaite viimeistään ennen kuin ajoneuvoa käytetään asetuksen (EY) N:o 561/2006 soveltamisalaan kuuluvalla tavalla.

386) Valvontalaitteen aktivoinnin on käynnistyttävä automaattisesti, kun sen jompaankumpaan korttiliitäntälaitteeseen ensimmäisen kerran asetetaan voimassa oleva korjaamokortti.

387) Mikäli liiketunnistimen ja ajoneuvoyksikön toisiinsa liittäminen vaatii erityisiä toimintoja, niiden on tapahduttava automaattisesti ennen aktivointia tai sen aikana.

388) Samalla tavoin, ulkoisen GNSS-laitteiston ja ajoneuvoyksikön toisiinsa kytkemisen on tapahduttava automaattisesti ennen aktivointia tai sen aikana.

389) Aktivoinnin tapahduttua valvontalaitteen toimintojen ja tietojen käyttöoikeuksien on oltava täysin käytettävissä.

390) Sen aktivoinnin jälkeen valvontalaitteen on lähetettävä etäviestintälaitteistoon suojatut tarvittavat tiedot kohdistettuja tienvarsitarkastuksia varten.

391) Valvontalaitteen tietojen kirjaamis- ja tallennustoimintojen on laitteen aktivoinnin jälkeen oltava täysin toimintakuntoiset.

392) Asennuksen jälkeen laite on kalibroitava. Ajoneuvon rekisteritunnusta ei välttämättä syötetä ensimmäisen kalibroinnin yhteydessä, jos kalibroinnin suorittava hyväksytty korjaamo ei tiedä sitä. Näissä olosuhteissa ajoneuvon omistajan on oltava mahdollista, ja vain tällöin, syöttää ajoneuvon rekisteritunnus käyttäen yrityskorttiaan ennen ajoneuvon käyttämistä asetuksen (EY) N:o 561/2006 soveltamisalaan kuuluvalla tavalla (esim. käyttämällä komentoja ajoneuvoyksikön käyttöliittymän asianmukaisen valikkorakenteen kautta.) ([1]). Näiden tietojen päivitys tai vahvistus saa olla mahdollista vain korjaamokortin avulla.

393) Ulkoisen GNSS-laitteiston asennus edellyttää sen kytkemistä ajoneuvoyksikköön ja sen jälkeen GNSS-sijaintitietojen tarkastusta.

394) Valvontalaite on sijoitettava ajoneuvoon siten, että kuljettaja kykenee käyttämään tarvittavia toimintoja istuimeltaan käsin.

([1]) EUVL L 102, 11.4.2006, s. 1.

▼B

5.2 **Asennuskilpi**

395) Sen jälkeen, kun valvontalaite on tarkastettu asennuksen yhteydessä, siihen on kiinnitettävä helppopääsyiseen paikkaan selvästi näkyvä kaiverrettu tai pysyvästi painettu asennuskilpi. Tilanteissa, joissa tämä ei ole mahdollista, kilpi on kiinnitettävä ajoneuvon B-pilariin niin, että se näkyy selvästi. Ajoneuvoissa, joissa ei ole B-pilaria, asennuskilpi on kiinnitettävä ajoneuvon kuljettajanpuoleiseen oven kehykseen, ja sen on oltava selvästi näkyvä kaikissa tapauksissa.

Aina kun hyväksytty asentaja tai korjaamo on suorittanut tarkastuksen, edellisen kilven tilalle on kiinnitettävä uusi kilpi.

396) Kilvestä on käytävä ilmi ainakin seuraavat tiedot:

— hyväksytyn asentajan tai korjaamon nimi, osoite tai tavaramerkki,

— ajoneuvon ominaiskerroin muodossa ”w = … imp/km”,

— valvontalaitteen vakio muodossa ”k = … imp/km”,

— pyörien renkaiden tehollinen ympärysmitta muodossa ”l = … mm”,

— rengaskoko,

— päivämäärä, jolloin ajoneuvon ominaiskerroin ja pyörien renkaiden tehollinen ympärysmitta on mitattu,

— ajoneuvon valmistenumero,

— se, onko käytössä ulkoista GNSS-laitteistoa,

— ulkoisen GNSS-laitteiston sarjanumero,

— etäviestintälaitteen sarjanumero,

— kaikkien käytössä olevien sinetöintien sarjanumerot,

— ajoneuvon osa, johon muunnin on asennettu, jos ajoneuvossa on sellainen,

— ajoneuvon osa, johon liiketunnistin on asennettu, jos sitä ei ole liitetty vaihdelaatikkoon tai ei käytetä muunninta,

— sen kaapelin väri, joka yhdistää muuntimen syöttöimpulsseja tuottavaan ajoneuvon osaan,

— muuntimeen sulautetun liiketunnistimen sarjanumero.

397) Ainoastaan M1- ja N1-luokkien ajoneuvoissa, joihin on asennettu muunnin komission asetuksen (EY) N:o 68/2009 ([1]), sellaisena kuin se on viimeksi muutettuna, mukaisesti ja joihin ei ole mahdollista sisällyttää kaikkea vaatimuksessa 396 kuvattua tarpeellista tietoa, voidaan käyttää toista lisäkilpeä. Tällaisissa tapauksissa lisäkilvessä on oltava vähintään neljä viimeistä vaatimuksen 396 luetelmakohtaa.

([1]) Komission asetus (EY) N:o 68/2009, annettu 23 päivänä tammikuuta 2009, tieliikenteen valvontalaitteista annetun neuvoston asetuksen (ETY) N:o 3821/85 mukauttamisesta tekniikan kehitykseen yhdeksännen kerran (EUVL L 21, 24.1.2009, s. 3).

▼B

Jos tällaista toista lisäkilpeä käytetään, se on kiinnitettävä vaatimuksessa 396 kuvatun ensimmäisen ensisijaisen kilven viereen ja sillä on oltava sama suojaustaso. Lisäksi toisesta kilvestä on käytävä ilmi asennuksen suorittaneen hyväksytyn asentajan tai korjaamon nimi, osoite tai toiminimi sekä asennuspäivämäärä.

5.3 **Sinetöinti**

398) Seuraavat osat on sinetöitävä:

— jokainen liitäntä, joka irrottaessaan aiheuttaisi muutoksia, joita on mahdoton havaita, tai tietojen tuhoutumista, jota on mahdoton havaita (tämä voi koskea esim. liiketunnistimen asentamista vaihdelaatikkoa, M1- ja N1-luokan ajoneuvojen sovitinta, ulkoista GNSS-yhteyttä tai ajoneuvoyksikköä),

— asennuskilpi, jollei sitä ole kiinnitetty siten, että sitä ei voida poistaa tuhoamatta siinä olevia merkintöjä.

399) Edellä mainitut sinetit voidaan poistaa:

— hätätapauksessa,

— nopeudenrajoittimen tai muun liikenneturvallisuutta parantavan laitteen asentamiseksi, säätämiseksi tai korjaamiseksi edellyttäen, että valvontalaitteen toiminta jatkuu luotettavasti ja moitteettomasti ja että hyväksytty asentaja tai korjaamo sinetöi sen uudelleen (6 luvun mukaisesti) välittömästi nopeudenrajoittimen tai muun liikenneturvallisuutta parantavan laitteen asentamisen jälkeen tai seitsemän päivän kuluessa muissa tapauksissa.

400) Aina kun sinetit poistetaan, toimivaltaiselle viranomaiselle on laadittava ja toimitettava kirjallinen ilmoitus, jossa esitetään toimenpiteen syyt.

401) Sineteissä on oltava niiden valmistajan antamat tunnistenumerot. Numero on yksilöllinen ja se eroaa kaikista muista sinetinvalmistajien antamista sinettien numeroista.

Tämä yksilöllinen tunnistenumero määritellään seuraavasti. MMNNNNN ei-irrotettavalla merkinnällä, jossa MM on yksilöllinen valmistajan tunnistusmerkintä (EY:n hallinnoima tietokannan rekisteröinti) ja NNNNN sinetin aakkosnumeerinen merkki, joka yksilöi valmistajan verkkotunnuksen.

402) Sineteissä on oltava vapaa tila, johon hyväksytyt asentajat, korjaamot tai ajoneuvon valmistajat voivat lisätä erityismerkin asetuksen (EU) N:o 165/2014 22 artiklan 3 kohdan mukaisesti.

Tämä merkki ei peitä sinetin tunnistenumeroa.

403) Sinetinvalmistajat on rekisteröitävä erityiseen tietokantaan ja niiden on julkistettava tunnisteina käytettävien sinettien numerot Euroopan komission käyttöönottaman menettelyn mukaisesti.

404) Hyväksyttyjen korjaamojen ja ajoneuvojen valmistajien pitää käyttää asetuksen (EU) N:o 165/2014 mukaisesti ainoastaan sinettejä, jotka ovat peräisin edellä mainitussa tietokannassa luetelluilta valmistajilta.

▼B

405) Sinetinvalmistajien ja niiden jakelijoiden on pidettävä täydellinen jäljitysrekisteri myydyistä sineteistä, joita käytetään asetuksen (EU) N:o 165/2014 mukaisesti ja niiden on voitava toimittaa ne toimivaltaisille kansallisille viranomaisille tarvittaessa.

406) Sinettien yksilölliset tunnistenumerot ovat näkyvissä asennuskilvessä.

6. TARKASTUKSET, MÄÄRÄAIKAISTARKASTUKSET JA KORJAUKSET

Niitä olosuhteita koskevat vaatimukset, joissa sinetit saadaan poistaa ja joihin viitataan asetuksen (EY) N:o 165/2014 22 artiklan 5 kohdassa, on määritelty tämän liitteen 5.3 kohdassa.

6.1 **Asentajien, korjaamoiden ja ajoneuvovalmistajien hyväksyntä**

Jäsenvaltiot hyväksyvät, tarkastavat säännöllisesti ja laillistavat elimet, jotka saavat suorittaa:

— asennuksia,

— tarkistuksia,

— tarkastuksia,

— korjauksia.

Korjaamokortteja myönnetään vain asentajille ja/tai testausasemille, jotka on hyväksytty suorittamaan valvontalaitteen aktivointi ja/tai kalibrointi tämän liitteen mukaisesti ja (paitsi milloin tästä poikkeamiseen on perusteltu syy):

— jotka eivät ole oikeutettuja yrityskorttiin,

— ja joiden muut työtehtävät eivät vaaranna lisäyksessä 10 edellytettyä järjestelmän kokonaistietoturvaa.

6.2 **Uusien tai korjattujen laitteiden tarkastaminen**

407) Jokaisen uuden tai korjatun laitteen moitteeton toiminta ja sen lukemien ja tallennusten tarkkuus suhteessa 3.2.1, 3.2.2, 3.2.3 ja 3.3 kohdassa annettuihin rajoihin on tarkastettava 5.3 kohdan mukaisen sinetöinnin ja kalibroinnin avulla.

6.3 **Asennustarkastus**

408) Ajoneuvoon asentamisen jälkeen koko laitteiston (valvontalaite mukaan lukien) on oltava 3.2.1, 3.2.2, 3.2.3 ja 3.3 kohdassa esitettyjen enimmäisvirherajoihin liittyvien määräysten mukainen.

6.4 **Määräaikaistarkastukset**

409) Ajoneuvoihin asennettujen laitteiden määräaikaistarkastukset on suoritettava laitteiden korjaamisen jälkeen tai ajoneuvon ominaiskertoimen tai pyörän renkaiden tehollisen ympärysmitan muutoksen jälkeen tai silloin, jos laitteen UTC-aika poikkeaa oikeasta enemmän kuin 20 minuuttia tai kun ajoneuvon rekisteritunnus on muuttunut, tai vähintään kerran kahden vuoden (24 kuukauden) kuluessa edellisestä tarkastuksesta.

410) Näissä tarkastuksissa on tarkastettava ainakin:

— että valvontalaite, mukaan lukien tiedon säilytys ajopiirturikortilla ja yhteys etäviestintälukijoihin, toimii moitteettomasti,

▼B

— että 3.2.1 ja 3.2.2 kohdassa esitettyjä enimmäisvirherajoihin liittyviä määräyksiä noudatetaan,

— että 3.2.3 ja 3.3 kohdassa esitettyjä määräyksiä noudatetaan,

— että valvontalaitteessa on tyyppihyväksyntämerkintä,

— että vaatimuksessa 396 määritelty asennuskilpi ja vaatimuksessa 225 määritelty tunnistekilpi ovat kiinnitettyinä,

— rengaskoko ja pyörien renkaiden todellinen ympärysmitta,

— että laitteeseen ei ole kytketty käsittelylaitteita,

— että sinetit on asennettu oikein, ne ovat hyvässä tilassa, että niiden tunnistenumerot ovat voimassa (yksilöity sinetinvalmistaja EU:n tietokannassa) ja että niiden tunnistenumerot vastaavat asennuskilven merkintöjä (ks. vaatimus 401).

411) Jos jonkin 3.9 kohdassa (Tapahtumien ja/tai vikojen havaitseminen) mainitun tapahtuman todetaan ilmenneen viimeisen tarkastuksen jälkeen ja ajopiirturin valmistajat ja/tai kansalliset viranomaiset katsovat sen mahdollisesti vaarantavan laitteen turvallisuuden, korjaamon on:

a. verrattava vaihdelaatikkoon sijoitetun liiketunnistimen tunnistetietoja ajoneuvoyksikköön liitetyn liiketunnistimen tunnistetietoihin,

b. tarkistettava, vastaavatko asennuskilven tiedot ajoneuvoyksikköön tallennettuja tietoja,

c. tarkistettava, vastaavatko liiketunnistimen sarjanumero ja hyväksyntänumero, jos ne ovat liiketunnistimen kyljessä, valvontalaitteen datamuistiin tallennettuja tietoja,

d. vertailtava ulkoisen GNSS-laitteiston tunnistekilpeen merkittyjä tunnistetietoja, jos niitä on, ajoneuvoyksikön datamuistiin tallennettuihin tietoihin.

412) Korjaamojen on kirjattava tarkastusraportteihinsa kaikki havainnot murretuista sineteistä tai käsittelylaitteista. Korjaamojen on säilytettävä näitä raportteja vähintään kahden vuoden ajan ja annettava ne pyydettäessä toimivaltaisen viranomaisen käyttöön.

413) Näihin tarkastuksiin on sisällyttävä kalibrointi ja sellaisten sinettien ennaltaehkäisevä korvaaminen, joiden asentaminen on korjaamojen vastuulla.

6.5 **Virheiden mittaus**

414) Virheiden mittaaminen asennuksen yhteydessä tai käytön aikana on suoritettava seuraavissa olosuhteissa, joiden on katsottava olevan standardinmukaiset testausolosuhteet:

— ajoneuvo kuormaamattomana, tavanomaisessa ajokunnossa,

— rengaspaine valmistajan ohjeiden mukainen,

▼B

— renkaiden kuluminen kansallisen lainsäädännön sallimissa rajoissa,

— ajoneuvon liikkuminen:

— ajoneuvon on kuljettava oman moottorinsa teholla suoraan tasaisella alustalla nopeudella 50 ± 5 km/t, mittausmatkan on oltava ainakin 1 000 m,

— testaus voidaan suorittaa myös muilla menetelmillä, kuten tarkoitukseen soveltuvassa testipenkissä, edellyttäen, että siten saavutetaan vastaava tarkkuus.

6.6 **Korjaukset**

415) Testausasemien on kyettävä kopioimaan tietoja valvontalaitteesta tarkoituksenaan toimittaa tiedot takaisin kuljetusyhtiölle.

416) Hyväksyttyjen testausasemien on annettava kuljetusyhtiöille todistus tietojen kopioinnin mahdottomuudesta tapauksissa, joissa valvontalaite ei salli aiemmin tallennettujen tietojen kopioimista tällaisen testausaseman suorittaman korjauksen jälkeenkään. Tällaiset korjaamot säilyttävät jäljennöksen antamistaan todistuksista vähintään kahden vuoden ajan.

7. KORTTIEN MYÖNTÄMINEN

Jäsenvaltioiden käyttöön ottamien korttien myöntämiseen liittyvien menettelyjen on oltava seuraavien säännösten mukaisia:

417) Ensimmäisen hakijalle myönnetyn ajopiirturikortin haltijakohtaisen sarjanumeron (jos sellainen on), korvausnumeron ja uusintanumeron on oltava asetettu nollaksi (0).

418) Kaikkien tietylle valvontaelimelle tai tietylle korjaamolle tai tietylle kuljetusyhtiölle myönnettyjen muiden kuin henkilökohtaisten ajopiirturikorttien numeroissa on oltava samat 13 ensimmäistä merkkiä ja niillä on oltava eri järjestysnumero.

419) Entisen ajopiirturikortin tilalle annetulla ajopiirturikortilla on oltava sama numero kuin kortilla, jonka se korvaa, lukuun ottamatta korvausnumeroa, jota suurennetaan yhdellä (järjestyksessä 0, …, 9, A, …, Z).

420) Entisen ajopiirturikortin tilalle annetulla ajopiirturikortilla on oltava sama viimeinen voimassaolopäivä kuin kortilla, jonka se korvaa.

421) Uusittavan ajopiirturikortin tilalle annetulla ajopiirturikortilla on oltava sama numero kuin kortilla, jonka se korvaa, lukuun ottamatta korvausnumeroa, joka on asetettava nollaksi (0), ja uusintanumeroa, jota suurennetaan yhdellä (järjestyksessä 0, …, 9, A, …, Z).

422) Ajopiirturikortin vaihtamisessa hallinnollisten tietojen muuttamiseksi noudatetaan kortin uusimista koskevia sääntöjä, jos vaihtaminen tapahtuu samassa jäsenvaltiossa, ja kortin ensi kertaa myöntämistä koskevia sääntöjä, jos vaihtaminen tapahtuu jossakin muussa jäsenvaltiossa.

423) Kortin haltijan sukunimi muille kuin henkilökohtaisille korjaamo- tai valvontakorteille täytetään korjaamon tai valvontaelimen nimellä tai asentajan tai valvontaviranomaisen nimelle, jos jäsenvaltiot näin päättävät.

▼B

424) Jäsenvaltioiden on vaihdettava tietoja sähköisesti, jotta varmistetaan, että niiden myöntämät kuljettajakortit ovat ainutkertaisia asetuksen (EU) N:o 165/2014 31 artiklan mukaisesti.

8. VALVONTALAITTEIDEN JA AJOPIIRTURIKORTTIEN TYYPPIHYVÄKSYNTÄ

8.1 **Yleistä**

Tässä luvussa valvontalaitteella tarkoitetaan valvontalaitetta tai sen osia. Mitään tyyppihyväksyntää ei vaadita kaapeleille, jotka yhdistävät liiketunnistimen ajoneuvoyksikköön, ulkoisen GNSS-laitteiston ajoneuvoyksikköön tai etäviestintälaitteiston ajoneuvoyksikköön. Valvontalaitteen käyttämä paperi katsotaan valvontalaitteen osaksi.

Valmistajat voivat pyytää valmistamansa osan tyyppihyväksyntää minkä tahansa tyyppisen liiketunnistimen, ulkoisen GNSS-laitteiston kanssa ja toisin päin, edellyttäen, että osat ovat tämän liitteen vaatimuksien mukaisia. Vaihtoehtoisesti valmistajat voivat myös pyytää valvontalaitteen tyyppihyväksyntää.

425) Valvontalaite on tyyppihyväksytettävä täydellisenä kaikkien siihen kiinteästi liitettyjen lisälaitteiden kanssa.

426) Valvontalaitteiden ja ajopiirturikorttien tyyppihyväksyntään on sisällyttävä tietoturvaan liittyviä testejä, toimintaan liittyviä testejä ja yhteentoimivuuteen liittyviä testejä. Kunkin testityypin hyväksytyt tulokset esitetään asianmukaisessa todistuksessa.

427) Jäsenvaltioiden tyyppihyväksyntäviranomaiset eivät myönnä tyyppihyväksyntää, ellei heillä ole käytettävissään:

— tietoturvavarmennetta,

— tietoturvatodistusta,

— toiminnallisuustodistusta

sekä yhteentoimivuustodistusta, jolle tyyppihyväksyntää anotaan.

428) Kaikista laitteiden ohjelmistojen tai varusteiden taikka niiden valmistuksessa käytettävien materiaalien muutoksista on ennen niiden käyttöönottoa ilmoitettava tyyppihyväksynnän myöntäneelle viranomaiselle. Tämän viranomaisen on joko vahvistettava valmistajalle, että tyyppihyväksyntä ulotetaan käsittämään nämä muutokset, tai vaadittava asianomaisten toiminnallisuus-, tietoturva- ja/tai yhteentoimivuustodistusten ajan tasalle saattamista tai vahvistamista.

429) Toimenpiteet, joilla päivitetään käytössä olevien valvontalaitteiden ohjelmistoja, on hyväksytettävä sillä viranomaisella, joka on myöntänyt valvontalaitteen tyyppihyväksynnän. Ohjelmiston päivitys ei saa muuttaa tai pyyhkiä pois mitään valvontalaitteeseen tallennettuja kuljettajan toimintaa koskevia tietoja. Ohjelmistoja voidaan päivittää vain laitteen valmistajan vastuulla.

430) Sellaisia ohjelmistojen muutoksiin liittyviä tyyppihyväksyntöjä, joilla pyritään päivittämään aiemmat tyyppihyväksytyt valvontalaitteet, ei voida evätä, jos tällaisilla muutoksilla pelkästään otetaan käyttöön toimintoja, joita ei määritellä tässä liitteessä. Valvontalaitteen ohjelmiston päivityksessä voidaan sulkea ulkopuolelle uusien merkistöjen käyttöönotto, jos tämä ei ole teknisesti mahdollista.

▼B

8.2 **Tietoturvatodistus**

431) Tietoturvatodistus annetaan tämän liitteen lisäyksen 10 määräysten mukaisesti. Sertifioitavat valvontalaitteen osat ovat ajoneuvoyksikkö, liiketunnistin, ulkoinen GNSS-laitteisto ja ajopiirturikortit.

432) Siinä poikkeuksellisessa tilanteessa, että tietoturvasertifioinnista vastaavat viranomaiset kieltäytyvät sertifioimasta uutta laitetta tietoturvamekanismien vanhentuneisuuden vuoksi, tyyppihyväksynnän myöntämistä on jatkettava tässä erityisessä ja poikkeuksellisessa tilanteessa, kun asetuksen mukaista vaihtoehtoista ratkaisua ei ole.

433) Tällöin kyseisen jäsenvaltion on viipymättä ilmoitettava asiasta Euroopan komissiolle, jonka on kahdentoista kalenterikuukauden kuluessa tyyppihyväksynnän myöntämisestä käynnistettävä menettely, jonka avulla varmistetaan, että tietoturvan taso palautetaan alkuperäiselle tasolleen.

8.3 **Toiminnallisuustodistus**

434) Jokaisen tyyppihyväksyntää hakevan on annettava jäsenvaltion tyyppihyväksyntäviranomaisen käyttöön kaikki aineisto ja asiakirjat, jotka kyseinen viranomainen katsoo tarpeellisiksi.

435) Valmistajien on toimitettava tyyppihyväksyttäviksi ehdotetuista tuotteista asianmukaiset näytteet ja niihin liittyvä dokumentaatio, joita toimintaan liittyvät testit suorittamaan valitut laboratoriot pyytävät, ja tämä on tehtävä yhden kuukauden kuluessa pyynnön esittämisestä. Tästä pyynnöstä mahdollisesti aiheutuvista kustannuksista vastaa pyynnön esittänyt taho. Laboratorioiden on käsiteltävä kaikkia kaupallisesti arkaluonteisia tietoja luottamuksellisina.

436) Toiminnallisuustodistus annetaan valmistajalle vasta, kun vähintään kaikista lisäyksessä 9 määritellyistä testeistä on saatu hyväksyttävä tulos.

437) Toiminnallisuustodistuksen antaa tyyppihyväksyntäviranomainen. Todistukseen on sen saajan nimen ja mallin tunnistetietojen lisäksi sisällyttävä yksityiskohtainen luettelo suoritetuista testeistä ja saaduista tuloksista.

438) Valvontalaitteen osien toimintatodistuksista on käytävä ilmi myös sen sertifiointia varten testattujen muiden tyyppihyväksyttyjen yhteensopivien valvontalaitteen osien tyyppihyväksyntänumerot.

439) Valvontalaitteen osien toimintatodistuksista on käytävä ilmi myös ISO- tai CEN-standardi, jonka perusteella toiminnallinen liitäntä on sertifioitu.

8.4 **Yhteentoimivuustodistus**

440) Yhteentoimivuustestit suoritetaan yhdessä laboratoriossa Euroopan komission valtuuttamana ja vastuulla.

441) Laboratorion on kirjattava valmistajien esittämät yhteentoimivuutta koskevat testauspyynnöt siinä aikajärjestyksessä, kun ne saapuvat.

442) Pyynnöt kirjataan virallisesti vain, jos laboratoriolla on käytettävissään:

— kaikki kyseisten yhteentoimivuustestien suorittamisessa tarvittava aineisto ja asiakirjat,

▼B

— vastaava tietoturvatodistus,

— vastaava toiminnallisuustodistus.

Pyynnön kirjaamispäivämäärä on ilmoitettava valmistajalle.

443) Laboratorio ei saa suorittaa sellaisten valvontalaitteiden tai ajopiirturikorttien yhteentoimivuustestejä, joille ei ole myönnetty tietoturvatodistusta ja toiminnallisuustodistusta, muutoin kuin vaatimuksessa 432 kuvatuissa poikkeuksellisissa tilanteissa.

444) Valmistajan, joka pyytää yhteentoimivuustestien suorittamista, on sitouduttava antamaan laboratorion vastata näistä testeistä sekä kaikesta aineistosta ja asiakirjoista, jotka valmistaja on testien suorittamiseksi antanut laboratorion käyttöön.

445) Yhteentoimivuustestit on suoritettava tämän liitteen lisäyksen 9 mukaisesti kaikkien niiden valvontalaite- tai ajopiirturikorttityyppien kanssa:

— joiden tyyppihyväksyntä on vielä voimassa tai,

— joiden tyyppihyväksyntää on haettu ja joilla on voimassa oleva yhteentoimivuustodistus.

446) Yhteentoimivuustestien on koskettava valvontalaitteiden tai ajopiirturikorttien kaikkia käytössä olevia sukupolvia.

447) Laboratorio antaa valmistajalle yhteentoimivuustodistuksen vasta, kun kaikista yhteentoimivuustesteistä on saatu hyväksyttävät tulokset.

448) Jos yhteentoimivuustestit eivät anna hyväksyttäviä tuloksia yhden tai useamman valvontalaitteen tai ajopiirturikortin osalta, yhteentoimivuustodistusta ei anneta, ennen kuin sitä pyytänyt valmistaja on tehnyt tarvittavat muutokset ja saanut yhteentoimivuustesteissä hyväksyttävät tulokset. Laboratorion on määritettävä ongelman syy tähän yhteentoimivuusongelmaan liittyvien valmistajien avulla ja pyrittävä auttamaan todistusta pyytänyttä valmistajaa teknisen ratkaisun löytämisessä. Kun valmistaja tekee tuotteeseensa muutoksia, hänen itsensä on varmistettava asiaankuuluvilta viranomaisilta, että tietoturva- ja toiminnallisuustodistukset ovat vielä voimassa.

449) Yhteentoimivuustodistus on voimassa kuusi kuukautta. Se peruutetaan tämän ajan kuluttua, ellei valmistaja ole saanut vastaavaa tyyppihyväksyntätodistusta. Valmistaja toimittaa yhteentoimivuustodistuksen sille jäsenvaltion tyyppihyväksyntäviranomaiselle, joka on antanut toiminnallisuustodistuksen.

450) Mitään tekijää, joka saattaa aiheuttaa yhteentoimivuusongelman, ei saa käyttää voiton tavoitteluun tai määräävän aseman hankkimiseen.

8.5 **Tyyppihyväksyntätodistus**

451) Jäsenvaltion tyyppihyväksyntäviranomainen saa antaa tyyppihyväksyntätodistuksen heti, kun sillä on käytettävissään vaadittavat kolme todistusta.

▼B

452) Valvontalaitteen osien tyyppihyväksyntätodistuksista on käytävä ilmi myös kaikkien muiden tyyppihyväksyttyjen yhteensopivien valvontalaitteiden tyyppihyväksyntänumerot.

453) Tyyppihyväksyntäviranomaisen on toimitettava jäljennös tyyppihyväksyntätodistuksesta laboratoriolle, joka vastasi yhteensopivuustesteistä silloin, kun todistus annettiin valmistajalle.

454) Yhteentoimivuustestejä suorittamaan valtuutetun testauslaboratorion on ylläpidettävä julkista WWW-sivustoa, jolla on ajan tasalla pidettävä luettelo valvontalaite- ja ajopiirturikorttimalleista:

— joita koskeva yhteentoimivuuden testauspyyntö on kirjattu,

— jotka ovat saaneet yhteentoimivuustodistuksen (myös väliaikaisen),

— jotka ovat saaneet tyyppihyväksyntätodistuksen.

8.6 **Poikkeusmenettely: ensimmäiset yhteentoimivuustodistukset toisen sukupolven valvontalaitteille ja ajopiirturikorteille**

455) Neljän kuukauden ajan siitä lukien, kun ensimmäiset toisen sukupolven valvontalaitteet ja toisen sukupolven ajopiirturikortit (kuljettaja-, korjaamo-, valvonta- ja yrityskortit) ovat saaneet yhteentoimivuustodistuksen, kaikki annettavat yhteentoimivuustodistukset (ensimmäiset mukaan lukien) ovat väliaikaisia.

456) Jos kaikki nämä tuotteet ovat mainitun ajan kuluttua keskenään yhteentoimivia, kaikki vastaavat yhteentoimivuustodistukset muuttuvat lopullisiksi.

457) Jos tämän ajan kuluessa havaitaan yhteentoimivuusongelmia, yhteentoimivuustesteistä vastaavan laboratorion on määritettävä ongelmien syyt kaikkien asianosaisten valmistajien avulla sekä kehotettava näitä tekemään vaadittavat muutokset.

458) Jos tämän ajan kuluttua vielä esiintyy yhteentoimivuusongelmia, on yhteentoimivuustesteistä vastaavan laboratorion yhteistyössä kaikkien asianosaisten valmistajien ja vastaavat toiminnallisuustodistukset antaneiden tyyppihyväksyntäviranomaisten kanssa määritettävä yhteentoimivuusongelmien syyt ja päätettävä, mitä muutoksia kunkin asianomaisen valmistajan on tehtävä. Teknisten ratkaisujen hakeminen saa kestää enintään kaksi kuukautta, minkä jälkeen, ellei ratkaisua ole löytynyt, komission on yhteentoimivuustesteistä vastaavaa laboratoriota kuultuaan päätettävä, mikä tai mitkä valvontalaitteet ja kortit saavat lopullisen yhteentoimivuustodistuksen ja perusteltava ratkaisunsa.

459) Kaikki yhteentoimivuutta koskevat testauspyynnöt, jotka laboratorio on kirjannut ensimmäistä yhteensopivuustodistusta seuraavan neljän kuukauden ajan päättymisen ja vaatimuksessa 455 mainitun komission päätöksen välisenä aikana, on lykättävä siihen asti, kunnes alkuperäiset yhteentoimivuusongelmat on ratkaistu. Sen jälkeen nämä pyynnöt on käsiteltävä siinä aikajärjestyksessä, jossa ne on kirjattu.

▼B

Lisäys 1

DATAHAKEMISTO

SISÄLLYSLUETTELO

1. JOHDANTO

1.1. Datatyyppien määrittelytapa

1.2. Viitetiedot

2. DATATYYPPIEN MÄÄRITTELYT

2.1. ActivityChangeInfo

2.2. Address

2.3. AESKey

2.4. AES128Key

2.5. AES192Key

2.6. AES256Key

2.7. BCDString

2.8. CalibrationPurpose

2.9. CardActivityDailyRecord

2.10. CardActivityLengthRange

2.11. CardApprovalNumber

2.12. CardCertificate

2.13. CardChipIdentification

2.14. CardConsecutiveIndex

2.15. CardControlActivityDataRecord

2.16. CardCurrentUse

2.17. CardDriverActivity

2.18. CardDrivingLicenceInformation

2.19. CardEventData

2.20. CardEventRecord

2.21. CardFaultData

2.22. CardFaultRecord

2.23. CardIccIdentification

2.24. CardIdentification

2.25. CardMACertificate

2.26. CardNumber

2.27. CardPlaceDailyWorkPeriod

2.28. CardPrivateKey

2.29. CardPublicKey

▼B

2.30. CardRenewalIndex

2.31. CardReplacementIndex

2.32. CardSignCertificate

2.33. CardSlotNumber

2.34. CardSlotsStatus

2.35. CardSlotsStatusRecordArray

2.36. CardStructureVersion

2.37. CardVehicleRecord

2.38. CardVehiclesUsed

2.39. CardVehicleUnitRecord

2.40. CardVehicleUnitsUsed

2.41. Certificate

2.42. CertificateContent

2.43. CertificateHolderAuthorisation

2.44. CertificateRequestID

2.45. CertificationAuthorityKID

2.46. CompanyActivityData

2.47. CompanyActivityType

2.48. CompanyCardApplicationIdentification

2.49. CompanyCardHolderIdentification

2.50. ControlCardApplicationIdentification

2.51. ControlCardControlActivityData

2.52. ControlCardHolderIdentification

2.53. ControlType

2.54. CurrentDateTime

2.55. CurrentDateTimeRecordArray

2.56. DailyPresenceCounter

2.57. Datef

2.58. DateOfDayDownloaded

2.59. DateOfDayDownloadedRecordArray

2.60. Distance

2.61. DriverCardApplicationIdentification

▼B

2.62. DriverCardHolderIdentification

2.63. DSRCSecurityData

2.64. EGFCertificate

2.65. EmbedderIcAssemblerId

2.66. EntryTypeDailyWorkPeriod

2.67. EquipmentType

2.68. EuropeanPublicKey

2.69. EventFaultRecordPurpose

2.70. EventFaultType

2.71. ExtendedSealIdentifier

2.72. ExtendedSerialNumber

2.73. FullCardNumber

2.74. FullCardNumberAndGeneration

2.75. Generation

2.76. GeoCoordinates

2.77. GNSSAccuracy

2.78. GNSSContinuousDriving

2.79. GNSSContinuousDrivingRecord

2.80. GNSSPlaceRecord

2.81. HighResOdometer

2.82. HighResTripDistance

2.83. HolderName

2.84. InternalGNSSReceiver

2.85. K-ConstantOfRecordingEquipment

2.86. KeyIdentifier

2.87. KMWCKey

2.88. Language

2.89. LastCardDownload

2.90. LinkCertificate

2.91. L-TyreCircumference

2.92. MAC

2.93. ManualInputFlag

2.94. ManufacturerCode

2.95. ManufacturerSpecificEventFaultData

2.96. MemberStateCertificate

▼B

2.97. MemberStateCertificateRecordArray

2.98. MemberStatePublicKey

2.99. Name

2.100. NationAlpha

2.101. NationNumeric

2.102. NoOfCalibrationRecords

2.103. NoOfCalibrationsSinceDownload

2.104. NoOfCardPlaceRecords

2.105. NoOfCardVehicleRecords

2.106. NoOfCardVehicleUnitRecords

2.107. NoOfCompanyActivityRecords

2.108. NoOfControlActivityRecords

2.109. NoOfEventsPerType

2.110. NoOfFaultsPerType

2.111. NoOfGNSSCDRecords

2.112. NoOfSpecificConditionRecords

2.113. OdometerShort

2.114. OdometerValueMidnight

2.115. OdometerValueMidnightRecordArray

2.116. OverspeedNumber

2.117. PlaceRecord

2.118. PreviousVehicleInfo

2.119. PublicKey

2.120. RecordType

2.121. RegionAlpha

2.122. RegionNumeric

2.123. RemoteCommunicationModuleSerialNumber

2.124. RSAKeyModulus

2.125. RSAKeyPrivateExponent

2.126. RSAKeyPublicExponent

2.127. RtmData

2.128. SealDataCard

▼B

2.129. SealDataVu

2.130. SealRecord

2.131. SensorApprovalNumber

2.132. SensorExternalGNSSApprovalNumber

2.133. SensorExternalGNSSCoupledRecord

2.134. SensorExternalGNSSIdentification

2.135. SensorExternalGNSSInstallation

2.136. SensorExternalGNSSOSIdentifier

2.137. SensorExternalGNSSSCIdentifier

2.138. SensorGNSSCouplingDate

2.139. SensorGNSSSerialNumber

2.140. SensorIdentification

2.141. SensorInstallation

2.142. SensorInstallationSecData

2.143. SensorOSIdentifier

2.144. SensorPaired

2.145. SensorPairedRecord

2.146. SensorPairingDate

2.147. SensorSCIdentifier

2.148. SensorSerialNumber

2.149. Signature

2.150. SignatureRecordArray

2.151. SimilarEventsNumber

2.152. SpecificConditionRecord

2.153. SpecificConditions

2.154. SpecificConditionType

2.155. Speed

2.156. SpeedAuthorised

2.157. SpeedAverage

2.158. SpeedMax

2.159. TachographPayload

2.160. TachographPayloadEncrypted

▼B

2.161. TDesSessionKey

2.162. TimeReal

2.163. TyreSize

2.164. VehicleIdentificationNumber

2.165. VehicleIdentificationNumberRecordArray

2.166. VehicleRegistrationIdentification

2.167. VehicleRegistrationNumber

2.168. VehicleRegistrationNumberRecordArray

2.169. VuAbility

2.170. VuActivityDailyData

2.171. VuActivityDailyRecordArray

2.172. VuApprovalNumber

2.173. VuCalibrationData

2.174. VuCalibrationRecord

2.175. VuCalibrationRecordArray

2.176. VuCardIWData

2.177. VuCardIWRecord

2.178. VuCardIWRecordArray

2.179. VuCardRecord

2.180. VuCardRecordArray

2.181. VuCertificate

2.182. VuCertificateRecordArray

2.183. VuCompanyLocksData

2.184. VuCompanyLocksRecord

2.185. VuCompanyLocksRecordArray

2.186. VuControlActivityData

2.187. VuControlActivityRecord

2.188. VuControlActivityRecordArray

▼B

2.189. VuDataBlockCounter

2.190. VuDetailedSpeedBlock

2.191. VuDetailedSpeedBlockRecordArray

2.192. VuDetailedSpeedData

2.193. VuDownloadablePeriod

2.194. VuDownloadablePeriodRecordArray

2.195. VuDownloadActivityData

2.196. VuDownloadActivityDataRecordArray

2.197. VuEventData

2.198. VuEventRecord

2.199. VuEventRecordArray

2.200. VuFaultData

2.201. VuFaultRecord

2.202. VuFaultRecordArray

2.203. VuGNSSCDRecord

2.204. VuGNSSCDRecordArray

2.205. VuIdentification

2.206. VuIdentificationRecordArray

2.207. VuITSConsentRecord

2.208. VuITSConsentRecordArray

2.209. VuManufacturerAddress

2.210. VuManufacturerName

2.211. VuManufacturingDate

2.212. VuOverSpeedingControlData

2.213. VuOverSpeedingControlDataRecordArray

2.214. VuOverSpeedingEventData

▼B

2.215. VuOverSpeedingEventRecord

2.216. VuOverSpeedingEventRecordArray

2.217. VuPartNumber

2.218. VuPlaceDailyWorkPeriodData

2.219. VuPlaceDailyWorkPeriodRecord

2.220. VuPlaceDailyWorkPeriodRecordArray

2.221. VuPrivateKey

2.222. VuPublicKey

2.223. VuSerialNumber

2.224. VuSoftInstallationDate

2.225. VuSoftwareIdentification

2.226. VuSoftwareVersion

2.227. VuSpecificConditionData

2.228. VuSpecificConditionRecordArray

2.229. VuTimeAdjustmentData

2.230. VuTimeAdjustmentGNSSRecord

2.231. VuTimeAdjustmentGNSSRecordArray

2.232. VuTimeAdjustmentRecord

2.233. VuTimeAdjustmentRecordArray

2.234. WorkshopCardApplicationIdentification

2.235. WorkshopCardCalibrationData

2.236. WorkshopCardCalibrationRecord

2.237. WorkshopCardHolderIdentification

2.238. WorkshopCardPIN

2.239. W-VehicleCharacteristicConstant

2.240. VuPowerSupplyInterruptionRecord

▼B

2.241. VuPowerSupplyInterruptionRecordArray

2.242. VuSensorExternalGNSSCoupledRecordArray

2.243. VuSensorPairedRecordArray

3. ARVOALUEIDEN MÄÄRITTELYT

4. MERKKIJONOT

5. KOODAUS

6. OLIOTUNNISTEET JA SOVELLUSTUNNISTEET

6.1. Oliotunnisteet

6.2. Sovellustunnisteet

1. JOHDANTO

Tässä lisäyksessä määritellään valvontalaitteissa ja ajopiirturikorteissa käytettävän datan muodot, elementit ja rakenteet.

1.1. **Datatyyppien määrittelytapa**

Tässä lisäyksessä käytetään ASN.1-merkintätavan mukaisia datatyyppien määrittelyjä. Näin erilliset dataelementit ja datarakenteet voidaan määritellä ilman sidonnaisuutta mihinkään datansiirron vaatimaan muotorakenteeseen (koodaussääntöön), jolloin määrittelyt ovat sovelluksesta ja ympäristöstä riippumattomia.

ASN.1-merkintätavan mukaiset datatyypin määrittelyt on tehty ISO/IEC 8824-1 -standardin mukaisesti. Tästä seuraa, että:

— mikäli mahdollista, datatyypille valittu nimi viittaa sen käyttötarkoitukseen,

— milloin datatyyppi on muiden datatyyppien yhdistelmä, sen nimi on silti yhteen kirjoitettu sarja kirjainmerkkejä, joka alkaa isolla kirjaimella, kuitenkin siten, että isoja kirjaimia on käytetty myös nimen keskellä välittämään tietoa nimen osien merkityksestä,

— yleensä datatyyppien nimet liittyvät niiden datatyyppien nimiin, joista ne on rakennettu, niiden laitteiden nimiin, joissa dataa tallennetaan, ja niihin toimintoihin, joihin data liittyy.

Jos ASN.1-datatyyppi on jo määritelty osana jotain muuta standardia, ja sitä käytetään myös valvontalaitteissa, määritellään kyseinen ASN.1-datatyyppi tässä lisäyksessä.

Jotta useiden erilaisten koodaussääntöjen käyttäminen olisi mahdollista, joillakin tämän lisäyksen ASN.1-datatyypeillä on rajoituksia arvoalueiden osalta. Nämä arvoalueiden rajoitukset on määritelty kohdassa 3 ja lisäyksessä 2.

1.2. **Viitetiedot**

Tässä lisäyksessä käytetään seuraavia viitetietoja:

ISO 639	Code for the representation of names of languages. First Edition: 1988.

▼B

ISO 3166	Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, 2013
ISO 3779	Road vehicles – Vehicle identification number (VIN) – Content and structure. 2009
ISO/IEC 7816-5	Identification cards – Integrated circuit cards – Part 5: Registration of application providers. Second edition: 2004.
ISO/IEC 7816-6	Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange, 2004 + Technical Corrigendum 1: 2006
ISO/IEC 8824-1	Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2008 + Technical Corrigendum 1: 2012 and Technical Corrigendum 2: 2014.
ISO/IEC 8825-2	Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). 2008.
ISO/IEC 8859-1	Information technology – 8 bit single-byte coded graphic character sets – Part 1: Latin alphabet No.1. First edition: 1998.
ISO/IEC 8859-7	Information technology – 8 bit single-byte coded graphic character sets – Part 7: Latin/Greek alphabet. 2003.
ISO 16844-3	Road vehicles – Tachograph systems – Motion Sensor Interface. 2004 + Technical Corrigendum 1: 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, version 2.20, 3. February 2015

2. DATATYYPPIEN MÄÄRITTELYT

Kaikkien seuraavien datatyyppien oletusarvoinen dataelementin arvo tapauksissa, joissa arvo on tuntematon tai ei sovellettavissa, saadaan täyttämällä dataelementti tavuilla, joiden arvo on ‘FF’.

Kaikkia datatyyppejä käytetään sukupolven 1 ja sukupolven 2 laitteissa, ellei toisin mainita.

2.1. **ActivityChangeInfo**

Tämän datatyypin avulla voidaan kaksitavuista sanaa käyttäen koodata korttiaukon tilanne klo 00.00 ja/tai kuljettajatilanne klo 00.00 ja/tai toiminnan muutoksia ja/tai ajoneuvon miehityksen muutoksia ja/tai kuljettajan tai apukuljettajan kortin tilan muutoksia. Tämä datatyyppi liittyy liitteen 1 C vaatimuksiin 105, 266, 291, 320, 321, 343 ja 344.

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

Asetettava arvo — Octet Aligned (tavuittain ryhmitelty): ‘scpaatttttttttt’B (16 bittiä)

Datamuistin tallenteille (tai korttiaukon tilanteelle):

‘s’B	Korttiaukko: ‘0’B: DRIVER (kuljettaja), ‘1’B: CO-DRIVER (apukuljettaja),

▼B

‘c’B	Ajoneuvon miehitys:
	‘0’B: SINGLE (yksin),
	‘1’B: CREW (miehistö),
‘p’B	Kuljettajakortin (tai korjaamokortin) tila kyseisessä korttiaukossa:
	‘0’B: INSERTED (kortti on asetettuna aukkoon),
	‘1’B: NOT INSERTED (korttia ei ole asetettu aukkoon (tai se on poistettu),
‘aa’B	Toiminta:
	‘00’B: BREAK/REST (tauko/lepo),
	‘01’B: AVAILABILITY (varallaolo)
	‘10’B: WORK (työ),
	‘11’B: DRIVING (ajo),
‘ttttttttttt’B	Muutoksen aika: minuutteina klo 00.00 lukien kyseisenä päivänä.

Kuljettajakortin (tai korjaamokortin) tallenteille (ja kuljettajatilanteelle):

‘s’B	Korttiaukko (ei oleellinen, kun ‘p’ = 1, paitsi alla olevan huomautuksen tapauksessa):
	‘0’B: DRIVER (kuljettaja),
	‘1’B: CO-DRIVER (apukuljettaja),
‘c’B	Ajoneuvon miehitys (tapaus ‘p’=0) tai
	seuraava toiminnan tila (tapaus ‘p’=1):
	‘0’B: SINGLE (yksin),
	‘0’B: UNKNOWN (tuntematon)
	‘1’B: CREW (miehistö),
	‘1’B: KNOWN (= käsin syötetty)
‘p’B	Kortin tila:
	‘0’B: INSERTED, (kortti on asetettuna valvontalaitteeseen),
	‘1’B: NOT INSERTED, (korttia ei ole asetettu laitteeseen (tai se on postettu)),
‘aa’B	Toiminta (ei oleellinen, kun ‘p’ = 1, paitsi alla olevan huomautuksen tapauksessa):
	‘00’B: BREAK/REST (tauko/lepo),
	‘01’B: AVAILABILITY (varallaolo)
	‘10’B: WORK (työ),
	‘11’B: DRIVING (ajo),
‘ttttttttttt’B	Muutoksen aika: minuutteina klo 00.00 lukien kyseisenä päivänä.

▼B

Huomautus, joka koskee tapausta ”kortin poistaminen”:

Kun kortti poistetaan:

— ‘s’ on oleellinen ja osoittaa korttiaukon, josta kortti poistetaan,

— ‘c’ on asetettava arvoon 0,

— ‘p’ on asetettava arvoon 1,

— ‘aa’ on asetettava kortin poistamishetkellä valittuna ollutta toimintaa vastaavaksi.

Käsin syöttämisen tuloksena kortille tallennetun tietueen tavujen ‘c’ ja ‘aa’ päälle voidaan myöhemmin kirjoittaa uudet tilannetta kuvaavat tiedot.

2.2. **Address**

Osoite.

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

codePage määrittää 4 luvussa määritellyn merkistön,

address on määritetyn merkistön avulla koodattu osoite.

2.3. **AESKey**

Sukupolvi 2:

AES-avain, jonka pituus on 128, 192 tai 256 bittiä.

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

Asetettava arvo: ei lisämäärittelyjä.

2.4. **AES128Key**

Sukupolvi 2:

AES128-avain.

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

length osoittaa AES128-avaimen pituuden oktetteina.

aes128Key on AES-avain, jonka pituus on 128 bittiä.

Asetettava arvo:

pituuden arvoksi asetetaan 16.

▼B

2.5. **AES192Key**

Sukupolvi 2:

AES192-avain.

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

length osoittaa AES192-avaimen pituuden oktetteina.

aes192Key on AES-avain, jonka pituus on 192 bittiä.

Asetettava arvo:

pituuden arvoksi asetetaan 24.

2.6. **AES256Key**

Sukupolvi 2:

AES256-avain.

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

length osoittaa AES256-avaimen pituuden oktetteina.

aes256Key on AES-avain, jonka pituus on 256 bittiä.

Asetettava arvo:

pituuden arvoksi asetetaan 32.

2.7. **BCDString**

BCDString-datatyypillä esitetään luvut BCD- eli binaarikoodatussa desimaalimuodossa. Tätä datatyyppiä käytetään esittämään yksi desimaali yhdellä nelibittisellä (puoli)tavulla. BCDString perustuu ISO/IEC 8824-1 -standardin ‘CharacterStringType’-määrittelyyn.

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

BCDString-datatyypissä käytetään ”hstring”-merkintätapaa. Vasemmanpuoleisin heksadesimaaliluku on ensimmäisen tavun merkitsevin puolitavu. Muodostettaessa useita tavuja on tarvittaessa lisättävä nollan arvoisia puolitavuja ensimmäisen tavun vasemmanpuoleisesta puolitavusta alkaen.

Sallitut luvut ovat: 0, 1, … 9.

2.8. **CalibrationPurpose**

Koodi, joka ilmaisee, miksi joukko kalibrointiparametreja on tallennettu. Tämä datatyyppi liittyy liitteen 1 B vaatimukseen 097 ja 098 sekä liitteen 1 C vaatimukseen 119.

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

▼B

Asetettava arvo:

Sukupolvi 1:

‘00’H	varattu arvo,
‘01’H	aktivointi: ajoneuvoyksikköä aktivoitaessa tunnettujen kalibrointiparametrien tallennus,
‘02’H	ensiasennus: ajoneuvoyksikön ensimmäinen kalibrointi sen aktivoinnin jälkeen,
‘03’H	asennus: ajoneuvoyksikön ensimmäinen kalibrointi sen ollessa nykyisessä ajoneuvossa,
‘04’H	määräaikaistarkastus.

Sukupolvi 2:

Sukupolven 1 arvojen lisäksi käytetään seuraavia arvoja:

‘05’H	yritys syöttää ajoneuvon rekisteritunnus,
‘06’H	ajan asetus ilman kalibrointia,
‘07’H … ‘7F’H	varattu tulevaan käyttöön,
‘80’H … ‘FF’H	Arvo määräytyy laitevalmistajan mukaan.

2.9. **CardActivityDailyRecord**

Kortille tallennetut tiedot, jotka liittyvät kuljettajan toimintaan tietyn kalenterivuorokauden aikana. Tämä datatyyppi liittyy liitteen 1 C vaatimukseen 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 edellisen päivätietueen kokonaispituus tavuina. Tämän maksimiarvon määrää sen OCTET STRING -tavujonon pituus, johon nämä tietueet tallennetaan (ks. CardActivityLengthRange-muuttujan selitystä, lisäyksessä 2 oleva 4 kohta). Kun kyseinen tietue on vanhin päivittäinen tietue, on activityPreviousRecordLength-muuttujan arvoksi asetettava 0.

activityRecordLength on tämän tietueen kokonaispituus tavuina. Tämän maksimiarvon määrää sen OCTET STRING -tavujonon pituus, johon nämä tiedot tallennetaan.

activityRecordDate on tietueen päiväys.

▼B

activityDailyPresenceCounter on kyseistä päivää vastaava kortin käyttökertalaskurin arvo.

activityDayDistance on kyseisenä päivänä kuljettu kokonaismatka.

activityChangeInfo on kuljettajan ActivityChangeInfo-tiedot kyseiseltä päivältä. Se voi sisältää enintään 1440 tietoa (yksi toiminnan tilan muutos minuuttia kohden). Tämä sarja sisältää aina ActivityChangeInfo-tiedot, jotka ilmoittavat kuljettajatilanteen klo 00.00.

2.10. **CardActivityLengthRange**

Kuljettaja- tai korjaamokortilla oleva tavumäärä kuljettajan toimintaa koskevien tietojen tallentamiseksi.

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

Asetettava arvo: ks. lisäys 2.

2.11. **CardApprovalNumber**

Kortin tyyppihyväksyntänumero.

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

Asetettava arvo:

hyväksyntänumero annetaan sellaisena kuin se julkaistaan Euroopan komission vastaavalla verkkosivustolla, mukaan lukien mahdolliset yhdysviivat. Hyväksyntänumero on tasattu vasemmalle.

2.12. **CardCertificate**

Sukupolvi 1:

Kortin julkisen avaimen varmenne.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Kortille tallennetut tiedot, jotka liittyvät kortin integroituun piiriin (IC:hen) (liitteen 1 C vaatimus 249). Tietue icSerialNumber yhdessä tietueen icManufacturingReferences kanssa yksilöi kortin sirun täydellisesti. Pelkästään icSerialNumber ei yksilöi kortin sirua täydellisesti.

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

icSerialNumber on integroidun piirin sarjanumero.

icManufacturingReferences on integroidun piirin valmistajan tunniste ja valmisteosat.

2.14. **CardConsecutiveIndex**

Kortin haltijakohtainen sarjanumero (määritelmä h)).

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

Asetettava arvo: (ks. liitteessä 1 C oleva 7 kappale)

Suurennusjärjestys: ‘0, …, 9, A, …, Z, a, …, z’

▼B

2.15. **CardControlActivityDataRecord**

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät viimeisimpään tarkastustoimeen, jonka kohteeksi kuljettaja on joutunut (liitteen 1 C vaatimus 274, 299, 327 ja 350).

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

controlType on tarkastuksen tyyppi.

controlTime on tarkastuksenpäivämäärä ja aika.

controlCardNumber on tarkastuksen suorittaneen virkailijan FullCardNumber-tieto.

controlVehicleRegistration on sen ajoneuvon rekisteritunnus ja rekisteröinyt jäsenvaltio, jota käytettäessä tarkastus tapahtui.

controlDownloadPeriodBegin ja **controlDownloadPeriodEnd** sisältävät tiedot tietojen kopioinnin alku- ja päättymishetkestä, jos tietoja kopioitiin.

2.16. **CardCurrentUse**

Kortin käyttöjaksoon liittyvät tiedot (liitteen 1 C vaatimus 273, 298, 326 ja 349).

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

sessionOpenTime on aika, jolloin kortti asetettiin paikoilleen kuluvan käyttöjakson aluksi. Tämän elementin arvo asetetaan nollaksi korttia poistettaessa.

sessionOpenVehicle on parhaillaan käytettävän ajoneuvon tunnistetiedot, jotka on asetettu korttia paikoilleen asetettaessa. Tämän elementin arvo asetetaan nollaksi korttia poistettaessa.

2.17. **CardDriverActivity**

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kuljettajan toimintaan (liitteen 1 C vaatimus 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 sen tallennuspaikan alun määrittely (tavuina merkkijonon alusta lukien), johon on tallennettu vanhin täydellinen activityDailyRecords-merkkijonoon sisältyvä päivätietue. Osoitinmuuttujan maksimiarvon määrää merkkijonon pituus.

▼B

activityPointerNewestRecord on sen tallennuspaikan alun määrittely (tavuina merkkijonon alusta lukien), johon on tallennettu viimeisin täydellinen activityDailyRecords-merkkijonoon sisältyvä päivätietue. Osoitinmuuttujan maksimiarvon määrää merkkijonon pituus.

activityDailyRecords on kuljettajan päivittäiseen toimintaan liittyvien tietojen tallennukseen käytettävissä oleva tila (datarakenne: CardActivityDailyRecord) jokaista sellaista kalenterivuorokautta kohden, jolloin korttia on käytetty.

Asetettava arvo: tätä tavujonoa täytetään kiertävästi CardActivityDailyRecord-tiedoilla. Ensimmäisellä kerralla tallennus aloitetaan jonon ensimmäisestä tavusta. Kaikki uudet tietueet lisätään edellisen perään. Kun tavujono on täynnä, tallennusta jatketaan jonon ensimmäisestä tavusta välittämättä dataelementin sisälle syntyvästä katkoksesta. Ennen kuin tavujonoon lisätään uusia toimintatietoja (laajentamalla käytössä olevaa activityDailyRecord-tilaa tai avaamalla uusi activityDailyRecord-tila), jotka korvaavat vanhempia toimintatietoja, activityPointerOldestDayRecord-osoitin on asetettava vanhimman täydellisen päivittäisen tietueen sijaintia vastaavaksi ja tämän (uuden) vanhimman täydellisen päivittäisen tietueen activityPreviousRecordLength-tieto on asetettava nollaksi.

2.18. **CardDrivingLicenceInformation**

Kuljettajakortille tallennetut tiedot, jotka liittyvät kortin haltijan ajokortin tietoihin (liitteen 1 C vaatimus 259 ja 284).

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

drivingLicenceIssuingAuthority on kortin myöntänyt viranomainen.

drivingLicenceIssuingNation on kortin myöntäneen viranomaisen kansallisuus.

drivingLicenceNumber on ajokortin numero.

2.19. **CardEventData**

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijaa koskeviin tapahtumiin (liitteen1 C vaatimus 260, 285, 318 ja 341).

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

CardEventData on sarja cardEventRecords-tietueita, järjestettynä nousevaan järjestykseen EventFaultType-muuttujan arvon mukaan (paitsi tietoturvan murtoyritykset, jotka kerätään tietuesarjan viimeiseen osaan).

cardEventRecords on sarja tietyn tyypin tapahtumiin liittyviä tietueita (tai tietoturvan murtoyrityksiin liittyvä tapahtumaluokka).

▼B

2.20. **CardEventRecord**

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijaa koskeviin tapahtumiin (liitteen 1 C vaatimus 261, 286, 318 ja 341).

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

eventType on tapahtuman tyyppi.

eventBeginTime on päivämäärä ja aika, jolloin tapahtuma alkoi.

eventEndTime on päivämäärä ja aika, jolloin tapahtuma päättyi.

eventVehicleRegistration on sen ajoneuvon rekisteritunnus ja rekisteröinyt jäsenvaltio, jossa tapahtuma sattui.

2.21. **CardFaultData**

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijaa koskeviin vikatapahtumiin (liitteen 1 C vaatimus 263, 288, 318 ja 341).

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

CardFaultData on sarja valvontalaitevikoihin liittyviä tietueita ja sen perässä oleva sarja korttivikoihin liittyviä tietueita.

cardFaultRecords on sarja tiettyihin vikatyyppeihin liittyviä tietueita (valvontalaite- tai korttivika).

2.22. **CardFaultRecord**

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijaa koskevaan vikatapahtumaan (liitteen 1 C vaatimus 264, 289, 318 ja 341).

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

faultType on vikatapahtuman tyyppi.

faultBeginTime on päivämäärä ja aika, jolloin vikatapahtuma alkoi.

faultEndTime on päivämäärä ja aika, jolloin vikatapahtuma päättyi.

faultVehicleRegistration on sen ajoneuvon rekisteritunnus ja rekisteröinyt jäsenvaltio, jossa vikatapahtuma sattui.

▼B

2.23. **CardIccIdentification**

Kortille tallennetut tiedot, jotka liittyvät integroidun piirin sisältävän kortin (IC-kortin) tunnistukseen (liitteen 1 C vaatimus 248).

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

clockStop on lisäyksessä 2 määritelty Clockstop-tila.

cardExtendedSerialNumber on IC-kortin sarjanumero siten kuin se on määritelty ExtendedSerialNumber-datatyypillä.

cardApprovalNumber on kortin tyyppihyväksyntänumero.

cardPersonaliserID on kortin yksilöintitunnus koodattuna koodilla ManufacturerCode.

embedderIcAssemblerId on kortin laminoijan/IC:n asentajan tunniste.

icIdentifier on kortilla olevan integroidun piirin ja piirin valmistajan Identifier-tunnus siten kuin se on määritelty standardissa ISO/IEC 7816-6.

2.24. **CardIdentification**

Kortille tallennetut tiedot, jotka liittyvät kortin tunnistukseen (liitteen 1 C vaatimus 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 kortin myöntäneen jäsenvaltion tunnus.

cardNumber on kortin numero.

cardIssuingAuthorityName on kortin myöntäneen viranomaisen nimi.

cardIssueDate on päivämäärä, jolloin kortti myönnettiin nykyiselle haltijalleen.

cardValidityBegin on kortin ensimmäinen voimassaolopäivä.

cardExpiryDate on kortin viimeinen voimassaolopäivä.

▼B

2.25. **CardMACertificate**

Sukupolvi 2:

Kortin julkisen avaimen varmenne ajoneuvoyksikön molemminpuolista todentamista varten. Varmenteen rakenne määritetään lisäyksessä 11.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Määritelmän g mukainen kortin numero.

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

driverIdentification on tunniste, joka yksilöi kuljettajan jäsenvaltiossa.

ownerIdentification on tunniste, joka yksilöi yrityksen tai korjaamon tai tarkastuksia suorittavan elimen jäsenvaltiossa.

cardConsecutiveIndex on kortin haltijakohtainen sarjanumero.

cardReplacementIndex on kortin korvausnumero.

cardRenewalIndex on kortin uusintanumero.

Tietokokonaisuuden (CHOICE) ensimmäiseen kohtaan (SEQUENCE) voi sisällyttää kuljettajakortin numeron ja toiseen kohtaan (SEQUENCE) korjaamokortin, valvontakortin ja yrityskortin numeron.

2.27. **CardPlaceDailyWorkPeriod**

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät paikkaan, jossa päivän työaika alkaa ja/tai päättyy (liitteen 1 C vaatimus 272, 297, 325 ja 348).

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

placePointerNewestRecord on viimeksi päivitetyn paikkaan liittyvän tiedon järjestysnumero.

Asetettava arvo: numero, joka vastaa paikkaan liittyvän tietueen järjestysnumeroa, alkaen numerosta ‘0’ ensimmäiselle paikkaan liittyvälle tietueelle datarakenteessa.

placeRecords on sarja tietueita, jotka sisältävät syötettyihin paikkoihin liittyviä tietoja.

▼B

2.28. **CardPrivateKey**

Sukupolvi 1:

Kortin yksityinen avain.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Kortin julkinen avain.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Kortin uusintanumero (määritelmä i).

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

Asetettava arvo: (ks. tämän liitteen VII luku).

‘0’ Ensi kerran myönnetty.

Suurennusjärjestys: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

Kortin korvausnumero (määritelmä j).

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

Asetettava arvo: (ks. tämän liitteen VII luku).

‘0’ Alkuperäinen kortti.

Suurennusjärjestys: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

Sukupolvi 2:

Allekirjoitettavan kortin julkisen avaimen varmenne. Varmenteen rakenne määritetään lisäyksessä 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Tunnus, jolla erotetaan toisistaan ajoneuvoyksikön kaksi korttiaukkoa.

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

Asetettava arvo: ei lisämäärittelyjä.

2.34. **CardSlotsStatus**

Tunnus, joka osoittaa ajoneuvoyksikön kahteen korttiaukkoon asetettujen korttien tyypin.

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

▼B

Asetettava arvo — Octet Aligned (tavuittain ryhmitelty): ‘ccccdddd’B

‘cccc’B apukuljettajan korttiaukkoon asetetun kortin tunnistus,

‘dddd’B kuljettajan korttiaukkoon asetetun kortin tunnistus,

jossa käytetään seuraavia tunnuksia:

‘0000’B aukossa ei ole korttia,

‘0001’B aukossa on kuljettajakortti,

‘0010’B aukossa on korjaamokortti,

‘0011’B aukossa on valvontakortti,

‘0100’B aukossa on yrityskortti.

2.35. **CardSlotsStatusRecordArray**

Sukupolvi 2:

CardSlotsStatus ja metadata, siten kuin sitä käytetään kopiointiprotokollassa.

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

recordType osoittaa tietueen tyypin (CardSlotsStatus). **Asetettava arvo**: ks. RecordType

recordSize on CardSlotsStatus-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja CardSlotsStatus-tietueita.

2.36. **CardStructureVersion**

Tunnus, joka osoittaa ajopiirturikortille annetun datarakenteen versionumeron.

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

Asetettava arvo: ‘aabb’H:

‘aa’H rakenteen muutoksen järjestysnumero,

‘00’H sukupolven 1 laitteille

‘01’H sukupolven 2 laitteille.

‘bb’H eniten merkitsevän tavun mukaiselle datarakenneversiolle määriteltyjen dataelementtien käyttöä koskevan muutoksen järjestysnumero,

‘00’H sukupolven 1 laitteen tälle versiolle

‘00’H sukupolven 2 laitteen tälle versiolle.

▼B

2.37. **CardVehicleRecord**

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät ajoneuvon käyttöjaksoon kalenterivuorokauden aikana (lisäyksen 1 C vaatimus 269, 294, 322 ja 345).

Sukupolvi 1:

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

vehicleOdometerBegin on ajoneuvon matkamittarin lukema ajoneuvon käyttöjakson alussa.

vehicleOdometerEnd on ajoneuvon matkamittarin lukema ajoneuvon käyttöjakson lopussa.

vehicleFirstUse on päivämäärä ja aika, jolloin ajoneuvon käyttöjakso alkoi.

vehicleLastUse on päivämäärä ja aika, jolloin ajoneuvon käyttöjakso päättyi.

vehicleRegistration on ajoneuvon rekisteritunnus ja ajoneuvon rekisteröinyt jäsenvaltio.

vuDataBlockCounter on VuDataBlockCounter-laskurin arvo, kun kortti poistetaan viimeisen kerran ajoneuvon käyttöjakson aikana.

Sukupolvi 2:

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

Sukupolven 1 arvojen lisäksi käytetään seuraavia dataelementtejä:

VehicleIdentificationNumber on ajoneuvon valmistenumero, joka viittaa koko ajoneuvoon.

2.38. **CardVehiclesUsed**

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijan käyttämiin ajoneuvoihin (liitteen 1 C vaatimus 270, 295, 323 ja 346).

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

vehiclePointerNewestRecord on viimeksi päivitetyn ajoneuvoon liittyvän tietueen järjestysnumero.

▼B

Asetettava arvo: numero, joka vastaa ajoneuvoon liittyvän tietueen järjestysnumeroa, alkaen numerosta ‘0’ ensimmäiselle ajoneuvoon liittyvälle tietueelle datarakenteessa.

cardVehicleRecords on sarja tietueita, jotka sisältävät haltijan käyttämiin ajoneuvoihin liittyviä tietoja.

2.39. **CardVehicleUnitRecord**

Sukupolvi 2:

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät käytettyyn ajoneuvoyksikköön (liitteen 1 C vaatimus 303 ja 351).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   manufacturerCode                       ManufacturerCode,
   deviceID                               INTEGER(0..255),
   vuSoftwareVersion                      VuSoftwareVersion
}
```

timeStamp on ajoneuvoyksikön käyttöajan alku (eli hetki, jolloin kortti asetettiin ensimmäisen kerran paikoilleen ajoneuvoyksikköön käyttöajaksi).

manufacturerCode yksilöi ajoneuvoyksikön valmistajan.

deviceID yksilöi valmistajan ajoneuvoyksikön tyypin. Arvo on valmistajakohtainen.

vuSoftwareVersion on ajoneuvoyksikön ohjelmistoversion numero.

2.40. **CardVehicleUnitsUsed**

Sukupolvi 2:

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijan käyttämiin ajoneuvoyksikköihin (liitteen 1 C vaatimus 306 ja 352).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord on viimeksi päivitetyn ajoneuvoyksikköön liittyvän tietueen järjestysnumero.

Asetettava arvo: numero, joka vastaa ajoneuvoyksikköön liittyvän tietueen järjestysnumeroa, alkaen numerosta ‘0’ ensimmäiselle ajoneuvoyksikköön liittyvälle tietueelle datarakenteessa.

cardVehicleUnitRecords on sarja tietueita, jotka sisältävät haltijan käyttämiin ajoyksikköihin liittyviä tietoja.

2.41. **Certificate**

Varmenneviranomaisen antama julkisen avaimen varmenne.

Sukupolvi 1:

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

▼B

Asetettava arvo: digitaalinen allekirjoitus, joka sisältää CertificateContent-tietueen sisällön osittaisen palautuksen lisäyksen 11 (Yhteiset turvamekanismit) mukaisesti: allekirjoitus (128 tavua) julkisen avaimen jakojäännös (58 tavua) varmenteen antaneen viranomaisen viite (8 tavua).

Sukupolvi 2:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Asetettava arvo: ks. lisäys 11.

2.42. **CertificateContent**

Sukupolvi 1:

Julkisen avaimen varmenteen (selväkielinen) sisältö lisäyksen 11 (Yhteiset turvamekanismit) mukaisesti.

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

certificateProfileIdentifier on vastaavan varmenteen versio.

Asetettava arvo: ‘01h’ tälle versiolle.

certificationAuthorityReference yksilöi varmenneviranomaisen, joka on antanut tämän varmenteen. Se antaa tämän varmenneviranomaisen julkisen avaimen viitetiedot.

certificateHolderAuthorisation yksilöi varmenteen haltijan oikeudet.

certificateEndOfValidity on varmenteen viimeinen hallinnollinen voimassaolopäivä.

certificateHolderReference yksilöi varmenteen haltijan. Se antaa myös hänen julkisen avaimensa viitetiedot.

publicKey on tämän varmenteen avulla varmennettu julkinen avain.

2.43. **CertificateHolderAuthorisation**

Varmenteen haltijan oikeuksien tunniste.

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

Sukupolvi 1:

tachographApplicationID on piirturisovelluksen tunniste.

Asetettava arvo: ‘FFh’ ‘54h’ ‘41h’ ‘43h’ ‘48h’ ‘4Fh’. Tämä sovellustunniste on ISO/IEC 7816-5 -standardin mukainen varattu rekisteröimätön sovellustunniste.

equipmentType on sen laitetyypin tunniste, jonka yhteydessä varmennetta käytetään.

Asetettava arvo: EquipmentType-datatyypin mukaan. 0, jos kyseessä on jäsenvaltion oma varmenne.

▼B

Sukupolvi 2:

tachographApplicationID osoittaa sukupolven 2 ajopiirturikortin sovellustunnisteen (AID) kuusi merkittävintä tavua. Ajopiirturikortin sovellustunniste määritetään 6.2 kohdassa.

Asetettava arvo: ‘FF 53 4D 52 44 54’.

equipmentType on sen sukupolven 2 määritellyn laitetyypin tunniste, jonka yhteydessä varmennetta käytetään.

Asetettava arvo: EquipmentType-datatyypin mukaan.

2.44. **CertificateRequestID**

Varmennepyynnön täysin yksilöivä tunniste. Tunnistetta voidaan käyttää myös ajoneuvoyksikön julkisen avaimen tunnisteena, mikäli sen ajoneuvoyksikön sarjanumero, johon avain on tarkoitettu, ei ole tiedossa silloin, kun varmenne luodaan.

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

requestSerialNumber on varmennepyynnön sarjanumero, joka täysin yksilöi valmistajan ja alla määritellyn kuukauden.

requestMonthYear on sen kuukauden ja vuoden tunniste, jolloin varmennepyyntö tehtiin.

Asetettava arvo: kuukausi (kaksi numeroa) ja vuosi (kaksi viimeistä numeroa) binaarikoodatussa desimaalimuodossa (BCD).

crIdentifier: on tunniste, jolla varmennepyyntö erotetaan laajennetusta sarjanumerosta.

Asetettava arvo: ‘FFh’.

manufacturerCode: on varmennetta pyytävän valmistajan numerotunniste.

2.45. **CertificationAuthorityKID**

Varmenneviranomaisen (jäsenvaltion tai eurooppalainen varmenneviranomainen) julkisen avaimen tunniste.

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

nationNumeric on varmenneviranomaisen maan numerotunnus.

nationAlpha on varmenneviranomaisen maan kirjaintunnus.

▼B

keySerialNumber on sarjanumero, jonka avulla tunnistetaan varmenneviranomaisen eri avaimet siinä tapauksessa, että avain vaihtuu.

additionalInfo on kaksitavuinen kenttä lisäkoodeja varten (varmenneviranomaisen mukaan).

caIdentifier on tunnus, jolla varmenneviranomaisen avaimen tunniste erotetaan muista avaimen tunnisteista.

Asetettava arvo: ‘01h’.

2.46. **CompanyActivityData**

Yrityskortille tallennetut tiedot, jotka liittyvät kortilla suoritettuihin toimiin (liitteen 1 C vaatimus 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 viimeksi päivitetyn companyActivityRecord-tietueen järjestysnumero.

Asetettava arvo: numero, joka vastaa yrityksen toimiin liittyvän tietueen järjestysnumeroa, alkaen numerosta ‘0’ ensimmäiselle yrityksen toimiin liittyvälle tietueelle datarakenteessa.

companyActivityRecords on sarja tietueita, joka sisältää kaikki yrityksen toimiin liittyvät tiedot.

companyActivityRecord on yhteen yrityksen toimeen liittyviä tietoja sisältävä tietue.

companyActivityType on yrityksen toimen tyyppi.

companyActivityTime on yrityksen toimen päivämäärä ja aika.

cardNumberInformation on sen kortin numero ja myöntänyt jäsenvaltio, jonka tiedot kopioitiin, jos tällainen kopiointi suoritettiin.

vehicleRegistrationInformation on sen ajoneuvon rekisteritunnus ja rekisteröinyt jäsenvaltio, jossa lukitus tehtiin tai avattiin.

downloadPeriodBegin ja **downloadPeriodEnd** ovat sen ajanjakson alku ja loppu, jota vastaavat tiedot kopioitiin ajoneuvoyksiköstä, jos tällainen kopiointi suoritettiin.

2.47. **CompanyActivityType**

Tunnus, joka osoittaa yrityksen toimen tyypin yrityskorttia käytettäessä.

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

▼B

2.48. **CompanyCardApplicationIdentification**

Yrityskortille tallennetut tiedot, jotka liittyvät kortilla olevan sovelluksen tunnistamiseen (liitteen 1 C vaatimus 369 ja 375).

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

typeOfTachographCardId määrittelee kortilla käytetyn tunnisteen tyypin.

cardStructureVersion määrittelee kortilla käytetyn datarakenteen version.

noOfCompanyActivityRecords on kortille tallennettavissa olevien yrityksen toimiin liittyvien tietueiden määrä.

2.49. **CompanyCardHolderIdentification**

Yrityskortille tallennetut tiedot, jotka liittyvät kortin haltijan tunnistukseen (liitteen 1 C vaatimus 372 ja 378).

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

companyName on kortin haltijayrityksen nimi.

companyAddress on kortin haltijayrityksen osoite.

cardHolderPreferredLanguage on kortin haltijan ensisijaisesti käyttämä kieli.

2.50. **ControlCardApplicationIdentification**

Valvontakortille tallennetut tiedot, jotka liittyvät kortilla olevan sovelluksen tunnistamiseen (liitteen 1 C vaatimus 357 ja 363).

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

typeOfTachographCardId määrittelee kortilla käytetyn tunnisteen tyypin.

cardStructureVersion määrittelee kortilla käytetyn datarakenteen version.

noOfControlActivityRecords on kortille tallennettavissa olevien tarkastustoimiin liittyvien tietueiden määrä.

▼B

2.51. **ControlCardControlActivityData**

Valvontakortille tallennetut tiedot, jotka liittyvät kortilla suoritettuihin valvontatoimiin (liitteen 1 C vaatimus 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 viimeksi päivitetyn valvontatoimeen liittyvän tietueen järjestysnumero.

Asetettava arvo: numero, joka vastaa tarkastustoimiin liittyvän tietueen järjestysnumeroa, alkaen numerosta ‘0’ ensimmäiselle tarkastustoimiin liittyvälle tietueelle datarakenteessa.

controlActivityRecords on sarja tietueita, jotka sisältävät kaikki tarkastustoimiin liittyvät tiedot.

controlActivityRecord on yhteen tarkastustoimeen liittyviä tietoja sisältävä tietue.

controlType on tarkastuksen tyyppi.

controlTime on tarkastustoimen päivämäärä ja aika.

controlledCardNumber on sen kortin numero ja myöntänyt jäsenvaltio, johon tarkastustoimi kohdistui.

controlVehicleRegistration on sen ajoneuvon rekisteritunnus ja rekisteröinyt jäsenvaltio, jota käytettäessä tarkastus tapahtui.

controlDownloadPeriodBegin ja **controlDownloadPeriodEnd** ovat sen ajanjakson alku ja loppu, jota koskevat tiedot mahdollisesti kopioitiin.

2.52. **ControlCardHolderIdentification**

Valvontakortille tallennetut tiedot, jotka liittyvät kortin haltijan tunnistamiseen (liitteen 1 C vaatimus 360 ja 366).

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

controlBodyName on sen tarkastuselimen nimi, johon kortin haltija kuuluu.

controlBodyAddress on sen tarkastuselimen osoite, johon kortin haltija kuuluu.

cardHolderName on kortin haltijan nimi ja etunimi (etunimet).

▼B

cardHolderPreferredLanguage on kortin haltijan ensisijaisesti käyttämä kieli.

2.53. **ControlType**

Tunnus, joka osoittaa tarkastuksen aikana suoritetut toimet. Tämä datatyyppi liittyy liitteen 1 C vaatimuksiin 126, 274, 299, 327 ja 350.

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

Sukupolvi 1:

Asetettava arvo — Octet Aligned (tavuittain ryhmitelty): ‘cvpdxxxx’B (8 bits)

‘c’B kortin tietojen kopiointi:

‘0’B: kortin tietoja ei kopioitu tämän tarkastustoimen aikana,

‘1’B: kortin tietoja kopioitiin tämän tarkastustoimen aikana

‘v’B ajoneuvoyksikön tietojen kopiointi:

‘0’B: ajoneuvoyksikön tietoja ei kopioitu tämän tarkastustoimen aikana,

‘1’B: ajoneuvoyksikön tietoja kopioitiin tämän tarkastustoimen aikana

‘p’B tietojen tulostaminen:

‘0’B: tietoja ei tulostettu tämän tarkastustoimen aikana,

‘1’B: tietoja tulostettiin tämän tarkastustoimen aikana,

‘d’B näyttö:

‘0’B: näyttöä ei käytetty tämän tarkastustoimen aikana,

‘1’B: näyttöä käytettiin tämän tarkastustoimen aikana,

‘xxxx’B ei käytetty.

Sukupolvi 2:

Asetettava arvo — Octet Aligned (tavuittain ryhmitelty): ‘cvpdxxxx’B (8 bittiä)

‘c’B kortin tietojen kopiointi:

‘0’B: kortin tietoja ei kopioitu tämän tarkastustoimen aikana,

‘1’B: kortin tietoja kopioitiin tämän tarkastustoimen aikana

‘v’B ajoneuvoyksikön tietojen kopiointi:

‘0’B: ajoneuvoyksikön tietoja ei kopioitu tämän tarkastustoimen aikana,

‘1’B: ajoneuvoyksikön tietoja kopioitiin tämän tarkastustoimen aikana

‘p’B tietojen tulostaminen:

‘0’B: tietoja ei tulostettu tämän tarkastustoimen aikana,

‘1’B: tietoja tulostettiin tämän tarkastustoimen aikana,

▼B

‘d’B	näyttö:
	‘0’B: näyttöä ei käytetty tämän tarkastustoimen aikana,
	‘1’B: näyttöä käytettiin tämän tarkastustoimen aikana,
‘e’B	kalibroinnin tarkastus tien varrella:
	‘0’B: kalibrointiparametrejä ei tarkastettu tämän tarkastustoimen aikana,
	‘1’B: kalibrointiparametrit tarkastettiin tämän tarkastustoimen aikana,
‘xxx’B	varattu tulevaan käyttöön.

2.54. **CurrentDateTime**

Valvontalaitteessa meneillään oleva päivämäärä ja aika.

```
CurrentDateTime ::= TimeReal
```

Asetettava arvo: ei lisämäärittelyjä.

2.55. **CurrentDateTimeRecordArray**

Sukupolvi 2:

Meneillään oleva päivämäärä ja aika ja metadata, siten kuin sitä käytetään kopiointiprotokollassa.

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

recordType osoittaa tietueen tyypin (CurrentDateTime). **Asetettava arvo**: ks. RecordType

recordSize on CurrentDateTime-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on kuluvaan päivämäärään ja aikaan liittyvä tietuejoukko.

2.56. **DailyPresenceCounter**

Kuljettaja- tai korjaamokortille tallennettu laskuri, jonka arvoa suurennetaan yhdellä jokaisena sellaisena kalenterivuorokautena, jolloin kortti on ollut asetettuna ajoneuvoyksikköön. Tämä datatyyppi liittyy liitteen 1 C vaatimukseen 266, 299, 320 ja 343.

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

Asetettava arvo: juokseva numero, jonka maksimiarvo on 9 999 ja joka sen jälkeen alkaa jälleen nollasta. Korttia ensi kerran myönnettäessä numero asetetaan nollaksi.

▼B

2.57. **Datef**

Päivämäärä ilmaistuna helposti tulostettavassa numeerisessa muodossa.

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

Asetettava arvo:

yyyy	vuosi
mm	kuukausi
dd	päivä
‘00000000’H	merkitsee nimenomaan, ettei päivämäärätietoa ole.

2.58. **DateOfDayDownloaded**

Sukupolvi 2:

Päivämäärä, jolloin tieto kopioitiin.

```
DateOfDayDownloaded ::= TimeReal
```

Asetettava arvo: ei lisämäärittelyjä.

2.59. **DateOfDayDownloadedRecordArray**

Sukupolvi 2:

Kopioinnin päivämäärä ja aika ja metadata, siten kuin sitä käytetään kopiointiprotokollassa.

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

recordType osoittaa tietueen tyypin (DateOfDayDownloaded). **Asetettava arvo**: ks. RecordType

recordSize on CurrentDateTime-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on ladattujen tietueiden päivämäärään ja aikaan liittyvä tietuejoukko.

2.60. **Distance**

Kuljettu matka (ajoneuvon kahden matkamittarilukeman laskettu ero kilometreinä).

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

Asetettava arvo: etumerkitön binaariluku. Arvo kilometreinä alueella 0–9 999 km.

2.61. **DriverCardApplicationIdentification**

Kuljettajakortille tallennetut tiedot, jotka liittyvät kortilla olevan sovelluksen tunnistamiseen (liitteen 1 C vaatimus 253 ja 278).

▼B

Sukupolvi 1:

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

typeOfTachographCardId määrittelee kortilla käytetyn tunnisteen tyypin.

cardStructureVersion määrittelee kortilla käytetyn datarakenteen version.

noOfEventsPerType on niiden tapahtumien määrä tapahtumatyyppiä kohden, jotka voidaan tallentaa kortille.

noOfFaultsPerType on niiden vikatapahtumien määrä vikatyyppiä kohden, jotka voidaan tallentaa kortille.

activityStructureLength osoittaa niiden tavujen määrän, jotka ovat käytettävissä kuljettajan toimintaan liittyvien tietojen tallennukseen.

noOfCardVehicleRecords on niiden ajoneuvoon liittyviä tietoja sisältävien tietueiden määrä, jotka voidaan tallentaa kortille.

noOfCardPlaceRecords on niiden paikkoihin liittyviä tietoja sisältävien tietueiden määrä, jotka voidaan tallentaa kortille.

Sukupolvi 2:

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

Sukupolven 1 arvojen lisäksi käytetään seuraavia dataelementtejä:

noOfGNSSCDRecords on kortille tallennettavissa olevien keskeytymätöntä ajoaikaa koskevien GNSS-tietueiden määrä.

noOfSpecificConditionRecords on kortille tallennettavissa olevien erityisolosuhteisiin liittyvien tietueiden määrä.

2.62. **DriverCardHolderIdentification**

Kuljettajakortille tallennetut tiedot, jotka liittyvät kortin haltijan tunnistamiseen (liitteen 1 C vaatimus 256 ja 281).

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

▼B

cardHolderName on kuljettajakortin haltijan nimi ja etunimi (etunimet).

cardHolderBirthDate on kuljettajakortin haltijan syntymäaika.

cardHolderPreferredLanguage on kortin haltijan ensisijaisesti käyttämä kieli.

2.63. **DSRCSecurityData**

Sukupolvi 2:

Koodaamattomat tiedot ja MAC-koodi, joka lähetetään DSRC-laitteella ajopiirturista etäkyselylaitteeseen (RI), lisätietoja lisäyksessä 11 olevan B osan 13 kappaleessa.

```
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 osa DER-TLV-koodausta, ja arvoksi on asetettava ‘81 10’ (ks. lisäyksessä 11 olevan B osan 13 kappale).

currentDateTime on ajoneuvoyksikön meneillään oleva päivämäärä ja aika.

counter on luettelo RTM-viesteistä.

vuSerialNumber on ajoneuvoyksikön sarjanumero.

dSRCMKVersionNumber on sen DSRC-pääavaimen versionumero, josta ajoneuvoyksikkökohtaiset DSRC-avaimet olivat peräisin.

tagLengthMac on MAC-dataobjektin tuntomerkki ja pituus osana DER-TLV-koodausta. Tuntomerkin arvoksi asetetaan ‘8E’, pituus koodataan MAC-koodin pituuden oktetteina (ks. lisäys 11, B osa, 13 kappale).

mac on MAC-koodi laskettuna RTM-viestistä (ks. lisäyksessä 11 olevan B osan 13 kappale).

2.64. **EGFCertificate**

Sukupolvi 2:

Ulkoisen GNSS-laitteiston julkisen avaimen varmenne ajoneuvoyksikön molemmipuolista todentamista varten. Varmenteen rakenne määritetään lisäyksessä 11.

```
EGFCertificate ::= Certificate
```

▼B

2.65. **EmbedderIcAssemblerId**

Tarjoaa tietoa IC:n laminoijasta.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode on moduulin laminoijan kaksikirjaiminen maakoodi standardin ISO 3166 perusteella.

moduleEmbedder yksilöi moduulin laminoijan.

manufacturerInformation valmistajan sisäiseen käyttöön.

2.66. **EntryTypeDailyWorkPeriod**

Tunnus, jolla tehdään ero päivän työajan alkamis- ja päättymispaikkaa koskevien syötettyjen tietojen alkamis- ja päättymisaikojen sekä erilaisten tiedon syöttämisolosuhteiden välillä.

Sukupolvi 1:

```
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)
}
```

Asetettava arvo: standardin ISO/IEC8824-1 mukaisesti.

Sukupolvi 2:

```
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)
}
```

Asetettava arvo: standardin ISO/IEC8824-1 mukaisesti.

2.67. **EquipmentType**

Tunnus, jolla erotetaan erilaiset ajopiirturisovelluksessa käytettävät laitteet.

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

▼B

Sukupolvi 1:

```
--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)
```

Asetettava arvo: standardin ISO/IEC8824-1 mukaisesti.

Arvo 0 on varattu tietyn jäsenvaltion tai Euroopan yksilöimiseen varmenteen CHA-kentässä.

Sukupolvi 2:

Seuraavissa lisäyksissä käytetään samoja arvoja kuin sukupolven 1 tapauksessa:

```
--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)
```

Huomautus: SealRecord-tietuesarjassa voidaan käyttää tarvittaessa sukupolven 2 arvoja kilvelle, muuntimelle ja ulkoiselle GNSS-yhteydelle sekä sukupolven 1 arvoja ajoneuvoyksikölle ja liiketunnistimille.

2.68. **EuropeanPublicKey**

Sukupolvi 1:

Eurooppalainen julkinen avain.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Tunnus, joka ilmaisee, miksi tietty tapahtuma tai vika on kirjattu.

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

Asetettava arvo.

'00'H	yksi kymmenestä viimeksi tapahtuneesta tapahtumasta tai viasta
'01'H	pisimpään kestänyt tapahtuma jonain niistä kymmenestä viimeisestä päivästä, jolloin tapahtumia sattui
'02'H	yksi viidestä pisimpään kestäneestä tapahtumasta viimeisen 365 vuorokauden aikana
'03'H	päivän viimeinen tapahtuma jonain niistä kymmenestä viimeisestä päivästä, jolloin tapahtumia sattui
'04'H	vakavin tapahtuma jonain niistä kymmenestä viimeisestä päivästä, jolloin tapahtumia sattui
'05'H	yksi viidestä vakavimmasta tapahtumasta viimeisen 365 vuorokauden aikana
'06'H	ensimmäinen tapahtuma tai vika, joka sattui viimeisimmän kalibroinnin jälkeen
'07'H	aktiivinen/meneillään oleva vika tai tapahtuma
'08'H to '7F'H	varattu tulevaan käyttöön
'80'H to 'FF'H	arvo määräytyy laitevalmistajan mukaan

▼B

2.70. **EventFaultType**

Tunnus, jolla merkitään tapahtuman tai vian tyyppi.

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

Asetettava arvo.

Sukupolvi 1:

‘0x’H	Luonteeltaan yleiset tapahtumat,
‘00’H	Ei lisätietoja,
‘01’H	Ei voimassa olevan kortin asettaminen laitteeseen,
‘02’H	Korttiristiriita,
‘03’H	Aikojen päällekkäisyys,
‘04’H	Ajo ilman asianmukaista korttia,
‘05’H	Kortin paikoilleen asettaminen ajon aikana,
‘06’H	Edellistä kortin käyttöjaksoa ei lopetettu oikein,
‘07’H	Ylinopeus,
‘08’H	Keskeytynyt virransyöttö,
‘09’H	Virhe liikedatassa,
‘0A’H	Ajoneuvon liikeristiriita,
‘0B’ to ‘0F’H	Varattu tulevaan käyttöön,

‘1x’H	Ajoneuvoyksikköön liittyvät tietoturvan murtoyritykset,
‘10’H	Ei lisätietoja,
‘11’H	Liiketunnistimen tunnistaminen epäonnistui,
‘12’H	Ajopiirturikortin tunnistaminen epäonnistui,
‘13’H	Liiketunnistimen luvaton vaihtaminen,
‘14’H	Virhe kortille syötettävien tietojen eheydessä
‘15’H	Virhe tallennettujen käyttäjään liittyvien tietojen eheydessä,
‘16’H	Virhe sisäisessä tiedonsiirrossa,
‘17’H	Laitteen kotelon luvaton avaaminen,
‘18’H	Laitteiden tahallinen vahingoittaminen,
‘19’H to ‘1F’H	Varattu tulevaan käyttöön,

‘2x’H	Liiketunnistimeen liittyvät tietoturvan murtoyritykset,
‘20’H	Ei lisätietoja,
‘21’H	Tunnistaminen epäonnistui,
‘22’H	Virhe tallennettujen tietojen eheydessä,
‘23’H	Virhe sisäisessä tiedonsiirrossa,
‘24’H	Laitteen kotelon luvaton avaaminen,
‘25’H	Laitteiden tahallinen vahingoittaminen,
‘26’H to ‘2F’H	Varattu tulevaan käyttöön,

‘3x’H	Valvontalaiteviat,
‘30’H	Ei lisätietoja,
‘31’H	Ajoneuvoyksikön sisäinen vika,
‘32’H	Vika tulostimessa,
‘33’H	Vika näytössä,
‘34’H	Tietojen kopioinnissa ilmennyt vika,
‘35’H	Vika liiketunnistimessa,
‘36’H to ‘3F’H	Varattu tulevaan käyttöön,

‘4x’H	Korttiviat,
‘40’H	Ei lisätietoja,
‘41’H to ‘4F’H	Varattu tulevaan käyttöön,

‘50’H to ‘7F’H	Varattu tulevaan käyttöön,

‘80’H to ‘FF’H	Arvo määräytyy laitevalmistajan mukaan

▼B

Sukupolvi 2:

Seuraavissa lisäyksissä käytetään samoja arvoja kuin sukupolven 1 tapauksessa:

'0B'H	Aikojen päällekkäisyys (GNSS-laitteiston/ajoneuvoyksikön sisäinen kello),
'0C' to '0F'H	Varattu tulevaan käyttöön,

'5x'H	GNSS-laitteistoon liittyvät viat,
'50'H	Ei lisätietoja,
'51'H	Sisäisen GNSS-vastaanottimen vika,
'52'H	Ulkoisen GNSS-vastaanottimen vika,
'53'H	Ulkoisen GNSS-laitteiston viestintävika,
'54'H	Ei GNSS-laitteiston sijaintitietoja,
'55'H	GNSS-laitteiston havainnointiin kajoaminen,
'56'H	Ulkoisen GNSS-laitteiston varmenteen voimassaoloajan päättyminen,
'57'H to '5F'H	Varattu tulevaan käyttöön,

'6x'H	Etäviestintämoduuliin liittyvät viat,
'60'H	Ei lisätietoja,
'61'H	Etäviestintämoduuliin liittyvä vika,
'62'H	Etäviestintämoduulin viestintään liittyvä vika,
'63'H to '6F'H	Varattu tulevaan käyttöön,

'7x'H	ITS-järjestelmän rajapintaan liittyvät viat,
'70'H	Ei lisätietoja,
'71'H to '7F'H	Varattu tulevaan käyttöön

2.71. **ExtendedSealIdentifier**

Sukupolvi 2:

Laajennettu sinetin tunnus yksilöi sinetin täydellisesti (liitteen 1 C vaatimus 401).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode on sinetin valmistajan tunniste.

sealIdentifier on valmistajakohtainen tunniste sinetille.

2.72. **ExtendedSerialNumber**

Laitteen yksilöivä tunnus. Sitä voidaan käyttää myös laitteen julkisen avaimen tunnisteena.

Sukupolvi 1:

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

serialNumber on laitteen sarjanumero, joka täysin yksilöi tietyn valmistajan, laitetyypin ja alla määritellyn kuun ja vuoden.

monthYear on sen kuukauden ja vuoden tunniste, jolloin laite on valmistettu (tai jolloin sitä varten varattiin sarjanumero).

▼B

Asetettava arvo: kuukausi (kaksi numeroa) ja vuosi (kaksi viimeistä numeroa) binaarikoodatussa desimaalimuodossa (BCD).

type on laitetyypin tunniste.

Asetettava arvo: arvo määräytyy laitevalmistajan mukaan, arvo'FFh' on varattu muihin tarkoituksiin.

manufacturerCode on numerotunniste, jolla yksilöidään tyyppihyväksytyn laitteen valmistaja.

Sukupolvi 2:

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

serialNumber ks. sukupolvi 1

monthYear ks. sukupolvi 1

type ilmoittaa laitetyypin.

manufacturerCode ks. sukupolvi 1

2.73. **FullCardNumber**

Tunnus, joka yksilöi ajopiirturikortin täydellisesti.

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

cardType on ajopiirturikortin tyyppi.

cardIssuingMemberState on kortin myöntäneen jäsenvaltion tunnus.

cardNumber on kortin numero.

2.74. **FullCardNumberAndGeneration**

Sukupolvi 2:

Tunnus, joka yksilöi ajopiirturikortin ja sen sukupolven täydellisesti.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber yksilöi ajopiirturikortin.

generation yksilöi käytetyn ajopiirturikortin sukupolven.

▼B

2.75. **Generation**

Sukupolvi 2:

Yksilöi käytetyn ajopiirturin sukupolven.

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

Asetettava arvo:

‘00’H	Varattu tulevaan käyttöön
‘01’H	Sukupolvi 1
‘02’H	Sukupolvi 2
‘03’H ‘FF’H	Varattu tulevaan käyttöön

2.76. **GeoCoordinates**

Sukupolvi 2:

Maantieteelliset koordinaatit koodataan kokonaislukuina. Nämä kokonaisluvut ovat leveysasteen ± DDMM.M -koodauksen ja pituusasteen ± DDDMM.M -koodauksen kerrannaisia. Tässä ± DD ja vastaavasti ± DDD tarkoittavat asteita ja MM.M minuutteja.

```
GeoCoordinates ::= SEQUENCE {
   latitude                                INTEGER(-90000..90001),
   longitude                               INTEGER(-180000..180001)
}
```

latitude koodataan ± DDMM.M -koodauksen kerrannaisena (kerroin 10).

longitude koodataan ± DDDMM.M -koodauksen kerrannaisena (kerroin 10).

2.77. **GNSSAccuracy**

Sukupolvi 2:

GNSS-sijaintitietojen tarkkuus (määritelmä eee). Tämä tarkkuus on koodattu kokonaislukuna ja se on NMEA:n GSA- lausekkeen tarjoaman X.Y-arvon kerrannainen (kerroin 10).

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Sukupolvi 2:

Tiedot, jota on tallennettu kuljettaja- tai korjaamokortille ja jotka liittyvät ajoneuvon GNSS-sijaintiin, jos kuljettajan keskeytymätön ajoaika on yli kolmen tunnin jakso (liitteen 1 C vaatimus 306 ja 354).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord               INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords            SET SIZE(NoOfGNSSCDRecords) OF
                                           GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord on indeksi viimeksi päivitetylle keskeytymätöntä ajoaikaa koskevalle GNSS-tietueelle.

▼B

Asetettava arvo: numero, joka vastaa keskeytymätöntä ajoaikaa koskevan GNSS-tietueen järjestysnumeroa, alkaen numerosta ‘0’ ensimmäiselle keskeytymätöntä ajoaikaa koskevalle GNSS-tietueelle datarakenteessa.

gnssContinuousDrivingRecords on tietuesarja, johon sisältyy päivämäärä ja aika keskeytymättömästä ajosta, joka on yli kolmen tunnin jakso, ja tiedot ajoneuvon sijainnista.

2.79. **GNSSContinuousDrivingRecord**

Sukupolvi 2:

Tiedot, jota on tallennettu kuljettaja- tai korjaamokortille ja jotka liittyvät ajoneuvon GNSS-sijaintiin, jos kuljettajan keskeytymätön ajoaika on yli kolmen tunnin jakso (liitteen 1 C vaatimus 305 ja 353).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssPlaceRecord                          GNSSPlaceRecord
}
```

timeStamp on päivämäärä ja aika, jolloin kuljettajan keskeytymätön ajoaika on yli kolmen tunnin jakso.

gnssPlaceRecord sisältää tiedot ajoneuvon sijainnista.

2.80. **GNSSPlaceRecord**

Sukupolvi 2:

GNSS-järjestelmän määrittämään ajoneuvon paikannukseen liittyvät tiedot (liitteen 1 C vaatimus 108, 109, 110, 296, 305, 347, ja 353).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssAccuracy                             GNSSAccuracy,
   geoCoordinates                           GeoCoordinates
}
```

timeStamp on päivämäärä ja aika, jolloin ajoneuvon sijainti määritettiin GNSS-järjestelmällä.

gnssAccuracy on GNSS-järjestelmän sijaintitietojen tarkkuus.

geoCoordinates on GNSS-järjestelmää käyttäen tallennettu paikkatieto.

2.81. **HighResOdometer**

Ajoneuvon matkamittarin lukema: Kokonaismatka, jonka ajoneuvo on kulkenut tähänastisen käyttöikänsä aikana.

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

▼B

Asetettava arvo: etumerkitön binaariluku. Arvo kilometrin kahdessadasosina alueella 0–21 055 406 km.

2.82. **HighResTripDistance**

Yksittäisen matkan välimatkamittarilukema.

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

Asetettava arvo: etumerkitön binaariluku. Arvo kilometrin kahdessadasosina alueella 0–21 055 406 km.

2.83. **HolderName**

Kortin haltijan sukunimi ja etunimi (etunimet).

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

holderSurname on haltijan sukunimi. Sukunimeen ei sisällytetä titteleitä.

Asetettava arvo: jos kortti ei ole tarkoitettu henkilökohtaiseen käyttöön, holderSurname-tietue sisältää samat tiedot kuin companyName- tai workshopName- tai controlBodyName-tietueet.

holderFirstNames on haltijan etunimi (etunimet) ja etunimen alkukirjaimet.

2.84. **InternalGNSSReceiver**

Sukupolvi 2:

Tiedot siitä, onko GNSS-vastaanotin ajoneuvoyksikön sisä- tai ulkopuolella. Niiden tietojen oikeellisuus, että GNSS-vastaanotin on ajoneuvoyksikön sisäpuolella. Niiden tietojen virheellisyys, että GNSS-vastaanotin on yksikön ulkopuolella.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Valvontalaitteen vakio (määritelmä m).

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

Asetettava arvo: impulsseja kilometriä kohti alueella 0–64 255 impulssia/km.

2.86. **KeyIdentifier**

Julkisen avaimen täysin yksilöivä tunniste, jota käytetään avaimen viitetietona ja avaimen valinnassa. Se yksilöi myös avaimen haltijan.

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

▼B

Ensimmäinen vaihtoehto on sopiva ajoneuvoyksikön tai ajopiirturikortin julkisen avaimen tunnisteeksi.

Toinen vaihtoehto on sopiva ajoneuvoyksikön julkisen avaimen tunnisteeksi (tapauksissa, joissa ajoneuvoyksikön sarjanumero ei ole tiedossa silloin, kun varmenne luodaan).

Kolmas vaihtoehto on sopiva jäsenvaltion julkisen avaimen tunnisteeksi.

2.87. **KMWCKey**

Sukupolvi 2:

AES-avain ja siihen liittyvän avaimen versio, jota käytetään ajoneuvoyksikön liittämiseen liiketunnistimeen. Lisätietoja on lisäyksessä 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                                 AESKey,
   keyVersion                              INTEGER (SIZE(1))
}
```

kMWCKey on AES-avaimen pituus, joka ketjutetaan sen avaimen kanssa, jota käytetään ajoneuvoyksikön liittämiseen liiketunnistimeen.

keyVersion osoittaa AES-avaimen version.

2.88. **Language**

Kielen yksilöivä tunnus.

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

Asetettava arvo: ISO 639 -standardin mukainen merkintä kahdella pienellä kirjaimella.

2.89. **LastCardDownload**

Kuljettajakortille tallennettu viimeisimmän (muussa kuin valvontatarkoituksessa tehdyn) kortin tietojen kopioinnin päivämäärä ja aika; liitteen 1 C vaatimus 257 ja 282. Päivämäärä on päivitettävissä ajoneuvoyksiköstä tai mistä tahansa kortinlukulaitteesta.

```
LastCardDownload ::= TimeReal
```

Asetettava arvo: ei lisämäärittelyjä.

2.90. **LinkCertificate**

Sukupolvi 2:

Eurooppalaisten juuriavainparien välinen linkkivarmenne.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Pyörien renkaiden tehollinen ympärysmitta (määritelmä u).

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

▼B

Asetettava arvo: arvo millimetrin kahdeksasosina alueella 0–8 031 mm.

2.92. **MAC**

Sukupolvi 2:

Salauksen 8, 12 tai 16 tavun pituinen tarkistussumma, joka vastaa lisäyksessä 11 määriteltyjä salausohjelmia.

```
MAC ::= CHOICE {
   mac8                                    OCTET STRING (SIZE(8)),
   mac12                                   OCTET STRING (SIZE(12)),
   mac16                                   OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Erote, joka ilmaisee, onko kortin haltija kortin paikoilleen asettamisen yhteydessä syöttänyt kuljettajan toimintaa koskevia tietoja käsin (liitteen 1 B vaatimus 081 ja liitteen 1 C vaatimus 102).

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

Asetettava arvo: ei lisämäärittelyjä.

2.94. **ManufacturerCode**

Tyyppihyväksytyn laitteen valmistajan yksilöivä tunnus.

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

Yhteentoimivuustestit suorittamaan valtuutettu laboratorio ylläpitää ja julkaisee verkkosivustollaan valmistustunnusten luetteloa (liitteen 1 C vaatimus 454).

ManufacturerCodes-valmistustunnukset annetaan väliaikaisesti ajopiirturilaitteiden kehittäjille yhteentoimivuustestit suorittamaan valtuutetulle laboratoriolle toimitettua hakemusta vastaan.

2.95. **ManufacturerSpecificEventFaultData**

Sukupolvi 2:

Valmistajakohtaiset virhekoodit yksinkertaistavat virheanalyysiä ja ajoneuvoyksikköjen huoltoa.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                        ManufacturerCode,
   manufacturerSpecificErrorCode           OCTET STRING(SIZE(3))
}
```

manufacturerCode yksilöi ajoneuvoyksikön valmistajan.

manufacturerSpecificErrorCode on valmistajakohtainen virhekoodi.

▼B

2.96. **MemberStateCertificate**

Eurooppalaisen varmenneviranomaisen myöntämä jäsenvaltion julkisen avaimen varmenne.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Sukupolvi 2:

Jäsenvaltion varmenne ja metadata, siten kuin sitä käytetään kopiointiprotokollassa.

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

recordType osoittaa tietueen tyypin (MemberStateCertificate). **Asetettava arvo**: ks. RecordType

recordSize on MemberStateCertificate-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä. Arvoksi asetetaan 1, koska varmenteilla voi olla erilaiset pituudet.

records on sarja jäsenvaltion varmenteita.

2.98. **MemberStatePublicKey**

Sukupolvi 1:

Jäsenvaltion julkinen avain.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Nimi.

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

codePage määrittää 4 luvussa määritellyn merkistön.

name on määritetyn merkistön avulla koodattu nimi.

2.100. **NationAlpha**

Maan kirjainlyhenteen on vastattava kansainvälisen liikenteen ajoneuvoissa käytettyjä kansainvälisiä tunnuksia (tieliikennettä koskeva Yhdistyneiden kansakuntien Wienin yleissopimus, 1968).

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

Maan kirjaintunnus ja numerotunnukset on pidettävä liitteen 1 C vaatimuksen 440 mukaisesti yhteentoimivuustestauksen suorittamaan valitun laboratorion verkkosivustolla.

▼B

2.101. **NationNumeric**

Maan numeroviite.

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

Asetettava arvo: ks. datatyyppi 2.100 (NationAlpha).

Edellä olevassa kohdassa kuvattuihin maan kirjaintunnukseen tai numerotunnukseen saa tehdä muutoksia tai päivityksiä vasta sen jälkeen, kun valittu laboratorio on saanut tyyppihyväksytyn digitaalisen ja älykkään ajopiirturin ajoneuvoyksikön valmistajien näkemykset.

2.102. **NoOfCalibrationRecords**

Korjaamokortille mahtuvien kalibrointitietoja sisältävien tietueiden määrä.

Sukupolvi 1:

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

Asetettava arvo: ks. lisäys 2.

Sukupolvi 2:

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

Asetettava arvo: ks. lisäys 2.

2.103. **NoOfCalibrationsSinceDownload**

Laskuri, joka osoittaa korjaamokortilla suoritettujen kalibrointien määrän sen jälkeen, kun kortin tietoja on viimeksi kopioitu (liitteen 1 C vaatimus 317 ja 340).

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

Asetettava arvo: ei lisämäärittelyjä.

2.104. **NoOfCardPlaceRecords**

Kuljettaja- tai korjaamokortille mahtuvien paikkaan liittyviä tietoja sisältävien tietueiden määrä.

Sukupolvi 1:

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

Asetettava arvo: ks. lisäys 2.

Sukupolvi 2:

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

Asetettava arvo: ks. lisäys 2.

▼B

2.105. **NoOfCardVehicleRecords**

Kuljettaja- tai korjaamokortille mahtuvien käytössä olleisiin ajoneuvoihin liittyviä tietoja sisältävien tietueiden määrä.

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

Asetettava arvo: ks. lisäys 2.

2.106. **NoOfCardVehicleUnitRecords**

Sukupolvi 2:

Kuljettaja- tai korjaamokortille mahtuvien käytössä olleisiin ajoneuvoyksikköihin liittyviä tietoja sisältävien tietueiden määrä.

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

Asetettava arvo: ks. lisäys 2.

2.107. **NoOfCompanyActivityRecords**

Yrityskortille mahtuvien yrityksen toimiin liittyviä tietoja sisältävien tietueiden määrä.

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

Asetettava arvo: ks. lisäys 2.

2.108. **NoOfControlActivityRecords**

Valvontakortille mahtuvien tarkastustoimiin liittyviä tietoja sisältävien tietueiden määrä.

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

Asetettava arvo: ks. lisäys 2.

2.109. **NoOfEventsPerType**

Kortille mahtuvien tapahtumatyyppikohtaisiin tapahtumien lukumääriin liittyviä tietoja sisältävien tietueiden määrä.

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

Asetettava arvo: ks. lisäys 2.

2.110. **NoOfFaultsPerType**

Kortille mahtuvien vikatyyppikohtaisiin vikatapahtumien lukumääriin liittyviä tietoja sisältävien tietueiden määrä.

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

Asetettava arvo: ks. lisäys 2.

▼B

2.111. **NoOfGNSSCDRecords**

Sukupolvi 2:

Kortille tallennettavissa olevien keskeytymätöntä ajoaikaa koskevien GNSS-tietueiden määrä.

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

Asetettava arvo: ks. lisäys 2.

2.112. **NoOfSpecificConditionRecords**

Sukupolvi 2:

Kortille tallennettavissa olevien erityisolosuhteisiin liittyvien tietueiden määrä.

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

Asetettava arvo: ks. lisäys 2.

2.113. **OdometerShort**

Ajoneuvon matkamittarin lukema lyhyessä muodossa.

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

Asetettava arvo: etumerkitön binaariluku. Arvo kilometreinä alueella 0–9 999 999km.

2.114. **OdometerValueMidnight**

Ajoneuvon matkamittarin lukema keskiyöllä tiettynä päivänä (liitteen 1 B vaatimus 090 ja liitteen 1 C vaatimus 113).

```
OdometerValueMidnight ::= OdometerShort
```

Asetettava arvo: ei lisämäärittelyjä.

2.115. **OdometerValueMidnightRecordArray**

Sukupolvi 2:

OdometerValueMidnight ja kopiointiprotokollassa käytetty metadata.

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

recordType osoittaa tietueen tyypin (OdometerValueMidnight). **Asetettava arvo**: ks. RecordType

recordSize on OdometerValueMidnight-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja OdometerValueMidnight-tietueita.

▼B

2.116. **OverspeedNumber**

Ylinopeustapahtumien määrä viimeksi suoritetun ylinopeustarkastuksen jälkeen.

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

Asetettava arvo: 0 tarkoittaa, ettei viimeksi suoritetun ylinopeustarkastuksen jälkeen ole sattunut ylinopeustapauksia, 1 tarkoittaa, että viimeksi suoritetun ylinopeustarkastuksen jälkeen on sattunut yksi ylinopeustapaus … 255 tarkoittaa, että viimeksi suoritetun ylinopeustarkastuksen jälkeen on sattunut 255 tai useampia ylinopeustapauksia.

2.117. **PlaceRecord**

Tiedot, jotka liittyvät paikkaan, jossa päivän työaika alkaa tai päättyy (liitteen 1 C vaatimus 108, 271, 296, 324, ja 347).

Sukupolvi 1:

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

entryTime on syötettyyn tietoon liittyvä päivämäärä ja aika.

entryTypeDailyWorkPeriod on syötetyn tiedon tyyppi.

dailyWorkPeriodCountry on syötetty maatieto.

dailyWorkPeriodRegion on syötetty aluetieto.

vehicleOdometerValue on matkamittarin lukema silloin, kun paikkaan liittyvä tieto syötettiin.

Sukupolvi 2:

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

Sukupolven 1 arvojen lisäksi käytetään seuraavaa komponenttia:

entryGNSSPlaceRecord on tallennettu paikka- ja aikatieto.

▼B

2.118. **PreviousVehicleInfo**

Tiedot, jotka liittyvät ajoneuvoon, jota kuljettaja käytti asettaessaan edellisen kerran kuljettajakorttinsa ajoneuvoyksikköön (liitteen 1 B vaatimus 081 ja liitteen 1 C vaatimus 102).

Sukupolvi 1:

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

vehicleRegistrationIdentification on ajoneuvon rekisteritunnus ja ajoneuvon rekisteröinyt jäsenvaltio.

cardWithdrawalTime on päivämäärä ja aika, jolloin kortti poistettiin.

Sukupolvi 2:

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

Sukupolven 1 arvojen lisäksi käytetään seuraavaa dataelementtiä:

vuGeneration yksilöi ajoneuvoyksikön sukupolven.

2.119. **PublicKey**

Sukupolvi 1:

Julkinen RSA-avain.

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

rsaKeyModulus on avainparin kongruenssimoduuli.

rsaKeyPublicExponent on avainparin julkinen eksponentti.

2.120. **RecordType**

Sukupolvi 2:

Viitaus tietuetyyppiin. Tätä datatyyppiä käytetään RecordArrays-tietueessa.

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

▼B

Asetettava arvo:

‘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	VuDownloadablePeriod,
‘15’H	VuDownloadablePeriod,
‘16’H	VuDownloadablePeriod,
‘17’H	VuDownloadablePeriod,
‘18’H	VuDownloadablePeriod,
‘19’H	VuDownloadablePeriod,
‘1A’H	VehicleRegistrationNumber,
‘1B’H	VehicleRegistrationNumber,
‘1C’H	VuCertificate,
‘1D’H	VuTimeAdjustmentGNSSRecord,
‘1E’H	VuTimeAdjustmentRecord,
‘1F’H	VuPowerSupplyInterruptionRecord,
‘20’H	SensorPairedRecord,
‘21’H	SensorExternalGNSSCoupledRecord,
‘22’H to ‘7F’H	Varattu tulevaan käyttöön,
‘80’H to ‘FF’H	Arvo määräytyy laitevalmistajan mukaan

2.121. **RegionAlpha**

Tietyn maan alueen kirjainviite.

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

Sukupolvi 1:

Asetettava arvo:

‘ ’	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

▼B

Sukupolvi 2:

RegionAlpha -tunnukset on pidettävä yhteentoimivuustestauksen suorittamaan valitun laboratorion verkkosivustolla olevassa luettelossa.

2.122. **RegionNumeric**

Tietyn valtion alueen numeroviite.

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

Sukupolvi 1:

Asetettava arvo:

```
'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
```

Sukupolvi 2:

RegionNumeric -tunnukset on pidettävä yhteentoimivuustestauksen suorittamaan valitun laboratorion verkkosivustossa olevassa luettelossa.

2.123. **RemoteCommunicationModuleSerialNumber**

Sukupolvi 2:

Etäviestintämoduulin sarjanumero.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Sukupolvi 1:

RSA-avainparin kongruenssimoduuli.

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

Asetettava arvo: määrittelemätön.

2.125. **RSAKeyPrivateExponent**

Sukupolvi 1:

RSA-salauksessa käytettävän avainparin salainen eksponentti.

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

Asetettava arvo: määrittelemätön.

▼B

2.126. **RSAKeyPublicExponent**

Sukupolvi 1:

RSA-salauksessa käytettävän avainparin julkinen eksponentti

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

Asetettava arvo: määrittelemätön.

2.127. **RtmData**

Sukupolvi 2:

Ks. tämän datatyypin määritelmästä lisäys 14.

2.128. **SealDataCard**

Sukupolvi 2:

Tämä datatyyppi tallentaa tietoja sinetöinneistä, jotka on liitetty ajoneuvon eri osiin, ja se on tarkoitettu tallennukseen kortille. Tämä datatyyppi liittyy liitteen 1 C vaatimukseen 337.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords on sealRecords -tietuesarjaan tallennettujen tietueiden määrä.

sealRecords on sarja sinetöinteihin liittyviä tietueita.

2.129. **SealDataVu**

Sukupolvi 2:

Tämä datatyyppi tallentaa tietoja sinetöinneistä, jotka on liitetty ajoneuvon eri osiin, ja se on tarkoitettu tallennukseen ajoneuvoyksikössä.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords on sarja sinetöinteihin liittyviä tietueita. Jos käytössä on alle 5 sinetöintiä, EquipmentType -arvo kaikissa käyttämättömissä sealRecords -tietusarjoissa asetetaan arvoon 16, eli käyttämätön.

2.130. **SealRecord**

Sukupolvi 2:

Tämä datatyyppi tallentaa tietoa sinetöinnistä, joka on liitetty ajoneuvon osaan. Tämä datatyyppi liittyy liitteen 1 C vaatimukseen 337.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType yksilöi sen laitetyypin, johon sinetöinti liitetään.

extendedSealIdentifier on laitteeseen liitetyn sinetöinnin tunniste.

▼B

2.131. **SensorApprovalNumber**

Liiketunnistimen tyyppihyväksyntänumero.

Sukupolvi 1:

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

Asetettava arvo: määrittelemätön.

Sukupolvi 2:

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

Asetettava arvo:

hyväksyntänumero annetaan sellaisena kuin se julkaistaan Euroopan komission vastaavalla verkkosivustolla, mukaan lukien mahdolliset yhdysviivat. Hyväksyntänumero on tasattu vasemmalle.

2.132. **SensorExternalGNSSApprovalNumber**

Sukupolvi 2:

Ulkoisen GNSS-laitteiston tyyppihyväksyntänumero.

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

Asetettava arvo:

hyväksyntänumero annetaan sellaisena kuin se julkaistaan Euroopan komission vastaavalla verkkosivustolla, mukaan lukien mahdolliset yhdysviivat. Hyväksyntänumero on tasattu vasemmalle.

2.133. **SensorExternalGNSSCoupledRecord**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajoneuvoyksikköön liitetyn ulkoisen GNSS-laitteiston tunnistamiseen (liitteen 1 C vaatimus 100).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber on ulkoiseen GNSS-laitteeseen kytketyn liiketunnistimen sarjanumero.

sensorSerialNumber on tämän ulkoisen GNSS-laitteiston hyväksyntänumero.

sensorCouplingDate on päivämäärä, jolloin ulkoinen GNSS-laitteisto kytkettiin ajoneuvoyksikköön.

2.134. **SensorExternalGNSSIdentification**

Sukupolvi 2:

Tiedot, jotka liittyvät ulkoisen GNSS-laitteiston tunnistukseen (liitteen 1 C vaatimus 98).

▼B

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorGNSSSerialNumber,
   sensorApprovalNumber                  SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                    SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                    SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber on ulkoisen GNSS-laitteiston sarjanumero pitkässä muodossa.

sensorSerialNumber on ulkoisen GNSS-laitteiston hyväksyntänumero.

sensorSCIdentifier on ulkoisen GNSS-laitteiston turvakomponentin tunniste.

sensorOSIdentifier on ulkoisen GNSS-laitteiston käyttöjärjestelmän tunniste.

2.135. **SensorExternalGNSSInstallation**

Sukupolvi 2:

Ulkoiseen GNSS-laitteistoon tallennetut tiedot, jotka liittyvät ulkoisen GNSS-laitteiston tunnistimen asentamiseen (liitteen 1 C vaatimus 123).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst               SensorGNSSCouplingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorCouplingDateCurrent             SensorGNSSCouplingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorCouplingDateFirst on päivämäärä, jolloin ulkoinen GNSS-laitteisto ensimmäisen kerran liitettiin ajoneuvoyksikköön.

firstVuApprovalNumber on ensimmäisen ajoneuvoyksikön hyväksyntänumero, johon ulkoinen GNSS-laitteisto kytkettiin.

firstVuSerialNumber on ensimmäisen ajoneuvoyksikön sarjanumero, johon ulkoinen GNSS-laitteisto liitettiin.

sensorCouplingDateCurrent on päivämäärä, jolloin tällä hetkellä ajoneuvoyksikköön kytketty GNSS-laitteisto kytkettiin siihen.

currentVuApprovalNumber on sen ajoneuvoyksikön hyväksyntänumero, johon ulkoinen GNSS-laitteisto on tällä hetkellä kytketty.

currentVUSerialNumber on sen ajoneuvoyksikön sarjanumero, johon ulkoinen GNSS-laitteisto on tällä hetkellä kytketty.

▼B

2.136. **SensorExternalGNSSOSIdentifier**

Sukupolvi 2:

Ulkoisen GNSS-laitteiston käyttöjärjestelmän tunniste.

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

Asetettava arvo: arvo määräytyy laitevalmistajan mukaan.

2.137. **SensorExternalGNSSSCIdentifier**

Sukupolvi 2:

Tätä tyyppiä käytetään muun muassa tunnistamaan ulkoisen GNSS-laitteiston salausmoduuli.

Ulkoisen GNSS-laitteiston turvakomponentin tunniste.

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

Asetettava arvo: arvo määräytyy komponentin valmistajan mukaan.

2.138. **SensorGNSSCouplingDate**

Sukupolvi 2:

Päivämäärä, jolloin ulkoinen GNSS-laitteisto kytkettiin ajoneuvoyksikköön.

```
SensorGNSSCouplingDate ::= TimeReal
```

Asetettava arvo: määrittelemätön.

2.139. **SensorGNSSSerialNumber**

Sukupolvi 2:

Tätä tyyppiä käytetään tallentamaan GNSS-vastaanottimen sarjanumero silloin kun se sijaitsee ajoneuvoyksikön sisällä ja silloin, kun se on sen ulkopuolella.

GNSS-vastaanottimen sarjanumero.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Liiketunnistimeen tallennetut tiedot, jotka liittyvät liiketunnistimen tunnistukseen (liitteen 1 B vaatimus 077 ja liitteen 1 C vaatimus 95).

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

sensorSerialNumber on liiketunnistimen sarjanumero pitkässä muodossa (sisältää osanumeron ja valmistustunnuksen).

sensorApprovalNumber on liiketunnistimen hyväksyntänumero.

sensorSCIdentifier on liiketunnistimen turvakomponentin tunniste.

▼B

sensorOSIdentifier on liiketunnistimen käyttöjärjestelmän tunniste.

2.141. **SensorInstallation**

Liiketunnistimeen tallennetut tiedot, jotka liittyvät liiketunnistimen asentamiseen (liitteen 1 B vaatimus 099 ja liitteen 1 C vaatimus 122).

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

sensorPairingDateFirst on päivämäärä, jolloin liiketunnistin ensimmäisen kerran liitettiin ajoneuvoyksikköön.

firstVuApprovalNumber on ensimmäisen liiketunnistimeen liitetyn ajoneuvoyksikön hyväksyntänumero.

firstVuSerialNumber on ensimmäisen liiketunnistimeen liitetyn ajoneuvoyksikön sarjanumero.

sensorPairingDateCurrent on päivämäärä, jolloin liiketunnistin ensimmäisen kerran liitettiin nykyiseen ajoneuvoyksikköön.

currentVuApprovalNumber on liiketunnistimeen nykyisin liitetyn ajoneuvoyksikön hyväksyntänumero.

currentVUSerialNumber on liiketunnistimeen nykyisin liitetyn ajoneuvoyksikön sarjanumero.

2.142. **SensorInstallationSecData**

Korjaamokortille tallennetut tiedot, jotka liittyvät niihin turvatietoihin, joita tarvitaan liitettäessä liiketunnistin ajoneuvoyksikköön (liitteen 1 C vaatimus 308 ja 331).

Sukupolvi 1:

```
SensorInstallationSecData ::= TdesSessionKey
```

Asetettava arvo: standardin ISO 16844-3 mukaisesti.

Sukupolvi 2:

Kuten lisäyksessä 11a esitettiin, korjaamokortti tallentaa enintään kolme avainta ajoneuvoyksikön liiketunnistimen liitäntää varten. Näillä avaimilla on eri avaimen versiot.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

▼B

2.143. **SensorOSIdentifier**

Liiketunnistimen käyttöjärjestelmän tunniste.

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

Asetettava arvo: arvo määräytyy laitevalmistajan mukaan.

2.144. **SensorPaired**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajoneuvoyksikköön liitettyyn liiketunnistimeen (liitteen 1 B vaatimus 079).

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

sensorSerialNumber on ajoneuvoyksikköön nykyisin liitetyn liiketunnistimen sarjanumero.

sensorApprovalNumber on ajoneuvoyksikköön nykyisin liitetyn liiketunnistimen hyväksyntänumero.

sensorPairingDateFirst on päivämäärä, jolloin liiketunnistin ensimmäistä kertaa liitettiin ajoneuvoyksikköön, johon se nykyisin on liitetty.

2.145. **SensorPairedRecord**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajoneuvoyksikköön liitettyyn liiketunnistimeen (liitteen 1 C vaatimus 97).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDate                     SensorPairingDate
}
```

sensorSerialNumber on ajoneuvoyksikköön liitetyn liiketunnistimen sarjanumero.

sensorApprovalNumber on tämän liiketunnistimen hyväksyntänumero.

sensorPairingDate on päivämäärä, jolloin tämä liiketunnistin liitettiin ajoneuvoyksikköön.

2.146. **SensorPairingDate**

Päivämäärä, jolloin liiketunnistin liitettiin ajoneuvoyksikköön.

```
SensorPairingDate ::= TimeReal
```

Asetettava arvo: määrittelemätön.

▼B

2.147. **SensorSCIdentifier**

Liiketunnistimen turvakomponentin tunniste.

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

Asetettava arvo: arvo määräytyy komponentin valmistajan mukaan.

2.148. **SensorSerialNumber**

Liiketunnistimen sarjanumero.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Digitaalinen allekirjoitus.

Sukupolvi 1:

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

Asetettava arvo: lisäyksen 11 (Yhteiset turvamekanismit) mukaisesti.

Sukupolvi 2:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Asetettava arvo: lisäyksen 11 (Yhteiset turvamekanismit) mukaisesti.

2.150. **SignatureRecordArray**

Sukupolvi 2:

Sarja signatures-tietueita ja kopiointiprotokollassa käytetty metadata.

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

recordType osoittaa tietueen tyypin (Signature). **Asetettava arvo**: ks. RecordType

recordSize on Signature-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä. Arvoksi asetetaan 1, koska signature-tietueilla voi olla erilaiset pituudet.

records on sarja signatures-tietueita.

2.151. **SimilarEventsNumber**

Tiettynä päivänä sattuneiden vastaavien tapahtumien määrä (liitteen 1 B vaatimus 094 ja liitteen 1 C vaatimus 117).

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

Asetettava arvo: arvoa 0 ei käytetä, 1 tarkoittaa, että kyseisenä päivänä on sattunut ja tallennettu yksi kyseisentyyppinen tapahtuma, 2 tarkoittaa, että kyseisenä päivänä on sattunut kaksi kyseisentyyppistä tapahtumaa (vain yksi on tallennettu), … 255 tarkoittaa, että kyseisenä päivänä on sattunut 255 tai useampia kyseisentyyppisiä tapahtumia.

▼B

2.152. **SpecificConditionRecord**

Kuljettajakortille, korjaamokortille tai ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät erityisolosuhteeseen (liitteen 1 C vaatimus130, 276, 301, 328 ja 355).

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

entryTime on päivämäärä ja aika, jolloin tieto syötettiin.

specificConditionType on tunnus, joka yksilöi erityisolosuhteet.

2.153. **SpecificConditions**

Kuljettajakortille, korjaamokortille tai ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät erityisolosuhteeseen (liitteen 1 C vaatimus 131, 277, 302, 329 ja 356).

Sukupolvi 2:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord         INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords             SET SIZE(NoOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

conditionPointerNewestRecord on viimeksi päivitetyn erityisolosuhteeseen liittyvän tietueen järjestysnumero.

Asetettava arvo: numero, joka vastaa erityisolosuhteeseen liittyvän tietueen järjestysnumeroa, alkaen numerosta ‘0’ ensimmäiselle erityisolosuhteeseen liittyvälle tietueelle datarakenteessa.

specificConditionRecords on sarja tietueita, jotka sisältävät kirjattuihin erityisolosuhteisiin liittyviä tietoja.

2.154. **SpecificConditionType**

Erityisolosuhteen yksilöivä tunnus (liitteen 1 B vaatimus 050b, 105a, 212a ja 230a sekä liitteen 1 C vaatimus 62).

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

Sukupolvi 1:

Asetettava arvo:

‘00’H	Varattu tulevaan käyttöön
‘01’H	Asetuksen piiriin kuulumaton – alku
‘02’H	Asetuksen piiriin kuulumaton – loppu
‘03’H	Lautta-/junakuljetus
‘04’H … ‘FF’H	Varattu tulevaan käyttöön

Sukupolvi 2:

Asetettava arvo:

‘00’H	Varattu tulevaan käyttöön
‘01’H	Asetuksen piiriin kuulumaton – alku
‘02’H	Asetuksen piiriin kuulumaton – loppu
‘03’H	Lautta-/junakuljetus – alku
‘04’H	Lautta-/junakuljetus – loppu
‘05’H … ‘FF’H	Varattu tulevaan käyttöön

▼B

2.155. **Speed**

Ajoneuvon nopeus (km/t).

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

Asetettava arvo: kilometreinä tunnissa alueella 0–220 km/t.

2.156. **SpeedAuthorised**

Ajoneuvon suurin sallittu nopeus (määritelmä hh).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Keskimääräinen nopeus aiemmin määritellyn jakson aikana (km/t).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Suurin nopeus aiemmin määritellyn jakson aikana.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Sukupolvi 2:

Tämän datatyypin määritelmä, ks. lisäys 14.

2.160. **TachographPayloadEncrypted**

Sukupolvi 2:

DER-TLV-koodattu salattu ajopiirturin hyötydata, eli data lähetetään salattuna RTM-viestissä. Lisätietoja salauksesta, ks. lisäyksessä 11 olevan B osan 13 kappale.

```
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 osa DER-TLV-koodausta, ja arvoksi on asetettava ‘87’ (ks. lisäyksessä 11 olevan B osan 13 kappale).

length on osa DER-TLV-koodausta ja se koodaa seuraavien paddingContentIndicatorByte- ja encryptedData -tietojen pituuden.

paddingContentIndicatorByte-arvoksi on asetettava ‘00’.

encryptedData on salattu tachographPayload, kuten määritellään lisäyksen 11 B osassa oleva 13 kappale. Näiden tietojen pituus oktetteina on aina jaollinen 16:lla.

2.161. **TDesSessionKey**

Sukupolvi 1:

Kolminkertaisessa DES-salauksessa käytettävä avain.

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

Asetettava arvo: ei lisämäärittelyjä.

▼B

2.162. **TimeReal**

Tunnus yhdistetyssä päivämäärä- ja aikakentässä, jossa päivämäärä ja aika ilmaistaan ajan kello 00:00:00 1. tammikuuta 1970 jälkeen kuluneina sekunteina (GMT).

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

Asetettava arvo — Octet Aligned (tavuittain ryhmitelty): keskiyön 1. tammikuuta 1970 (GMT) jälkeen kuluneiden sekuntien määrä.

Viimeinen mahdollinen päivämäärä/aika on vuonna 2106.

2.163. **TyreSize**

Rengaskoon merkintä.

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

Asetettava arvo: direktiivin 92/23 (ETY) mukaisesti, EYVL L 129, 31.3.1992, s. 95.

2.164. **VehicleIdentificationNumber**

Ajoneuvon valmistenumero (VIN), joka viittaa koko ajoneuvoon, yleensä korin sarjanumero.

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

Asetettava arvo: kuten standardissa ISO 3779 on määritelty.

2.165. **VehicleIdentificationNumberRecordArray**

Sukupolvi 2:

Ajoneuvon tunnistenumero ja metadata, siten kuin sitä käytetään kopiointiprotokollassa.

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

recordType osoittaa tietueen tyypin (VehicleIdentificationNumber).
Asetettava arvo: ks. RecordType

recordSize on VehicleIdentificationNumber-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja ajoneuvon tunnistenumeroita.

2.166. **VehicleRegistrationIdentification**

Ajoneuvon tunniste, joka yksilöi eurooppalaisen ajoneuvon (rekisteritunnus ja jäsenvaltio).

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

vehicleRegistrationNation on valtio, jossa ajoneuvo on rekisteröity.

▼B

vehicleRegistrationNumber on ajoneuvon rekisteritunnus (VRN).

2.167. **VehicleRegistrationNumber**

Ajoneuvon rekisteritunnus (VRN). Rekisteritunnuksen antaa ajoneuvojen rekisteröinnistä vastaava viranomainen.

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

codePage määrittää 4 luvussa määritellyn merkistön,

vehicleRegNumber on määritetyn merkistön avulla koodattu ajoneuvon rekisteritunnus.

Asetettava arvo: rekisteröintimaan mukaan.

2.168. **VehicleRegistrationNumberRecordArray**

Sukupolvi 2:

Ajoneuvon rekisteritunnus ja metadata, siten kuin sitä käytetään kopiointiprotokollassa.

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

recordType osoittaa tietueen tyypin (VehicleRegistrationNumber). **Asetettava arvo**: ks. RecordType

recordSize on VehicleRegistrationNumber-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja ajoneuvon rekisterinumeroita.

2.169. **VuAbility**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot siitä, voiko ajoneuvoyksikkö käyttää sukupolven 1 ajopiirturikortteja (liitteen 1 C vaatimus 121).

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

Asetettava arvo — Octet Aligned (tavuittain ryhmitelty): ‘xxxxxxxa’B (8 bitti)

Tuetaanko sukupolven 1 korttien käyttöä:

‘a’B	Pystytäänkö sukupolven 1 ajopiirturikortteja tukemaan:
	‘0’ B sukupolven 1 kortteja tuetaan,
	‘1’ B sukupolven 1 kortteja ei tueta,
‘xxxxxxx’B	varattu tulevaan käyttöön.

▼B

2.170. **VuActivityDailyData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät toiminnan tyypin muutoksiin ja/tai ajoneuvon miehityksen muutoksiin ja/tai kortin tilan muutoksiin tietyn kalenterivuorokauden aikana (liitteen 1 B vaatimus 084 ja liitteen 1 C vaatimus 105, 106, 107) ja korttiaukkojen tilaan kyseisenä päivänä klo 00.00.

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

noOfActivityChanges on activityChangeInfos-sarjassa olevien ActivityChangeInfo-sanojen määrä.

activityChangeInfos on ajoneuvoyksikköön tallennettu tiettyä päivää koskeva ActivityChangeInfo-sanojen sarja. Se sisältää aina kaksi ActivityChangeInfo-sanaa, jotka ilmaisevat kummankin korttiaukon tilan kyseisenä päivänä klo 00.00.

2.171. **VuActivityDailyRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät toiminnan tyypin muutoksiin ja/tai ajoneuvon miehityksen muutoksiin ja/tai kortin tilan muutoksiin tietyn kalenterivuorokauden aikana (liitteen 1 C vaatimus 105, 106, 107) ja korttiaukkojen tilaan kyseisenä päivänä klo 00.00.

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

recordType osoittaa tietueen tyypin (ActivityChangeInfo). **Asetettava arvo**: ks. RecordType

recordSize on ActivityChangeInfo-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on ajoneuvoyksikköön tallennettu tiettyä päivää koskeva ActivityChangeInfo-sanojen sarja. Se sisältää aina kaksi ActivityChangeInfo-sanaa, jotka ilmaisevat kummankin korttiaukon tilan kyseisenä päivänä klo 00.00.

2.172. **VuApprovalNumber**

Ajoneuvoyksikön tyyppihyväksyntänumero.

Sukupolvi 1:

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

Asetettava arvo: määrittelemätön.

Sukupolvi 2:

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

▼B

Asetettava arvo:

hyväksyntänumero annetaan sellaisena kuin se julkaistaan Euroopan komission vastaavalla verkkosivustolla, mukaan lukien mahdolliset yhdysviivat. Hyväksyntänumero on tasattu vasemmalle.

2.173. **VuCalibrationData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät valvontalaitteen kalibrointeihin (liitteen 1 B vaatimus 098).

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

noOfVuCalibrationRecords on vuCalibrationRecords-tietuesarjan sisältämien tietueiden määrä.

vuCalibrationRecords on sarja kalibrointeihin liittyviä tietueita.

2.174. **VuCalibrationRecord**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät valvontalaitteen kalibrointiin (liitteen 1 B vaatimus 098 ja liitteen 1 C vaatimus 119 ja 120).

Sukupolvi 1:

```
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 syy, jonka vuoksi kalibrointi suoritettiin.

workshopName, workshopAddress ovat korjaamon nimi ja osoite.

workshopCardNumber yksilöi kalibroinnin aikana käytetyn korjaamokortin.

workshopCardExpiryDate on kortin viimeinen voimassaolopäivä.

vehicleIdentificationNumber on ajoneuvon valmistenumero (VIN).

▼B

vehicleRegistrationIdentification sisältää ajoneuvon rekisteritunnuksen (VRN) ja sen rekisteröineen jäsenvaltion.

wVehicleCharacteristicConstant on ajoneuvon ominaiskerroin.

kConstantOfRecordingEquipment on valvontalaitteen vakio.

lTyreCircumference on pyörien renkaiden tehollinen ympärysmitta.

tyreSize on ajoneuvoon asennettujen renkaiden kokomerkintä.

authorisedSpeed on ajoneuvon suurin sallittu nopeus.

oldOdometerValue, newOdometerValue ovat matkamittarin vanha ja uusi lukema.

oldTimeValue, newTimeValue ovat päivämäärän ja ajan vanhat ja uudet arvot.

nextCalibrationDate on päivämäärä, jolloin valtuutetun tarkastusviranomaisen on suoritettava seuraava CalibrationPurpose-muuttujan määrittelemä kalibrointi.

Sukupolvi 2:

```
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
}
```

Sukupolven 1 arvojen lisäksi käytetään seuraavaa dataelementtiä:

sealDataVu antaa tietoa sinetöinneistä, jotka on liitetty ajoneuvon eri osiin.

2.175. **VuCalibrationRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät valvontalaitteen kalibrointeihin (liitteen 1 C vaatimus 119 ja 120).

▼B

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

recordType osoittaa tietueen tyypin (VuCalibrationRecord). **Asetettava arvo**: ks. RecordType

recordSize on VuCalibrationRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja kalibrointitietueita.

2.176. **VuCardIWData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät kuljettaja- tai korjaamokorttien ajoneuvoyksikköön asettamis- ja poistojaksoihin (liitteen 1 B vaatimus 081 ja liitteen 1 C vaatimus 103).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords on vuCardIWRecords-tietuesarjassa olevien tietueiden määrä.

vuCardIWRecords on sarja tietueita, jotka liittyvät kortin paikoilleen asettamis- ja poistojaksoihin.

2.177. **VuCardIWRecord**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät kuljettaja- tai korjaamokortin ajoneuvoyksikköön asettamis- ja poistojaksoon (liitteen 1 B vaatimus 081 ja liitteen 1 C vaatimus 102).

Sukupolvi 1:

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

cardHolderName on kuljettaja- tai korjaamokortin haltijan sukunimi ja etunimet siinä muodossa kuin ne on tallennettu kortille.

fullCardNumber on kortin tyyppi, sen myöntänyt jäsenvaltio sekä kortin numero siinä muodossa kuin ne on tallennettu kortille.

▼B

cardExpiryDate on kortin viimeinen voimassaolopäivä siinä muodossa kuin se on tallennettu kortille.

cardInsertionTime on päivämäärä ja aika, jolloin kortti asetettiin paikoilleen.

vehicleOdometerValueAtInsertion on ajoneuvon matkamittarin lukema silloin, kun kortti asetettiin paikoilleen.

cardSlotNumber on korttiaukko, johon kortti asetettiin.

cardWithdrawalTime on päivämäärä ja aika, jolloin kortti poistettiin.

vehicleOdometerValueAtWithdrawal on ajoneuvon matkamittarin lukema silloin, kun kortti poistettiin.

previousVehicleInfo sisältää tietoja edellisestä kuljettajan käyttämästä ajoneuvosta siinä muodossa kuin ne on tallennettu kortille.

manualInputFlag on erote, joka ilmaisee, onko kortin haltija kortin paikoilleen asettamisen yhteydessä syöttänyt kuljettajan toimintaa koskevia tietoja käsin.

Sukupolvi 2:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

Sukupolven 2 datarakenne käyttää fullCardNumber-tietueen sijasta seuraavaa datarakennetta.

fullCardNumberAndGeneration on kortin tyyppi, sen myöntänyt jäsenvaltio sekä kortin numero ja sukupolvi siinä muodossa kuin ne on tallennettu kortille.

2.178. **VuCardIWRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät kuljettaja- tai korjaamokorttien ajoneuvoyksikköön asettamis- ja poistojaksoihin (liitteen 1 C vaatimus 103).

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

recordType osoittaa tietueen tyypin (VuCardIWRecord). **Asetettava arvo**: ks. RecordType

recordSize on VuCardIWRecord-tietueen koko tavuina.

▼B

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja tietueita, jotka liittyvät kortin paikoilleen asettamis- ja poistojaksoihin.

2.179. **VuCardRecord**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät käytettyyn ajopiirturikorttiin (liitteen 1 C vaatimus 132).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber luettuna kortin MF-tiedoston EF_ICC-tiedostosta.

cardPersonaliserID luettuna kortin MF-tiedoston EF_ICC-tiedostosta.

typeOfTachographCardId luettuna DF_Tachograph_G2-tiedoston EF_Application_Identification-tiedostosta.

cardStructureVersion luettuna DF_Tachograph_G2-tiedoston EF_Application_Identification-tiedostosta.

cardNumber luettuna DF_Tachograph_G2-tiedoston EF_Identification-tiedostosta.

2.180. **VuCardRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät tässä ajoneuvoyksikössä käytettyihin ajopiirturikortteihin. Nämä tiedot on tarkoitettu ajoneuvoyksikön kortteihin liittyvien ongelmien arviointiin (liitteen 1 C vaatimus 132).

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

recordType osoittaa tietueen tyypin (VuCardRecord). **Asetettava arvo**: ks. RecordType

recordSize on VuCardRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja tietueita, jotka liittyvät ajoneuvoyksiköissä käytettäviin ajopiirturikortteihin.

▼B

2.181. **VuCertificate**

Ajoneuvoyksikön julkisen avaimen varmenne.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Sukupolvi 2:

Ajoneuvoyksikön varmenne ja metadata, sellaisina kuin niitä käytetään kopiointiprotokollassa.

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

recordType osoittaa tietueen tyypin (VuCertificate). **Asetettava arvo**: ks. RecordType

recordSize on VuCertificate-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä. Arvoksi asetetaan 1, koska varmenteilla voi olla erilaiset pituudet.

records on sarja ajoneuvoyksiköiden varmenteita.

2.183. **VuCompanyLocksData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yrityksen tekemiin lukituksiin (liitteen 1 B vaatimus 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                           INTEGER(0..255),
   vuCompanyLocksRecords               SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks on vuCompanyLocksRecords-tietueissa lueteltujen lukitusten määrä.

vuCompanyLocksRecords on sarja tietueita, jotka sisältävät yrityksen tekemiin lukituksiin liittyviä tietoja.

2.184. **VuCompanyLocksRecord**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yrityksen tekemään lukitukseen (liitteen 1 B vaatimus 104 ja liitteen 1 C vaatimus 128).

Sukupolvi 1:

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

▼B

lockInTime, lockOutTime ovat päivämäärä ja aika, jolloin lukitus tehtiin ja avattiin.

companyName, companyAddress ovat lukitukseen liittyvän yrityksen nimi ja osoite.

companyCardNumber yksilöi lukituksessa käytetyn kortin.

Sukupolvi 2:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Sukupolven 2 datarakenne käyttää companyCardNumber-tietueen sijasta seuraavaa datarakennetta

companyCardNumberAndGeneration yksilöi lukituksessa käytetyn kortin ja sen sukupolven.

2.185. **VuCompanyLocksRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yrityksen tekemiin lukituksiin (liitteen 1 C vaatimus 128).

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

recordType osoittaa tietueen tyypin (VuCompanyLocksRecord). **Asetettava arvo**: ks. RecordType

recordSize on VuCompanyLocksRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä. Arvo 0..255.

records on sarja tietueita, jotka sisältävät yrityksen tekemiin lukituksiin liittyviä tietoja.

2.186. **VuControlActivityData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät tätä ajoneuvoyksikköä käytettäessä suoritettuihin tarkastuksiin (liitteen 1 B vaatimus 102).

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

▼B

noOfControls on vuControlActivityRecords-tietueissa lueteltujen tarkastusten määrä.

vuControlActivityRecords on sarja tarkastustoimiin liittyviä tietueita.

2.187. **VuControlActivityRecord**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yksittäiseen tätä ajoneuvoyksikköä käytettäessä suoritettuun tarkastukseen (liitteen 1 B vaatimus 102 ja liitteen 1 C vaatimus 126).

Sukupolvi 1:

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

controlType on tarkastustoimen tyyppi.

controlTime on tarkastustoimen päivämäärä ja aika.

controlCardNumber yksilöi valvontakortin, jota tarkastuksessa käytettiin.

downloadPeriodBeginTime on tietojen kopioinnin päättymisaika, jos kopiointia tapahtui.

downloadPeriodEndTime on tietojen kopioinnin alkamisaika, jos kopiointia tapahtui.

Sukupolvi 2:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Sukupolven 2 datarakenne käyttää controlCardNumber-tietueen sijasta seuraavaa datarakennetta

controlCardNumberAndGeneration yksilöi tarkastuksessa käytetyn valvontakortin, mukaan lukien sen sukupolven.

2.188. **VuControlActivityRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät tätä ajoneuvoyksikköä käytettäessä suoritettuihin tarkastuksiin (liitteen 1 C vaatimus 126).

▼B

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

recordType osoittaa tietueen tyypin (VuControlActivityRecord). **Asetettava arvo**: ks. RecordType

recordSize on VuControlActivityRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja ajoneuvoyksikön tarkastustoimiin liittyviä tietueita.

2.189. **VuDataBlockCounter**

Kortille tallennettu laskuri, joka yksilöi järjestyksessä kortin ajoneuvoyksiköihin asettamis- ja poistamisjaksot.

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

Asetettava arvo: juokseva numero, jonka maksimiarvo on 9 999, minkä jälkeen se alkaa jälleen nollasta.

2.190. **VuDetailedSpeedBlock**

Ajoneuvoyksikköön tallennetut yksityiskohtaiset tiedot, jotka liittyvät ajoneuvon nopeuteen niinä minuutteina, jolloin se on ollut liikkeellä (liitteen 1 B vaatimus 093 ja liitteen 1 C vaatimus 116).

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

speedBlockBeginDate on osion ensimmäisen nopeusarvon päivämäärä ja aika.

speedsPerSecond on sarja aikajärjestyksessä olevia sekunnin välein mitattuja nopeuksia, jotka liittyvät speedBlockBeginDate-muuttujan ilmaisemalla hetkellä alkaneeseen minuuttiin (kyseinen hetki mukaan lukien).

2.191. **VuDetailedSpeedBlockRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut yksityiskohtaiset tiedot, jotka liittyvät ajoneuvon nopeuteen.

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

recordType osoittaa tietueen tyypin (VuDetailedSpeedBlock). **Asetettava arvo**: ks. RecordType

▼B

recordSize on VuDetailedSpeedBlock-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja tietueosioita, jotka sisältävät yksityiskohtaisia tietoja ajoneuvon nopeudesta.

2.192. **VuDetailedSpeedData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut yksityiskohtaiset tiedot, jotka liittyvät ajoneuvon nopeuteen.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                    INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks              SET SIZE(noOfSpeedBlocks) OF
                                      VuDetailedSpeedBlock
}
```

noOfSpeedBlocks on vuDetailedSpeedBlocks-tietuesarjan sisältämien nopeustietueosioiden määrä.

vuDetailedSpeedBlocks on sarja tietueosioita, jotka sisältävät yksityiskohtaisia tietoja ajoneuvon nopeudesta.

2.193. **VuDownloadablePeriod**

Aikaisin ja viimeisin päivämäärä, jota koskevia kuljettajan toimiin liittyviä tietoja ajoneuvoyksikössä on tallennettuna (liitteen 1 B vaatimus 081, 084 tai 087 ja liitteen 1 C vaatimus 102, 105, 108).

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

minDownloadableTime on aikaisin kortin paikoilleen asettamiseen tai toiminnan muutokseen tai paikkaan liittyvä päivämäärä- ja aikatieto, joka on tallennettuna ajoneuvoyksikköön.

maxDownloadableTime on viimeisin kortin poistamiseen tai toiminnan muutokseen tai paikkaan liittyvä päivämäärä- ja aikatieto, joka on tallennettuna ajoneuvoyksikköön.

2.194. **VuDownloadablePeriodRecordArray**

Sukupolvi 2:

VUDownloadablePeriod ja kopiointiprotokollassa käytetty metadata.

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

recordType osoittaa tietueen tyypin (VuDownloadablePeriod). **Asetettava arvo**: ks. RecordType

▼B

recordSize on VuDownloadablePeriod-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja VuDownloadablePeriod-tietueita.

2.195. **VuDownloadActivityData**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät viimeksi tapahtuneeseen sen tietojen kopiointiin (liitteen 1 B vaatimus 105 ja liitteen 1 C vaatimus 129).

Sukupolvi 1:

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

downloadingTime on päivämäärä ja aika, jolloin tiedot kopioitiin.

fullCardNumber yksilöi kortin, jonka oikeutta tietojen kopiointiin käytettiin.

companyOrWorkshopName on yrityksen tai korjaamon nimi.

Sukupolvi 2:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                    TimeReal,
   fullCardNumberAndGeneration        FullCardNumberAndGeneration,
   companyOrWorkshopName              Name
}
```

Sukupolven 2 datarakenne käyttää fullCardNumber-tietueen sijasta seuraavaa datarakennetta.

fullCardNumberAndGeneration yksilöi kortin, jonka oikeutta tietojen kopiointiin käytettiin, mukaan lukien sen sukupolven.

2.196. **VuDownloadActivityDataRecordArray**

Sukupolvi 2:

Tiedot, jotka liittyvät ajoneuvoyksikön viimeksi tapahtuneeseen sen tietojen kopiointiin (liitteen 1 C vaatimus 129).

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

recordType osoittaa tietueen tyypin (VuDownloadActivityData). **Asetettava arvo**: ks. RecordType

recordSize on VuDownloadActivityData-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

▼B

records on sarja tietojen kopiointitapahtumiin liittyviä tietueita.

2.197. **VuEventData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät tapahtumiin (liitteen 1 B vaatimus 094, paitsi ylinopeustapaukset).

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

noOfVuEvents on vuEventRecords-tietuesarjaan tallennettujen tapahtumien määrä.

vuEventRecords on sarja tapahtumiin liittyviä tietueita.

2.198. **VuEventRecord**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät tapahtumiin (liitteen 1 B vaatimus 094 ja liitteen 1 C vaatimus 117, paitsi ylinopeustapaukset).

Sukupolvi 1:

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

eventType on tapahtuman tyyppi.

eventRecordPurpose on syy, jonka vuoksi kyseinen tapahtuma on kirjattu.

eventBeginTime on päivämäärä ja aika, jolloin tapahtuma alkoi.

eventEndTime on päivämäärä ja aika, jolloin tapahtuma päättyi.

cardNumberDriverSlotBegin yksilöi kortin, joka oli kuljettajan korttiaukossa tapahtuman alkaessa.

cardNumberCodriverSlotBegin yksilöi kortin, joka oli apukuljettajan korttiaukossa tapahtuman alkaessa.

cardNumberDriverSlotEnd yksilöi kortin, joka oli kuljettajan korttiaukossa tapahtuman päättyessä.

cardNumberCodriverSlotEnd yksilöi kortin, joka oli apukuljettajan korttiaukossa tapahtuman päättyessä.

similarEventsNumber on kyseisenä päivänä sattuneiden vastaavien tapahtumien määrä.

Tätä sarjaa voidaan käyttää kaikkien muiden paitsi ylinopeuksiin liittyvien tapahtumien kirjaamiseen.

▼B

Sukupolvi 2:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Sukupolven 1 arvojen lisäksi käytetään seuraavia dataelementtejä:

manufacturerSpecificEventFaultData sisältää täydentäviä valmistajakohtaisia tietoja tapahtumasta.

Sukupolven 2 datarakenne käyttää tietuiden cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd ja cardNumberCodriverSlotEnd sijasta seuraavaa datarakennetta:

cardNumberAndGenDriverSlotBegin yksilöi kortin, joka oli kuljettajan korttiaukossa tapahtuman alkaessa, mukaan lukien sen sukupolvi.

cardNumberAndGenCodriverSlotBegin yksilöi kortin, joka oli apukuljettajan korttiaukossa tapahtuman alkaessa, mukaan lukien sen sukupolvi.

cardNumberAndGenDriverSlotEnd yksilöi kortin, joka oli kuljettajan korttiaukossa tapahtuman päättyessä, mukaan lukien sen sukupolvi.

cardNumberAndGenCodriverSlotEnd yksilöi kortin, joka oli apukuljettajan korttiaukossa tapahtuman päättyessä, mukaan lukien sen sukupolvi.

Jos tapahtuma on aikojen päällekkäisyys, eventBeginTime ja eventEndTime on tulkittava seuraavasti:

eventBeginTime on valvontalaitteen toiminnan päivämäärä ja -aika.

eventEndTime on GNSS-laitteiston toiminnan päivämäärä ja aika.

2.199. **VuEventRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät tapahtumiin (liitteen 1 C vaatimus 117, paitsi ylinopeustapaukset).

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

recordType osoittaa tietueen tyypin (VuEventRecord). **Asetettava arvo**: ks. RecordType

▼B

recordSize on VuEventRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja tapahtumiin liittyviä tietueita.

2.200. **VuFaultData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät vikoihin (liitteen 1 B vaatimus 096).

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

noOfVuFaults on vuFaultRecords-tietuesarjaan tallennettujen vikatapahtumien määrä.

vuFaultRecords on sarja vikatapahtumiin liittyviä tietueita.

2.201. **VuFaultRecord**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät vikatapahtumaan (liitteen 1 B vaatimus 096 ja liitteen 1 C vaatimus 118).

Sukupolvi 1:

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

faultType on valvontalaitteen vian tyyppi.

faultRecordPurpose on syy, jonka vuoksi kyseinen vikatapahtuma on kirjattu.

faultBeginTime on päivämäärä ja aika, jolloin vikatapahtuma alkoi.

faultEndTime on päivämäärä ja aika, jolloin vikatapahtuma päättyi.

cardNumberDriverSlotBegin yksilöi kortin, joka oli kuljettajan korttiaukossa vikatapahtuman alkaessa.

cardNumberCodriverSlotBegin yksilöi kortin, joka oli apukuljettajan korttiaukossa vikatapahtuman alkaessa.

cardNumberDriverSlotEnd yksilöi kortin, joka oli kuljettajan korttiaukossa vikatapahtuman päättyessä.

cardNumberCodriverSlotEnd yksilöi kortin, joka oli apukuljettajan korttiaukossa vikatapahtuman päättyessä.

▼B

Sukupolvi 2:

```
VuFaultRecord ::= SEQUENCE {
   faultType                            EventFaultType,
   faultRecordPurpose                   EventFaultRecordPurpose,
   faultBeginTime                       TimeReal,
   faultEndTime                         TimeReal,
   cardNumberAndGenDriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd      FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Sukupolven 1 arvojen lisäksi käytetään seuraavaa dataelementtiä:

manufacturerSpecificEventFaultData sisältää täydentäviä valmistajakohtaisia tietoja vikatapahtumasta.

Sukupolven 2 datarakenne käyttää tietuiden cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd ja cardNumberCodriverSlotEnd sijasta seuraavaa datarakennetta:

cardNumberAndGenDriverSlotBegin yksilöi kortin, joka oli kuljettajan korttiaukossa vikatapahtuman alkaessa, mukaan lukien sen sukupolvi.

cardNumberAndGenCodriverSlotBegin yksilöi kortin, joka oli apukuljettajan korttiaukossa tapahtuman alkaessa, mukaan lukien sen sukupolvi.

cardNumberAndGenDriverSlotEnd yksilöi kortin, joka oli kuljettajan korttiaukossa tapahtuman päättyessä, mukaan lukien sen sukupolvi.

cardNumberAndGenCodriverSlotEnd yksilöi kortin, joka oli apukuljettajan korttiaukossa tapahtuman päättyessä, mukaan lukien sen sukupolvi.

2.202. **VuFaultRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät vikoihin (liitteen 1 C vaatimus 118).

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

recordType osoittaa tietueen tyypin (VuFaultRecord). **Asetettava arvo**: ks. RecordType

recordSize on VuFaultRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja vikatapahtumiin liittyviä tietueita.

▼B

2.203. **VuGNSSCDRecord**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajoneuvon GNSS-sijaintiin, jos kuljettajan keskeytymätön ajoaika saavuttaa yli kolmen tunnin jakson (liitteen 1 C vaatimus 108 ja 110).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp on päivämäärä ja aika, jolloin kuljettajan keskeytymätön ajoaika on yli kolmen tunnin jakso.

cardNumberAndGenDriverSlot yksilöi kortin, joka oli kuljettajan korttiaukossa, mukaan lukien sen sukupolvi.

cardNumberAndGenCodriverSlot yksilöi kortin, joka oli apukuljettajan korttiaukossa, mukaan lukien sen sukupolvi.

gnssPlaceRecord sisältää tiedot ajoneuvon sijainnista.

2.204. **VuGNSSCDRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajoneuvon GNSS-sijaintiin, jos kuljettajan keskeytymätön ajoaika on yli kolmen tunnin jakso (liitteen 1 C vaatimus 108 ja 110).

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

recordType osoittaa tietueen tyypin (VuGNSSCDRecord). **Asetettava arvo**: ks. RecordType

recordSize on VuGNSSCDRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja GNSS-laitteiston keskeytymätöntä ajoa koskevia tietueita.

2.205. **VuIdentification**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajoneuvoyksikön tunnistukseen (liitteen 1 B vaatimus 075 ja liitteen 1 C vaatimus 93 ja 121).

▼B

Sukupolvi 1:

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

vuManufacturerName on ajoneuvoyksikön valmistajan nimi.

vuManufacturerAddress on ajoneuvoyksikön valmistajan osoite.

vuPartNumber on ajoneuvoyksikön osanumero.

vuSerialNumber on ajoneuvoyksikön sarjanumero.

vuSoftwareIdentification yksilöi ajoneuvoyksikössä käytettävän ohjelmiston.

vuManufacturingDate on ajoneuvoyksikön valmistuspäivä.

vuApprovalNumber on ajoneuvoyksikön tyyppihyväksyntänumero.

Sukupolvi 2:

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

Sukupolven 1 arvojen lisäksi käytetään seuraavaa dataelementtiä:

vuGeneration yksilöi ajoneuvoyksikön sukupolven.

vuAbility tarjoaa tietoaa siitä, tukeeko ajoneuvoyksikkö sukupolven 1 ajopiirturikortteja vai ei.

2.206. **VuIdentificationRecordArray**

Sukupolvi 2:

VuIdentification ja kopiointiprotokollassa käytetty metadata.

▼B

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

recordType osoittaa tietueen tyypin (VuIdentification). **Asetettava arvo**: ks. RecordType

recordSize on VuIdentification-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja VuIdentification-tietueita.

2.207. **VuITSConsentRecord**

Sukupolvi 2:

Ajoneuvoyksikössä tallennetut tiedot, jotka liittyvät kuljettajan suostumukseen käyttää älykkäitä liikennejärjestelmiä.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen yksilöivät kortin ja sen sukupolven. Tämän on oltava kuljettaja- tai korjaamokortti.

consent on erote, joka ilmaisee, onko kuljettaja suostunut käyttämään tämän ajoneuvon/ajoneuvoyksikön älykkäitä liikennejärjestelmiä.

Asetettava arvo:

TRUE	osoittaa, että kuljettaja on suostunut käyttämään älykkäitä liikennejärjestelmiä
FALSE	osoittaa, että kuljettaja on kieltäynyt käyttämästä älykkäitä liikennejärjestelmiä

2.208. **VuITSConsentRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät suostumukseen käyttää älykkäitä liikennejärjestelmiä (liitteen 1 C vaatimus 200).

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

recordType osoittaa tietueen tyypin (VuITSConsentRecord). **Asetettava arvo**: ks. RecordType

recordSize on VuITSConsentRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja tietueita, jotka liittyvät suostumukseen käyttää älykkäitä liikennejärjestelmiä.

▼B

2.209. **VuManufacturerAddress**

Ajoneuvoyksikön valmistajan osoite.

```
VuManufacturerAddress ::= Address
```

Asetettava arvo: määrittelemätön.

2.210. **VuManufacturerName**

Ajoneuvoyksikön valmistajan nimi.

```
VuManufacturerName ::= Name
```

Asetettava arvo: määrittelemätön.

2.211. **VuManufacturingDate**

Ajoneuvoyksikön valmistuspäivä.

```
VuManufacturingDate ::= TimeReal
```

Asetettava arvo: määrittelemätön.

2.212. **VuOverSpeedingControlData**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät viimeksi suoritetun ylinopeustarkastuksen jälkeen sattuneisiin ylinopeustapauksiin (liitteen 1 B vaatimus 095 ja liitteen 1 C vaatimus 117).

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

lastOverspeedControlTime on päivämäärä ja aika, jolloin ylinopeustarkastus viimeksi suoritettiin.

firstOverspeedSince on päivämäärä ja aika, jolloin ensimmäinen ylinopeustapaus sattui tämän ylinopeustarkastuksen jälkeen.

numberOfOverspeedSince on viimeisen ylinopeustarkastuksen jälkeen sattuneiden ylinopeustapausten määrä.

2.213. **VuOverSpeedingControlDataRecordArray**

Sukupolvi 2:

VuOverSpeedingControlData ja kopiointiprotokollassa käytetty metadata.

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

▼B

recordType osoittaa tietueen tyypin (VuOverSpeedingControlData).
Asetettava arvo: ks. RecordType

recordSize on VuOverSpeedingControlData-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja ylinopeustapauksien valvontaan liittyviä tietueita.

2.214. **VuOverSpeedingEventData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ylinopeustapauksiin (liitteen 1 B vaatimus 094).

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

noOfVuOverSpeedingEvents on vuOverSpeedingEventRecords-tietuesarjaan tallennettujen tapahtumien määrä.

vuOverSpeedingEventRecords on sarja ylinopeustapauksiin liittyviä tietueita.

2.215. **VuOverSpeedingEventRecord**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät vikatapahtumaan (liitteen 1 B vaatimus 094 ja liitteen 1 C vaatimus 117).

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

eventType on tapahtuman tyyppi.

eventRecordPurpose on syy, jonka vuoksi kyseinen tapahtuma on kirjattu.

eventBeginTime on päivämäärä ja aika, jolloin tapahtuma alkoi.

eventEndTime on päivämäärä ja aika, jolloin tapahtuma päättyi.

maxSpeedValue on suurin tapahtuman aikana mitattu nopeus.

averageSpeedValue on tapahtuman aikana mitattujen nopeuslukemien aritmeettinen keskiarvo.

▼B

cardNumberDriverSlotBegin yksilöi kortin, joka oli kuljettajan korttiaukossa tapahtuman alkaessa.

similarEventsNumber on kyseisenä päivänä sattuneiden vastaavien tapahtumien määrä.

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät vikatapahtumaan (liitteen 1 B vaatimus 094 ja liitteen 1 C vaatimus 117).

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

Sukupolven 2 datarakenne käyttää cardNumberDriverSlotBegin-tietueen sijasta seuraavaa datarakennetta:

cardNumberAndGenDriverSlotBegin yksilöi kortin, joka oli kuljettajan korttiaukossa tapahtuman alkaessa, mukaan lukien sen sukupolvi.

2.216. **VuOverSpeedingEventRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ylinopeustapauksiin (liitteen 1 C vaatimus 117).

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

recordType osoittaa tietueen tyypin (VuOverSpeedingEventRecord).
Asetettava arvo: ks. RecordType

recordSize on VuOverSpeedingEventRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja ylinopeustapauksiin liittyviä tietueita.

2.217. **VuPartNumber**

Ajoneuvoyksikön osanumero.

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

Asetettava arvo: arvo määräytyy ajoneuvoyksikön valmistajan mukaan.

▼B

2.218. **VuPlaceDailyWorkPeriodData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät paikkoihin, joissa kuljettajan päivän työaika alkaa tai päättyy (liitteen 1 B vaatimus 087 ja liitteen 1 C vaatimus 108 ja 110).

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

noOfPlaceRecords on vuPlaceDailyWorkPeriodRecords-tietuesarjaan tallennettujen tietueiden määrä.

vuPlaceDailyWorkPeriodRecords on sarja paikkaan liittyviä tietoja sisältäviä tietueita.

2.219. **VuPlaceDailyWorkPeriodRecord**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät paikkaan, jossa kuljettajan päivän työaika alkaa tai päättyy (liitteen 1 B vaatimus 087 ja liitteen 1 C vaatimus 108 ja 110).

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

fullCardNumber on kuljettajan kortin tyyppi, kortin myöntänyt jäsenvaltio ja kortin numero.

placeRecord sisältää syötettyyn paikkaan liittyvät tiedot.

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät paikkaan, jossa kuljettajan päivän työaika alkaa tai päättyy (liitteen 1 B vaatimus 087 ja liitteen 1 C vaatimus 108 ja 110).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Sukupolven 2 datarakenne käyttää fullCardNumber-tietueen sijasta seuraavaa datarakennetta:

fullCardNumberAndGeneration on kortin tyyppi, sen myöntänyt jäsenvaltio sekä kortin numero ja sukupolvi siinä muodossa kuin ne on tallennettu kortille.

▼B

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät paikkoihin, joissa kuljettajan päivän työaika alkaa tai päättyy (liitteen 1 C vaatimus 108 ja 110).

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

recordType osoittaa tietueen tyypin (VuPlaceDailyWorkPeriodRecord).
Asetettava arvo: ks. RecordType

recordSize on VuPlaceDailyWorkPeriodRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja paikkaan liittyviä tietoja sisältäviä tietueita.

2.221. **VuPrivateKey**

Sukupolvi 1:

Ajoneuvoyksikön yksityinen avain.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Sukupolvi 1:

Ajoneuvoyksikön julkinen avain.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Ajoneuvoyksikön sarjanumero (liitteen 1 B vaatimus 075 ja liitteen 1 C vaatimus 93).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Päivämäärä, jolloin ajoneuvoyksikön ohjelmistoversio asennettiin.

```
VuSoftInstallationDate ::= TimeReal
```

Asetettava arvo: määrittelemätön.

▼B

2.225. **VuSoftwareIdentification**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät asennettuun ohjelmistoon.

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

vuSoftwareVersion on ajoneuvoyksikön ohjelmistoversion numero.

vuSoftInstallationDate on päivämäärä, jolloin ohjelmistoversio asennettiin.

2.226. **VuSoftwareVersion**

Ajoneuvoyksikön ohjelmistoversion numero.

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

Asetettava arvo: määrittelemätön.

2.227. **VuSpecificConditionData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät erityisolosuhteisiin.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords on specificConditionRecords-tietuesarjaan tallennettujen tietueiden määrä.

specificConditionRecords on sarja erityisolosuhteisiin liittyviä tietoja sisältäviä tietueita.

2.228. **VuSpecificConditionRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät erityisolosuhteisiin (liitteen 1 C vaatimus 130).

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

recordType osoittaa tietueen tyypin (SpecificConditionRecord). **Asetettava arvo**: ks. RecordType

recordSize on SpecificConditionRecord-tietueen koko tavuina.

noOfIWRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja eritysolosuhteisiin liittyviä tietoja sisältäviä tietueita.

▼B

2.229. **VuTimeAdjustmentData**

Sukupolvi 1:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajan asettamistapahtumiin muulloin kuin tavanomaisen kalibroinnin yhteydessä (liitteen 1 B vaatimus 101).

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

noOfVuTimeAdjRecords on vuTimeAdjustmentRecords-tietuesarjaan tallennettujen tietueiden määrä.

vuTimeAdjustmentRecords on sarja ajan asettamisiin liittyviä tietoja sisältäviä tietueita.

2.230. **VuTimeAdjustmentGNSSRecord**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät GNSS-laitteiston aikatietoihin perustuvaan ajan asetukseen (liitteen 1 C vaatimus 124 ja 125).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal
}
```

oldTimeValue, newTimeValue ovat päivämäärän ja ajan vanhat ja uudet arvot.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät GNSS-laitteiston aikatietojen perusteella suoritettuun ajan asetukseen (liitteen 1 C vaatimus 124 ja 125).

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

recordType osoittaa tietueen tyypin (VuTimeAdjustmentGNSSRecord).
Asetettava arvo: ks. RecordType

recordSize on VuTimeAdjustmentGNSSRecord-tietueen koko tavuina.

noOfRecords on tietuesarjassa olevien tietueiden määrä.

records on GNSS-laitteiston ajan asettamisiin liittyviä tietoja koskeva tietuesarja.

▼B

2.232. **VuTimeAdjustmentRecord**

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajan asettamistapahtumaan muulloin kuin tavanomaisen kalibroinnin yhteydessä (liitteen 1 B vaatimus 101 ja liitteen 1 C vaatimus 124 ja 125).

Sukupolvi 1:

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

oldTimeValue, newTimeValue ovat päivämäärän ja ajan vanhat ja uudet arvot.

workshopName, workshopAddress ovat korjaamon nimi ja osoite.

workshopCardNumber yksilöi ajan asettamisessa käytetyn korjaamokortin.

Sukupolvi 2:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumberAndGeneration       FullCardNumberAndGeneration
}
```

Sukupolven 2 datarakenne käyttää workshopCardNumber-tietueen sijasta seuraavaa datarakennetta

workshopCardNumberAndGeneration yksilöi ajan asettamisessa käytetyn korjaamokortin ja sen sukupolven.

2.233. **VuTimeAdjustmentRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajan asettamistapahtumiin muulloin kuin tavanomaisen kalibroinnin yhteydessä (liitteen 1 C vaatimus 124 ja 125).

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

recordType osoittaa tietueen tyypin (VuTimeAdjustmentRecord). **Asetettava arvo**: ks. RecordType

recordSize on VuTimeAdjustmentRecord-tietueen koko tavuina.

▼B

noOfRecords on tietuesarja

records on sarja ajan asettamisiin liittyviä tietoja sisältäviä tietueita.

2.234. **WorkshopCardApplicationIdentification**

Korjaamokortille tallennetut tiedot, jotka liittyvät kortilla olevan sovelluksen tunnistamiseen (liitteen 1 C vaatimus 307 ja 330).

Sukupolvi 1:

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

typeOfTachographCardId määrittelee kortilla käytetyn tunnisteen tyypin.

cardStructureVersion määrittelee kortilla käytetyn datarakenteen version.

noOfEventsPerType on niiden tapahtumien määrä tapahtumayyppiä kohden, jotka voidaan tallentaa kortille.

noOfFaultsPerType on niiden vikatapahtumien määrä vikatyyppiä kohden, jotka voidaan tallentaa kortille.

activityStructureLength osoittaa niiden tavujen määrän, jotka ovat käytettävissä kuljettajan toimintaan liittyvien tietojen tallennukseen.

noOfCardVehicleRecords on niiden ajoneuvoon liittyviä tietoja sisältävien tietueiden määrä, jotka voidaan tallentaa kortille.

noOfCardPlaceRecords on niiden paikkoihin liittyviä tietoja sisältävien tietueiden määrä, jotka voidaan tallentaa kortille.

noOfCalibrationRecords on niiden kalibrointeihin liittyviä tietoja sisältävien tietueiden määrä, jotka voidaan tallentaa kortille.

Sukupolvi 2:

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

Sukupolven 1 arvojen lisäksi käytetään seuraavia dataelementtejä:

noOfGNSSCDRecords on kortille tallennettavissa olevien keskeytymätöntä ajoaikaa koskevien GNSS-tietueiden määrä.

▼B

noOfSpecificConditionRecords on kortille tallennettavissa olevien erityisolosuhteisiin liittyvien tietueiden määrä.

2.235. **WorkshopCardCalibrationData**

Korjaamokortille tallennetut tiedot, jotka liittyvät kortilla suoritettuihin korjaamon toimiin (liitteen 1 C vaatimukset 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 kaikkien korttia käyttäen suoritettujen kalibrointien määrä.

calibrationPointerNewestRecord on viimeksi päivitetyn kalibrointitiedon järjestysnumero.

Asetettava arvo: numero, joka vastaa kalibrointiin liittyvän tietueen järjestysnumeroa, alkaen numerosta ‘0’ ensimmäiselle kalibrointiin liittyvälle tietueelle datarakenteessa.

calibrationRecords on sarja tietueita, joissa on kalibrointiin ja/tai ajan asetukseen liittyviä tietoja.

2.236. **WorkshopCardCalibrationRecord**

Korjaamokortille tallennetut tiedot, jotka liittyvät kortilla suoritettuun kalibrointiin (liitteen 1 C vaatimus 314 ja 337).

Sukupolvi 1:

```
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 syy, jonka vuoksi kalibrointi suoritettiin.

vehicleIdentificationNumber on ajoneuvon valmistenumero (VIN).

vehicleRegistration sisältää ajoneuvon rekisteritunnuksen (VRN) ja ajoneuvon rekisteröineen jäsenvaltion.

wVehicleCharacteristicConstant on ajoneuvon ominaiskerroin.

▼B

kConstantOfRecordingEquipment on valvontalaitteen vakio.

lTyreCircumference on pyörien renkaiden tehollinen ympärysmitta.

tyreSize on ajoneuvoon asennettujen renkaiden kokomerkintä.

authorisedSpeed on ajoneuvon suurin sallittu nopeus.

oldOdometerValue, newOdometerValue ovat matkamittarin vanha ja uusi lukema.

oldTimeValue, newTimeValue ovat päivämäärän ja ajan vanhat ja uudet arvot.

nextCalibrationDate on päivämäärä, jolloin valtuutetun tarkastusviranomaisen on suoritettava seuraava CalibrationPurpose-muuttujan määrittelemä kalibrointi.

vuPartNumber, **vuSerialNumber** ja **sensorSerialNumber** ovat valvontalaitteen tunnistuksessa käytettävät dataelementit.

Sukupolvi 2:

```
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
}
```

Sukupolven 1 arvojen lisäksi käytetään seuraavia dataelementtejä:

sensorGNSSSerialNumber, joka yksilöi ulkoisen GNSS-laitteiston.

rcmSerialNumber, joka yksilöi etäviestintämoduulin.

sealDataCard antaa tietoa sinetöinneistä, jotka on liitetty ajoneuvon eri osiin.

▼B

2.237. **WorkshopCardHolderIdentification**

Korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijan tunnistamiseen (liitteen 1 C vaatimus 311 ja 334).

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

workshopName on sen korjaamon nimi, jossa kortin haltija työskentelee.

workshopAddress on sen korjaamon osoite, jossa kortin haltija työskentelee.

cardHolderName on kortin haltijan (esim. mekaanikon) nimi ja etunimi (etunimet).

cardHolderPreferredLanguage on kortin haltijan ensisijaisesti käyttämä kieli.

2.238. **WorkshopCardPIN**

Korjaamokortin henkilökohtainen tunnusluku (liitteen 1 C vaatimus 309 ja 332).

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

Asetettava arvo: kortin haltijan tiedossa oleva henkilökohtainen tunnusluku, jonka perään tarvittaessa lisätään arvoltaan ‘FF’ olevia tavuja siten, että kokonaistavumääräksi tulee kahdeksan.

2.239. **W-VehicleCharacteristicConstant**

Ajoneuvon ominaiskerroin (määritelmä k).

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

Asetettava arvo: impulsseja kilometriä kohti alueella 0–64 255 impulssia/km.

2.240. **VuPowerSupplyInterruptionRecord**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät keskeytynyttä virransyöttöä koskeviin tapauksiin (liitteen 1 C vaatimus 117).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberAndGenDriverSlotBegin       FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd         FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd       FullCardNumberAndGeneration,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType on tapahtuman tyyppi.

eventRecordPurpose on syy, jonka vuoksi kyseinen tapahtuma on kirjattu.

eventBeginTime on päivämäärä ja aika, jolloin tapahtuma alkoi.

▼B

eventEndTime on päivämäärä ja aika, jolloin tapahtuma päättyi.

cardNumberAndGenDriverSlotBegin yksilöi kortin, joka oli kuljettajan korttiaukossa tapahtuman alkaessa, mukaan lukien sen sukupolvi.

cardNumberAndGenDriverSlotEnd yksilöi kortin, joka oli kuljettajan korttiaukossa tapahtuman päättyessä, mukaan lukien sen sukupolvi.

cardNumberAndGenCodriverSlotBegin yksilöi kortin, joka oli apukuljettajan korttiaukossa tapahtuman alkaessa, mukaan lukien sen sukupolvi.

cardNumberAndGenCodriverSlotEnd yksilöi kortin, joka oli apukuljettajan korttiaukossa tapahtuman päättyessä, mukaan lukien sen sukupolvi.

similarEventsNumber on kyseisenä päivänä sattuneiden vastaavien tapahtumien määrä.

2.241. **VuPowerSupplyInterruptionRecordArray**

Sukupolvi 2:

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät keskeytynyttä virransyöttöä koskeviin tapauksiin (liitteen 1 C vaatimus 117).

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

recordType osoittaa tietueen tyypin (VuPowerSupplyInterruptionRecord). **Asetettava arvo**: ks. RecordType

recordSize on VuPowerSupplyInterruptionRecord-tietueen koko tavuina.

noOfRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja keskeytynyttä virransyöttöä koskeviin tapauksiin liittyviä tietueita.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Sukupolvi 2:

Sarja SensorExternalGNSSCoupledRecord-tietueita ja kopiointiprotokollassa käytetty metadata.

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

recordType osoittaa tietueen tyypin (SensorExternalGNSSCoupledRecord). **Asetettava arvo**: ks. RecordType

▼B

recordSize on SensorExternalGNSSCoupledRecord-tietueen koko tavuina.

noOfRecords on tietuesarjassa olevien tietueiden määrä.

records on ulkoiseen GNSS-vastaanottimeen kytketyn tunnistimen tietuejoukko.

2.243. **VuSensorPairedRecordArray**

Sukupolvi 2:

Sarja SensorPairedRecord-tietueita ja kopiointiprotokollassa käytetty metadata.

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

recordType osoittaa tietueen tyypin (SensorPairedRecord). **Asetettava arvo**: ks. RecordType

recordSize on SensorPairedRecord-tietueen koko tavuina.

noOfRecords on tietuesarjassa olevien tietueiden määrä.

records on sarja tunnistimeen liittyviä tietoja sisältäviä tietueita.

3. ARVOALUEIDEN MÄÄRITTELYT

Kohdassa 2 määriteltyjen muuttujien arvojen määrittely.

```
TimeRealRange ::= 2^32-1
```

4. MERKKIJONOT

IA5 (International Alphabet 5) -merkkijonoissa käytetään standardin ISO/IEC 8824-1 mukaisia ASCII-merkkejä. Selvyyden vuoksi ja avuksi on kyseiset merkit näytetty alla. Ristiriitatapauksissa on standardin ISO/IEC 8824-1 sisältö ratkaiseva.

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

Muissa merkkijonoissa (Address, Name, VehicleRegistrationNumber) käytetään lisäksi merkkejä desimaalimerkkien koodialueelta 161–255, joka kuuluu seuraaviin koodisivun numeron määrittämiin 8-bittisiin standardimerkistöihin: Standardimerkistö	Koodisivu (Desimaali)
ISO/IEC 8859-1, latinalaisaakkosto nro 1, länsieurooppalainen	1
ISO/IEC 8859-2, latinalaisaakkosto nro 2, keskieurooppalainen	2
ISO/IEC 8859-3, latinalaisaakkosto nro 3, eteläeurooppalainen	3
ISO/IEC 8859-5, latinalainen/kyrillinen	5
ISO/IEC 8859-7, latinalainen/kreikkalainen	7
ISO/IEC 8859-9, latinalaisaakkosto nro 5, turkkilainen	9

▼B

Muissa merkkijonoissa (Address, Name, VehicleRegistrationNumber) käytetään lisäksi merkkejä desimaalimerkkien koodialueelta 161–255, joka kuuluu seuraaviin koodisivun numeron määrittämiin 8-bittisiin standardimerkistöihin: Standardimerkistö	Koodisivu (Desimaali)
ISO/IEC 8859-13, latinalaisaakkosto nro 7, balttilaiset kielet	13
ISO/IEC 8859-15, latinalaisaakkosto nro 9	15
ISO/IEC 8859-16, latinalaisaakkosto nro 10, kaakkoiseurooppalainen	16
KOI8-R, latinalainen/kyrillinen	80
KOI8-U, latinalainen/kyrillinen	85

5. KOODAUS

Kun koodataan ASN.1-merkintätavan koodaussääntöjä käyttäen, kaikki datatyypit on koodattava standardin ISO/IEC 8825-2 aligned-vaihtoehdon mukaisesti.

6. OLIOTUNNISTEET JA SOVELLUSTUNNISTEET

6.1. **Oliotunnisteet**

Tässä kappaleessa luetellut oliotunnisteet koskevat ainoastaan sukupolvea 2. Nämä oliotunnisteet määritellään viitteessä TR-03110-3, ja ne toistetaan tässä täsmällisyyden vuoksi. Nämä oliotunnisteet sisältyvät bsi-de:n alipuuhun:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Ajoneuvoyksikön todentamisprotokollan tunnisteet

```
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}
```

Esimerkki: Oletetaan, että ajoneuvoyksikön todentaminen suoritetaan SHA-384-algoritmiä käyttäen, jolloin oliotunnisteena käytetään (ASN.1-merkintätavan mukaan) `bsi-de protocols(2) smartcard(2) 2 2 4`. Tämän oliotunnisteen arvo pistenotaatiossa on `0.4.0.127.0.7.2.2.2.2.4`.

	Pistenotaatio	Tavun notaatio
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’

▼B

Sirun todentamisprotokollan tunnisteet

```
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}
```

Esimerkki: Oletetaan, että sirun todennus tehdään käyttämällä ECDH-algoritmia, minkä tuloksena tilapäisen AES-avaimen pituus on 128 bittiä. Tätä tilapäistä avainta käytetään myöhemmin salauslohkoja ketjuttavassa käyttötilassa (CBC), jolla varmistetaan tietojen luottamuksellisuus ja CMAC-algoritmiä käyttäen, jolla varmistetaan tietojen aitous. Siksi oliotunnisteena käytetään (ASN.1-merkintätavan mukaan) `bsi-de protocols(2) smartcard(2) 3 2 2`. Tämän oliotunnisteen arvo pistenotaatiossa on `0.4.0.127.0.7.2.2.3.2.2`.

	Pistenotaatio	Tavun notaatio
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. **Sovellustunnisteet**

Sukupolvi 2:

Sovellustunnisteen (AID) ulkoiselle GNSS-laitteistolle (sukupolvi 2) määrää ‘FF 44 54 45 47 4D’. Tämä on varattu sovellustunniste standardin ISO/IEC 7816-4 mukaisesti.

Huomautus: viimeinen 5 tavun koodattu DTEGM älykkään ajopiirturin ulkoiselle GNSS-laitteelle.

Sovellustunnisteen sukupolven 2 ajopiirturin kortin sovellukselle määrää ‘FF 53 4D 52 44 54’. Tämä on varattu sovellustunniste standardin ISO/IEC 7816-4 mukaisesti.

▼B

Lisäys 2

AJOPIIRTURIKORTTIEN ERITTELY

SISÄLLYSLUETTELO

1. JOHDANTO

1.1. Lyhenteet

1.2. Viitetiedot

2. SÄHKÖISET JA MEKAANISET OMINAISUUDET

2.1. Käyttöjännite ja virrankulutus

2.2. Ohjelmointijännite V_{pp}

2.3. Kellopulssin synnyttäminen ja kellotaajuus

2.4. I/O-liitin

2.5. Kortin toimintatilat

3. LAITTEISTO JA VIESTINTÄ

3.1. Johdanto

3.2. Lähetysprotokolla

3.2.1 Protokollat

3.2.2 ATR-signaali

3.2.3 PTS-komento

3.3. Käyttöoikeussäännöt

3.4. Komentojen ja virhekoodien tiivistelmä

3.5. Komentojen kuvaukset

3.5.1 SELECT

3.5.2 READ BINARY

3.5.3 UPDATE BINARY

3.5.4 GET CHALLENGE

3.5.5 VERIFY

3.5.6 GET RESPONSE

3.5.7 PSO: VERIFY CERTIFICATE

3.5.8 INTERNAL AUTHENTICATE

3.5.9 EXTERNAL AUTHENTICATE

3.5.10 GENERAL AUTHENTICATE

3.5.11 MANAGE SECURITY ENVIRONMENT

3.5.12 PSO: HASH

▼B

3.5.13 PERFORM HASH of FILE

3.5.14 PSO: COMPUTE DIGITAL SIGNATURE

3.5.15 PSO: VERIFY DIGITAL SIGNATURE

3.5.16 PROCESS DSRC MESSAGE

4. AJOPIIRTURIKORTTIEN TIEDOSTORAKENNE

4.1. MF-tiedosto

4.2. Kuljettajakortin sovellukset

4.2.1 Kuljettajakortin ensimmäisen sukupolven sovellus

4.2.2 Kuljettajakortin toisen sukupolven sovellus

4.3. Korjaamokortin sovellukset

4.3.1 Korjaamokortin ensimmäisen sukupolven sovellus

4.3.2 Korjaamokortin toisen sukupolven sovellus

4.4. Valvontakortin sovellukset

4.4.1 Valvontakortin ensimmäisen sukupolven sovellus

4.4.2 Valvontakortin toisen sukupolven sovellus

4.5. Yrityskortin sovellukset

4.5.1 Yrityskortin ensimmäisen sukupolven sovellus

4.5.2 Yrityskortin toisen sukupolven sovellus

1. JOHDANTO

1.1. **Lyhenteet**

Tässä lisäyksessä käytetään seuraavia lyhenteitä.

AC	(Access conditions) Käyttöehdot
AES	(Advanced encryption standard) AES-salaus
AID	(Application Identifier) Sovellustunniste
ALW	(Always) ALW-ehto; Aina
APDU	(Application protocol data unit) APDU-rakenne; Sovelluskerroksen tietoyksikkö
ATR	(Answer To Reset) Signaali, joka annetaan vastauksena RST-komentoon
AUT	(Authenticated) Alkuperä todennettu
C6, C7	Standardin ISO/IEC 7816-2 mukaiset kortin liittimet N:o 6 ja 7
cc	(clock cycles) Kellopulssi(a)
CHV	(Card holder verification information) Kortin haltijan kontrollitiedot
CLA	(Class byte of an APDU command) APDU-komennon luokkaa ilmaiseva tavu

▼B

DSRC	(Dedicated Short Range Communication) Lyhyen kantaman DSRC-tiedonsiirto
DF	(Dedicated File) DF-tiedosto DF-tiedosto voi sisältää muita (EF- tai DF-) tiedostoja
ECC	(Elliptic curve cryptography) Elliptisen käyrän salaus
EF	(Elementary File) EF-tiedosto
etu	(elementary time unit) Ajan perusyksikkö
G1	(Generation 1) Ensimmäinen sukupolvi
G2	(Generation 2) Toinen sukupolvi
IC	(Integrated circuit) Integroitu piiri
ICC	(Integrated Circuit Card) Integroidulla piirillä varustettu kortti
ID	(Identifier) Tunniste
IFD	(Interface Device) Liitäntälaite
IFS	(Information Field Size) Tietokentän koko
IFSC	(Information Field Size for the card) Kortin tietokentän koko
IFSD	(Information Field Size Device [for the Terminal]) Laitteen (päälaitteen) tietokentän koko
INS	(Instruction byte of an APDU command) APDU-komennon käskytavu
Lc	(Length of the input data for a APDU command) APDU-komennolla annettavan datan pituus
Le	(Length of the expected data [output data for a command]) Vastauksena odotettavan datan pituus (komennon vastauksena saatava data)
MF	(Master File) MF-tiedosto; Root-tason hakemistotiedosto
NAD	(Node address) T=1-protokollassa käytettävä solmun osoite
NEV	(Never) NEV-ehto; Ei koskaan
P1-P2	(Parameter bytes) Parametritavuja
PIN	(Personal identification number) PIN-koodi; Henkilökohtainen tunnusluku
PRO SM	(Protected with secure messaging) PRO SM -ehto; Salattu viesti
PTS	(Protocol transmission selection) PTS-komento; Lähetysprotokollan valinta
RFU	(Reserved for Future Use) Varattu myöhempään käyttöön
RST	(Reset [of the card]) RST-komento; (Kortin) alkutilaan palauttava komento
SFID	(Short EF Identifier) Lyhyt EF-tunniste
SM	(Secure messaging) Salattu sanomanvälitys
SW1-SW2	(Status bytes) Tilaa osoittavat tavut
TS	(Initial ATR character) ATR-signaalin ensimmäinen merkki
VPP	(Programming Voltage) Ohjelmointijännite
VU	(Vehicle Unit) Ajoneuvoyksikkö
XXh	Heksadesimaaliluku XX
‘XXh’	Heksadesimaaliluku XX
||	Ketjutusmerkki 03||04=0304

▼B

1.2. **Viitetiedot**

Tässä lisäyksessä käytetään seuraavia viitetietoja:

ISO/IEC 7816-2 Identification cards – Integrated circuit cards – Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Identification cards – Integrated circuit cards – Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Identification cards – Integrated circuit cards – Part 8: Commands for security operations. 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. ISO/IEC 9797-2:2011

2. SÄHKÖISET JA MEKAANISET OMINAISUUDET

TCS_01 Kaikkien sähköisten signaalien on oltava standardin ISO/IEC 7816-3 mukaisia, ellei muuta määrätä.

TCS_02 Kortin liittimien paikkojen ja mittojen on oltava standardin ISO/IEC 7816-2 mukaiset.

2.1. **Käyttöjännite ja virrankulutus**

TCS_03 Kortin on toimittava erittelyjen mukaisesti siten, että sen kulutus on standardissa ISO/IEC 7816-3 määritellyissä rajoissa.

TCS_04 Kortin on toimittava jännitteellä Vcc = 3V (± 0.3V) tai jännitteellä Vcc = 5V (± 0.5V).

Jännitteen valinnan on tapahduttava standardin ISO/IEC 7816-3 mukaisesti.

2.2. **Ohjelmointijännite V_{pp}**

TCS_05 Kortti ei saa tarvita ohjelmointijännitettä liittimelle C6. Liittimen C6 ei oleteta olevan kytkettynä liitäntälaitteessa. Kortin liitin C6 voidaan kytkeä jännitteeseen V_{cc} mutta sitä ei saa kytkeä maahan. Liittimellä olevaa jännitettä ei kuitenkaan saa ottaa huomioon.

2.3. **Kellopulssin synnyttäminen ja kellotaajuus**

TCS_06 Kortin on toimittava taajuusalueella 1–5 MHz; se voi kestää korkeampia taajuuksia. Yhden kortin käyttöjakson aikana kellotaajuus saa vaihdella ± 2 %. Kellotaajuus synnytetään ajoneuvoyksikössä eikä itse kortilla. Pulssileveyden suhde pulssiväliin saa vaihdella rajoissa 40–60 %.

TCS_07 Kortin EF ICC -tiedoston sisältämillä ehdoilla ulkoinen kello voidaan pysäyttää. EF ICC -tiedoston ensimmäinen tavu määrää Clockstop-tilan ehdot:

▼B

Matala	Korkea		
Bitti 3	Bitti 2	Bitti 1	
0	0	1	Clockstop-tila sallittu, looginen taso ei merkitsevä
0	1	1	Clockstop-tila sallittu, looginen taso 1 etusijalla
1	0	1	Clockstop-tila sallittu, looginen taso 0 etusijalla
0	0	0	Clockstop-tila ei sallittu
0	1	0	Clockstop-tila sallittu vain loogisen tason ollessa 1
1	0	0	Clockstop-tila sallittu vain loogisen tason ollessa 0

Bitit 4–8 eivät ole käytössä.

2.4. **I/O-liitin**

TCS_08 I/O-liitin C7 vastaanottaa ja siltä lähetetään dataa liitäntälaitteelle. Korttia käytettäessä saa vain joko kortti tai liitäntälaite olla lähetystilassa. Kortti ei kuitenkaan saa vahingoittua, vaikka molemmat olisivatkin lähetystilassa. Kortin on siirryttävä vastaanottotilaan aina, kun se ei lähetä dataa.

2.5. **Kortin toimintatilat**

TCS_09 Käyttöjännitteen ollessa kytkettynä kortilla on kaksi toimintatilaa:

käyttötila, jossa kortti on suorittaessaan komentoja tai ollessaan yhteydessä ajoneuvoyksikön kanssa,

lepotila, jossa kortti on aina muulloin; tässä tilassa kortin on säilytettävä kaikki sillä oleva data.

3. LAITTEISTO JA VIESTINTÄ

3.1. **Johdanto**

Tässä kohdassa kuvataan ne toiminnot, jotka ajopiirturikorteilta ja ajoneuvoyksiköiltä vähintään vaaditaan, jotta ne toimisivat oikein ja yhdessä.

Ajopiirturikortit ovat olemassa olevien ISO/IEC-standardien (erityisesti standardin ISO/IEC 7816) mukaisia niin paljon kuin mahdollista. Komennot ja protokollat on kuitenkin kuvattu täysin, jotta eräät käyttörajoitukset tai erot, mikäli niitä on, tulisivat määritellyiksi. Määritellyt komennot ovat täysin mainittujen standardien mukaisia paitsi tapauksissa, jotka on erikseen osoitettu.

3.2. **Lähetysprotokolla**

TCS_10 Lähetysprotokollan on oltava standardin ISO/IEC 7816-3 mukainen T=0-protokollan ja T=1-protokollan yhteydessä. Erityisesti ajoneuvoyksikön on tunnistettava kortin lähettämät odotusajan pidennykset.

3.2.1 *Protokollat*

TCS_11 Kortin on kyettävä käyttämään sekä **T=0**-protokollaa että **T=1**-protokollaa. Niiden lisäksi kortti voi tukea muita liitinorientoituneita protokollia.

TCS_12 **T=0** on oletusarvoinen protokolla, minkä vuoksi **PTS** (lähetysprotokollan valinta) -komento tarvitaan vaihtamaan käytettäväksi protokollaksi **T=1**.

▼B

TCS_13 Laitteiden on tuettava **suoraa koodaustapaa** (direct convention) molemmissa protokollissa; suora koodaustapa on näin ollen pakollinen kortille.

TCS_14 **Information field size card** (kortin tietokentän koko) -tavun tulee olla ATR-signaalin merkissä TA3. Tavun arvon on oltava vähintään ‘F0h’ (= 240 tavua).

Protokollia koskevat seuraavat rajoitukset:

TCS_15 **T=0**

— Liitäntälaitteen on kyettävä ottamaan vastaus I/O-liittimelle 400 kellopulssin kuluessa RST-signaalin etureunasta.

— Liitäntälaitteen on kyettävä lukemaan merkkejä 12 etu-yksikön (perusaikayksikön) välein.

— Liitäntälaitteen on luettava virheellinen merkki ja sen toisto, jos niiden välillä on 13 etu-yksikköä. Jos virheellinen merkki havaitaan, Error (virhe) -signaali voidaan antaa I/O-liittimelle 1 ja 2 etu-yksikön välillä. Laitteen on tuettava 1 etu-yksikön viivettä.

— Liitäntälaiteen on hyväksyttävä 33-tavuinen ATR-signaali (TS (ensimmäinen merkki) + 32).

— Jos ATR-signaalissa on merkki TC1, liitäntälaiteen lähettämille merkeille on annettava ylimääräinen varoaika (Extra Guard Time), vaikka kortin lähettämät merkit voidaan silti erottaa 12 etu-yksiköllä. Tämä pätee myös kortin lähettämään ACK-merkkiin liitäntälaitteen lähettämän P3-merkin jälkeen.

— Liitäntälaitteen on otettava huomioon kortin lähettämä NUL-merkki.

— Liitäntälaitteen on hyväksyttävä ACK-merkin antaminen vastakkaisvaiheisena (complementary mode).

— GET RESPONSE -komentoa ei voida käyttää chaining mode (ketjutus) -tilassa hakemaan dataa, jonka pituus saattaa ylittää 255 tavua.

TCS_16 **T=1**

— NAD (solmun osoite) -tavu: ei käytössä (NAD-tavun arvoksi on asetettava ‘00’).

— S-block ABORT -komento: ei käytössä.

— S-block VPP state error: ei käytössä.

— Tietokentän ketjutettu pituus ei saa ylittää 255:tä tavua (liitäntälaitteen varmistettava).

— Liitäntälaitteen on annettava information field size device (IFSD) (laitteen tietokentän koko) -arvo heti ATR-signaalin jälkeen: Liitäntälaiteen on lähetettävä S-Block IFS (tietokentän koko) -pyyntö ATR-signaalin jälkeen ja kortin on lähettävä takaisin S-Block IFS -tieto. IFSD:n suositeltava arvo on 254 tavua.

— Kortti ei pyydä IFS-koon muuttamista.

▼B

3.2.2 *ATR-signaali*

TCS_17 Laite tarkastaa ATR-signaalin tavut standardin ISO/IEC 7816-3 mukaisesti. ATR-signaaliin sisältyviä merkkejä, jotka liittyvät kortin historiaan (historical characters), ei todenneta.

Esimerkki kahta protokollaa tukevasta ATR-perussignaalista standardin ISO/IEC 7816-3 mukaisesti

Merkki	Arvo	Huomautukset
TS	‘3Bh’	Osoittaa suoraa koodaustapaa
T0	‘85h’	TD1 mukana; mukana on 5 kortin historiaan liittyvää tavua.
TD1	‘80h’	TD2 mukana; käytetään T=0-protokollaa
TD2	‘11h’	TD3 mukana; käytetään T=1-protokollaa
TA3	‘XXh’ (vähintään ‘F0h’)	Kortin tietokentän koko (IFSC)
TH1–TH5	‘XXh’	Kortin historiaan liittyvät merkit
TCK	‘XXh’	Tarkistusmerkki (XOR)

TCS_18 ATR (Answer To Reset) -signaalin jälkeen valitaan MF-tiedosto automaattisesti oletushakemistoksi.

3.2.3 *PTS-komento*

TCS_19 Oletusarvoinen protokolla on T=0. T=1-protokollan valitsemiseksi on kortin lähetettävä laitteelle PTS-komento (tunnetaan myös nimellä PPS-komento).

TCS_20 Koska kortin on tuettava sekä T=0- että T=1-protokollia, sen on myös tuettava PTS (protokollan vaihto) -perustoimintoa.

Kuten standardista ISO/IEC 7816-3 ilmenee, PTS-komentoa voidaan käyttää muuttamaan siirtonopeus suuremmaksi kuin kortin ATR-signaalissa mahdollisesti (TA(1)-tavussa) ehdottama.

Suurempien siirtonopeuksien tuki kortilla on valinnainen ominaisuus.

TCS_21 Jos kortti ei tue muita kuin oletusarvoista siirtonopeutta (tai jos se ei tue valittua siirtonopeutta), kortin on vastattava PTS-komentoon standardin ISO/IEC 7816-3 mukaisesti jättämällä PPS1-tavu pois.

Seuraavassa on esimerkkejä PTS-peruskomennosta protokollan valitsemiseksi:

Merkki	Arvo	Huomautukset
PPSS	‘FFh’	Käynnistysmerkki
PPS0	‘00h’ tai ‘01h’	PPS1–PPS3 eivät ole mukana; ‘00h’ valitsee T0-, ‘01h’ valitsee T1-protokollan.
PK	‘XXh’	Tarkistusmerkki: ‘XXh’ = ‘FFh’ jos PPS0 = ‘00h’, ‘XXh’ = ‘FEh’ jos PPS0 = ‘01h’.

▼B

3.3. **Käyttöoikeussäännöt**

TCS_22 Käyttöoikeussääntö määrittää käyttötilalle, eli komennolle, sitä vastaavat turvallisuusehdot. Jos turvallisuusehdot täyttyvät, komento käsitellään.

TCS_23 Ajopiirturikorttiin sovelletaan seuraavia turvallisuusehtoja:

Lyhenne	Merkitys
ALW	Toiminto on aina mahdollinen ja voidaan toteuttaa ilman rajoituksia. Komennon ja vastauksen tietoyksiköt lähetetään selväkielisinä, ts. ilman salattua sanomanvälitystä.
NEV	Toiminto ei ole koskaan mahdollinen.
PLAIN-C	Komennon tietoyksikkö lähetetään selväkielisenä, ts. ilman salattua sanomanvälitystä.
PWD	Toiminto voidaan suorittaa vain, jos korjaamokortin tunnusluku on tarkistettu onnistuneesti, ts. jos kortin sisäiseksi tietoturvatilaksi on määritetty ”PIN_Verified”. Komento on lähetettävä ilman salattua sanomanvälitystä.
EXT-AUT-G1	Toiminto voidaan suorittaa vain, jos ensimmäisen sukupolven todentamisen External Authenticate -komento (ks. myös lisäys 11, A osa) on suoritettu onnistuneesti.
SM-MAC-G1	Tietoyksikkö (komento ja vastaus) on suoritettava ensimmäisen sukupolven salatulla sanomanvälityksellä todentamisen vaativassa käyttötilassa (authentication-only mode) (ks. lisäys 11, A osa).
SM-C-MAC-G1	Komennon tietoyksikkö on suoritettava ensimmäisen sukupolven salatulla sanomanvälityksellä todentamisen vaativassa käyttötilassa (authentication-only mode) (ks. lisäys 11, A osa).
SM-R-ENC-G1	Vastauksen tietoyksikkö on suoritettava ensimmäisen sukupolven salatulla sanomanvälityksellä salauksen vaativassa käyttötilassa (encryption mode) (ks. lisäys 11, A osa), ts. sanoman autentikointikoodia ei palauteta.
SM-R-ENC-MAC-G1	Vastauksen tietoyksikkö on suoritettava ensimmäisen sukupolven salatulla sanomanvälityksellä käyttötilassa, joka edellyttää salauksen ja sen jälkeen todennuksen (encrypt-then-authenticate mode) (ks. lisäys 11, A osa).
SM-MAC-G2	Tietoyksikkö (komento ja vastaus) on suoritettava toisen sukupolven salatulla sanomanvälityksellä todentamisen vaativassa käyttötilassa (authentication-only mode) (ks. lisäys 11, B osa).
SM-C-MAC-G2	Komennon tietoyksikkö on suoritettava toisen sukupolven salatulla sanomanvälityksellä todentamisen vaativassa käyttötilassa (authentication-only mode) (ks. lisäys 11, B osa).
SM-R-ENC-MAC-G2	Vastauksen tietoyksikkö on suoritettava toisen sukupolven salatulla sanomanvälityksellä käyttötilassa, joka edellyttää salauksen ja sen jälkeen todennuksen (encrypt-then-authenticate mode) (ks. lisäys 11, B osa).

TCS_24 Edellä lueteltuja turvallisuusehtoja voidaan yhdistellä seuraavin tavoin:

AND: Kaikkien turvallisuusehtojen on täytyttävä

OR: Vähintään yhden turvallisuusehdon on täytyttävä

Tiedostojärjestelmän käyttöoikeussäännöt, eli SELECT-, READ BINARY- ja UPDATE BINARY -komennot, on käsitelty luvussa 4. Muiden komentojen käyttöoikeussäännöt on esitetty seuraavissa taulukoissa.

▼B

TCS_25 DF Tachograph G1 -sovelluksessa noudatetaan seuraavia käyttöoikeussääntöjä:

Komento	Kuljettajakortti	Korjaamokortti	Valvontakortti	Yrityskortti
External Authenticate				
— Ensimmäisen sukupolven todentamiseen	ALW	ALW	ALW	ALW
— Toisen sukupolven todentamiseen	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 sovelleta	Ei sovelleta	Ei sovelleta	Ei sovelleta
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ei sovelleta	Ei sovelleta
PSO: Hash	Ei sovelleta	Ei sovelleta	ALW	Ei sovelleta
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ei sovelleta	Ei sovelleta
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ei sovelleta	Ei sovelleta	ALW	Ei sovelleta
Verify	Ei sovelleta	ALW	Ei sovelleta	Ei sovelleta

TCS_26 DF Tachograph G2 -sovelluksessa noudatetaan seuraavia käyttöoikeussääntöjä:

Komento	Kuljettajakortti	Korjaamokortti	Valvontakortti	Yrityskortti
External Authenticate				
— Ensimmäisen sukupolven todentamiseen	Ei sovelleta	Ei sovelleta	Ei sovelleta	Ei sovelleta
— Toisen sukupolven todentamiseen	ALW	PWD	ALW	ALW
Internal Authenticate	Ei sovelleta	Ei sovelleta	Ei sovelleta	Ei sovelleta

▼B

Komento	Kuljettajakortti	Korjaamokortti	Valvontakortti	Yrityskortti
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 sovelleta	ALW	ALW	Ei sovelleta
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ei sovelleta	Ei sovelleta
PSO: Hash	Ei sovelleta	Ei sovelleta	ALW	Ei sovelleta
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ei sovelleta	Ei sovelleta
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ei sovelleta	Ei sovelleta	ALW	Ei sovelleta
Verify	Ei sovelleta	ALW	Ei sovelleta	Ei sovelleta

TCS_27 MF-tiedostossa noudatetaan seuraavia käyttöoikeussääntöjä:

Komento	Kuljettajakortti	Korjaamokortti	Valvontakortti	Yrityskortti
External Authenticate				
— Ensimmäisen sukupolven todentamiseen	Ei sovelleta	Ei sovelleta	Ei sovelleta	Ei sovelleta
— Toisen sukupolven todentamiseen	ALW	PWD	ALW	ALW
Internal Authenticate	Ei sovelleta	Ei sovelleta	Ei sovelleta	Ei sovelleta
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 sovelleta	Ei sovelleta	Ei sovelleta	Ei sovelleta

▼B

Komento	Kuljettajakortti	Korjaamokortti	Valvontakortti	Yrityskortti
PSO: Compute Digital Signature	Ei sovelleta	Ei sovelleta	Ei sovelleta	Ei sovelleta
PSO: Hash	Ei sovelleta	Ei sovelleta	Ei sovelleta	Ei sovelleta
PSO: Hash of File	Ei sovelleta	Ei sovelleta	Ei sovelleta	Ei sovelleta
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Ei sovelleta	ALW	Ei sovelleta	Ei sovelleta

TCS_28 Ajopiirturikortti voi hyväksyä tai hylätä komennon, jonka tietoturvan taso on turvallisuusehtojen vaatimuksia korkeampi. Jos turvallisuusehto on siis ALW (tai PLAIN-C), kortti voi hyväksyä komennon salatulla sanomanvälityksellä (salauksen ja / tai todentamisen vaativa käyttötila). Jos turvallisuusehto edellyttää salattua sanomanvälitystä todentamisen vaativassa käyttötilassa, ajopiirturikortti voi hyväksyä komennon saman sukupolven salatulla sanomanvälityksellä todentamisen ja salauksessa vaativassa käyttötilassa.

Huomautus: Komentojen kuvauksissa on lisätietoja komentojen tuesta ajopiirturikorttien eri tyypeille ja eri DF:ille.

3.4. **Komentojen ja virhekoodien tiivistelmä**

Komennot ja tiedostorakenne on saatu standardista ISO/IEC 7816-4 ja ne ovat tämän standardin mukaisia.

Tässä osassa kuvataan seuraavia APDU-rakenteen komento-vastauspareja. Ensimmäisen ja toisen sukupolven tukemat komentovariantit on esitetty niitä vastaavissa komentojen kuvauksissa.

Komento	INS (käskytavu)
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’

▼B

Komento	INS (käskytavu)
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 Tilaa ilmaisevat tavut SW1 ja SW2 sisällytetään kaikkiin vastausviesteihin, ja ne osoittavat komennon suorittamisen tilan.

SW1	SW2	Merkitys
90	00	Normaali suoritus.
61	XX	Normaali suoritus. XX = vastaukseen käytettävissä olevien tavujen määrä.
62	81	Varoituksen suoritus. Osa palautettavista tiedoista on voinut tuhoutua
63	00	Todentaminen epäonnistui (varoitus)
63	CX	Väärä CHV (PIN). ‘X’ on jäljellä olevien yrityskertojen laskuri.
64	00	Toteutusvirhe – haihtumattoman muistin tila muuttumaton. Virhe eheydessä.
65	00	Toteutusvirhe – haihtumattoman muistin tila muuttunut
65	81	Toteutusvirhe – haihtumattoman muistin tila muuttunut – muistivirhe
66	88	Tietoturvavirhe: väärä tarkistussumma (salatun sanomanvälityksen yhteydessä) tai väärä varmenne (varmenteen todennuksen yhteydessä) tai väärä kryptogrammi (ulkoisen todennuksen yhteydessä) tai väärä allekirjoitus (allekirjoituksen todennuksen yhteydessä)
67	00	Väärä pituus (väärä Lc tai Le)

▼B

SW1	SW2	Merkitys
68	82	Salattua sanomanvälitystä ei tueta
68	83	Odotettu ketjun viimeinen komento
69	00	Kielletty komento (protokollassa T=0 ei käytettävissä vastausta)
69	82	Tietoturvatilan vaatimuksia ei täytetty.
69	83	Todennusmenetelmän käyttö estetty.
69	85	Käyttöehtoja ei täytetty.
69	86	Komento ei sallittu (ei käytössä olevaa EF-tiedostoa).
69	87	Odotettuja salattuja viestitietoja puuttuu
69	88	Salatuissa viestitiedoissa virheitä
6A	80	Datakentässä väärät parametrit
6A	82	Tiedostoa ei löydy.
6A	86	Väärät parametrit P1-P2.
6A	88	Kyseessä olevaa dataa ei löydy.
6B	00	Väärät parametrit (suhteellinen osoite EF-tiedoston ulkopuolella).
6C	XX	Väärä pituus, SW2 osoittaa tarkan pituuden. Mitään tietokenttää ei palauteta vastauksena.
6D	00	Käskykoodia ei tueta tai se ei ole voimassa.
6E	00	Luokkaa ei tueta.
6F	00	Muut tarkastusvirheet

TCS_30 Jos yhdessä komennon tietoyksikössä toteutuu enemmän kuin yksi virhe-ehto, kortti voi palauttaa minkä tahansa asianmukaisista tilaa osoittavista tavuista.

3.5. **Komentojen kuvaukset**

Tässä luvussa kuvataan ajopiirturikorttien pakolliset komennot.

Salaustoimiin liittyviä lisätietoja on lisäyksessä 11 (Yhteiset turvamekanismit) ensimmäisen ja toisen sukupolven ajopiirturien osalta.

Kaikki komennot on kuvattu käytetystä protokollasta (T=0 tai T=1) riippumatta. APDU-rakenteen tavut CLA, INS, P1, P2, Lc ja Le on aina näytetty. Jos kuvattavassa komennossa ei tarvita Lc- tai Le-tavuja, niihin liittyvän pituuden, arvon ja kuvauksen kohta on jätetty tyhjäksi.

TCS_31 Jos molempia pituutta osoittavia tavuja (Lc ja Le) pyydetään, kuvattu komento on jaettava kahteen osaan, jos liitäntälaite käyttää T=0-protokollaa: liitäntälaite lähettää kuvauksen mukaisen komennon, jossa P3=Lc + data ja sen jälkeen GET RESPONSE -komennon (ks. kohta 3.5.6), jossa P3=Le.

TCS_32 Jos molempia pituutta osoittavia tavuja pyydetään ja Le=0:

▼B

— käytettäessä T=1-protokollaa, kortin on vastattava tietoon Le=0 lähettämällä kaikki tulostettavissa olevat tiedot.

— käytettäessä T=0-protokollaa, liitäntälaitteen on lähetettävä ensimmäinen komento, jossa P3=Lc + data, ja kortin on vastattava (tästä käytännössä aiheutuvaan) tietoon Le=0 tilaa osoittavilla tavuilla '**61La**', missä La on vastaukseen käytettävissä olevien tavujen määrä. Liitäntälaite antaa sitten GET RESPONSE -komennon, jossa P3 = La, lukeakseen tiedot.

TCS_33 Ajopiirturi voi lisätoimintona tukea laajennettuja pituuskenttiä standardin ISO/IEC 7816-4 mukaisesti. Laajennettuja pituuskenttiä tukevan ajopiirturikortin on

— ilmoitettava laajennetun pituuskentän tuki ATR-signaalissa

— annettava tuetut puskurikoot laajennettuja pituuskenttiä koskevan tiedon avulla EF ATR/INFO -tiedostossa, ks. TCS_146.

— ilmoitettava, tukeeko se laajennettuja pituuskenttiä T=1- ja / tai T=0-protokollan osalta EF Extended_Length -tiedostossa, ks. TCS_147.

— tuettava laajennettuja pituuskenttiä ajopiirturisovelluksen ensimmäisen ja toisen sukupolven osalta.

Huomautus:

Kaikki komennot on määritetty lyhyitä pituuskenttiä varten. Laajennetun pituuskentän tietoyksiköiden käyttö ilmenee standardista ISO/IEC 7816-4.

Komennot on määritetty pääasiassa selväkielistä tilaa varten, siis ilman salattua sanomanvälitystä, sillä salatun sanomavälityksen kerros on määritetty lisäyksessä 11. Komennon käyttöoikeussäännöistä käy ilmi, tukeeko komento salattua sanomanvälitystä ja tukeeko komento ensimmäisen ja / tai toisen sukupolven salattua sanomanvälitystä. Joitain komentovariantteja on kuvattu salatun sanomanvälityksen kanssa esimerkkien antamiseksi salatun sanomanvälityksen käytöstä.

TCS_34 Ajoneuvoyksikön on suoritettava toisen sukupolven ajoneuvoyksikön ja kortin molemminpuolinen todentamisprotokolla käyttöjaksoa varten kokonaisuudessaan varmenteen todentaminen mukaan lukien (mikäli sitä edellytetään) joko DF Tachograph-, DF Tachograph_G2- tai MF-tiedostossa.

3.5.1 *SELECT*

Tämä komento on standardin ISO/IEC 7816-4 mukainen, mutta sen käyttö on rajoitettua standardissa määriteltyyn komentoon verrattuna.

SELECT-komentoa käytetään:

— valitsemaan sovelluksen sisältävä DF-tiedosto (on käytettävä valintaa nimen perusteella)

— valitsemaan EF-tiedosto annetun tiedostotunnisteen perusteella

3.5.1.1 Valinta nimen (AID) perusteella

Tällä komennolla voidaan valita kortilla oleva sovelluksen sisältävä DF-tiedosto.

TCS_35 Tämä komento voidaan antaa mistä hyvänsä tiedostorakenteessa (ATR-signaalin jälkeen tai milloin hyvänsä).

▼B

TCS_36 Sovelluksen valitseminen asettaa senhetkisen tietoturvaympäristön alkutilaansa. Sovelluksen valitsemisen jälkeen mikään käytössä oleva julkinen avain ei ole enää valittuna. Myöskään EXT-AUT-G1-käyttöehto ei enää ole voimassa. Jos komento suoritettiin ilman salattua sanomanvälitystä, aiemmat avaimet eivät ole enää käytettävissä salattuun sanomanvälitykseen.

TCS_37 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘A4h’	
P1	1	‘04h’	Valinta nimen (AID) perusteella
P2	1	‘0Ch’	Vastausta ei odoteta
Lc	1	‘NNh’	Kortille lähetettävien tavujen määrä (sovellustunnisteen (AID) pituus): ‘06h’ ajopiirturisovellukselle
#6-#(5+NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ ensimmäisen sukupolven ajopiirturisovellukselle AID: ‘FF 53 4D 52 44 54’ toisen sukupolven ajopiirturisovellukselle

SELECT-komentoon ei tarvita vastausta (Le-tavu puuttuu käytettäessä T=1-protokollaa, tai vastausta ei pyydetä käytettäessä T=0-protokollaa).

TCS_38 **Vastausviesti (vastausta ei pyydetty)**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos sovellustunnistetta vastaavaa sovellusta ei löytynyt, suorittamisen tilaa kuvaava vastaus on ‘**6A82**’.

— T=1-protokollaa käytettäessä tavun Le ollessa mukana tilaa kuvaava vastaus on ‘**6700**’.

— T=0-protokollaa käytettäessä, kun vastausta on pyydetty SELECT-komennon jälkeen, tilaa kuvaava vastaus on ‘**6900**’.

— Jos valittu sovellus katsotaan vialliseksi (tiedoston ominaisuuksissa on todettu eheysvirhe), suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

3.5.1.2 EF-tiedoston valinta sen tiedostotunnisteen perusteella

TCS_39 **Komentoviesti**

TCS_40 Ajopiirturikortin on tuettava lisäyksen 11 B osassa määritettyä toisen sukupolven salattua sanomanvälitystä tämän komentovariantin osalta.

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘A4h’	
P1	1	‘02h’	Käytössä olevan DF-tiedoston alaisen EF-tiedoston valinta

▼B

Tavu	Pituus	Arvo	Kuvaus
P2	1	‘0Ch’	Vastausta ei odoteta
Lc	1	‘02h’	Kortille lähetettävien tavujen määrä
#6-#7	2	‘XXXXh’	Tiedostotunniste

SELECT-komentoon ei tarvita vastausta (Le-tavu puuttuu käytettäessä T=1-protokollaa, tai vastausta ei pyydetä käytettäessä T=0-protokollaa).

TCS_41 **Vastausviesti (vastausta ei pyydetty)**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos tiedostotunnistetta vastaavaa tiedostoa ei löytynyt, suorittamisen tilaa kuvaava vastaus on ‘**6A82**’.

— T=1-protokollaa käytettäessä tavun Le ollessa mukana tilaa kuvaava vastaus on ‘**6700**’.

— T=0-protokollaa käytettäessä, kun vastausta on pyydetty SELECT-komennon jälkeen, tilaa kuvaava vastaus on ‘**6900**’.

— Jos valittu tiedosto katsotaan vialliseksi (tiedoston ominaisuuksissa on todettu eheysvirhe), suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

3.5.2 *READ BINARY*

Tämä komento on standardin ISO/IEC 7816-4 mukainen, mutta sen käyttö on rajoitettua standardissa määriteltyyn komentoon verrattuna.

READ BINARY -komentoa käytetään lukemaan tietoja transparenttityyppisestä EF-tiedostosta.

Kortin vastaus koostuu luetuista tiedoista, jotka voidaan tarvittaessa suojata salatun sanomanvälityksen rakenteella.

3.5.2.1 Komento, jos suhteellinen osoite parametreissa P1-P2

Tämän komennon avulla liitäntälaite voi lukea tietoja kulloinkin valitusta EF-tiedostosta ilman salattua sanomanvälitystä.

Huomautus: Tätä komentoa voidaan käyttää ilman salattua sanomanvälitystä vain sellaisten tiedostojen lukemiseen, jotka tukevat ALW-turvallisuusehtoa Lue (Read) -käyttötilassa.

TCS_42 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘B0h’	READ BINARY
P1	1	‘XXh’	Suhteellinen osoite tavuina tiedoston alusta laskien: merkitsevin tavu

▼B

Tavu	Pituus	Arvo	Kuvaus
P2	1	‘XXh’	Suhteellinen osoite tavuina tiedoston alusta laskien: vähiten merkitsevä tavu
Le	1	‘XXh’	Vastauksena odotettavan datan pituus. Luettavien tavujen määrä.

Huomautus: P1-tavun bitti 8 on asetettava nollaksi.

TCS_43 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
#1-#X	X	‘XX..XXh’	Tiedot luettu
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos mitään EF-tiedostoa ei valita, suorittamisen tilaa kuvaava vastaus on ‘**6986**’.

— Jos valitun tiedoston turvallisuusehtoja ei täytetty, komennon suorittaminen keskeytetään viestillä ‘**6982**’.

— Jos suhteellinen osoite ei ole EF-tiedoston koon mukainen (suhteellinen osoite > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6B00**’.

— Jos luettavan datan pituus ei ole EF-tiedoston koon mukainen (suhteellinen osoite + Le > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6700**’ tai ‘**6Cxx**’, jossa ‘xx’ ilmaisee tarkan pituuden.

— Jos tiedoston ominaisuuksissa on todettu eheysvirhe, kortin on pidettävä tiedostoa vaurioituneena ja lukukelvottomana, ja suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

— Jos tallennetuissa tiedoissa todetaan eheysvirhe, kortin on palautettava pyydetyt tiedot ja suorittamisen tilaa kuvaava vastaus on ‘**6281**’.

3.5.2.1.1 Komento salattua sanomanvälitystä käyttäen (esimerkkejä)

Tämän komennon avulla liitäntälaite voi lukea tietoja kulloinkin valitusta EF-tiedostosta käyttäen salattua sanomanvälitystä, jonka avulla vastaanotetun datan eheys voidaan todentaa ja pitää data salassa, mikäli turvallisuusehtoa SM-R-ENC-MAC-G1 (1. sukupolvi) tai SM-R-ENC-MAC-G2 (2. sukupolvi) sovelletaan.

TCS_44 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘0Ch’	Salattua sanomanvälitystä pyydetään
INS (käskytavu)	1	‘B0h’	READ BINARY
P1	1	‘XXh’	P1 (suhteellinen osoite tavuina tiedoston alusta laskien): merkitsevin tavu
P2	1	‘XXh’	P2 (suhteellinen osoite tavuina tiedoston alusta laskien): vähiten merkitsevä tavu

▼B

Tavu	Pituus	Arvo	Kuvaus
Lc	1	‘XXh’	Salattua sanomanvälitystä varten kortille lähetettävän datan pituus
#6	1	‘97h’	T_{LE}: odotetun pituusmääritteen tuntomerkki.
#7	1	‘01h’	L_{LE}: odotettu datan pituus
#8	1	‘NNh’	Odotetun pituuden määrite (alkuperäinen Le): luettavien tavujen määrä
#9	1	‘8Eh’	T_{CC}: salauksen tarkistussumman tuntomerkki
#10	1	‘XXh’	L_{CC}: seuraavan salauksen tarkistussumman pituus ‘04h’ ensimmäisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, A osa) ‘08h’, ‘0Ch’ tai ‘10h’ riippuen AES-avaimen pituudesta toisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, B osa)
#11-#(10+L)	L	‘XX..XXh’	Salauksen tarkistussumma
Le	1	‘00h’	Kuten standardissa ISO/IEC 7816-4 on määritelty

TCS_45 **Vastausviesti, jos turvallisuusehtoa SM-R-ENC-MAC-G1 (1. sukupolvi) / SM-R-ENC-MAC-G2 (2. sukupolvi) ei vaadita ja salattua sanomanvälitystä varten lähetetyn datan muoto on oikea:**

Tavu	Pituus	Arvo	Kuvaus
#1	1	‘99h’	suorittamisen tilan tuntomerkki (SW1-SW2) – valinnainen ensimmäisen sukupolven salatussa sanomavälityksessä
#2	1	‘02h’	Suorittamisen tilan pituus
#3 – #4	2	‘XX XXh’	Suojaamattoman vastauksen tietoyksikön suorittamisen tila
#5	1	‘81h’	T_{PV}: salaamattoman datan tuntomerkki
#6	L	‘NNh’ tai ‘81 NNh’	L_{PV}: vastauksena saadun datan pituus (= alkuperäinen Le). L sisältää kaksi tavua, jos L_{PV}> 127 tavua.
#(6+L)-#(5+L+NN)	NN	‘XX..XXh’	Salaamatonta dataa
#(6+L+NN)	1	‘8Eh’	T_{CC}: salauksen tarkistussumman tuntomerkki
#(7+L+NN)	1	‘XXh’	L_{CC}: seuraavan salauksen tarkistussumman pituus ‘04h’ ensimmäisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, A osa) ‘08h’, ‘0Ch’ tai ‘10h’ riippuen AES-avaimen pituudesta toisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, B osa)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Salauksen tarkistussumma
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

▼B

TCS_46 **Vastausviesti, jos turvallisuusehtoa SM-R-ENC-MAC-G1 (1. sukupolvi) / SM-R-ENC-MAC-G2 (2. sukupolvi) vaaditaan ja salattua sanomanvälitystä varten lähetetyn datan muoto on oikea:**

Tavu	Pituus	Arvo	Kuvaus
#1	1	‘87h’	$T_{PI\ CG}$: salatun datan (kryptogrammin) tuntomerkki (tag)
#2	L	‘MMh’ tai ‘81 MMh’	$L_{PI\ CG}$: Vastauksena saadun salatun datan pituus (täyttämisen takia eri kuin komennon alkuperäinen Le): L sisältää kaksi tavua, jos $L_{PI\ CG} > 127$ tavua.
#(2+L)-#(1+L+MM)	MM	‘01XX..XXh’	Salattu data: täytön osoitin ja kryptogrammi
#(2+L+MM)	1	‘99h’	suorittamisen tilan tuntomerkki (SW1-SW2) – valinnainen ensimmäisen sukupolven salatussa sanomavälityksessä
#(3+L+MM)	1	‘02h’	Suorittamisen tilan pituus
#(4+L+MM) – #(5+L+MM)	2	‘XX XXh’	Suojaamattoman vastauksen tietoyksikön suorittamisen tila
#(6+L+MM)	1	‘8Eh’	T_{CC}: salauksen tarkistussumman tuntomerkki
#(7+L+MM)	1	‘XXh’	L_{CC}: seuraavan salauksen tarkistussumman pituus ‘04h’ ensimmäisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, A osa) ‘08h’, ‘0Ch’ tai ‘10h’ riippuen AES-avaimen pituudesta toisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, B osa)
#(8+L+MM)-#(7+N+L+MM)	määrä	‘XX..XXh’	Salauksen tarkistussumma
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

READ BINARY -komento voi palauttaa normaalit suorittamisen tilat, jotka on lueteltu kohdassa TCS_43 tuntomerkin ‘99h’ alla, kuten kuvattu kohdassa TCS_59 salatun sanomanvälityksen vastausviestirakenteiden avulla.

Tämän lisäksi saattaa ilmetä joitakin erityisesti salattuun sanomanvälitykseen liittyviä virhetilanteita. Tällöin vastauksena annetaan pelkkä suorittamisen tilan kuvaus ilman salatun sanomanvälityksen rakenteita:

TCS_47 **Vastausviesti, jos salattua sanomanvälitystä varten lähetetyn datan muoto on väärä**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos käytössä ei ole voimassa olevaa tilapäistä avainta, suorittamisen tilaa kuvaava vastaus on ‘**6A88**’. Näin tapahtuu, jos tilapäistä avainta ei vielä ole luotu tai sen voimassaolo on päättynyt (tässä tapauksessa liitäntälaitteen on suoritettava uudelleen molemminpuolinen todentamisprosessi uuden tilapäisen avaimen luomiseksi).

▼B

— Jos datasta puuttuu joitakin odotettuja osia, suorittamisen tilaa kuvaava vastaus on ‘**6987**’: tämä virhe tapahtuu, jos odotettu tuntomerkki puuttuu tai komennon rakenne on väärä.

— Jos jotkin datan osat ovat virheellisiä, suorittamisen tilaa kuvaava vastaus on ‘**6988**’: tämä virhe tapahtuu, jos kaikki tarvittavat tuntomerkit ovat mukana, mutta jotkin datan pituudet eroavat odotetuista pituuksista.

— Jos salauksen tarkistussumman todentaminen epäonnistuu, suorittamisen tilaa kuvaava vastaus on ‘**6688**’.

3.5.2.2 Komento lyhyellä EF (Elementary File) -tunnisteella

Tämän komentovariantin avulla liitäntälaite voi valita EF-tiedoston lyhyellä EF-tunnisteella ja lukea tietoja valitusta EF-tiedostosta.

TCS_48 Ajopiirturikortin on tuettava tätä komentovarianttia kaikkien sellaisten EF-tiedostojen osalta, joilla on määritetty lyhyt EF-tunniste. Lyhyet EF-tunnisteet on esitetty luvussa 4.

TCS_49 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘B0h’	READ BINARY
P1	1	‘XXh’	Bitin 8 arvoksi on asetettu 1 Bittien 7 ja 6 arvoksi on asetettu 00 Bitit 5–1 koodaavat vastaavan EF-tiedoston lyhyen EF-tunnisteen
P2	1	‘XXh’	Koodaa suhteellisen osoitteen 0 tavusta 255 tavuun P1:n viittaamassa EF-tiedostossa
Le	1	‘XXh’	Vastauksena odotettavan datan pituus. Luettavien tavujen määrä.

Huomautus: Toisen sukupolven ajopiirturisovelluksessa käytettävät lyhyet EF-tunnisteet on esitetty luvussa 4.

Jos P1 koodaa lyhyen EF-tunnisteen ja komennon suorittaminen onnistuu, tunnistetusta EF-tiedostosta tulee kulloinkin valittu EF-tiedosto (käytössä oleva EF).

TCS_50 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
#1-#L	L	‘XX..XXh’	Tiedot luettu
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos lyhyttä EF-tunnistetta vastaavaa tiedostoa ei löytynyt, suorittamisen tilaa kuvaava vastaus on ‘**6A82**’.

— Jos valitun tiedoston turvallisuusehtoja ei täytetty, komennon suorittaminen keskeytetään viestillä ‘**6982**’.

▼B

— Jos suhteellinen osoite ei ole EF-tiedoston koon mukainen (suhteellinen osoite > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6B00**’.

— Jos luettavan datan pituus ei ole EF-tiedoston koon mukainen (suhteellinen osoite + Le > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6700**’ tai ‘**6Cxx**’, jossa ‘xx’ ilmaisee tarkan pituuden.

— Jos tiedoston ominaisuuksissa on todettu eheysvirhe, kortin on pidettävä tiedostoa vaurioituneena ja lukukelvottomana, ja suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

— Jos tallennetuissa tiedoissa todetaan eheysvirhe, kortin on palautettava pyydetyt tiedot ja suorittamisen tilaa kuvaava vastaus on ‘**6281**’.

3.5.2.3 Komento, jossa pariton käskytavu

Tämän komentovariantin avulla liitäntälaite voi lukea tietoja EF-tiedostosta, jossa on yli 32 768 tavua.

TCS_51 Ajopiirturikortin, joka tukee yli 32 768 tavun EF-tiedostoja, on tuettava tätä komentovarianttia tällaisten EF-tiedostojen kohdalla. Ajopiirturikortti voi tukea tai olla tukematta tätä komentoa muiden EF-tiedostojen kohdalla poikkeuksena EF-tiedosto Sensor_Installation_Data, ks. TCS_156 ja TCS_160.

TCS_52 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘B1h’	READ BINARY
P1	1	‘00h’	Käytössä oleva EF-tiedosto
P2	1	‘00h’	
Lc	1	‘NNh’	Lc Offset-dataobjektin pituus.
#6-#(5+NN)	NN	‘XX..XXh’	Offset-dataobjekti: Tuntomerkki ‘54h’ Pituus ‘01h’ tai ‘02h’ Arvo offset
Le	1	‘XXh’	Luettavien tavujen määrä.

Liitäntälaitteen on koodattava offset-dataobjektin pituus mahdollisimman pienellä määrällä tavuja, ts. liitäntälaitteen on koodattava käyttäen pituutta osoittavaa tavua ‘01h’ suhteellinen osoite välillä 0–255 tavua ja käyttäen pituutta osoittavaa tavua ‘02h’ suhteellinen osoite välillä ‘256’–‘65 535’ tavua.

TCS_53 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
#1-#L	L	‘XX..XXh’	Luetut tiedot suojataan valinnaiseen (discretionary) dataobjektiin tuntomerkillä ‘53h’.
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

▼B

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos mitään EF-tiedostoa ei valita, suorittamisen tilaa kuvaava vastaus on ‘**6986**’.

— Jos valitun tiedoston turvallisuusehtoja ei täytetty, komennon suorittaminen keskeytetään viestillä ‘**6982**’.

— Jos suhteellinen osoite ei ole EF-tiedoston koon mukainen (suhteellinen osoite > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6B00**’.

— Jos luettavan datan pituus ei ole EF-tiedoston koon mukainen (suhteellinen osoite + Le > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6700**’ tai ‘**6Cxx**’, jossa ‘xx’ ilmaisee tarkan pituuden.

— Jos tiedoston ominaisuuksissa on todettu eheysvirhe, kortin on pidettävä tiedostoa vaurioituneena ja lukukelvottomana, ja suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

— Jos tallennetuissa tiedoissa todetaan eheysvirhe, kortin on palautettava pyydetyt tiedot ja suorittamisen tilaa kuvaava vastaus on ‘**6281**’.

3.5.2.3.1 Komento salattua sanomanvälitystä käyttäen (esimerkki)

Seuraavalla esimerkillä havainnollistetaan salatun sanomanvälityksen käyttöä tilanteessa, jossa turvallisuusehtoa SM-MAC-G2 sovelletaan.

TCS_54 Komentoviesti

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘0Ch’	Salattua sanomanvälitystä pyydetään
INS (käskytavu)	1	‘B1h’	READ BINARY
P1	1	‘00h’	Käytössä oleva EF-tiedosto
P2	1	‘00h’	
Lc	1	‘XXh’	Varmistetun tietokentän pituus
#6	1	‘B3h’	BER-TLV-koodatun salaamattoman datan tuntomerkki
#7	1	‘NNh’	L_{PV}: lähetettävän datan pituus
#(8)-#(7+NN)	NN	‘XX..XXh’	Salaamaton data, joka on BER-TLV-koodattu, ts. offset-dataobjekti tuntomerkillä ‘54’
#(8+NN)	1	‘97h’	T_{LE}: odotetun pituusmääritteen tuntomerkki.
#(9+NN)	1	‘01h’	L_{LE}: odotettu datan pituus
#(10+NN)	1	‘XXh’	Odotetun pituuden määrite (alkueräinen Le): luettavien tavujen määrä
#(11+NN)	1	‘8Eh’	T_{CC}: salauksen tarkistussumman tuntomerkki
#(12+NN)	1	‘XXh’	L_{CC}: seuraavan salauksen tarkistussumman pituus ‘08h’, ‘0Ch’ tai ‘10h’ riippuen AES-avaimen pituudesta toisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, B osa)
#(13+NN)-#(12+M+NN)	M	‘XX..XXh’	Salauksen tarkistussumma
Le	1	‘00h’	Kuten standardissa ISO/IEC 7816-4 on määritelty

▼B

TCS_55 Vastausviesti, jos komennon tulos on onnistunut

Tavu	Pituus	Arvo	Kuvaus
#1	1	‘B3h’	Salaamaton data, joka on BER-TLV-koodattu
#2	L	‘NNh’ tai ‘81 NNh’	L_{PV}: vastauksena saadun datan pituus (= alkuperäinen Le). L sisältää kaksi tavua, jos L_{PV}> 127 tavua.
#(2+L)-#(1+L+NN)	NN	‘XX..XXh’	BER-TLV-koodattu salaamaton data, ts. luetut tiedot suojataan valinnaiseen (discretionary) dataobjektiin tuntomerkillä ‘53h’.
#(2+L+NN)	1	‘99h’	Suojaamattoman vastauksen tietoyksikön suorittamisen tila
#(3+L+NN)	1	‘02h’	Suorittamisen tilan pituus
#(4+L+NN) – #(5+L+NN)	2	‘XX XXh’	Suojaamattoman vastauksen tietoyksikön suorittamisen tila
#(6+L+NN)	1	‘8Eh’	T_{CC}: salauksen tarkistussumman tuntomerkki
#(7+L+NN)	1	‘XXh’	L_{CC}: seuraavan salauksen tarkistussumman pituus ‘08h’, ‘0Ch’ tai ‘10h’ riippuen AES-avaimen pituudesta toisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, B osa)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Salauksen tarkistussumma
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

3.5.3 *UPDATE BINARY*

Tämä komento on standardin ISO/IEC 7816-4 mukainen, mutta sen käyttö on rajoitettua standardissa määriteltyyn komentoon verrattuna.

UPDATE BINARY -komento käynnistää EF-binaaritiedostossa jo olevien bittien päivittämisen (poistamisen + kirjoittamisen) komennon tietoyksikössä olevilla biteillä.

3.5.3.1 Komento, jos suhteellinen osoite parametreissa P1–P2

Tämän komennon avulla liitäntälaite voi kirjoittaa tietoja kulloinkin valittuun EF-tiedostoon ilman, että kortti todentaa vastaanotetun datan eheyttä.

Huomautus: Tällä komennolla, joka toimii ilman salattua sanomanvälitystä, voidaan päivittää vain tiedosto, joka tukee ALW-turvallisuusehtoa Päivitä (Update) -käyttötilassa.

TCS_56 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘D6h’	UPDATE BINARY
P1	1	‘XXh’	Suhteellinen osoite tavuina tiedoston alusta laskien: merkitsevin tavu
P2	1	‘XXh’	Suhteellinen osoite tavuina tiedoston alusta laskien: vähiten merkitsevä tavu

▼B

Tavu	Pituus	Arvo	Kuvaus
Lc	1	‘NNh’	Lc päivitettävän datan pituus. Kirjoitettavien tavujen määrä.
#6-#(5+NN)	NN	‘XX..XXh’	Kirjoitettava data

Huomautus: P1-tavun bitti 8 on asetettava nollaksi.

TCS_57 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos mitään EF-tiedostoa ei valita, suorittamisen tilaa kuvaava vastaus on ‘**6986**’.

— Jos valitun tiedoston turvallisuusehtoja ei täytetty, komennon suorittaminen keskeytetään viestillä ‘**6982**’.

— Jos suhteellinen osoite ei ole EF-tiedoston koon mukainen (suhteellinen osoite > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6B00**’.

— Jos kirjoitettavan datan pituus ei ole EF-tiedoston koon mukainen (suhteellinen osoite + Lc > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6700**’.

— Jos tiedoston ominaisuuksissa on todettu eheysvirhe, kortin on pidettävä tiedostoa vaurioituneena ja lukukelvottomana, ja suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6500**’.

— Jos kirjoittaminen ei onnistu, suorittamisen tilaa kuvaava vastaus on ‘**6581**’.

3.5.3.1.1 Komento salattua sanomanvälitystä käyttäen (esimerkkejä)

Tämän komennon avulla liitäntälaite voi kirjoittaa tietoja kulloinkin valittuun EF-tiedostoon siten, että kortti todentaa vastaanotetun datan eheyden. Koska salassapitoa ei vaadita, dataa ei salata.

TCS_58 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘0Ch’	Salattua sanomanvälitystä pyydetään
INS (käskytavu)	1	‘D6h’	UPDATE BINARY
P1	1	‘XXh’	Suhteellinen osoite tavuina tiedoston alusta laskien: merkitsevin tavu
P2	1	‘XXh’	Suhteellinen osoite tavuina tiedoston alusta laskien: vähiten merkitsevä tavu
Lc	1	‘XXh’	Varmistetun tietokentän pituus
#6	1	‘81h’	T_{PV}: salaamattoman datan tuntomerkki
#7	L	‘NNh’ tai ‘81 NNh’	L_{PV}: lähetettävän datan pituus. L sisältää kaksi tavua, jos L_{PV}> 127 tavua.

▼B

Tavu	Pituus	Arvo	Kuvaus
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Salaamatonta dataa (kirjoitettava data)
#(7+L+NN)	1	‘8Eh’	T_{CC}: salauksen tarkistussumman tuntomerkki
#(8+L+NN)	1	‘XXh’	L_{CC}: seuraavan salauksen tarkistussumman pituus ‘04h’ ensimmäisen sukupolven salatussa sanomanvälityksessä (katso lisäys 11, A osa) ‘08h’, ‘0Ch’ tai ‘10h’ riippuen AES-avaimen pituudesta toisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, B osa)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Salauksen tarkistussumma
Le	1	‘00h’	Kuten standardissa ISO/IEC 7816-4 on määritelty

TCS_59 **Vastausviesti, jos salattua sanomanvälitystä varten lähetetyn datan muoto on oikea**

Tavu	Pituus	Arvo	Kuvaus
#1	1	‘99h’	T_{SW}: tilaa osoittavien tavujen tuntomerkki (suojataan CC:llä)
#2	1	‘02h’	L_{SW}: vastauksena annettujen tilaa osoittavien tavujen pituus
#3-#4	2	‘XXXXh’	Suojaamattoman vastauksen tietoyksikön suorittamisen tila
#5	1	‘8Eh’	T_{CC}: salauksen tarkistussumman tuntomerkki
#6	1	‘XXh’	L_{CC}: seuraavan salauksen tarkistussumman pituus ‘04h’ ensimmäisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, A osa) ‘08h’, ‘0Ch’ tai ‘10h’ riippuen AES-avaimen pituudesta toisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, B osa)
#7-#(6+L)	L	‘XX..XXh’	Salauksen tarkistussumma
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

UPDATE BINARY -komennolle ilman salattua sanomanvälitystä (ks. kohta 3.5.3.1) kuvatut ”normaalit” suorittamisen tilaa kuvaavat vastaukset voidaan antaa edellä kuvattujen vastausviestirakenteiden avulla.

Tämän lisäksi saattaa ilmetä joitakin erityisesti salattuun sanomanvälitykseen liittyviä virhetilanteita. Tällöin vastauksena annetaan pelkkä suorittamisen tilan kuvaus ilman salatun sanomanvälityksen rakenteita:

TCS_60 **Vastausviesti jos salattua sanomanvälitystä varten lähetetyn datan muoto ei ole oikea**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

▼B

— Jos käytössä ei ole voimassa olevaa tilapäistä avainta, suorittamisen tilaa kuvaava vastaus on ‘**6A88**’.

— Jos datasta puuttuu joitakin odotettuja osia, suorittamisen tilaa kuvaava vastaus on ‘**6987**’: tämä virhe tapahtuu, jos odotettu tuntomerkki puuttuu tai komennon rakenne on väärä.

— Jos jotkin datan osat ovat virheellisiä, suorittamisen tilaa kuvaava vastaus on ‘**6988**’: tämä virhe tapahtuu, jos kaikki tarvittavat tuntomerkit ovat mukana, mutta jotkin datan pituudet eroavat odotetuista pituuksista.

— Jos salauksen tarkistussumman todentaminen epäonnistuu, suorittamisen tilaa kuvaava vastaus on ‘**6688**’.

3.5.3.2 Komento lyhyellä EF-tunnisteella

Tämän komentovariantin avulla liitäntälaite voi valita EF-tiedoston lyhyellä EF-tunnisteella ja kirjoittaa tietoja valitusta EF-tiedostosta.

TCS_61 Ajopiirturikortin on tuettava tätä komentovarianttia kaikkien sellaisten EF-tiedostojen osalta, joilla on määritetty lyhyt EF-tunniste. Lyhyet EF-tunnisteet on esitetty luvussa 4.

TCS_62 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘D6h’	UPDATE BINARY
P1	1	‘XXh’	Bitin 8 arvoksi on asetettu 1 Bittien 7 ja 6 arvoksi on asetettu 00 Bitit 5–1 koodaavat vastaavan EF-tiedoston lyhyen EF-tunnisteen
P2	1	‘XXh’	Koodaa suhteellisen osoitteen 0 tavusta 255 tavuun P1:n viittaamassa EF-tiedostossa
Lc	1	‘NNh’	Lc päivitettävän datan pituus. Kirjoitettavien tavujen määrä.
#6-#(5+NN)	NN	‘XX..XXh’	Kirjoitettava data

TCS_63 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

Huomautus: Toisen sukupolven ajopiirturisovelluksessa käytettävät lyhyet EF-tunnisteet on esitetty luvussa 4.

Jos P1 koodaa lyhyen EF-tunnisteen ja komennon suorittaminen onnistuu, tunnistetusta EF-tiedostosta tulee kulloinkin valittu EF-tiedosto (käytössä oleva EF).

▼B

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos lyhyttä EF-tunnistetta vastaavaa tiedostoa ei löytynyt, suorittamisen tilaa kuvaava vastaus on ‘**6A82**’.

— Jos valitun tiedoston turvallisuusehtoja ei täytetty, komennon suorittaminen keskeytetään viestillä ‘**6982**’.

— Jos suhteellinen osoite ei ole EF-tiedoston koon mukainen (suhteellinen osoite > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6B00**’.

— Jos kirjoitettavan datan pituus ei ole EF-tiedoston koon mukainen (suhteellinen osoite + Lc > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6700**’.

— Jos tiedoston ominaisuuksissa on todettu eheysvirhe, kortin on pidettävä tiedostoa vaurioituneena ja lukukelvottomana, ja suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

— Jos kirjoittaminen ei onnistu, suorittamisen tilaa kuvaava vastaus on ‘**6581**’.

3.5.3.3 Komento, jossa pariton käskytavu

Tämän komentovariantin avulla liitäntälaite voi kirjoittaa tietoja EF-tiedostoon, jossa on yli 32 768 tavua.

TCS_64 Ajopiirturikortin, joka tukee yli 32 768 tavun EF-tiedostoja, on tuettava tätä komentovarianttia tällaisten EF-tiedostojen kohdalla. Ajopiirturikortti voi tukea tai olla tukematta tätä komentoa muiden EF-tiedostojen kohdalla.

TCS_65 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘D7h’	UPDATE BINARY
P1	1	‘00h’	Käytössä oleva EF-tiedosto
P2	1	‘00h’	
Lc	1	‘NNh’	Lc komennon datakentässä olevan datan pituus
#6-#(5+NN)	NN	‘XX..XXh’	Offset-dataobjekti tuntomerkillä ‘54h’ || Valinnainen (discretionary) dataobjekti tuntomerkillä ‘53h’ suojaa kirjoitettavat tiedot

Liitäntälaitteen on koodattava offset-dataobjektin ja valinnaisen (discretionary) dataobjektin pituus mahdollisimman pienellä määrällä tavuja, ts. liitäntälaitteen on koodattava käyttäen pituutta osoittavaa tavua ‘01h’ suhteellinen osoite / pituus välillä 0–255 tavua ja käyttäen pituutta osoittavaa tavua ‘02h’ suhteellinen osoite / pituus välillä ‘256’–‘65 535’ tavua.

TCS_66 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

▼B

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos mitään EF-tiedostoa ei valita, suorittamisen tilaa kuvaava vastaus on ‘**6986**’.

— Jos valitun tiedoston turvallisuusehtoja ei täytetty, komennon suorittaminen keskeytetään viestillä ‘**6982**’.

— Jos suhteellinen osoite ei ole EF-tiedoston koon mukainen (suhteellinen osoite > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6B00**’.

— Jos kirjoitettavan datan pituus ei ole EF-tiedoston koon mukainen (suhteellinen osoite + Lc > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on ‘**6700**’.

— Jos tiedoston ominaisuuksissa on todettu eheysvirhe, kortin on pidettävä tiedostoa vaurioituneena ja lukukelvottomana, ja suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6500**’.

— Jos kirjoittaminen ei onnistu, suorittamisen tilaa kuvaava vastaus on ‘**6581**’.

3.5.3.3.1 Komento salattua sanomanvälitystä käyttäen (esimerkki)

Seuraavalla esimerkillä havainnollistetaan salatun sanomanvälityksen käyttöä tilanteessa, jossa turvallisuusehtoa SM-MAC-G2 sovelletaan.

TCS_67 Komentoviesti

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘0Ch’	Salattua sanomanvälitystä pyydetään
INS (käskytavu)	1	‘D7h’	UPDATE BINARY
P1	1	‘00h’	Käytössä oleva EF-tiedosto
P2	1	‘00h’	
Lc	1	‘XXh’	Varmistetun tietokentän pituus
#6	1	‘B3h’	BER-TLV-koodatun salaamattoman datan tuntomerkki
#7	L	‘NNh’ tai ‘81 NNh’	L_{PV}: lähetettävän datan pituus. L sisältää kaksi tavua, jos L_{PV}> 127 tavua.
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	BER-TLV-koodattu koodaamaton data, ts. offset-dataobjekti tuntomerkillä ‘54h’ || Valinnainen (discretionary) dataobjekti tuntomerkillä ‘53h’ suojaa kirjoitettavat tiedot
#(7+L+NN)	1	‘8Eh’	T_{CC}: salauksen tarkistussumman tuntomerkki
#(8+L+NN)	1	‘XXh’	L_{CC}: seuraavan salauksen tarkistussumman pituus ‘08h’, ‘0Ch’ tai ‘10h’ riippuen AES-avaimen pituudesta toisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, B osa)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Salauksen tarkistussumma
Le	1	‘00h’	Kuten standardissa ISO/IEC 7816-4 on määritelty

▼B

TCS_68 Vastausviesti, jos komennon tulos on onnistunut

Tavu	Pituus	Arvo	Kuvaus
#1	1	‘99h’	T_{SW}: tilaa osoittavien tavujen tuntomerkki (suojataan CC:llä)
#2	1	‘02h’	L_{SW}: vastauksena annettujen tilaa osoittavien tavujen pituus
#3-#4	2	‘XXXXh’	Suojaamattoman vastauksen tietoyksikön suorittamisen tila
#5	1	‘8Eh’	T_{CC}: salauksen tarkistussumman tuntomerkki
#6	1	‘XXh’	L_{CC}: seuraavan salauksen tarkistussumman pituus ‘08h’, ‘0Ch’ tai ‘10h’ riippuen AES-avaimen pituudesta toisen sukupolven salatussa sanomanvälityksessä (ks. lisäys 11, B osa)
#7-#(6+L)	L	‘XX..XXh’	Salauksen tarkistussumma
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

3.5.4 *GET CHALLENGE*

Tämä komento on standardin ISO/IEC 7816-4 mukainen, mutta sen käyttö on rajoitettua standardissa määriteltyyn komentoon verrattuna.

GET CHALLENGE -komento pyytää korttia antamaan haasteen (alkuluvun) käytettäväksi tietoturvaan liittyvässä menettelyssä, jolla salattua dataa lähetetään kortille.

TCS_69 Kortin antama haaste on voimassa vain seuraavassa haastetta käyttävässä komennossa, joka lähetetään kortille.

TCS_70 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘84h’	INS (käskytavu)
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Le	1	‘08h’	Le (odotettu haasteen pituus).

TCS_71 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
#1-#8	8	‘XX..XXh’	Haaste
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos Le:n arvo on muu kuin ‘08h’, tilaa kuvaava vastaus on ‘**6700**’.

— Jos parametrit P1-P2 ovat virheellisiä, suorituksen tila on ‘**6A86**’.

▼B

3.5.5 *VERIFY*

Tämä komento on standardin ISO/IEC 7816-4 mukainen, mutta sen käyttö on rajoitettua standardissa määriteltyyn komentoon verrattuna.

Vain korjaamokortin täytyy tukea tätä komentoa.

Muuntyyppiset ajopiirturikortit voivat suorittaa tämän komennon tai olla suorittamatta sitä, mutta niille ei määritetä vertailtavia kontrollitietoja. Sen vuoksi nämä kortit eivät voi suorittaa komentoa onnistuneesti. Tässä erittelyssä käsitellään ainoastaan korjaamokorttien vastausta, ts. kortin palauttamaa virhekoodia, tähän komentoon; tässä yhteydessä ei käsitellä muiden ajopiirturikorttityyppien toimintaa.

VERIFY-komento käynnistää komennon lähettämien kortin haltijan kontrollitietojen (käyttäjän henkilökohtaisen tunnusluvun, PIN) kortilla tapahtuvan vertaamisen sillä oleviin kortin haltijan kontrollitietoihin.

TCS_72 Liitäntälaitteen on ASCI-koodattava käyttäjän syöttämä henkilökohtainen tunnusluku (PIN) ja täydennettävä se lisäämällä sen perään tavuja arvoltaan FFh siten, että sen kokonaispituudeksi tulee 8 tavua, ks. myös datatyyppi WorkshopCardPIN lisäyksessä 1.

TCS_73 Ajopiirturisovelluksen ensimmäisen ja toisen sukupolven on käytettävä samoja vertailtavia kontrollitietoja.

TCS_74 Ajopiirturikortin on tarkistettava, onko komento koodattu oikein. Jos komentoa ei ole koodattu oikein, kortti ei vertaa kontrollitietojen arvoja, ei vähennä kontrollitietojen syöttämisyrityksiä laskevasta laskurista syöttämiskertojen määrää eikä palauta tietoturvatilaa ”PIN_Verified”, vaan keskeyttää komennon suorittamisen. Komento on koodattu oikein, jos tavuissa CLA, INS, P1, P2, Lc on määritetyt arvot, jos Le-tavua ei ole ja jos komennon datakentän pituus on oikea.

TCS_75 Jos komento suoritetaan onnistuneesti, kontrollitietojen syöttämisyrityksiä laskeva laskuri asetetaan takaisin alkutilaansa. Kontrollitietojen syöttämisyrityksiä laskevan laskurin alkuarvo on 5. Jos komento suoritetaan onnistuneesti, kortti asettaa sisäiseksi tietoturvatilaksi ”PIN_Verified”. Kortti palauttaa tämän tietoturvatilan, jos kortti palautettiin alkutilaan tai jos komennossa lähetetyt kontrollitiedot eivät vastaa tallennettuja vertailtavia kontrollitietoja.

Huomautus: Käyttämällä samoja vertailtavia kontrollitietoja ja yleistä tietoturvatilaa vältytään siltä, että korjaamon työntekijän tarvitsee antaa PIN-tunnusluku uudelleen valittuaan toisen ajopiirturisovelluksen DF-tiedoston.

TCS_76 Jos tietojen vertailu ei anna hyväksyttävää tulosta, tämä kirjataan kortille, ts. kontrollitietojen syöttämisyrityksiä laskevasta laskurista vähennetään yksi syöttämiskerta, mikä rajoittaa kontrollitietojen tulevien käyttöyrityksien määrää.

TCS_77 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘20h’	INS (käskytavu)
P1	1	‘00h’	P1

▼B

Tavu	Pituus	Arvo	Kuvaus
P2	1	‘00h’	P2 (todennetut kortin haltijan kontrollitiedot ovat automaattisesti tiedossa)
Lc	1	‘08h’	Lähetettävien kontrollitietojen pituus
#6-#13	8	‘XX..XXh’	Kortin haltijan kontrollitiedot (CHV)

TCS_78 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos vertailtavia kontrollitietoja ei löydy, suorittamisen tilaa kuvaava vastaus on ‘**6A88**’.

— Jos kontrollitietojen käyttö on estetty (jäljellä olevien tunnuksen syöttämisyritysten laskurin arvo on nolla), suorittamisen tilaa kuvaava vastaus on ‘**6983**’. Kun tämä tila syntyy, kortin haltijan kontrollitietoja ei enää koskaan voida onnistuneesti syöttää.

— Jos tietojen vertailu ei anna hyväksyttävää tulosta, jäljellä olevien yrityskertojen laskurin arvoa vähennetään ja annetaan tilaa kuvaava vastaus ‘**63CX**’ (X>0 ja X on jäljellä olevien yrityskertojen määrä.

— Jos vertailtavat kontrollitiedot katsotaan virheellisiksi, suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

— Jos Lc:n arvo on muu kuin ‘08h’, tilaa kuvaava vastaus on ‘**6700**’.

3.5.6 *GET RESPONSE*

Tämä komento on standardin ISO/IEC 7816-4 mukainen.

Tätä komentoa (joka on tarpeen ja käytettävissä vain T=0-protokollan yhteydessä) käytetään lähettämään valmisteltua dataa kortilta liitäntälaitteelle (tapaus, jolloin komento on sisältänyt sekä Lc- että Le-tavun).

GET RESPONSE -komento on annettava välittömästi dataa valmistelevan komennon jälkeen; muussa tapauksessa data menetetään. GET RESPONSE -komennon suorittamisen jälkeen (paitsi silloin, kun tapahtuu virhe ‘**61xx**’ tai ‘**6Cxx**’, ks. alla) ei aiemmin valmisteltu data ole enää käytettävissä.

TCS_79 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘C0h’	
P1	1	‘00h’	
P2	1	‘00h’	
Le	1	‘XXh’	Odotettu tavujen määrä

▼B

TCS_80 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
#1-#X	X	‘XX..XXh’	Data
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos kortti ei ole valmistellut dataa, suorittamisen tilaa kuvaava vastaus on ‘**6900**’ tai ‘**6F00**’.

— Jos Le on suurempi kuin käytettävissä olevien tavujen määrä tai jos se on nolla, suorittamisen tilaa kuvaava vastaus on ‘**6Cxx**’, missä ‘xx’ on käytettävissä olevien tavujen tarkka määrä. Tässä tapauksessa valmisteltu data on vielä seuraavan GET RESPONSE -komennon käytettävissä.

— Jos Le ei ole nolla, mutta pienempi kuin käytettävissä olevien tavujen määrä, kortti lähettää vaaditun datan normaalisti ja suorittamisen tilaa kuvaava vastaus on ‘**61xx**’, jossa ‘xx’ on seuraavan GET RESPONSE -komennon käytettävissä olevien tavujen määrä. Jäljelle jäänyt data (jota ei pyydetty) ei enää ole käytettävissä.

— Jos komentoa ei tueta (T=1-protokolla), kortti vastaa ‘**6D00**’.

3.5.7 *PSO: VERIFY CERTIFICATE*

Tämä komento on standardin ISO/IEC 7816-8 mukainen, mutta sen käyttö on rajoitettua standardissa määriteltyyn komentoon verrattuna.

VERIFY CERTIFICATE -komennon avulla kortti saa ulkopuolelta julkisen avaimen ja tarkastaa sen kelpoisuuden.

3.5.7.1 1. sukupolven komento-vastauspari

TCS_81 Tätä komentovarianttia tukee vain ensimmäisen sukupolven ajopiirturisovellus.

TCS_82 Jos VERIFY CERTIFICATE -komennon tulos on hyväksyttävä, julkinen avain tallennetaan, jotta sitä voidaan tulevaisuudessa käyttää tietoturvaympäristössä. Tämä avain asetetaan nimenomaan MSE-komennon (ks. kohta 3.5.11) käyttöön tietoturvaan liittyvien komentojen (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE tai VERIFY CERTIFICATE) yhteydessä sen avaintunnisteen avulla.

TCS_83 VERIFY CERTIFICATE -komento käyttää kuitenkin MSE-komennon aiemmin valitsemaa julkista avainta varmenteen avaamiseen. Kyseessä on oltava tietyn jäsenvaltion tai Euroopan julkinen avain.

TCS_84 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘2Ah’	PSO (Suorita turvatoimi)
P1	1	‘00h’	P1

▼B

Tavu	Pituus	Arvo	Kuvaus
P2	1	‘AEh’	P2: data, jota ei ole BER-TLV-koodattu (dataelementtien ketjutus)
Lc	1	‘C2h’	Lc: varmenteen pituus, 194 tavua.
#6-#199	194	‘XX..XXh’	Varmenne: dataelementit ketjutettu (kuten lisäyksessä 11 on kuvattu)

TCS_85 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos varmenteen todentaminen ei onnistu, suorittamisen tilaa kuvaava vastaus on ‘**6688**’. Varmenteen todennus- ja purkumenettely on kuvattu lisäyksessä 11 sekä ensimmäisen että toisen sukupolven osalta.

— Jos tietoturvaympäristössä ei ole julkista avainta, vastaus on ‘**6A88**’.

— Jos valittu julkinen avain (jota käytetään varmenteen avaamiseen) katsotaan vialliseksi, suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

— Vain ensimmäisen sukupolvi: Jos (varmenteen avaamiseen käytettävän) julkisen avaimen CHA.LSB-arvo (`CertificateHolderAuthorisation.equipmentType`) on muu kuin ‘00’ (eli muu kuin tietyn jäsenvaltion tai Euroopan kyseinen arvo), suorittamisen tilaa kuvaava vastaus on ‘**6985**’.

3.5.7.2 2. sukupolven komento-vastauspari

Käyrän koosta riippuen ECC-varmenteet voivat olla niin pitkiä, että niitä ei voi lähettää yhdessä tietoyksikössä. Tällöin on noudatettava standardin ISO/IEC 7816-4 mukaista komentojen ketjutusta ja varmenne on lähetettävä kahdessa peräkkäisessä PSO: Verify Certificate -tietoyksikössä.

Varmenteen rakenne ja domain-parametrit on määritetty lisäyksessä 11.

TCS_86 Komento voidaan suorittaa MF-, DF Tachograph- ja DF Tachograph_G2 -tiedostossa, ks. myös TCS_33.

TCS_87 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘X0h’	Komennon ketjutusta osoittava CLA-tavu: ‘00h’ ketjun ainoa tai viimeinen komento ‘10h’ muu kuin ketjun viimeinen komento
INS (käskytavu)	1	‘2Ah’	PSO (Suorita turvatoimi)
P1	1	‘00h’	
P2	1	‘BEh’	Tarkista itseään kuvaava (self-descriptive) varmenne

▼B

Tavu	Pituus	Arvo	Kuvaus
Lc	1	‘XXh’	Komennon datakentän pituus, ks. TCS_88 ja TCS_89.
#6-#5+L	L	‘XX..XXh’	DER-TLV-koodattu data: Ensimmäisenä dataobjektina ECC-varmenteen rungon dataobjekti, joka on ketjutettu toisena dataobjektina tai ketjutuksen muuna osana olevan ECC-varmenteen allekirjoituksen dataobjektin kanssa. Tuntomerkkiä ‘7F21’ ja vastaavaa pituutta ei lähetetä. Näiden dataobjektien järjestys on kiinteä.

TCS_88 Lyhyisiin tietoyksiköihin sovelletaan seuraavia määräyksiä: Liitäntälaite käyttää pienimmän mahdollisen määrän tietoyksiköitä, joka tarvitaan komennon lähettämiseksi, ja lähettää komennon ensimmäisessä tietoyksikössä suurimman mahdollisimman määrän tavuja Information Field Size Card -tavun mukaisesti, ks. TCS_14. Tästä mahdollisesti poikkeavaa kortin toimintaa ei käsitellä tässä ohjeessa.

TCS_89 Laajennetun pituuskentän tietoyksiköihin sovelletaan seuraavia määräyksiä: Jos varmenne ei mahdu yhteen tietoyksiköön, kortin on tuettava komentojen ketjutusta. Liitäntälaite käyttää pienimmän mahdollisen määrän tietoyksiköitä, joka tarvitaan komennon lähettämiseksi, ja lähettää komennon ensimmäisessä tietoyksikössä suurimman mahdollisimman määrän tavuja. Tästä mahdollisesti poikkeavaa kortin toimintaa ei käsitellä tässä ohjeessa.

Huomautus: Lisäyksen 11 mukaisesti kortti tallentaa varmenteen tai sen keskeisen sisällön ja päivittää currentAuthenticatedTime -ajan.

Vastausviestin rakenne ja tilaa osoittavat tavut on esitetty kohdassa TCS_85.

TCS_90 Kohdassa TCS_85 lueteltujen virhekoodien lisäksi kortti voi palauttaa jonkin seuraavista virhekoodeista:

— Jos (varmenteen avaamiseen käytettävän) julkisen avaimen CHA.LSB-arvo (CertificateHolderAuthorisation.equipmentType) ei sovellu lisäyksen 11 mukaan varmenteen tarkistamiseen, suorittamisen tilaa kuvaava vastaus on ‘**6985**’.

— Jos kortin currentAuthenticatedTime on myöhäisempi kuin varmenteen vanhenemispäivä, suorittamisen tilaa kuvaava vastaus on ‘**6985**’.

— Jos ketjun viimeinen komento on odotettu, kortti palauttaa vastauksen ‘**6883**’.

— Jos komennon datakentässä lähetetetään vääriä parametreja, kortti palauttaa vastauksen ‘**6A80**’ (käytetään myös, jos dataobjekteja ei ole lähetetty määrätyssä järjestyksessä.

▼B

3.5.8 *INTERNAL AUTHENTICATE*

Tämä komento on standardin ISO/IEC 7816-4 mukainen.

TCS_91 Kaikkien ajopiirturikorttien on tuettava tätä komentoa ensimmäisen sukupolven DF Tachograph -tiedostoissa. Komento saattaa olla käytettävissä MF- ja / tai DF Tachograph_G2 -tiedostoissa. Tällöin komennon on päätyttävä asianmukaiseen virhekoodiin, sillä kortin yksityinen avain (Card.SK) ensimmäisen sukupolven todentamisprotokollaa varten on käytettävissä vain ensimmäisen sukupolven DF_Tachograph -tiedostoissa.

INTERNAL AUTHENTICATE -komennon avulla liitäntälaite voi todentaa kortin. Todennusmenettely on kuvattu lisäyksessä 11. Siihen sisältyy seuraavat lausumat:

TCS_92 INTERNAL AUTHENTICATE -komento käyttää kortin yksityistä avainta (valitaan automaattisesti), kun se allekirjoittaa todennusdatan, johon sisältyy K1 (ensimmäinen dataelementti tilapäisestä avaimesta sovittaessa) ja RND1, ja kulloinkin (viimeisimmän MSE-komennon avulla) valittua julkista avainta, kun se salaa allekirjoituksen ja muodostaa todennustunnisteen (lisätietoja tästä on lisäyksessä 11).

TCS_93 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	CLA
INS (käskytavu)	1	‘88h’	INS (käskytavu)
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Lc	1	‘10h’	Kortille lähetettävän datan pituus
#6 – #13	8	‘XX..XXh’	Kortin todennukseen käytettävä haaste
#14 -#21	8	‘XX..XXh’	VU.CHR (ks. lisäys 11)
Le	1	‘80h’	Kortilta odotettavan datan pituus

TCS_94 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
#1-#128	128	‘XX..XXh’	Kortin todennustunniste (ks. lisäys 11)
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos tietoturvaympäristössä ei ole julkista avainta, suorittamisen tilaa kuvaava vastaus on ‘**6A88**’.

— Jos tietoturvaympäristössä ei ole yksityistä avainta, suorittamisen tilaa kuvaava vastaus on ‘**6A88**’.

— Jos VU.CHR ei täsmää käytössä olevan julkisen avaimen tunnisteen kanssa, suorittamisen tilaa kuvaava vastaus on ‘**6A88**’.

▼B

— Jos valittu yksityinen avain katsotaan vialliseksi, suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

TCS_95 Jos INTERNAL AUTHENTICATE -komennon tulos on onnistunut, poistetaan käytössä oleva tilapäinen avain, jos sellainen on, eikä se sen jälkeen ole käytettävissä. Uusi tilapäinen avain saadaan käyttöön ensimmäisen sukupolven todennusmekanismin EXTERNAL AUTHENTICATE -komennon onnistuneen suorittamisen jälkeen.

3.5.9 *EXTERNAL AUTHENTICATE*

Tämä komento on standardin ISO/IEC 7816-4 mukainen.

EXTERNAL AUTHENTICATE -komennon avulla kortti voi todentaa liitäntälaitteen. Todentamisprosessi on kuvattu lisäyksessä 11 ensimmäisen ja toisen sukupolven ajopiirtureiden osalta (ajoneuvoyksikön todentaminen).

TCS_96 Ensimmäisen sukupolven todennusmekanismin komentovarianttia tukee vain ensimmäisen sukupolven ajopiirturisovellus.

TCS_97 Toisen sukupolven ajoneuvoyksikön ja kortin molemminpuolisen todentamisen komentovariantti voidaan suorittaa MF-, DF Tachograph- ja DF Tachograph_G2 -tiedostossa, ks. myös TCS_34.

TCS_98 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	CLA (komennon luokan ilmaiseva tavu)
INS (käskytavu)	1	‘82h’	INS (käskytavu)
P1	1	‘00h’	Avaimet ja algoritmit automaattisesti tiedossa
P2	1	‘00h’	
Lc	1	‘XXh’	Lc (kortille lähetettävän datan pituus)
#6-#(5+L)	L	‘XX..XXh’	Ensimmäisen sukupolven todentaminen: Kryptogrammi (ks. lisäys 11, A osa) Toisen sukupolven todentaminen: Liitäntälaitteen tuottama allekirjoitus (ks. lisäys 11, B osa)

TCS_99 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos valitun julkisen avaimen CHA (varmenteen haltijan valtuutus) ei ole ajopiirturisovelluksen tunnisteen (AID) ja ajoneuvoyksikön tyypin yhdistelmä, suorittamisen tilaa kuvaava vastaus on ‘**6F00**’.

— Jos komentoa ei välittömästi edeltänyt GET CHALLENGE -komento, suorittamisen tilaa kuvaava vastaus on ‘**6985**’.

▼B

Ensimmäisen sukupolven ajopiirturisovellus voi palauttaa lisäksi seuraavat virhekoodit:

— Jos tietoturvaympäristössä ei ole julkista avainta, vastaus on ‘**6A88**’.

— Jos tietoturvaympäristössä ei ole yksityistä avainta, suorittamisen tilaa kuvaava vastaus on ‘**6A88**’.

— Jos kryptogrammin todentamisen tulos on väärä, suorittamisen tilaa kuvaava vastaus on ‘**6688**’.

— Jos valittu yksityinen avain katsotaan vialliseksi, suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

Toisen sukupolven todentamisen komentovariantti voi palauttaa lisäksi seuraavan virhekoodin:

— Jos allekirjoituksen todentaminen epäonnistuu, kortti vastaa ‘**6300**’.

3.5.10 *GENERAL AUTHENTICATE*

Tätä komentoa käytetään toisen sukupolven sirun todentamisprotokollassa, joka on esitetty lisäyksen 11 B osassa; se on standardin ISO/IEC 7816-4 mukainen.

TCS_100 Komento voidaan suorittaa MF-, DF Tachograph- ja DF Tachograph_G2 -tiedostossa, ks. myös TCS_34.

TCS_101 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘86h’	
P1	1	‘00h’	Avaimet ja protokolla automaattisesti tiedossa
P2	1	‘00h’	
Lc	1	‘NNh’	Lc: seuraavan datakentän pituus
#6-#(5+L)	L	‘7Ch’ + L_{7C} + ‘80h’ + L_{80} + ‘XX..XXh’	DER-TLV-koodattu lyhytaikaisen julkisen avaimen arvo (ks. lisäys 11) Ajoneuvoyksikön on lähetettävä dataobjektit tässä järjestyksessä.

TCS_102 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
#1-#L	L	‘7Ch’ + L_{7C} + ‘81h’ + ‘08h’ + ‘XX..XXh’ + ‘82h’ + L_{82} + ‘XX..XXh’	DER-TLV-koodatut dynaamiset todentamistiedot (Dynamic Authentication Data): nonceluku ja todennustunniste (ks. lisäys 11)
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Kortti vastaa ‘**6A80**’, jos datakentässä on vääriä parametreja.

▼B

— Kortti vastaa ‘**6982**’, jos External Authenticate -komentoa ei ole suoritettu onnistuneesti

Dynaamisen todentamisen (Dynamic Authentication) -data-objektin ‘7Ch’

— on oltava mukana, jos operaatio on onnistunut, ts. tilaa osoittavat tavut ovat ‘**9000**’,

— on puututtava, jos on tapahtunut toteutusvirhe tai tarkistusvirhe, ts. jos tilaa osoittavat tavut ovat välillä ‘**6400**’ – ‘**6FFF**’;

— lisäksi se voi olla läsnä, jos kyseessä on varoitus, ts. jos tilaa osoittavat tavut ovat välillä ‘**6200**’ – ‘**63FF**’.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Tällä komennolla valitaan todennukseen käytettävä julkinen avain.

3.5.11.1 1. sukupolven komento-vastauspari

Tämä komento on standardin ISO/IEC 7816-4 mukainen. Komennon käyttö on rajoitettua siihen liittyvään standardiin nähden.

TCS_103 Tätä komentoa tukee vain ensimmäisen sukupolven ajopiirturisovellus.

TCS_104 Avain, johon viitataan MSE-komennon datakentässä, pysyy käytössä olevana julkisena avaimena siihen asti, kunnes seuraava oikein annettu MSE-komento suoritetaan, DF-tiedosto valitaan tai kortti palautetaan alkutilaan.

TCS_105 Jos kyseistä avainta ei (jo) ole kortilla, ei tietoturvaympäristö muutu.

TCS_106 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	CLA (komennon luokan ilmaiseva tavu)
INS (käskytavu)	1	‘22h’	INS (käskytavu)
P1	1	‘C1h’	P1: avain, johon viitataan, kelpaa kaikkiin salaustoimiin
P2	1	‘B6h’	P2 (digitaalista allekirjoitusta koskevan datan viite)
Lc	1	‘0Ah’	Lc: seuraavan datakentän pituus
#6	1	‘83h’	Tuntomerkki, jolla viitataan epäsymmetrisen salauksen yhteydessä käytettävään julkiseen avaimeen
#7	1	‘08h’	Avainviitteen (avaimen tunnisteen) pituus
#8-#15	8	‘XX..XXh’	Avaimen tunniste siten kuin se on määritelty lisäyksessä 11

TCS_107 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

▼B

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos avainta, johon viitataan, ei ole kortilla, suorittamisen tilaa kuvaava vastaus on ‘**6A88**’.

— Jos salatun sanomanvälityksen muodossa olevasta datasta puuttuu joitakin odotettuja osia, annetaan suorittamisen tilaa kuvaava vastaus ‘**6987**’. Näin voi tapahtua, jos tuntomerkki ‘83h’ puuttuu.

— Jos jotkin datan osat ovat virheellisiä, suorittamisen tilaa kuvaava vastaus on ‘**6988**’: Näin voi tapahtua, jos avaimen tunnisteen pituus ei ole ‘08h’.

— Jos valittu avain katsotaan vialliseksi, suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

3.5.11.2 2. sukupolven komento-vastauspari

Toisen sukupolven todentamisessa ajopiirturi tukee seuraavia MSE: Set -komentoversioita, jotka ovat standardin ISO/IEC 7816-4 mukaisia. Ensimmäisen sukupolven todentaminen ei tue näitä komentoversioita.

3.5.11.2.1 MSE:SET AT sirun todennusta varten

Seuraavalla MSE:SET AT -komennolla valitaan parametrit sirun todennukseen, joka tehdään sen jälkeen General Authenticate -komennolla.

TCS_108 Komento voidaan suorittaa MF-, DF Tachograph- ja DF Tachograph_G2 -tiedostossa, ks. myös TCS_34.

TCS_109 **MSE:SET AT -komentoviesti sirun todennusta varten**

Tavu	Pituus	Arvo	Kuvaus
CLA (komennon luokan ilmaiseva tavu)	1	‘00h’	
INS (käskytavu)	1	‘22h’	
P1	1	‘41h’	Asetettu sisäiseen todentamiseen
P2	1	‘A4h’	Todentaminen
Lc	1	‘NNh’	Lc: seuraavan datakentän pituus
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	DER-TLV-koodattu salausmekanismin viite: Sirun todentamisen oliotunniste (vain arvo, tuntomerkki ‘06h’ jätetään pois). Oliotunnisteiden arvot on esitetty lisäyksessä 1; tavun notaatiota on käytettävä. Ohjeita oikean oliotunnisteen valintaan on esitetty lisäyksessä 11.

3.5.11.2.2 MSE:SET AT ajoneuvoyksikön todennusta varten

Seuraavalla MSE:SET AT -komennolla valitaan parametrit ja avaimet ajoneuvoyksikön todennukseen, joka tehdään sen jälkeen External Authenticate -komennolla.

▼B

TCS_110 Komento voidaan suorittaa MF-, DF Tachograph- ja DF Tachograph_G2 -tiedostossa, ks. myös TCS_34.

TCS_111 **MSE:SET AT -komentoviesti ajoneuvoyksikön (VU) todennusta varten**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	
INS (käskytavu)	1	‘22h’	
P1	1	‘81h’	Asetettu ulkoiseen todentamiseen
P2	1	‘A4h’	Todentaminen
Lc	1	‘NNh’	Lc: seuraavan datakentän pituus
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	DER-TLV-koodattu salausmekanismin viite: Ajoneuvoyksikön todentamisen oliotunniste (vain arvo, tuntomerkki ‘06h’ jätetään pois). Oliotunnisteiden arvot on esitetty lisäyksessä 1; tavun notaatiota on käytettävä. Ohjeita oikean oliotunnisteen valintaan on esitetty lisäyksessä 11.
		‘83h’ + ‘08h’ + ‘XX..XXh’	Ajoneuvoyksikön lyhytaikaisen julkisen avaimen DER-TLV-koodattu viite mainittu avaimen varmenteessa varmenteen haltijan viitteellä (Certificate Holder Reference).
		‘91h’ + L_{91} + ‘XX..XXh’	DER-TLV-koodattu ajoneuvoyksikön julkisen avaimen tiivistetty esitys, jota käytetään sirun todentamisen aikana (ks. lisäys 11)

3.5.11.2.3 MSE:SET DST

Seuraavalla MSE:SET DST -komennolla asetetaan julkinen avain joko

— allekirjoituksen tarkistamiseen, joka suoritetaan sen jälkeen PSO: Verify Digital Signature -komennolla, tai

— varmenteen allekirjoituksen tarkistamiseen, joka suoritetaan sen jälkeen PSO: Verify Certificate –komennolla.

TCS_112 Komento voidaan suorittaa MF-, DF Tachograph- ja DF Tachograph_G2 -tiedostossa, ks. myös TCS_33.

TCS_113 **MSE:SET DST -komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA (komennon luokan ilmaiseva tavu)	1	‘00h’	
INS (käskytavu)	1	‘22h’	
P1	1	‘81h’	Asetettu tarkistamiseen
P2	1	‘B6h’	Digitaalinen allekirjoitus

▼B

Lc	1	‘NNh’	Lc: seuraavan datakentän pituus
#6-#(5+L)	L	‘83h’ + ‘08h’ + ‘XX...XXh’	DER-TLV-koodattu julkisen avaimen viite, ts. varmenteen haltijan viite julkisen avaimen varmenteessa (ks. lisäys 11)

Kaikilla komentoversioilla vastausviestin rakenteen ja tilaa osoittavat tavut antaa:

TCS_114 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’. Protokolla on valittu ja alustettu.

— ‘**6A80**’ osoittaa väärät parametrit komennon datakentässä.

— ‘**6A88**’ osoittaa, että viitattu data (ts. avain, johon viitataan) ei ole käytettävissä.

3.5.12 *PSO: HASH*

Tällä komennolla siirretään jonkin datan hash (hajautus) -algoritmilla laskettu tulos kortille. Tätä komentoa käytetään digitaalisten allekirjoitusten todentamisessa. Hash-algoritmin antama tulos tallennetaan tilapäisesti seuraavaa PSO: Verify Digital Signature -komentoa varten.

Tämä komento on standardin ISO/IEC 7816-8 mukainen. Komennon käyttö on rajoitettua siihen liittyvään standardiin nähden.

Tämän komennon tukeminen DF Tachograph- ja DF Tachograph_G2 -tiedostossa edellyttää vain valvontakorttia.

Muut ajopiirturikorttityypit saattavat toteuttaa tämän komennon. Komento saattaa olla käytettävissä MF-tiedostossa.

Ensimmäisen sukupolven valvontakortin sovellus tukee vain SHA-1-algoritmia.

TCS_115 Tilapäisesti tallennettu hash-algoritmin tulos poistetaan, jos PSO: HASH -komennolla lasketaan uusi hash-algoritmin tulos, jos DF-tiedosto valitaan ja jos ajopiirturin kortti palautetaan alkutilaan.

TCS_116 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	CLA (komennon luokan ilmaiseva tavu)
INS (käskytavu)	1	‘2Ah’	PSO (Suorita turvatoimi)
P1	1	‘90h’	Palauta hash-algoritmin tulos (hash code)

▼B

Tavu	Pituus	Arvo	Kuvaus
P2	1	‘A0h’	Tuntomerkki: datakentässä on hash-algoritmilla käsiteltävää dataa
Lc	1	‘XXh’	Seuraavan datakentän pituus Lc
#6	1	‘90h’	Hash-algoritmin tuloksen (hash code) tuntomerkki
#7	1	‘XXh’	Hash-algoritmin tuloksen (hash code) pituus L: ‘14h’ ensimmäisen sukupolven sovelluksessa (ks. lisäys 11, A osa) ‘20h’, ‘30h’ tai ‘40h’ toisen sukupolven sovelluksessa (ks. lisäys 11, B osa)
#8-#(7+L)	L	‘XX..XXh’	Hash-algoritmin tulos (hash code)

TCS_117 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos datasta puuttuu joitain (yllä määriteltyjä) osia, annetaan suorittamisen tilaa kuvaava vastaus ‘**6987**’. Näin voi tapahtua, jos jompikumpi tuntomerkeistä arvoltaan ‘90h’ puuttuu.

— Jos jotkin datan osat ovat virheellisiä, suorittamisen tilaa kuvaava vastaus on ‘**6988**’: Tämä virhe tapahtuu, jos asianmukaista tuntomerkkiä on käytetty mutta pituus on eri kuin ‘14h’ SHA-1-algoritmillä, ‘20h’ SHA-256-algoritmillä, ‘30h’ SHA-384-algoritmillä tai ‘40h’ SHA-512-algoritmillä (toisen sukupolven sovellus).

3.5.13 *PERFORM HASH of FILE*

Tämä komento ei ole standardin ISO/IEC 7816-8 mukainen. Näin ollen tämän komennon luokkaa osoittava CLA-tavu osoittaa, että komentoa PERFORM SECURITY OPERATION / HASH käytetään erikoistarkoituksessa.

Vain kuljettajakortin ja korjaamokortin täytyy tukea tätä komentoa DF Tachograph- ja DF Tachograph_G2 -tiedostossa.

Muut ajopiirturikorttityypit saattavat toteuttaa tämän komennon. Jos yritys- tai valvontakortti suorittaa tämän komennon, komento on suoritettava tässä luvussa annettujen ohjeiden mukaisesti.

Komento saattaa olla käytettävissä MF-tiedostossa. Tällöin komento on suoritettava tässä luvussa annettujen ohjeiden mukaisesti, ts. sen ei pidä sallia hash-tuloksen laskemista, vaan sen on päätyttävä sopivaan virhekoodiin.

TCS_118 PERFORM HASH OF FILE -komennon avulla käsitellään kulloinkin valittua transparent-tyyppisen EF-tiedoston dataa hash-algoritmilla.

TCS_119 Ajopiirturikortin on tuettava tätä komentoa vain niiden EF-tiedostojen osalta, jotka on lueteltu luvussa 4 DF_Tachograph- ja DF_Tachograph_G2 -tiedoston alla, lukuun ottamatta seuraavaa poikkeusta. Ajopiirturikortin ei pidä tukea komentoa DF Tachograph_G2:n EF-tiedostossa Sensor_Installation_Data.

▼B

TCS_120 Hash-algoritmin antama tulos tallennetaan kortille tilapäisesti. Sitä voidaan sen jälkeen käyttää tiedoston digitaalisen allekirjoituksen luomiseen komennolla PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Tilapäisesti tallennettu tiedoston tietoja vastaava hash-algoritmin tulos poistetaan, jos PSO: HASH OF FILE -komennolla lasketaan uusi tiedoston tietoja vastaava hash-algoritmin tulos, jos DF-tiedosto valitaan ja jos ajopiirturin kortti palautetaan alkutilaan.

TCS_122 Ensimmäisen sukupolven ajopiirturisovelluksen on tuettava SHA-1-algoritmia.

TCS_123 Toisen sukupolven ajopiirturisovelluksen on tuettava SHA-1- ja SHA-2-algoritmeja (256, 384 ja 512 bittiä).

TCS_124 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘80h’	CLA (komennon luokan ilmaiseva tavu)
INS (käskytavu)	1	‘2Ah’	PSO (Suorita turvatoimi)
P1	1	‘90h’	Tuntomerkki: Hash
P2	1	‘XXh’	P2: osoittaa algoritmin, jolla käsitellään kulloinkin valitun transparent-tyyppisen tiedoston dataa hash-algoritmilla: ‘00h’ algoritmille SHA-1 ‘01h’ algoritmille SHA-256 ‘02h’ algoritmille SHA-384 ‘03h’ algoritmille SHA-512

TCS_125 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos valittu EF-tiedosto ei salli tätä komentoa (EF-tiedosto Sensor_Installation_Data DF Tachograph_G2 -tiedostossa), suorittamisen tilaa kuvaava vastaus on ‘**6985**’.

— Jos valittu EF-tiedosto katsotaan vialliseksi (tiedoston ominaisuuksissa tai tallennetuissa tiedoissa eheysvirhe), suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

— Jos valittu tiedosto ei ole transparent-tyyppinen tai jos EF-tiedostoa ei ole valittu, suorittamisen tilaa kuvaava vastaus on ‘**6986**’.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Tämän komennon avulla lasketaan digitaalinen allekirjoitus aiemmin lasketun hash-algoritmin antaman tuloksen avulla (ks. PERFORM HASH OF FILE, kohta 3.5.13).

Vain kuljettajakortin ja korjaamokortin täytyy tukea tätä komentoa DF Tachograph- ja DF Tachograph_G2 -tiedostossa.

▼B

Muuntyyppiset ajopiirturikortit voivat suorittaa tämän komennon tai olla suorittamatta sitä, mutta niillä ei ole allekirjoituksen avainta. Sen vuoksi nämä kortit eivät voi suorittaa komentoa onnistuneesti, vaan palauttavat asianmukaisen virhekoodin.

Komento saattaa olla käytettävissä MF-tiedostossa. Tällöin komennon on päätyttävä asianmukaiseen virhekoodiin.

Tämä komento on standardin ISO/IEC 7816-8 mukainen. Komennon käyttö on rajoitettua siihen liittyvään standardiin nähden.

TCS_126 Tämän komennon ei pidä laskea digitaalista allekirjoitusta aiemmin lasketun hash-algoritmin tuloksen avulla käyttäen komentoa PSO: HASH.

TCS_127 Digitaalinen allekirjoitus lasketaan siten, että käytetään kortin yksityistä avainta, joka on automaattisesti kortin tiedossa.

TCS_128 Ensimmäisen sukupolven ajopiirturisovellus tekee digitaalisen allekirjoituksen käyttäen RSA-salausta koskevan PKCS1-standardin mukaista täyttömenetelmää (lisätietoja on lisäyksessä 11).

TCS_129 Toisen sukupolven ajopiirturisovellus laskee elliptisen käyrän digitaalisen allekirjoituksen perusteella (lisätietoja on lisäyksessä 11).

TCS_130 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	CLA (komennon luokan ilmaiseva tavu)
INS (käskytavu)	1	‘2Ah’	PSO (Suorita turvatoimi)
P1	1	‘9Eh’	Palautettava digitaalinen allekirjoitus
P2	1	‘9Ah’	Tuntomerkki: datakentässä on allekirjoitettavaa dataa. Koska mukana ei ole datakenttää, oletetaan kyseisen datan olevan jo kortilla (tiedoston hash-algoritmilla käsitelty tulos)
Le	1	‘NNh’	Odotetun allekirjoituksen pituus

TCS_131 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
#1-#L	L	‘XX..XXh’	Aiemmin lasketun hash-algoritmin tuloksen allekirjoitus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos automaattisesti valittu yksityinen avain katsotaan vialliseksi, suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

— Jos hash-algoritmin tulos, joka laskettiin aiemmalla PERFORM HASH OF FILE -komennolla, ei ole käytettävissä, suorittamisen tilaa kuvaava vastaus on ‘**6985**’.

▼B

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Tämän komennon avulla todennetaan sellaisen kortille annetun viestin digitaalinen allekirjoitus, jonka hash-algoritmilla laskettu tulos on kortin tiedossa. Allekirjoitukseen käytetty algoritmi on automaattisesti kortin tiedossa.

Tämä komento on standardin ISO/IEC 7816-8 mukainen. Komennon käyttö on rajoitettua siihen liittyvään standardiin nähden.

Tämän komennon tukeminen DF Tachograph- ja DF Tachograph_G2 -tiedostossa edellyttää vain valvontakorttia.

Muut ajopiirturikorttityypit saattavat toteuttaa tämän komennon. Komento saattaa olla käytettävissä MF-tiedostossa.

TCS_132 VERIFY DIGITAL SIGNATURE -komento käyttää aina aiemmalla MANAGE SECURITY ENVIRONMENT MSE: Set DST -komennolla valittua julkista avainta ja aiempaa PSO: HASH -komennolla syötettyä hash-algoritmin tulosta.

TCS_133 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘00h’	CLA (komennon luokan ilmaiseva tavu)
INS (käskytavu)	1	‘2Ah’	PSO (Suorita turvatoimi)
P1	1	‘00h’	
P2	1	‘A8h’	Tuntomerkki: datakentässä on todennettavaa dataa
Lc	1	‘83h’	Seuraavan datakentän pituus Lc
6	1	‘9Eh’	Digitaalisen allekirjoituksen tuntomerkki
#7-#8	2	‘81 XXh’	Digitaalisen allekirjoituksen pituus: 128 tavua koodattuna lisäyksen 11 A osan mukaisesti ensimmäisen sukupolven ajopiirturisovelluksessa Riippuen valitusta käyrästä toisen sukupolven ajopiirturisovelluksessa (ks. lisäys 11, B osa)
#9-#(8+L)	L	‘XX..XXh’	Itse digitaalinen allekirjoitus

TCS_134 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— Jos allekirjoituksen todentaminen epäonnistuu, suorittamisen tilaa kuvaava vastaus on ‘**6688**’. Todentamisprosessi on kuvattu lisäyksessä 11.

— Jos julkista avainta ei ole valittu, suorittamisen tilaa kuvaava vastaus on ‘**6A88**’.

— Jos datasta puuttuu joitain (yllä määriteltyjä) osia, annetaan suorittamisen tilaa kuvaava vastaus ‘**6987**’. Näin voi tapahtua, jos jokin vaadituista tuntomerkeistä puuttuu.

▼B

— Jos komennon suorittamiseen tarvittavaa hash-algoritmin tulosta ei ole (aiemmin suoritetun PSO: HASH -komennon tuloksena), suorittamisen tilaa kuvaava vastaus on ‘**6985**’.

— Jos jotkin datan osat ovat virheellisiä, suorittamisen tilaa kuvaava vastaus on ‘**6988**’: Näin voi tapahtua, jos jonkin vaadittavan datan osan pituus on väärä.

— Jos valittu julkinen avain katsotaan virheelliseksi, suorittamisen tilaa kuvaava vastaus on ‘**6400**’ tai ‘**6581**’.

3.5.16 *PROCESS DSRC MESSAGE*

Tämän komennon avulla tarkistetaan DSRC-viestin eheys ja aitous sekä avataan ajoneuvoyksiköstä valvontaviranomaiselle tai korjaamolle DSRC-yhteyden kautta lähetetyn datan salaus. Kortti luo salausavaimen ja MAC-avaimen DSRC-viestin suojaamiseksi lisäyksen 11 B osan 13 kappaleessa kuvatulla tavalla.

Vain valvontakortin ja korjaamokortin täytyy tukea tätä komentoa DF Tachograph_G2 -tiedostossa.

Muuntyyppiset ajopiirturikortit voivat suorittaa tämän komennon tai olla suorittamatta sitä, mutta niillä ei ole DSRC-pääavainta. Sen vuoksi nämä kortit eivät voi suorittaa komentoa onnistuneesti, vaan palauttavat asianmukaisen virhekoodin.

Komento saattaa olla käytettävissä MF-tiedostossa ja/tai DF Tachograph -tiedostossa. Tällöin komennon on päätyttävä asianmukaiseen virhekoodiin.

TCS_135 DSRC-pääavain on käytettävissä vain DF Tachograph_G2 -tiedostossa, ts. valvontakortin ja korjaamokortin on tuettava komennon onnistunutta suorittamista vain DF Tachograph_G2 -tiedostossa.

TCS_136 Komennolla ainoastaan puretaan DSRC-datan salaus ja tarkistetaan salauksen tarkistussumma; sillä ei tulkita lähetettyä dataa.

TCS_137 Dataobjektien järjestys komennon datakentässä on määrätty tässä erittelyssä.

TCS_138 **Komentoviesti**

Tavu	Pituus	Arvo	Kuvaus
CLA	1	‘80h’	CLA-tavu erikoistarkoituksessa
INS (käskytavu)	1	‘2Ah’	PSO (Suorita turvatoimi)
P1	1	‘80h’	Vastauksen data: salaamaton
P2	1	‘B0h’	Komennon data: salaamaton data, joka on BER-TLV-koodattu, mukaan lukien salatun sanomanvälityksen dataobjektit
Lc	1	‘NNh’	Seuraavan datakentän pituus Lc

▼B

Tavu	Pituus	Arvo	Kuvaus
#6-#(5+L)	L	‘87h’ + L_{87} + ‘XX..XXh’	DER-TLV-koodattu täytetyn sisällön osoitintavu, jota seuraavat salatut ajopiirturin hyötykuormatiedot. Täytetyn sisällön osoitintavussa käytetään arvoa ‘00h’ (standardin ISO/IEC 7816-4:2013 taulukon 52 mukaan ”no further indication” [”ei tarkempia tietoja”]). Lisätietoja salausmekanismista, ks. lisäyksen 11 B osan 13 kappale. Pituudelle L_{87} sallittuja arvoja ovat AES-avainten lohkon pituuden kerrannaiset plus yksi tavu täytetyn sisällön osoitintavua varten, ts. vähintään 17 tavua ja enintään 193 tavua. *Huomautus:* Ks. lisätietoja salatun sanomanvälityksen dataobjektista tuntomerkillä ‘87h’ standardin ISO/IEC 7816-4:2013 taulukosta 49.
		‘81h’ + ‘10h’	DER-TLV-koodattu Control Reference Template for Confidentiality -malli, joka sijoittaa sisäkkäin seuraavien dataelementtien ketjutuksen (ks. lisäys 1 DSRCSecurityData ja lisäyksen 11 B osan 13 kappale): — 4-tavuinen aikaleima — 3-tavuinen laskuri — 8-tavuinen ajoneuvoyksikön sarjanumero — 1-tavuinen DSRC-pääavaimen versio *Huomautus:* Ks. lisätietoja salatun sanomanvälityksen dataobjektista tuntomerkillä ‘81h’ standardin ISO/IEC 7816-4:2013 taulukosta 49.
		‘8Eh’ + L_{8E} + ‘XX..XXh’	DER-TLV-koodattu MAC-koodi DSRC-viestillä. Lisätietoja MAC-algoritmista ja laskennasta, ks. lisäys 11, B osa, 13 kappale. *Huomautus:* Ks. lisätietoja salatun sanomanvälityksen dataobjektista tuntomerkillä ‘8Eh’ standardin ISO/IEC 7816-4:2013 taulukosta 49.

TCS_139 **Vastausviesti**

Tavu	Pituus	Arvo	Kuvaus
#1-#L	L	‘XX..XXh’	Puuttuva data (virhetapauksessa) tai data, jonka salaus on avattu (täyttö poistettu)
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, kortti vastaa ‘**9000**’.

— ‘**6A80**’ osoittaa väärät parametrit komennon datakentässä (käytetään myös, jos dataobjekteja ei lähetetä oikeassa järjestyksessä).

— ‘**6A88**’ osoittaa, että viitattu data ei ole käytettävissä, ts. viitattu DSRC-pääavain ei ole käytettävissä.

— ‘**6900**’ osoittaa, että salauksen tarkistussumman todentaminen tai datan salauksen avaus epäonnistui

4. AJOPIIRTURIKORTTIEN TIEDOSTORAKENNE

Tässä kohdassa määritellään ajopiirturikorteilla olevan käytettävän datan tallennukseen käytettävät tiedostorakenteet.

▼B

Kortin valmistajista riippuvia sisäisiä rakenteita kuten tiedostojen ylätunnisteita ei määritellä tässä, kuten ei myöskään sellaisten dataelementtien tallennusta ja käsittelyä, joita tarvitaan vain sisäiseen käyttöön, esimerkkeinä `EuropeanPublicKey`,`CardPrivateKey`,`TdesSessionKey` tai `WorkshopCardPin`.

TCS_140 Toisen sukupolven ajopiirturikortin on isännöitävä MF-tiedostoa (Master File) sekä samantyyppistä ensimmäisen ja toisen sukupolven ajopiirturisovellusta (esim. kuljettajakortin sovellukset).

TCS_141 Ajopiirturikortin on tuettava vähintään vastaavissa sovelluksissa määritettyä tietueiden vähimmäismäärää; sen tukemien tietueiden määrä ei saa ylittää vastaavissa sovelluksissa määritettyä tietueiden enimmäismäärää.

Tietueiden enimmäis- ja vähimmäismäärät on esitetty tässä kappaleessa kunkin sovelluksen osalta.

Lisätietoja tässä kappaleessa käytettyjen käyttöoikeussääntöjen turvallisuusehdoista on kappaleessa 3.3. Yleisesti ottaen käyttötila ”lue” (read) osoittaa READ BINARY -komennon, jossa on parillinen ja, mikäli sitä tuetaan, pariton INS-tavu, poikkeuksena EF-tiedoston Sensor_Installation_Data korjaamokortilla, ks. TCS_156 ja TCS_160. Käyttötila ”päivitä” (update) osoittaa Update Binary -komennon, jossa on parillinen ja, mikäli sitä tuetaan, pariton INS-tavu ja käyttötila ”valitse” (select) osoittaa SELECT-komennon.

4.1. **MF-tiedosto**

TCS_142 Sen jälkeen, kun MF-tiedostoon on liitetty sen yksilöivät tiedot, tiedostolla on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöoikeussäännöt:

Huomautus: .Lyhyt EF-tunniste SFID annetaan desimaalilukuna, esim. arvo 30 vastaa arvoa 11110 binaarisessa muodossa.

			Käyttöoikeussäännöt	
Tiedosto	**Tiedoston tunniste**	**SFID**	**Lue / Valitse**	**Päivitä**
`MF`	‘3F00h’			
`├─EF ICC`	‘0002h’		ALW	NEV
`├─EF IC`	‘0005h’		ALW	NEV
`├─EF DIR`	‘2F00h’	30	ALW	NEV
`├─EF ATR/INFO (ehdollinen)`	‘2F01h’	29	ALW	NEV
`├─EF Extended_Length (ehdollinen)`	‘0006h’	28	ALW	NEV
`├─DF Tachograph`	‘0500h’		SC1	
`└─DF Tachograph_G2`			SC1	

Tässä taulukossa käytetään seuraavaa turvallisuusehdon lyhennettä:

SC1 ALW OR SM-MAC-G2

TCS_143 Kaikkien EF-tiedostorakenteiden on oltava transparenttyyppisiä.

TCS_144 MF-tiedostolla on oltava seuraava tiedostorakenne:

▼B

Tiedosto / Dataelementti	Tietueiden lkm	Koko (tavua) Min.	Koko (tavua) Maks.	Oletusarvot
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 EF-tiedoston EF DIR on sisällettävä seuraavat sovelluskohtaiset dataobjektit: ‘61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54’

TCS_146 EF-tiedoston EF ATR/INFO on oltava läsnä, jos ajopiirturikortti ilmoittaa ATR-signaalissa tukevansa laajennettuja pituuskenttiä. Tällöin EF ATR/INFO -tiedoston on sisällettävä laajennettuja pituuskenttiä koskevaa tietoa osoittava dataobjekti (DO‘7F66’) standardin ISO/IEC 7816-4:2013 lausekkeen 12.7.1 mukaisesti.

TCS_147 EF-tiedoston EF Extended_Length on oltava läsnä, jos ajopiirturikortti ilmoittaa ATR-signaalissa tukevansa laajennettuja pituuskenttiä. Tällöin EF-tiedoston on sisällettävä seuraava dataobjekti: ‘02 01 xx’, jossa arvo ‘xx’ ilmoittaa tuetaanko laajettuja pituuskenttiä T=1-protokollassa ja / tai T=0-protokollassa.

Arvo ‘01’ ilmoittaa laajennettujen pituuskenttien tuen T=1-protokollassa.

Arvo ‘10’ ilmoittaa laajennettujen pituuskenttien tuen T=0-protokollassa.

Arvo ‘11’ ilmoittaa laajennettujen pituuskenttien tuen T=0-protokollassa ja T=1-protokollassa.

4.2. Kuljettajakortin sovellukset

4.2.1 *Kuljettajakortin ensimmäisen sukupolven sovellus*

TCS_148 Sen jälkeen, kun kuljettajakortin ensimmäisen sukupolven sovellukseen on liitetty sen yksilöivät tiedot, sillä on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöoikeussäännöt:

Tiedosto	Tiedoston tunniste	Käyttöoikeussäännöt: Lue	Valitse	Päivitä
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

▼B

Tässä taulukossa käytetään seuraavia turvallisuusehtojen lyhenteitä:

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 Kaikkien EF-tiedostorakenteiden on oltava transparent-tyyppisiä.

TCS_150 Kuljettajakortin ensimmäisen sukupolven sovelluksella on oltava seuraava tiedostorakenne:

Tiedosto / Dataelementti	Tietueiden lkm	Koko (tavua) Min.	Koko (tavua) Maks.	Oletusarvot
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				

▼B

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}

▼B

TCS_151 Seuraavat arvot, joita käytetään kokojen ilmaisemiseen edellä olevassa taulukossa, ovat niiden tietueiden vähimmäis- ja enimmäislukumääriä, joita kuljettajakortin tiedostorakenteessa on käytettävä ensimmäisen sukupolven sovellusta varten:

		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 tavua (28 päivää * 93 toiminnan muutosta)	13 776 tavua (28 päivää * 240 toiminnan muutosta)

4.2.2 *Kuljettajakortin toisen sukupolven sovellus*

TCS_152 Sen jälkeen, kun kuljettajakortin toisen sukupolven sovellukseen on liitetty sen yksilöivät tiedot, sillä on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöoikeussäännöt.

Huomautus: .Lyhyt EF-tunniste SFID annetaan desimaalilukuna, esim. arvo 30 vastaa arvoa 11110 binaarisessa muodossa.

			Käyttöoikeussäännöt	
Tiedosto	**Tiedoston tunniste**	**SFID**	**Lue / Valitse**	**Päivitä**
└─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

Tässä taulukossa käytetään seuraavaa turvallisuusehdon lyhennettä:

SC1 ALW OR SM-MAC-G2

TCS_153 Kaikkien EF-tiedostorakenteiden on oltava transparenttyyppisiä.

TCS_154 Kuljettajakortin toisen sukupolven sovelluksella on oltava seuraava tiedostorakenne:

▼B

Tiedosto / Dataelementti	Tietueiden lkm	Koko (tavua) Min.	Koko (tavua) Maks.	Oletusarvot
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*	

▼B

├─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}

▼B

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 Seuraavat arvot, joita käytetään kokojen ilmaisemiseen edellä olevassa taulukossa, ovat niiden tietueiden vähimmäis- ja enimmäislukumääriä, joita kuljettajakortin tiedostorakenteessa on käytettävä toisen sukupolven sovellusta varten:

		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 tavua (28 päivää * 93 toiminnan muutosta)	13 776 tavua (28 päivää * 240 toiminnan muutosta)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. **Korjaamokortin sovellukset**

4.3.1 *Korjaamokortin ensimmäisen sukupolven sovellus*

TCS_156 Sen jälkeen, kun korjaamokortin ensimmäisen sukupolven sovellukseen on liitetty sen yksilöivät tiedot, sillä on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöoikeussäännöt:

▼B

Tiedosto	Tiedoston tunniste	Käyttöoikeussäännöt		
		Lue	Valitse	Päivitä
└─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

Tässä taulukossa käytetään seuraavia turvallisuusehtojen lyhenteitä:

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 READ BINARY -komento parillisella INS-tavulla:

(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)

READ BINARY -komento parittomalla INS-tavulla (jos tuettu): NEV

TCS_157 Kaikkien EF-tiedostorakenteiden on oltava transparent-tyyppisiä.

TCS_158 Korjaamokortin ensimmäisen sukupolven sovelluksella on oltava seuraava tiedostorakenne:

▼B

Tiedosto / Dataelementti	Tietueiden lkm	Koko (tavua) Min.	Koko (tavua) Maks.	Oletusarvot
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}

▼B

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}

▼B

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 Seuraavat arvot, joita käytetään kokojen ilmaisemiseen edellä olevassa taulukossa, ovat niiden tietueiden vähimmäis- ja enimmäislukumääriä, joita korjaamokortin tiedostorakenteessa on käytettävä ensimmäisen sukupolven sovellusta varten:

		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 tavua (1 päivä * 93 toiminnan muutosta)	492 tavua (1 päivä * 240 toiminnan muutosta)

4.3.2 *Korjaamokortin toisen sukupolven sovellus*

TCS_160 Sen jälkeen, kun korjaamokortin toisen sukupolven sovellukseen on liitetty sen yksilöivät tiedot, sillä on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöoikeussäännöt.

Huomautus: .Lyhyt EF-tunniste SFID annetaan desimaalilukuna, esim. arvo 30 vastaa arvoa 11110 binaarisessa muodossa.

			Käyttöoikeussäännöt		
Tiedosto	**Tiedoston tunniste**	**SFID**	**Lue**	**Valitse**	**Päivitä**
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-G2	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

▼B

Tässä taulukossa käytetään seuraavia turvallisuusehtojen lyhenteitä:

SC1 ALW OR SM-MAC-G2

SC5 Read Binary -komento parillisella INS-tavulla: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

Read Binary -komento parittomalla INS-tavulla (jos tuettu): NEV

TCS_161 Kaikkien EF-tiedostorakenteiden on oltava transparent-tyyppisiä.

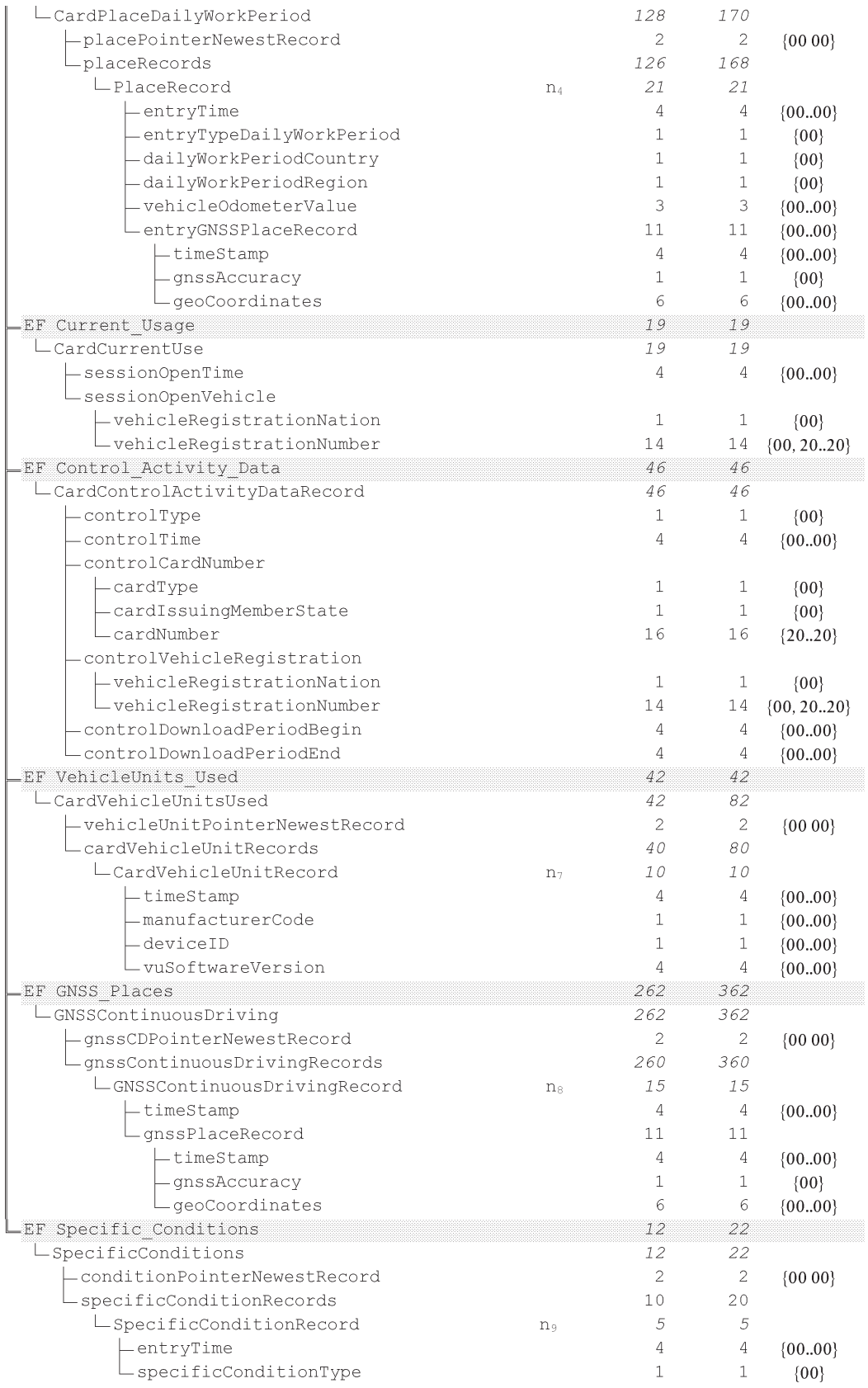
TCS_162 Korjaamokortin toisen sukupolven sovelluksella on oltava seuraava tiedostorakenne:

Tiedosto / Dataelementti	Tietueiden lkm	Koko (tavua) Min.	Koko (tavua) Maks.	Oletusarvot
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}

▼B

├─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*	

▼B



└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}

▼B

TCS_163 Seuraavat arvot, joita käytetään kokojen ilmaisemiseen edellä olevassa taulukossa, ovat niiden tietueiden vähimmäis- ja enimmäislukumääriä, joita korjaamokortin tiedostorakenteessa on käytettävä toisen sukupolven sovellusta varten:

		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 tavua (1 päivä * 93 toiminnan muutosta)	492 tavua (1 päivä * 240 toiminnan muutosta)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Valvontakortin sovellukset

4.4.1 *Valvontakortin ensimmäisen sukupolven sovellus*

TCS_164 Sen jälkeen, kun valvontakortin ensimmäisen sukupolven sovellukseen on liitetty sen yksilöivät tiedot, sillä on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttösäännöt:

		Käyttöoikeussäännöt		
Tiedosto	**Tiedoston tunniste**	**Lue**	**Valitse**	**Päivitä**
└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

Tässä taulukossa käytetään seuraavia turvallisuusehtojen lyhenteitä:

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 Kaikkien EF-tiedostorakenteiden on oltava transparenttyyppisiä.

TCS_166 Valvontakortin ensimmäisen sukupolven sovelluksella on oltava seuraava tiedostorakenne:

▼B

Tiedosto / Dataelementti	Tietueiden lkm	Koko (tavua) 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 Seuraavat arvot, joita käytetään kokojen ilmaisemiseen edellä olevassa taulukossa, ovat niiden tietueiden vähimmäis- ja enimmäislukumääriä, joita valvontakortin tiedostorakenteessa on käytettävä ensimmäisen sukupolven sovellusta varten:

		Min.	Maks.
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Valvontakortin toisen sukupolven sovellus*

TCS_168 Sen jälkeen, kun valvontakortin toisen sukupolven sovellukseen on liitetty sen yksilöivät tiedot, sillä on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöoikeussäännöt.

Huomautus: .Lyhyt EF-tunniste SFID annetaan desimaalilukuna, esim. arvo 30 vastaa arvoa 11110 binaarisessa muodossa.

▼B

Tiedosto	Tiedoston tunniste	SFID	Käyttöoikeussäännöt	
			Lue / Valitse	Päivitä
└─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

Tässä taulukossa käytetään seuraavaa turvallisuusehdon lyhennettä:

SC1 ALW OR SM-MAC-G2

TCS_169 Kaikkien EF-tiedostorakenteiden on oltava transparenttyyppisiä.

TCS_170 Valvontakortin toisen sukupolven sovelluksella on oltava seuraava tiedostorakenne:

Tiedosto / Dataelementti	Tietueiden lkm	Koko (tavua) 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 Seuraavat arvot, joita käytetään kokojen ilmaisemiseen edellä olevassa taulukossa, ovat niiden tietueiden vähimmäis- ja enimmäislukumääriä, joita valvontakortin tiedostorakenteessa on käytettävä toisen sukupolven sovellusta varten:

▼B

		Min.	Maks.
n_7	NoOfControlActivityRecords	230	520

4.5. **Yrityskortin sovellukset**

4.5.1 *Yrityskortin ensimmäisen sukupolven sovellus*

TCS_172 Sen jälkeen, kun yrityskortin ensimmäisen sukupolven sovellukseen on liitetty sen yksilöivät tiedot, sillä on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöoikeussäännöt:

		Käyttöoikeussäännöt		
Tiedosto	**Tiedoston tunniste**	**Lue**	**Valitse**	**Päivitä**
└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

Tässä taulukossa käytetään seuraavia turvallisuusehtojen lyhenteitä:

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 Kaikkien EF-tiedostorakenteiden on oltava transparenttyyppisiä.

TCS_174 Yrityskortin ensimmäisen sukupolven sovelluksella on oltava seuraava tiedostorakenne:

Tiedosto / Dataelementti	Tietueiden lkm	Koko (tavua) Min.	Koko (tavua) Maks.	Oletusarvot
└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}

▼B

TCS_175 Seuraavat arvot, joita käytetään kokojen ilmaisemiseen edellä olevassa taulukossa, ovat niiden tietueiden vähimmäis- ja enimmäislukumääriä, joita yrityskortin tiedostorakenteessa on käytettävä ensimmäisen sukupolven sovellusta varten:

		Min.	Maks.
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Yrityskortin toisen sukupolven sovellus*

TCS_176 Sen jälkeen, kun yrityskortin toisen sukupolven sovellukseen on liitetty sen yksilöivät tiedot, sillä on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöoikeussäännöt:

Huomautus: .Lyhyt EF-tunniste SFID annetaan desimaalilukuna, esim. arvo 30 vastaa arvoa 11110 binaarisessa muodossa.

			Käyttöoikeussäännöt	
Tiedosto	**Tiedoston tunniste**	**SFID**	**Lue / Valitse**	**Päivitä**
└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

Tässä taulukossa käytetään seuraavaa turvallisuusehdon lyhennettä:

SC1 ALW OR SM-MAC-G2

TCS_177 Kaikkien EF-tiedostorakenteiden on oltava transparenttyyppisiä.

TCS_178 Yrityskortin toisen sukupolven sovelluksella on oltava seuraava tiedostorakenne:

Tiedosto / Dataelementti	**Tietueiden lkm**	**Koko (tavua) Min.**	**Maks.**	**Oletusarvot**
└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}

▼B

TCS_179 Seuraavat arvot, joita käytetään kokojen ilmaisemiseen edellä olevassa taulukossa, ovat niiden tietueiden vähimmäis- ja enimmäislukumääriä, joita yrityskortin tiedostorakenteessa on käytettävä toisen sukupolven sovellusta varten:

		Min.	Maks.
n_8	NoOfCompanyActivityRecords	230	520

▼B

Lisäys 3

KUVAKKEET

PIC_001 Ajopiirturi saa haluttaessa käyttää seuraavia kuvakkeita ja kuvakkeiden yhdistelmiä (tai kuvakkeita ja yhdistelmiä, jotka ovat riittävän samanlaisia, että ne voidaan yksiselitteisesti tunnistaa näiksi):

1. PERUSKUVAKKEET

	Toimijat	**Tehtävät**	**Toimintatavat**
	Yritys		Yritystila
	Tarkastaja	Valvonta	Tarkastustila
	Kuljettaja	Ajo	Normaalitila
	Korjaamo/testausasema	Tarkastus/kalibrointi	Kalibrointitila
	Valmistaja		

	Toiminta	**Kesto**
	Varalla	Kuluva varallaoloaika
	Ajo	Keskeytymätön ajoaika
	Lepo	Kuluva lepoaika
	Muu työ	Kuluva työaika
	Tauko	Yhteenlaskettu taukoaika
	Tuntematon	

	Laitteet	**Toiminnot**
	Kuljettajan korttiaukko	
	Apukuljettajan korttiaukko	
	Kortti	
	Kello	
	Näyttö	Näyttäminen
	Ulkoinen tallennus	Lataaminen
	Virtalähde	
	Tulostin/tuloste	Tulostaminen
	Tunnistin	
	Rengaskoko	
	Ajoneuvo/ajoneuvoyksikkö (VU)	
	GNSS-laitteisto	
	Havaitsemiseen tarkoitettu etäyhteyslaite	
	ITS-rajapinta	

▼B

Erityisolosuhteet

OUT	Asetuksen piiriin kuulumaton
	Juna-/lauttamatka

Muut

	Tapahtumat		Viat
	Päivän työaika alkaa		Päivän työaika päättyy
	Sijainti		
	Kuljettajan toimintaa koskevien tietojen syöttö käsin		
	Turvallisuus		
	Nopeus		
	Aika		
	Yhteensä/yhteenveto		

Määritteet

24h	Päivittäin
	Viikoittain
	Kaksi viikkoa
	Jostain alkaen tai johonkin asti

2. KUVAKEYHDISTELMÄT

Muut

	Tarkastuspaikka		
	Päivän työaika alkaa sijainnissa		Päivän työaika päättyy sijainnissa
	Alkaa kello		Päättyy kello
	Ajoneuvosta		
OUT	Asetuksen piiriin kuulumaton ajo alkaa	OUT	Asetuksen piiriin kuulumaton ajo päättyy

Kortit

	Kuljettajakortti
	Yrityskortti
	Valvontakortti
	Korjaamokortti
– – –	Ei korttia

Ajo

	Ajo miehitettynä
	Yhden viikon ajoaika
	Kahden viikon ajoaika

▼B

	Tulosteet
24h	Kuljettajan toimintaa koskevien tietojen päivittäinen tuloste kortilta
24h	Kuljettajan toimintaa koskevien tietojen päivittäinen tuloste ajoneuvoyksiköstä (VU)
	Tapahtumat ja viat kortin tietojen mukaan tulostettuina
	Ajoneuvoyksikön (VU) muistissa olevia tapahtumiin ja vikoihin liittyviä tietoja sisältävä tuloste
	Teknisten tietojen tuloste
	Ylinopeustuloste
	Tapahtumat
	Ei voimassa olevan kortin asettaminen laitteeseen
	Korttiristiriita
	Aikojen päällekkäisyys
	Ajo ilman asianmukaista korttia
	Kortin paikoilleen asettaminen ajon aikana
	Edellistä kortin käyttöjaksoa ei lopetettu oikein
	Ylinopeus
	Keskeytynyt virransyöttö
	Virhe liikedatassa
	Ajoneuvon liikeristiriita
	Tietoturvamurto
	Ajan asetus (korjaamon tekemä)
	Ylinopeuden valvonta
	Viat
	Korttivika (kuljettajan korttiaukko)
	Korttivika (apukuljettajan korttiaukko)
	Vika näytössä
	Tietojen kopiointiin liittyvä vika
	Vika tulostimessa
	Vika liiketunnistimessa
	Vika ajoneuvoyksikön (VU) sisällä
	Vika GNSS-laitteistossa
	Vika havaitsemiseen tarkoitetussa etäyhteyslaitteessa
	Tietojen syöttäminen käsin
	Koskevatko tiedot vielä saman päivän työaikaa?
	Päättyykö edellisen päivän työaika?
	Vahvista tai syötä paikka, jossa työaika päättyi
	Syötä aloitusaika
	Syötä paikka, jossa työaika alkaa.

Huomautus: Lisäyksessä 4 on määritelty muita kuvakeyhdistelmiä, joita käytetään tulostettavien lohkojen tai tietueiden tunnisteena.

▼B

Lisäys 4

TULOSTEET

SISÄLLYSLUETTELO

1. YLEISTÄ

2. DATALOHKOJEN ERITTELY

3. TULOSTEIDEN ERITTELYT

3.1. Kortilla olevia kuljettajan toimintaa koskevia tietoja sisältävä päivittäinen tuloste

3.2. Ajoneuvoyksikön muistissa olevia kuljettajan toimintaa koskevia tietoja sisältävä päivittäinen tuloste

3.3. Tapahtumat ja viat kortin tietojen mukaan tulostettuna

3.4. Ajoneuvoyksikön (VU) muistissa olevia tapahtumiin ja vikoihin liittyviä tietoja sisältävä tuloste

3.5. Teknisten tietojen tuloste

3.6. Ylinopeustuloste

3.7 Asetettujen korttien historia

1. YLEISTÄ

Kaikki tulosteet syntyvät ketjuttamalla eri datalohkoja, joilla mahdollisesti on lohkon tunniste.

Datalohko sisältää yhden tai useamman tietueen, jolla mahdollisesti on tietueen tunniste.

PRT_001 Jos lohkotunniste on välittömästi ennen tietuetunnistetta, tietueen tunnistetta ei tulosteta.

PRT_002 Jos jotain datan osaa ei tunneta tai sitä ei käyttöoikeussyistä saa tulostaa, tulostetaan välilyöntejä.

PRT_003 Jos koko rivin sisältö on tuntematon tai sen tulostaminen ei ole tarpeen, jätetään koko rivi pois

PRT_004 Numerotietoja sisältävät datakentät tulostetaan oikealle tasattuna, tuhannet ja miljoonat välilyönnillä erotettuna ja ilman etunollia.

PRT_005 Merkkijonoja sisältävät datakentät tulostetaan vasemmalle tasattuna ja välilyönneillä oikeaan pituuteen täytettyinä tai tarpeen mukaan lyhennettyinä (nimet ja osoitteet).

PRT_006 Jos pitkän tekstin takia tarvitaan rivinsiirto, uuden rivin ensimmäiseksi merkiksi on tulostettava erikoismerkki (rivin keskikorkeudella oleva piste, ”•”).

2. DATALOHKOJEN ERITTELY

Tässä luvussa käytetään seuraavia muotoilujen merkintätapoja:

— **lihavoitu** teksti merkitsee tavallista tekstiä, joka tulostetaan (tulostaminen tapahtuu ilman lihavointia),

▼B

— normaali teksti merkitsee muuttujia (kuvakkeita tai dataa), jotka tulostettaessa korvataan vastaavilla muuttujan arvoilla,

— muuttujien nimet on täytetty alleviivausmerkein osoittamaan kullekin muuttujalle varatun datan osan pituutta,

— päivämäärät on esitetty muodossa ’pp/kk/vvvv’ (päivä, kuukausi, vuosi); muotoa ’pp.kk.vvvv’ voidaan myös käyttää,

— kortin tunniste koostuu kortin tyyppiä kuvaavasta kuvakeyhdistelmästä, kortin myöntäneen jäsenvaltion tunnuksesta, vinoviivasta sekä kortin numerosta, jossa sen korvaus- ja uusintanumerot on erotettu välilyönnillä:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kortin kuvakeyhdistelmä		Kortin myöntäneen jäsenvaltion tunnus				Kortin numeron 14 ensimmäistä merkkiä (sisältää mahdollisesti järjestysnumeron)														Korvausnumero		Uusintanumero

▼B

PRT_007 Tulosteissa on käytettävä seuraavia datalohkoja ja/tai tietueita seuraavissa merkityksissä ja muodoissa:

Lohkon tai tietueen numero Merkitys	Data Format
1 ***Päivämäärä ja aika, jolloin asiakirja on tulostettu.***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Tulosteen tyyppi*** Lohkon tunniste Tulosteen kuvakeyhdistelmä (ks. lisäys 3), nopeudenrajoittimen asetus (vain ylinopeustapauksia koskeva tuloste)	----------▼---------- Picto xxx **km/h**
3 ***Kortin haltijan tunniste*** Lohkon tunniste. P = henkilöihin liittyvä kuvake Kortin haltijan sukunimi Kortin haltijan etunimi (-nimet) (jos sellainen on) Kortin tunniste Kortin viimeinen voimassaolopäivä (jos sellainen on) ja kortin sukupolvinumero (GEN 1 tai GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

Jos kortti ei ole henkilökohtainen eikä sisällä kortin haltijan sukunimeä, tulostetaan sen sijaan yrityksen tai korjaamon tai valvontaelimen nimi.

(*) Kortin sukupolvinumero voidaan tulostaa vain älykkäällä ajopiirturilla.

4	***Ajoneuvon tunniste*** Lohkon tunniste VIN Rekisteröinyt jäsenvaltio ja rekisteritunnus (VRN)	----------🚘---------- 🚘 VIN_____ Nat/VRN_____
5	***Ajoneuvoyksikön (VU) tunniste*** Lohkon tunniste Ajoneuvoyksikön valmistajan nimi Ajoneuvoyksikön osanumero Ajoneuvoyksikön sukupolvinumero (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Kortin sukupolvinumero voidaan tulostaa vain älykkäällä ajopiirturilla.

6	***Ajopiirturin viimeisin kalibrointi*** Lohkon tunniste Korjaamon nimi Korjaamokortin tunniste Kalibroinnin päivämäärä	----------🔧---------- 🔧 Last_Name_____ Card_Identification_____ 🔧 dd/mm/yyyy

▼B

7 ***Viimeisin (valvontaviranomaisen suorittama) tarkastus***

Lohkon tunniste

Valvontakortin tunniste

Tarkastuksen päivämäärä, aika ja tyyppi

```
----------▯----------
Card_Identification_____
▯ dd/mm/yyyy hh:mm ppppp
```

Tarkastuksen tyyppi: Korkeintaan viisi kuvaketta. Tarkastuksen tyyppi voi olla jokin (yhdistelmä) seuraavista:

▮: kortin tietojen kopiointi, ↧: ajoneuvoyksikön tietojen kopiointi, ⍑: tulostus, ▯: tietojen näyttö, ⊺: kalibroinnin tarkastus tien varrella

8 ***Kortille tallennetut kuljettajan toimintaa koskevat tiedot aikajärjestyksessä***

Lohkon tunniste

Kyseinen päivä (kalenterivuorokausi, jota tuloste koskee) + kortin päivittäisten käyttökertojen laskuri

```
----------⊙----------
    dd/mm/yyyy  xxx
```

8a *Out of scope olosuhteet päivän alussa* (ei täytetä, jos out of scope olosuhteita ei ole voimassa)

```
----------OUT----------
```

8.1 *Ajanjakso, jolloin kortti ei ollut paikoillaan laitteessa*

8.1a Tietueen tunniste (ajanjakson alku)

8.1b *Tuntematon jakso*. Alkamisaika, kesto

8.1c *Käsin syötetyt toimintatiedot*. Toimintakuvake, alkamisaika, kesto

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Kortin asetus korttiaukkoon S*

Tietueen tunniste; S = korttiaukkokuvake

Ajoneuvon rekisteröinyt jäsenvaltio ja ajoneuvon rekisteritunnus

Ajoneuvon matkamittarin lukema silloin, kun kortti asetettiin paikoilleen

```
  ---------S---------
Nat/VRN_____________
  x xxx xxx km
```

8.3 *Toiminta (kortin ollessa paikoillaan)*

Toimintakuvake, alkamisaika, kesto, miehitys (miehityskuvake, jos tila on CREW, tyhjää, jos SINGLE).

```
A       hh:mm hhhmm ⊙⊙
```

8.3a *Erityisolosuhteet*. Aika, jolloin tieto syötettiin, erityisolosuhteisiin liittyvä kuvake (tai kuvakkeiden yhdistelmä).

```
        hh:mm ---pppp---
```

8.4 *Kortin poisto*

Ajoneuvon matkamittarin lukema ja viimeisin sellaisen kortin paikoilleen asettamisen jälkeen kuljettu matka, jota vastaava matkamittarin lukema on tiedossa

```
  x xxx xxx km; x xxx km
```

9 ***Ajoneuvoyksikköön tallennetut kuljettajan toimintaa koskevat tiedot korttiaukoittain aikajärjestyksessä***

Lohkon tunniste

Kyseinen päivä (kalenterivuorokausi, jota tuloste koskee)

Ajoneuvon matkamittarin lukema klo 00:00 ja klo 24:00

```
----------⊙----------
       dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10 ***Korttiaukkoon S liittyvät tehdyt toimet***

Lohkon tunniste

```
----------S----------
```

10a *Out of scope olosuhteet päivän alussa* (ei täytetä, jos out of scope olosuhteita ei ole voimassa)

```
----------OUT----------
```

10.1 *Jakso, jolloin aukossa S ei ole korttia*

Tietueen tunniste.

Korttia ei ole asetettu

Ajoneuvon matkamittarin lukema jakson alussa

```
  --------------------
⊙▮---
  x xxx xxx km
```

10.2 *Kortin paikoilleen asettaminen*

Kortin paikoilleen asetusta koskevan tietueen tunniste

Kuljettajan nimi

```
  --------------------
⊙ Last_Name_____________
```

▼B

	Kuljettajan etunimi	First_Name_____
	Kuljettajakortin tunniste	Card_Identification_____
	Kortin viimeinen voimassaolopäivä (jos sellainen on) ja kortin sukupolvinumero (GEN 1 tai GEN 2) (*)	dd/mm/yyyy - GEN 2
	Kuljettajan tätä ennen käyttämän ajoneuvon rekisteröinyt jäsenvaltio ja ajoneuvon rekisteritunnus	Nat/VRN_____
	Päivämäärä ja aika, jolloin kortti poistettiin edellisestä ajoneuvosta	dd/mm/yyyy hh:mm
	Tyhjä rivi	
	Ajoneuvon matkamittarin lukema korttia paikoilleen asetettaessa, kuljettajan toimintaa koskevien tietojen käsin syöttämistä koskeva tunnusmerkki (M, jos käsin syötetty, muuten tyhjä). Jos kuljettajakorttia ei asetettu paikoilleen sinä päivänä, jota tuloste koskee, lohkossa 10.2 on käytettävä matkamittarin lukemaa viimeiseltä käytettävissä olevalta kerralta, jolloin kortti asetettiin paikoilleen ennen kyseistä päivää.	x xxx xxx **km** M
10.3	*Toiminta*	
	Toimintakuvake, alkamisaika, kesto, miehitys (miehityskuvake, jos tila on CREW, tyhjää, jos SINGLE).	A hh:mm hh**h**mm
10.3a	*Erityisolosuhteet*. Aika, jolloin tieto syötettiin, erityisolosuhteisiin liittyvä kuvake (tai kuvakkeiden yhdistelmä).	hh:mm ---pppp---
10.4	*Kortin poisto tai "ilman korttia" -jakson päättyminen*	
	Ajoneuvon matkamittarin lukema korttia poistettaessa tai "ilman korttia" jakson päättyessä sekä kortin paikoilleen asettamisen tai "ei korttia" jakson alkamisen jälkeen kuljettu matka.	x xxx xxx **km**; x xxx **km**

(*) Kortin sukupolvinumero voidaan tulostaa vain älykkäällä ajopiirturilla.

11	***Päivittäinen yhteenveto***	
	Lohkon tunniste	----------Σ----------
11.1	***Ajoneuvoyksikön tietojen yhteenveto jaksoista, jolloin kuljettajan korttiaukossa ei ollut korttia***	
	Lohkon tunniste	1----
11.2	***Ajoneuvoyksikön tietojen yhteenveto jaksoista, jolloin apukuljettajan korttiaukossa ei ollut korttia***	
	Lohkon tunniste	2----
11.3	***Ajoneuvoyksikön tietojen päivittäinen kuljettajakohtainen yhteenveto***	
	Tietueen tunniste	----------
	Kuljettajan sukunimi	Last_Name_____
	Kuljettajan etunimi (etunimet)	First_Name_____
	Kuljettajakortin tunniste	Card_Identification_____
11.4	*Päivittäisen työajan alkamis- ja/tai päättymispaikkaa koskevat tiedot*	
	pi = alkamis-/päättymispaikan kuvake, aika, maa, alue	pihh:mm Cou Reg
	Matkamittari	x xxx xxx **km**
11.5	*Päivittäisen työajan alkamis- ja/tai päättymispaikkaa koskevat tiedot*	
	ja kolmen tunnin jälkeen keskeytymätön ajoaika	hh:mm
	Matkamittari	x xxx xxx **km**
11.6	*Toiminnan kokonaiskestoajat (kortilta)*	
	Kokonaisajoaika, kuljettu matka	hh**h**mm x xxx **km**
	Työn ja varallaolon kokonaisaika	hh**h**mm hh**h**mm
	Levon ja tuntemattoman toiminnan kokonaisaika	hh**h**mm ? hh**h**mm
	Ajoneuvon miehistön toiminnan kokonaisaika	hh**h**mm
11.7	*Toiminnan kokonaiskestoajat (jaksot ilman kuljettajan korttiaukkoa)*	
	Kokonaisajoaika, kuljettu matka	hh**h**mm x xxx **km**
	Työn ja varallaolon kokonaisaika	hh**h**mm hh**h**mm
	Kokonaislepoaika	hh**h**mm

▼B

11.8	*Toiminnan kokonaiskestoajat (jaksot ilman apukuljettajan korttiaukkoa)*	
	Työn ja varallaolon kokonaisaika	`hhhmm hhhmm`
	Kokonaislepoaika	`hhhmm`
11.9	*Toiminnan kokonaiskestoajat (kuljettajaa kohden molemmat korttiaukot mukaan lukien)*	
	Kokonaisajoaika, kuljettu matka	`hhhmm x xxx km`
	Työn ja varallaolon kokonaisaika	`hhhmm hhhmm`
	Kokonaislepoaika	`hhhmm`
	Ajoneuvon miehistön toiminnan kokonaisaika	`hhhmm`

Tarvittaessa kuluvaa päivää koskeva päivittäinen tuloste, päivittäiset yhteenvetotiedot lasketaan tiedoista, jotka ovat käytettävissä tulostushetkellä.

12	***Kortille tallennetut tapahtumia ja/tai vikoja koskevat tiedot***	
12.1	Viittä viimeistä tapahtumaa ja vikaa koskevan kortilla olevan tietuelohkon tunniste	`----------!×----------`
12.2	Kaikkia tallennettuja tapahtumia koskevan kortilla olevan tietuelohkon tunniste	`----------!----------`
12.3	Kaikkia tallennettuja vikoihin liittyviä tietoja koskevan kortilla olevan tietuelohkon tunniste	`----------×----------`
12.4	*Tapahtumaa ja/tai vikaa koskeva tietue*	
	Tietueen tunniste	`----------`
	Tapahtumaa/vikaa tarkoittava kuvake, syy tietojen tallentamiseen, alkamispäivämäärä ja -aika	`Pic (p) dd/mm/yyyy hh:mm`
	Lisätietona annettu tapahtuman/vian tunnus (jos on), kesto	`!xx hhhmm`
	Sen ajoneuvon rekisteröinyt jäsenvaltio ja rekisteritunnus, jossa tapahtuma tai vika sattui	`Nat/VRN_____`

13	***Ajoneuvoyksikköön tallennetut tai meneillään olevia tapahtumia ja/tai vikoja koskevat tiedot***	
13.1	Viittä viimeistä tapahtumaa ja vikaa koskevan, ajoneuvoyksikön muistissa olevan tietuelohkon tunniste	`----------!×----------`
13.2	Kaikkia tallennettuja tai meneillään olevia tapahtumia koskevan, ajoneuvoyksikön muistissa olevan tietuelohkon tunniste	`----------!----------`
13.3	Kaikkia tallennettuja tai meneillään oleviin vikoihin liittyviä tietoja koskevan, ajoneuvoyksikön muistissa olevan tietuelohkon tunniste	`----------×----------`
13.4	*Tapahtumaa ja/tai vikaa koskeva tietue*	
	Tietueen tunniste	`----------`
	Tapahtumaa/vikaa tarkoittava kuvake, syy tietojen tallentamiseen, alkamispäivämäärä ja -aika	`Pic (p) dd/mm/yyyy hh:mm`
	Lisätietona annettu tapahtuman/vian tunnus (jos on), kyseisenä päivänä sattuneiden vastaavien tapahtumien määrä, kesto	`!xx (xxx) hhhmm`
	Tapahtuman tai vikatapahtuman alkaessa paikoilleen asetettuna olleiden korttien tunnisteet (enintään neljä riviä ilman, että samoja kortin numeroita toistetaan)	`Card_Identification_____` (4 rivi)
	Jos mitään korttia ei ollut asetettu paikoilleen	`---`
	Valmistajakohtaiset tiedot	`< Literal><ErrorCode>`

Tietojen tallentamisen syy (p) on numerotunnus, joka ilmaisee, miksi tapahtumaa tai vikaa koskevat tiedot tallennettiin, koodattuna dataelementin `EventFaultRecordPurpose` mukaisesti.

`Literal` on ajopiirturin valmistajan erityinen literaali, jossa on korkeintaan 12 merkkiä.

`ErrorCode` on ajopiirturin valmistajan erityinen virhekoodi, jossa on korkeintaan 12 merkkiä.

▼B

14	***Ajoneuvoyksikön tunniste***	
	Lohkon tunniste	----------⊟----------
	Ajoneuvoyksikön valmistajan nimi	⊟ Name_____
	Ajoneuvoyksikön valmistajan osoite	Address_____
	Ajoneuvoyksikön osanumero	PartNumber_____
	Ajoneuvoyksikön hyväksyntänumero	Apprv_____
	Ajoneuvoyksikön sarjanumero	S/N_____
	Ajoneuvoyksikön valmistusvuosi	yyyy
	Ajoneuvoyksikön ohjelmiston versio ja asennuspäivä	V xxxx dd/mm/yyyy
15	***Liiketunnistimen tunniste***	
	Lohkon tunniste	----------Л----------
15.1	*Liittämistietue*	
	Liiketunnistimen sarjanumero	Л S/N_____
	Liiketunnistimen hyväksyntänumero	Apprv_____
	Tunnistimen liittämispäivämäärä	dd/mm/yyyy hh:mm
16	***GNSS-tunniste***	
	Lohkon tunniste	----------▚----------
16.1	*Kytkemistietue*	
	Ulkoisen GNSS-laitteiston sarjanumero	▚ S/N_____
	Ulkoisen GNSS-laitteiston hyväksyntänumero	Apprv_____
	Ulkoisen GNSS-laitteiston kytkentäpäivämäärä	dd/mm/yyyy hh:mm
17	***Kalibrointiin liittyvät tiedot***	
	Lohkon tunniste	----------T----------
17.1	*Kalibrointitietue*	
	Tietueen tunniste	----------
	Kalibroinnin tehnyt korjaamo	T Workshop_name_____
	Korjaamon osoite	Workshop_address_____
	Korjaamokortin tunniste	Card_Identification_____
	Korjaamokortin viimeinen voimassaolopäivä	dd/mm/yyyy
	Tyhjä rivi	
	Kalibrointipäivä + kalibroinnin tarkoitus	T dd/mm/yyyy (p)
	VIN	A VIN_____
	Rekisteröinyt jäsenvaltio ja VRN	Nat/VRN_____
	Ajoneuvon ominaiskerroin	w xx xxx Imp/km
	Valvontalaitteen vakio	k xx xxx Imp/km
	Effective circumference of wheel tyres	l xx xxx mm
	Ajoneuvoon asennettujen renkaiden koko	● TyreSize_____
	Nopeudenrajoittimen asetukset	> xxx km/h
	Vanha ja uusi matkamittarin lukema	x xxx xxx – x xxx xxx km

Kalibroinnin syy (p) on numerotunnus, joka ilmaisee, miksi kalibrointiparametrit tallennettiin, koodattuna dataelementin `CalibrationPurpose` mukaisesti.

▼B

18	***Ajan asetus***	
	Lohkon tunniste	`----------◷----------`
18.1	*Ajan asetusta koskeva tietue*	
	Tietueen tunniste	`--------------------`
	Vanha päivä ja aika	`!◷ dd/mm/yyyy hh:mm`
	Uusi päivä ja aika	`◷ dd/mm/yyyy hh:mm`
	Ajan asetuksen tehnyt korjaamo	`T Workshop_name_____`
	Korjaamon osoite	`Workshop_address_____`
	Korjaamokortin tunniste	`Card_Identification_____`
	Korjaamokortin viimeinen voimassaolopäivä	`dd/mm/yyyy`
19	***Viimeisin ajoneuvoyksikön muistiin tallennettu tapahtuma ja vika***	
	Lohkon tunniste	`----------!×д----------`
	Viimeisimmän tapahtuman päivämäärä ja aika	`! dd/mm/yyyy hh:mm`
	Viimeisimmän vian päivämäärä ja aika	`× dd/mm/yyyy hh:mm`
20	***Ylinopeusvalvontaan liittyvät tiedot***	
	Lohkon tunniste	`----------►►----------`
	Viimeisimmän OVER SPEEDING CONTROL toimenpiteen päivämäärä ja aika	`►◘dd/mm/yyyy hh:mm`
	Ensimmäisen ylinopeustapauksen päivämäärä/aika ja ylinopeustapausten määrä sen jälkeen	`►►dd/mm/yyyy hh:mm (nnn)`
21	***Ylinopeuteen liittyvä tietue***	
21.1	Lohkon tunniste 'Ensimmäinen ylinopeustapaus viimeisimmän kalibroinnin jälkeen'	`--------►►T---------`
21.2	Lohkon tunniste 'Viisi vakavinta tapahtumaa viimeisimmän 365 vuorokauden aikana'	`-------►►(365)------`
21.3	Lohkon tunniste 'Vakavin tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui'	`-------►►(10)-------`
21.4	Tietueen tunniste	`--------------------`
	Päivämäärä, aika ja kesto	`►►dd/mm/yyyy hh:mm hhhmm`
	Enimmäisnopeus ja keskimääräinen nopeus, kyseisenä päivänä sattuneiden vastaavien tapahtumien määrä	`xxx km/h xxx km/h(xxx)`
	Kuljettajan sukunimi	`◙ Last_Name_____`
	Kuljettajan etunimi (etunimet)	`First_Name_____`
	Kuljettajakortin tunniste	`Card_Identification_____`
21.5	Jos lohkossa ole yhtään ylinopeutta koskevaa tietuetta	`►►---`
22	***Käsin kirjoitetut tiedot***	
	Lohkon tunniste	`------------------------`
22.1	Tarkastuspaikka	`◘• ..................`
22.2	Tarkastajan allekirjoitus	`◘ ..................`
22.3	Ajasta	`◷+ ..................`
22.4	Aikaan	`+◷ ..................`
22.5	Kuljettajan allekirjoitus	`◙ ..................`

'Käsin kirjoitetut tiedot'; käsin kirjoitettuja tietoja ennen on asetettava riittävä määrä tyhjiä rivejä, jotta tarvittavat tiedot tai allekirjoitus mahtuvat niille varatuille paikoille.

▼B

23 ***Viimeisimmät ajoneuvoyksikköön asetetut kortit***

Lohkon tunniste

23.1 Asetettu kortti

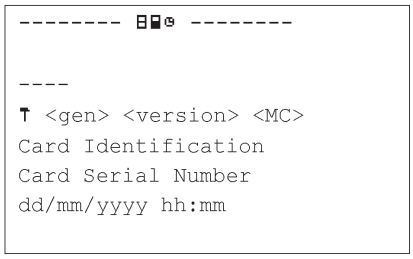
Tietueen tunniste

Korttityyppi, sukupolvi, versio, valmistaja (*)

Kortin tunniste

Card Serial Number

Viimeisimmän kortin asetuksen päivämäärä ja aika



(*) (kaikki yhdelle riville)

jolloin

korttityyppi: kuvake, yksi merkki + välilyönti

gen: GEN1 tai GEN2, 4 merkkiä + välilyönti

versio: korkeintaan 10 merkkiä

MC: valmistajan koodi, 3 merkkiä

3. TULOSTEIDEN ERITTELYT

Tässä luvussa käytetään seuraavia muotoilujen merkintätapoja:

N	Tulostetaan tulostelohko tai tietue numero N
N	Tulostetaan tulostelohko tai tietue numero N niin monta kertaa kuin on tarpeen
X/Y	Tulostetaan tarpeen mukaan lohko tai tietue X ja/tai Y niin monta kertaa kuin on tarpeen.

3.1. **Kortilla olevia kuljettajan toimintaa koskevia tietoja sisältävä päivittäinen tuloste**

PRT_008 Kortilla olevia kuljettajan toimintaa koskevia tietoja sisältävän päivittäisen tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Tarkastajan tunniste (jos ajoneuvoyksikköön on asetettu valvontakortti)
3	Kuljettajan tunniste (kortilta, jota tuloste koskee + GEN)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
5	Ajoneuvoyksikön tunniste (sen ajoneuvoyksikön, jota tuloste koskee + GEN)
6	Kyseisen ajoneuvoyksikön viimeisin kalibrointi
7	Edellinen tarkastustoimi, jonka kohteena nyt tarkastettava kuljettaja on ollut
8	Kuljettajan toimintaa koskevien tietojen erotinmerkki
8a	Out of scope -olosuhteet päivän alussa
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Kuljettajan toimintaa koskevat tiedot esiintymisjärjestyksessä
11	Päivittäisen yhteenvedon erotinmerkki

▼B

11.4	Syötettyjä paikkoja koskevat tiedot aikajärjestyksessä
11.5	GNSS-data
11.6	Toiminnan kokonaiskestoajat
12.1	Kortilta tulostettavien tapahtumia tai vikoja koskevien tietojen erotinmerkki
12.4	Tapahtumia/vikoja koskevat tietueet (viisi viimeistä kortille tallennettua tapahtumaa tai vikaa)
13.1	Ajoneuvoyksikön muistista tulostettavien tapahtumia tai vikoja koskevien tietojen erotinmerkki
13.4	Tapahtumia/vikoja koskevat tietueet (viisi viimeistä ajoneuvoyksikön muistiin tallennettua tai meneillään olevaa tapahtumaa tai vikaa)
22.1	Tarkastuspaikka
22.2	Tarkastajan allekirjoitus
22.5	Kuljettajan allekirjoitus

3.2. **Ajoneuvoyksikön muistissa olevia kuljettajan toimintaa koskevia tietoja sisältävä päivittäinen tuloste**

PRT_009 Ajoneuvoyksikön muistissa olevia kuljettajan toimintaa koskevia tietoja sisältävän päivittäisen tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Kortin haltijan tunnistetiedot (kaikki kortit VU:ssa + GEN)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
5	Ajoneuvoyksikön tunniste (sen ajoneuvoyksikön, jota tuloste koskee + GEN)
6	Kyseisen ajoneuvoyksikön viimeisin kalibrointi
7	Viimeisin kyseiseen ajopiirturiin kohdistunut tarkastus
9	Kuljettajan toimintaa koskevien tietojen erotinmerkki
10	Kuljettajan korttiaukon erotinmerkki (korttiaukko 1)
10a	Out of scope -olosuhteet päivän alussa
10.1 / 10.2 / 10.3 /10.3a / 10.4	Toimintaan liittyvät tiedot aikajärjestyksessä (kuljettajan korttiaukko)
10	Apukuljettajan korttiaukon erotinmerkki (korttiaukko 2)
10a	Out of scope -olosuhteet päivän alussa
10.1 / 10.2 / 10.3 /10.3a / 10.4	Toimintaan liittyvät tiedot aikajärjestyksessä (apukuljettajan korttiaukko)
11	Päivittäisen yhteenvedon erotinmerkki
11.1	Niiden jaksojen yhteenveto, jolloin kuljettajan korttiaukossa ei ollut korttia
11.4	Syötettyjä paikkoja koskevat tiedot aikajärjestyksessä
11.5	GNSS-data

▼B

11.6	Toiminnan kokonaiskestoajat
11.2	Niiden jaksojen yhteenveto, jolloin apukuljettajan korttiaukossa ei ollut korttia
11.4	Syötettyjä paikkoja koskevat tiedot aikajärjestyksessä
11.5	GNSS-data
11.7	Toiminnan kokonaiskestoajat
11.3	Tietyn kuljettajan toimintaa koskevien tietojen yhteenveto molemmat korttipaikat mukaan lukien
11.4	Kyseisen kuljettajan syöttämät paikkoihin liittyvät tiedot aikajärjestyksessä
11.5	GNSS-data
11.8	Kyseisen kuljettajan toiminnan kokonaiskestoajat
13.1	Tapahtumiin/vikoihin liittyvien tietojen erotinmerkki
12.4	Tapahtumia/vikoja koskevat tietueet (viisi viimeistä ajoneuvoyksikön muistiin tallennettua tai meneillään olevaa tapahtumaa tai vikaa)
13.1	Tarkastuspaikka
22.2	Tarkastajan allekirjoitus
22.3	Alkamisaika (tila, johon ilman korttia oleva kuljettaja voi merkitä kyseiset ajat)
22.4	Päättymisaika
22.5	Kuljettajan allekirjoitus

3.3. **Tapahtumat ja viat kortin tietojen mukaan tulostettuna**

PRT_010 Kortilla olevia tapahtumiin ja vikoihin liittyviä tietoja sisältävän tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Tarkastajan tunniste (jos ajoneuvoyksikköön on asetettu valvontakortti + GEN)
3	Kuljettajan tunniste (kortilta, jota tuloste koskee)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
12.2	Tapahtumiin liittyvien tietojen erotinmerkki
12.4	Tapahtumiin liittyvät tietueet (kaikki kortille tallennetut tapahtumat)
12.3	Vikoihin liittyvien tietojen erotinmerkki
12.4	Vikoihin liittyvät tietueet (kaikki kortille tallennetut viat)
22.1	Tarkastuspaikka
22.2	Tarkastajan allekirjoitus
22.5	Kuljettajan allekirjoitus

▼B

3.4. **Ajoneuvoyksikön (VU) muistissa olevia tapahtumiin ja vikoihin liittyviä tietoja sisältävä tuloste**

PRT_011 Ajoneuvoyksikön muistissa olevia tapahtumiin ja vikoihin liittyviä tietoja sisältävän tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Kortin haltijan tunnistetiedot (kaikki kortit VU:ssa + GEN)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
13.2	Tapahtumiin liittyvien tietojen erotinmerkki
13.4	Tapahtumiin liittyvät tietueet (kaikki ajoneuvoyksikön muistiin tallennetut tai meneillään olevat tapahtumat)
13.3	Vikoihin liittyvien tietojen erotinmerkki
13.4	Vikoihin liittyvät tietueet (kaikki ajoneuvoyksikön muistiin tallennetut tai meneillään olevat viat)
22.1	Tarkastuspaikka
22.2	Tarkastajan allekirjoitus
22.5	Kuljettajan allekirjoitus

3.5. **Teknisten tietojen tuloste**

PRT_012 Teknisten tietojen tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Kortin haltijan tunnistetiedot (kaikki kortit VU:ssa + GEN)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
14	Ajoneuvoyksikön tunniste
15	Liiketunnistimen tunniste
15,1	Tunnistimen liittämistiedot (kaikki saatavilla olevat tiedot aikajärjestyksessä)
16	GNSS-tunniste
16,1	Ulkoisen GNSS-laitteiston kytkemistiedot (kaikki saatavilla olevat tiedot aikajärjestyksessä)
17	Kalibrointiin liittyvien tietueiden erotinmerkki
17.1	Kalibrointeihin liittyvät tietueet (kaikki käytettävissä olevat tietueet aikajärjestyksessä)
18	Ajan asetuksen erotinmerkki
18.1	Ajan asetukseen liittyvät tietueet (kaikki käytettävissä olevat ajan asetukseen liittyvissä ja kalibrointitiedoissa olevat tietueet)
19	Viimeisin ajoneuvoyksikön muistiin tallennettu tapahtuma ja vika

▼B

3.6. **Ylinopeustuloste**

PRT_013 Ylinopeustulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Kortin haltijan tunnistetiedot (kaikki kortit VU:ssa + GEN)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
20	Ylinopeusvalvontaan liittyvät tiedot
21.1	Ylinopeuteen liittyvien tietojen tunniste
21.4 / 21.5	Ensimmäinen ylinopeustapaus viimeisimmän kalibroinnin jälkeen
21.2	Ylinopeuteen liittyvien tietojen tunniste
21.4 / 21.5	Viisi vakavinta ylinopeustapausta 365 viimeisimmän vuorokauden aikana
21.3	Ylinopeuteen liittyvien tietojen tunniste
21.4 / 21.5	Vakavin ylinopeustapaus kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui
22.1	Tarkastuspaikka
22.2	Tarkastajan allekirjoitus
22.5	Kuljettajan allekirjoitus

3.7. **Asetettujen korttien historia**

PRT_014 Asetettujen korttien historiaa koskevan tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Kortin haltijan tunnistetiedot (kaikki kortitVU:ssa)
23	Viimeisin ajoneuvoyksikköön asetettu kortti
23.1	Asetetut kortit (korkeintaan 88 tietuetta)
12.3	Vikoihin liittyvien tietojen erotinmerkki

▼B

Lisäys 5

NÄYTTÖ

Tässä lisäyksessä käytetään seuraavia merkintätapoja:

— **lihavoitu** teksti merkitsee tavallista tekstiä, joka näytetään (näytössä ei käytetä lihavoitua tekstiä),

— normaali teksti merkitsee muuttujia (kuvakkeita tai dataa), jotka tulostettaessa korvataan vastaavilla muuttujan arvoilla:

  — dd mm yyyy: päivä, kuukausi, vuosi

  — hh: tunnit

  — mm: minuutit

  — D: kestoaikaa merkitsevä kuvake

  — EF: tapahtumaa tai vikaa merkitsevien kuvakkeiden yhdistelmä

  — O: toimintatapaa merkitsevä kuvake.

DIS_001 Ajopiirturinn on näytettävä tiedot seuraavassa muodossa:

Tiedot	Muoto
Oletusarvoinen näyttö	
Paikallinen aika	hh:mm
Toimintatila	O
Kuljettajaan liittyvät tiedot	1 Dhh**h**mm ▮▮hh**h**mm
Apukuljettajaan liittyvät tiedot	2 Dhh**h**mm
Asetuksen piiriin kuulumaton olosuhde voimassa	OUT
Varoitusnäyttö	
Keskeytymätön ajoaika yli sallitun	1 ⊙hh**h**mm ▮▮hh**h**mm
Tapahtuma tai vika	EF
Muut näytöt	
UTC-päivämäärä aika	UTC ⊙ dd/mm/yyyy tai UTC ⊙ dd.mm.yyyy hh:mm
Kuljettajan keskeytymätön ajoaika ja yhteenlaskettu taukoaika	1 ⊙hh**h**mm ▮▮hh**h**mm
Apukuljettajan keskeytymätön ajoaika ja yhteenlaskettu taukoaika	2 ⊙hh**h**mm ▮▮hh**h**mm
Kuljettajan yhteenlaskettu ajoaika edellisen ja kuluvan viikon aikana	1 ⊙▮▮ hhh**h**mm
Apukuljettajan yhteenlaskettu ajoaika edellisen ja kuluvan viikon aikana	2 ⊙▮▮ hhh**h**mm

▼B

Lisäys 6

ETULEVYSSÄ OLEVA KALIBROINTI-/KOPIOINTILIITIN

SISÄLLYSLUETTELO

1. LAITTEET

1.1. Liitin

1.2. Liittimen johdotus

1.3. Lohkokaavio

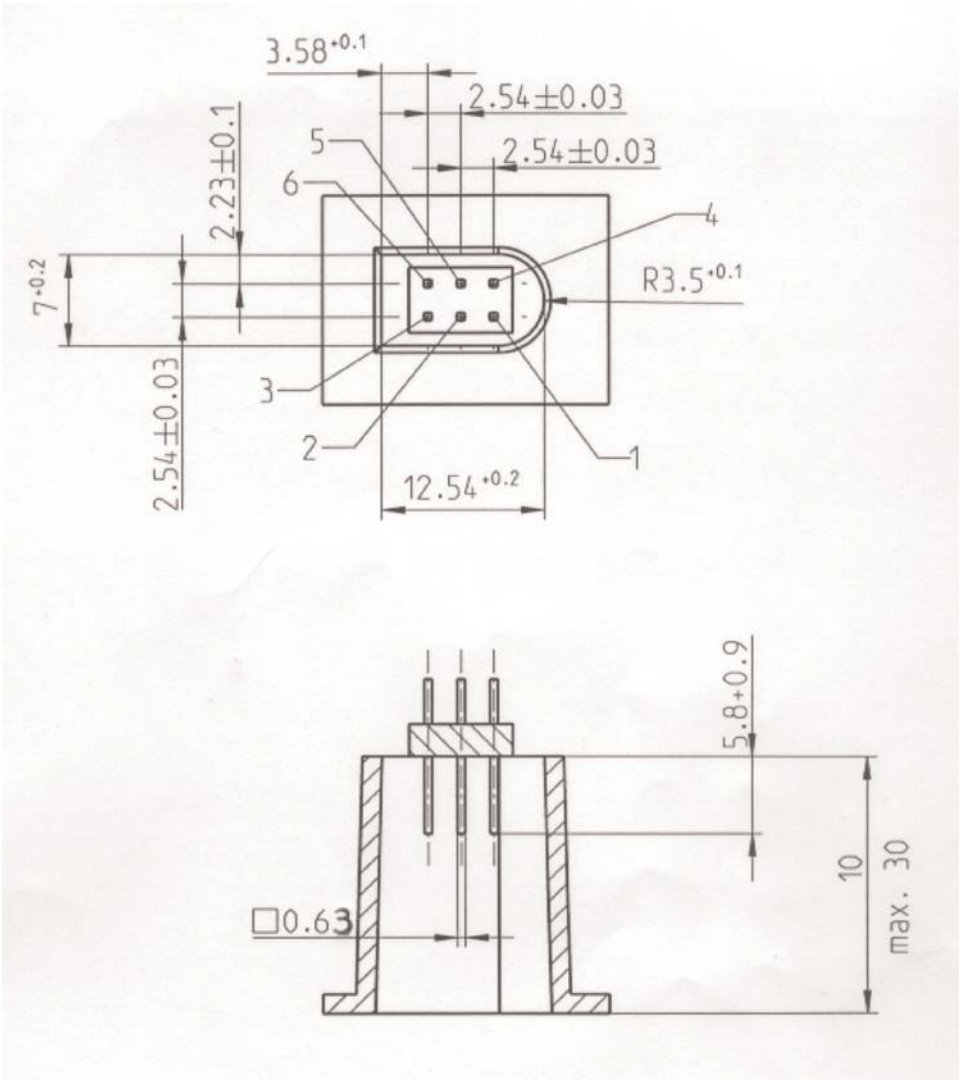
2. TIETOJEN KOPIOINNISSA KÄYTETTÄVÄ LIITÄNTÄ-LAITE

3. KALIBROINNISSA KÄYTETTÄVÄ LIITÄNTÄLAITE

1. LAITTEET

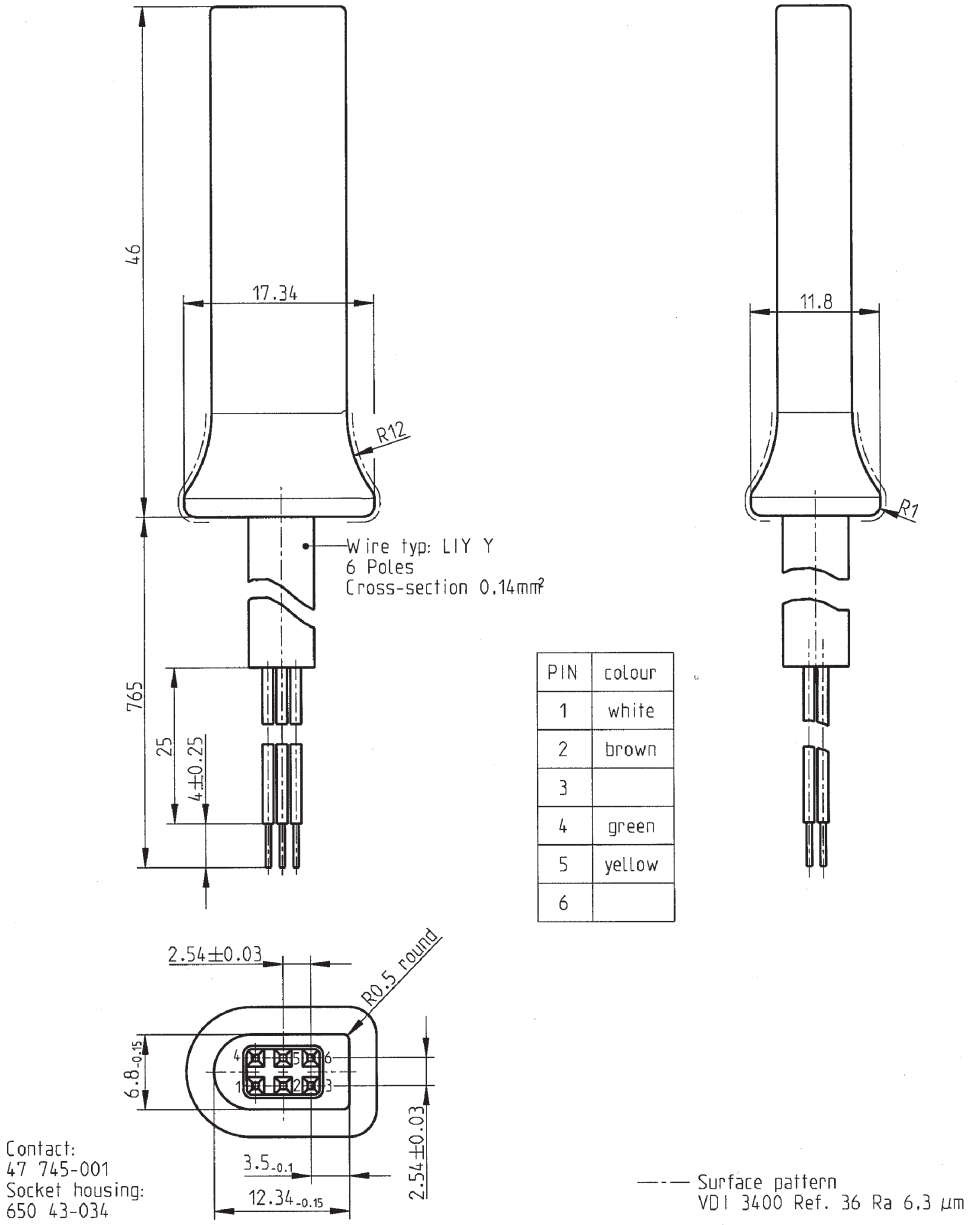
1.1. **Liitin**

INT_001 Tietojen kopiointiin ja kalibrointiin käytettävän liittimen on oltava kuusinapainen ja sen on oltava käsillä laitteen etulevyssä ilman, että on tarpeen irrottaa mitään ajopiirturin osaa. Liittimen on oltava seuraavan piirroksen mukainen (kaikki mitat millimetreinä):



▼B

Seuraavassa kuvassa on tyypillinen kuusinapainen liitinpistoke:



1.2. **Liittimen johdotus**

INT_002 Liitin on johdotettava seuraavan taulukon mukaisesti:

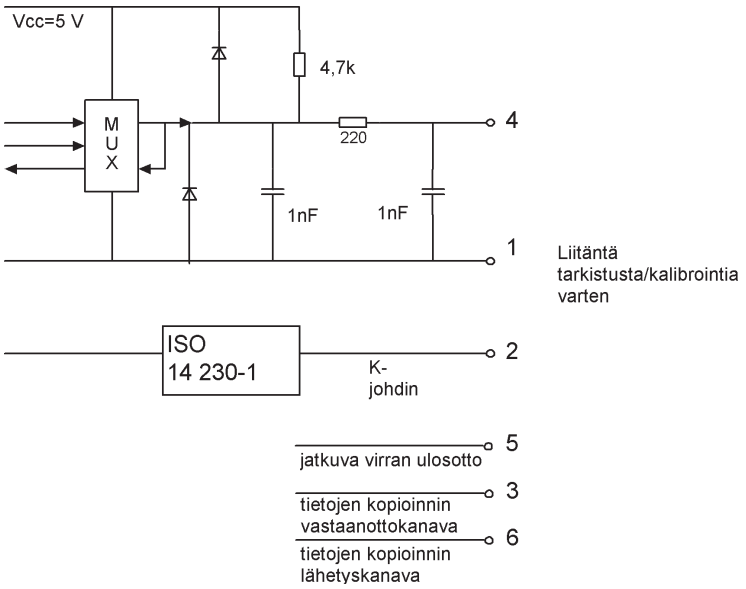
Napa	Kuvaus	Huomautus
1	Akun miinusnapa	Yhdistetty ajoneuvon akun miinusnapaan
2	Dataliikenne	K-johdin (standardin ISO 14230-1 mukainen)
3	RxD – Tietojen kopioinnissa käytettävä vastaanottonapa	Datan tulosignaali ajopiirturiin
4	Tulo-/lähtösignaali	Kalibrointiin

▼B

Napa	Kuvaus	Huomautus
5	Jatkuva virran ulosotto	Laitteen suojapiirien synnyttämän jännitehäviön vuoksi jännite on määritelty olemaan 3 V vähemmän kuin ajoneuvossa käytettävä jännite Virran ulosotto enintään 40 mA
6	TxD – Tietojen kopioinnissa käytettävä lähetysnapa	Datan lähtösignaali ajopiirturista

1.3. **Lohkokaavio**

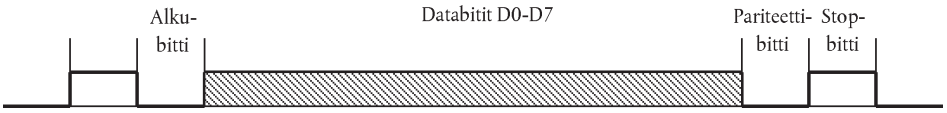
INT_003 Lohkokaavion on oltava seuraavan kuvan mukainen:



2. TIETOJEN KOPIOINNISSA KÄYTETTÄVÄ LIITÄNTÄLAITE

INT_004 Tietojen kopioinnissa käytettävän liitäntälaitteen on oltava standardin RS232 erittelyjen mukainen.

INT_005 Tietojen kopioinnissa käytettävän liitäntälaitteen on käytettävä yhtä alkubittiä, kahdeksaa databittiä vähiten merkitsevä bitti ensimmäisenä, yhtä pariteettibittiä ja yhtä stop-bittiä.



Datatavujen rakenne

Alkubitti: yksi bitti, jonka looginen taso on 0;

Databitit: lähetetään vähiten merkitsevä bitti ensimmäisenä;

Pariteettibitti: parillinen

Stop-bitti: yksi bitti, jonka looginen taso on 1

Lähetettäessä numeerista dataa, joka koostuu useammasta kuin yhdestä tavusta, lähetetään merkitsevin tavu ensimmäisenä ja vähiten merkitsevä tavu viimeisenä.

INT_006 Datansiirtonopeuden on oltava aseteltavissa välillä 9 600 bps–115 200 bps. Datansiirto on suoritettava suurimmalla mahdollisella nopeudella, mutta aloitusnopeus yhteyden syntyessä on asetettu arvoon 9 600 bps.

▼B

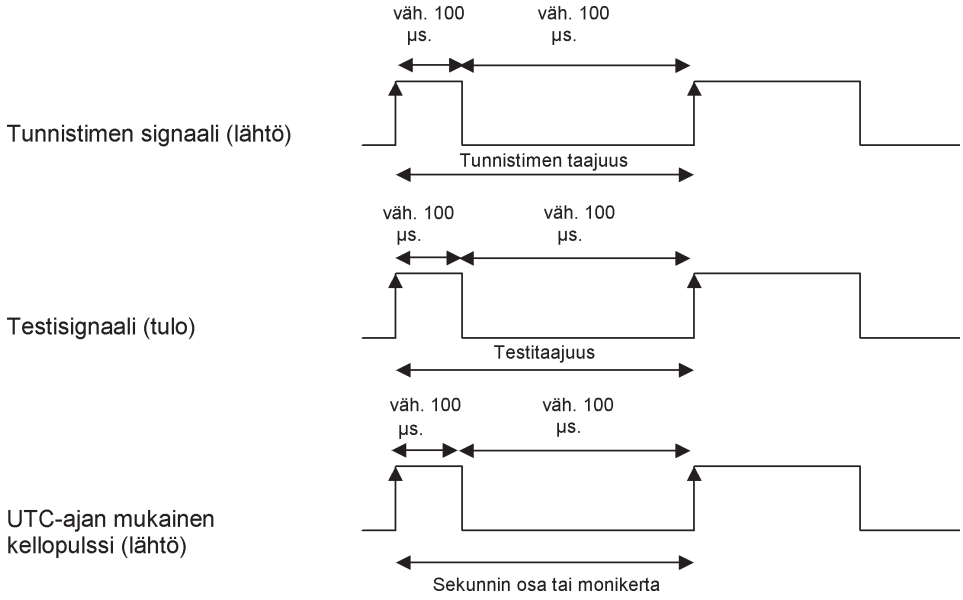
3. KALIBROINNISSA KÄYTETTÄVÄ LIITÄNTÄLAITE

INT_007 Tiedonsiirron on tapahduttava seuraavan standardin mukaisesti: ISO 14230-1 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 1: Physical layer, First edition: 1999 (Tieliikenteessä käytettävät ajoneuvot. Diagnostiikkajärjestelmät. Avainsanaprotokolla 2000. Osa 1: Fyysinen kerros. Ensimmäinen painos: 1999).

INT_008 Tulo-/lähtösignaalin on oltava seuraavan sähköisen erittelyn mukainen:

Parametri	Vähimmäisarvo	Tyypillinen arvo	Enimmäisarvo	Huomautus
U_{low} (tulo)			1,0 V	I = 750 µA
U_{high} (tulo)	4 V			I = 200 µA
Taajuus			4 kHz	
U_{low} (lähtö)			1,0 V	I = 1 mA
U_{high} (lähtö)	4 V			I = 1 mA

INT_009 Tulo-/lähtösignaalin on oltava seuraavien ajoituskaavioiden mukainen:



▼B

Lisäys 7

TIETOJEN KOPIOINTIPROTOKOLLAT

SISÄLLYSLUETTELO

1. JOHDANTO

1.1. Soveltamisala

1.2. Lyhenteet ja merkinnät

2. AJONEUVOYKSIKÖSSÄ OLEVIEN TIETOJEN KOPIOINTI

2.1. Tietojen kopiointimenettely

2.2. Tietojen kopiointiprotokolla

2.2.1 Viestin rakenne

2.2.2 Viestityypit

2.2.2.1 Start Communication Request (SID 81)

2.2.2.2 Positive Response Start Communication (SID C1)

2.2.2.3 Start Diagnostic Session Request (SID 10)

2.2.2.4 Positive Response Start Diagnostic (SID 50)

2.2.2.5 Link Control Service (SID 87)

2.2.2.6 Link Control Positive Response (SID C7)

2.2.2.7 Request Upload (SID 35)

2.2.2.8 Positive Response Request Upload (SID 75)

2.2.2.9 Transfer Data Request (SID 36)

2.2.2.10 Positive Response Transfer Data (SID 76)

2.2.2.11 Request Transfer Exit (SID 37)

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

2.2.2.13 Stop Communication Request (SID 82)

2.2.2.14 Positive Response Stop Communication (SID C2)

2.2.2.15 Acknowledge Sub Message (SID 83)

2.2.2.16 Negative Response (SID 7F)

2.2.3 Viestien kulku

2.2.4 Ajoitus

▼B

2.2.5 Virheenkäsittely

2.2.5.1 Start Communication phase

2.2.5.2 Communication phase

2.2.6 Vastausviestien sisältö

2.2.6.1 Positive Response Transfer Data Overview

2.2.6.2 Positive Response Transfer Data Activities

2.2.6.3 Positive Response Transfer Data Events and Faults

2.2.6.4 Positive Response Transfer Data Detailed Speed

2.2.6.5 Positive Response Transfer Data Technical Data

2.3. Tiedostojen tallennus ulkoisille tietovälineille (ESM)

3. AJOPIIRTURIKORTILLA OLEVIEN TIETOJEN KOPIOINTIPROTOKOLLA

3.1. Soveltamisala

3.2. Määritelmät

3.3. Kortilla olevien tietojen kopiointi

3.3.1 Kopioinnin aloittava komentosarja

3.3.2 Komentosarja tiedostoille, joilla ei ole allekirjoitusta

3.3.3 Komentosarja tiedostoille, joilla on allekirjoitus

3.3.4 Komentosarja, jolla kalibrointilaskuri asetetaan alkutilaansa

3.4. Tiedontallennuksen muoto

3.4.1 Johdanto

3.4.2 Tiedostomuoto

4. AJOPIIRTURIKORTILLA OLEVIEN TIETOJEN KOPIOINTI AJONEUVOYKSIKÖN KAUTTA

1. JOHDANTO

Tässä lisäyksessä määritellään menettelyt, joiden avulla tietoja kopioidaan eri tavoin ulkoisille tietovälineille, sekä menettelyt, joiden avulla varmistetaan virheetön tiedonsiirto ja kopioitujen tietojen muodon täysi yhteensopivuus, jotta kuka hyvänsä tarkastaja voi tarkastaa tiedot sekä varmistua niiden aitoudesta ja eheydestä ennen niiden analysointia.

1.1. **Soveltamisala**

Tietoja voidaan kopioida ulkoiselle tietovälineelle

— ajoneuvoyksiköstä siihen kytketyn IDE-laitteen avulla

— ajopiirturikortilta sellaisen IDE-laitteen avulla, johon on kytketty korttiliitäntälaite

▼B

— ajopiirturikortilta ajoneuvoyksikköön kytketyn IDE-laitteen avulla.

Jotta olisi mahdollista tarkastaa ulkoiselle tietovälineelle tallennettujen kopioitujen tietojen aitous ja eheys, tiedot kopioidaan liittämällä niihin lisäyksen 11 (Yhteiset turvamekanismit) mukainen allekirjoitus. Lähdelaitteen (ajoneuvoyksikön tai kortin) tunniste ja sen tietoturvavarmenteet (jäsenvaltion ja laitteen) kopioidaan myös. Tietojen varmentajalla on erikseen oltava hallussaan luotettava julkinen eurooppalainen avain.

DDP_001 Yhden kopiointikerran aikana kopioidut tiedot on tallennettava ulkoiselle tietovälineelle yhteen tiedostoon.

1.2. **Lyhenteet ja merkinnät**

Tässä lisäyksessä käytetään seuraavia lyhenteitä:

AID (Application Identifier) Sovellustunniste

ATR (Answer To Reset) Signaali, joka annetaan vastauksena RST-komentoon

CS (Checksum byte) Tarkistussummatavu

DF (Dedicated File) Hakemistotiedosto

DS_ (Diagnostic Session) Diagnostinen jakso

EF (Elementary File) EF-tiedosto

ESM (External Storage Medium) Ulkoinen tietoväline

FID (File Identifier) Tiedostotunniste

FMT (Format Byte) Muotoilutavu (viestin ylätunnisteen ensimmäinen tavu)

ICC (Integrated Circuit Card) Integroidulla piirillä varustettu kortti

IDE (Intelligent Dedicated Equipment)Tietojen kopioimiseen ulkoisille tietovälineille tarkoitettu älykäs laite, (IDE-laite) (laite, jonka avulla tietoja kopioidaan ulkoisille tietovälineille, esim. PC)

IFD (Interface Device) Liitäntälaite

KWP (Keyword Protocol 2000) Avainsanaprotokolla 2000

LEN (Length Byte) Pituustavu(viestin ylätunnisteen viimeinen tavu))

PPS (Protocol Parameter Selection) Protokollan parametrin valinta

PSO (Perform Security Operation) Suorita turvatoimi

SID (Service Identifier) Palvelun tunniste

SRC (Source byte) Lähdetavu

TGT (Target Byte) Kohdetavu

TLV (Tag Length Value) Tuntomerkki-pituus-sisältö-koodaustapa

TREP (Transfer Response Parameter) Lähetyspyyntöä koskevan vastauksen parametri

TRTP (Transfer Request Parameter) Lähetyspyynnön parametri

VU (Vehicle Unit) Ajoneuvoyksikkö

▼B

2. AJONEUVOYKSIKÖSSÄ OLEVIEN TIETOJEN KOPIOINTI

2.1. **Tietojen kopiointimenettely**

Tiedot kopioidaan ajoneuvoyksiköstä seuraavasti:

— ajopiirturikortti asetetaan ajoneuvoyksikön korttiaukkoon (*);

— IDE-laite yhdistetään ajoneuvoyksikön kopiointiliittimeen;

— luodaan yhteys IDE-laitteen ja ajoneuvoyksikön välille;

— valitaan IDE-laitteen avulla kopioitavat tiedot ja lähetetään niitä koskeva pyyntö ajoneuvoyksikölle;

— lopetetaan kopiointijakso.

2.2. **Tietojen kopiointiprotokolla**

Protokolla rakentuu isäntä-renki-periaatteelle siten, että IDE-laite on isäntä ja ajoneuvoyksikkö on renki.

Viestien rakenne, tyypit ja virta perustuvat periaatteessa Avainsanaprotokolla 2000:een (ISO 14230-2 Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 2: Data Link Layer).

Sovelluskerros perustuu pääpiirteissään tämänhetkiseen 22. helmikuuta 2001 hyväksyttyyn versioon 6 standardista ISO 14229-1 (Road vehicles – Diagnostic systems – Part 1: Diagnostic services).

2.2.1 *Viestin rakenne*

DDP_002 Kaikkien IDE-laitteen ja ajoneuvoyksikön välillä kulkevien viestien muoto perustuu rakenteeseen, jossa on kolme osaa:

— ylätunniste, jossa on muotoilutavu (FMT), kohdetavu (TGT), lähdetavu (SRC) sekä mahdollisesti pituustavu (LEN),

— datakenttä, jossa on palvelun tunnistetavu (SID) sekä vaihteleva määrä datatavuja, joihin voi sisältyä valinnainen diagnostiikkajakson osoitustavu (DS_) tai valinnainen lähetysparametritavu (TRTP tai TREP),

— tarkistussummatavun (CS) sisältämä tarkistussumma.

Ylätunniste				Datakenttä					Tarkistussumma
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 tavua				Enintään 255 tavua					1 tavu

TGT- ja SRC-tavu edustavat viestin vastaanottajan ja lähettäjän fyysisiä osoitteita. Heksadesimaalilukuina niiden arvot ovat F0h IDE-laitteelle ja EEh ajoneuvoyksikölle.

LEN-tavu on datakenttäosan pituus.

Tarkistussummatavu on kaikkien viestin sisältämien tavujen, paitsi itse CS-tavun, kahdeksan bitin ryhmissä laskettu summa modulo 256.

FMT-, SID-, DS_-, TRTP- ja TREP-tavut on määritelty jäljempänä tässä asiakirjassa.

(*) Kopiointia ja kopioitavia tietoja koskevat käyttöoikeudet määräytyvät korttiaukkoon asetetun kortin mukaan. Tietoja on kuitenkin voitava kopioida yhteen ajoneuvoyksikön korttiaukkoon asetetulta kuljettajakortilta, kun toiseen korttiaukkoon ei ole asetettu mitään muuta korttityyppiä.

▼B

DDP_003 Jos viestin sisältämän datan pituus ylittää datakentässä käytettävissä olevan tilan, lähetetään viesti useampina osaviesteinä. Jokaisella osaviestillä on ylätunniste, sama SID, TREP sekä kaksitavuinen osaviestilaskuri, joka osoittaa osaviestin järjestysnumeron kokonaisviestissä. Jotta virhetarkistus- ja viestin keskeyttämistoiminnot olisivat mahdollisia, IDE-laite kuittaa jokaisen osaviestin. IDE-laite voi joko hyväksyä kyseisen osaviestin, pyytää sen lähettämistä uudelleen, pyytää ajoneuvoyksikköä aloittamaan koko viestin uudelleen tai keskeyttää viestin lähetyksen kokonaan.

DDP_004 Jos viimeisen osaviestin datakentässä on täsmälleen 255 tavua, on kokonaisviestiin lisättävä vielä (SID-, TREP- ja osaviestilaskuritavuja lukuun ottamatta) tyhjä datakenttä osoittamaan viestin loppua.

Esimerkki:

Ylätunniste	SID	TREP	Viesti	CS
4 tavua	Enemmän kuin 255 tavua			

Lähetetään muodossa:

Ylätunniste	SID	TREP	00	01	Osaviesti 1	CS
4 tavua	255 tavua					

Ylätunniste	SID	TREP	00	02	Osaviesti 2	CS
4 tavua	255 tavua					

…

Ylätunniste	SID	TREP	xx	yy	Osaviesti n	CS
4 tavua	Enemmän kuin 255 tavua					

tai muodossa:

Ylätunniste	SID	TREP	00	01	Osaviesti 1	CS
4 tavua	255 tavua					

Ylätunniste	SID	TREP	00	02	Osaviesti 2	CS
4 tavua	255 tavua					

…

Ylätunniste	SID	TREP	xx	yy	Osaviesti n	CS
4 tavua	255 tavua					

Ylätunniste	SID	TREP	xx	yy + 1	CS
4 tavua	4 tavua				

▼B

2.2.2 *Viestityypit*

Tietojen kopioimiseen ajoneuvoyksikön ja IDE-laitteen välillä käytettävä viestintäprotokolla vaatii kahdeksan erilaisen viestityypin käyttöä.

Seuraavassa taulukossa on näiden viestityyppien yhteenveto.

Viestin rakenne	Max 4 Bytes Header				Max 255 Bytes Data			1 Byte Check-Sum
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (stage 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00,00,00,-FF,FF,FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06	Slot	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6

▼B

Viestin rakenne	Max 4 Bytes Header				Max 255 Bytes Data			1 Byte Check-Sum
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Huomautuksia:

— Sid Req = vastaavan pyynnön SID.

— TREP = vastaavan pyynnön TRTP.

— Musta ruutu tarkoittaa, että mitään ei lähetetä.

— Sanaa upload (IDE-laitteen kannalta) on käytetty ISO 14229 -standardin mukaan. Se tarkoittaa samaa kuin download (tietojen kopiointi) (ajoneuvoyksikön kannalta).

— Mahdolliset kaksitavuiset osaviestilaskurit eivät näy tässä taulukossa.

— Korttiaukko on korttiaukon numero, joko ”1” (kortti kuljettajan korttiaukossa) tai ”2” (kortti apukuljettajan korttiaukossa).

— Jos korttiaukkoa ei ole määritelty, ajoneuvoyksikkö valitsee korttiaukon 1, jos siinä on kortti, ja se valitsee korttiaukon 2 vain, jos käyttäjä on erityisesti valinnut sen.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 IDE-laite aloittaa viestintäyhteyden luomisen ajoneuvoyksikön kanssa lähettämällä tämän viestin. Alkuvaiheen viestintä tapahtuu aina 9 600 baudin nopeudella (kunnes nopeutta muutetaan tarvittavan yhteyskäytäntöpalvelun avulla).

▼B

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Ajoneuvoyksikkö vastaa tällä viestillä myönteisesti viestinnän aloitusta koskevaan pyyntöön. Viestiin sisältyvät tavut ‘EA’ ja ‘8F’, jotka osoittavat, että ajoneuvoyksikkö tukee protokollaa, jossa on kohde-, lähde- ja pituustiedot sisältävä ylätunniste.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 IDE-laite pyytää ajoneuvoyksiköltä uutta diagnostista jaksoa lähettämällä diagnostisen jakson aloitusta koskevan pyynnön. Alitoiminto ”default session” (81h) osoittaa, että avattava jakso vastaa oletusarvoa.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 Ajoneuvoyksikkö vastaa myöntävästi diagnostisen jakson aloitusta koskevaan pyyntöön lähettämällä myönteisen vastauksen.

2.2.2.5 Link Control Service (SID 87)

DDP_052 IDE-laite aloittaa lähetysnopeuden muuttamisen yhteyskäytäntöpalvelulla. Tämä tapahtuu kaksivaiheisesti. Ensimmäisessä vaiheessa IDE ehdottaa nopeuden muuttamista ja uutta nopeutta. Saatuaan ajoneuvoyksiköltä myönteisen vastauksen IDE lähettää ajoneuvoyksikölle vahvistuksen nopeuden muutoksesta (toinen vaihe). Tämän jälkeen IDE siirtyy käyttämään uutta nopeutta. Ajoneuvoyksikkö siirtyy käyttämään uutta nopeutta saatuaan vahvistuksen.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 Ajoneuvoyksikkö vastaa yhteyskäytäntöpalvelua koskevaan pyyntöön myönteisesti lähettämällä yhteyskäytännön myönteisen vastauksen (ensimmäinen vaihe). Vahvistusviestiin (toisessa vaiheessa) ei lähetetä vastausta.

2.2.2.7 Request Upload (SID 35)

DDP_009 IDE-laite kertoo lähetyspyyntöviestillä ajoneuvoyksikölle, että tietoja halutaan kopioida. ISO14229-standardin mukaisesti viesti sisältää tiedot pyydetyn datan osoitteesta, koosta ja formaatista. Koska nämä eivät ole IDE-laitteen tiedossa ennen kopiointia, muistiosoitteeksi asetetaan 0, formaatti ilmoitetaan salaamattomaksi ja tiivistämättömäksi ja muistikoko asetetaan mahdollisimman suureksi.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 Ajoneuvoyksikkö kertoo IDE-laitteelle lähetyspyynnön myönteisellä vastauksella, että se on valmis kopioimaan tietoja. ISO14229-standardin mukaisesti tämä myönteinen vastausviesti sisältää IDE-laitteelle tiedon siitä, että tulevat lähetyspyynnön myönteiset vastausviestit sisältävät enintään 00FFh tavua.

▼B

2.2.2.9 Transfer Data Request (SID 36)

DDP_011 IDE-laite määrittää ajoneuvoyksikölle tiedonsiirtopyynnöllä, minkä tyyppisiä tietoja on tarkoitus kopioida. Yhden tavun TRTP-parametri (Transfer Request Parameter) ilmoittaa siirron tyypin.

Tiedonsiirtoja on kuudentyyppisiä:

— Overview (TRTP 01),

— Activities of a specified date (TRTP 02),

— Events and faults (TRTP 03),

— Detailed speed (TRTP 04),

— Technical data (TRTP 05),

— Card download (TRTP 06).

DDP_054 IDE-laitteen on pyydettävä yleiskatsausta (TRTP 01) kopiointitilanteessa, koska ainoastaan näin voidaan varmistaa, että ajoneuvoyksikön varmenteet tallentuvat kopioitavaan tiedostoon (ja digitaalinen allekirjoitus voidaan todentaa).

Toisessa tyypissä (TRTP 02) tiedonsiirtopyyntöä koskevaan viestiin sisältyy (`TimeReal`-muodossa oleva) tieto siitä kalenterivuorokaudesta, jota koskevat tiedot on tarkoitus kopioida.

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 Ajoneuvoyksikkö vastaa tiedonsiirtopyyntöön lähettämällä tiedonsiirtopyynnön myönteisen vastauksen. Viesti sisältää pyydetyt tiedot ja TREP-parametrin (Transfer Response Parameter), joka vastaa pyynnön TRTP-parametria.

DDP_055 Ensimmäisessä tyypissä (TREP01) ajoneuvoyksikkö lähettää tietoja, jotka auttavat IDE-laitteen käyttäjää valitsemaan ne tiedot, jotka hän haluaa kopioida. Tähän viestiin sisältyvät seuraavat tiedot:

— tietoturvavarmenteet,

— ajoneuvon tunnistetiedot

— ajoneuvoyksikön kuluva päivämäärä ja aika

— ensimmäinen ja viimeinen päivämäärä, joita koskevat (ajoneuvoyksikön sisältämät) tiedot ovat kopioitavissa,

— tieto ajoneuvoyksikössä olevista korteista,

— edellinen yrityksen tekemä tietojen kopiointi,

— yrityksen asettamat lukitukset,

— aiemmat tarkastukset.

▼B

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 IDE-laite kertoo ajoneuvoyksikölle siirron lopetusta koskevalla pyynnöllä, että tietojen kopiointi on päättynyt.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 Ajoneuvoyksikkö kuittaa siirron lopetusta koskevan pyynnön lähettämällä myönteisen vastauksen.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 IDE-laite katkaisee viestintäyhteyden ajoneuvoyksikön kanssa lähettämällä viestin lopetusta koskevan pyynnön.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 Ajoneuvoyksikkö kuittaa viestinnän lopetusta koskevan pyynnön lähettämällä myönteisen vastauksen viestinnän lopetukseen.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 IDE-laite vahvistaa kunkin useassa osassa lähetettävän viestin osaviestin vastaanottamisen lähettämällä osaviestin kuittaus -viestin. Datakenttä sisältää ajoneuvoyksiköltä saadun SID-tunnisteen ja kaksitavuisen koodin seuraavasti:

— MsgC +1 kuittaa osaviestin numero MsgC virheettömän vastaanottamisen.

IDE-laite pyytää ajoneuvoyksikköä lähettämään seuraavan osaviestin.

— MsgC osoittaa, että osaviestin numero MsgC vastaanottamisessa ilmeni ongelma.

IDE-laite pyytää ajoneuvoyksikköä lähettämään osaviestin uudelleen.

— FFFF pyytää lopettamaan viestin lähetyksen.

IDE-laite voi käyttää tätä koodia lopettamaan ajoneuvoyksikön viestin lähetyksen mistä hyvänsä syystä.

Viestin viimeinen osaviesti (LEN-tavu < 255) voidaan kuitata millä hyvänsä näistä koodeista tai jättää kuittaamatta.

Ajoneuvoyksikön vastaukset tapauksissa, joissa viesti koostuu useista osaviesteistä, ovat:

— Positive Response Transfer Data (SID 76)

▼B

2.2.2.16 Negative Response (SID 7F)

DDP_018 Jos ajoneuvoyksikkö ei voi täyttää edellä selostetuilla viesteillä esitettyä pyyntöä, se vastaa kielteinen vastaus -viestillä. Viestin datakenttä sisältää vastauksen SID-tunnisteen (7F), pyynnön SID-tunnisteen sekä koodin, joka ilmaisee kieltävän vastauksen syyn. Käytettävissä on seuraavat koodit:

— 10 yleinen hylkäys

Toimintoa ei voida suorittaa muiden kuin jäljempänä selostettujen syiden vuoksi.

— 11 palvelua ei tueta

Pyynnön SID-tunnistetta ei tunnistettu.

— 12 osatoimintoa ei tueta

Pyynnön DS_- tai TRTP-tunnistetta ei tunnistettu tai lähetettäviä osaviestejä ei enää ole.

— 13 väärä viestin pituus

Vastaanotettu viestin on väärän mittainen.

— 22 väärät ehdot tai virhe pyynnön rakenteessa

Pyydetty palvelu ei ole toimintavalmiudessa tai pyynnön esittäneen viestin osien järjestys on väärä.

— 31 pyyntö alueen ulkopuolella

Pyynnön parametritietue (datakenttä) ei oikeanlainen.

— 50 lähetystä ei hyväksytty

Pyyntöä ei voida noudattaa (ajoneuvoyksikkö on väärässä toimintatilassa tai yksikössä on sisäinen vika).

— 78 vastausta odotetaan

Pyydettyä toimintoa ei ehditä suorittaa ajoissa, eikä ajoneuvoyksikkö ole valmis vastaanottamaan uutta pyyntöä.

— FA tietoja ei saatavilla

Tiedon siirtopyynnön kohteena olevat tiedot eivät ole käytettävissä ajoneuvoyksikössä (esim. yksikköön ei ole asetettu korttia, …).

2.2.3 *Viestien kulku*

Tyypillinen viestien kulku normaalin tietojen kopiointitapahtuman aikana on seuraavanlainen:

IDE		VU
Start Communication Request	⇨ ⇦	Positive Response
Start Diagnostic Service Request	⇨ ⇦	Positive Response
Request Upload	⇨ ⇦	Positive Response

▼B

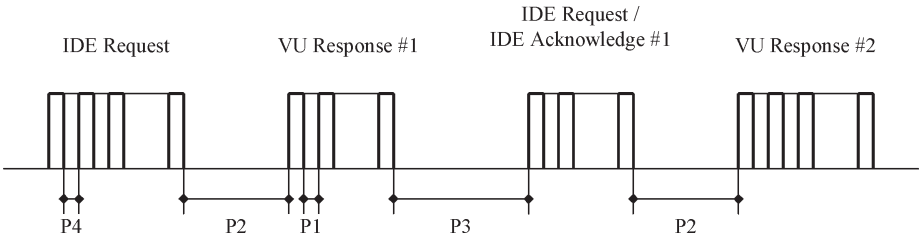
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field<255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Ajoitus*

DDP_019 Normaalikäytön aikana seuraavassa kuvassa näkyvät ajoitusparametrit ovat oleellisia:

Kuva 1

Viestien kulku, ajoitus



Missä:

P1 = Tavujen välinen aika ajoneuvoyksikön vastauksessa.

P2 = Aika IDE-laitteen pyynnön lopusta ajoneuvoyksikön vastauksen alkuun tai aika IDE-laitteen kuittauksen lopusta ajoneuvoyksikön seuraavan vastauksen alkuun.

P3 = Aika ajoneuvoyksikön vastauksen lopusta IDE-laitteen seuraavan pyynnön alkuun tai aika ajoneuvoyksikön vastauksen lopusta IDE-laitteen kuittauksen alkuun tai aika IDE-laitteen pyynnön lopusta IDE-laitteen seuraavan pyynnön alkuun tapauksissa, jolloin ajoneuvoyksikkö ei vastaa.

P4 = Tavujen välinen aika IDE-laitteen pyynnöissä.

P5 = Ajan P3 pidennetty arvo kortilta kopiointia varten.

▼B

Ajoitusparametrien sallitut arvot on esitetty seuraavassa taulukossa (KWP-avainsanaprotokollan laajennettu ajoitusparametriluettelo, jota käytetään fyysisessä osoitteistamisessa viestintänopeuden kohottamiseksi).

Ajoitusparametri	Alaraja Arvo (ms)	Yläraja Arvo (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minuuttia

(*) Jos ajoneuvoyksikkö antaa kielteisen vastauksen, joka sisältää koodin, joka tarkoittaa ”pyyntö vastaanotettu oikein, vastausta odotetaan”, arvo nostetaan samaan ylärajaan kuin P3.

2.2.5 *Virheenkäsittely*

Jos viestejä vaihdettaessa tapahtuu virhe, viestien kulku muuttuu sen mukaan, mikä laite havaitsi virheen ja mikä viesti synnytti virheen.

Kuvissa 2 ja 3 on esitetty ajoneuvoyksikön ja IDE-laitteen virheenkäsittelymenettelyt.

2.2.5.1 Viestinnän aloitus -vaihe

DDP_020 Jos IDE-laite havaitsee ajoituksen tai bittivirtaan liittyvän virheen viestinnän aloitusvaiheessa, se odottaa ajan P3 min, ennen kuin se lähettää pyynnön uudelleen.

DDP_021 Jos ajoneuvoyksikkö havaitsee virheen IDE-laitteelta tulevassa viestissä, se ei lähetä vastausta, vaan odottaa uutta viestinnän aloitus -pyyntöä ajan P3 kuluessa.

2.2.5.2 Viestintävaihe

Virheenkäsittely jakautuu kahteen osa-alueeseen:

1. **Ajoneuvoyksikkö havaitsee virheen IDE-laitteen lähetteessä.**

DDP_022 Ajoneuvoyksikön on havaittava kaikkien saapuvien viestien ajoitusvirheet, tavujen muotovirheet (kuten alku- ja stop-bitteihin liittyvät virheet) sekä kehysten virheet (väärä vastaanotettujen tavujen määrä, väärä tarkistussummatavu).

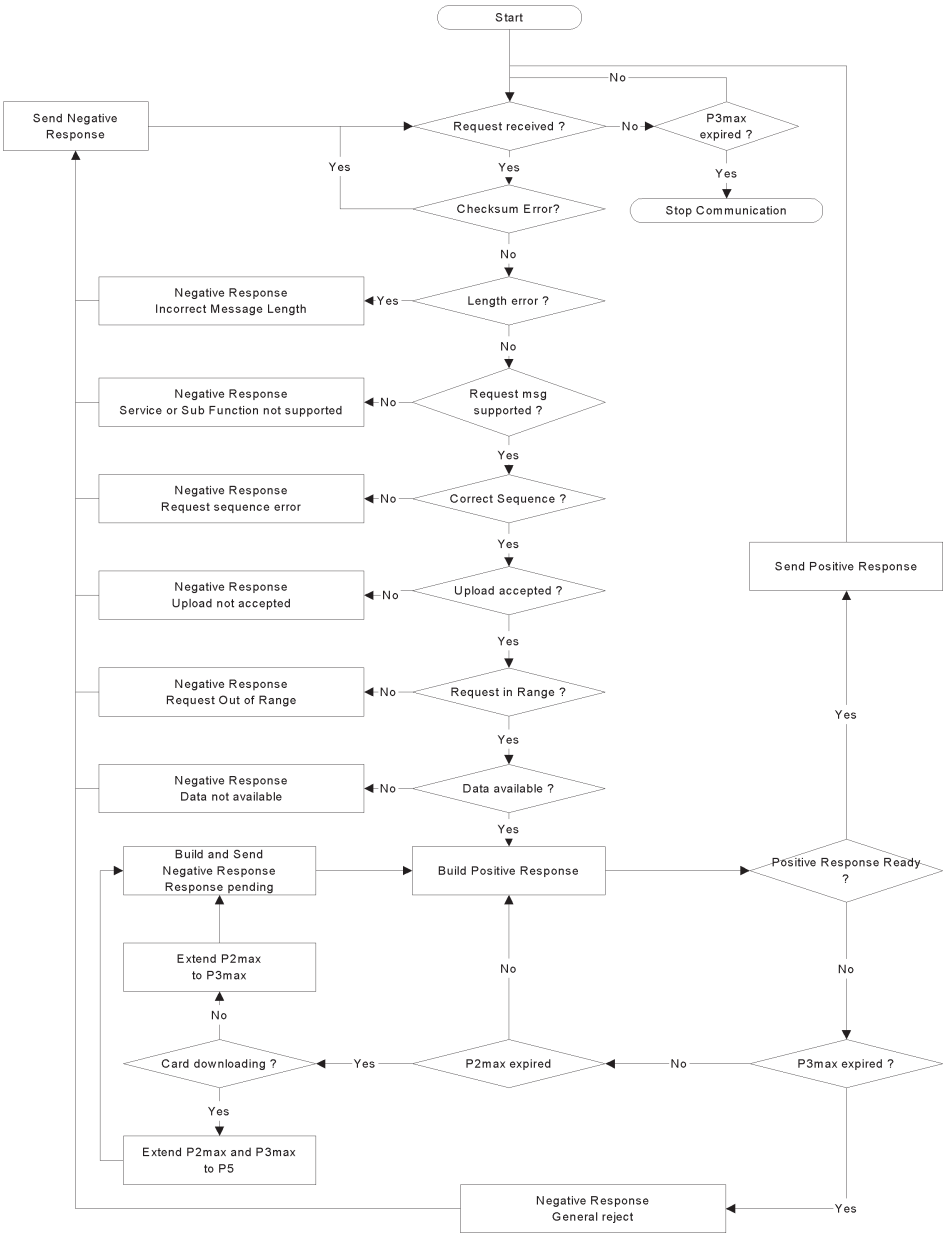
DDP_023 Jos ajoneuvoyksikkö havaitsee jonkin edellä mainituista virheistä, se ei lähetä vastausta eikä ota kyseistä viestiä huomioon.

DDP_024 Ajoneuvoyksikkö saattaa havaita muita vastaanotetun viestin muotoon tai sisältöön liittyviä virheitä (kuten, että viestin mukaista toimintoa ei tueta), vaikka viestin pituus ja tarkistussumma olisivatkin oikein; tällöin ajoneuvoyksikön on vastattava IDE-laitteelle kieltävällä virheen luonteen selvittävällä viestillä.

▼B

Kuva 2

Ajoneuvoyksikön virheenkäsittely



2. **IDE-LAITE HAVAITSEE VIRHEEN AJONEUVOYKSIKÖN LÄHETTEESSÄ.**

DDP_025 IDE-laitteen on havaittava kaikkien saapuvien viestien ajoitusvirheet, tavujen muotovirheet (kuten alku- ja stop-bitteihin liittyvät virheet) sekä kehysten virheet (väärä vastaanotettujen tavujen määrä, väärä tarkistussummatavu).

DDP_026 IDE-laitteen on havaittava viestien rakenteeseen liittyvät virheet, kuten peräkkäin vastanotettujen viestien väärät osaviestilaskurin arvonmuutokset.

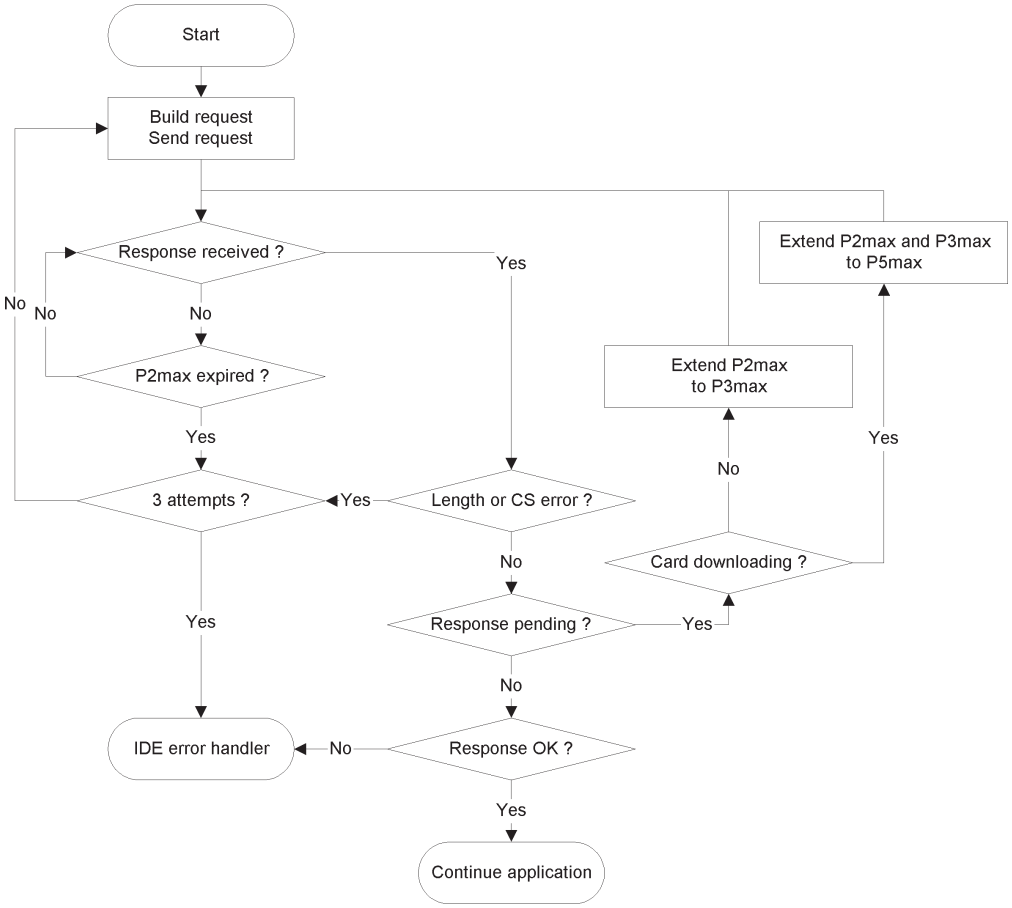
DDP_027 Jos IDE-laite havaitsee virheen tai ajoneuvoyksikkö ei vastaa ajan P2 kuluessa, pyynnön sisältävä viesti lähetetään uudelleen enintään kolme kertaa. Tässä virheen havaitsemista koskevassa tarkastelussa katsotaan osaviestin kuittaus -viesti ajoneuvoyksiköllе osoitetuksi pyynnöksi.

▼B

DDP_028 IDE-laitteen on odotettava vähintään P3:n vähimmäisaika ennen jokaista lähetystä; odotusaika mitataan viimeisestä virheen havaitsemisen jälkeen lasketusta stop-bitistä.

Kuva 3

IDE-laitteen virheenkäsittely



2.2.6 *Vastausviestien sisältö*

Tässä kohdassa määritellään erilaisten myöntävien vastausviestien datakenttien sisältö.

Dataelementit on määritelty lisäyksessä 1 (Datatermistö).

Huomautus: Toisen sukupolven kopioissa jokaista ylätason dataelementtiä edustaa tietueryhmä, vaikka se sisältäisi vain yhden tietueen. Tietueryhmä alkaa ylätunnisteella; kyseinen ylätunniste sisältää tietuetyypin, tietueen koon ja tietueiden määrän. Tietueryhmät on nimetty ”…RecordArray” (ylätunnisteen kanssa) seuraavissa taulukoissa.

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 Myönteisen vastauksen tiedonsiirron yleiskatsaus -viestin datakentän on sisällettävä seuraavat tiedot seuraavassa järjestyksessä palvelun SID-tunnisteen arvon ollessa 76h ja TREP-tunnisteen ollessa 01h sekä noudatettava asianmukaista osaviesteihin jakamista ja osaviestien laskemista:

▼B

Sukupolven 1 tiedostorakenne

Dataelementti	Huomautukset
MemberStateCertificate VUCertificate	Ajoneuvoyksikön tietoturvavarmenteet
VehicleIdentificationNumber VehicleRegistrationIdentification	Ajoneuvon tunnistetiedot
CurrentDateTime	Ajoneuvoyksikön kuluva päivämäärä ja aika
VuDownloadablePeriod	Kopiointikausi
CardSlotsStatus	Ajoneuvoyksikössä olevien korttien tyyppi
VuDownloadActivityData	Edellinen ajoneuvoyksikön kopiointi
VuCompanyLocksData	Kaikki yritysten tekemät lukitukset. Jos tämä jakso on tyhjä, lähetetään vain noOfLocks = 0.
VuControlActivityData	Kaikki ajoneuvoyksikköön tallennetut tarkastustiedot. Jos tämä jakso on tyhjä, lähetetään vain noOfControls = 0.
Signature	Kaikkien tietojen RSA-allekirjoitus (varmenteita lukuun ottamatta) välillä VehicleIdentificationNumber – viimeinen VuControlActivityData (viimeinen tavu).

Sukupolven 2 tiedostorakenne

Dataelementti	Huomautukset
MemberStateCertificateRecordArray	Jäsenvaltion myöntämä todistus
VUCertificateRecordArray	Ajoneuvoyksikön tietoturvavarmenne
VehicleIdentificationNumberRecordArray	Ajoneuvon tunnistetiedot
VehicleRegistrationNumberRecordArray	Ajoneuvon rekisterinumero
CurrentDateTimeRecordArray	Ajoneuvoyksikön kuluva päivämäärä ja aika
VuDownloadablePeriodRecordArray	Kopiointikausi
CardSlotsStatusRecordArray	Ajoneuvoyksikössä olevien korttien tyyppi
VuDownloadActivityDataRecordArray	Edellinen ajoneuvoyksikön kopiointi
VuCompanyLocksRecordArray	Kaikki yritysten tekemät lukitukset. Jos tämä jakso on tyhjä, lähetetään ryhmän ylätunniste noOfRecords = 0.
VuControlActivityRecordArray	Kaikki ajoneuvoyksikköön tallennetut tarkastustiedot. Jos tämä jakso on tyhjä, lähetetään ryhmän ylätunniste noOfRecords = 0.
SignatureRecordArray	Kaikkien edeltävien tietojen ECC-allekirjoitus varmenteita lukuun ottamatta.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 Myönteinen vastaus tiedonsiirtotoimiin -viestin datakentän on sisällettävä seuraavat tiedot seuraavassa järjestyksessä palvelun SID-tunnisteen arvon ollessa 76h ja TREP-tunnisteen ollessa 02h sekä noudatettava asianmukaista osaviesteihin jakamista ja osaviestien laskemista:

▼B

Sukupolven 1 tiedostorakenne

Dataelementti	Huomautukset
TimeReal	Kopioinnin päivämäärä
OdometerValueMidnight	Matkamittarin lukema kopiointipäivän lopussa
VuCardIWData	Korttien asettamis- ja poistotapahtumia koskevat tiedot. — Jos tässä jaksossa ei ole saatavilla tietoja, lähetetään vain noOfVuCardIWRecords = 0. — Jos VuCardIWRecord ylittää rajat 00:00 (kortin asettaminen edellisen vuorokauden aikana) tai 24:00 (kortin poisto seuraavana vuorokauden aikana), se näkyy kokonaan kyseisen kahden vuorokauden sisällä.
VuActivityDailyData	Korttiaukkojen tila 00:00 ja kopiointivuorokauden aikana tallennetut toiminnan tilan muutokset.
VuPlaceDailyWorkPeriodData	Kopiointivuorokauden aikana tallennetut paikkaa koskevat tiedot. Jos tämä jakso on tyhjä, lähetetään vain noOfPlaceRecords = 0.
VuSpecificConditionData	Kopiointivuorokauden aikana tallennetut erityisolosuhteita koskevat tiedot. Jos tämä jakso on tyhjä, lähetetään vain noOfSpecificConditionRecords = 0.
Signature	Kaikkien tietojen RSA-allekirjoitus välillä TimeReal – viimeinen erityisolosuhde -tietueen viimeinen tavu.

Sukupolven 2 tiedostorakenne:

Dataelementti	Huomautukset
DateOfDayDownloadedRecordArray	Kopioinnin päivämäärä
OdometerValueMidnightRecordArray	Matkamittarin lukema kopiointinpäivän lopussa
VuCardIWRecordArray	Korttien asettamis- ja poistotapahtumia koskevat tiedot. — Jos tässä jaksossa ei ole saatavilla tietoja, lähetetään ryhmän ylätunniste noOfRecords = 0. — Jos VuCardIWRecord ylittää rajat 00:00 (kortin asettaminen edellisen vuorokauden aikana) tai 24:00 (kortin poisto seuraavana vuorokauden aikana), se näkyy kokonaan kyseisen kahden vuorokauden sisällä.
VuActivityDailyRecordArray	Korttiaukkojen tila 00:00 ja kopiointivuorokauden aikana tallennetut toiminnan tilan muutokset.
VuPlaceDailyWorkPeriodRecordArray	Kopiointivuorokauden aikana tallennetut paikkaa koskevat tiedot. Jos tämä jakso on tyhjä, lähetetään ryhmän ylätunniste noOfRecords = 0.
VuGNSSCDRecordArray	Ajoneuvon GNSS-sijainnit, joissa kuljettajan keskeytymätön ajoaika on yli kolmen tunnin jakso. Jos tämä jakso on tyhjä, lähetetään ryhmän ylätunniste noOfRecords = 0.
VuSpecificConditionRecordArray	Kopiointivuorokauden aikana tallennetut erityisolosuhteita koskevat tiedot. Jos tämä jakso on tyhjä, lähetetään ryhmän ylätunniste noOfRecords = 0.
SignatureRecordArray	Kaikkien edeltävien tietojen ECC-allekirjoitus.

▼B

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 Myönteinen vastaus tapahtumien ja vikojen siirtoon -viestin datakentän on sisällettävä seuraavat tiedot seuraavassa järjestyksessä palvelun SID-tunnisteen arvon ollessa 76h ja TREP-tunnisteen arvon ollessa 03h sekä noudatettava asianmukaista osaviesteihin jakamista ja osaviestien laskemista:

Sukupolven 1 tiedostorakenne

Dataelementti	Huomautukset
VuFaultData	Kaikki ajoneuvoyksikön muistiin tallennetut tai meneillään olevat viat. Jos tämä jakso on tyhjä, lähetetään vain noOfVuFaults = 0.
VuEventData	Kaikki ajoneuvoyksikön muistiin tallennetut tai meneillään olevat tapahtumat (ylinopeutta lukuun ottamatta). Jos tämä jakso on tyhjä, lähetetään vain noOfVuEvents = 0.
VuOverSpeedingControlData	Viimeisintä ylinopeustarkastusta koskevat tiedot (oletusarvo, jos ei tietoja).
VuOverSpeedingEventData	Kaikki ajoneuvoyksikköön tallennetut ylinopeustiedot. Jos tämä jakso on tyhjä, lähetetään vain noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Kaikki ajoneuvoyksikköön tallennetut ajan asettamista koskevat tiedot (täyden kalibroinnin ulkopuolella). Jos tämä jakso on tyhjä, lähetetään vain noOfVuTimeAdjRecords = 0.
Signature	Kaikkien tietojen RSA-allekirjoitus kohdasta noOfVuFaults viimeisen ajan asettamista koskevan tietueen viimeiseen tavuun.

Sukupolven 2 tiedostorakenne:

Dataelementti	Huomautukset
VuFaultRecordArray	Kaikki ajoneuvoyksikön muistiin tallennetut tai meneillään olevat viat. Jos tämä jakso on tyhjä, lähetetään ryhmän ylätunniste noOfRecords = 0.
VuEventRecordArray	Kaikki ajoneuvoyksikön muistiin tallennetut tai meneillään olevat tapahtumat (ylinopeutta lukuun ottamatta). Jos tämä jakso on tyhjä, lähetetään ryhmän ylätunniste noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Viimeisintä ylinopeustarkastusta koskevat tiedot (oletusarvo, jos ei tietoja).
VuOverSpeedingEventRecordArray	Kaikki ajoneuvoyksikköön tallennetut ylinopeustiedot. Jos tämä jakso on tyhjä, lähetetään ryhmän ylätunniste noOfRecords = 0.
VuTimeAdjustmentRecordArray	Kaikki ajoneuvoyksikköön tallennetut ajan asettamista koskevat tiedot (täyden kalibroinnin ulkopuolella). Jos tämä jakso on tyhjä, lähetetään ryhmän ylätunniste noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Kaikkien edeltävien tietojen ECC-allekirjoitus.

▼B

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 Myönteinen vastaus yksityiskohtaisten nopeustietojen siirtoon -viestin datakentän on sisällettävä seuraavat tiedot seuraavassa järjestyksessä palvelun SID-tunnisteen arvon ollessa 76h ja TREP-tunnisteen arvon ollessa 04h sekä noudatettava asianmukaista osaviesteihin jakamista ja osaviestien laskemista:

Sukupolven 1 tiedostorakenne

Dataelementti	Huomautukset
VuDetailedSpeedData	Kaikki ajoneuvoyksikköön tallennetut yksityiskohtaiset tiedot nopeudesta (yksi tietueosio minuuttia kohden ajalta, jolloin ajoneuvo on liikkunut). 60 nopeusarvoa minuuttia kohden (yksi sekuntia kohden).
Signature	Kaikkien tietojen RSA-allekirjoitus kohdasta noOfSpeedBlocks viimeisen nopeutta koskevan tietueosion viimeiseen tavuun.

Sukupolven 2 tiedostorakenne:

Dataelementti	Huomautukset
VuDetailedSpeedBlockRecordArray	Kaikki ajoneuvoyksikköön tallennetut yksityiskohtaiset tiedot nopeudesta (yksi tietueosio minuuttia kohden ajalta, jolloin ajoneuvo on liikkunut). 60 nopeusarvoa minuuttia kohden (yksi sekuntia kohden).
SignatureRecordArray	Kaikkien edeltävien tietojen ECC-allekirjoitus.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 Myönteinen vastaus teknisten tietojen siirtoon -viestin datakentän on sisällettävä seuraavat tiedot seuraavassa järjestyksessä palvelun SID-tunnisteen arvon ollessa 76h ja TREP-tunnisteen arvon ollessa 05h sekä noudatettava asianmukaista osaviesteihin jakamista ja osaviestien laskemista:

Sukupolven 1 tiedostorakenne

Dataelementti	Huomautukset
VuIdentification	
SensorPaired	
VuCalibrationData	Kaikki ajoneuvoyksikköön tallennetut kalibrointitiedot.
Signature	Kaikkien tietojen RSA-allekirjoitus kohdasta vuManufacturerName viimeisen VuCalibrationRecord-tapahtuman viimeiseen tavuun.

▼B

Sukupolven 2 tiedostorakenne:

Dataelementti	Huomautukset
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Kaikki ajoneuvoyksikköön tallennetut MS-liitännät
VuSensorExternalGNSSCoupledRecordArray	Kaikki ajoneuvoyksikköön tallennetut GNSS-laitteiston ulkoiset kytkennät
VuCalibrationRecordArray	Kaikki ajoneuvoyksikköön tallennetut kalibrointitiedot
VuCardRecordArray	Kaikki ajoneuvoyksikköön tallennetut kortin asettamista koskevat tiedot
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Kaikkien edeltävien tietojen ECC-allekirjoitus.

2.3. **Tiedostojen tallennus ulkoisille tietovälineille (ESM)**

DDP_034 Kun tietojen kopiointiin on liittynyt niiden siirto ajoneuvoyksiköstä, IDE-laitteen on tallennettava yhteen fyysiseen tiedostoon kaikki ajoneuvoyksiköstä kopioinnin aikana myönteinen vastaus tiedonsiirtoon -viesteissä saadut tiedot. Viestien otsikoita, osaviestien laskureita, tyhjiä osaviestejä tai tarkistussummia ei tallenneta, mutta SID- ja TREP-tunnisteet tallennetaan (vain ensimmäisen osaviestin tunnisteet tapauksissa, joissa on useita osaviestejä).

3. AJOPIIRTURIKORTILLA OLEVIEN TIETOJEN KOPIOINTIPROTOKOLLA

3.1. **Soveltamisala**

Tässä kohdassa kuvataan kortilla olevien tietojen kopiointia suoraan IDE-laitteeseen. Koska IDE-laite ei ole osa tietoturvattua ympäristöä, kortin ja IDE-laitteen välillä ei suoriteta todentamista.

3.2. **Määritelmät**

Kopiointijakso: Jokainen kerta, jolloin ICC-kortilla olevia tietoja kopioidaan. Jaksoon sisältyy kaikki toimenpiteet IFD-laitteen ICC-kortille antamasta Reset-komennosta ICC-kortin deaktivointiin (kortin poistamiseen tai uuteen Reset-komentoon) saakka.

Allekirjoitettu tiedosto: ICC-kortilta peräisin oleva tiedosto. Tiedosto siirretään IFD-laitteelle selväkielisenä. ICC-kortilla tiedosto käsitellään hash-algoritmilla ja allekirjoitetaan ja näin saatu allekirjoitus siirretään IFD-laitteelle.

3.3. **Kortilla olevien tietojen kopiointi**

DDP_035 Ajopiirturikortilla olevien tietojen kopiointi tapahtuu seuraavasti:

— Kopioidaan kortin EF-tiedostoissa ICCja ICOlevat yleiset tiedot. Nämä tiedot ovat valinnaisia, eikä niitä ole suojattu digitaalisella allekirjoituksella.

▼B

— Kopioidaan tiedostojen Card_Certificate (tai CardSignCertificate) ja CA_Certificate tiedot. Niitä ei ole suojattu digitaalisella allekirjoituksella.

Näiden tiedostojen tiedot on kopioitava aina, kun kortilla olevia tietoja kopioidaan.

— Kopioidaan muiden sovellustietoja sisältävien (Tachograph DF-ja Tachograph_G2 DF-tiedoston alaisten) EF-tiedostojen paitsi EF Card_Download-tiedoston tiedot. Nämä tiedot on suojattu digitaalisella allekirjoituksella.

— Aina, kun kortilla olevia tietoja kopioidaan, on kopioitava ainakin tiedot, jotka ovat EF-tiedostoissa nimeltään Application_Identification ja ID.

— Kuljettajakortilla olevia tietoja kopioitaessa on myös kopioitava ainakin seuraavien EF-tiedostojen sisältämät tiedot:

- Events_Data
- Faults_Data
- Driver_Activity_Data
- Vehicles_Used
- Places
- GNSS_Places (if relevant)
- Control_Activity_Data
- Specific_Conditions.

— Kuljettajakortilla olevia tietoja kopioitaessa päivitetään EF-tiedostossa Card_Download sijaitseva LastCardDownload-päivämäärä.

— Korjaamokortilla olevia tietoja kopioitaessa asetetaan EF-tiedostossa Card_Download oleva kalibrointilaskuri alkutilaansa.

— Korjaamokortilla olevia tietoja kopioitaessa ei kopioida EF-tiedostoa Sensor_Installation_Data.

3.3.1 *Kopioinnin aloittava komentosarja*

DDP_036 IDE-laitteen on aloitettava komentosarja seuraavasti:

Kortti	Komennon suunta	IDE-laite/liitäntälaite	Merkitys/huomautuksia
	⇦	Alkutilaan asettava Reset-komento	
ATR-signaali	⇨		

Valinnaisesti voidaan PPS-toiminnon avulla valita suurempi siirtonopeus, jos kortti tukee sitä.

3.3.2 *Komentosarja tiedostoille, joilla ei ole allekirjoitusta*

DDP_037 EF-tiedostojen ICC, IC, Card_Certificate (tai CardSignCertificate) ja CA_Certificate sisältämät tiedot kopioidaan seuraavan komentosarjan avulla:

Kortti	Komennon suunta	IDE-laite/liitäntälaite	Merkitys/huomautuksia
	⇦	**Select File**	Valitaan tiedosto tunnisteensa perusteella
OK	⇨		

▼B

Kortti	Komennon suunta	IDE-laite/liitäntälaite	Merkitys/huomautuksia
	⇦	**Read Binary**	Jos tiedostossa on enemmän tietoja kuin kortinlukulaitteen tai kortin puskuriin mahtuu, komento on toistettava, kunnes koko tiedoston tiedot on luettu.
File Data OK	⇨	Tallenna tiedot ulkoiselle muistivälineelle	**3.4**:n mukaisesti Data storage format

1 huomautus: Ennen kuin valitaan EF-tiedosto Card_Certificate (tai CardSignCertificate), on valittava ajopiirturikortin sovellus (sovellustunnisteen (AID) perusteella).

2 huomautus: Tiedosto voidaan valita ja lukea myös yhdessä vaiheessa käyttäen Read Binary -komentoa lyhyellä EF-tunnisteella.

3.3.3 *Komentosarja tiedostoille, joilla on allekirjoitus*

DDP_038 Seuraavaa komentosarjaa on käytettävä kaikille niille tiedostoille, joiden sisältämät tiedot on kopioitava allekirjoituksen kera:

Kortti	Suunta	IDE-laite/liitäntälaite	Merkitys/huomautuksia
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	Laskee valitun tiedoston tietoja vastaavan hash-algoritmin tuloksen lisäyksen 11 mukaisen hash-algoritmin avulla. Tämä komento ei ole ISO-standardin mukainen.
Laske tiedoston tietoja vastaava hash-algoritmin tulos ja tallenna se väliaikaisesti.			
OK	⇨		
	⇦	**Read Binary**	Jos tiedostossa on enemmän tietoja kuin kortinlukulaitteen tai kortin puskuriin mahtuu, komento on toistettava, kunnes koko tiedoston tiedot on luettu.
File Data OK	⇨	Tallenna tiedot ulkoiselle muistivälineelle	**3.4**:n mukaisesti Data storage format

▼B

Kortti	Suunta	IDE-laite/liitäntälaite	Merkitys/huomautuksia
	⇦	**PSO: Compute Digital Signature**	
Suorita Compute Digital Signature -turvatoimi tilapäisesti tallennetun hash-algoritmin tuloksen avulla.			
Signature OK	⇨	Liitä tiedot ulkoiselle muistivälineelle aiemmin tallennettuihin tietoihin	**3.4**:n mukaisesti Data storage format

Huomautus: Tiedosto voidaan valita ja lukea myös yhdessä vaiheessa käyttäen Read Binary -komentoa lyhyellä EF-tunnisteella. Siinä tapauksessa EF voidaan valita ja lukea ennen kuin käytetään komentoa Perform Hash of File.

3.3.4 *Komentosarja, jolla kalibrointilaskuri asetetaan alkutilaansa*

DDP_039 EF-tiedostossa `Card_Download` oleva `NoOfCalibrationsSinceDownload`- laskuri asetetaan alkutilaansa seuraavan komentosarjan avulla:

Kortti	Suunta	IDE-laite/liitäntälaite	Merkitys/huomautuksia
	⇦	**Select File** EF Card_Download	Valitaan tiedosto tunnisteensa perusteella
OK	⇨		
	⇦	**Update Binary** NoOfCalibrationsSinceDownload = ‘00 00’	
asettaa kortin tietojen kopiointikertoja osoittavan luvun alkutilaansa			
OK	⇨		

Huomautus: Tiedosto voidaan valita ja lukea myös yhdessä vaiheessa käyttäen Update Binary -komentoa lyhyellä EF-tunnisteella.

3.4. **Tiedontallennuksen muoto**

3.4.1 *Johdanto*

DDP_040 Kopioidut tiedot on tallennettava seuraavasti:

— Tiedot on tallennettava transparent-tiedostorakenteen mukaisesti. Tämä tarkoittaa, että sekä tavujen järjestys että tavujen sisältämien bittien järjestys on tallennettaessa säilytettävä.

— Kaikki yhdellä kertaa kopioidut kortilla olevien tiedostojen tiedot tallennetaan yhteen ulkoisen tietovälineen tiedostoon.

▼B

3.4.2 *Tiedostomuoto*

DDP_041 Tiedostomuoto koostuu sarjasta TLV-koodattuja (tuntomerkki, pituus, sisältö) tietueita.

DDP_042 EF-tiedoston tuntomerkin on oltava tiedostotunniste (FID), johon on lisätty jatke 00h.

DDP_043 EF-tiedoston allekirjoituksen tuntomerkin on oltava kyseisen tiedoston tiedostotunniste (FID), johon on lisätty jatke 01h.

DDP_044 Pituus ilmaistaan kahdella tavulla. Ne määrittelevät sisältökentässä olevien tavujen määrän. Pituuskentän arvo FFh FFh on varattu tulevaan käyttöön.

DDP_045 Jos tiedoston tietoja ei ole kopioitu, mitään tähän tiedostoon liittyviä tietoja ei tallenneta (ei tunnusmerkkiä eikä nollapituutta).

DDP_046 Allekirjoitus on tallennettava seuraavana TLV-koodattuna tietueena heti tiedoston tiedot sisältävän TLV-koodatun tietueen jälkeen.

Määritelmä	Merkitys	Pituus
FID (2 tavua) || ”00”	EF-tiedoston tuntomerkki (FID)	3 tavua
FID (2 tavua) || ”01”	EF-tiedoston allekirjoituksen tuntomerkki (FID)	3 tavua
xx xx	Sisältökentän pituus	2 tavua

Esimerkki ulkoisella muistivälineellä olevaan tiedostoon kopioiduista tiedoista:

Tuntomerkki	Pituus	Arvo
00 02 00	00 11	EF-tiedoston ICC tiedot
C1 00 00	00 C2	EF-tiedoston Card_Certificate tiedot
		…
05 05 00	0A 2E	EF-tiedoston tiedotVehicles_Used
05 05 01	00 80	EF-tiedoston allekirjoitusVehicles_Used

4. AJOPIIRTURIKORTILLA OLEVIEN TIETOJEN KOPIOINTI AJONEUVOYKSIKÖN KAUTTA

DDP_047 Ajoneuvoyksikön on sallittava siihen asetetun kuljettajakortin tietojen kopioiminen siihen kytkettyyn IDE-laitteeseen.

DDP_048 IDE-laitteen on käynnistettävä tämä toimintatila lähettämällä ajoneuvoyksikölle kortilla olevien tietojen siirtoa koskeva pyyntö (ks. 2.2.2.9).

DDP_049 Ajoneuvoyksikön on tämän jälkeen kopioitava kaikki kortilla olevat tiedot, tiedosto kerrallaan kohdassa 3 määritellyn kortilla olevien tietojen kopiointiprotokollan mukaisesti, ja siirrettävä kaikki kortilta saadut tiedot edelleen IDE-laitteeseen asianmukaisesti TLV-koodattuina (ks. 3.4.2) ja myönteinen vastaus tiedonsiirtoon -viestiin sisällytettyinä.

▼B

DDP_050 IDE-laitteen on palautettava tiedot myönteinen vastaus tiedonsiirtoon -viestistä (poistamalla kaikki ylätunnisteet, SID-tunnisteet, TREP-tunnisteet, osaviestilaskurit ja tarkistussummat) ja tallennettava ne yhteen fyysisen tiedostoon siten kuin kohdassa 2.3 on kuvattu.

DDP_051 Ajoneuvoyksikön on sen jälkeen tarvittaessa päivitettävä kuljettajakortilla olevien `Control_Activity_Data`- tiedoston tai `Card_Download`-tiedoston tiedot.

▼B

Lisäys 8

KALIBROINTIPROTOKOLLA

SISÄLLYSLUETTELO

1. JOHDANTO

2. NIMITYKSET, MÄÄRITELMÄT JA VIITETIEDOT

3. PALVELUJEN YHTEENVETO

3.1. Käytettävissä olevat palvelut

3.2. Vastauskoodit

4. VIESTINTÄPALVELUT

4.1. StartCommunication-palvelu

4.2. StopCommunication-palvelu

4.2.1 Viestin kuvaus

4.2.2 Viestin muoto

4.2.3 Parametrien määrittely

4.3. TesterPresent-palvelu

4.3.1 Viestin kuvaus

4.3.2 Viestin muoto

5. HALLINTAPALVELUT

5.1. StartDiagnosticSession-palvelu

5.1.1 Viestin kuvaus

5.1.2 Viestin muoto

5.1.3 Parametrien määrittely

5.2. SecurityAccess-palvelu

5.2.1 Viestin kuvaus

5.2.2 Viestin muoto – SecurityAccess – requestSeed

5.2.3 Viestin muoto – SecurityAccess – sendKey

6. TIEDONSIIRTOPALVELUT

6.1. ReadDataByIdentifier-palvelu

6.1.1 Viestin kuvaus

6.1.2 Viestin muoto

6.1.3 Parametrien määrittely

6.2. WriteDataByIdentifier-palvelu

6.2.1 Viestin kuvaus

6.2.2 Viestin muoto

6.2.3 Parametrien määrittely

▼B

7. TESTIPULSSIEN OHJAUS – TULO-/LÄHTÖSIGNAALIEN OHJAUKSEN TOIMINTAYKSIKKÖ

7.1. InputOutputControlByIdentifier-palvelu

7.1.1 Viestin kuvaus

7.1.2 Viestin muoto

7.1.3 Parametrien määrittely

8. DATATIETUEIDEN MUOTO

8.1. Lähetettävät parametriarvot

8.2. Datatietueiden muoto

1. JOHDANTO

Tässä lisäyksessä kuvataan tietojen vaihtoa ajoneuvoyksikön ja testauslaitteen välillä käyttäen K-johdinta, joka on osa lisäyksessä 6 kuvattua kalibrointiliitäntälaitetta. Tässä lisäyksessä kuvataan myös kalibrointiliittimen tulo-/lähtösignaalijohtimen ohjausta.

K-johtimen kautta tapahtuvan viestiyhteyden luonti kuvataan kohdassa 4, Viestintäpalvelut.

Tässä lisäyksessä käytetään käsitettä diagnostiset ’jaksot’, joiden avulla määritellään K-johtimen ohjauksen vaikutusala eri olosuhteissa. Oletusarvoinen jakso on StandardDiagnosticSession, jonka aikana kaikki ajoneuvoyksikössä olevat tiedot voidaan lukea, mutta ajoneuvoyksikköön ei voida kirjoittaa mitään tietoja.

Diagnostisen käyttöjakson valinta on selostettu kohdassa 5, Hallintapalvelut.

Tätä lisäystä on pidettävä ajoneuvoyksikköjen ja korjaamokorttien eri sukupolvien kannalta tarpeellisena tässä asetuksessa säädettyjen yhteentoimivuusvaatimusten mukaisesti.

CPR_001 ECUProgrammingSession-jakson aikana voidaan syöttää tietoja ajoneuvoyksikköön. Kun syötetään kalibrointiin liittyviä tietoja, ajoneuvoyksikön on lisäksi oltava KALIBROINTI-toimintatilassa.

K-johtimen kautta tapahtuva tiedonsiirto kuvataan kohdassa 6, Tiedonsiirtopalvelut. Siirrettävän datan formaatit kuvataan kohdassa 8, Datatietueiden muoto.

CPR_002 ECUAdjustmentSession-jakson aikana voidaan valita kalibroinnin tulo-/lähtösignaalijohtimen tila K-johdinliitännän avulla. Kalibroinnin tulo-/lähtösignaalijohtimen ohjaus on selostettu kohdassa 7, Testipulssien ohjaus – Tulo-/lähtösignaalien ohjauksen toimintayksikkö.

CPR_003 Tässä asiakirjassa on testauslaitteen osoitteesta käytetty merkintää ’tt’. Vaikka testauslaitteilla saattaakin olla ensisijaisia osoitteita, ajoneuvoyksikön on vastattava oikein mihin hyvänsä testauslaitteen osoitteeseen. Ajoneuvoyksikön fyysinen osoite on 0xEE.

▼B

2. NIMITYKSET, MÄÄRITELMÄT JA VIITETIEDOT

Protokollat, viestit ja virhekoodit perustuvat pääpiirteissään nykyiseen standardiin ISO 14229-1 (Road vehicles – Diagnostic systems – Part 1: Diagnostic services. Tieliikenteessä käytettävät ajoneuvot. Diagnostiikkajärjestelmät. Osa 1: Diagnostiikkapalvelut, versio 6, 22. helmikuuta 2001).

Palvelutunnisteet, palvelupyynnöt ja niiden vastaukset sekä standardiparametrit on esitetty tavuittain koodattuina heksadesimaalilukuina.

Nimitys ’testauslaite’ tarkoittaa laitteita, joilla ajoneuvoyksikköön syötetään tietoja ohjelmoinnin/kalibroinnin yhteydessä.

Nimitykset ’asiakas’ ja ’palvelin’ viittaavat testauslaitteeseen ja ajoneuvoyksikköön.

Nimitys ECU (Electronic Control Unit, elektroninen ohjausyksikkö) viittaa ajoneuvoyksikköön.

Viitetiedot:

ISO 14230-2: Road Vehicles – Diagnostic Systems – Keyword Protocol 2000 – Part 2: Data Link Layer. First edition: 1999. (Tieliikenteessä käytettävät ajoneuvot. Diagnostiikkajärjestelmät. Avainsanaprotokolla 2000. Osa 2: Siirtotaso.

Ensimmäinen painos: 1999.)

Ajoneuvot – Diagnostiikkajärjestelmät.

3. PALVELUJEN YHTEENVETO

3.1. **Käytettävissä olevat palvelut**

Seuraavassa taulukossa on yhteenveto valvontalaitteessa käytettävissä olevista palveluista, jotka on määritelty tässä asiakirjassa.

CPR_004 Taulukossa on esitetty palvelut, jotka ovat käytettävissä toimintakykyisen diagnostisen jakson aikana.

— **Ensimmäisessä sarakkeessa** luetellaan käytettävissä olevat palvelut.

— **Toisessa sarakkeessa** on sen kohdan numero tässä lisäyksessä, jossa kyseinen palvelu on määritelty.

— **Kolmannessa sarakkeessa** on palvelupyynnöissä käytettävä kyseisen palvelun palvelutunniste (SID).

— **Neljännessä sarakkeessa** määritellään ne **StandardDiagnosticSession-jakson (SD)** palvelut, jotka tarvitaan kaikissa ajoneuvoyksiköissä.

— **Viidennessä sarakkeessa** määritellään ne **ECUAdjustmentSession-jakson (ECUAS)** palvelut, joiden on oltava käytettävissä ajoneuvoyksikön etulevyssä olevan kalibrointiliittimen tulo-/lähtösignaalijohtimen ohjaukseen.

— **Kuudennessa sarakkeessa** määritellään ne **ECUProgrammingSession-jakson (ECUPS)** palvelut, jotka tarvitaan ajoneuvoyksikön parametrien ohjelmoimiseen.

▼B

Taulukko 1

Palvelutunnisteiden yhteenveto

			Diagnostiset jaksot		
Diagnostinen palvelu	Kohdan nro	SId pyynnön arvo	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		■	

■ Tämä merkki tarkoittaa, että kyseinen palvelu on pakollinen tämän diagnostisen jakson aikana. Ei merkkiä tarkoittaa, että kyseinen palvelu ei ole sallittu tämän diagnostisen jakson aikana.

3.2. **Vastauskoodit**

Vastauskoodit on määritelty kullekin palvelulle.

4. VIESTINTÄPALVELUT

Jotkin palvelut ovat tarpeen viestintäyhteyden luomiseksi ja ylläpitämiseksi. Ne eivät ole mukana sovellustasossa. Käytettävissä olevat palvelut on esitetty seuraavassa taulukossa:

Taulukko 2

Viestintäpalvelut

Palvelu	Kuvaus
StartCommunication	Asiakas pyytää, että aloitetaan viestintäjakso palvelimen (palvelimien) kanssa
StopCommunication	Asiakas pyytää, että meneillään oleva viestintäjakso lopetetaan
TesterPresent	Asiakas ilmoittaa palvelimelle, että se on edelleen valmiudessa

CPR_005 StartCommunication-palvelua käytetään aloittamaan viestintä. Ennen kuin mitään palvelua voidaan suorittaa, viestintäyhteys on alustettava ja viestintäparametrien on oltava halutun toimintatilan mukaisia.

4.1. **StartCommunication-palvelu**

CPR_006 Vastaanotettuaan StartCommunication-pyynnön esittävän perusalkion ajoneuvoyksikön on tarkastettava, voidaanko viestintäyhteys näissä olosuhteissa alustaa. Olosuhteet, joissa viestintäyhteys voidaan alustaa, on kuvattu asiakirjassa ISO 14230-2.

▼B

CPR_007 Tämän jälkeen ajoneuvoyksikön on tehtävä kaikki toimet, joita vaaditaan viestintäyhteyden alustamiseksi ja lähetettävä StartCommunication-vastauksen antava perusalkio valittujen myöntävän vastauksen (Positive Response) parametrien kanssa.

CPR_008 Jos ajoneuvoyksikkö, joka on jo alustettu (ja aloittanut jonkin diagnostisen jakson), vastaanottaa uuden StartCommunication-pyynnön (esimerkiksi testauslaitteen virhetilasta palautumisen takia), on pyyntö hyväksyttävä ja ajoneuvoyksikkö alustettava uudelleen.

CPR_009 Jos viestintäyhteyttä ei jostain syystä voida alustaa, ajoneuvoyksikön on jatkettava sitä toimintaa, jota se oli suorittamassa juuri ennen viestintäyhteyden alustusyritystä.

CPR_010 StartCommunication-pyynnölle on annettava fyysinen osoite.

CPR_011 Ajoneuvoyksikön alustus palveluja varten tapahtuu käyttäen 'nopeaa alustustapaa':

— Ennen kutakin toimintoa on jakso, jolloin väylä on tyhjänä.

— Tämän jälkeen testauslaite lähettää alustusmerkkijonon.

— Kaikki viestintäyhteyden luomisessa tarvittavat tiedot sisältyvät ajoneuvoyksikön vastaukseen.

CPR_012 Alustuksen päätyttyä:

— Kaikki viestintäparametrit on asetettu avaintavujen mukaisiin taulukossa 4 – Viestinnässä käytettävät ajoitusarvot – määriteltyihin arvoihin.

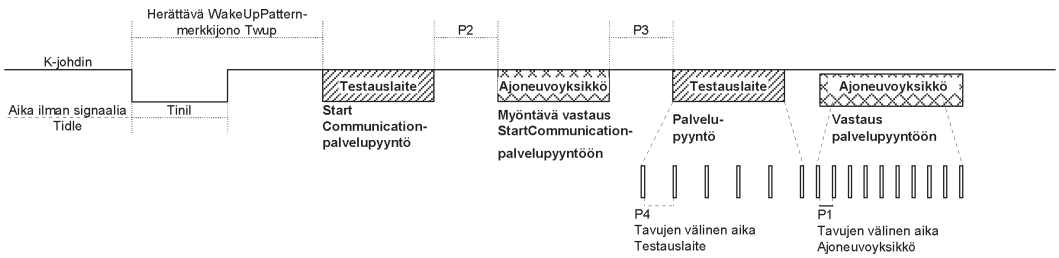
— Ajoneuvoyksikkö odottaa testauslaitteen ensimmäistä pyyntöä.

— Ajoneuvoyksikkö on oletusarvoisessa diagnostisessa toimintatilassa eli StandardDiagnosticSession-tilassa.

— Kalibroinnin tulo-/lähtösignaalijohdin on oletusarvoisessa eli toimintakyvyttömässä tilassa.

CPR_014 K-johtimen nopeudeksi on säädetty 10 400 baudia.

CPR_016 Nopea alustus alkaa siten, että testauslaite lähettää herättävän WakeUpPattern (Wup) -merkkijonon K-johtimen kautta. Merkkijono alkaa Tinil-ajan pituisella loogisen tason pidolla nollassa K-johtimen oltua siihen asti ilman signaalia. Testauslaite lähettää StartCommunication-palvelun ensimmäisen bitin, kun signaalin ensimmäisestä laskevasta reunasta on kulunut aika Twup.



▼B

CPR_017 Nopeassa alustuksessa ja viestinnässä yleensä käytettävät ajoitusarvot on esitetty seuraavissa taulukoissa. Ilman signaalia olevalle ajalle (Tidle) on erilaisia vaihtoehtoja:

— Ensimmäinen lähetys virran kytkemisen jälkeen: Tidle = 300 ms.

— StopCommunication-palvelun päättymisen jälkeen: Tidle = ajan P3 vähimmäisarvo.

— Viestinnän päätyttyä P3:n enimmäisarvoa vastaavan odotusajan kuluttua: Tidle = 0.

Taulukko 3

Nopeassa alustuksessa käytettävät ajoitusarvot

Parametri		vähimmäisarvo	enimmäisarvo
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Taulukko 4

Viestinnässä käytettävät ajoitusarvot

Ajoitusparametri	Parametrin selite	Alemmat rajaarvot [ms]	Ylemmät rajaarvot [ms]
		vähintään	enintään
P1	Tavujen välinen aika ajoneuvoyksikön vastauksessa	0	20
P2	Testauslaitteen palvelupyynnön ja ajoneuvoyksikön vastauksen tai ajoneuvoyksikön kahden vastauksen välinen aika	25	250
P3	Ajoneuvoyksikön vastauksen lopun ja testauslaitteen uuden palvelupyynnön alun välinen aika	55	5 000
P4	Tavujen välinen aika testauslaitteen palvelupyynnössä	5	20

CPR_018 Nopeassa alustuksessa käytettävien viestien muoto on esitetty seuraavissa taulukoissa. (Huomautus: Hex merkitsee heksadesimaalia)

Taulukko 5

StartCommunication-pyynnön sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	81	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC

▼B

Tavun #	Parametri	Arvo (Hex)	Muistikas
#4	**StartCommunication-palvelupyynnön tunniste**	**81**	**SCR**
#5	Tarkistussumma	00-FF	CS

Taulukko 6

StartCommunication-palvelupyyntöön annettavan myöntävän vastauksen sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	**StartCommunication-palvelupyyntöön annettavan myöntävän vastauksen tunniste**	**C1**	**SCRPR**
#6	Avaintavu 1	EA	KB1
#7	Avaintavu 2	8F	KB2
#8	Tarkistussumma	00-FF	CS

CPR_019 StartCommunication-palvelupyyntöön ei ole olemassa kieltävää vastausta; jos myöntävää vastausta ei voida lähettää, ajoneuvoyksikköä ei alusteta, mitään ei lähetetä ja ajoneuvoyksikkö jatkaa normaalia toimintaansa.

4.2. **StopCommunication-palvelu**

4.2.1 *Viestin kuvaus*

Tätä liikennekerroksen palvelua käytetään päättämään viestintäjakso.

CPR_020 Vastaanotettuaan StopCommunication-pyynnön esittävän perusalkion, ajoneuvoyksikön on tarkastettava, voidaanko viestintäyhteys näissä olosuhteissa katkaista. Tässä tapauksessa ajoneuvoyksikön on suoritettava kaikki tämän viestintäyhteyden katkaisemisessa tarvittavat toimet.

CPR_021 Jos viestintäyhteyden katkaiseminen on mahdollista, ajoneuvoyksikön on annettava StopCommunication-palvelupyynnön vastauksen esittävä perusalkio valittujen myöntävän vastauksen (Positive Response) parametrien kanssa, ennen kuin viestintäyhteys katkaistaan.

CPR_022 Jos viestintäyhteyttä ei jostain syystä voida katkaista, ajoneuvoyksikön on annettava StopCommunication-palvelupyynnön vastauksen esittävä perusalkio valittujen kieltävän vastauksen (Negative Response) parametrien kanssa.

CPR_023 Jos ajoneuvoyksikkö havaitsee, että ajan P3 enimmäisarvoa vastaava odotusaika on ylitetty, viestintäyhteys katkaistaan ilman, että annetaan mitään vastausta esittävää perusalkiota.

▼B

4.2.2 *Viestin muoto*

CPR_024 StopCommunication-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

Taulukko 7

StopCommunication-palvelupyynnön sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	01	LEN
#5	**StopCommunication-palvelupyynnön tunniste**	**82**	**SPR**
#6	Tarkistussumma	00-FF	CS

Taulukko 8

StopCommunication-palvelupyyntöön annettavan myöntävän vastauksen tunniste

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	01	LEN
#5	**StartCommunication-palvelupyyntöön annettavan myöntävän vastauksen tunniste**	**C2**	**SPRPR**
#6	Tarkistussumma	00-FF	CS

Taulukko 9

StopCommunication-palvelupyyntöön annettavan kieltävän vastauksen sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN

▼B

Tavun #	Parametri	Arvo (Hex)	Muistikas
#5	**Palvelupyyntöön annettavan kieltävän vastauksen tunniste**	**7F**	**NR**
#6	StopCommunication-palvelupyynnön tunniste	82	SPR
#7	responseCode = generalReject (vastauskoodi = yleinen hylkääminen)	10	RC_GR
#8	Tarkistussumma	00-FF	CS

4.2.3 *Parametrien määrittely*

Tämä palvelu ei tarvitse parametrien määrittelyä.

4.3. **TesterPresent-palvelu**

4.3.1 *Viestin kuvaus*

Testauslaite ilmoittaa TesterPresent-palvelun avulla palvelimelle olevansa vielä valmiudessa. Näin palvelin ei palaudu automaattisesti normaalitilaan ja mahdollisesti katkaise viestintäyhteyttä. Tämä määräajoin lähetettävä palvelu pitää diagnostiikkajakson/viestintäyhteyden aktiivisena nollaamalla P3-laskurin aina, kun tällainen palvelupyyntö vastaanotetaan.

4.3.2 *Viestin muoto*

CPR_079 TesterPresent-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

Taulukko 10

TesterPresent-palvelupyynnön sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	02	LEN
#5	**TesterPresent-palvelupyynnön tunniste**	**3E**	**TP**
#6	Sub Function = responseRequired = [kyllä (yes)]	01	RESPREQ_Y
	ei (no)]	02	RESP-REQ_NO
#7	Tarkistussumma	00-FF	CS

CPR_080 Jos responseRequired-parametrin arvon on ’yes’, palvelin vastaa seuraavalla myönteisellä vastausviestillä. Jos arvo on ’no’, palvelin ei lähetä vastausta.

▼B

Taulukko 11

TesterPresent-palvelupyyntöön annettavan myöntävän vastauksen sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	01	LEN
#5	**TesterPresent-palvelupyyntöön annettavan myöntävän vastauksen tunniste**	**7E**	**TPPR**
#6	Tarkistussumma	00-FF	CS

CPR_081 Palvelun on tuettava seuraavia kielteisiä vastauskoodeja:

Taulukko 12

TesterPresent-palvelupyyntöön annettavan kieltävän vastauksen sisältävä viesti

Tavun #	Parametri		Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen		80	FMT
#2	Kohteen osoitetavu		tt	TGT
#3	Lähteen osoitetavu		EE	SRC
#4	Pituutta osoittava lisätavu		03	LEN
#5	**Palvelupyyntöön annettavan kieltävän vastauksen tunniste**		**7F**	**NR**
#6	TesterPresent-palvelupyynnön tunniste		3E	TP
#7	responseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Tarkistussumma		00-FF	CS

▼B

5. HALLINTAPALVELUT

Käytettävissä olevat palvelut on esitetty seuraavassa taulukossa:

Taulukko 13

Hallintapalvelut

Palvelu	Kuvaus
StartDiagnosticSession	Asiakas pyytää, että aloitetaan diagnostinen jakso ajoneuvoyksikön kanssa
SecurityAccess	Asiakas pyytää saada käyttöönsä toimintoja, joiden käyttöoikeudet on vain tietyillä käyttäjillä

5.1. **StartDiagnosticSession-palvelu**

5.1.1 *Viestin kuvaus*

CPR_025 StartDiagnosticSession-palvelun avulla käynnistetään palvelimessa erilaisia diagnostisia jaksoja. Diagnostinen jakso mahdollistaa tiettyjen palvelujen käytön taulukon 17 – diagnosticSession-parametrin arvojen määritelmät – mukaisesti. Jakso voi mahdollistaa ajoneuvovalmistajakohtaisia palveluja, joita ei kuvata tässä asiakirjassa. Suoritussäännöt ovat seuraavien vaatimusten mukaiset:

— Ajoneuvoyksikössä on aina oltava tasan yksi diagnostinen jakso aktiivisena.

— Virran kytkeydyttyä ajoneuvoyksikön on aina käynnistettävä StandardDiagnosticSession-jakso. Ellei muuta diagnostista jaksoa aloiteta, StandardDiagnosticSession-jakson on jatkuttava niin kauan kuin ajoneuvoyksikön virta on kytkettynä.

— Jos testauslaite pyytää jo aktiivisena olevaa diagnostista jaksoa, ajoneuvoyksikön on lähetettävä myönteinen vastausviesti.

— Aina testauslaitteen pyytäessä uutta diagnostista jaksoa ajoneuvoyksikkö lähettää ensin myönteisen vastauksen StartDiagnosticSession-pyyntöön ennen kuin uusi jakso aktivoituu ajoneuvoyksikössä. Jos ajoneuvoyksikkö ei voi käynnistää pyydettyä uutta diagnostista jaksoa, se vastaa StartDiagnosticSession-pyyntöön kielteisellä viestillä ja jatkaa meneillään olevaa jaksoa.

CPR_026 Diagnostinen jakso saa alkaa vain, jos asiakkaan ja ajoneuvoyksikön välille on luotu viestintäyhteys.

CPR_027 Taulukossa 4 määritellyt ajoitusparametrit on otettava käyttöön, kun StartDiagnosticSession-pyyntöön, johon on liitetty diagnosticSession-parametri asetettuna arvoon StandardDiagnosticSession, annetaan myöntävä vastaus, jos jokin diagnostinen jakso oli aikaisemmin käynnissä.

5.1.2 *Viestin muoto*

CPR_028 StartDiagnosticSession-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

▼B

Taulukko 14

StartDiagnosticSession-palvelupyynnön sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	02	LEN
#5	**StartDiagnosticSession-palvelupyynnön tunniste**	**10**	**STDS**
#6	diagnosticSession = (diagnostinen jakso) [jokin taulukon 17 arvo]	xx	DS_ …
#7	Tarkistussumma	00-FF	CS

Taulukko 15

StartDiagnosticSession-palvelupyyntöön annettavan myöntävän vastauksen sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	02	LEN
#5	**StartDiagnosticSession-palvelupyyntöön annettavan myöntävän vastauksen tunniste**	**50**	**STDSPR**
#6	diagnosticSession = [sama kuin tavun #6 arvo taulukossa 14]	xx	DS_ …
#7	Tarkistussumma	00-FF	CS

Taulukko 16

StartDiagnosticSession-palvelupyyntöön annettavan kieltävän vastauksen sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC

▼B

Tavun #	Parametri		Arvo (Hex)	Muistikas
#4	Pituutta osoittava lisätavu		03	LEN
#5	**Palvelupyyntöön annettavan kieltävän vastauksen tunniste**		**7F**	**NR**
#6	StartDiagnosticSession-palvelupyynnön tunniste		10	STDS
#7	Response-Code =	[subFunctionNotSupported ([a])	12	RC_SFNS
		incorrectMessageLength ([b])	13	RC_IML
		conditionsNotCorrect ([c])	22	RC_CNC
#8	Tarkistussumma		00-FF	CS

([a]) – Palvelupyyntöviestin tavulle #6 annettua arvoa ei tueta, ts. sitä ei ole taulukossa 17.
([b]) – Viestin pituus on väärä.
([c]) – StartDiagnosticSession-pyynnölle asetetut vaatimukset eivät täyty.

5.1.3 *Parametrien määrittely*

CPR_029 ***diagnosticSession (DS_)*** -parametrin avulla StartDiagnosticSession-palvelu valitsee tietyn palvelimen (palvelimien) toimintatavan. Tässä asiakirjassa on määritelty seuraavat diagnostiset jaksot:

Taulukko 17

DiagnosticSession-parametrin arvojen määritelmät

Hex	Kuvaus	Muistikas
81	**StandardDiagnosticSession** Mahdollistaa kaikki **taulukossa 1, sarakkeessa 4 SD** kuvatut palvelut. Näiden palvelujen avulla voidaan tietoja lukea palvelimelta (ajoneuvoyksiköstä). Tämä diagnostinen jakso on käynnissä sen jälkeen, kun asiakkaan (testauslaitteen) ja palvelimen (ajoneuvoyksikön) välinen alustus on onnistuneesti suoritettu. Muut tässä kohdassa määritellyt diagnostiset jaksot voivat syrjäyttää tämän diagnostisen jakson.	**SD**
85	**ECUProgrammingSession** Mahdollistaa kaikki **taulukossa 1, sarakkeessa 6 ECUPS** kuvatut palvelut. Nämä palvelut tukevat palvelimen (ajoneuvoyksikön) muistin ohjelmointia. Muut tässä kohdassa määritellyt diagnostiset jaksot voivat syrjäyttää tämän diagnostisen jakson.	**ECUPS**

▼B

Hex	Kuvaus	Muistikas
87	**ECUAdjustmentSession** Mahdollistaa kaikki **taulukossa 1, sarakkeessa 5 ECUAS** kuvatut palvelut. Nämä palvelut tukevat palvelimen (ajoneuvoyksikön) tulo-lähtösignaalin ohjausta. Muut tässä kohdassa määritellyt diagnostiset jaksot voivat syrjäyttää tämän diagnostisen jakson.	**ECUAS**

5.2. **SecurityAccess-palvelu**

Kalibrointitietojen kirjoittaminen on mahdollista vain, jos ajoneuvoyksikkö on KALIBROINTI-toimintatilassa Sen lisäksi, että ajoneuvoyksikköön on asettava voimassa oleva korjaamokortti, on siihen syötettävä oikea henkilökohtainen tunnusluku (PIN), jotta KALIBROINTI-toimintatila saadaan käyttöön.

Kalibrointia varten olevan tulo-/lähtösignaalijohtimen käyttö on myös mahdollista, jos ajoneuvoyksikkö on KALIBROINTI- tai TARKASTUS-toimintatilassa.

SecurityAccess-palvelun avulla voidaan syöttää PIN-tunnusluku ja antaa testauslaitteelle tieto siitä, onko ajoneuvoyksikkö KALIBROINTI-toimintatilassa.

PIN-tunnusluvun syöttäminen muilla tavoin on sallittu.

5.2.1 *Viestin kuvaus*

SecurityAccess-palvelu muodostuu palvelun requestSeed-viestistä ja sitä mahdollisesti seuraavasta palvelun sendKey-viestistä. SecurityAccess-palvelu on suoritettava StartDiagnosticSession-palvelun jälkeen.

CPR_033 Testauslaitteen on käytettävä SecurityAccess-palvelun requestSeed-viestiä varmistamaan, että ajoneuvoyksikkö on valmis vastaanottamaan PIN-tunnusluvun.

CPR_034 Jos ajoneuvoyksikkö on jo KALIBROINTI-toimintatilassa, sen on vastattava palvelupyyntöön lähettämällä ’siemenluku’ 0x0000 käyttäen SecurityAccess-palvelupyynnön myöntävää vastausta.

CPR_035 Jos ajoneuvoyksikkö on valmis vastaanottamaan PIN-tunnusluvun, jotta se voitaisiin todentaa korjaamokortin avulla, sen on vastattava lähettämällä arvoa 0x0000 suurempi ’siemenluku’ käyttäen SecurityAccess-palvelupyynnön myöntävää vastausta.

CPR_036 Jos ajoneuvoyksikkö ei ole valmis vastaanottamaan PIN-tunnuslukua testauslaitteelta joko siksi, että korjaamokortti ei ole voimassa tai siksi, että ajoneuvoyksikkö odottaa, että PIN-tunnusluku syötetään jollain muulla tavoin, sen on vastattava antamalla kieltävä vastaus, jossa vastauskoodille on asetettu vastausta conditionsNotCorrectOrRequestSequenceError vastaava arvo.

CPR_037 Testauslaitteen on tämän jälkeen mahdollisesti lähetettävä PIN-tunnusluku ajoneuvoyksikölle SecurityAccess-palvelun sendKey-viestin avulla. Jotta kortin tunnistamisprosessille jäisi riittävästi aikaa, ajoneuvoyksikön on jatkettava vastausaikaa kielteisellä viestillä requestCorrectlyReceived-ResponsePending. Vastausaika ei kuitenkaan saa ylittää 5:tä minuuttia. Heti kun pyydetty palvelu on suoritettu, ajoneuvoyksikön

▼B

on lähetettävä myönteinen tai kielteinen vastausviesti, jolla on eri vastauskoodi. Ajoneuvoyksikkö voi toistaa kielteistä vastauskoodia requestCorrectlyReceived-ResponsePending, kunnes pyydetty palvelu on suoritettu ja lopullinen vastausviesti lähetetty.

CPR_038 Ajoneuvoyksikkö saa vastata tähän pyyntöön antamalla SecurityAccess-palvelupyyntöön myöntävän vastauksen vain, jos se on KALIBROINTI-toimintatilassa.

CPR_039 Seuraavissa tapauksissa ajoneuvoyksikön on annettava tähän palvelupyyntöön kieltävä vastaus siten, että vastauskoodin arvoksi on asetettu:

— subFunctionNot supported: alitoimintoparametrin (accessType) väärä muoto,

— conditionsNotCorrectOrRequestSequenceError: ajoneuvoyksikkö ei ole valmis vastaanottamaan PIN-tunnuslukua,

— invalidKey: PIN-tunnusluku ei ole oikea, mutta tunnusluvun sallittujen syöttöyritysten määrää ei ole ylitetty,

— exceededNumberOfAttempts: PIN-tunnusluku ei ole oikea ja tunnusluvun sallittujen syöttöyritysten määrä on ylitetty,

— generalReject: PIN-tunnusluku on oikea, mutta yksikön ja korjaamokortin välinen todentaminen epäonnistui.

5.2.2 *Viestin muoto – SecurityAccess – requestSeed*

CPR_040 SecurityAccess-palvelun requestSeed-perusalkioiden viestien muodot on esitetty seuraavissa taulukoissa.

Taulukko 18

SecurityAccess-palvelupyynnön requestSeed-viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	02	LEN
#5	**SecurityAccess-palvelupyynnön tunniste**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Tarkistussumma	00-FF	CS

▼B

Taulukko 19

SecurityAccess-palvelupyynnön myönteinen requestSeed-vastausviesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	04	LEN
#5	**SecurityAccess-palvelupyyntöön annettavan myöntävän vastauksen tunniste**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	Siemenluvun (Seed) merkitsevämpi tavu	00-FF	SEEDH
#8	Siemenluvun (Seed) vähemmän merkitsevä tavu	00-FF	SEEDL
#9	Tarkistussumma	00-FF	CS

Taulukko 20

SecurityAccess-palvelupyyntöön annettavan kieltävän vastauksen sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	**Palvelupyyntöön annettavan kieltävän vastauksen tunniste**	**7F**	**NR**
#6	SecurityAccess-palvelupyynnön tunniste	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Tarkistussumma	00-FF	CS

▼B

5.2.3 *Viestin muoto – SecurityAccess – sendKey*

CPR_041 SecurityAccess-palvelun sendKey-perusalkioiden viestien muodot on esitetty seuraavissa taulukoissa.

Taulukko 21

SecurityAccess-palvelupyynnön sendKey-viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	m+2	LEN
#5	**SecurityAccess-palvelupyynnön tunniste**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7–#m+6	Avain #1 (merkitsevin) … Avain #m (vähiten merkitsevä, m:n arvon tulee olla vähintään 4 ja enintään 8)	xx … xx	KEY
#m+7	Tarkistussumma	00-FF	CS

Taulukko 22

SecurityAccess-palvelupyynnön myönteinen sendKey-vastausviesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	02	LEN
#5	**SecurityAccess-palvelupyyntöön annettavan myöntävän vastauksen tunniste**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Tarkistussumma	00-FF	CS

▼B

Taulukko 23

SecurityAccess-palvelupyyntöön annettavan kieltävän vastauksen sisältävä viesti

Tavun #	Parametri		Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen		80	FMT
#2	Kohteen osoitetavu		tt	TGT
#3	Lähteen osoitetavu		EE	SRC
#4	Pituutta osoittava lisätavu		03	LEN
#5	**Palvelupyyntöön annettavan kieltävän vastauksen tunniste**		**7F**	**NR**
#6	SecurityAccess-palvelupyynnön tunniste		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	Tarkistussumma		00-FF	CS

6. TIEDONSIIRTOPALVELUT

Käytettävissä olevat palvelut on esitetty seuraavassa taulukossa:

Taulukko 24

Tiedonsiirtopalvelut

Palvelu	Kuvaus
ReadDataByIdentifier	Asiakas pyytää, että lähetetään recordDataIdentifier-tunnisteen perusteella käyttöön saatavan tietueen nykyinen arvo.
WriteDataByIdentifier	Asiakas pyytää saada kirjoittaa recordDataIdentifier-tunnisteen perusteella käyttöön saatavan tietueen.

▼B

6.1. **ReadDataByIdentifier-palvelu**

6.1.1 *Viestin kuvaus*

CPR_050 ReadDataByIdentifier-palvelun avulla asiakas pyytää datatietueiden arvoja palvelimelta. Data tunnistetaan recordDataIdentifier-tunnisteen avulla. Ajoneuvoyksikön valmistaja vastaa siitä, että palvelimen vaatimukset täytetään tätä palvelua suoritettaessa.

6.1.2 *Viestin muoto*

CPR_051 ReadDataByIdentifier-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

Taulukko 25

ReadDataByIdentifier-palvelupyynnön sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	**ReadDataByIdentifier-palvelupyynnön tunniste**	**22**	**RDBI**
#6–#7	recordDataIdentifier = [arvo taulukosta 28]	xxxx	RDI_ …
#8	Tarkistussumma	00-FF	CS

Taulukko 26

ReadDataByIdentifier-palvelupyyntöön annettavan myöntävän vastauksen sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	m+3	LEN
#5	**ReadDataByIdentifier-palvelupyyntöön annettavan myöntävän vastauksen tunniste**	**62**	**RDBIPR**
#6 ja #7	recordDataIdentifier = [sama arvo kuin tavuilla #6 ja #7 taulukosta 25]	xxxx	RDI_ …

▼B

Tavun #	Parametri		Arvo (Hex)	Muistikas
#8–#m+7	dataRecord[] =	[data#1	xx	DREC_DATA1
		:	:	:
		data#m]	xx	DREC_DATAm
#m+8	Tarkistussumma		00-FF	CS

Taulukko 27

ReadDataByIdentifier-palvelupyyntöön annettavan kieltävän vastauksen sisältävä viesti

Tavun #	Parametri		Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen		80	FMT
#2	Kohteen osoitetavu		tt	TGT
#3	Lähteen osoitetavu		EE	SRC
#4	Pituutta osoittava lisätavu		03	LEN
#5	**Palvelupyyntöön annettavan kieltävän vastauksen tunniste**		**7F**	**NR**
#6	ReadDataByIdentifier-palvelupyynnön tunniste		22	RDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Tarkistussumma		00-FF	CS

6.1.3 *Parametrien määrittely*

CPR_052 ReadDataByIdentifier-pyynnön parametri ***recordDataIdentifier (RDI_)*** määrittää datatietueen.

CPR_053 Tässä asiakirjassa määritellyt RecordDataIdentifier-parametrin arvot on esitetty seuraavassa taulukossa.

RecordDataIdentifier-parametria koskevassa taulukossa on neljä saraketta ja useita rivejä.

— **Ensimmäinen sarake (Hex)** sisältää kolmannessa sarakkeessa määritellylle recordDataIdentifier-parametrille annetun arvon heksadesimaalilukuna.

— **Toinen sarake (dataelementti)** määrittelee lisäyksessä 1 määritellyn dataelementin, johon recordDataIdentifier-parametri perustuu (muunto saattaa olla tarpeen).

▼B

— **Kolmas sarake** (parametrin kuvaus) määrittelee vastaavan recordDataIdentifier-parametrin nimen.

— **Neljäs sarake** (Muistikas) määrittelee kyseisen recordDataIdentifier-parametrin muistikkaan.

Taulukko 28

RecordDataIdentifier-parametrin arvojen määritelmät

Hex	Dataelementti	Nimi Ks. muoto kohdasta 8.2	Muistikas
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicle-Distance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 ReadDataByIdentifier-palvelupyyntöön annettavan myönteisen vastauksen sisältävässä viestissä käytetään ***dataRecord (DREC_)*** -parametria hakemaan recordDataIdentifier-tunnisteen mukainen tietue asiakkaalle (testauslaitteelle). Dataformaatit määritellään kohdassa 8. Käyttäjä voi toteuttaa valinnaisia dataRecord-parametrin arvoja esimerkiksi ajoneuvoyksikkökohtaisille syöttö- ja tulostustiedoille ja laitteen sisäiseen tiedonsiirtoon. Näitä ei määritellä tässä asiakirjassa.

6.2. WriteDataByIdentifier-palvelu

6.2.1 *Viestin kuvaus*

CPR_056 WriteDataByIdentifier-palvelun avulla asiakas voi kirjoittaa datatietueiden arvoja palvelimelle. Data tunnistetaan recordDataIdentifier-tunnisteen avulla. Ajoneuvoyksikön valmistaja vastaa siitä, että palvelimen vaatimukset täytetään tätä palvelua suoritettaessa. Taulukossa 28 lueteltuja parametreja voidaan päivittää vain, kun ajoneuvoyksikkö on KALIBROINTI-toimintatilassa.

6.2.2 *Viestin muoto*

CPR_057 WriteDataByIdentifier-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

▼B

Taulukko 29

WriteDataByIdentifier-palvelupyynnön sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	m+3	LEN
#5	**WriteDataByIdentifier-palvelupyynnön tunniste**	**2E**	**WBDI**
#6–#7	recordDataIdentifier = [arvo taulukosta 28]	xxxx	RDI_ …
#8–#m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Tarkistussumma	00-FF	CS

Taulukko 30

WriteDataByIdentifier-palvelupyyntöön annettavan myöntävän vastauksen sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	**WriteDataByIdentifier-palvelupyyntöön annettavan myöntävän vastauksen tunniste**	**6E**	**WDBIPR**
#6–#7	recordDataIdentifier = [sama arvo kuin taulukon 29 tavuilla #6 ja #7]	xxxx	RDI_ …
#8	Tarkistussumma	00-FF	CS

▼B

Taulukko 31

WriteDataByIdentifier-palvelupyyntöön annettavan kieltävän vastauksen sisältävä viesti

Tavun #	Parametri		Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen		80	FMT
#2	Kohteen osoitetavu		tt	TGT
#3	Lähteen osoitetavu		EE	SRC
#4	Pituutta osoittava lisätavu		03	LEN
#5	**Palvelupyyntöön annettavan kieltävän vastauksen tunniste**		**7F**	**NR**
#6	WriteDataByIdentifier-palvelupyynnön tunniste		2E	WBDI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Tarkistussumma		00-FF	CS

6.2.3 *Parametrien määrittely*

Parametri ***recordDataIdentifier (RDI_)*** on määritelty taulukossa 28.

WriteDataByIdentifier-palvelupyyntöön annettavan myönteisen vastauksen sisältävässä viestissä käytetään ***dataRecord (DREC_)*** -parametria hakemaan recordDataIdentifier-tunnisteen mukaisten tietueiden arvot palvelimelle (ajoneuvoyksikölle). Dataformaatit määritellään kohdassa 8.

7. TESTIPULSSIEN OHJAUS – TULO-/LÄHTÖSIGNAALIEN OHJAUKSEN TOIMINTAYKSIKKÖ

Käytettävissä olevat palvelut on esitetty seuraavassa taulukossa:

Taulukko 32

Tulo-/lähtösignaalien ohjauksen toimintayksikkö

Palvelu	Kuvaus
InputOutputControlByIdentifier	Asiakas pyytää saada ohjata palvelinkohtaista tulo-/lähtösignaalia

7.1. **InputOutputControlByIdentifier-palvelu**

7.1.1 *Viestin kuvaus*

Laitteen etukannessa olevan liittimen johtimen kautta voidaan testipulsseja ohjata tai seurata tarkoitukseen sopivan testauslaitteen avulla.

▼B

CPR_058 Tämän kalibroinnin tulo-/lähtösignaalijohtimen asetukset voidaan määritellä InputOutputControlByIdentifier-palvelun avulla annetulla K-johdinta koskevalla komennolla, jolloin johtimelle otetaan käyttöön valittu tulo- tai lähtösignaalitoiminto. Johtimen tilat ovat:

— ei käytössä,

— speedSignalInput, jossa kalibroinnin tulo-/lähtösignaalijohdinta käytetään syötettäessä nopeussignaalia (testisignaalia), joka korvaa liikeanturin nopeussignaalin. Toiminto ei ole käytettävissä TARKASTUS-toimintatilassa.

— realTimeSpeedSignalOutputSensor, jossa kalibroinnin tulo-/lähtösignaalijohdinta käytetään tulostettaessa liikeanturin nopeussignaalia,

— RTCOutput, jossa kalibroinnin tulo-/lähtösignaalijohdinta käytetään tulostettaessa UTC-kellosignaalia, toiminto ei ole käytettävissä TARKASTUS-toimintatilassa.

CPR_059 Ajoneuvoyksiköllä on oltava käynnissä säätöjakso ja sen tulee olla KALIBROINTI- tai TARKASTUS-toimintatilassa, jotta johtimen tilaa koskeva asetus voidaan määrittää. Jos ajoneuvoyksikkö on KALIBROINTI-toimintatilassa, valittavissa on neljä johtimen tilaa (ei käytössä, speedSignalInput, realTimeSpeedSignalOutputSensor ja RTCOutput). Jos ajoneuvoyksikkö on TARKASTUS-toimintatilassa, on valittavissa vain kaksi johtimen tilaa (ei käytössä ja realTimeSpeedOutputSensor). Säätöjakson tai KALIBROINTI- tai TARKASTUS-toimintatilan päättyessä ajoneuvoyksikön on varmistettava, että kalibroinnin tulo-/lähtösignaalijohdin palautetaan ’ei käytössä’ -tilaan (oletusarvoinen tila).

CPR_060 Jos ajoneuvoyksikön liikepulsseja tosiajassa vastaanottavaan tulojohtimeen saapuu liikepulsseja, kun kalibroinnin tulo-/lähtösignaalijohdin on asetettu vastaanottamaan pulsseja, on kalibroinnin tulo-/lähtösignaalijohdin asetettava lähetystilaan tai palautettava ’ei käytössä’ -tilaan.

CPR_061 Komentosarjaan on kuuluttava seuraavat toimet:

— Luodaan viestintäyhteys StartCommunication-palvelun avulla.

— Siirrytään säätöjaksoon StartDiagnosticSession-palvelun avulla ja asetetaan laite KALIBROINTI-toimintatilaan (nämä kaksi tointa voidaan suorittaa kummassa järjestyksessä hyvänsä).

— Vaihdetaan lähtösignaalitila tulosignaalitilaksi InputOutputControlByIdentifier-palvelun avulla.

7.1.2 *Viestin muoto*

CPR_062 InputOutputControlByIdentifier-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

▼B

Taulukko 33

InputOutputControlByIdentifierr-palvelupyynnön sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	xx	LEN
#5	**inputOutputControlByIdentifier-palvelupyynnön tunniste**	**2F**	**IOCBI**
#6 ja #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 tai #8–#9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter – arvo taulukosta 36	xx	IOCP_…
	controlState – arvo taulukosta 37 (ks. huomautus)]	xx	CS_…
#9 tai #10	Tarkistussumma	00-FF	CS

Huomautus: controlState-parametria käytetään vain tietyissä tapauksissa (ks. 7.1.3).

Taulukko 34

InputOutputControlByIdentifier-palvelupyyntöön annettavan myöntävän vastauksen sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	xx	LEN
#5	**inputOutputControlByIdentifier-palvelupyyntöön annettavan myöntävän vastauksen tunniste**	**6F**	**IOCBIPR**
#6 ja #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 tai #8–#9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (sama arvo kuin tavulla #8, taulukko 33)	xx	IOCP_…
	controlState (sama arvo kuin tavulla #9, taulukko 33)] (tarvittaessa)	xx	CS_…
#9 tai #10	Tarkistussumma	00-FF	CS

▼B

Taulukko 35

InputOutputControlByIdentifier-palvelupyyntöön annettavan kieltävän vastauksen sisältävä viesti

Tavun #	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	**Palvelupyyntöön annettavan kieltävän vastauksen tunniste**	**7F**	**NR**
#6	inputOutputControlByIdentifier-palvelupyynnön tunniste	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Tarkistussumma	00-FF	CS

7.1.3 *Parametrien määrittely*

CPR_064 ***inputOutputControlParameter (IOCP_)*** -parametri on määritelty seuraavassa taulukossa.

Taulukko 36

InputOutputControlParameter-parametrin arvojen määritelmät

Hex	Kuvaus	Muistikas
00	**ReturnControlToECU** Tämä arvo osoittaa palvelimelle (ajoneuvoyksikkö), että testauslaite ei enää ohjaa kalibroinnin tulo-/lähtösignaalijohdinta.	RCTECU
01	**ResetToDefault** Tämä arvo osoittaa palvelimelle (ajoneuvoyksikölle), että sitä pyydetään asettamaan kalibroinnin tulo-/lähtösignaalijohdin oletusarvoiseen tilaansa.	RTD

▼B

Hex	Kuvaus	Muistikas
03	**ShortTermAdjustment** Tämä arvo osoittaa palvelimelle (ajoneuvoyksikölle), että sitä pyydetään asettamaan kalibroinnin tulo-/lähtösignaalijohdin controlState-parametrin sisältämän arvon mukaiseksi.	STA

CPR_065 **ControlState**-parametria käytetään vain, kun inputOutputControlParameter-parametri on asetettu arvoon ShortTermAdjustment, ja se on määritelty seuraavassa taulukossa:

Taulukko 37

ControlState-parametrin arvojen määritelmät

Tila	Arvo (Hex)	Kuvaus
Ei käytössä	00	Tulo-/lähtösignaalijohdin ei käytössä (oletusarvo)
Käytössä	01	Kalibroinnin tulo-/lähtösignaalijohdin käytössä tilassa speedSignalInput
Käytössä	02	Kalibroinnin tulo-/lähtösignaalijohdin käytössä tilassa realTimeSpeedSignalOutputSensor
Käytössä	03	Kalibroinnin tulo-/lähtösignaalijohdin käytössä tilassa RTCOutput

8. DATATIETUEIDEN MUOTO

Tämä kohta sisältää:

— yleissäännöt, joita on sovellettava ajoneuvoyksikön testauslaitteelle lähettämiin parametriarvoihin,

— formaatit, joita kohdassa 6 kuvattujen tiedonsiirtopalvelujen kautta siirretyn datan on noudatettava.

CPR_067 Ajoneuvoyksikön on tuettava kaikkia yksilöityjä parametreja.

CPR_068 Ajoneuvoyksikön testauslaitteelle vastauksena pyyntöön lähettämän datan on oltava mitattua tyyppiä (eli vastattava ajoneuvoyksikön mittaamaa tai toteamaan pyydetyn parametrin arvoa).

8.1. **Lähetettävät parametriarvot**

CPR_069 Taulukossa 38 määritellään alueet, joiden perusteella lähetetyn parametrin kelpoisuus määritellään.

CPR_070 Alueella ’error indicator’ olevien arvojen avulla ajoneuvoyksikkö voi heti ilmoittaa, että oikeita parametritietoja ei kyseisellä hetkellä ole saatavissa tallennuslaitteen virheen vuoksi.

CPR_071 Alueella ’not available’ olevien arvojen avulla ajoneuvoyksikkö voi lähettää viestin, joka sisältää sellaisen parametrin, jota ei ole saatavilla tai jota ei tueta kyseisessä laitteessa. Alueella ’not requested’ olevien arvojen avulla laite voi lähettää komentoviestin ja osoittaa ne parametrit, joihin ei odoteta vastausta vastaanottavalta laitteelta.

▼B

CPR_072 Jos komponenttivirhe estää parametria koskevan oikean tiedon lähettämisen, parametrin tiedon sijasta olisi käytettävä virhekoodia taulukossa 38 kuvatulla tavalla. Jos mitattu tai laskettu data on kuitenkin tuottanut arvon, joka on periaatteessa kelvollinen, mutta asetetun arvoalueen ulkopuolella, virhekoodia ei tulisi käyttää. Data olisi lähetettävä käyttäen parametrin asianmukaista vähimmäis- tai enimmäisarvoa.

Taulukko 38

DataRecords-parametrien arvoalueet

Alueen nimi	1 tavu Arvo (Hex)	2 tavua Arvo (Hex)	4 tavua Arvo (Hex)	ASCII
Kelvollinen signaali	00-FA	0000-FAFF	00000000-FAFFFFFF	1–254
Parametrikohtainen osoitin	FB	FB00-FBFF	FB000000-FBFFFFFF	ei ole
Tuleville osoitinbiteille varattu alue	FC-FD	FC00-FDFF	FC000000-FDFFFFFF	ei ole
Virhekoodi	FE	FE00-FEFF	FE000000-FEFFFFFF	0
Ei saatavilla tai ei pyydetty	FF	FF00-FFFF	FF000000-FFFFFFFF	FF

CPR_073 ASCII-koodattujen parametrien erottimeksi varataan ASCII-merkki ”*”.

8.2. **Datatietueiden muoto**

Alla Taulukoissa 39–42 kuvataan muodot, joita on käytettävä ReadDataByIdentifier- ja WriteDataByIdentifier-palveluissa.

CPR_074 Taulukossa 39 ilmoitetaan recordDataIdentifier-tunnisteen ilmoittamien parametrien pituus, tarkkuus ja käyttöalue.

Taulukko 39

Datatietueiden muoto

Parametri	Datan pituus (tavua)	Tarkkuus	Käyttöalue
TimeDate	8	Ks. tiedot taulukossa 40	
HighResolutionTotalVehicleDistance	4	5 m/bit, lähtöarvo 0 m	0–21 055 406 km
Kfactor	2	0,001 pulssia/m/bit, lähtöarvo 0	0–64,255 pulssia/m
LfactorTyreCircumference	2	0,125 10^{-3} m/bit, lähtöarvo 0	0–8,031 m
WvehicleCharacteristicFactor	2	0,001 pulssia/m/bit, lähtöarvo 0	0–64,255 pulssia/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Ks. tiedot taulukossa 41	
SpeedAuthorised	2	1/256 km/h/bit, lähtöarvo 0	0–250,996 km/h

▼B

Parametri	Datan pituus (tavua)	Tarkkuus	Käyttöalue
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Ks. tiedot taulukossa 42	
VIN	17	ASCII	ASCII

CPR_075 Taulukossa 40 kuvataan TimeDate-parametrin tavujen muoto:

Taulukko 40

TimeDate-parametrin muoto (recordDataIdentifier-parametri arvo # F90B)

Tavu	Parametrien määrittely	Tarkkuus	Käyttöalue
1	sekunnit	0,25 s/bit, lähtöarvo 0 s	0–59,75 s
2	minuutit	1 min/bit, lähtöarvo 0 min	0–59 min
3	tunnit	1 h/bit, lähtöarvo 0 h	0–23 h
4	kuukausi	1 kk/bit, lähtöarvo 0 kk	1–12 kuukautta
5	päivä	0,25 päivää/bit, lähtöarvo 0 päivää (ks. huomautus, taulukko 41)	0,25–31,75 päivää
6	vuosi	1 vuosi/bit, lähtöarvo vuosi 1985 (ks. huomautus, taulukko 41)	1985–2235 (vuosi)
7	paikallinen minuuttipoikkeama	1 min/bit, – lähtöarvo 125 min	– 59–59 min
8	paikallinen tuntipoikkeama	1 h/bit, lähtöarvo 125 h	– 23– +23 h

CPR_076 Taulukossa 41 kuvataan NextCalibrationDate-parametrin tavujen muoto:

Taulukko 41

NextCalibrationDate-parametrin muoto (recordDataIdentifier-parametrin arvo # F922)

Tavu	Parametrien määrittely	Tarkkuus	Käyttöalue
1	kuukausi	1 kk/bit, lähtöarvo 0 kk	1–12 kuukautta
2	päivä	0,25 päivää/bit, lähtöarvo 0 päivää (ks. huomautus)	0,25–31,75 päivää
3	vuosi	1 vuosi/bit, lähtöarvo vuosi 1985 (ks. huomautus)	1985–2235 (vuosi)

▼B

Huomautus päiväparametrin käytöstä:

1) 0 päivämäärän arvona merkitsee tyhjää. Arvoja 1, 2, 3 ja 4 käytetään ilmaisemaan kuukauden ensimmäistä päivää, arvoja 5, 6, 7 ja 8 ilmaisemaan kuukauden toista päivää jne.

2) Tämä parametri ei vaikuta tuntiparametriin.

Huomautus vuosiparametrin käytöstä:

0 vuoden arvona merkitsee vuotta 1985, arvo 1 merkitsee vuotta 1986 jne.

CPR_078 Taulukossa 42 kuvataan VehicleRegistrationNumber-parametrin tavujen muoto:

Taulukko 42

VehicleRegistrationNumber-parametrin muoto (recordDataIdentifier-parametrin arvo # F97E)

Tavu	Parametrien määrittely	Tarkkuus	Käyttöalue
1	Koodisto (Code Page, lisäyksen 1 mukaisesti)	ASCII	01–0An
2–14	Ajoneuvon rekisterinumero (lisäyksen 1 mukaisesti)	ASCII	ASCII

▼B

Lisäys 9

TYYPPIHYVÄKSYNTÄ JA LUETTELO VÄHINTÄÄN VAADITTAVISTA TESTEISTÄ

SISÄLLYSLUETTELO

1. JOHDANTO

2. AJONEUVOYKSIKÖN TOIMINNALLISET TESTIT

3. LIIKETUNNISTIMEN TOIMINNALLISET TESTIT

4. AJOPIIRTURIKORTTIEN TOIMINNALLISET TESTIT

5. ULKOISEEN GNSS-LAITTEISTOON LIITTYVÄT TESTIT

6. ETÄYHTEYSLAITTEISTOON LIITTYVÄT TESTIT

7. PAPERIN TOIMINNALLISET TESTIT

8. YHTEENTOIMIVUUSTESTAUS

1. JOHDANTO

1.1. **Tyyppihyväksyntä**

Valvontalaitteen (tai sen osan) EY-tyyppihyväksyntä perustuu seuraaviin sertifiointeihin:

— **tietoturvasertifiointi**, joka perustuu Common Criteria -eritelmiin käyttäen vertailukohtana tietoturvatavoitetta, joka on täysin tämän liitteen lisäyksen 10 mukainen (täydennettävä/muutettava),

— **toiminnallinen sertifiointi**, jonka tekee jäsenvaltion viranomainen antamalla todistuksen siitä, että koestettu laite täyttää tämän lisäyksen vaatimukset, jotka koskevat suoritettuja toimintoja, mittaustarkkuutta ja ympäristönsuojeluun liittyviä ominaisuuksia,

— **yhteentoimivuuden sertifiointi**, jonka tekee toimivaltainen elin antamalla todistuksen siitä, että valvontalaite (tai ajopiirturikortti) on täysin yhteentoimiva vaadittavien ajopiirturikorttimallien (tai valvontalaitemallien) kanssa (ks. tämän lisäyksen 8 luku).

Tässä lisäyksessä määritellään ne testit, jotka jäsenvaltion viranomaisen on vähintään tehtävä toiminnallisuutta koestettaessa, ja testit, jotka toimivaltaisen elimen on vähintään tehtävä yhteentoimivuutta koestettaessa. Testejä tehtäessä käytettäviä menettelyjä ei ole määritelty tätä yksityiskohtaisemmin.

Tässä lisäyksessä ei käsitellä tietoturvasertifiointiin liittyviä asioita. Jos jotkin tyyppihyväksyntää varten tarvittavat testit tehdään tietoturva-arvioinnin ja -sertifioinnin yhteydessä, niitä ei tarvitse tehdä uudelleen. Tässä tapauksessa riittää, että tarkastetaan kyseisten tietoturvatestien tulokset. Yleisenä ohjeena voidaan sanoa, että ne vaatimukset, joiden täyttämistä voidaan olettaa testattavan (tai jotka läheisesti liittyvät testeihin, jotka voidaan olettaa tehtäväksi) tietoturvatestien yhteydessä, on tässä liitteessä merkitty tähdellä (*).

Numeroidut vaatimukset viittaavat liitteen tekstiin ja muut vaatimukset muihin lisäyksiin (esim. PIC 001 viittaa lisäyksessä 3 (Kuvakkeet) olevaan vaatimukseen PIC 001.

Tässä lisäyksessä käsitellään liiketunnistimen, ajoneuvoyksikön ja ulkoisen GNSS-laitteiston tyyppihyväksyntää erikseen valvontalaitteen osina. Jokainen osa saa oman tyyppihyväksyntätodistuksensa, jossa ilmoitetaan muut

▼B

yhteensopivat osat. Liiketunnistimen (tai ulkoisen GNSS-laitteiston) toiminnallinen testi tehdään yhdessä ajoneuvoyksikön kanssa ja päinvastoin.

Kaikkien liiketunnistinmallien (ja vastaavasti GNSS-laitteistomallien) ja kaikkien ajoneuvoyksikkömallien välistä yhteentoimivuutta ei vaadita. Siinä tapauksessa liiketunnistimen (tai ulkoisen GNSS-laitteiston) tyyppihyväksyntä voidaan myöntää vain ajoneuvoyksikön tyyppihyväksynnän kanssa ja päinvastoin.

1.2. **Viitetiedot**

Tässä lisäyksessä käytetään seuraavia viitetietoja:

IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold

IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat (sinusoidal).

IEC 60068-2-6: Environmental testing – Part 2: Tests – Test Fc: Vibration

IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature

IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock

IEC 60068-2-30: Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)

IEC 60068-2-64: Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance

IEC 60068-2-78 Environmental testing – Part 2-78: Tests – Test Cab: Damp heat, steady state

ISO 16750-3 – Mechanical loads (2012-12)

ISO 16750-4 – Climatic loads(2010-04).

ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access

ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014 Road vehicles – Test methods for electrical disturbances from electrostatic discharge

ISO 7637-1:2002 + AMD1: 2008 Road vehicles – Electrical disturbances from conduction and coupling – Part 1: Definitions and general considerations.

ISO 7637-2 Road vehicles – Electrical disturbances from conduction and coupling – Part 2: Electrical transient conduction along supply lines only.

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.

ISO/IEC 7816-1 Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics..

▼B

ISO/IEC 7816-2 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts.

ISO/IEC 7816-3 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol.

ISO/IEC 10373-1:2006 + AMD1:2012 Identification cards – Test methods – Part 1: General characteristics

ISO/IEC 10373-3:2010 + Technical Corrigendum:2013 Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices

ISO 16844-3:2004, Cor 1:2006 Road vehicles – Tachograph systems – Part 3: Motion sensor interface (with vehicle units).

ISO 16844-4 Road vehicles – Tachograph systems – Part 4: CAN interface

ISO 16844-6 Road vehicles – Tachograph systems – Part 6: Diagnostics

ISO 16844-7 Road vehicles – Tachograph systems – Part 7: Parameters

ISO 534 Paper and board – Determination of thickness, density and specific volume

UN ECE R10 Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility (United Nation Economic Commission for Europe)

2. AJONEUVOYKSIKÖN TOIMINNALLISET TESTIT

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
1	**Hallinnollinen tarkastus**		
1.1	Asiakirjat	Kirjallisen aineiston oikeellisuus	
1.2	Valmistajan testitulokset	Valmistajan kokoonpanovaiheessa suorittaman testin tulokset. Kirjalliset todisteet	88, 89,91
2	**Silmämääräinen tarkastus**		
2.1	Yhtäpitävyys kirjallisen aineiston kanssa		
2.2	Tunniste/merkinnät		224–226
2.3	Materiaalit		219–223
2.4	Sinetöinti		398, 401–405
2.5	Ulkoiset liitäntälaitteet		
3	**Toiminnalliset testit**		
3.1	Laitteessa mukana olevat toiminnot		03, 04, 05, 07, 382,
3.2	Toimintatilat		09–11*, 132, 133
3.3	Toiminnot ja tietojen käyttöoikeudet		12* 13*, 382, 383, 386–389
3.4	Korttien paikoilleen asettamisen ja poistamisen seuranta		15, 16, 17, 18, 19*, 20*, 132
3.5	Nopeuden ja matkan mittaus		21–31

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
3,6	Ajan mittaus (20 celsiusasteessa tehtävä testi)		38–43
3.7	Kuljettajan toiminnan seuranta		44–53, 132
3.8	Ajoneuvon miehityksen seuranta		54, 55, 132
3.9	Tietojen syöttö käsin		56–62
3.10	Yritysten tekemien lukitusten hallinta		63–68
3.11	Tarkastustoimien seuranta		69, 70
3.12	Tapahtumien ja/tai vikojen havaitseminen		71–88, 132
3.13	Laitteen tunnistetiedot		93*, 94*, 97, 100
3.14	Kuljettajakortin paikoilleen asettamiseen ja poistamiseen liittyvät tiedot		102*–104*
3.15	Kuljettajan toimintaan liittyvät tiedot		105*–107*
3.16	Paikkoihin ja sijainteihin liittyvät tiedot		108*–112*
3.17	Matkamittariin liittyvät tiedot		113*–115*
3.18	Nopeuteen liittyvät yksityiskohtaiset tiedot		116*
3.19	Tapahtumiin liittyvät tiedot		117*
3.20	Vikoihin liittyvät tiedot		118*
3.21	Kalibrointiin liittyvät tiedot		119*–121*
3.22	Ajan asetukseen liittyvät tiedot		124*, 125*
3.23	Tarkastustoimiin liittyvät tiedot		126*, 127*
3.24	Yritysten tekemiin lukituksiin liittyvät tiedot		128*
3.25	Tietojen kopiointitapahtumiin liittyvät tiedot		129*
3.26	Erityisolosuhteisiin liittyvät tiedot		130*, 131*
3.27	Tietojen tallennus ja säilytys ajopiirturikorteilla		134, 135,, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Tietojen näyttö		90, 132, 149–166, PIC_001, DIS_001
3.29	Tulostus		90, 132, 167–179, PIC_001, PRT_001–PRT_014
3.30	Varoitukset		132, 180–189, PIC_001
3.31	Tietojen kopioiminen ulkoisille tietovälineille		90, 132, 190–194
3.32	Kohdistettuihin tienvarsitarkastuksiin liittyvä etäviestintä		195–197
3.33	Tietojen tulostus ulkoisille lisälaitteille		198, 199

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
3.34	Kalibrointi		202–206*, 383, 384, 386–391
3.35	Kalibroinnin tarkastus tien varrella		207–209
3.36	Ajan asetus		210–212*
3.37	Lisätoimintojen aiheuttamat häiriöt		06, 425
3.38	Liiketunnistimen rajapinta		02, 122
3.39	Ulkoinen GNSS-laitteisto		03, 123
3.40	Todennetaan, että ajoneuvoyksikkö havaitsee, tallentaa ja säilyttää ajoneuvoyksikön valmistajan määrittelemän tapahtuman (tapahtumat) ja/tai vian (viat), kun siihen liitetty liiketunnistin reagoi ajoneuvon liikkeen havaitsemista häiritseviin magneettikenttiin.		217
3.41	Salaussarja ja vakiomuotoiset domain-parametrit		CSM_48, CSM_50
4	**Ympäristötestit**		
4.1	Lämpötila	Todennetaan laitteen toiminta seuraavissa oloissa: Testataan standardin ISO 16750-4, Chapter 5.1.1.2: Low temperature operation test vaatimusten mukaisesti (72 h lämpötilassa – 20 °C) Tämä testi viittaa standardiin IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold Testataan standardin ISO 16750-4: Chapter 5.1.2.2: High temperature operation test mukaisesti (72 h lämpötilassa 70 °C) Tämä testi viittaa standardiin IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Testataan standardin ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration vaatimusten mukaisesti (– 20 °C/70 °C, 20 jaksoa, viipymisaika 2 h jokaisessa lämpötilassa) Alimmassa ja korkeimmassa lämpötilassa sekä lämpötilan muutosjaksojen aikana voidaan tehdä rajoitettu testisarja (joka sisältää tämän taulukon osassa 3 olevia testejä)	213
4.2	Kosteus	Todennetaan, että ajoneuvoyksikkö sietää jaksoittaista kosteutta (lämpötesti) tekemällä standardin IEC 60068-2-30 mukainen testi Db, kuusi 24 tunnin jaksoa, joista jokaisessa lämpötila vaihtelee välillä + 25 °C … + 55 °C ja suhteellinen kosteus on 97 % lämpötilassa + 25 °C ja 93 % lämpötilassa + 55 °C	214

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
4.3	Mekaaninen	1. Sinimuotoinen tärinä: Todennetaan, että ajoneuvoyksikkö sietää sinimuotoista tärinää, jolla on seuraavat ominaisuudet: vakioamplitudi taajuusalueella 5–11 Hz: 10 mm huipusta huippuun mitattuna vakiokiihtyvyys taajuusalueella 11–300 Hz: 5 g Tämän vaatimuksen täyttäminen todennetaan tekemällä standardin IEC 60068-2-6 mukainen testi Fc, vähimmäiskestoltaan 3 × 12 tuntia (12 tuntia kutakin akselia kohden) ISO 16750-3 ei edellytä sinimuotoista tärinätestiä ajoneuvon irrotetussa hytissä oleville laitteille. 2. Satunnainen tärinä Testataan standardin ISO 16750-3: Chapter 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab vaatimusten mukaisesti Satunnaisen tärinän testi, 10–2 000 Hz, vertikaalinen tehollisarvo (RMS) 21,3 m/s^2, pitkittäinen tehollisarvo 11,8 m/s^2, poikittainen tehollisarvo 13,1 m/s^2, 3 akselia, 32 h akselia kohti, mukaan lukien lämpötilajakso – 20 … 70 °C. Tämä testi viittaa standardiin IEC 60068-2-64: Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance 3. Iskut: 3 gramman puolisinimuotoinen mekaaninen isku standardin ISO 16750 vaatimusten mukaisesti. Edellä kuvatut testit tehdään kahdelle eri näytteelle, jotka edustavat testattavaa laitetyyppiä.	219
4.4	Suojaus vettä ja vieraita esineitä vastaan	Testataan standardin ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access vaatimusten mukaisesti (Ei muutoksia parametreissa); vähimmäisarvo IP 40	220, 221
4.5	Ylijännitesuojaus	Todennetaan, että ajoneuvoyksikkö sietää seuraavia käyttöjännitteitä: 24 V:n mallit: 34 V lämpötilassa + 40 °C 1 tunnin ajan 12 V:n mallit: 17 V lämpötilassa + 40 °C 1 tunnin ajan (ISO 16750-2)	216

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
4.6	Suojaus väärää napaisuutta vastaan	Todennetaan, että ajoneuvoyksikkö sietää virtalähteen napojen vaihtamisen toisin päin (ISO 16750-2)	216
4.7	Oikosulkusuojaus	Todennetaan, että laitteen tulo- ja lähtösignaalit on suojattu oikosululta käyttöjännitettä ja maata vastaan (ISO 16750-2)	216
5	**Sähkömagneettisen yhteensopivuuden (EMC) testaus**		
5.1	Laitteen tuottama säteily ja magneettinen vastaanottavuus	Asetuksen ECE R10 vaatimusten noudattaminen	218
5.2	Staattisen sähkön purkaukset	Standardin ISO 10605:2008 + teknisen oikaisun Technical Corrigendum: 2010 + tarkistuksen 1:2014 vaatimusten noudattaminen: +/– 4kV kontakti ja +/– 8kV ilma	218
5.3	Virtajohtimia pitkin tulevien jännitepiikkien sietokyky	24 V:n mallit: standardin ISO 7637-2 + ECE-asetuksen nro 10 version 3 noudattaminen: pulssi 1a: Vs = – 450V, Ri = 50 ohmia pulssi 2a: Vs = + 37V, Ri = 2 ohmia pulssi 2b: Vs = + 20V, Ri = 0,05 ohmia pulssi 3a: Vs = – 150V, Ri = 50 ohmia pulssi 3b: Vs = + 150V, Ri = 50 ohmia pulssi 4: Vs = – 16V, Va = – 12V, t6 = 100 ms pulssi 5: Vs = + 120V, Ri = 2,2 ohmia, td = 250 ms 12 V:n mallit: standardin ISO 7637-1 + ECE-asetuksen nro 10 version 3 noudattaminen: pulssi 1: Vs = -75V, Ri = 10 ohmia pulssi 2a: Vs = + 37V, Ri = 2 ohmia pulssi 2b: Vs = + 10V, Ri = 0,05 ohmia pulssi 3a: Vs = – 112V, Ri = 50 ohmia pulssi 3b: Vs = + 75V, Ri = 50 ohmia pulssi 4: Vs = – 6V, Va = – 5V, t6 = 15 ms pulssi 5: Vs = + 65V, Ri = 3 ohmia, td = 100 ms Pulssin 5 sietokyky testataan vain ajoneuvoyksiköillä, jotka on tarkoitettu asennettavaksi ajoneuvoihin, joissa ei ole erillistä suojausta sähköisen kuormituksen äkillisen katkeamisen varalta Katso sähköisen kuormituksen äkillistä katkeamista koskeva ehdotus standardista ISO 16750-2, neljäs painos, luku 4.6.4.	218

▼B

3. LIIKETUNNISTIMEN TOIMINNALLISET TESTIT

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
1.	**Hallinnollinen tarkastus**		
1.1	Asiakirjat	Kirjallisen aineiston oikeellisuus	
2.	**Silmämääräinen tarkastus**		
2.1.	Yhtäpitävyys kirjallisen aineiston kanssa		
2.2.	Tunniste/merkinnät		225, 226,
2.3	Materiaalit		219–223
2.4.	Sinetöinti		398, 401–405
3.	**Toiminnalliset testit**		
3.1	Liiketunnistimen tunnistetiedot		95–97*
3.2	Liiketunnistimen liittäminen ajoneuvoyksikköön		122*, 204
3.3	Liikkeen havaitseminen Liikkeen mittauksen tarkkuus		30–35
3.4	Ajoneuvoyksikön rajapinta		02
3.5	Tarkastetaan, ettei liiketunnistin reagoi jatkuvaan magneettikenttään. Vaihtoehtoisesti todennetaan, että liiketunnistin reagoi ajoneuvon liikkeen havaitsemista häiritseviin jatkuviin magneettikenttiin, niin että liiketunnistimeen liitetty ajoneuvoyksikkö pystyy havaitsemaan, tallentamaan ja säilyttämään liiketunnistimen viat		217
4.	**Ympäristötestit**		
4.1	Käyttölämpötila	Todennetaan toiminnallisuus (niin kuin se on määritelty testin 3.3 kohdalla) lämpötila-alueella [– 40 °C … + 135 °C] tekemällä standardin IEC 60068-2-1 mukainen testi Ad kestoltaan 96 tuntia alimmassa lämpötilassa To_{min} standardin IEC 60068-2-2 mukainen testi Bd kestoltaan 96 tuntia ylimmässä lämpötilassa To_{max} Testataan standardin ISO 16750-4: Chapter 5.1.1.2: Low temperature operation test vaatimusten mukaisesti (24 h lämpötilassa – 40 °C) Tämä testi viittaa standardiin IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold IEC 68-2-2 mukaiseen testiin Bd, kestoltaan 96 tuntia alimmassa lämpötilassa – 40 °C. Testataan standardin ISO 16750-4: Chapter 5.1.2.2: High temperature operation test vaatimusten mukaisesti (96 h lämpötilassa 135 °C) Tämä testi viittaa standardiin IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat	213

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
4.2	Lämpötilan jaksoittainen vaihtelu	Testataan standardin ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (– 40 °C/135 °C, 20 jaksoa, viipymisaika 30 min jokaisessa lämpötilassa) ja standardin IEC 60068-2-14: Environmental testing – Part 2-14: Tests; Test N: vaatimusten mukaisesti Lämpötilan vaihtelu	213
4.3	Kosteuden jaksoittainen vaihtelu	Todennetaan toiminnallisuus (niin kuin se on määritelty testin 3.3 kohdalla) tekemällä standardin IEC 60068-2-30 mukainen testi Db, kuusi 24 tunnin jaksoa, joista jokaisessa lämpötila vaihtelee välillä + 25 °C … + 55 °C ja suhteellinen kosteus on 97 % lämpötilassa + 25 °C ja 93 % lämpötilassa + 55 °C	214
4.4	Tärinä	ISO 16750-3 Chapter 4.1.2.6: Test VI: Commercial vehicle, engine, gearbox Yhdistetyn tilan tärinätesti, mukaan lukien a) sinimuotoisen tärinän testi, 20–520 Hz, 11,4–120 m/s^2, <= 0,5 oktaavia/min b) satunnaisen tärinän testi, 10–2 000 Hz, tehollisarvo 177 m/s^2 94 h akselia kohti, mukaan lukien lämpötilajakso – 20 …70°C) Tämä testi viittaa standardiin IEC 60068-2-80: Environmental testing – Part 2-80: Tests – Test Fi: Vibration – Mixed mode	219
4.5	Mekaaniset iskut	ISO 16750-3 Chapter 4.2.3: Test VI: Test for devices in or on the gearbox Puolisinimuotoinen isku, kiihtyvyys sovittava alueelle 3 000–15 000 m/s^2, pulssin kesto sovittava, joka tapauksessa < 1 ms, iskujen määrä: sovittava Tämä testi viittaa standardiin IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock	219
4.6	Suojaus vettä ja vieraita esineitä vastaan	Testataan standardin ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access vaatimusten mukaisesti (kohdearvo IP 64)	220, 221
4.7	Suojaus väärää napaisuutta vastaan	Todennetaan, että liiketunnistin sietää virtalähteen napojen vaihtamisen toisin päin	216
4.8	Oikosulkusuojaus	Todennetaan, että laitteen tulo- ja lähtösignaalit on suojattu oikosululta käyttöjännitettä ja maata vastaan	216

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
5.	**Sähkömagneettinen yhteensopivuus**		
5.1	Laitteen tuottama säteily ja magneettinen vastaanottavuus	Todennetaan asetuksen ECE R10 vaatimusten noudattaminen	218
5.2	Staattisen sähkön purkaukset	Standardin ISO 10605:2008 + teknisen oikaisun Technical Corrigendum: 2010 + tarkistuksen 1:2014 noudattaminen: +/– 4kV kontakti ja +/– 8kV ilma	218
5.3	Datakaapeleita pitkin tulevien jännitepiikkien sietokyky	24 V:n mallit: standardin ISO 7637-2 + ECE-asetuksen nro 10 version 3 noudattaminen: pulssi 1a: Vs = – 450V, Ri = 50 ohmia pulssi 2a: Vs = + 37V, Ri = 2 ohmia pulssi 2b: Vs = + 20V, Ri = 0,05 ohmia pulssi 3a: Vs = – 150V, Ri = 50 ohmia pulssi 3b: Vs = + 150V, Ri = 50 ohmia pulssi 4: Vs = – 16V, Va = – 12V, t6 = 100 ms pulssi 5: Vs = + 120V, Ri = 2,2 ohmia, td = 250 ms 12 V:n mallit: standardin ISO 7637-1 + ECE-asetuksen nro 10 version 3 noudattaminen: pulssi 1: Vs = – 75V, Ri = 10 ohmia pulssi 2a: Vs = + 37V, Ri = 2 ohmia pulssi 2b: Vs = + 10V, Ri = 0,05 ohmia pulssi 3a: Vs = – 112V, Ri = 50 ohmia pulssi 3b: Vs = + 75V, Ri = 50 ohmia pulssi 4: Vs = – 6V, Va = – 5V, t6 = 15 ms pulssi 5: Vs = + 65V, Ri = 3 ohmia, td = 100 ms Pulssin 5 sietokyky testataan vain ajoneuvoyksiköillä, jotka on tarkoitettu asennettavaksi ajoneuvoihin, joissa ei ole erillistä suojausta sähköisen kuormituksen äkillisen katkeamisen varalta Katso sähköisen kuormituksen äkillistä katkeamista koskeva ehdotus standardista ISO 16750-2, 4. painos, luku 4.6.4	218

4. AJOPIIRTURIKORTTIEN TOIMINNALLISET TESTIT

Tämän 4 kohdan mukaiset testit

nro 5 Tiedonsiirtoprotokolliin liittyvät testi

nro 6 Valvontakortin tiedostorakenne ja

nro 7 Toiminnalliset testit

voi suorittaa arvioija tai sertifioija mikrosiruyksikön Common Criteria (CC) -tietoturvasertifiointiprosessin aikana.

Testit numero 2.3 ja 4.2 ovat samoja. Ne ovat korttirungon ja mikrosiruyksikön yhdistelmän mekaanisia testejä. Jos toista näistä osista (korttirunko, mikrosiruyksikkö) muutetaan, testit on tehtävä.

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
1.	**Hallinnollinen tarkastus**		
1.1	Asiakirjat	Kirjallisen aineiston oikeellisuus	
2	**Korttirunko**		
2.1	Painatus	Varmistetaan, että turvakuviointi ja näkyviksi tarkoitetut tiedot on painettu korttiin oikein ja vaatimusten mukaisesti [Tunnus] Liite 1C, luku 4.1, Näkyvissä olevat tiedot, 227) Etupuolella on oltava kortin tyypin mukaan sana ”kuljettajakortti” tai ”valvontakortti” tai ”korjaamokortti” tai ”yrityskortti” painettuna suurikokoisin kirjaimin kortin myöntävän jäsenvaltion virallisella kielellä tai kielillä; [Jäsenvaltion nimi] Liite 1C, luku 4.1, Näkyvissä olevat tiedot, 228) Etupuolella on oltava kortin myöntävän jäsenvaltion nimi (vapaaehtoinen merkintä); [Maatunnus] Liite 1C, luku 4.1, Näkyvissä olevat tiedot, 229) Etupuolella on oltava kortin myöntävän jäsenvaltion kansainvälinen tunnus negatiivina sinisessä suorakulmiossa ja kahdentoista keltaisen tähden ympäröimänä. [Numerointi] Liite 1C, luku 4.1, Näkyvissä olevat tiedot, 232) Kääntöpuolella on oltava kortin etupuolella olevien numeroitujen kohtien selitykset; [Väri] Liite 1C, luku 4.1, Näkyvissä olevat tiedot, 234) Ajopiirturikortit on painettava käyttäen seuraavia hallitsevia taustavärejä: — kuljettajakortti: valkoinen, — korjaamokortti: punainen, — valvontakortti: sininen, — yrityskortti: keltainen.	227–229, 232, 234–236

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
		[Turvallisuus] Liite 1C, luku 4.1, Näkyvissä olevat tiedot, 235) Ajopiirturikorteilla on oltava ainakin seuraavat ominaisuudet, jotka suojaavat niitä väärentämiseltä ja vilpilliseltä käsittelyltä: — turvakuviointi, jossa on ohut aaltomainen viivakuvio ja iirispainatus, — ainakin yksi kaksiväristä mikrokirjoitusta sisältävä rivi.	
		[Merkinnät] Liite 1C, luku 4.1, Näkyvissä olevat tiedot, 236 Jäsenvaltiot voivat lisätä korttiin värejä tai merkintöjä, kuten kansallisia tunnuksia ja turvallisuutta lisääviä ominaisuuksia.	
		[Tyyppihyväksyntämerkki] Ajopiirturikortissa on oltava tyyppihyväksyntämerkki. Tyyppihyväksyntämerkki muodostuu — suorakulmiosta, jonka sisälle on sijoitettu pieni ”e”-kirjain ja sen jäljessä tyyppihyväksynnän antaneen maan tunnusnumero tai -kirjain, — ajopiirturikortin tyyppihyväksyntätodistuksen numeroa vastaava hyväksyntänumero sijoitettuna johonkin tämän suorakulmion vieressä olevaan kohtaan.	
2.2	Mekaaniset testit	[Kortin koko] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.1] Card dimensions and tolererances, card type ID-1 Unused card vaatimusten mukaisia	240, 243 ISO/IEC 7810
		[Kortin reunat] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.2] Card edges vaatimusten mukaisia	

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
		[Kortin tiedostorakenne] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [6] Card construction vaatimusten mukaisia	
		[Korttimateriaalit] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [7] Card materials vaatimusten mukaisia	
		[Taivutusjäykkyys] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.1] Bending stiffness vaatimusten mukaisia	
		[Myrkyllisyys] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.3] Toxicity vaatimusten mukaisia	
		[Kemikaalinkestävyys] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.4] Resistance to chemicals vaatimusten mukaisia	
		[Kortin säilyvyys] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.5] Card dimensional stability and warpage with temperature and humidity vaatimusten mukaisia	

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
		[Valo] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.6] Light vaatimusten mukaisia	
		[Kestävyys] Liite 1C, luku 4.4, Ympäristöön liittyvät ja sähkötekniset eritelmät, 241) Ajopiirturikorttien on voitava toimia moitteettomasti viiden vuoden ajan, jos niitä käytetään ympäristöön liittyvien ja sähköteknisten eritelmien rajoissa.	
		[Hilseilynkesto] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.8] Peel strength vaatimusten mukaisia	
		[Tarttuminen tai kiinnittyminen] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.9] Adhesion or blocking vaatimusten mukaisia	
		[Vääntyminen] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.11] Overall card warpage vaatimusten mukaisia	
		[Lämmönkestävyys] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.12] Resistance to heat vaatimusten mukaisia	

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
		[Pinnan vääristymät] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.13] Surface distortions vaatimusten mukaisia	
		[Likaantuminen] Ajopiirturikorttien on oltava standardin ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.14] Contamination and interaction of card components vaatimusten mukaisia	
2.3	Mekaaniset testit, kun mikrosiruyksikkö on sulautettu	[Taipuminen] Ajopiirturikorttien on oltava standardin ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress vaatimusten mukaisia Taipumisjaksojen kokonaismäärä: 4 000.	ISO/IEC 7810
		[Vääntyminen] Ajopiirturikorttien on oltava standardin ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress vaatimusten mukaisia Vääntymisjaksojen kokonaismäärä: 4 000.	
3	**Yksikkö**		
3.1	Yksikkö	Yksikkö tarkoittaa mikrosirukoteloa ja kosketuslaattaa [Pintaprofiili] Ajopiirturikorttien on oltava standardin ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.2] Surface profile of contacts vaatimusten mukaisia	ISO/IEC 7816

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
		[Mekaaninen lujuus] Ajopiirturikorttien on oltava standardin ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.3] Mechanical strength (of a card and contacts) vaatimusten mukaisia	
		[Sähkövastus] Ajopiirturikorttien on oltava standardin ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.4] Electrical resistance (of contacts) vaatimusten mukaisia	
		[Mitat] Ajopiirturikorttien on oltava standardin ISO/IEC 7816-2:2007, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts [3] Dimension of the contacts vaatimusten mukaisia	
		[Sijainti] Ajopiirturikorttien on oltava standardin ISO/IEC 7816-2:2007, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts [4] Number and location of the contacts vaatimusten mukaisia Jos kyse on yksiköistä, joissa on kuusi kosketinta, koskettimet C4 ja C8 eivät kuulu tähän testivaatimukseen.	
4	**Mikrosiru**		
4.1	Mikrosiru	[Käyttölämpötila] Ajopiirturikortin mikrosirun on toimittava lämpötila-alueella – 25 °C … + 85 °C.	241–244 ECE R10 ISO/IEC 7810 ISO/IEC 10373

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
		[Lämpötila ja kosteus] Liite 1C, luku 4.4, Ympäristöön liittyvät ja sähkötekniset eritelmät, 241) Ajopiirturikorttien on kyettävä toimimaan moitteettomasti kaikissa yhteisön alueella tavattavissa ilmasto-olosuhteissa sekä vähintään lämpötila-alueella – 25 °C … + 70 °C, jolloin satunnaiset lämpötilahuiput voivat olla jopa + 85 °C, missä satunnainen tarkoittaa enintään neljän tunnin jaksoja kerrallaan enintään sata kertaa kortin käyttöiän aikana. Ajopiirturikortit altistetaan seuraaville lämpötiloille ja kosteuksille peräkkäin ilmoitetuksi ajaksi Ajopiirturikorttien sähkötekninen toiminnallisuus testataan jokaisen vaiheen jälkeen. 1. Lämpötila – 20 °C, 2 h 2. Lämpötila +/– 0 °C, 2 h 3. Lämpötila + 20 °C, suhteellinen kosteus 50 %, 2 h 4. Lämpötila + 50 °C, suhteellinen kosteus 50 %, 2 h 5. Lämpötila + 70 °C, suhteellinen kosteus 50 %, 2 h Lämpötila nostetaan jaksoittaisesti 85 celsiusasteeseen, kun suhteellinen kosteus on 50 %, 60 minuutin ajaksi. 6. Lämpötila + 70 °C, suhteellinen kosteus 85 %, 2 h Lämpötila nostetaan jaksoittaisesti 85 celsiusasteeseen, kun suhteellinen kosteus on 85 %, 30 minuutin ajaksi.	
		[Kosteus] Liite 1C, luku 4.4, Ympäristöön liittyvät ja sähkötekniset eritelmät, 242 Ajopiirturikorttien on voitava toimia moitteettomasti kosteuden ollessa 10–90 %.	
		[Sähkömagneettinen yhteensopivuus] Liite 1C, luku 4.4, Ympäristöön liittyvät ja sähkötekniset eritelmät, 244 Käytön aikana ajopiirturikorttien on oltava sähkömagneettiseen yhteensopivuuteen liittyvän asetuksen ECE R10 mukaisia.	

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
		[Staattinen sähkö] Liite 1C, luku 4.4, Ympäristöön liittyvät ja sähkötekniset eritelmät, 244 Käytön aikana ajopiirturikortit on suojattava sähköstaattisilta purkauksilta. Ajopiirturikorttien on oltava standardin ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.4] Static electricity [9.4.1] Contact IC cards vaatimusten mukaisia Testausjännite: 4 000 V.	
		[Läpivalaisu] Ajopiirturikorttien on oltava standardin ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.1] X-rays vaatimusten mukaisia	
		[Ultraviolettivalo] ISO/IEC 10373-1:2006, Identification cards – Test methods – Part 1: General characteristics [5.11] Ultraviolet light	
		[Kolmivalssi] Ajopiirturikorttien on oltava standardin ISO/IEC 10373-1:2006/Amd. 1:2012, Identification cards – Test methods – Part 1: General characteristics, Amendment 1 [5.22] ICC – Mechanical strength: 3 wheel test for ICCs with contacts vaatimusten mukaisia	
		[Pakkaaminen] Ajopiirturikorttien on oltava standardin MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Wrapping Test Robustness [13.2.1.32] TM-422: Mechanical Reliability: Wrapping Test vaatimusten mukaisia	

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
4.2	Mekaaniset testit, kun mikrosiruyksikkö on sulautettu korttirunkoon -> sama kuin 2.3 kohdassa	[Taipuminen] Ajopiirturikorttien on oltava standardin ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress vaatimusten mukaisia Taipumisjaksojen kokonaismäärä: 4 000. [Vääntyminen] Ajopiirturikorttien on oltava standardin ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress vaatimusten mukaisia Vääntymisjaksojen kokonaismäärä: 4 000.	ISO/IEC 7810
5	**Tiedonsiirtoprotokolliin liittyvät testit**		
5.1	ATR-signaali	Tarkastetaan, että ATR-signaali on vaatimusten mukainen	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Tarkastetaan, että T=0-protokolla on vaatimusten mukainen	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS-komento	Tarkastetaan, että PTS-komento on vaatimusten mukainen, vaihtamalla käytössä oleva protokolla T=0:sta T=1:ksi.	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Tarkastetaan, että T=1-protokolla on vaatimusten mukainen	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Kortin tiedostorakenne**		
6.1		Testataan, että kortin tiedostorakenne on vaatimusten mukainen, tarkastamalla, että kortilla on vaadittavat tiedostot ja että niiden käyttöehdot ovat asianmukaiset	TCS_22–TCS_28 TCS_140–TCS_179
7	**Toiminnalliset testit**		
7.1	Normaali suoritus	Testataan jokaisen komennon jokainen sallittu käyttö vähintään kertaalleen (esim. testataan UPDATE BINARY -komento luokkaa osoittavan CLA-tavun arvolla 00 ja arvolla 0C sekä käyttäen eri arvoja parametreissa P1, P2 ja Lc). Tarkastetaan, että komennon mukaiset toiminnot on todella suoritettu kortilla (esim. lukemalla sen tiedoston tiedot, jota komento koski)	TCS_29–TCS_139

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
7.2	Virheilmoitukset	Testataan jokainen (lisäyksessä 2 määritelty) virheilmoitus vähintään kerran jokaisessa komennossa. Testataan jokainen yleinen virhe vähintään kerran (paitsi datan eheyteen liittyvät virheet, joiden vastauskoodi on **6400** ja jotka tarkastetaan tietoturvasertifioinnin yhteydessä)	
7.3	Salaussarja ja vakiomuotoiset domain-parametrit		CSM_48, CSM_50
8	**Räätälöinti**		
8.1	Optinen räätälöinti	Liite 1C, luku 4.1, Näkyvissä olevat tiedot, 230 Etupuolella on oltava myönnettyä korttia koskevat tiedot. Liite 1C, luku 4.1, Näkyvissä olevat tiedot, 231 Etupuolella on oltava päivämäärät kirjoitettuna muotoon ”pp/kk/vvvv” tai ”pp.kk.vvvv” (päivä, kuukausi, vuosi). Liite 1C, luku 4.1, Näkyvissä olevat tiedot, 235 Ajopiirturikorteilla on oltava ainakin seuraavat ominaisuudet, jotka suojaavat niitä väärentämiseltä ja vilpilliseltä käsittelyltä: — valokuvan kohdalla on taustan turvakuvioinnin ja valokuvan mentävä osittain päällekkäin.	230, 231, 235

5. ULKOISEEN GNSS-LAITTEISTOON LIITTYVÄT TESTIT

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
1.	**Hallinnollinen tarkastus**		
1.1	Asiakirjat	Kirjallisen aineiston oikeellisuus	
2.	**Ulkoisen GNSS-laitteiston silmämääräinen tarkastus**		
2.1.	Yhtäpitävyys kirjallisen aineiston kanssa		
2.2.	Tunniste/merkinnät		224–226
2.3	Materiaalit		219–223
3.	**Toiminnalliset testit**		
3.1	Liiketunnistimen tunnistetiedot		98, 99
3.2	Ulkoisen GNSS-yksikön liittäminen ajoneuvoyksikköön		123, 205

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
3.3	GNSS-sijainti		36, 37
3.4	Ajoneuvoyksikön käyttöliittymä, kun GNSS-vastaanotin on ajoneuvoyksikön ulkopuolella		03
3.5	Salaussarja ja vakiomuotoiset domain-parametrit		CSM_48, CSM_50
4.	**Ympäristötestit**		
4.1	Lämpötila	Todennetaan laitteen toiminta seuraavissa oloissa: Testataan standardin ISO 16750-4, Chapter 5.1.1.2: Low temperature operation test vaatimusten mukaisesti (72 h lämpötilassa – 20 °C) Tämä testi viittaa standardiin IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold Testataan standardin ISO 16750-4: Chapter 5.1.2.2: High temperature operation test vaatimusten mukaisesti (72 h lämpötilassa 70 °C) Tämä testi viittaa standardiin IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Testataan standardin ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration vaatimusten mukaisesti (– 20 °C/70 °C, 20 jaksoa, viipymisaika 1 h jokaisessa lämpötilassa) Alimmassa ja korkeimmassa lämpötilassa sekä lämpötilan muutosjaksojen aikana voidaan tehdä rajoitettu testisarja (joka sisältää tämän taulukon osassa 3 olevia testejä)	213
4.2	Kosteus	Todennetaan, että ajoneuvoyksikkö sietää jaksoittaista kosteutta (lämpötesti) tekemällä standardin IEC 60068-2-30 mukainen testi Db, kuusi 24 tunnin jaksoa, joista jokaisessa lämpötila vaihtelee välillä + 25 °C … + 55 °C ja suhteellinen kosteus on 97 % lämpötilassa + 25 °C ja 93 % lämpötilassa + 55 °C	214
4.3	Mekaaninen	1. Sinimuotoinen tärinä: Todennetaan, että ajoneuvoyksikkö sietää sinimuotoista tärinää, jolla on seuraavat ominaisuudet: vakioamplitudi taajuusalueella 5–11 Hz: 10 mm huipusta huippuun mitattuna vakiokiihtyvyys taajuusalueella 11–300 Hz: 5 g Tämän vaatimuksen täyttäminen todennetaan tekemällä standardin IEC 60068-2-6 mukainen testi Fc, vähimmäiskestoltaan 3 × 12 tuntia (12 tuntia kutakin akselia kohden) ISO 16750-3 ei edellytä sinimuotoista tärinätestiä ajoneuvon irrotetussa hytissä oleville laitteille.	219

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
		2. Satunnainen tärinä Testataan standardin ISO 16750-3: Chapter 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab vaatimusten mukaisesti Satunnaisen tärinän testi, 10–2 000 Hz, vertikaalinen tehollisarvo (RMS) 21,3 m/s^2, pitkittäinen tehollisarvo 11,8 m/s^2, poikittainen tehollisarvo 13,1 m/s^2, 3 akselia, 32 h akselia kohti, mukaan lukien lämpötilajakso – 20 … 70°C. Tämä testi viittaa standardiin IEC 60068-2-64: Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance 3. Iskut: 3 gramman puolisinimuotoinen mekaaninen isku standardin ISO 16750 vaatimusten mukaisesti. Edellä kuvatut testit tehdään kahdelle eri näytteelle, jotka edustavat testattavaa laitetyyppiä.	
4.4	Suojaus vettä ja vieraita esineitä vastaan	Testataan standardin ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access vaatimusten mukaisesti (ei muutoksia parametreissa)	220, 221
4.5	Ylijännitesuojaus	Todennetaan, että ajoneuvoyksikkö sietää seuraavia käyttöjännitteitä: 24 V:n mallit: 34 V lämpötilassa + 40 °C 1 tunnin ajan 12 V:n mallit: 17 V lämpötilassa + 40 °C 1 tunnin ajan (ISO 16750-2, luku 4.3)	216
4.6	Suojaus väärää napaisuutta vastaan	Todennetaan, että ajoneuvoyksikkö sietää virtalähteen napojen vaihtamisen toisin päin (ISO 16750-2, luku 4.7)	216
4.7	Oikosulkusuojaus	Todennetaan, että laitteen tulo- ja lähtösignaalit on suojattu oikosululta käyttöjännitettä ja maata vastaan (ISO 16750-2, luku 4.10])	216
5	**Sähkömagneettisen yhteensopivuuden (EMC) testaus**		
5.1	Laitteen tuottama säteily ja magneettinen vastaanottavuus	Asetuksen ECE R10 vaatimusten noudattaminen	218

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
5.2	Staattisen sähkön purkaukset	Standardin ISO 10605:2008 + teknisen oikaisun Technical Corrigendum: 2010 + tarkistuksen 1:2014 noudattaminen: +/– 4kV kontakti ja +/– 8kV ilma	218
5.3	Virtajohtimia pitkin tulevien jännitepiikkien sietokyky	24 V:n mallit: standardin ISO 7637-2 + ECE-asetuksen nro 10 version 3 noudattaminen: pulssi 1a: Vs = – 450V, Ri = 50 ohmia pulssi 2a: Vs = + 37V, Ri = 2 ohmia pulssi 2b: Vs = + 20V, Ri = 0,05 ohmia pulssi 3a: Vs = – 150V, Ri = 50 ohmia pulssi 3b: Vs = + 150V, Ri = 50 ohmia pulssi 4: Vs = – 16V, Va = – 12V, t6 = 100 ms pulssi 5: Vs = + 120V, Ri = 2,2 ohmia, td = 250 ms 12 V:n mallit: standardin ISO 7637-1 + ECE-asetuksen nro 10 version 3 noudattaminen: pulssi 1: Vs = – 75V, Ri = 10 ohmia pulssi 2a: Vs = + 37V, Ri = 2 ohmia pulssi 2b: Vs = + 10V, Ri = 0,05 ohmia pulssi 3a: Vs = – 112V, Ri = 50 ohmia pulssi 3b: Vs = + 75V, Ri = 50 ohmia pulssi 4: Vs = – 6V, Va = – 5V, t6 = 15 ms pulssi 5: Vs = + 65V, Ri = 3 ohmia, td = 100 ms Pulssin 5 sietokyky testataan vain ajoneuvoyksiköillä, jotka on tarkoitettu asennettavaksi ajoneuvoihin, joissa ei ole erillistä suojausta sähköisen kuormituksen äkillisen katkeamisen varalta Katso sähköisen kuormituksen äkillistä katkeamista koskeva ehdotus standardista ISO 16750-2, neljäs painos, luku 4.6.4.	218

6. ETÄYHTEYSLAITTEISTOON LIITTYVÄT TESTIT

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
1.	**Hallinnollinen tarkastus**		
1.1	Asiakirjat	Kirjallisen aineiston oikeellisuus	
2.	**Silmämääräinen tarkastus**		
2.1.	Yhtäpitävyys kirjallisen aineiston kanssa		
2.2.	Tunniste/merkinnät		225, 226
2.3	Materiaalit		219–223
4.	**Ympäristötestit**		
4.1	Lämpötila	Todennetaan laitteen toiminta seuraavissa oloissa: Testataan standardin ISO 16750-4, Chapter 5.1.1.2: Low temperature operation test vaatimusten mukaisesti (72 h lämpötilassa – 20 °C) Tämä testi viittaa standardiin IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold	213

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
		Testataan standardin ISO 16750-4: Chapter 5.1.2.2: High temperature operation test vaatimusten mukaisesti (72 h lämpötilassa 70 °C) Tämä testi viittaa standardiin IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Testataan standardin ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration vaatimusten mukaisesti (– 20 °C/70 °C, 20 jaksoa, viipymisaika 1 h (?) jokaisessa lämpötilassa) Alimmassa ja korkeimmassa lämpötilassa sekä lämpötilan muutosjaksojen aikana voidaan tehdä rajoitettu testisarja (joka sisältää tämän taulukon osassa 3 olevia testejä)	
4.4	Suojaus vettä ja vieraita esineitä vastaan	Testataan standardin ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access vaatimusten mukaisesti (kohdearvo IP40)	220, 221
5	**Sähkömagneettisen yhteensopivuuden (EMC) testaus**		
5.1	Laitteen tuottama säteily ja magneettinen vastaanottavuus	Asetuksen ECE R10 vaatimusten noudattaminen	218
5.2	Staattisen sähkön purkaukset	Standardin ISO 10605:2008 + teknisen oikaisun Technical Corrigendum: 2010 + tarkistuksen 1:2014 noudattaminen: +/– 4kV kontakti ja +/– 8kV ilma	218
5.3	Virtajohtimia pitkin tulevien jännitepiikkien sietokyky	24 V:n mallit: standardin ISO 7637-2 + ECE-asetuksen nro 10 version 3 noudattaminen: pulssi 1a: Vs = – 450V, Ri = 50 ohmia pulssi 2a: Vs = + 37V, Ri = 2 ohmia pulssi 2b: Vs = + 20V, Ri = 0,05 ohmia pulssi 3a: Vs = – 150V, Ri = 50 ohmia pulssi 3b: Vs = + 150V, Ri = 50 ohmia pulssi 4: Vs = – 16V, Va = – 12V, t6 = 100 ms pulssi 5: Vs = + 120V, Ri = 2,2 ohmia, td = 250 ms 12 V:n mallit: standardin ISO 7637-1 + ECE-asetuksen nro 10 version 3 noudattaminen: pulssi 1: Vs = – 75V, Ri = 10 ohmia pulssi 2a: Vs = + 37V, Ri = 2 ohmia pulssi 2b: Vs = + 10V, Ri = 0,05 ohmia pulssi 3a: Vs = – 112V, Ri = 50 ohmia pulssi 3b: Vs = + 75V, Ri = 50 ohmia pulssi 4: Vs = – 6V, Va = – 5V, t6 = 15 ms pulssi 5: Vs = + 65V, Ri = 3 ohmia, td = 100 ms Pulssin 5 sietokyky testataan vain ajoneuvoyksiköillä, jotka on tarkoitettu asennettavaksi ajoneuvoihin, joissa ei ole erillistä suojausta sähköisen kuormituksen äkillisen katkeamisen varalta Katso sähköisen kuormituksen äkillistä katkeamista koskeva ehdotus standardista ISO 16750-2, neljäs painos, luku 4.6.4.	218

▼B

7. PAPERIN TOIMINNALLISET TESTIT

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
1.	**Hallinnollinen tarkastus**		
1.1	Asiakirjat	Kirjallisen aineiston oikeellisuus	
2	**Yleiset testit**		
2.1	Merkkimäärä riviä kohti	Tulosteiden silmämääräinen tarkastus	172
2.2	Merkkien vähimmäiskoko	Tulosteen silmämääräinen tarkastus ja merkkien tarkastus.	173
2.3	Tuettu standardimerkistö	Tulostimen on tuettava lisäyksen 1 luvussa 4 Merkistöt määritettyjä merkkejä.	174
2.4	Tulosteiden määrittäminen	Tarkastetaan ajopiirturin tyyppihyväksyntä ja tarkastetaan tulosteet silmämääräisesti	174
2.5	Tulosteiden luettavuus ja tunnistaminen	Tulosteiden tarkastaminen Osoitetaan valmistajan testiraporteilla ja testipöytäkirjoilla. Kaikki niiden ajopiirtureiden hyväksyntänumerot, joiden kanssa voidaan käyttää tulostuspaperia, tulostetaan paperille.	175, 177, 178
2.6	Käsin kirjoitettujen huomautusten lisääminen	Silmämääräinen tarkastus: Kuljettajan allekirjoitusta varten on saatavilla kenttä. Muita käsin kirjoitettuja lisätietoja varten on saatavilla kenttiä.	180
2.7	Lisätiedot paperin etu- ja takapuolella.	Paperin etu- ja takapuolilla voi olla lisätietoja ja -yksityiskohtia. Nämä lisätiedot ja -yksityiskohdat eivät saa haitata tulosteiden luettavuutta. Silmämääräinen tarkastus.	177, 178
3	**Varastointitestit**		
3.1	Kuiva lämpö	Vakauttaminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/ suhteellinen kosteus 55 % ± 3 % Testausympäristö. 72 tuntia lämpötilassa + 70 °C ± 2 °C Palautuminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/suhteellinen kosteus 55 % ± 3 %	176, 178 IEC 60068-2-2-Bb
2.2	Kostea lämpö	Vakauttaminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/ suhteellinen kosteus 55 % ± 3 % Testausympäristö. 144 tuntia lämpötilassa + 55 °C ± 2 °C ja suhteellinen kosteus 93 % ± 3 % Palautuminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/suhteellinen kosteus 55 % ± 3 %	176, 178 IEC 60068-2-78-Cab

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
4	**Työaikana tehtävät paperiin liittyvät testit**		
4.1	Kosteudenkestävä tausta (tulostamaton paperi)	Vakauttaminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/ suhteellinen kosteus 55 % ± 3 % Testausympäristö: 144 tuntia lämpötilassa + 55 °C ± 2 °C ja suhteellinen kosteus 93 % ± 3 % Palautuminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/suhteellinen kosteus 55 % ± 3 %	176, 178 IEC 60068-2-78-Cab
4.2	Tulostettavuus	Vakauttaminen: 24 tuntia lämpötilassa + 40 °C ± 2 °C/ suhteellinen kosteus 93 % ± 3 % Testausympäristö: tuloste tuotettu lämpötilassa + 23 °C ± 2 °C Palautuminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/ suhteellinen kosteus 55 % ± 3 %	176, 178
4.3	Kuumuudenkesto	Vakauttaminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/ suhteellinen kosteus 55 % ± 3 % Testausympäristö: 2 tuntia lämpötilassa + 70 °C ± 2 °C, kuiva lämpö Palautuminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/ suhteellinen kosteus 55 % ± 3 %	176, 178 IEC 60068-2-2-Bb
4.4	Matalan lämpötilan sietokyky	Vakauttaminen: 16 tuntia lämpötilassa +23 °C ± 2 °C/ suhteellinen kosteus 55 % ± 3 % Testausympäristö: 24 tuntia lämpötilassa – 20 °C ± 3 °C, kuiva kylmyys Palautuminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/suhteellinen kosteus 55 % ± 3 %	176, 178 ISO 60068-2-1-Ab
4.5	Valonkestävyys	Vakauttaminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/ suhteellinen kosteus 55 % ± 3 % Testausympäristö: 100 tuntia 5 000 luksin valaistuksessa lämpötilassa + 23 °C ± 2 °C/suhteellinen kosteus 55 % ± 3 % Palautuminen: 16 tuntia lämpötilassa + 23 °C ± 2 °C/ suhteellinen kosteus 55 % ± 3 %	176, 178

Luettavuusvaatimukset testeille 3.x ja 4.x:

Tulosteen luettavuus on vahvistettu, jos optiset tiheydet noudattavat seuraavia rajoja:

Tulostetut merkit: väh. 1,0

Tausta (paperin osa, jolla ei ole tulostetta): enint. 0,2

Saatavien tulosteiden optiset tiheydet mitataan standardin DIN EN ISO 534 vaatimusten mukaisesti.

Tulosteen mitat eivät saa muuttua, ja niiden on pysyttävä selkeästi luettavina.

8. YHTEENTOIMIVUUSTESTAUS

Nro	Testi	Kuvaus
9.1 Yhteentoimivuustestit ajoneuvoyksikköjen ja ajopiirturikorttien välillä		
1	Molemminpuolinen varmentaminen	Tarkastetaan, että ajoneuvoyksikön ja ajopiirturikortin välinen molemminpuolinen varmentaminen sujuu normaalisti

▼B

Nro	Testi	Kuvaus
2	Tietojen kirjoittamisen ja lukemisen testaus	Suoritetaan tyypillinen käyttötilannetta vastaava toiminto ajoneuvoyksikössä. Toiminto on valittava testattavan kortin tyypin mukaan, ja sen on kirjoitettava tietoja mahdollisimman moneen kortilla olevaan EF-tiedostoon Todennetaan kopioimalla ajoneuvoyksikön tiedot, että kaikki asianmukaiset tallenteet on tehty oikein Todennetaan kopioimalla kortin tiedot, että kaikki asianmukaiset tallenteet on tehty oikein Todennetaan tulostamalla päivittäinen tuloste, että kaikki asianmukaiset tallenteet ovat luettavissa
9.2 Yhteentoimivuustestit ajoneuvoyksikköjen ja liiketunnistimien välillä		
1	Liittäminen	Tarkastetaan, että ajoneuvoyksikköjen ja liiketunnistimen välinen liittäminen sujuu normaalisti
2	Toimintotestit	Suoritetaan tyypillinen käyttötilannetta vastaava toiminto liiketunnistimessa. Testissä luodaan tavallisen toiminnan lisäksi mahdollisimman monta tapahtumaa tai vikaa. Todennetaan kopioimalla ajoneuvoyksikön tiedot, että kaikki asianmukaiset tallenteet on tehty oikein Todennetaan kopioimalla kortin tiedot, että kaikki asianmukaiset tallenteet on tehty oikein Todennetaan tulostamalla päivittäinen tuloste, että kaikki asianmukaiset tallenteet ovat luettavissa
9.3 Yhteentoimivuustestit ajoneuvoyksikköjen ja ulkoisten GNSS-laitteistojen välillä (soveltuvin osin)		
1	Molemminpuolinen varmentaminen	Tarkastetaan, että ajoneuvoyksikön ja ulkoisen GNSS-yksikön välinen molemminpuolinen varmentaminen (yhdistäminen) sujuu normaalisti
2	Toimintotestit	Suoritetaan tyypillinen käyttötilannetta vastaava toiminto ulkoisessa GNSS-laitteistossa. Testissä luodaan tavallisen toiminnan lisäksi mahdollisimman monta tapahtumaa tai vikaa. Todennetaan kopioimalla ajoneuvoyksikön tiedot, että kaikki asianmukaiset tallenteet on tehty oikein Todennetaan kopioimalla kortin tiedot, että kaikki asianmukaiset tallenteet on tehty oikein Todennetaan tulostamalla päivittäinen tuloste, että kaikki asianmukaiset tallenteet ovat luettavissa

▼B

Lisäys 10

TURVALLISUUSVAATIMUKSET

Tässä lisäyksessä määritellään älykkäiden ajopiirturijärjestelmien osia (toisen sukupolven ajopiirtureita) koskevat tietoturvavaatimukset.

SEC_001 Älykkään ajopiirturijärjestelmän seuraavien osien on oltava turvavarmennettuja yhteisten perusteiden mukaisesti:

— ajoneuvoyksikkö

— ajopiirturikortti

— liiketunnistin

— ulkoinen GNSS-laitteisto.

SEC_002 Kaikkien niiden osien, joiden on oltava turvavarmennettuja, tietoturvaa koskevat vähimmäisvaatimukset on määriteltävä osan suojausprofiilissa yhteisten perusteiden mukaisesti.

SEC_003 Euroopan komissio varmistaa, että valtiolliset tietotekniikan turvallisuudesta vastaavat sertifiointielimet, jotka kuuluvat yhteiseen tulkintatyöryhmään (JIWG), joka tukee todistusten keskinäistä tunnustamista EU:n SOGIS-MRA:n (tietotekniikan tuotteiden turvallisuusarviointitodistusten vastavuoroista tunnustamista koskeva sopimus) puitteissa, tukevat ja kehittävät tämän liitteen mukaista neljää suojausprofiilia ja hyväksyvät ne sekä rekisteröivät seuraavat:

— ajoneuvoyksikön suojausprofiili

— ajopiirturikortin suojausprofiili

— liiketunnistimen suojausprofiili

— ulkoisen GNSS-laitteiston suojausprofiili.

Ajoneuvoyksikön suojausprofiilissa on käsiteltävä tapaukset, joissa ajoneuvoyksikkö on suunniteltu käytettäväksi ulkoisen GNSS-laitteiston kanssa tai ilman sitä. Ensin mainitussa tapauksessa ulkoista GNSS-laitteistoa koskevat vaatimukset annetaan sitä koskevassa suojausprofiilissa.

SEC_004 Luodakseen tietoturvatavoitteet, joiden mukaan voidaan hakea osien turvavarmennusta, osien valmistajien on tarpeen mukaan hiottava ja täydennettävä suojausprofiili ilman, että siinä olevien uhkien, tavoitteiden, menettelytapojen ja tietoturvan toteuttamistoimintojen erittelyjen osalta muutetaan tai poistetaan mitään.

SEC_005 Arviointiprosessissa on todettava erityisen tietoturvatavoitteen ja vastaavan suojausprofiilin tiukka noudattaminen.

SEC_006 Jokaisen suojausprofiilin varmuustason on oltava EAL4 ja sitä on laajennettava varmistusosilla ATE_DPT.2 ja AVA_VAN.5.

▼B

Lisäys 11

YHTEISET TURVALLISUUSMEKANISMIT

SISÄLLYSLUETTELO

ALKUSANAT

OSA A ENSIMMÄISEN SUKUPOLVEN AJOPIIRTURIJÄRJESTELMÄ

1. JOHDANTO

1.1. Viitetiedot

1.2. Merkintätavat ja lyhenteet

2. SALAUSJÄRJESTELMÄT JA -ALGORITMIT

2.1. Salausjärjestelmät

2.2. Salausalgoritmit

2.2.1 RSA-algoritmi

2.2.2 Hajautus (Hash) -algoritmi

2.2.3 DES-salausalgoritmi

3. AVAIMET JA VARMENTEET

3.1. Avainten luonti ja jakelu

3.1.1 RSA-salausavainten luonti ja jakelu

3.1.2 RSA-testausavaimet

3.1.3 Liikkeentunnistinavaimet

3.1.4 Kolminkertaisessa DES-salauksessa käytettävien avainten luonti ja jakelu

3.2. Avaimet

3.3. Varmenteet

3.3.1 Varmenteiden sisältö

3.3.2 Annetut varmenteet

3.3.3 Varmenteen todentaminen ja purkaminen

4. MOLEMMINPUOLINEN TODENNUSMEKANISMI

5. AJONEUVOYKSIKÖN JA KORTIN VÄLISEN TIEDONSIIRRON SALASSAPIDON, EHEYDEN TURVAAMISEN JA TODENNUKSEN MEKANISMIT

5.1. Salattu sanomanvälitys

5.2. Salatun sanomanvälityksen virheiden käsittely

5.3. Algoritmi salauksen tarkistussumman laskemiseksi

5.4. Algoritmi salattavien dataobjektien kryptogrammien laskemiseksi

6. TIETOJEN KOPIOINNISSA KÄYTETTÄVÄT DIGITAALISET ALLEKIRJOITUSMEKANISMIT

6.1. Allekirjoituksen luominen

▼B

6.2.	Allekirjoituksen todentaminen
OSA B	TOISEN SUKUPOLVEN AJOPIIRTURIJÄRJESTELMÄ
7.	JOHDANTO
7.1.	Viitetiedot
7.2.	Merkintätavat ja lyhenteet
7.3.	Määritelmät
8.	SALAUSJÄRJESTELMÄT JA -ALGORITMIT
8.1.	Salausjärjestelmät
8.2.	Salausalgoritmit
8.2.1	Symmetriset algoritmit
8.2.2	Epäsymmetriset algoritmit ja standardoidut domain-parametrit
8.2.3	Hajautusalgoritmit
8.2.4	Salausohjelmat (cipher suite)
9.	AVAIMET JA VARMENTEET
9.1.	Epäsymmetriset avainparit ja julkisen avaimen varmenteet
9.1.1	Yleistä
9.1.2	Eurooppalainen taso
9.1.3	Jäsenvaltiotaso
9.1.4	Laitetaso: ajoneuvoyksiköt
9.1.5	Laitetaso: ajopiirturikortit
9.1.6	Laitetaso: ulkoiset GNSS-laitteistot
9.1.7	Yhteenveto: varmenteen korvaus
9.2.	Symmetriset avaimet
9.2.1	Ajoneuvoyksikön ja liiketunnistimen välisen viestinnän salausavaimet
9.2.2	DSRC-tiedonsiirron salausavaimet
9.3.	Varmenteet
9.3.1	Yleistä
9.3.2	Varmenteen sisältö
9.3.3	Varmenteiden pyytäminen
10.	AJONEUVOYKSIKÖN JA KORTIN MOLEMMINPUOLINEN TODENTAMINEN JA SALATTU SANOMANVÄLITYS
10.1.	Yleistä
10.2.	Molemminpuolinen varmenneketjun todentaminen
10.2.1	Ajoneuvoyksikön suorittama kortin varmenneketjun todentaminen

▼B

10.2.2 Kortin suorittama ajoneuvoyksikön varmenneketjun todentaminen

10.3. Ajoneuvoyksikön todentaminen

10.4. Sirun todentaminen ja tilapäisestä avaimesta sopiminen

10.5. Salattu sanomanvälitys

10.5.1 Yleistä

10.5.2 Salatun sanomanvälityksen rakenne

10.5.3 Salatun sanomanvälitysjakson lopettaminen

11. AJONEUVOYKSIKÖN JA ULKOISEN GNSS-LAITTEISTON KYTKEMINEN, MOLEMMINPUOLINEN TODENTAMINEN JA SALATTU SANOMANVÄLITYS

11.1. Yleistä

11.2. Ajoneuvoyksikön kytkeminen ulkoiseen GNSS-laitteistoon

11.3. Molemminpuolinen varmenneketjun todentaminen

11.3.1 Yleistä

11.3.2 Ajoneuvoyksikön ja ulkoisen GNSS-laitteiston kytkemisen aikana

11.3.3 Tavanomaisen toiminnan aikana

11.4. Ajoneuvoyksikön todentaminen, sirun todentaminen ja tilapäisestä avaimesta sopiminen

11.5. Salattu sanomanvälitys

12. AJONEUVOYKSIKÖN JA LIIKETUNNISTIMEN LIITTÄMINEN SEKÄ VIESTINTÄ

12.1. Yleistä

12.2. Ajoneuvoyksikön ja liiketunnistimen liittäminen eri sukupolvien avaimilla

12.3. Ajoneuvoyksikön ja liiketunnistimen liittäminen sekä viestintä AES-avaimilla

12.4. Ajoneuvoyksikön ja liiketunnistimen liittäminen eri sukupolvien laitteissa

13. DSRC-TIEDONSIIRRON KAUTTA TAPAHTUVAN ETÄVIESTINNÄN TIETOTURVA

13.1. Yleistä

13.2. Ajopiirturin hyötykuormatietojen salaus ja MAC-koodin luominen

13.3. Ajopiirturin hyötykuormatietojen todentaminen ja salauksen avaus

14. KOPIOITUJEN TIETOJEN ALLEKIRJOITTAMINEN JA ALLEKIRJOITUSTEN TODENTAMINEN

14.1. Yleistä

14.2. Allekirjoituksen luominen

14.3. Allekirjoituksen todentaminen

▼B

ALKUSANAT

Tässä lisäyksessä määritellään turvallisuusmekanismit, joiden avulla varmistetaan

— ajopiirturijärjestelmän eri osien molemminpuolinen todentaminen

— ajopiirturijärjestelmän eri osien välillä siirrettyjen tai ulkoisille tietovälineille kopioitujen tietojen luottamuksellisuus, eheys, aitous ja/tai kiistämättömyys.

Lisäys koostuu kahdesta osasta. Osassa A määritellään ensimmäisen sukupolven ajopiirturijärjestelmän (digitaalinen ajopiirturi) turvallisuusmekanismit. Osassa B määritellään toisen sukupolven ajopiirturijärjestelmän (älykäs ajopiirturi) turvallisuusmekanismit.

Lisäyksen osassa A määriteltyjä mekanismeja sovelletaan, jos molemminpuolisessa todennus- ja/tai tiedonsiirtoprosessissa on osallisena vähintään yksi ensimmäisen sukupolven ajopiirturijärjestelmän osa.

Lisäyksen osassa B määriteltyjä mekanismeja sovelletaan, jos molemmat molemminpuolisessa todennus- ja/tai tiedonsiirtoprosessissa osallisena olevat ajopiirturijärjestelmän osat ovat toisen sukupolven osia.

Lisäyksessä 15 esitetään lisätietoa ensimmäisen sukupolven osien käytöstä yhdessä toisen sukupolven osien kanssa.

OSA A

ENSIMMÄISEN SUKUPOLVEN AJOPIIRTURIJÄRJESTELMÄ

1. JOHDANTO

1.1. **Viitetiedot**

Tässä lisäyksessä käytetään seuraavia viitetietoja:

SHA-1	National Institute of Standards and Technology (NIST). *FIPS Publication 180-1: Secure Hash Standard*. April 1995.
PKCS1	RSA Laboratories. PKCS # 1: *RSA Encryption Standard*. Version 2.0. October 1998.
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3: Data Encryption Standard*. Draft 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. First edition: 1995 + Amendment 1: 1997.
ISO/IEC 7816-6	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. First edition 1999.
ISO/IEC 9796-2	Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function. First edition: 1997.

▼B

ISO/IEC 9798-3	Information Technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm. Second edition 1998.
ISO 16844-3	Road vehicles – Tachograph systems – Part 3: Motion sensor interface.

1.2. **Merkintätavat ja lyhenteet**

Tässä lisäyksessä käytetään seuraavia merkintätapoja ja lyhenteitä:

(K_a, K_b, K_c)	Avainnippu, jota kolminkertainen salausalgoritmi käyttää
CA	(Certification authority) Varmenneviranomainen
CAR	(Certification authority reference) Varmenneviranomaisen viite
CC	(Cryptographic checksum) Salauksen tarkistussumma
CG	(Cryptogram) Kryptogrammi
CH	(Command header) Komennon ylätunniste
CHA	(Certificate holder authorisation) Varmenteen haltijan valtuutus
CHR	(Certificate holder reference) Varmenteen haltijan viite
D()	Salauksen avaaminen DES-algoritmilla
DE	(Data element) Dataelementti
DO	(Data object) Dataobjekti
d	RSA-salauksessa käytettävä yksityinen avain eli yksityinen eksponentti
e	RSA-salauksessa käytettävä julkinen avain eli julkinen eksponentti
E()	Salaaminen DES-algoritmilla
EQT	(Equipment) Laitteet
Hash()	*Hash*-hajautusalgoritmilla laskettu tulos
Hash	Hajautusalgoritmi
KID	(Key identifier) Avaimen tunniste
Km	TDES-avain. ISO 16844-3 -standardissa määritelty pääavain
Km_{VU}	Ajoneuvoyksikköön asetettava TDES-avain
Km_{WC}	Korjaamokorttiin asetettava TDES-avain
m	Viestiä edustava luku, kokonaisluku välillä 0–*n*-1
n	RSA-avaimien yhteinen osa, (kongruenssi)moduuli
PB	(Padding bytes) Täyttötavut
PI	(Padding indicator byte) Täyttämistä ilmaiseva tavu (käytetään salatun datan kryptogrammissa)
PV	(Plain value) Koodaamaton datan arvo
s	Allekirjoitusta edustava luku, kokonaisluku välillä 0–*n*-1
SSC	(Send sequence counter) Lähetysvaihelaskuri
SM	(Secure messaging) Salattu sanomanvälitys
TCBC	(TDEA cipher block chaining mode of operation) TDEA-salauksen salauslohkoja ketjuttava käyttötila

▼B

TDEA	(Triple data encryption algorithm) Kolminkertainen tiedonsalausalgoritmi
TLV	(Tag length value) TLV-koodaustapa; tuntomerkki-pituus-sisältö-koodaustapa
VU	(Vehicle unit) Ajoneuvoyksikkö
X.C	Varmenneviranomaisen antama käyttäjä X:n varmenne
X.CA	Käyttäjä X:n varmenneviranomainen
X.CA.PK $_{o}$ X.C	Toimenpide, jolla varmenne avataan sen sisältämän julkisen avaimen saamiseksi. Kyseessä on operandien väliin tuleva operaattori, jonka vasemmanpuoleinen kohdemuuttuja (operandi) on varmenneviranomaisen julkinen avain ja oikeanpuoleinen kohdemuuttuja on tämän varmenneviranomaisen antama varmenne. Tulos on sen käyttäjä X:n julkinen avain, jonka varmenne on oikeanpuoleisena kohdemuuttujana
X.PK	Käyttäjä X:n julkinen RSA-avain
X.PK[I]	Käyttäjä X:n julkista avainta käyttäen tehty tiedon I RSA-salaus
X.SK	Käyttäjä X:n yksityinen RSA-avain
X.SK[I]	Käyttäjä X:n yksityistä avainta käyttäen tehty tiedon I RSA-salaus
‘xx’	Heksadesimaalilukuna ilmaistu arvo
||	Ketjutusmerkki

2. SALAUSJÄRJESTELMÄT JA -ALGORITMIT

2.1. **Salausjärjestelmät**

CSM_001 Ajoneuvoyksikköjen ja ajopiirturikorttien on käytettävä klassista julkiseen avaimeen perustuvaa RSA-salausjärjestelmää luomaan seuraavat turvallisuusmekanismit:

— ajoneuvoyksikköjen ja korttien välinen todentaminen,

— kolminkertaisessa DES-salauksessa käytettävien avainten siirtäminen ajoneuvoyksikköjen ja ajopiirturikorttien välillä,

— ajoneuvoyksiköistä tai ajopiirturikorteilta ulkoisille tallennusvälineille kopioitujen tietojen digitaalinen allekirjoitus.

CSM_002 Ajoneuvoyksikköjen ja ajopiirturikorttien on käytettävä kolminkertaista symmetristä DES-salausjärjestelmää luomaan mekanismi, jolla taataan tietojen eheys vaihdettaessa käyttäjätietoja ajoneuvoyksikköjen ja ajopiirturikorttien välillä, sekä tarvittaessa käytettävä sitä salaamaan ajoneuvoyksikköjen ja ajopiirturikorttien välillä vaihdettavat tiedot.

2.2. **Salausalgoritmit**

2.2.1 *RSA-algoritmi*

CSM_003 Seuraavat riippuvuudet määrittelevät täysin RSA-algoritmin:

▼B

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

RSA-funktio on kuvattu yksityiskohtaisesti viitteessä PKCS1. RSA-laskelmissa käytettävä julkinen eksponentti e on välillä 3 ja n-1 oleva kokonaisluku, joka täyttää ehdon gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Hajautus (Hash) -algoritmi*

CSM_004 Digitaalisten allekirjoitusmekanismien on käytettävä viitteessä SHA-1 määriteltyä SHA-1-hajautusalgoritmia.

2.2.3 *DES-salausalgoritmi*

CSM_005 DES-perustaisia algoritmeja on käytettävä ketjuttaen salattavat lohkot.

3. AVAIMET JA VARMENTEET

3.1. **Avainten luonti ja jakelu**

3.1.1 *RSA-salausavainten luonti ja jakelu*

CSM_006 RSA-avaimet on luotava kolmella toiminnallisesti hierarkkisella tasolla:

— eurooppalaisella tasolla,

— jäsenvaltiotasolla,

— laitetasolla.

CSM_007 Eurooppalaisella tasolla on luotava yksi eurooppalainen avainpari (EUR.SK ja EUR.PK). Eurooppalaista yksityistä avainta on käytettävä varmentamaan jäsenvaltioiden julkiset avaimet. Kaikista varmennetuista avaimista on pidettävä rekisteriä. Euroopan varmenneviranomaisen on hoidettava nämä tehtävät Euroopan komission valtuuttamana ja vastuulla.

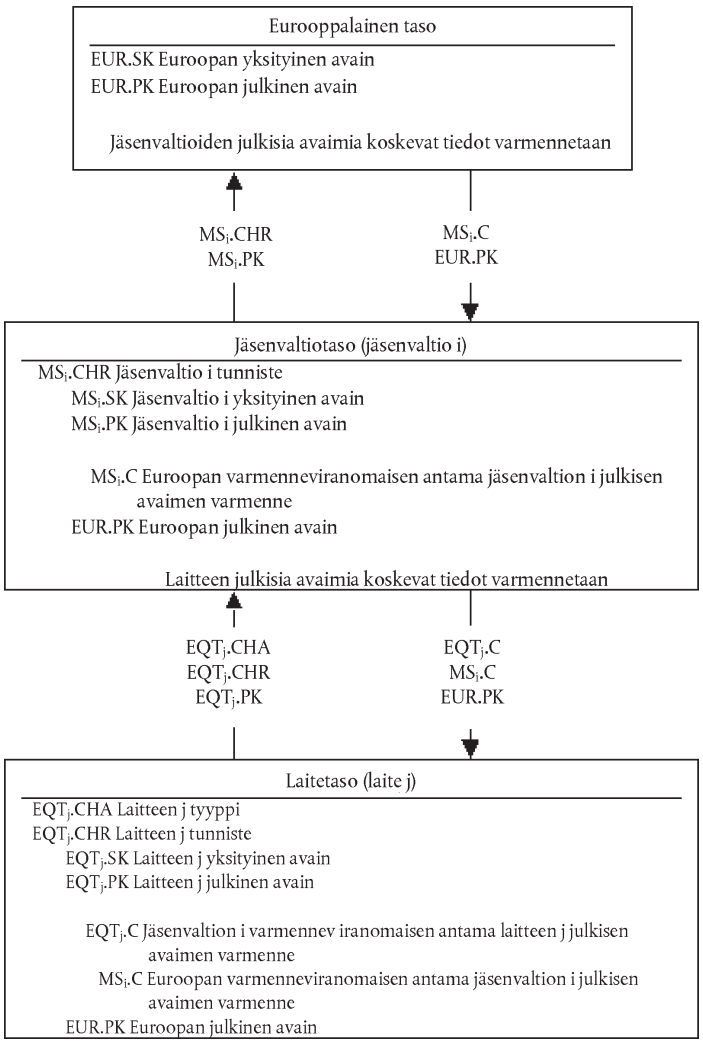
CSM_008 Jäsenvaltiotasolla on luotava jäsenvaltion avainpari (MS.SK ja MS.PK). Euroopan varmenneviranomaisen on varmennettava jäsenvaltioiden julkiset avaimet. Jäsenvaltioiden yksityistä avainta on käytettävä varmentamaan laitteisiin (ajoneuvoyksikköön tai ajopiirturikorteille) asennetut julkiset avaimet. Kaikista varmennetuista julkisista avaimista on pidettävä rekisteriä, jossa on kunkin avaimen osalta sen laitteen tunniste, johon avain on tarkoitettu. Jäsenvaltion varmenneviranomaisen on hoidettava nämä tehtävät. Jäsenvaltio saa vaihtaa avainpariaan säännöllisesti.

CSM_009 Laitetasolla on jokaiselle laitteelle luotava ja siihen lisättävä yksi avainpari (EQT.SK ja EQT.PK). Jäsenvaltion varmenneviranomaisen on varmennettava laitteiden julkinen avain. Nämä tehtävät voi hoitaa laitteen valmistaja, se, joka syöttää laitteeseen haltijan henkilötiedot, tai jäsenvaltion viranomainen. Tätä avainparia käytetään todennuksessa, digitaalisessa allekirjoituksessa ja salauksessa.

CSM_010 Yksityiset avaimet on pidettävä salassa niitä luotaessa, siirrettäessä (jos niitä siirretään) ja säilytettäessä.

▼B

Seuraavassa kuvassa on tämän prosessin tietovirran yhteenveto:



3.1.2 *RSA-testausavaimet*

CSM_011 Laitteiden testausta varten (mukaan lukien yhteentoimivuustestit) Euroopan varmenneviranomaisen on luotava yksi erillinen Euroopan testausavainpari ja vähintään kaksi jäsenvaltioiden testausavainparia, joiden julkiset avaimet on varmennettava Euroopan yksityisellä testausavaimella. Laitteiden valmistajien on asennettava tyyppihyväksyntää varten testattaviin laitteisiin jollain näistä jäsenvaltioiden testausavaimista varmennettu testausavain.

3.1.3 *Liikkeentunnistinavaimet*

Alla kuvatut kolme TDES-avainta on pidettävä asianmukaisesti salassa luonnin, (mahdollisen) siirron ja säilytyksen aikana.

ISO 16844 -standardin mukaisten ajopiirturin osien tukemiseksi Euroopan varmenneviranomaisen ja jäsenvaltioiden varmenneviranomaisten on lisäksi toimittava seuraavasti:

CSM_036 Euroopan varmenneviranomaisen on luotava kaksi itsenäistä ja ainutkertaista TDES-avainta (KmVU ja KmWC) ja luotava Km seuraavasti: $Km = Km_{VU}$ XOR Km_{WC}. Euroopan varmenneviranomaisen on toimitettava nämä avaimet tarvittavin turvatoimin pyynnöstä jäsenvaltioiden varmenneviranomaisille.

▼B

CSM_037 Jäsenvaltioiden varmenneviranomaisten on:

— käytettävä Km:ää salatessaan liikkeentunnistinvalmistajien pyytämät liikkeentunnistintiedot (Km:llä salattavat tiedot määritellään ISO 16844-3 -standardissa),

— toimitettava tarvittavin turvatoimin Km_{VU} ajoneuvoyksiköiden valmistajille asennettavaksi ajoneuvoyksiköihin,

— varmistettava, että Km_{WC} asennetaan kaikkiin korjaamokortteihin (`SensorInstallationSecData` tiedostossa `Sensor_Installation_Data`) kortin asiakaskohtaisia asetuksia tehtäessä.

3.1.4 *Kolminkertaisessa DES-salauksessa käytettävien avainten luonti ja jakelu*

CSM_012 Ajoneuvoyksikköjen ja ajopiirturikorttien on osana molemminpuolista todennusprosessia luotava ja vaihdettava tarvittavat tiedot yhteisen kolminkertaisen DES-salauksen avaimen luomiseksi. Tämä tiedonvaihto on salattava RSA-salausmekanismia käyttäen.

CSM_013 Tätä avainta on käytettävä kaikkiin myöhempiin salaustoimiin, joissa käytetään salattua sanomanvälitystä. Sen voimassaolo päättyy kortin käyttöjakson päättyessä (kun kortti poistetaan tai asetetaan alkutilaansa) ja/tai 240 käyttökerran jälkeen (yksi avaimen käyttökerta = yksi salattua sanomanvälitystä käyttäen kortille lähetetty komento ja siihen liittyvä vastaus).

3.2. **Avaimet**

CSM_014 RSA-avaimen pituuden (kaikilla tasoilla) on oltava seuraava: moduuli *n* 1 024 bittiä, julkinen eksponentti *e* enintään 64 bittiä, yksityinen eksponentti *d* 1 024 bittiä.

CSM_015 Kolminkertaisen DES-salauksen avainten on oltava muotoa (K_a, K_b, K_a), missä K_a ja K_b ovat toisistaan riippumattomia 64 bitin pituisia avaimia. Pariteettibittejä ei aseteta.

3.3. **Varmenteet**

CSM_016 Julkisten RSA-avainten varmenteiden on oltava heterologisia (non self descriptive) kortin avulla todennettavia (card verifiable) varmenteita (viite: ISO/IEC 7816-8).

3.3.1 *Varmenteiden sisältö*

CSM_017 Julkisten RSA-avainten varmenteet koostuvat seuraavista tiedoista seuraavassa järjestyksessä:

Data	Muoto	Tavuja	Selite
CPI	INTEGER	1	Varmenteen profiilin tunniste (tässä versiossa ‘01’)
CAR	OCTET STRING	8	Varmenneviranomaisen viite
CHA	OCTET STRING	7	Varmenteen haltijan valtuutus

▼B

Data	Muoto	Tavuja	Selite
EOV	TimeReal	4	Varmenteen viimeinen voimassaoloaika. Valinnainen, täytetään tavuilla ‘FF’, jos ei käytössä.
CHR	OCTET STRING	8	Varmenteen haltijan viite
n	OCTET STRING	128	Julkinen avain (moduuli)
e	OCTET STRING	8	Julkinen avain (julkinen eksponentti)
		164	

Huomautuksia:

1. Varmenteen profiilin tunniste (CPI) kuvaa todennusvarmenteen tarkan rakenteen. Sitä voidaan käyttää laitteen sisäisesti yksilöimään tietty ylätunnisteluettelo, joka kuvaa varmenteessa olevien dataelementtien ketjutuksen.

Tämän varmenteen sisältöön liittyvä ylätunnisteluettelo on seuraava:

‘4D’	‘16’	‘5F 29’	‘01’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	‘81 80’	‘82’	‘08’
Pidennetyn ylätunnisteluettelon tuntomerkki	Ylätunnisteluettelon pituus	CPI:n tuntomerkki	CPI:n pituus	CAR:n tuntomerkki	CAR:n pituus	CHA:n tuntomerkki	CHA:n pituus	EOV:n tuntomerkki	EOV:n pituus	CHR:n tuntomerkki	CHR:n pituus	Julkisen avaimen tuntomerkki (koottu)	Seuraavien dataobjektien pituus	Moduulin tuntomerkki	Moduulin pituus	Julkisen eksponentin tuntomerkki	Julkisen eksponentin pituus

2. Varmenneviranomaisen viitteen (CAR) avulla tunnistetaan varmenteen antanut varmenneviranomainen siten, että dataelementtiä voidaan käyttää samanaikaisesti viranomaisen avaimen tunnisteen kanssa löytämään varmenneviranomaisen julkinen avain (koodaus on selitetty jäljempänä avaimen tunnistetta käsittelevässä kohdassa).

3. Varmenteen haltijan valtuutusta (CHA) käytetään yksilöimään varmenteen haltijan oikeudet. Se koostuu ajopiirturisovelluksen tunnisteesta ja sen laitteen tyypistä, johon varmenne on tarkoitettu (`EquipmentType`- dataelementin mukaisesti; jäsenvaltiota vastaava arvo on 00).

▼B

4. Varmenteen haltijan viitteen (CHR) avulla yksilöidään varmenteen haltija siten, että dataelementtiä voidaan käyttää samanaikaisesti kyseisen avaimen tunnisteen kanssa löytämään varmenteen haltijan julkinen avain.

5. Avaimen tunnisteet yksilöivät varmenteen haltijan tai varmenneviranomaisen. Ne koodataan seuraavasti:

5.1 Laite (ajoneuvoyksikkö tai kortti):

Data	Laitteen sarjanumero	Päivämäärä	Tyyppi	Valmistaja
Pituus	4 tavua	2 tavua	1 tavu	1 tavu
Arvo	Kokonaisluku	kk vv BCD-koodattuna	Valmistajan mukaan	Valmistajan koodi

Varmennetta pyytäessään ajoneuvoyksikön valmistaja joko tietää tai ei tiedä sen laitteen tunnistetta, johon avaimet tullaan asentamaan.

Ensin mainitussa tapauksessa valmistaja lähettää laitteen tunnisteen julkisen avaimen kanssa jäsenvaltionsa viranomaiselle saadakseen varmenteen. Varmenne sisältää tällöin laitteen tunnisteen ja valmistajan on varmistettava, että avain ja varmenne asennetaan aiottuun laitteeseen. Avaimen tunniste on jäljempänä esitetyn muotoinen.

Jälkimmäisessä tapauksessa valmistajan on yksilöitävä jokainen varmennepyyntö ja lähetettävä tämä tunniste julkisen avaimen kanssa jäsenvaltionsa viranomaiselle saadakseen varmenteen. Varmenne sisältää pyynnön tunnisteen. Kun avain on asennettu johonkin laitteeseen, valmistajan on annettava jäsenvaltion viranomaiselle tieto siitä, mihin laitteeseen se asennettiin (ts. pyynnön tunniste, laitteen tunniste). Avaimen tunniste on seuraavan muotoinen:

Data	Varmennepyynnön järjestysnumero	Päivämäärä	Tyyppi	Valmistaja
Pituus	4 tavua	2 tavua	1 tavu	1 tavu
Arvo	Kokonaisluku	kk vv BCD-koodattuna	‘FF’	Valmistajan koodi

▼B

5.2 Varmenneviranomainen:

Data	Viranomaisen tunniste	Avaimen järjestysnumero	Lisätiedot	Tunniste
Pituus	4 tavua	1 tavu	2 tavua	1 tavu
Arvo	1 tavu: valtion numerotunnus 3 tavua: valtion aakkosnumeerinen tunnus	Kokonaisluku	Koodatut lisätiedot (CA:n mukaan) 'FF FF', jos ei käytössä	'01'

Avaimen järjestysnumeroa käytetään erottamaan toisistaan jäsenvaltion eri avaimet tapauksissa, joissa avain vaihdetaan.

6. Varmenteiden todentajien on saatava tieto siitä, että varmennettu julkinen avain on RSA-avain, jota käytetään todentamiseen, digitaaliseen allekirjoitukseen ja salaukseen (varmenne ei sisällä tunnistetta, joka kertoisi sen).

3.3.2 *Annetut varmenteet*

CSM_018 Annettu varmenne on digitaalinen allekirjoitus, joka sisältää varmenteen sisällön osittaisen palautuksen ISO/IEC 9796-2 -standardin (lukuun ottamatta sen liitettä A4) mukaisesti ja johon on liitetty varmenneviranomaisen viite.

$$X.C = X.CA.SK[\text{'6A'} \parallel C_r \parallel \mathit{Hash}(Cc) \parallel \text{'BC'}] \parallel C_n \parallel X.CAR$$

Varmenteen sisällön ollessa = $Cc = C_r \parallel C_n$

106 tavua 58 tavua

Huomautuksia:

1. Tämä varmenne on 194 tavun pituinen.

2. Allekirjoituksella peitetty varmenneviranomaisen viite (CAR) liitetään myös allekirjoitukseen, jotta varmenteen todentamiseksi voidaan valita varmenneviranomaisen julkinen avain.

3. Varmenteen todentajan on automaattisesti tunnettava algoritmi, jota varmenneviranomainen on käyttänyt allekirjoittaessaan varmenteen.

4. Tähän annettuun varmenteeseen liittyvä ylätunnisteluettelo on seuraavanlainen:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Todennettavan varmenteen tuntomerkki (koottu)	Seuraavien dataobjektien pituus	Allekirjoituksen tuntomerkki	Allekirjoituksen pituus	Jakojäännöksen tuntomerkki	Jakojäännöksen pituus	CAR:n tuntomerkki	CAR:n pituus

▼B

3.3.3 *Varmenteen todentaminen ja purkaminen*

Varmenteen todentaminen ja purkaminen sisältää allekirjoituksen todentamisen ISO/IEC 9796-2 -standardin mukaisesti, varmenteen sisällön ja siihen sisältyvän julkisen avaimen palauttamisen: X.PK = X.CA.PK $_{o}$ X.C sekä varmenteen voimassaolon todentamisen.

CSM_019 Siihen liittyy seuraavat vaiheet:

Todennetaan allekirjoitus ja palautetaan sisältö:

— X.C:stä palautetaan allekirjoitus C_n' ja CAR': X.C = allekirjoitus (128 tavua) || C_n' (58 tavua) || CAR' (8 tavua)

— CAR':sta valitaan oikea varmenneviranomaisen julkinen avain (ellei sitä ole aiemmin saatu muilla tavoin),

— avataan allekirjoitus CA:n julkisella avaimella: Sr'= X.CA.PK [Sign],

— tarkastetaan, että merkkijono Sr' alkaa tavulla ‘6A’ ja päättyy tavuun ‘BC’,

— lasketaan C_r' ja H' allekirjoituksesta: Sr' = ‘6A’ || C_r' (106 tavua) || H' (20 tavua) || ‘BC’

— palautetaan varmenteen sisältö C' = C_r' || C_n',

— tarkastetaan, että *Hash*(C') = H'

Jos tarkastusten tulos on oikea ja varmenne on aito, sen sisältö on C'.

Todennetaan voimassaolo C':n sisällöstä:

— tarkastetaan viimeinen voimassaolopäivä, jos sellainen on.

Palautetaan C':n sisällöstä ja tallennetaan julkinen avain, avaimen tunniste, varmenteen haltijan valtuutus ja varmenteen viimeinen voimassaolopäivä:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MOLEMMINPUOLINEN TODENNUSMEKANISMI

Korttien ja ajoneuvoyksikköjen molemminpuolinen todennus perustuu seuraavaan periaatteeseen:

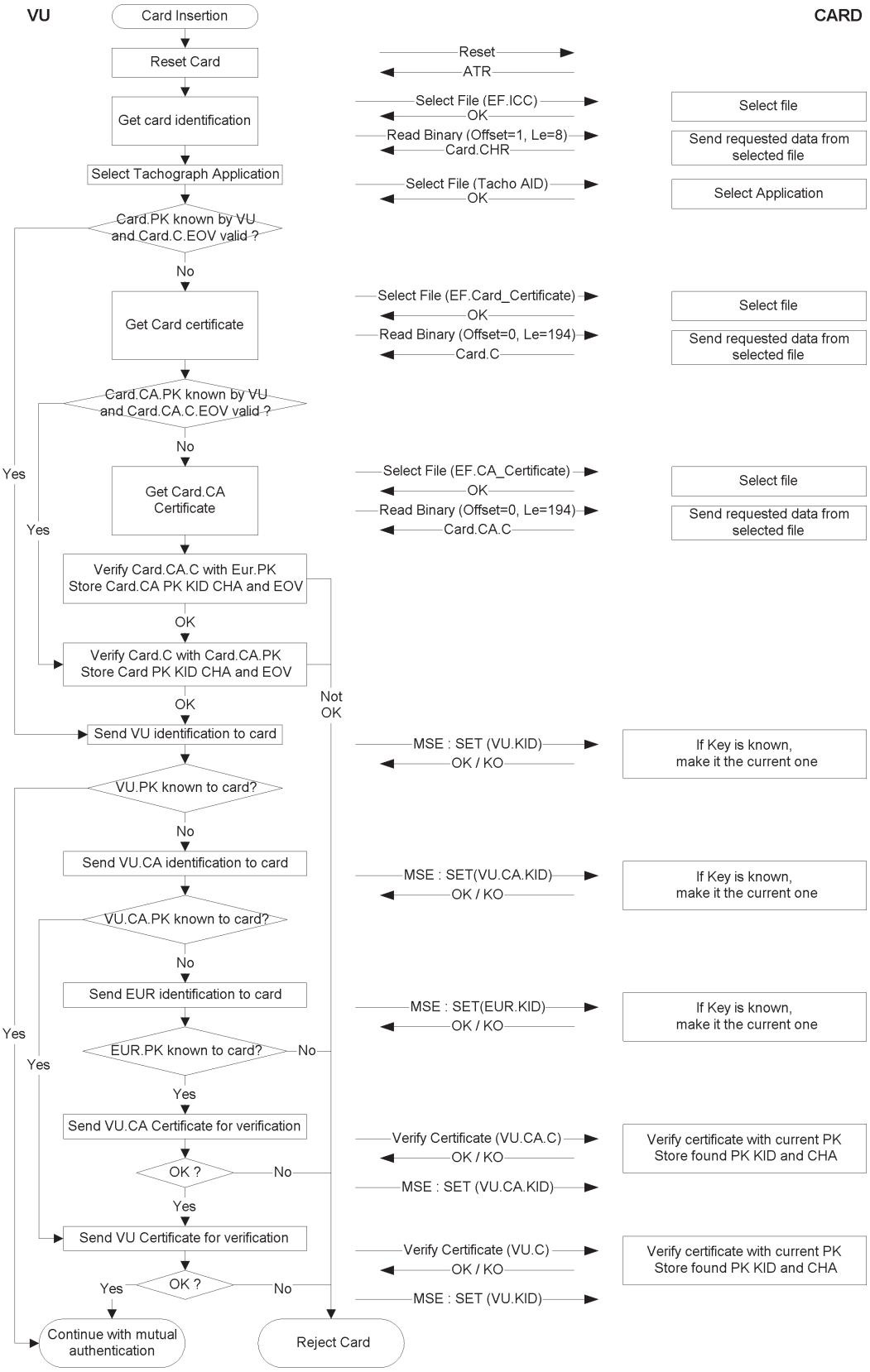
Kummankin osapuolen on osoitettava toiselle osapuolelle, että sillä on hallussaan voimassa oleva avainpari, jonka julkisen avaimen on varmentanut jäsenvaltion varmenneviranomainen, joka puolestaan on Euroopan varmenneviranomaisen varmentama.

Tämän osoittaminen tehdään allekirjoittamalla yksityistä avainta käyttäen toisen osapuolen lähettämä satunnaisluku, joka lähettäneen osapuolen on toistettava allekirjoitusta todentaessaan.

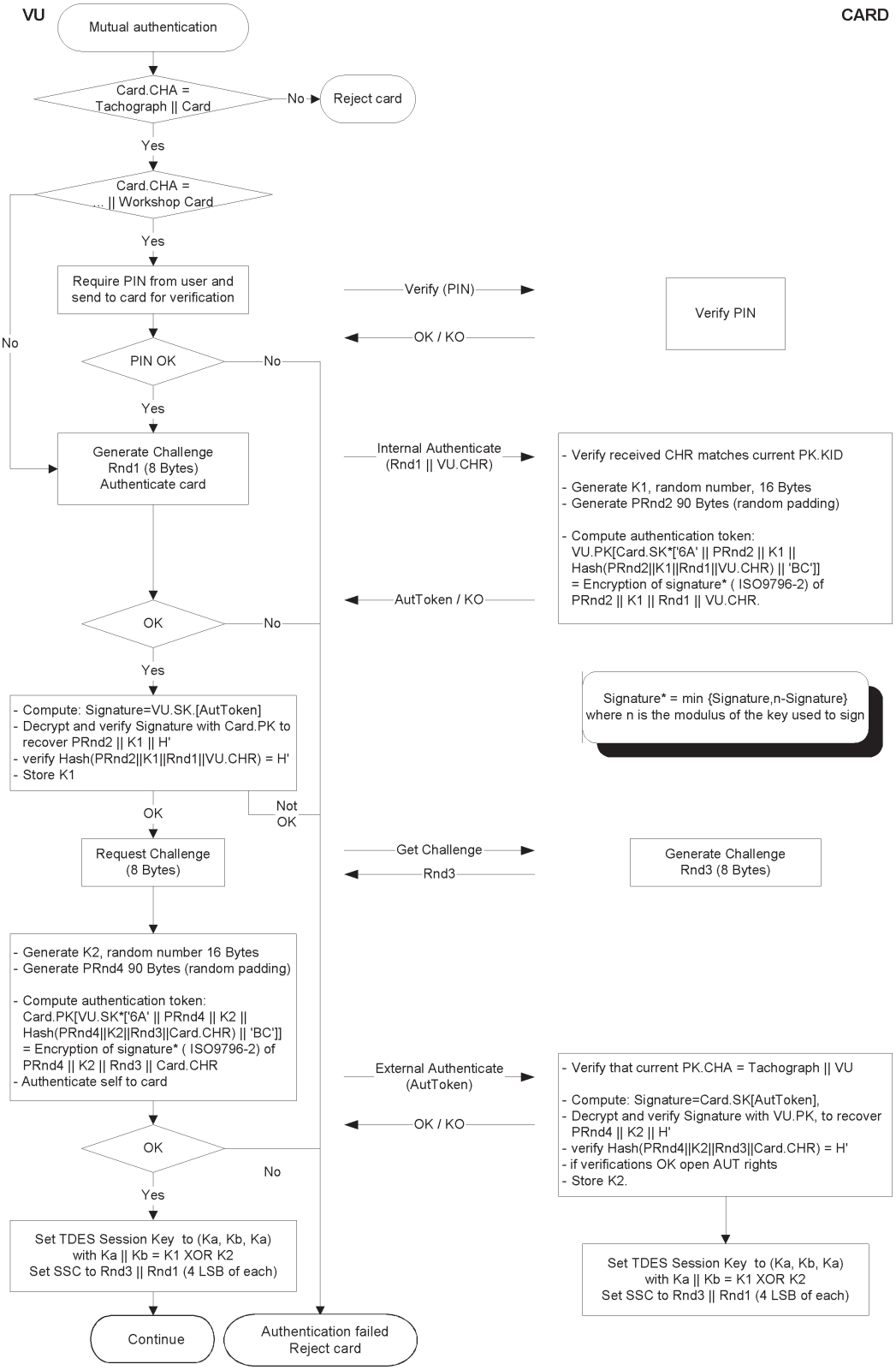
Tämä mekanismi käynnistyy, kun kortti asetetaan ajoneuvoyksikköön. Se alkaa varmenteiden vaihtamisella ja julkisten avainten purkamisella ja päättyy tilapäisen avaimen luomiseen.

▼B

CSM_020 Mekanismin on käytettävä seuraavaa protokollaa (nuolet merkitsevät komentoja ja vaihdettavia tietoja (ks. lisäys 2)):



▼B


VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
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
OK
Not 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

▼B

5. AJONEUVOYKSIKÖN JA KORTIN VÄLISEN TIEDONSIIRRON SALASSAPIDON, EHEYDEN TURVAAMISEN JA TODENNUKSEN MEKANISMIT

5.1. **Salattu sanomanvälitys**

CSM_021 Ajoneuvoyksikön ja kortin välisen tiedonsiirron eheys on turvattava käyttämällä salattua sanomanvälitystä viitteiden ISO/IEC 7816-4 ja ISO/IEC 7816-8 mukaisesti.

CSM_022 Kun tiedot on suojattava siirron ajaksi, on komennon tai sen vastauksen mukana lähetettäviin dataobjekteihin liitettävä salauksen tarkistussumman sisältävä dataobjekti. Vastaanottajan on todennettava salauksen tarkistussumma.

CSM_023 Komennon mukana lähetettyyn tietojen salauksen tarkistussummaan on laskettava mukaan komennon ylätunniste ja kaikki lähetetyt dataobjektit (=>CLA = ‘0C’, ja kaikki dataobjektit on ympäröitävä tunnusmerkeillä, joissa b1 = 1).

CSM_024 Vastauksen tilaa osoittavat tavut on suojattava salauksen tarkistussummalla, kun vastauksessa ei ole datakenttää.

CSM_025 Salauksen tarkistussummien on oltava neljän tavun pituisia.

Salattua sanomanvälitystä käytettäessä komentojen ja vastausten rakenne on sen vuoksi seuraava:

Käytetyt dataobjektit ovat osa ISO/IEC 7816-4 -standardissa kuvatuista salatussa sanomanvälityksessä käytettävistä dataobjekteista:

Tuntomerkki	Muistikas	Merkitys
‘81’	T_{PV}	Koodaamaton data, jota ei ole BER-TLV-koodattu (suojataan CC:llä)
‘97’	$\mathbf{T_{LE}}$	Le:n arvo suojaamattomassa komennossa (suojataan CC:llä)
‘99’	T_{SW}	Status info (suojataan CC:llä)
‘8E’	T_{CC}	Salauksen tarkistussumma CC
‘87’	$T_{PI\ CG}$	Täyttämistä osoittava tavu || Kryptogrammi (koodaamaton data, jota ei ole BER-TLV-koodattu)

▼B

Kun suojaamaton komento-vastauspari on:

Komennon ylätunniste				Varsinainen komento		
CLA	INS	P1	P2	[L_c-kenttä]	[Datakenttä]	[L_e-kenttä]
neljä tavua				L tavua merkittynä B_1 bis B_L		

Varsinainen vastaus	Vastauksen lopuke	
[Datakenttä]	SW1	SW2
L_r datatavua	kaksi tavua	

Niin vastaava suojattu komento-vastauspari on:

Suojattu komento:

Komennon ylätunniste (CH)				Varsinainen komento										
CLA	INS	P1	P2	[Uusi L_c-kenttä]	[Uusi datakenttä]									[Uusi L_e-kenttä]
‘OC’				Uuden datakentän pituus	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	‘00’
					‘81’	L_c	Datakenttä	‘97’	‘01’	L_e	‘8E’	‘04’	CC	

Tarkistussummaan laskettava data = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Täyttötavut (80..00) standardin ISO-IEC 7816-4 ja ISO 9797 menetelmän 2 mukaisesti.

PV- ja LE-dataobjektit ovat mukana vain, jos suojaamattomassa komennossa on vastaavaa dataa.

Suojattu vastaus:

1. Tapaus, jossa vastauksen datakenttä ei ole tyhjä mutta sitä ei tarvitse pitää salassa:

Varsinainen vastaus						Vastauksen lopuke
[Uusi datakenttä]						Uusi SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Datakenttä	‘8E’	‘04’	CC	

Tarkistussummaan laskettava data = T_{PV} || L_{PV} || PV || PB

2. Tapaus, jossa vastauksen datakenttä ei ole tyhjä ja se on pidettävä salassa:

▼B

Varsinainen vastaus						Vastauksen lopuke
[Uusi datakenttä]						Uusi SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
‘87’		PI || CG	‘8E’	‘04’	CC	

CG-kryptogrammin sisältämä data: data ilman BER-TLV-koodausta ja täyttötavut.

Tarkistussummaan laskettava data = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Tapaus, jossa vastauksen datakenttä on tyhjä:

Varsinainen vastaus						Vastauksen lopuke
[Uusi datakenttä]						Uusi SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
‘99’	‘02’	SW1 SW2 Uusi	‘8E’	‘04’	CC	

Tarkistussummaan laskettava data = T_{SW} || L_{SW} || SW || PB

5.2. **Salatun sanomanvälityksen virheiden käsittely**

CSM_026 Kun ajopiirturikortti komentoa tulkitessaan havaitsee virheen salatussa sanomanvälityksessä, on tilaa osoittavat tavut lähetettävä takaisin ilman salattua sanomanvälitystä. ISO/IEC 7816-4 -standardin mukaisesti seuraavat tilaa osoittavat tavut on määritelty osoittamaan virheitä salatussa sanomanvälityksessä:

‘66 88’: Salauksen tarkistussumman todennus epäonnistui,

‘69 87’: Odotettuja salatun sanomanvälityksen dataobjekteja puuttuu,

‘69 88’: Salatun sanomanvälityksen dataobjektit virheellisiä.

CSM_027 Kun ajopiirturikortti lähettää takaisin tavuja ilman salatun sanomanvälityksen dataobjekteja tai virheellisen salatun sanomanvälityksen dataobjektin kanssa, ajoneuvoyksikön on lopetettava tiedonvaihtojakso.

5.3. **Algoritmi salauksen tarkistussumman laskemiseksi**

CSM_028 Salauksen tarkistussummat kootaan käyttäen ANSI X9.19 -standardin mukaisia retail MAC -tyyppisiä viestin todennuksen tarkistussummia ja DES-salausta:

— ensimmäinen vaihe: ensimmäinen tarkistuslohko y0 on E(Ka, SSC),

— seuraavat vaiheet: tarkistuslohkot y1–yn lasketaan Ka-avainta käyttäen,

— viimeinen vaihe: salauksen tarkistussumma lasketaan viimeisestä tarkistuslohkosta yn seuraavasti: E(Ka, D(Kb, yn)),

missä E() tarkoittaa salaamista DES-algoritmilla ja D() tarkoittaa salauksen avaamista DES-algoritmilla.

Salauksen tarkistussumman neljä merkitsevintä tavua lähetetään.

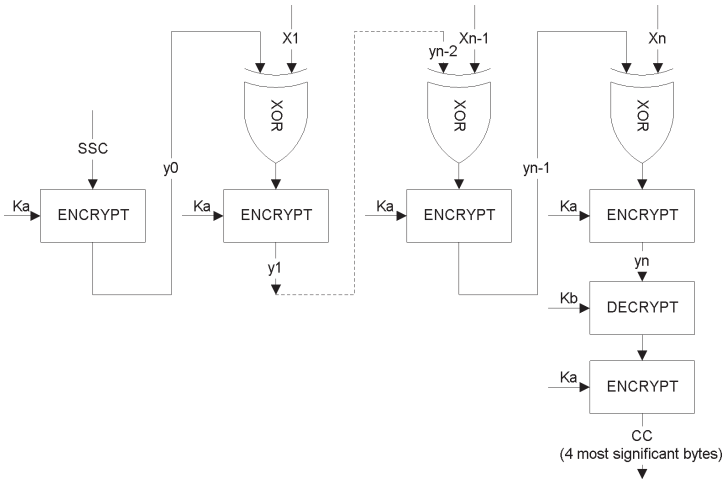
▼B

CSM_029 Lähetysvaihelaskuri (SSC) on avaimesta sopimismenettelyn aluksi asetettava tilaan:

SSC:n alkutila: Rnd3 (4 vähiten merkitsevää tavua) || Rnd1 (4 vähiten merkitsevää tavua).

CSM_030 Lähetysvaihelaskurin arvoa on lisättävä yhdellä joka kerran ennen viestin todennuksen tarkistussumman (MAC) laskemista (ts. SSC:n arvo ensimmäiselle komennolle on SSC:n alkutila +1 ja SSC:n arvo ensimmäiselle vastaukselle on SSC:n alkutila + 2).

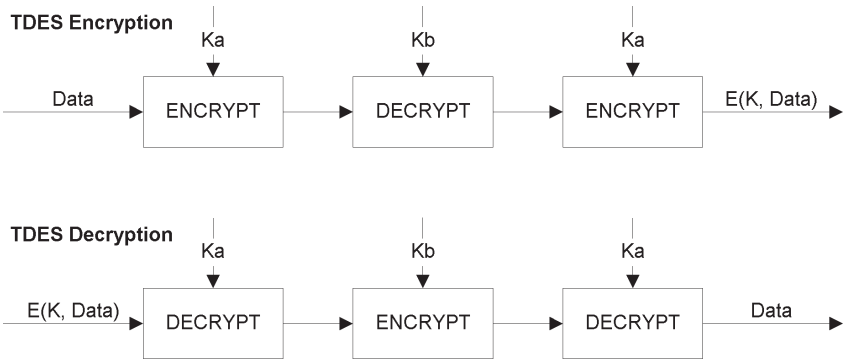
Seuraava kuva esittää retail MAC -tyyppisen viestin todennuksen tarkistussumman laskemista:



5.4. **Algoritmi salattavien dataobjektien kryptogrammien laskemiseksi**

CSM_031 Kryptogrammit lasketaan käyttäen viitteiden TDES ja TDES-OP mukaisesti kolminkertaista salausalgoritmia (TDEA) tilassa, jossa salauslohkot ketjutetaan (TCBC), ja siten, että ensimmäistä arvolohkoa edustaa nollavektori.

Seuraava kuva esittää avainten käyttöä TDES-salauksessa:



▼B

6. TIETOJEN KOPIOINNISSA KÄYTETTÄVÄT DIGITAALISET ALLEKIRJOITUSMEKANISMIT

CSM_032 Tietojen kopioimiseen ulkoisille tietovälineille tarkoitettu älykäs laite (IDE-laite) tallentaa laitteelta (ajoneuvoyksiköltä tai kortilta) yhden kopiointijakson aikana saadut tiedot yhteen fyysiseen tiedostoon. Tämän tiedoston on sisällettävä varmenteet MS_i.C ja EQT.C. Tiedosto sisältää datalohkojen digitaaliset allekirjoitukset siten kuin lisäyksessä 7 (Tietojen kopiointiprotokollat) on määritelty.

CSM_033 Kopioitujen tietojen digitaalisissa allekirjoituksissa on noudatettava sellaista lisäyksellä täydennettyä digitaalisen allekirjoituksen muodostamistapaa, joka sallii tietojen lukemisen haluttaessa ilman salauksen avaamista.

6.1. **Allekirjoituksen luominen**

CSM_034 Tietojen allekirjoituksen luomisessa on noudatettava viitteessä PKCS1 määriteltyä liitteellä täydennettyä SHA-1-hajautusfunktiota käyttävää allekirjoituksen muodostamiskaaviota:

Allekirjoitus = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1x(Data))]

PS = Arvoltaan ‘FF’ olevista tavuista muodostuva täyttömerkkijono, jolla pituus täydennetään 128 tavuksi.

DER(SHA-1(*M*)) on algoritmin tunnisteen koodaus Hash-hajautusfunktiota varten ja hajautusfunktion tuloksen koodaus ASN.1-standardin DigestInfo-datatyypin mukaiseksi (peruskoodaussäännöistä johdetut tiukemmat koodaussäännöt (DER, distinguished encoding rules)):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’||Hash-tulos.

6.2. **Allekirjoituksen todentaminen**

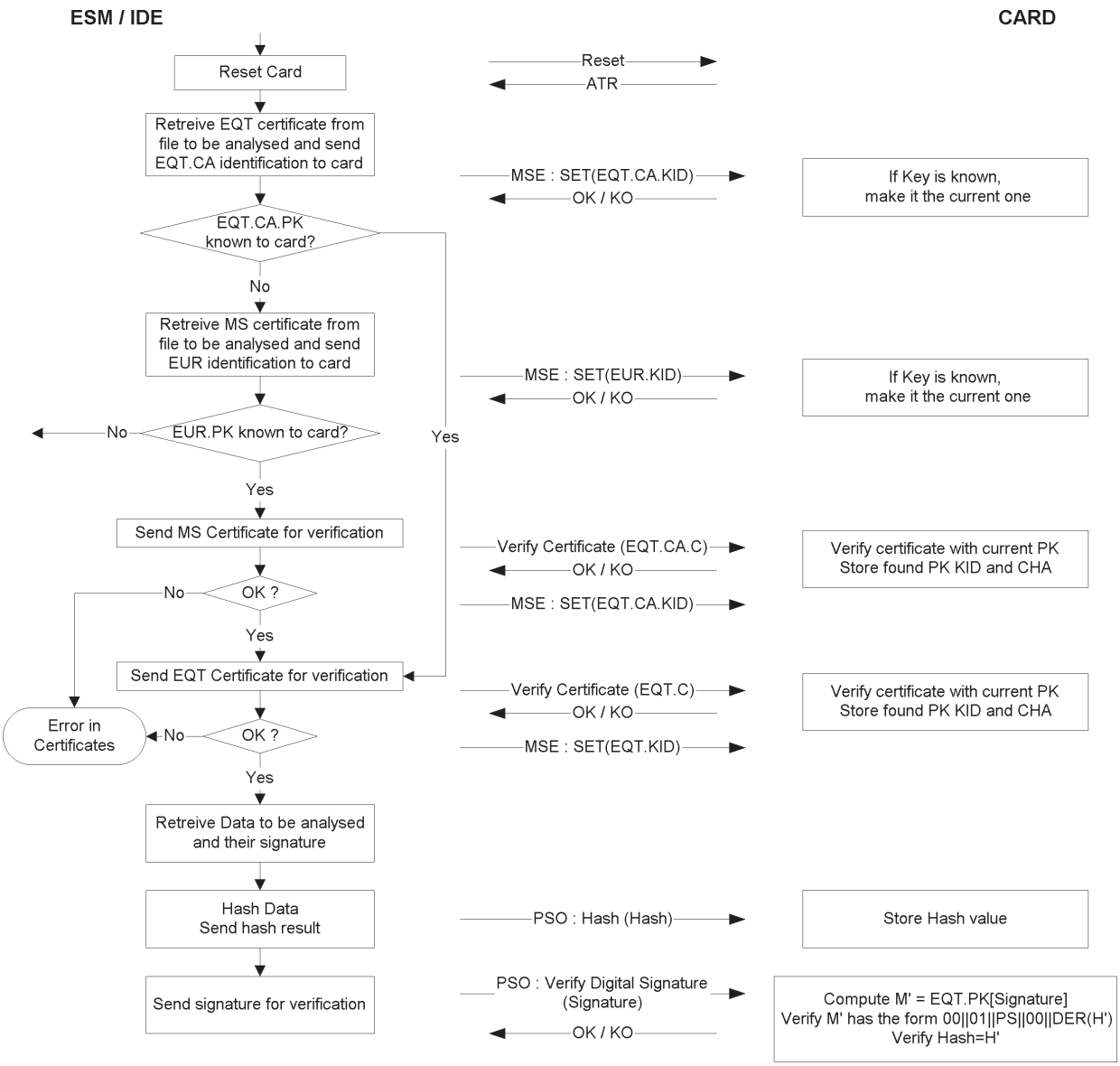
CSM_035 Kopioitujen tietojen allekirjoituksen todentamisessa on noudatettava viitteessä PKCS1 määriteltyä liitteellä täydennettyä SHA-1-hajautusfunktiota käyttävää allekirjoituksen muodostamiskaaviota.

Todennuksen tekijän on erikseen tiedettävä Euroopan julkinen avain EUR.PK (ja luotettava siihen).

Seuraava kaavio kuvaa protokollaa, jota IDE-laite, johon on asetettu valvontakortti, voi noudattaa todentaakseen ulkoiselle tietovälineelle (ESM, external storage media) tallennettujen tietojen eheyden. Valvontakorttia on käytetty purkamaan digitaalisten allekirjoitusten salaus. Tässä tapauksessa tätä toimintoa ei saa suorittaa IDE-laitteessa.

Analysoitavaa laitetta, josta tiedot on kopioitu ja joka on ne allekirjoittanut, kutsutaan lyhenteellä EQT.

▼B



OSA B

TOISEN SUKUPOLVEN AJOPIIRTURIJÄRJESTELMÄ

7. JOHDANTO

7.1. **Viitetiedot**

Lisäyksen tässä osassa käytetään seuraavia viitetietoja:

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), November 26, 2001
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
ISO 7816-4	ISO/IEC 7816-4, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. Third edition 2013-04-15
ISO 7816-8	ISO/IEC 7816-8, Identification cards – Integrated circuit cards – Part 8: Commands for security operations. Second edition 2004-06-01

▼B

ISO 8825-1	ISO/IEC 8825-1, Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15
ISO 9797-1	ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01
ISO 10116	ISO/IEC 10116, Information technology – Security techniques – Modes of operation of an *n*-bit block cipher. Third edition, 2006-02-01
ISO 16844-3	ISO/IEC 16844-3, Road vehicles – Tachograph systems – Part 3: Motion sensor interface. First edition 2004, including Technical Corrigendum 1 2006
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, March 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), May 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, March 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, version 2.00, 2012-06-28

7.2. **Merkintätavat ja lyhenteet**

Tässä lisäyksessä käytetään seuraavia merkintätapoja ja lyhenteitä:

AES	(Advanced encryption standard) AES-salaus
CA	(Certification authority) Varmenneviranomainen
CAR	(Certification authority reference) Varmenneviranomaisen viite
CBC	(Cipher block chaining mode of operation) Salauslohkoja ketjuttava käyttötila
CH	(Command header) Komennon ylätunniste
CHA	(Certificate holder authorisation) Varmenteen haltijan valtuutus
CHR	(Certificate holder reference) Varmenteen haltijan viite
CV	(Constant vector) Vakiovektori
DER	(Distinguished encoding rules) Peruskoodaussäännöistä johdetut tiukemmat koodaussäännöt
DO	(Data object) Dataobjekti
DSRC	(Dedicated short range communication) Lyhyen kantaman DSRC-tiedonsiirto
ECC	(Elliptic curve cryptography) Elliptisen käyrän salaus
ECDSA	(Elliptic curve digital signature algorithm) Elliptisen käyrän digitaalinen allekirjoitusalgoritmi
ECDH	(Elliptic curve Diffie-Hellman) Elliptisen käyrän Diffie-Hellmanin menetelmä (avaimesta sopimisen algoritmi)
EGF	(External GNSS facility) Ulkoinen GNSS-laitteisto
EQT	(Equipment) Laitteet

▼B

IDE	(Intelligent dedicated equipment) Tietojen kopioimiseen ulkoisille tietovälineille tarkoitettu älykäs laite (IDE-laite)
K_M	Liiketunnistimen pääavain, joka mahdollistaa ajoneuvoyksikön liittämisen liiketunnistimeen
$K_{M\text{-}VU}$	Ajoneuvoyksikköön asetettava avain, jonka avulla ajoneuvoyksikkö saa liiketunnistimen pääavaimen, jos ajoneuvoyksikköön on asetettu korjaamokortti
$K_{M\text{-}WC}$	Korjaamokorttiin asetettava avain, jonka avulla ajoneuvoyksikkö saa liiketunnistimen pääavaimen, jos ajoneuvoyksikköön on asetettu korjaamokortti
MAC	(Message authentication code) Sanoman autentikointikoodi
MoS	(Motion sensor) Liiketunnistin
MSB	(Most significant bit) Eniten merkitsevä bitti
PKI	(Public key infrastructure) Julkisen avaimen järjestelmä
RCF	(Remote communication facility) Etäviestintälaitteisto
SSC	(Send sequence counter) Lähetysvaihelaskuri
SM	(Secure messaging) Salattu sanomanvälitys
TDES	(Triple data encryption standard) Kolminkertainen DES-salaus
TLV	(Tag length value) TLV-koodaustapa; tuntomerkki-pituus-sisältö-koodaustapa
VU	(Vehicle unit) Ajoneuvoyksikkö
X.C	Käyttäjä X:n julkisen avaimen varmenne
X.CA	Varmenneviranomainen, joka myönsi käyttäjä X:n varmenteen
X.CAR	Käyttäjä X:n varmenteessa mainittu varmenneviranomaisen viite
X.CHR	Käyttäjä X:n varmenteessa mainittu varmenteen haltijan viite
X.PK	Käyttäjä X:n julkinen avain
X.SK	Käyttäjä X:n yksityinen avain
$X.PK_{eph}$	Käyttäjä X:n lyhytaikainen julkinen avain
$X.SK_{eph}$	Käyttäjä X:n lyhytaikainen yksityinen avain
‘xx’	Heksadesimaalilukuna ilmaistu arvo
||	Ketjutusmerkki

7.3. **Määritelmät**

Tässä lisäyksessä käytettyjen termien määritelmät sisältyvät liitteessä 1C olevaan I lukuun.

8. SALAUSJÄRJESTELMÄT JA -ALGORITMIT

8.1. **Salausjärjestelmät**

CSM_38 Ajoneuvoyksikköjen ja ajopiirturikorttien on käytettävä elliptiseen käyrään perustuvaa julkisen avaimen salausjärjestelmää luomaan seuraavat tietoturvamekanismit:

— ajoneuvoyksikön ja kortin molemminpuolinen todentaminen,

▼B

— tilapäisestä AES-avaimesta sopiminen ajoneuvoyksikön ja kortin välillä,

— ajoneuvoyksiköistä tai ajopiirturikorteilta ulkoisille tietovälineille kopioitujen tietojen aitouden, eheyden ja kiistämättömyyden varmistaminen.

CSM_39 Ajoneuvoyksikköjen ja ulkoisten GNSS-laitteistojen on käytettävä elliptiseen käyrään perustuvaa julkisen avaimen salausjärjestelmää luomaan seuraavat tietoturvamekanismit:

— ajoneuvoyksikön ja ulkoisen GNSS-laitteiston kytkeminen,

— ajoneuvoyksikön ja ulkoisen GNSS-laitteiston molemminpuolinen todentaminen,

— tilapäisestä AES-avaimesta sopiminen ajoneuvoyksikön ja ulkoisen GNSS-laitteiston välillä.

CSM_40 Ajoneuvoyksikköjen ja ajopiirturikorttien on käytettävä symmetristä AES-salausjärjestelmää luomaan seuraavat tietoturvamekanismit:

— ajoneuvoyksikön ja ajopiirturikortin välillä vaihdettujen tietojen aitouden ja eheyden varmistaminen,

— tarvittaessa ajoneuvoyksikön ja ajopiirturikortin välillä vaihdettujen tietojen luottamuksellisuuden varmistaminen.

CSM_41 Ajoneuvoyksikköjen ja ulkoisten GNSS-laitteistojen on käytettävä symmetristä AES-salausjärjestelmää luomaan seuraavat tietoturvamekanismit:

— ajoneuvoyksikön ja ulkoisen GNSS-laitteiston välillä vaihdettujen tietojen aitouden ja eheyden varmistaminen.

CSM_42 Ajoneuvoyksikköjen ja liiketunnistimien on käytettävä symmetristä AES-salausjärjestelmää luomaan seuraavat tietoturvamekanismit:

— ajoneuvoyksikön liittäminen liiketunnistimeen,

— ajoneuvoyksikön ja liiketunnistimen molemminpuolinen todentaminen,

— ajoneuvoyksikön ja liiketunnistimen välillä vaihdettujen tietojen luottamuksellisuuden varmistaminen.

CSM_43 Ajoneuvoyksikköjen ja valvontakorttien on käytettävä symmetristä AES-salausjärjestelmää luomaan seuraavat tietoturvamekanismit etäyhteyden rajapinnassa:

— ajoneuvoyksiköstä valvontakortille lähetettyjen tietojen luottamuksellisuuden, aitouden ja eheyden varmistaminen.

Huomautuksia:

— Tarkemmin ilmaistuna tiedot lähetetään ajoneuvoyksiköstä tarkastajan hallinnassa olevaan etäkyselylaitteeseen ajoneuvoyksikön sisäisen tai ulkoisen etäviestintälaitteiston kautta, ks. lisäys 14. Etäkyselylaite lähettää

▼B

vastaanotetut tiedot kuitenkin valvontakortille tietojen salauksen avaamista ja tietojen aitouden vahvistamista varten. Tietoturvan kannalta etäviestintälaitteiston ja etäkyselylaitteen on oltava täysin läpinäkyviä.

— Korjaamokortissa on samat DSRC-rajapintaa koskevat tietoturvamekanismit kuin valvontakortissa. Siten korjaamo voi vahvistaa ajoneuvoyksikön etäyhteyden rajapinnan asianmukaisen toiminnan, mukaan lukien tietoturvan. Ks. lisätietoa 9.2.2 kohdassa.

8.2. **Salausalgoritmit**

8.2.1 *Symmetriset algoritmit*

CSM_44 Ajoneuvoyksikköjen, ajopiirturikorttien, liiketunnistimien ja ulkoisten GNSS-laitteistojen on tuettava viitteessä AES määriteltyä AES-algoritmia, missä avaimen pituus on 128, 192 ja 256 bittiä.

8.2.2 *Epäsymmetriset algoritmit ja standardoidut domain-parametrit*

CSM_45 Ajoneuvoyksikköjen, ajopiirturikorttien ja ulkoisten GNSS-laitteistojen on tuettava elliptisen käyrän salausta, missä avaimen pituus on 256, 384 ja 512/521 bittiä.

CSM_46 Ajoneuvoyksikköjen, ajopiirturikorttien ja ulkoisten GNSS-laitteistojen on tuettava viitteessä DSS määriteltyä ECDSA-allekirjoitusalgoritmia.

CSM_47 Ajoneuvoyksikköjen, ajopiirturikorttien ja ulkoisten GNSS-laitteistojen on tuettava viitteessä TR-03111 määriteltyä avaimesta sopimisen ECKA-EG-algoritmia.

CSM_48 Ajoneuvoyksikköjen, ajopiirturikorttien ja ulkoisten GNSS-laitteistojen on tuettava kaikkia jäljempänä Taulukko 1 määriteltyjä, elliptisen käyrän salaukseen käytettäviä standardoituja domain-parametreja.

Taulukko 1

Standardoidut domain-parametrit

Nimi	Koko (bittiä)	Viite	Oliotunniste
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`

▼B

Huomautus: Taulukko 1 viimeisessä sarakkeessa luetellut oliotunnisteet määritellään viitteessä RFC 5639 Brainpool-käyrien osalta ja viitteessä RFC 5480 NIST-käyrien osalta.

Esimerkki 1: BrainpoolP256r1-käyrän oliotunniste on

```
{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}.
```

Tai pistenotaatiossa: `1.3.36.3.3.2.8.1.1.7.`

Esimerkki 2: NIST P-384 -käyrän oliotunniste on

```
{iso(1) identified-organization(3) certicom(132) curve(0) 34}.
```

Tai pistenotaatiossa: `1.3.132.0.34.`

8.2.3 *Hajautusalgoritmit*

CSM_49 Ajoneuvoyksikköjen ja ajopiirturikorttien on tuettava viitteessä SHS määriteltyjä SHA-256-, SHA-384- ja SHA-512-algoritmeja.

8.2.4 *Salausohjelmat (cipher suite)*

CSM_50 Symmetristen algoritmien tapauksessa epäsymmetrinen algoritmi ja/tai hajautusalgoritmi muodostavat yhdessä turvallisuusprotokollan, ja niiden avaimen pituuden ja hash-koon on oltava (suunnilleen) samanlaiset. Taulukko 2 esitetään sallitut salausohjelmat:

Taulukko 2

Sallitut salausohjelmat

Salausohjelman tunniste	ECC-avaimen koko (bittiä)	AES-avaimen pituus (bittiä)	Hajautusalgoritmi	MAC-koodin pituus (tavua)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Huomautus: 512- ja 521-bittisten ECC-avainten koon katsotaan olevan vahvuudeltaan vastaava tätä lisäystä sovellettaessa.

9. AVAIMET JA VARMENTEET

9.1. **Epäsymmetriset avainparit ja julkisen avaimen varmenteet**

9.1.1 *Yleistä*

Huomautus: Tässä kohdassa kuvattuja avaimia käytetään ajoneuvoyksikköjen ja ajopiirturikorttien sekä ajoneuvoyksikköjen ja ulkoisten GNSS-laitteistojen väliseen molemminpuoliseen todentamiseen ja salattuun sanomanvälitykseen. Prosessit kuvataan yksityiskohtaisesti tämän lisäyksen 10 ja 11 luvuissa.

CSM_51 Eurooppalaisessa älykkäässä ajopiirturijärjestelmässä ECC-avainpareja ja vastaavia varmenteita on luotava ja hallittava kolmella toiminnallisesti hierarkkisella tasolla:

— eurooppalaisella tasolla,

— jäsenvaltiotasolla,

— laitetasolla.

▼B

CSM_52 Koko eurooppalaisessa älykkäässä ajopiirturijärjestelmässä julkisia ja yksityisiä avaimia ja varmenteita on luotava, hallittava ja annettava tiedoksi käyttäen standardoituja ja suojattuja menetelmiä.

9.1.2 *Eurooppalainen taso*

CSM_53 Eurooppalaisella tasolla on luotava yksi ainutkertainen ECC-avainpari, joka nimetään EUR. Sen on koostuttava yksityisestä avaimesta (EUR.SK) ja julkisesta avaimesta (EUR.PK). Tämän avainparin on muodostettava koko eurooppalaisen älykkään ajopiirturijärjestelmän julkisen avaimen järjestelmän (PKI) juuriavainpari. Euroopan juurivarmenneviranomaisen (ERCA, European Root Certificate Authority) on hoidettava tämä tehtävä Euroopan komission valtuuttamana ja vastuulla.

CSM_54 ERCA:n on käytettävä eurooppalaista yksityistä avainta, jolla se allekirjoittaa eurooppalaisen julkisen avaimen (itse allekirjoitetun) juurivarmenteen, ja annettava tämä eurooppalainen juurivarmenne tiedoksi kaikille jäsenvaltioille.

CSM_55 ERCA:n on käytettävä eurooppalaista yksityistä avainta, jolla se allekirjoittaa pyynnöstä jäsenvaltioiden julkiset avaimet. ERCA:n on pidettävä rekisteriä kaikista allekirjoitetuista jäsenvaltioiden julkisen avaimen varmenteista.

CSM_56 Kuten jäljempänä 9.1.7 kohdassa olevassa kaaviossa 1 esitetään, ERCA:n on luotava uusi eurooppalainen juuriavainpari 17 vuoden välein. Kun ERCA luo uuden eurooppalaisen juuriavainparin, sen on luotava uudelle eurooppalaiselle julkiselle avaimelle uusi itse allekirjoitettu juurivarmenne. Eurooppalainen juurivarmenne on voimassa 34 vuotta ja kolme kuukautta.

Huomautus: Uuden juuriavainparin käyttöönotto tarkoittaa, että ERCA luo uuden liiketunnistimen pääavaimen sekä uuden DSRC-pääavaimen, ks. 9.2.1.2 ja 9.2.2.2 kohta.

CSM_57 Ennen uuden eurooppalaisen juuriavainparin luomista ERCA:n on tutkittava uuden avainparin edellyttämä salauksen vahvuus ottaen huomioon, että avainparin on oltava salattuna seuraavat 34 vuotta. Tarvittaessa ERCA:n on vaihdettava käytössä oleva salausohjelma vahvempaan siten kuin CSM_50 alakohdassa on määritelty.

CSM_58 Kun ERCA luo uuden eurooppalaisen juuriavainparin, sen on luotava uudelle eurooppalaiselle julkiselle avaimelle linkkivarmenne ja allekirjoitettava se edellisellä eurooppalaisella yksityisellä avaimella. Linkkivarmenne on voimassa 17 vuotta. Tämä esitetään myös jäljempänä 9.1.7 kohdassa olevassa kaaviossa 1.

Huomautus: Koska linkkivarmenne sisältää ERCA:n *X*-sukupolven julkisen avaimen ja se allekirjoitetaan ERCA:n *X-1*-sukupolven yksityisellä avaimella, linkkivarmenne tarjoaa menetelmän, jolla *X-1*-sukupolven laite voi luottaa *X*-sukupolven laitteeseen.

CSM_59 ERCA ei saa käyttää juuriavainparin yksityistä avainta mihinkään tarkoitukseen sen jälkeen, kun uusi juuriavaimen varmenne tulee voimaan.

▼B

CSM_60 ERCA:n on ajankohdasta riippumatta saatava käyttöönsä seuraavat salausavaimet ja varmenteet:

— voimassa oleva EUR-avainpari ja vastaava varmenne

— kaikki aikaisemmat EUR-varmenteet, joita käytetään vielä voimassa olevien, jäsenvaltion varmenneviranomaisen varmenteiden todentamiseen

— ensimmäistä lukuun ottamatta kaikkien sukupolvien EUR-varmenteiden linkkivarmenteet.

9.1.3 *Jäsenvaltiotaso*

CSM_61 Jäsenvaltiotasolla kaikkien jäsenvaltioiden, joiden on allekirjoitettava ajopiirturikortin varmenteita, on luotava yksi tai useampi ainutkertainen ECC-avainpari, joka nimetään MSCA_Card. Kaikkien jäsenvaltioiden, joiden on allekirjoitettava ajoneuvoyksikköjen tai ulkoisten GNSS-laitteistojen varmenteita, on lisäksi luotava yksi tai useampi ainutkertainen ECC-avainpari, joka nimetään MSCA_VU-EGF.

CSM_62 Jäsenvaltion varmenneviranomaisen (MSCA) on luotava jäsenvaltioiden avainparit. Kun jäsenvaltion varmenneviranomainen luo jäsenvaltion avainparin, sen on lähetettävä julkinen avain ERCA:lle saadakseen ERCA:n allekirjoittaman vastaavan jäsenvaltion varmenteen.

CSM_63 Jäsenvaltion varmenneviranomaisen on valittava jäsenvaltion avainparin vahvuus, joka vastaa vastaavan jäsenvaltion varmenteen allekirjoittamiseen käytettävän eurooppalaisen juuriavainparin vahvuutta.

CSM_64 Mahdollisen MSCA_VU-EGF-avainparin on koostuttava yksityisestä avaimesta MSCA_VU-EGF.SK ja julkisesta avaimesta MSCA_VU-EGF.PK. Jäsenvaltion varmenneviranomaisen on käytettävä yksityistä avainta MSCA_VU-EGF.SK yksinomaan ajoneuvoyksikköjen ja ulkoisten GNSS-laitteistojen julkisen avaimen varmenteiden allekirjoittamiseen.

CSM_65 MSCA_Card-avainparin on koostuttava yksityisestä avaimesta MSCA_Card.SK ja julkisesta avaimesta MSCA_Card.PK. Jäsenvaltion varmenneviranomaisen on käytettävä yksityistä avainta MSCA_Card.SK yksinomaan ajopiirturikorttien julkisen avaimen varmenteiden allekirjoittamiseen.

CSM_66 Jäsenvaltion varmenneviranomaisen on pidettävä rekisteriä kaikista allekirjoitetuista ajoneuvoyksikköjen varmenteista, ulkoisten GNSS-laitteistojen varmenteista ja korttien varmenteista sekä niiden laitteiden tunnisteista, joita varten kukin varmenne on tarkoitettu.

CSM_67 MSCA_VU-EGF-varmenne on voimassa 17 vuotta ja kolme kuukautta. MSCA_Card-varmenne on voimassa 7 vuotta ja yhden kuukauden.

CSM_68 Kuten 9.1.7 kohdassa olevassa kaaviossa 1 esitetään, MSCA_VU-EGF-avainparin yksityisen avaimen ja MSCA_Card-avainparin yksityisen avaimen käyttöajan on oltava kaksi vuotta.

▼B

CSM_69 Jäsenvaltion varmenneviranomainen ei saa käyttää MSCA_VU-EGF-avainparin yksityistä avainta mihinkään tarkoitukseen sen jälkeen, kun sen käyttöaika on päättynyt. Jäsenvaltion varmenneviranomainen ei myöskään saa käyttää MSCA_Card-avainparin yksityistä avainta mihinkään tarkoitukseen sen jälkeen, kun sen käyttöaika on päättynyt.

CSM_70 Jäsenvaltion varmenneviranomaisen on ajankohdasta riippumatta saatava käyttöönsä seuraavat salausavaimet ja varmenteet:

— voimassa oleva MSCA_Card-avainpari ja vastaava varmenne

— kaikki aikaisemmat MSCA_Card-varmenteet, joita käytetään vielä voimassa olevien ajopiirturikorttien varmenteiden todentamiseen

— voimassa oleva EUR-varmenne, jota tarvitaan voimassa olevan jäsenvaltion varmenneviranomaisen varmenteen todentamiseen

— kaikki aikaisemmat EUR-varmenteet, joita tarvitaan kaikkien vielä voimassa olevien jäsenvaltion varmenneviranomaisen varmenteiden todentamiseen.

CSM_71 Jos jäsenvaltion varmenneviranomaisen on allekirjoitettava ajoneuvoyksikköjen tai ulkoisten GNSS-laitteistojen varmenteita, sen on lisäksi saatava käyttöönsä seuraavat avaimet ja varmenteet:

— voimassa oleva MSCA_VU-EGF-avainpari ja vastaava varmenne

— kaikki aikaisemmat julkiset avaimet MSCA_VU-EGF, joita käytetään vielä voimassa olevien ajoneuvoyksikköjen tai ulkoisten GNSS-laitteistojen varmenteiden todentamiseen.

9.1.4 *Laitetaso: ajoneuvoyksiköt*

CSM_72 Kutakin ajoneuvoyksikköä varten on luotava kaksi ainutkertaista ECC-avainparia, jotka nimetään VU_MA ja VU_Sign. Ajoneuvoyksikköjen valmistajat hoitavat tämän tehtävän. Kun luodaan ajoneuvoyksikön avainpari, avaimen luovan osapuolen on lähetettävä julkinen avain asuinjäsenvaltionsa varmenneviranomaiselle saadakseen jäsenvaltion varmenneviranomaisen allekirjoittaman vastaavan ajoneuvoyksikön varmenteen. Yksityistä avainta on käytettävä yksinomaan kyseisessä ajoneuvoyksikössä.

CSM_73 Tietyn ajoneuvoyksikön VU_MA- ja VU_Sign-varmenteilla on oltava sama voimaantulopäivä.

CSM_74 Ajoneuvoyksikön valmistajan on valittava ajoneuvoyksikön avainparin vahvuus, joka vastaa vastaavan ajoneuvoyksikön varmenteen allekirjoittamiseen käytettävän jäsenvaltion varmenneviranomaisen avainparin vahvuutta.

CSM_75 Ajoneuvoyksikön on käytettävä VU_MA-avainpariaan, joka koostuu yksityisestä avaimesta VU_MA.SK ja julkisesta avaimesta VU_MA.PK, yksinomaan ajoneuvoyksikön todentamiseen ajopiirturikortteja ja ulkoisia GNSS-laitteistoja kohtaan, kuten tämän lisäyksen 10.3 ja 11.4 kohdassa on määritelty.

CSM_76 Ajoneuvoyksikön on voitava luoda lyhytaikaisia ECC-avainpareja ja käytettävä lyhytaikaista avainparia yksinomaan tilapäisestä avaimesta sopimiseen ajopiirturikortin tai ulkoisen GNSS-laitteiston kanssa, kuten tämän lisäyksen 10.4 ja 11.4 kohdassa on määritelty.

▼B

CSM_77 Ajoneuvoyksikön on käytettävä VU_Sign-avainparinsa yksityistä avainta VU_Sign.SK yksinomaan kopioitujen tiedostojen allekirjoittamiseen, kuten tämän lisäyksen 14 luvussa on määritelty. Vastaavaa julkista avainta VU_Sign.PK on käytettävä yksinomaan ajoneuvoyksikön luomien allekirjoitusten todentamiseen.

CSM_78 Kuten jäljempänä 9.1.7 kohdassa olevassa kaaviossa 1 esitetään, VU_MA-varmenne on voimassa 15 vuotta ja kolme kuukautta. VU_Sign-varmenne on myös voimassa 15 vuotta ja kolme kuukautta.

Huomautuksia:

— VU_Sign-varmenteen pidennetty voimassaoloaika antaa ajoneuvoyksikölle mahdollisuuden luoda voimassa olevia allekirjoituksia kopioiduista tiedoista ensimmäisten kolmen kuukauden ajan voimassaolon päätyttyä, kuten vaaditaan asetuksessa (EU) N:o 581/2010.

— VU_MA-varmenteen pidennetty voimassaoloaika on tarpeen, jotta ajoneuvoyksikkö voi todentaa itsensä valvontakortille tai yrityskortille ensimmäisten kolmen kuukauden ajan voimassaolon päätyttyä esimerkiksi tietojen kopioimiseksi.

CSM_79 Ajoneuvoyksikkö ei saa käyttää ajoneuvoyksikön avainparin yksityistä avainta mihinkään tarkoitukseen sen jälkeen, kun vastaavan varmenteen voimassaolo on päättynyt.

CSM_80 Tietyn ajoneuvoyksikön avainpareja (lukuun ottamatta lyhytaikaisia avainpareja) ja vastaavia varmenteita ei saa niiden käyttöolosuhteissa korvata tai uusia sen jälkeen, kun ajoneuvoyksikkö on otettu käyttöön.

Huomautuksia:

— Tämä vaatimus ei koske lyhytaikaisia avainpareja, sillä ajoneuvoyksikkö luo uuden lyhytaikaisen avainparin aina, kun suoritetaan sirun todentaminen ja sovitaan tilapäisestä avaimesta, ks. 10.4 kohta. On huomattava, että lyhytaikaisilla avainpareilla ei ole vastaavia varmenteita.

— Tällä vaatimuksella ei kielletä mahdollisuutta korvata pysyviä ajoneuvoyksikön avainpareja kunnostuksen tai korjauksen aikana suojatuissa olosuhteissa ja ajoneuvoyksikön valmistajan valvonnassa.

CSM_81 Käyttöönoton jälkeen ajoneuvoyksikköjen on sisällettävä seuraavat salausavaimet ja varmenteet:

— yksityinen avain VU_MA ja vastaava varmenne

— yksityinen avain VU_Sign ja vastaava varmenne

— MSCA_VU-EGF-varmenne, joka sisältää VU_MA-varmenteen ja VU_Sign-varmenteen todentamiseen käytettävän julkisen avaimen MSCA_VU-EGF.PK

▼B

— EUR-varmenne, joka sisältää MSCA_VU-EGF-varmenteen todentamiseen käytettävän julkisen avaimen EUR.PK

— tarvittaessa EUR-varmenne, jonka voimassaoloaika edeltää MSCA_VU-EGF-varmenteen todentamiseen käytettävän EUR-varmenteen voimassaoloaikaa

— tarvittaessa näiden kahden EUR-varmenteen yhdistävä linkkivarmenne.

CSM_82 Edellä CSM_81 alakohdassa lueteltujen salausavainten ja varmenteiden lisäksi ajoneuvoyksikköjen on sisällettävä tämän lisäyksen osassa A luetellut avaimet ja varmenteet, jotta ajoneuvoyksikkö voi olla vuorovaikutuksessa ensimmäisen sukupolven ajopiirturikorttien kanssa.

9.1.5 *Laitetaso: ajopiirturikortit*

CSM_83 Kutakin ajopiirturikorttia varten luodaan yksi ainutkertainen ECC-avainpari, joka nimetään Card_MA. Lisäksi kutakin kuljettajakorttia ja korjaamokorttia varten luodaan toinen ainutkertainen ECC-avainpari, joka nimetään Card_Sign. Tämän tehtävän voi hoitaa kortin valmistaja tai se, joka syöttää korttiin haltijan henkilötiedot. Kun luodaan kortin avainpari, avaimen luovan osapuolen on lähetettävä julkinen avain asuinjäsenvaltionsa varmenneviranomaiselle saadakseen jäsenvaltion varmenneviranomaisen allekirjoittaman vastaavan kortin varmenteen. Yksityistä avainta on käytettävä yksinomaan kyseisessä ajopiirturikortissa.

CSM_84 Tietyn kuljettajakortin tai korjaamokortin Card_MA- ja Card_Sign-varmenteilla on oltava sama varmenteen voimaantulopäivä.

CSM_85 Kortin valmistajan tai sen, joka syöttää korttiin haltijan henkilötiedot, on valittava kortin avainparin vahvuus, joka vastaa vastaavan kortin varmenteen allekirjoittamiseen käytettävän jäsenvaltion varmenneviranomaisen avainparin vahvuutta.

CSM_86 Ajopiirturikortin on käytettävä Card_MA-avainpariaan, joka koostuu yksityisestä avaimesta Card_MA.SK ja julkisesta avaimesta Card_MA.PK, yksinomaan molemminpuoliseen todentamiseen ja tilapäisestä avaimesta sopimiseen ajoneuvoyksikköjen kanssa, kuten tämän lisäyksen 10.3 ja 10.4 kohdassa on määritelty.

CSM_87 Kuljettajakortin tai korjaamokortin on käytettävä Card_Sign-avainparinsa yksityistä avainta Card_Sign.SK yksinomaan tallennettujen tiedostojen allekirjoittamiseen, kuten tämän lisäyksen 14 luvussa on määritelty. Vastaavaa julkista avainta Card_Sign.PK on käytettävä yksinomaan kortin luomien allekirjoitusten todentamiseen.

CSM_88 Card_MA-varmenne on voimassa seuraavasti:

— kuljettajakorteissa: 5 vuotta

— yrityskorteissa: 2 vuotta

— valvontakorteissa: 2 vuotta

— korjaamokorteissa: 1 vuosi

▼B

CSM_89 Card_Sign-varmenne on voimassa seuraavasti:

— kuljettajakorteissa:	5 vuotta ja yksi kuukausi
— korjaamokorteissa:	1 vuosi ja yksi kuukausi

Huomautus: Card_Sign-varmenteen pidennetty voimassaoloaika antaa kuljettajakortille mahdollisuuden luoda voimassa olevia allekirjoituksia kopioiduista tiedoista ensimmäisen kuukauden ajan voimassaolon päätyttyä. Tämä on tarpeen, sillä asetuksessa (EU) N:o 581/2010 vaaditaan, että tietoja on voitava kopioida kuljettajakortilta enintään 28 päivää viimeisimpien tietojen tallennuksen jälkeen.

CSM_90 Tietyn ajopiirturikortin avainpareja ja vastaavia varmenteita ei saa korvata tai uusia sen jälkeen, kun kortti on myönnetty.

CSM_91 Myöntämisen jälkeen ajopiirturikorttien on sisällettävä seuraavat salausavaimet ja varmenteet:

— yksityinen avain Card_MA ja vastaava varmenne

— kuljettajakorteissa ja korjaamokorteissa lisäksi yksityinen avain Card_Sign ja vastaava varmenne

— MSCA_Card-varmenne, joka sisältää Card_MA-varmenteen ja Card_Sign-varmenteen todentamiseen käytetyn julkisen avaimen MSCA_Card.PK

— EUR-varmenne, joka sisältää MSCA_Card-varmenteen todentamiseen käytetyn julkisen avaimen EUR.PK

— tarvittaessa EUR-varmenne, jonka voimassaoloaika edeltää MSCA_Card-varmenteen todentamiseen käytettävän EUR-varmenteen voimassaoloaikaa

— tarvittaessa näiden kahden EUR-varmenteen yhdistävä linkkivarmenne.

CSM_92 Edellä CSM_91 alakohdassa lueteltujen salausavainten ja varmenteiden lisäksi ajopiirturikorttien on sisällettävä tämän lisäyksen osassa A luetellut avaimet ja varmenteet, jotta kortit voivat olla vuorovaikutuksessa ensimmäisen sukupolven ajoneuvoyksikköjen kanssa.

9.1.6 *Laitetaso: ulkoiset GNSS-laitteistot*

CSM_93 Kutakin ulkoista GNSS-laitteistoa varten luodaan yksi ainutkertainen ECC-avainpari, joka nimetään EGF_MA. Ulkoisten GNSS-laitteistojen valmistajat hoitavat tämän tehtävän. Kun luodaan EGF_MA-avainpari, julkinen avain on lähetettävä asuinjäsenvaltion varmenneviranomaiselle, jotta saadaan jäsenvaltion varmenneviranomaisen allekirjoittama vastaava EGF_MA-varmenne. Yksityistä avainta on käytettävä yksinomaan kyseisessä ulkoisessa GNSS-laitteistossa.

CSM_94 Ulkoisen GNSS-laitteiston valmistajan on valittava EGF_MA-avainparin vahvuus, joka vastaa vastaavan EGF_MA-varmenteen allekirjoittamiseen käytettävän jäsenvaltion varmenneviranomaisen avainparin vahvuutta.

▼B

CSM_95 Ulkoisen GNSS-laitteiston on käytettävä EGF_MA-avainpariaan, joka koostuu yksityisestä avaimesta EGF_MA.SK ja julkisesta avaimesta EGF_MA.PK, yksinomaan molemminpuoliseen todentamiseen ja tilapäisestä avaimesta sopimiseen ajoneuvoyksikköjen kanssa, kuten tämän lisäyksen 11.4 kohdassa on määritelty.

CSM_96 EGF_MA-varmenne on voimassa 15 vuotta.

CSM_97 Ulkoinen GNSS-laitteisto ei saa käyttää EGF_MA-avainparin yksityistä avainta ajoneuvoyksikköön kytkemiseen sen jälkeen, kun vastaavan varmenteen voimassaolo on päättynyt.

Huomautus: Kuten jäljempänä 11.3.3 kohdassa selitetään, ulkoinen GNSS-laitteisto voi käyttää yksityistä avaintaan molemminpuoliseen todentamiseen sen ajoneuvoyksikön kanssa, johon se on jo kytketty, vaikka vastaavan varmenteen voimassaolo olisi päättynyt.

CSM_98 Tietyn ulkoisen GNSS-laitteiston EGF_MA-avainparia ja vastaavaa varmennetta ei saa niiden käyttöolosuhteissa korvata tai uusia sen jälkeen, kun ulkoinen GNSS-laitteisto on otettu käyttöön.

Huomautus: Tällä vaatimuksella ei kielletä mahdollisuutta korvata ulkoisen GNSS-laitteiston avainpareja kunnostuksen tai korjauksen aikana suojatuissa olosuhteissa ja ulkoisen GNSS-laitteiston valmistajan valvonnassa.

CSM_99 Käyttöönoton jälkeen ulkoisen GNSS-laitteiston on sisällettävä seuraavat salausavaimet ja varmenteet:

— yksityinen avain EGF_MA ja vastaava varmenne

— MSCA_VU-EGF-varmenne, joka sisältää EGF_MA-varmenteen todentamiseen käytettävän julkisen avaimen MSCA_VU-EGF.PK

— EUR-varmenne, joka sisältää MSCA_VU-EGF-varmenteen todentamiseen käytettävän julkisen avaimen EUR.PK

— tarvittaessa EUR-varmenne, jonka voimassaoloaika edeltää MSCA_VU-EGF-varmenteen todentamiseen käytettävän EUR-varmenteen voimassaoloaikaa

— tarvittaessa näiden kahden EUR-varmenteen yhdistävä linkkivarmenne.

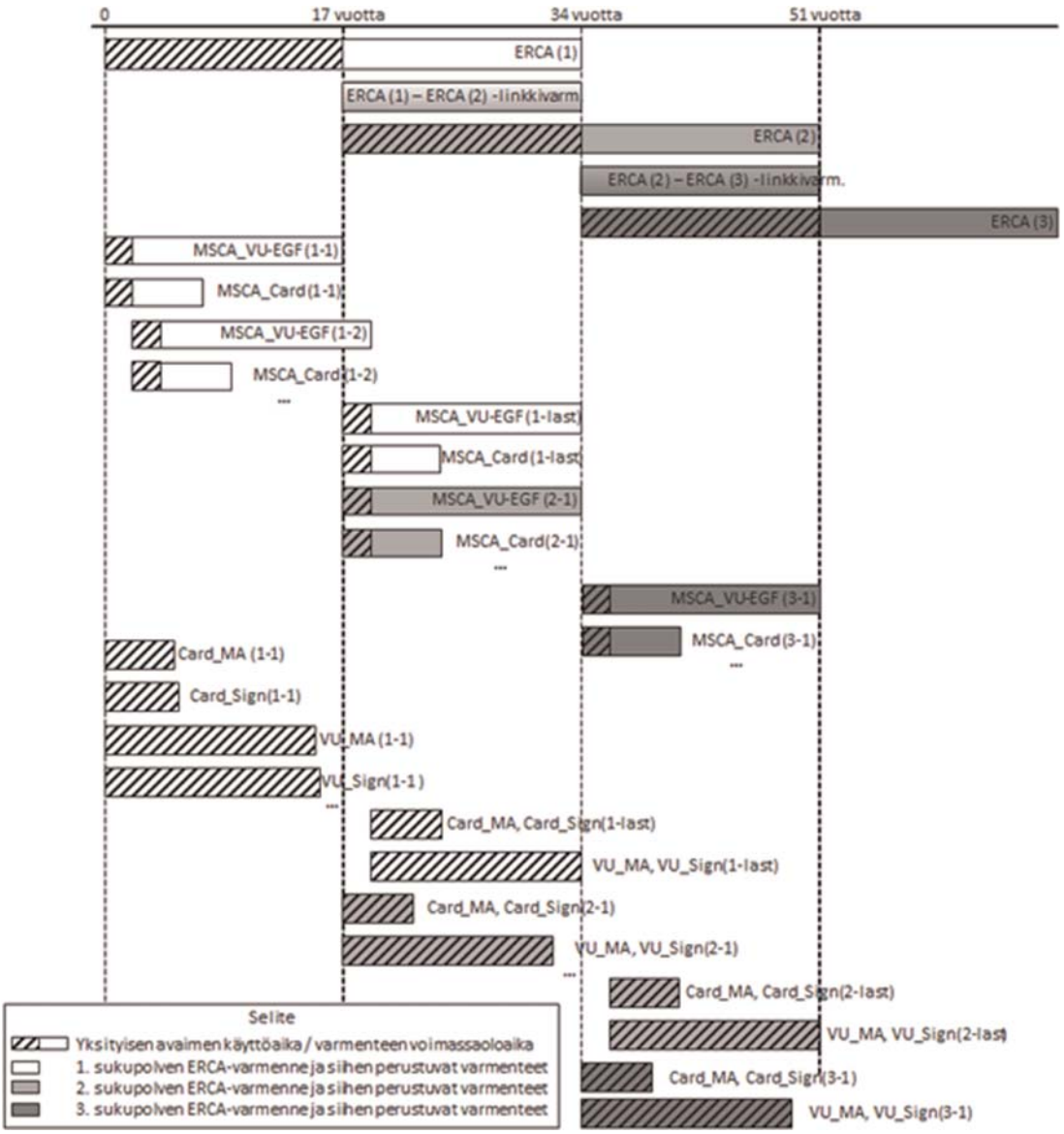
9.1.7 *Yhteenveto: varmenteen korvaus*

Jäljempänä kaaviossa 1 esitetään, miten eri sukupolvien ERCA:n juurivarmenteet, ERCA:n linkkivarmenteet, jäsenvaltion varmenneviranomaisen varmenteet ja laitteen (ajoneuvoyksikkö ja kortti) varmenteet annetaan ja miten niitä käytetään ajan kuluessa:

▼B

Kaavio 1

Eri sukupolvien ERCA:n juurivarmenteiden, ERCA:n linkkivarmenteiden, jäsenvaltion varmenneviranomaisen varmenteiden ja laitteen varmenteiden antaminen ja käyttö



Huomautuksia kaaviossa 1:

1. Juurivarmenteen eri sukupolvet ilmoitetaan sulkeissa olevalla numerolla. Esim. ERCA (1) on ensimmäisen sukupolven ja ERCA (2) toisen sukupolven ERCA:n juurivarmenne.

2. Muut varmenteet ilmoitetaan sulkeissa olevilla kahdella numerolla siten, että ensimmäinen numero tarkoittaa sen juurivarmenteen sukupolvea, jonka perusteella varmenteet on annettu, ja toinen numero tarkoittaa itse varmenteen sukupolvea. Esim. MSCA_Card (1-1) on ERCA (1) -juurivarmenteen perusteella annettu ensimmäinen MSCA_Card-varmenne; MSCA_Card (2-1) on ERCA (2) -juurivarmenteen perusteella annettu ensimmäinen MSCA_Card-varmenne; MSCA_Card (2-last) on ERCA (2) -juurivarmenteen perusteella annettu viimeinen MSCA_Card-varmenne; Card_MA(2-1) on ERCA (2) -juurivarmenteen perusteella annettu ensimmäinen kortin varmenne molemminpuolista todentamista varten.

▼B

3. Varmenteet MSCA_Card (2-1) ja MSCA_Card (1-last) on annettu lähes samana päivänä. MSCA_Card (2-1) on ERCA (2) -juurivarmenteen perusteella annettu ensimmäinen MSCA_Card-varmenne, ja se annetaan vain hieman myöhemmin kuin MSCA_Card (1-last), joka on ERCA (1) -juurivarmenteen perusteella annettu viimeinen MSCA_Card-varmenne.

4. Kuten kaaviossa esitetään, ERCA (2) -juurivarmenteen perusteella annetut ensimmäiset ajoneuvoyksikön ja kortin varmenteet ilmestyvät lähes kaksi vuotta ennen ERCA (1) -juurivarmenteen perusteella annettuja viimeisiä ajoneuvoyksikön ja kortin varmenteita. Tämä johtuu siitä, että ajoneuvoyksikön ja kortin varmenteet annetaan jäsenvaltion varmenneviranomaisen varmenteen perusteella eikä suoraan ERCA:n varmenteen perusteella. MSCA (2-1) annetaan heti sen jälkeen, kun ERCA (2) -juurivarmenne tulee voimaan, mutta MSCA (1-last) annetaan vain vähän tätä ennen eli ERCA (1) -juurivarmenteen voimassaolon viime hetkillä. Siten näillä kahdella jäsenvaltion varmenneviranomaisen varmenteella on lähes sama voimassaoloaika, vaikka ne ovat eri sukupolvien varmenteita.

5. Korttien osalta voimassaoloaika on sama kuin kuljettajakorttien osalta (5 vuotta).

6. Tilan säästämiseksi Card_MA- ja Card_Sign-varmenteiden sekä VU_MA- ja VU_Sign-varmenteiden voimassaoloaikojen ero esitetään ainoastaan ensimmäisen sukupolven osalta.

9.2. **Symmetriset avaimet**

9.2.1 *Ajoneuvoyksikön ja liiketunnistimen välisen viestinnän salausavaimet*

9.2.1.1 *Yleistä*

Huomautus: Tämän kohdan lukijoiden oletetaan tuntevan ISO 16844-3 -standardin sisältö, jossa kuvataan ajoneuvoyksikön ja liiketunnistimen välistä rajapintaa. Ajoneuvoyksikön ja liiketunnistimen välinen liittämisprosessi kuvataan yksityiskohtaisesti tämän lisäyksen 12 luvussa.

CSM_100 Ajoneuvoyksikköjen ja liiketunnistimien liittämistä, molemminpuolista todentamista sekä niiden välisen viestinnän salaamista varten tarvitaan useita symmetrisiä avaimia, kuten esitetään Taulukko 3. Kaikkien näiden avainten on oltava AES-avaimia, joissa avaimen pituus vastaa liiketunnistimen pääavaimen pituutta ja on sidoksissa (suunnitellun) eurooppalaisen juuriavainparin pituuteen, siten kuin CSM_50 alakohdassa on kuvattu.

Taulukko 3

Ajoneuvoyksikön ja liiketunnistimen välisen viestinnän salausavaimet

Avain	Symboli	Luonut	Luontimenetelmä	Tallentanut
Liiketunnistimen pääavain – VU-osa	$K_{M\text{-}VU}$	ERCA	Satunnainen	ERCA, VU-varmenteita antavat MSCA:t, ajoneuvoyksikköjen valmistajat, ajoneuvoyksiköt
Liiketunnistimen pääavain – Korjaamo-osa	$K_{M\text{-}WC}$	ERCA	Satunnainen	ERCA, MSCA:t, korttien valmistajat, korjaamokortit

▼B

Avain	Symboli	Luonut	Luontimenetelmä	Tallentanut
Liiketunnistimen pääavain	K_M	Ei luoda itsenäisesti	Lasketaan $K_M = K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$	ERCA, liiketunnistimen avaimia myöntävät MSCA:t (vapaaehtoinen) (*)
Tunnistusavain	K_{ID}	Ei luoda itsenäisesti	Lasketaan $K_{ID} = K_M$ XOR CV, missä CV on siten kuin CSM_106 alakohdassa on määritelty	ERCA, liiketunnistimen avaimia myöntävät MSCA:t (vapaaehtoinen) (*)
Liittämisavain	K_P	Liiketunnistimen valmistaja	Satunnainen	Yksi liiketunnistin
Tilapäinen avain	K_S	Ajoneuvoyksikkö (ajoneuvoyksikön ja liiketunnistimen liittämisen aikana)	Satunnainen	Yksi ajoneuvoyksikkö ja yksi liiketunnistin

(*) K_M- ja K_{ID}-avainten tallentaminen on vapaaehtoista, sillä ne voidaan luoda myös avainten $K_{M\text{-}VU}$, $K_{M\text{-}WC}$ ja vakiovektorin (CV) perusteella.

CSM_101 Euroopan juurivarmenneviranomaisen (ERCA) on luotava kaksi satunnaista ja ainutkertaista AES-avainta $K_{M\text{-}VU}$ ja $K_{M\text{-}WC}$, joista liiketunnistimen K_M-pääavain voidaan laskea kaavalla $K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$. ERCA:n on annettava avaimet K_M, $K_{M\text{-}VU}$ ja $K_{M\text{-}WC}$ tiedoksi jäsenvaltioiden varmenneviranomaisille niiden pyynnöstä.

CSM_102 ERCA:n on annettava kullekin liiketunnistimen K_M-pääavaimelle yksilöllinen versionumero, jota käytetään myös avainten $K_{M\text{-}VU}$ ja $K_{M\text{-}WC}$ sekä niihin liittyvän tunnistusavaimen K_{ID} muodostamiseen. ERCA:n on ilmoitettava jäsenvaltioiden varmenneviranomaisille versionumero lähettäessään niille avaimet $K_{M\text{-}VU}$ ja $K_{M\text{-}WC}$.

Huomautus: Versionumeroa käytetään näiden avainten eri sukupolvien erottamiseen, kuten 9.2.1.2 kohdassa yksityiskohtaisesti selitetään.

CSM_103 Jäsenvaltion varmenneviranomaisen on välitettävä $K_{M\text{-}VU}$-avain sekä sen versionumero ajoneuvoyksikköjen valmistajille niiden pyynnöstä. Ajoneuvoyksikköjen valmistajien on asennettava $K_{M\text{-}VU}$-avain ja sen versionumero kaikkiin valmistettuihin ajoneuvoyksiköihin.

CSM_104 Jäsenvaltion varmenneviranomaisen on varmistettava, että $K_{M\text{-}WC}$-avain ja sen versionumero asennetaan kaikkiin sen vastuulla myönnettyihin korjaamokortteihin.

Huomautuksia:

— Ks. datatyypin `SensorInstallationSecData` kuvaus lisäyksessä 2.

— Kuten jäljempänä 9.2.1.2 kohdassa selitetään, yhteen korjaamokorttiin voi olla tarpeen asentaa usean sukupolven $K_{M\text{-}WC}$-avaimia.

▼B

CSM_105 Edellä CSM_104 alakohdassa määritellyn AES-avaimen lisäksi jäsenvaltion varmenneviranomaisen on varmistettava, että kaikkiin sen vastuulla myönnettyihin korjaamokortteihin asennetaan TDES-avain Km_{WC}, siten kuin tämän lisäyksen osassa A olevassa CSM_037 alakohdassa on määritelty.

Huomautuksia:

— Tämä mahdollistaa ensimmäisen sukupolven ajoneuvoyksikön kytkemisen toisen sukupolven korjaamokortilla.

— Toisen sukupolven korjaamokortti sisältää kaksi erilaista sovellusta, joista toinen täyttää tämän lisäyksen osan B vaatimukset ja toinen osan A vaatimukset. Jälkimmäinen sisältää TDES-avaimen Km_{WC}.

CSM_106 Liiketunnistimien myöntämiseen osallistuvan jäsenvaltion varmenneviranomaisen on luotava tunnistusavain liiketunnistimen pääavaimesta XORaamalla se vakiovektorilla (CV). Vakiovektorin arvo on seuraava:

— 128-bittisten liiketunnistimen pääavainten osalta: CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83’

— 192-bittisten liiketunnistimen pääavainten osalta: 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-bittisten liiketunnistimen pääavainten osalta: 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’

Huomautus: Vakiovektorit on luotu seuraavasti:

Pi_10 = matemaattisen vakion π = ‘24 3F 6A 88 85 A3 08 D3 13 19’ desimaaliosan 10 ensimmäistä tavua

CV_128-bits = SHA-256(Pi_10):n 16 ensimmäistä tavua

CV_192-bits = SHA-384(Pi_10):n 24 ensimmäistä tavua

CV_256-bits = SHA-512(Pi_10):n 32 ensimmäistä tavua

CSM_107 Liiketunnistimien valmistajien on luotava kullekin liiketunnistimelle satunnainen ja ainutkertainen liittämisavain K_P ja lähetettävä kaikki liittämisavaimet jäsenvaltion varmenneviranomaiselle. Jäsenvaltion varmenneviranomaisen on salattava kukin liittämisavain erikseen liiketunnistimen pääavaimella K_M ja lähetettävä salattu avain liiketunnistimen valmistajalle. Jäsenvaltion varmenneviranomaisen on ilmoitettava liiketunnistimen valmistajalle kunkin salatun avaimen osalta siihen liittyvän K_M-avaimen versionumero.

Huomautus: Kuten 9.2.1.2 kohdassa selitetään, liiketunnistimen valmistajan voi olla tarpeen luoda useita ainutkertaisia liittämisavaimia yhtä liiketunnistinta varten.

▼B

CSM_108 Liiketunnistimien valmistajien on luotava kullekin liiketunnistimelle ainutkertainen sarjanumero ja lähetettävä kaikki sarjanumerot jäsenvaltion varmenneviranomaiselle. Jäsenvaltion varmenneviranomaisen on salattava kukin sarjanumero erikseen tunnistusavaimella K_{ID} ja lähetettävä salattu sarjanumero liiketunnistimen valmistajalle. Jäsenvaltion varmenneviranomaisen on ilmoitettava liiketunnistimen valmistajalle kunkin salatun sarjanumeron osalta siihen liittyvän K_{ID}-avaimen versionumero.

CSM_109 Edellä CSM_107 ja CSM_108 alakohdassa esitettyjen vaatimusten täyttämiseksi jäsenvaltion varmenneviranomaisen on käytettävä AES-algoritmia ISO 10116 -standardissa määritellyssä salauslohkoja ketjuttavassa käyttötilassa, missä limitysparametri $m = 1$ ja alustusvektori SV = '00' {16} (ts. 16 tavua ja binaariarvo 0). Tarvittaessa jäsenvaltion varmenneviranomaisen on käytettävä ISO 9797-1 -standardissa määriteltyä täyttömenetelmää 2.

CSM_110 Liiketunnistimen valmistajan on tallennettava salattu liittämisavain ja salattu sarjanumero aiottuun liiketunnistimeen, samoin kuin vastaavat selväkieliset arvot sekä salaukseen käytettävien K_M- ja K_{ID}-avainten versionumero.

Huomautus: Kuten 9.2.1.2 kohdassa selitetään, liiketunnistimen valmistajan voi olla tarpeen asentaa useita salattuja liittämisavaimia ja useita salattuja sarjanumeroita yhteen liiketunnistimeen.

CSM_111 Edellä CSM_110 alakohdassa määritellyn AES-salausmateriaalin lisäksi liiketunnistimen valmistaja voi tallentaa kuhunkin liiketunnistimeen myös TDES-salausmateriaalia siten kuin tämän lisäyksen osassa A olevassa CSM_037 alakohdassa on määritelty.

Huomautus: Näin mahdollistetaan toisen sukupolven liiketunnistimen liittäminen ensimmäisen sukupolven ajoneuvoyksikköön.

CSM_112 Ajoneuvoyksikkö luo tilapäisen avaimen K_S, kun se liitetään liiketunnistimeen, ja tämän avaimen pituuden on oltava sidoksissa sen $K_{M\text{-}VU}$-avaimen pituuteen, kuten CSM_50 alakohdassa on kuvattu.

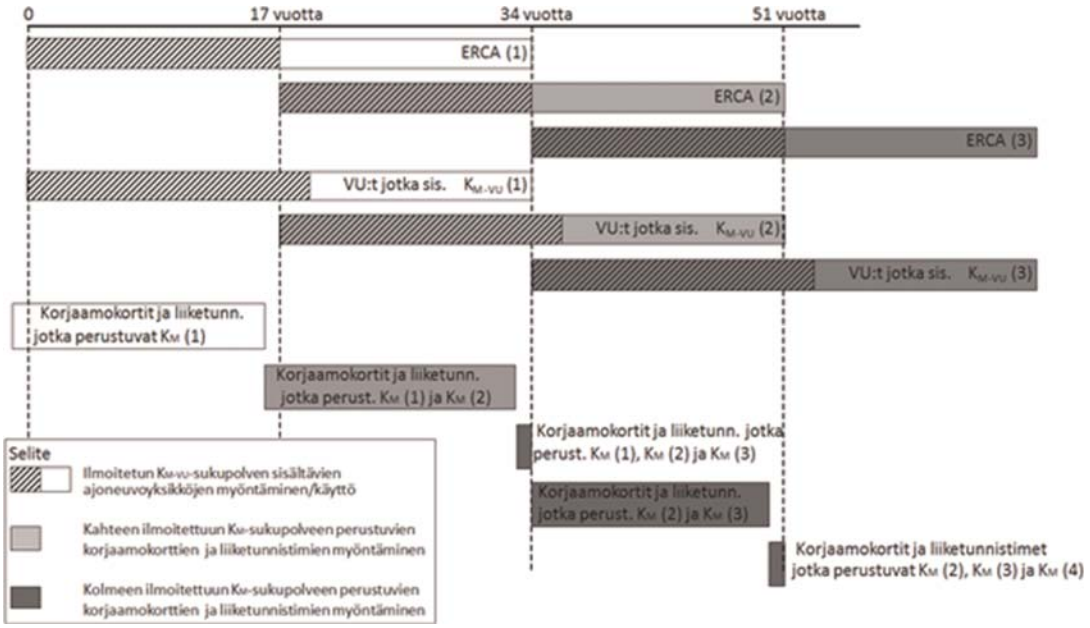
9.2.1.2 *Liiketunnistimen pääavaimen korvaaminen toisen sukupolven laitteessa*

CSM_113 Jokainen liiketunnistimen pääavain ja kaikki siihen liittyvät avaimet (ks. Taulukko 3) liittyvät tietyn sukupolven ERCA:n juuriavainpariin. Sen vuoksi nämä avaimet on korvattava 17 vuoden välein. Kunkin liiketunnistimen pääavainsukupolven voimassaoloaika alkaa yhden vuoden ennen siihen liittyvän ERCA:n juuriavainparin voimaantuloa ja päättyy, kun siihen liittyvän ERCA:n juuriavainparin voimassaoloaika päättyy. Tätä kuvataan kaaviossa 2.

▼B

Kaavio 2

Liiketunnistimen eri sukupolvien pääavainten antaminen ja käyttö ajoneuvoyksiköissä, liiketunnistimissa ja korjaamokorteissa



CSM_114 Vähintään yhden vuoden ennen uuden eurooppalaisen juuriavainparin luomista siten, kuin CSM_56 alakohdassa on kuvattu, ERCA:n on luotava uusi liiketunnistimen pääavain K_M luomalla uudet avaimet $K_{M\text{-}VU}$ ja $K_{M\text{-}WC}$. Liiketunnistimen pääavaimen pituuden on oltava sidoksissa uuden eurooppalaisen juuriavainparin suunniteltuun vahvuuteen CSM_50 alakohdan mukaisesti. ERCA:n on annettava uudet avaimet K_M, $K_{M\text{-}VU}$ ja $K_{M\text{-}WC}$ sekä niiden versionumero tiedoksi jäsenvaltioiden varmenneviranomaisille niiden pyynnöstä.

CSM_115 Jäsenvaltion varmenneviranomaisen on varmistettava, että kaikkiin sen valtuutuksella myönnettyihin korjaamokortteihin tallennetaan kaikkien voimassaolevien sukupolvien $K_{M\text{-}WC}$-avaimet sekä niiden versionumerot, kuten esitetään kaaviossa 2.

Huomautus: Tämä tarkoittaa, että ERCA:n varmenteen voimassaoloajan viimeisenä vuonna myönnettyihin korjaamokortteihin tallennetaan kolmen eri sukupolven $K_{M\text{-}WC}$-avaimet, kuten esitetään kaaviossa 2.

CSM_116 Edellä CSM_107 ja CSM_108 alakohdassa kuvatun prosessin osalta on otettava huomioon seuraavat näkökohdat: Jäsenvaltion varmenneviranomaisen on salattava jokainen K_P-liittämisavain, jonka se vastaanottaa liiketunnistimen valmistajalta, erikseen voimassa olevan sukupolven liiketunnistimen K_M-pääavaimella. Jäsenvaltion varmenneviranomaisen on salattava jokainen sarjanumero, jonka se vastaanottaa liiketunnistimen valmistajalta, erikseen voimassa olevan sukupolven K_{ID}-tunnistusavaimella. Liiketunnistimen valmistajan on tallennettava kaikki liittämisavaimen salaukset ja kaikki sarjanumeron salaukset aiottuun liiketunnistimeen, samoin kuin salaukseen käytettävien avainten K_M ja K_{ID} koodaamattomat arvot ja versionumero(t).

▼B

Huomautus: Tämä tarkoittaa, että ERCA:n varmenteen voimassaoloajan viimeisenä vuonna myönnettyihin liiketunnistimiin tallennetaan kolmen eri sukupolven K_M-avaimiin perustuvia salattua tietoja, kuten esitetään kaaviossa 2.

CSM_117 Edellä CSM_107 alakohdassa kuvatun prosessin osalta on otettava huomioon seuraavat näkökohdat: Koska K_P-liittämisavaimen pituuden on oltava sidoksissa K_M-avaimen pituuteen (ks. CSM_100 alakohta), liiketunnistimen valmistajan voi olla tarpeen luoda kolme erilaista (eripituista) liittämisavainta yhtä liiketunnistinta varten, mikäli myöhempien sukupolvien K_M-avaimet ovat eripituisia. Tällöin valmistajan on lähetettävä kukin liittämisavain jäsenvaltion varmenneviranomaiselle. Jäsenvaltion varmenneviranomaisen on varmistettava, että jokainen liittämisavain on salattu oikean sukupolven (samanpituisella) liiketunnistimen pääavaimella.

Huomautus: Jos liiketunnistimen valmistaja päättää luoda TDES-perustaisen liittämisavaimen toisen sukupolven liiketunnistinta varten (ks. CSM_111 alakohta), valmistajan on ilmoitettava jäsenvaltion varmenneviranomaiselle, että tämän liittämisavaimen salaukseen on käytettävä TDES-perustaista liiketunnistimen pääavainta. Tämä johtuu siitä, että TDES-avaimen pituus voi vastata AES-avaimen pituutta, jolloin jäsenvaltion varmenneviranomainen ei voi tehdä arviota ainoastaan avaimen pituuden perusteella.

CSM_118 Ajoneuvoyksikköjen valmistajien on asennettava kuhunkin ajoneuvoyksikköön ainoastaan yhden sukupolven $K_{M\text{-}VU}$-avain sekä sen versionumero. Tämän $K_{M\text{-}VU}$-avaimen sukupolven on oltava sidoksissa siihen ERCA:n varmenteeseen, johon ajoneuvoyksikön varmenteet perustuvat.

Huomautuksia:

— *X*-sukupolven ERCA:n varmenteeseen perustuva ajoneuvoyksikkö saa sisältää ainoastaan *X*-sukupolven $K_{M\text{-}VU}$-avaimen, vaikka se olisi myönnetty *X+1*-sukupolven ERCA:n varmenteen voimaantulon jälkeen. Tätä kuvataan kaaviossa 2.

— *X*-sukupolven ajoneuvoyksikköä ei voida liittää *X-1*-sukupolven liiketunnistimeen.

— Korjaamokortit ovat voimassa yhden vuoden, minkä vuoksi CSM_113–CSM_118 alakohdassa esitetyn perusteella kaikki korjaamokortit sisältävät uuden $K_{M\text{-}WC}$-avaimen siitä lähtien, kun ensimmäinen uuden $K_{M\text{-}VU}$-avaimen sisältävä ajoneuvoyksikkö myönnetään. Sen vuoksi tällaisen ajoneuvoyksikön on aina voitava laskea uusi K_M-avain. Lisäksi useimmat uudet liiketunnistimet sisältävät kyseiseen ajankohtaan mennessä salattuja tietoja, jotka perustuvat uuteen K_M-avaimeen.

9.2.2 *DSRC-tiedonsiirron salausavaimet*

9.2.2.1 *Yleistä*

CSM_119 Ajoneuvoyksiköstä valvontaviranomaiselle DSRC-etäviestintäkanavan kautta siirrettyjen tietojen aitous ja luottamuksellisuus on varmistettava joukolla ajoneuvoyksikkökohtaisia AES-avaimia, jotka luodaan yhden DSRC-pääavaimen KM_{DSRC} perusteella.

▼B

CSM_120 DSRC-pääavaimen KM_{DSRC} on oltava AES-avain, jonka ERCA on luonut, tallentanut ja jaellut suojatusti. Avaimen pituus voi olla 128, 192 tai 256 bittiä, ja sen on oltava sidoksissa eurooppalaisen juuriavainparin pituuteen, kuten CSM_50 alakohdassa on kuvattu.

CSM_121 ERCA:n on annettava DSRC-pääavain tiedoksi jäsenvaltioiden varmenneviranomaisille niiden pyynnöstä suojatusti, jotta jäsenvaltioiden varmenneviranomaiset voivat luoda sen perusteella ajoneuvoyksikkökohtaisia DSRC-avaimia ja varmistaa, että DSRC-pääavain asennetaan kaikkiin niiden vastuulla myönnettäviin valvontakortteihin ja korjaamokortteihin.

CSM_122 ERCA:n on annettava kullekin DSRC-pääavaimelle yksilöllinen versionumero. ERCA:n on ilmoitettava jäsenvaltioiden varmenneviranomaisille versionumero lähettäessään niille DSRC-pääavaimen.

Huomautus: Versionumeroa käytetään DSRC-pääavaimen eri sukupolvien erottamiseen, kuten 9.2.2.2 kohdassa yksityiskohtaisesti selitetään.

CSM_123 Ajoneuvoyksikön valmistajan on luotava kutakin ajoneuvoyksikköä varten ainutkertainen ajoneuvoyksikön sarjanumero ja lähetettävä tämä numero jäsenvaltionsa varmenneviranomaiselle saadakseen kaksi ajoneuvoyksikkökohtaista DSRC-avainta. Ajoneuvoyksikön sarjanumeron datatyyppi on `VuSerialNumber`, ja koodaukseen on käytettävä ISO 8825-1 -standardin mukaisesti peruskoodaussäännöistä johdettuja tiukempia koodaussääntöjä (DER, distinguished encoding rules).

CSM_124 Vastaanottaessaan ajoneuvoyksikkökohtaisia DSRC-avaimia koskevan pyynnön jäsenvaltion varmenneviranomaisen on luotava ajoneuvoyksikköä varten kaksi AES-avainta, jotka nimetään K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC. Näiden ajoneuvoyksikkökohtaisten avainten on oltava samanpituisia kuin DSRC-pääavain. Jäsenvaltion varmenneviranomaisen on käytettävä viitteessä RFC 5869 määriteltyä avaimen johtamisfunktiota. Hajautusfunktion, jota tarvitaan HMAC-Hash-funktion muodostamiseksi, on oltava sidoksissa DSRC-pääavaimen pituuteen, kuten CSM_50 alakohdassa on kuvattu. Viitteessä RFC 5869 määriteltyä avaimen johtamisfunktiota on käytettävä seuraavasti:

Vaihe 1 (Purkaminen):

— *PRK* = HMAC-Hash (*salt, IKM*), missä *salt* on tyhjä merkkijono ‘’ ja *IKM* on KM_{DSRC}.

Vaihe 2 (Laajentaminen):

— *OKM = T(1)*, missä

T(1) = HMAC-Hash (*PRK*, *T(0)* || *info* || ‘01’), missä

▼B

— *T(0)* = tyhjä merkkijono (‘’)

— *info* = ajoneuvoyksikön sarjanumero siten kuin CSM_123 alakohdassa on määritelty

— K_VU_{DSRC}_ENC = *OKM*:n ensimmäiset *L* tavua ja

K_VU_{DSRC}_MAC = *OKM*:n viimeiset *L* tavua,

missä *L* on avainten K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC vaadittu pituus tavuissa.

CSM_125 Jäsenvaltion varmenneviranomaisen on jaeltava avaimet K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC ajoneuvoyksikön valmistajalle suojatusti, jotta avaimet voidaan asentaa aiottuun ajoneuvoyksikköön.

CSM_126 Myöntämishetkellä avainten K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC on oltava tallennettuina ajoneuvoyksikön salattuun muistiin, jotta voidaan varmistaa etäviestintäkanavan kautta lähetettyjen tietojen eheys, aitous ja luottamuksellisuus. Ajoneuvoyksikön on tallennettava lisäksi näiden ajoneuvoyksikkökohtaisten avainten luomiseen käytettävän DSRC-pääavaimen versionumero.

CSM_127 Myöntämishetkellä KM_{DSRC}-avain on oltava tallennettuna valvontakorttien ja korjaamokorttien salattuun muistiin, jotta voidaan todentaa ajoneuvoyksikön etäviestintäkanavan kautta lähettämien tietojen eheys ja aitous ja avata tietojen salaus. Valvontakorttien ja korjaamokorttien on tallennettava lisäksi DSRC-pääavaimen versionumero.

Huomautus: Kuten jäljempänä 9.2.2.2 kohdassa selitetään, yhteen korjaamokorttiin tai valvontakorttiin voi olla tarpeen asentaa usean sukupolven KM_{DSRC}-avaimia.

CSM_128 Jäsenvaltion varmenneviranomaisen on pidettävä rekisteriä kaikista sen luomista ajoneuvoyksikkökohtaisista DSRC-avaimista, niiden versionumerosta ja sen ajoneuvoyksikön tunnistetiedoista, johon kukin avainjoukko on tarkoitettu.

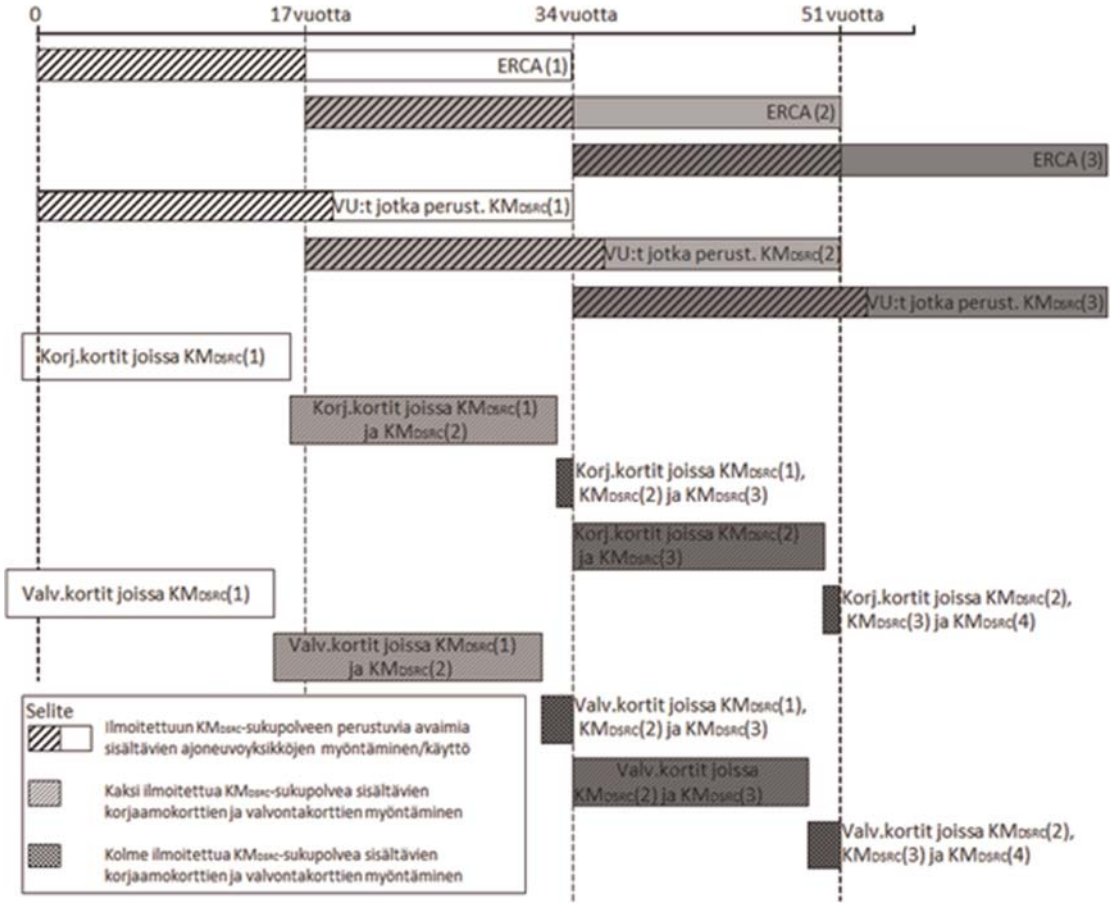
9.2.2.2 *DSRC-pääavaimen korvaaminen*

CSM_129 Jokainen DSRC-pääavain liittyy tietyn sukupolven ERCA:n juuriavainpariin. Sen vuoksi ERCA:n on korvattava DSRC-pääavain 17 vuoden välein. Kunkin DSRC-pääavainsukupolven voimassaoloaika alkaa kaksi vuotta ennen siihen liittyvän ERCA:n juuriavainparin voimaantuloa ja päättyy, kun siihen liittyvän ERCA:n juuriavainparin voimassaoloaika päättyy. Tätä kuvataan kaaviossa 3.

▼B

Kaavio 3

Eri sukupolvien DSRC-pääavainten antaminen ja käyttö ajoneuvoyksiköissä, korjaamokorteissa ja valvontakorteissa



CSM_130 Vähintään kaksi vuotta ennen uuden eurooppalaisen juuriavainparin luomista siten, kuin CSM_56 alakohdassa on kuvattu, ERCA:n on luotava uusi DSRC-pääavain. DSRC-avaimen pituuden on oltava sidoksissa uuden eurooppalaisen juuriavainparin suunniteltuun vahvuuteen CSM_50 alakohdan mukaisesti. ERCA:n on annettava uusi DSRC-pääavain sekä sen versionumero jäsenvaltioiden varmenneviranomaisille niiden pyynnöstä.

CSM_131 Jäsenvaltion varmenneviranomaisen on varmistettava, että kaikkiin sen valtuutuksella myönnettyihin valvontakortteihin tallennetaan kaikkien voimassaolevien sukupolvien KM_{DSRC}-avaimet sekä niiden versionumerot, kuten esitetään kaaviossa 3.

Huomautus: Tämä tarkoittaa, että ERCA:n varmenteen voimassaoloajan kahtena viimeisenä vuonna myönnettyihin valvontakortteihin tallennetaan kolmen eri sukupolven KM_{DSRC}-avaimet, kuten esitetään kaaviossa 3.

CSM_132 Jäsenvaltion varmenneviranomaisen on varmistettava, että kaikkiin sen valtuutuksella myönnettyihin korjaamokortteihin tallennetaan kaikkien sukupolvien $K_{M\text{-}WC}$-avaimet, jotka ovat olleet voimassa vähintään vuoden ja ovat edelleen voimassa, sekä niiden versionumerot, kuten esitetään kaaviossa 3.

▼B

Huomautus: Tämä tarkoittaa, että ERCA:n varmenteen voimassaoloajan viimeisenä vuonna myönnettyihin korjaamokortteihin tallennetaan kolmen eri sukupolven KM_{DSRC}-avaimet,, kuten esitetään kaaviossa 3.

CSM_133 Ajoneuvoyksikköjen valmistajien on asennettava kuhunkin ajoneuvoyksikköön ainoastaan yksi joukko ajoneuvoyksikkökohtaisia DSRC-avaimia sekä niiden versionumero. Nämä avaimet on luotava sen KM_{DSRC}-sukupolven perusteella, joka on sidoksissa ajoneuvoyksikön varmenteiden perustana käytettyyn ERCA:n varmenteeseen.

Huomautuksia:

— Tämä tarkoittaa, että *X*-sukupolven ERCA:n varmenteeseen perustuva ajoneuvoyksikkö saa sisältää ainoastaan *X*-sukupolven avaimet K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC, vaikka ajoneuvoyksikkö olisi myönnetty *X*+*1*-sukupolven ERCA:n varmenteen voimaantulon jälkeen. Tätä kuvataan kaaviossa 3.

— Korjaamokortit ovat voimassa yhden vuoden ja valvontakortit kaksi vuotta, minkä vuoksi CSM_131–CSM_133 kohdissa esitetyn perusteella kaikki korjaamokortit ja valvontakortit sisältävät uuden DSRC-pääavaimen siitä lähtien, kun ensimmäinen kyseiseen pääavaimeen perustuvia ajoneuvoyksikkökohtaisia avaimia sisältävä ajoneuvoyksikkö myönnetään.

9.3. **Varmenteet**

9.3.1 *Yleistä*

CSM_134 Eurooppalaisen älykkään ajopiirturijärjestelmän kaikkien varmenteiden on oltava ISO 7816-4- ja ISO 7816-8 -standardien mukaisesti itseään kuvaavia (self-descriptive) kortin avulla todennettavia (CV, card verifiable) varmenteita.

CSM_135 ISO 8825-1 -standardin mukaisia peruskoodaussäännöistä johdettuja tiukempia koodaussääntöjä (DER) on käytettävä sekä ASN.1-datarakenteiden että (sovelluskohtaisten) dataobjektien koodaukseen varmenteissa.

Huomautus: Tällaisen koodauksen tuloksena on seuraavanlainen tuntomerkki-pituus-sisältö-rakenne (TLV, Tag-Length-Value):

Tuntomerkki: Tuntomerkki on koodattu yhteen tai kahteen tavuun ja ilmoittaa sisällön.

Pituus: Pituus on koodattu etumerkittömänä kokonaislukuna yhteen, kahteen tai kolmeen tavuun, jolloin enimmäispituus on 65 535 tavua. Tavujen vähimmäismäärää on käytettävä.

Sisältö: Sisältö on koodattu nollaan tai useampaan tavuun.

9.3.2 *Varmenteen sisältö*

CSM_136 Kaikilla varmenteilla on oltava Taulukko 4 esitetyn varmenteen profiilin mukainen rakenne.

Taulukko 4

Varmenteen profiili, versio 1

Kenttä	Kentän tunniste	Tuntomerkki	Pituus (tavua)	ASN.1-datatyyppi (ks. lisäys 1)
ECC-varmenne	C	‘7F 21’	vaiht.	
ECC-varmenteen runko	B	‘7F 4E’	vaiht.	

▼B

Kenttä	Kentän tunniste	Tuntomerkki	Pituus (tavua)	ASN.1-datatyyppi (ks. lisäys 1)
Varmenteen profiilin tunniste	CPI	‘5F 29’	‘01’	`INTEGER(0..255)`
Varmenneviranomaisen viite	CAR	‘42’	‘08’	`KeyIdentifier`
Varmenteen haltijan valtuutus	CHA	‘5F 4C’	‘07’	`CertificateHolder Authorisation`
Julkinen avain	PK	‘7F 49’	vaiht.	
Domain-parametrit	DP	‘06’	vaiht.	`OBJECT IDENTIFIER`
Julkinen piste (public point)	PP	‘86’	vaiht.	`OCTET STRING`
Varmenteen haltijan viite	CHR	‘5F 20’	‘08’	`KeyIdentifier`
Varmenteen voimaantulopäivä	CEfD	‘5F 25’	‘04’	`TimeReal`
Varmenteen vanhenemispäivä	CExD	‘5F 24’	‘04’	`TimeReal`
ECC-varmenteen allekirjoitus	S	‘5F 37’	vaiht.	`OCTET STRING`

Huomautus: Kentän tunnisteella tarkoitetaan tämän lisäyksen myöhemmissä kohdissa varmenteen yksittäisiä kenttiä, esim. X.CAR on käyttäjän X varmenteessa ilmoitettu varmenneviranomaisen viite.

9.3.2.1 Varmenteen profiilin tunniste

CSM_137 Varmenteissa on oltava varmenteen profiilin tunniste, jolla ilmoitetaan käytetty varmenteen profiili. Versio 1, siten kuin Taulukko 4 on määritelty, ilmoitetaan arvona ‘00’.

9.3.2.2 Varmenneviranomaisen viite

CSM_138 Varmenneviranomaisen viitteellä on tunnistettava julkinen avain, jota käytetään varmenteen allekirjoituksen todentamiseen. Sen vuoksi varmenneviranomaisen viitteen on vastattava varmenteen haltijan viitettä, joka ilmoitetaan kyseisen varmenneviranomaisen varmenteessa.

CSM_139 ERCA:n juurivarmenteen on oltava itse allekirjoitettu, eli varmenneviranomaisen viitteen on oltava sama kuin varmenteen haltijan viite.

▼B

CSM_140 Varmenteen haltijan viitteen on vastattava uuden ERCA:n juurivarmenteen haltijan viitettä ERCA:n linkkivarmenteessa. Varmenneviranomaisen viitteen linkkivarmenteessa on vastattava edellisen ERCA:n juurivarmenteen haltijan viitettä.

9.3.2.3 Varmenteen haltijan valtuutus

CSM_141 Varmenteen haltijan valtuutuksella on yksilöitävä varmenteen tyyppi. Se koostuu ajopiirturisovelluksen tunnisteen kuudesta merkitsevimmästä tavusta, jotka ketjutetaan sen laitteen tyyppiin, johon varmenne on tarkoitettu.

9.3.2.4 Julkinen avain

Julkinen avain sisältää kaksi dataelementtiä: standardoidut domain-parametrit, joita käytetään julkisen avaimen kanssa varmenteessa, ja julkisen pisteen arvo.

CSM_142 Domain Parameters -dataelementin on sisällettävä yksi Taulukko 1 määritellyistä oliotunnisteista, jolla viitataan joukkoon standardoituja domain-parametreja.

CSM_143 Public Point -dataelementin on sisällettävä julkinen piste. Elliptisen käyrän julkiset pisteet on muunnettava tavujonoiksi siten kuin viitteessä TR-03111 on määritelty. Tässä yhteydessä on käytettävä tiivistämätöntä koodausmuotoa. Kun elliptisen käyrän piste palautetaan sen koodatusta muodosta, on aina suoritettava viitteessä TR-03111 kuvatut vahvistukset.

9.3.2.5 Varmenteen haltijan viite

CSM_144 Varmenteen haltijan viite on varmenteessa käytettävä julkisen avaimen tunniste. Sitä on käytettävä viitteenä tähän julkiseen avaimeen muissa varmenteissa.

CSM_145 Kortin ja ulkoisen GNSS-laitteiston varmenteissa varmenteen haltijan viitteellä on oltava lisäyksessä 1 määritelty datatyyppi `ExtendedSerialNumber`.

CSM_146 Varmennetta pyytäessään ajoneuvoyksikön valmistaja joko tietää tai ei tiedä sen ajoneuvoyksikön valmistajakohtaista sarjanumeroa, johon kyseinen varmenne ja siihen liittyvä yksityinen avain on tarkoitettu. Jos valmistaja tietää sarjanumeron, varmenteen haltijan viitteellä on oltava lisäyksessä 1 määritelty datatyyppi `ExtendedSerialNumber`. Jos valmistaja ei tiedä sarjanumeroa, varmenteen haltijan viitteellä on oltava lisäyksessä 1 määritelty datatyyppi `CertificateRequestID`.

CSM_147 ERCA:n ja jäsenvaltion varmenneviranomaisen varmenteissa varmenteen haltijan viitteellä on oltava lisäyksessä 1 määritelty datatyyppi `CertificationAuthorityKID`.

▼B

9.3.2.6 Varmenteen voimaantulopäivä

CSM_148 Varmenteen voimaantulopäivässä on ilmoitettava varmenteen voimassaolon alkamispäivä ja -aika. Varmenteen voimassaolopäivän on oltava varmenteen luomispäivä.

9.3.2.7 Varmenteen vanhenemispäivä

CSM_149 Varmenteen vanhenemispäivässä on ilmoitettava varmenteen voimassaolon päättymispäivä ja -aika.

9.3.2.8 Varmenteen allekirjoitus

CSM_150 Varmenteen allekirjoitus on luotava koodatun varmenteen rungosta, mukaan lukien varmenteen rungon tuntomerkki ja pituus. Allekirjoitukseen on käytettävä viitteessä DSS määriteltyä ECDSA-algoritmia sekä allekirjoittavan viranomaisen avainkokoon sidoksissa olevaa hajautusalgoritmia, kuten CSM_50 alakohdassa on määritelty. Allekirjoituksen on oltava tekstimuodossa, kuten viitteessä TR-03111 on määritelty.

9.3.3 *Varmenteiden pyytäminen*

CSM_151 Varmennetta pyytäessään pyytäjän on lähetettävä seuraavat tiedot asianomaiselle varmenneviranomaiselle:

— pyydetyn varmenteen profiilin tunniste

— varmenneviranomaisen viite, jota on tarkoitus käyttää varmenteen allekirjoittamiseen

— allekirjoitettava julkinen avain.

CSM_152 Edellä CSM_151 alakohdassa mainittujen tietojen lisäksi jäsenvaltion varmenneviranomaisen on lähetettävä varmennepyynnössä seuraavat tiedot ERCA:lle, jotta ERCA voi luoda uuden jäsenvaltion varmenneviranomaisen varmenteen haltijan viitteen:

— varmenneviranomaisen maan numerotunnus (lisäyksessä 1 määritelty datatyyppi `NationNumeric`)

— varmenneviranomaisen maan kirjaintunnus (lisäyksessä 1 määritelty datatyyppi `NationAlpha`)

— yksitavuinen sarjanumero, jonka avulla tunnistetaan varmenneviranomaisen eri avaimet siinä tapauksessa, että avain vaihtuu

— kaksitavuinen kenttä, joka sisältää varmenneviranomaisen erityisiä lisätietoja.

CSM_153 Edellä CSM_151 alakohdassa mainittujen tietojen lisäksi laitteen valmistajan on lähetettävä varmennepyynnössä seuraavat tiedot jäsenvaltion varmenneviranomaiselle, jotta tämä voi luoda uuden laitteen varmenteen haltijan viitteen:

— laitetyypin valmistajakohtainen tunniste

— laitteen sarjanumero, joka on tietyn valmistajan laitteille ainoa tietylle laitetyypille ja tietyssä valmistuskuussa annettu sarjanumero, jos se on tiedossa (ks. CSM_154 kohta); muutoin varmenteen pyytäjän yksilöllinen tunniste

▼B

— laitteen valmistuskuukausi ja -vuosi tai varmennepyynnön esittämiskuukausi ja -vuosi.

Valmistajan on varmistettava, että annetut tiedot ovat asianmukaisia ja että jäsenvaltion varmenneviranomaisen lähettämä varmenne asennetaan aiottuun laitteeseen.

CSM_154 Varmennetta pyytäessään ajoneuvoyksikön valmistaja joko tietää tai ei tiedä sen ajoneuvoyksikön valmistajakohtaista sarjanumeroa, johon kyseinen varmenne ja siihen liittyvä yksityinen avain on tarkoitettu. Jos ajoneuvoyksikön valmistaja tietää sarjanumeron, sen on lähetettävä sarjanumero jäsenvaltion varmenneviranomaiselle. Jos ajoneuvoyksikön valmistaja ei tiedä sarjanumeroa, sen on yksilöitävä kukin varmennepyyntö ja lähetettävä varmennepyynnön sarjanumero jäsenvaltion varmenneviranomaiselle. Annettava varmenne sisältää siten varmennepyynnön sarjanumeron. Asennettuaan varmenteen tiettyyn ajoneuvoyksikköön valmistajan on ilmoitettava jäsenvaltion varmenneviranomaiselle varmennepyynnön sarjanumeron ja ajoneuvoyksikön tunnisteen välinen yhteys.

10. AJONEUVOYKSIKÖN JA KORTIN MOLEMMINPUOLINEN TODENTAMINEN JA SALATTU SANOMANVÄLITYS

10.1. **Yleistä**

CSM_155 Ajoneuvoyksikön ja ajopiirturikortin välisen salatun viestinnän on korkealla tasolla perustuttava seuraaviin vaiheisiin:

— Ensimmäiseksi kunkin osapuolen on osoitettava toiselle, että sen hallussa on voimassa oleva julkisen avaimen varmenne, joka on jäsenvaltion varmenneviranomaisen allekirjoittama. Jäsenvaltion varmenneviranomaisen julkisen avaimen varmenteen on puolestaan oltava Euroopan juurivarmenneviranomaisen (ERCA) allekirjoittama. Tätä vaihetta kutsutaan varmenneketjun todentamiseksi ja sitä käsitellään yksityiskohtaisesti 10.2 kohdassa.

— Toiseksi ajoneuvoyksikön on osoitettava kortille, että sen hallussa on yksityinen avain, joka vastaa varmenteessa esitettyä julkista avainta. Se tekee tämän allekirjoittamalla kortin lähettämän satunnaisluvun. Kortti todentaa allekirjoituksen satunnaisluvusta. Jos tämä todennus onnistuu, ajoneuvoyksikkö on todennettu. Tätä vaihetta kutsutaan ajoneuvoyksikön todentamiseksi ja sitä käsitellään yksityiskohtaisesti 10.3 kohdassa.

— Kolmanneksi molemmat osapuolet laskevat itsenäisesti kaksi tilapäistä AES-avainta käyttäen epäsymmetristä avaimesta sopimisen algoritmia. Näiden tilapäisten avainten avulla kortti luo sanoman autentikointikoodin (MAC) ajoneuvoyksikön lähettämistä tiedoista. Ajoneuvoyksikkö todentaa MAC-koodin. Jos tämä todennus onnistuu, kortti on todennettu. Tätä vaihetta kutsutaan kortin todentamiseksi ja sitä käsitellään yksityiskohtaisesti 10.4 kohdassa.

— Neljänneksi ajoneuvoyksikön ja kortin on käytettävä sovittuja tilapäisiä avaimia varmistaakseen kaikkien vaihdettujen sanomien luottamuksellisuuden, eheyden ja aitouden. Tätä kutsutaan salatuksi sanomanvälitykseksi ja sitä käsitellään yksityiskohtaisesti 10.5 kohdassa.

CSM_156 Ajoneuvoyksikön on käynnistettävä edellä CSM_155 alakohdassa kuvattu mekanismi aina kun johonkin sen korttiaukkoon asetetaan kortti.

▼B

10.2. **Molemminpuolinen varmenneketjun todentaminen**

10.2.1 *Ajoneuvoyksikön suorittama kortin varmenneketjun todentaminen*

CSM_157 Ajoneuvoyksikköjen on käytettävä kaaviossa 4 kuvattua protokollaa ajopiirturikorttien varmenneketjun todentamiseen.

Huomautuksia kaavioon 4:

— Kaaviossa mainittuja Card-nimisiä varmenteita ja julkisia avaimia käytetään molemminpuoliseen todentamiseen. Edellä 9.1.5 kohdassa näistä käytetään nimitystä Card_MA.

— Kaaviossa mainittuja Card.CA-nimisiä varmenteita ja julkisia avaimia käytetään kortin varmenteiden allekirjoittamiseen ja ne ilmoitetaan kortin varmenteen varmenneviranomaisen viitteessä (CAR). Edellä 9.1.3 kohdassa näistä käytetään nimitystä MSCA_Card.

— Kaaviossa mainittu Card.CA.EUR-varmenne on eurooppalainen juurivarmenne, joka ilmoitetaan Card.CA-varmenteen varmenneviranomaisen viitteessä (CAR).

— Kaaviossa mainittu Card.Link-varmenne on mahdollinen kortin linkkivarmenne. Kuten edellä 9.1.2 kohdassa on määritelty, tämä on uuden eurooppalaisen juuriavainparin linkkivarmenne, jonka ERCA on luonut ja allekirjoittanut edellisellä eurooppalaisella yksityisellä avaimella.

— Card.Link.EUR-varmenne on eurooppalainen juurivarmenne, joka ilmoitetaan Card.Link-varmenteen varmenneviranomaisen viitteessä (CAR).

CSM_158 Kuten kaaviossa 4 kuvataan, kortin varmenneketjun todentaminen alkaa kortin asettamisesta. Ajoneuvoyksikön on luettava kortin haltijan viite (`cardExtendedSerialNumber`) EF-tiedoston ICC-tiedoista. Ajoneuvoyksikön on tarkistettava, tunteeko se kortin eli onko se aikaisemmin todentanut kortin varmenneketjun onnistuneesti ja tallentanut sen tulevaa käyttöä varten. Jos se tuntee kortin ja kortin varmenne on edelleen voimassa, prosessi jatkuu ajoneuvoyksikön varmenneketjun todentamisella. Muutoin ajoneuvoyksikön on luettava kortilta peräkkäin MSCA_Card-varmenne, jota käytetään kortin varmenteen todentamiseen, Card.CA.EUR-varmenne, jota käytetään MSCA_Card-varmenteen todentamiseen, sekä mahdollinen linkkivarmenne, kunnes se löytää varmenteen, jonka se tuntee tai voi todentaa. Jos tällainen varmenne löytyy, ajoneuvoyksikön on käytettävä kyseistä varmennetta muiden kortilta luettujen kortin varmenteiden todentamiseen. Jos tämä onnistuu, prosessi jatkuu ajoneuvoyksikön varmenneketjun todentamisella. Jos tämä ei onnistu, ajoneuvoyksikkö ei saa hyväksyä korttia.

▼B

Huomautus: Ajoneuvoyksikkö voi tuntea Card.CA.EUR-varmenteen kolmella tavalla:

— Card.CA.EUR-varmenne on sama kuin ajoneuvoyksikön oma EUR-varmenne;

— Card.CA.EUR-varmenne edeltää ajoneuvoyksikön omaa EUR-varmennetta ja ajoneuvoyksikkö sisältää tämän varmenteen jo myöntämishetkellä (ks. CSM_81 alakohta);

— Card.CA.EUR-varmenne on ajoneuvoyksikön oman EUR-varmenteen seuraaja ja ajoneuvoyksikkö on aikaisemmin vastaanottanut toiselta ajopiirturikortilta linkkivarmenteen, jonka se on todentanut ja tallentanut tulevaa käyttöä varten.

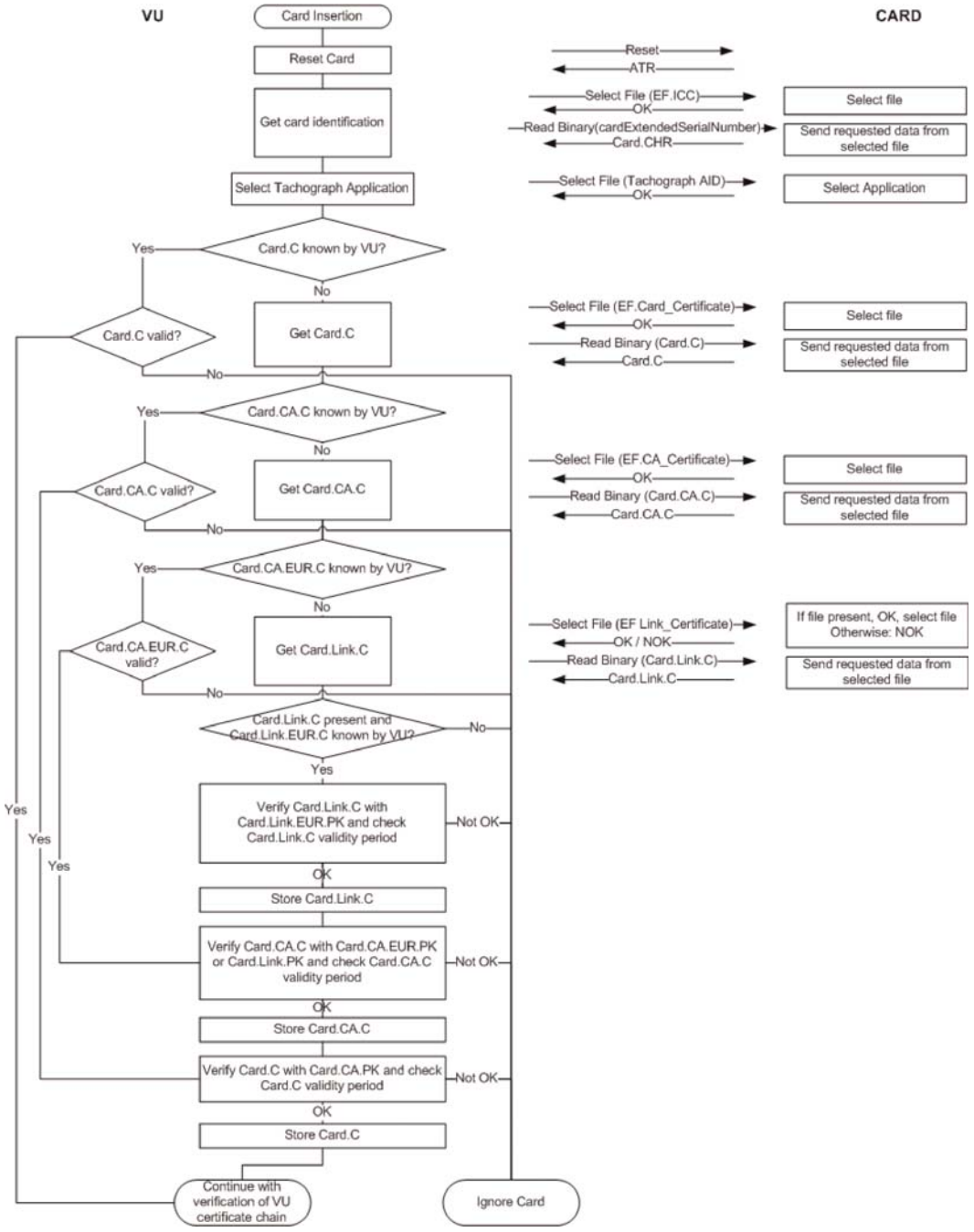
CSM_159 Kuten kaaviossa 4 todetaan, sen jälkeen, kun ajoneuvoyksikkö on todentanut aikaisemmin tuntemattoman varmenteen aitouden ja voimassaolon, se voi tallentaa kyseisen varmenteen tulevaa käyttöä varten, jotta sen ei tarvitse todentaa varmennetta uudelleen, jos se esitetään uudelleen ajoneuvoyksikölle. Koko varmenteen tallentamisen sijaan ajoneuvoyksikkö voi tallentaa ainoastaan varmenteen rungon sisällön, kuten 9.3.2 kohdassa on määritelty.

CSM_160 Ajoneuvoyksikön on todennettava jokaisen kortilta luetun ja sen muistiin tallennetun varmenteen voimassaoloaika ja hylättävä vanhentuneet varmenteet. Ajoneuvoyksikön on käytettävä kortin esittämän varmenteen voimassaoloajan todentamiseen sisäistä kelloaan.

▼B

Kaavio 4

Ajoneuvoyksikön suorittama kortin varmenneketjun todentamisprotokolla



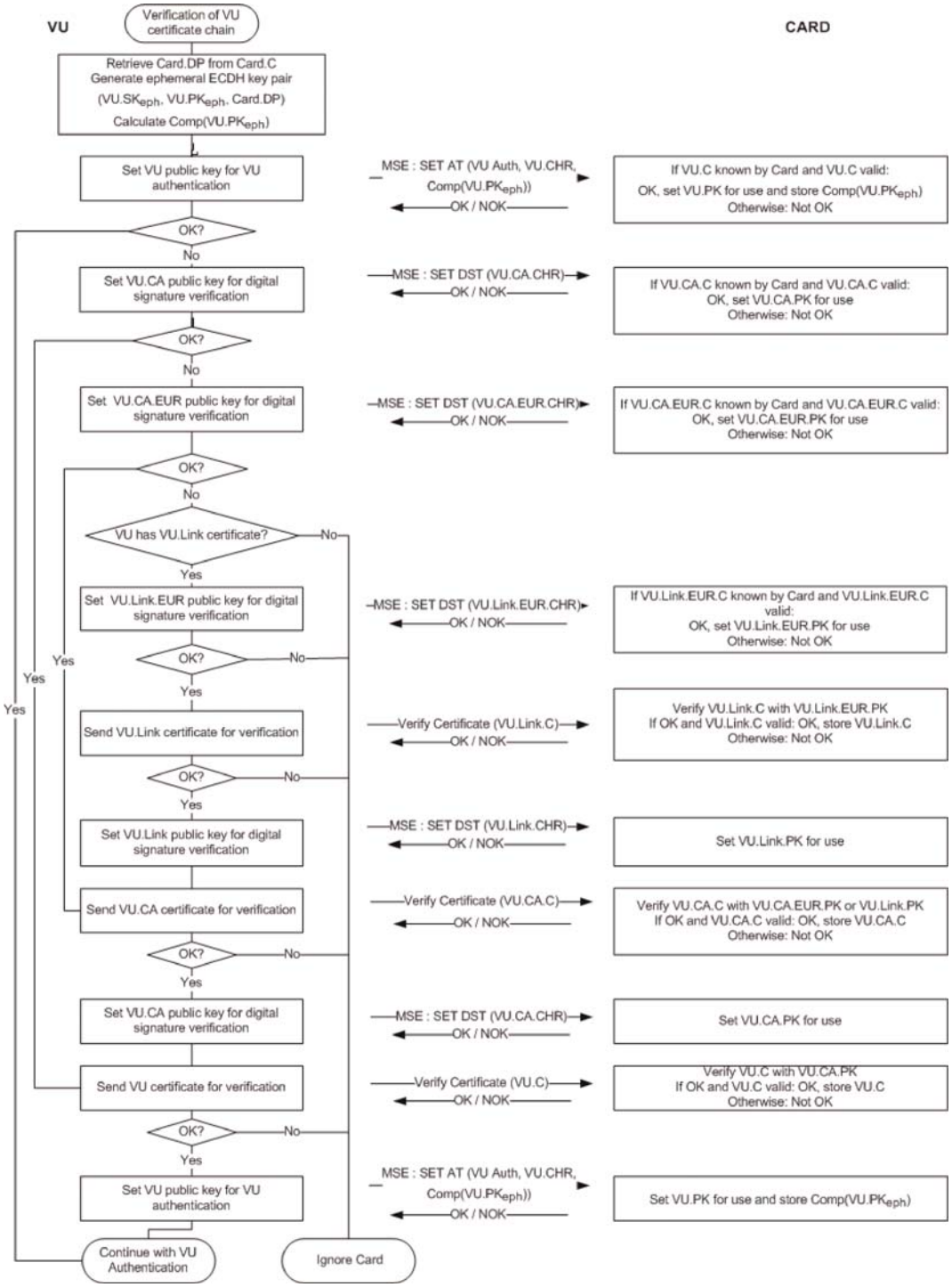
10.2.2 *Kortin suorittama ajoneuvoyksikön varmenneketjun todentaminen*

CSM_161 Ajopiirturikorttien on käytettävä kaaviossa 5 kuvattua protokollaa ajoneuvoyksikköjen varmenneketjun todentamiseen.

▼B

Kaavio 5

Kortin suorittama ajoneuvoyksikön varmenneketjun todentamisprotokolla



Huomautuksia kaavioon 5:

— Kaaviossa mainittuja VU-nimisiä varmenteita ja julkisia avaimia käytetään molemminpuoliseen todentamiseen. Edellä 9.1.4 kohdassa näistä käytetään nimitystä VU_MA.

▼B

— Kaaviossa mainittuja VU.CA-nimisiä varmenteita ja julkisia avaimia käytetään ajoneuvoyksikön ja ulkoisen GNSS-laitteiston varmenteiden allekirjoittamiseen. Edellä 9.1.3 kohdassa näistä käytetään nimitystä MSCA_VU-EGF.

— Kaaviossa mainittu VU.CA.EUR-varmenne on eurooppalainen juurivarmenne, joka ilmoitetaan VU.CA-varmenteen varmenneviranomaisen viitteessä (CAR).

— Kaaviossa mainittu VU.Link-varmenne on mahdollinen ajoneuvoyksikön linkkivarmenne. Kuten edellä 9.1.2 kohdassa on määritelty, tämä on uuden eurooppalaisen juuriavainparin linkkivarmenne, jonka ERCA on luonut ja allekirjoittanut edellisellä eurooppalaisella yksityisellä avaimella.

— VU.Link.EUR-varmenne on eurooppalainen juurivarmenne, joka ilmoitetaan VU.Link-varmenteen varmenneviranomaisen viitteessä (CAR).

CSM_162 Kuten kaaviossa 5 kuvataan, ajoneuvoyksikön varmenneketjun todentaminen alkaa, kun ajoneuvoyksikkö yrittää asettaa oman julkisen avaimensa ajopiirturikortin käyttöön. Jos tämä onnistuu, kortti on onnistuneesti todentanut ajoneuvoyksikön varmenneketjun aikaisemmin ja tallentanut ajoneuvoyksikön varmenteen tulevaa käyttöä varten. Tällöin ajoneuvoyksikön varmenne asetetaan käyttöön ja prosessi jatkuu ajoneuvoyksikön todentamisella. Jos kortti ei tunne ajoneuvoyksikön varmennetta, ajoneuvoyksikön on esitettävä peräkkäin VU.CA-varmenne, jota käytetään ajoneuvoyksikön varmenteen todentamiseen, VU.CA.EUR-varmenne, jota käytetään VU.CA-varmenteen todentamiseen, sekä mahdollinen linkkivarmenne, kunnes löydetään varmenne, jonka kortti tuntee tai voi todentaa. Jos tällainen varmenne löytyy, kortin on käytettävä kyseistä varmennetta muiden sille esitettyjen ajoneuvoyksikön varmenteiden todentamiseen. Jos tämä onnistuu, ajoneuvoyksikön on asetettava julkinen avaimensa käyttöön ajopiirturikortissa. Jos tämä ei onnistu, ajoneuvoyksikkö ei saa hyväksyä korttia.

Huomautus: Kortti voi tuntea VU.CA.EUR-varmenteen kolmella tavalla:

— VU.CA.EUR-varmenne on sama kuin kortin oma EUR-varmenne;

— VU.CA.EUR-varmenne edeltää kortin omaa EUR-varmennetta ja kortti sisältää tämän varmenteen jo myöntämishetkellä (ks. CSM_91 alakohta);

— VU.CA.EUR-varmenne on kortin oman EUR-varmenteen seuraaja ja kortti on aikaisemmin vastaanottanut toiselta ajoneuvoyksiköltä linkkivarmenteen, jonka se on todentanut ja tallentanut tulevaa käyttöä varten.

CSM_163 Ajoneuvoyksikön on käytettävä MSE: Set AT -komentoa asettaakseen julkisen avaimensa ajopiirturikortin käyttöön. Kuten lisäyksessä 2 on määritelty, tämä komento sisältää tiedon salausmekanismista, jota käytetään asetetun avaimen kanssa. Tämä mekanismi on ’ajoneuvoyksikön todentaminen, jossa käytetään ECDSA-algoritmia yhdessä ajoneuvoyksikön VU_MA-avainparin avainkokoon sidoksissa olevan hajautusalgoritmin kanssa, kuten CSM_50 alakohdassa on määritelty’.

▼B

CSM_164 MSE: Set AT -komento sisältää myös tiedon lyhytaikaisesta avainparista, jota ajoneuvoyksikkö käyttää tilapäisestä avaimesta sopimisen aikana (ks. 10.4 kohta). Sen vuoksi ennen MSE: Set AT -komennon lähettämistä ajoneuvoyksikön on luotava lyhytaikainen ECC-avainpari. Lyhytaikaisen avainparin luomiseksi ajoneuvoyksikön on käytettävä standardoituja domain-parametreja, jotka ilmoitetaan kortin varmenteessa. Lyhytaikainen avainpari nimetään ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). Ajoneuvoyksikön on otettava ECDH:n lyhytaikaisen julkisen pisteen x-koordinaatti avaimen tunnisteeksi; tätä kutsutaan julkisen avaimen tiivistetyksi esitykseksi ja se nimetään Comp($VU.PK_{eph}$).

CSM_165 Jos MSE: Set AT -komento onnistuu, kortin on asetettava ilmoitettu VU.PK-avain myöhemmin käyttöön ajoneuvoyksikön todentamisen aikana ja tallennettava tilapäisesti Comp($VU.PK_{eph}$). Jos vähintään kaksi onnistunutta MSE: Set AT -komentoa lähetetään, ennen kuin tilapäisistä avaimista on sovittu, kortin on tallennettava ainoastaan viimeisin vastaanotettu Comp($VU.PK_{eph}$).

CSM_166 Kortin on todennettava jokaisen ajoneuvoyksikön esittämän tai viittaaman ja kortin muistiin tallennetun varmenteen voimassaoloaika ja hylättävä vanhentuneet varmenteet.

CSM_167 Ajoneuvoyksikön esittämän varmenteen voimassaoloajan todentamista varten jokaisen ajopiirturikortin on tallennettava sisäisesti joitakin kuluvaa aikaa koskevia tietoja. Ajoneuvoyksikkö ei saa suoraan päivittää näitä tietoja. Myöntämishetkellä kortin kuluvaksi ajaksi on asetettava kortin Card_MA-varmenteen voimaantulopäivä. Kortin on päivitettävä kuluvaa aikaa koskevat tietonsa, jos ajoneuvoyksikön esittämän todennetun varmenteen, joka on ’pätevä aikalähde’ (valid source of time), voimaantulopäivä on aikaisempi kuin kortin kuluva aika. Tällöin kortin on asetettava kuluvaksi ajaksi kyseisen varmenteen voimaantulopäivä. Kortti saa käyttää pätevinä aikalähteinä ainoastaan seuraavia varmenteita:

— toisen sukupolven ERCA:n linkkivarmenteet

— toisen sukupolven jäsenvaltion varmenneviranomaisen varmenteet

— toisen sukupolven ajoneuvoyksikön varmenteet, jotka on annettu samassa maassa kuin yksi tai useampi kortin oma varmenne.

Huomautus: Viimeksi mainittu vaatimus edellyttää, että kortti voi tunnistaa ajoneuvoyksikön varmenteen (ts. MSCA_VU-EGF-varmenteen) varmenneviranomaisen viitteen (CAR). Tämä ei ole sama kuin sen oman varmenteen (ts. MSCA_Card-varmenteen) varmenneviranomaisen viite.

CSM_168 Kuten kaaviossa 5 todetaan, sen jälkeen, kun kortti on todentanut aikaisemmin tuntemattoman varmenteen aitouden ja voimassaolon, se voi tallentaa kyseisen varmenteen tulevaa käyttöä varten, jotta sen ei tarvitse todentaa varmennetta

▼B

uudelleen, jos se esitetään uudelleen kortille. Koko varmenteen tallentamisen sijaan kortti voi tallentaa ainoastaan varmenteen rungon sisällön, kuten 9.3.2 kohdassa on määritelty.

10.3. **Ajoneuvoyksikön todentaminen**

CSM_169 Ajoneuvoyksikköjen ja korttien on käytettävä kaaviossa 6 kuvattua ajoneuvoyksikön todentamisprotokollaa, jolla ajoneuvoyksikkö todennetaan kortille. Ajoneuvoyksikön todentamisen avulla ajopiirturikortti voi selkeästi todentaa ajoneuvoyksikön aitouden. Tätä varten ajoneuvoyksikön on käytettävä yksityistä avaintaan kortin luoman haasteen allekirjoittamiseen.

CSM_170 Kortin haasteen lisäksi ajoneuvoyksikön on sisällytettävä allekirjoitukseen kortin varmenteesta otettu kortin haltijan viite.

Huomautus: Näin varmistetaan, että kortti, jolle ajoneuvoyksikkö todentaa itsensä, on sama kortti, jonka varmenneketjun ajoneuvoyksikkö on aikaisemmin todentanut.

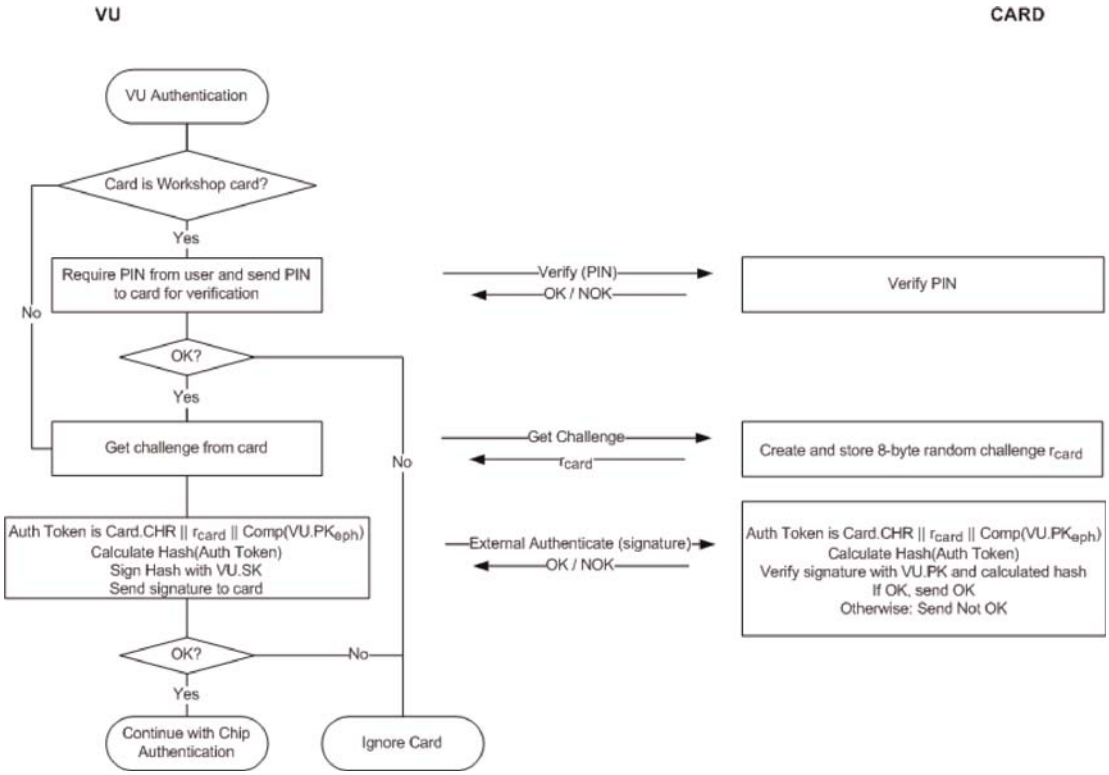
CSM_171 Ajoneuvoyksikön on sisällytettävä allekirjoitukseen lisäksi sen lyhytaikaisen julkisen avaimen Comp(VU.PK_{eph}) tunniste, jota ajoneuvoyksikkö käyttää aloittaakseen salatun sanomanvälityksen 10.4 kohdassa määritellyn sirun todentamisprosessin aikana.

Huomautus: Näin varmistetaan, että ajoneuvoyksikkö, jonka kanssa kortti on yhteydessä salatun sanomanvälitysjakson aikana, on sama ajoneuvoyksikkö, jonka kortti on todentanut.

▼B

Kaavio 6

Ajoneuvoyksikön todentamisprotokolla



CSM_172 Jos ajoneuvoyksikkö lähettää ajoneuvoyksikön todentamisen aikana useamman GET CHALLENGE -komennon, kortin on lähetettävä takaisin uusi 8-tavuinen satunnainen haaste joka kerta mutta tallennettava ainoastaan viimeisin haaste.

CSM_173 Ajoneuvoyksikön todentamisessa ajoneuvoyksikön on käytettävä allekirjoitukseen viitteen DSS mukaisesti ECDSA-algoritmia sekä ajoneuvoyksikön VU_MA-avainparin avainkokoon sidoksissa olevaa hajautusalgoritmia, kuten CSM_50 alakohdassa on määritelty. Allekirjoituksen on oltava tekstimuodossa, kuten viitteessä TR-03111 on määritelty. Ajoneuvoyksikön on lähetettävä tuloksena oleva allekirjoitus kortille.

CSM_174 Vastaanottaessaan ajoneuvoyksikön allekirjoituksen EXTERNAL AUTHENTICATE -komennossa kortin on

— laskettava todennustunniste ketjuttamalla Card.CHR, kortin haaste r_{card} sekä ajoneuvoyksikön lyhytaikaisen julkisen avaimen Comp($VU.PK_{eph}$) tunniste,

— laskettava hash-tulos todennustunnisteesta käyttäen ajoneuvoyksikön VU_MA-avainparin avainkokoon sidoksissa olevaa hajautusalgoritmia, kuten CSM_50 alakohdassa on määritelty,

— todennettava ajoneuvoyksikön allekirjoitus käyttäen ECDSA-algoritmia sekä VU.PK-avainta ja laskettua hash-tulosta.

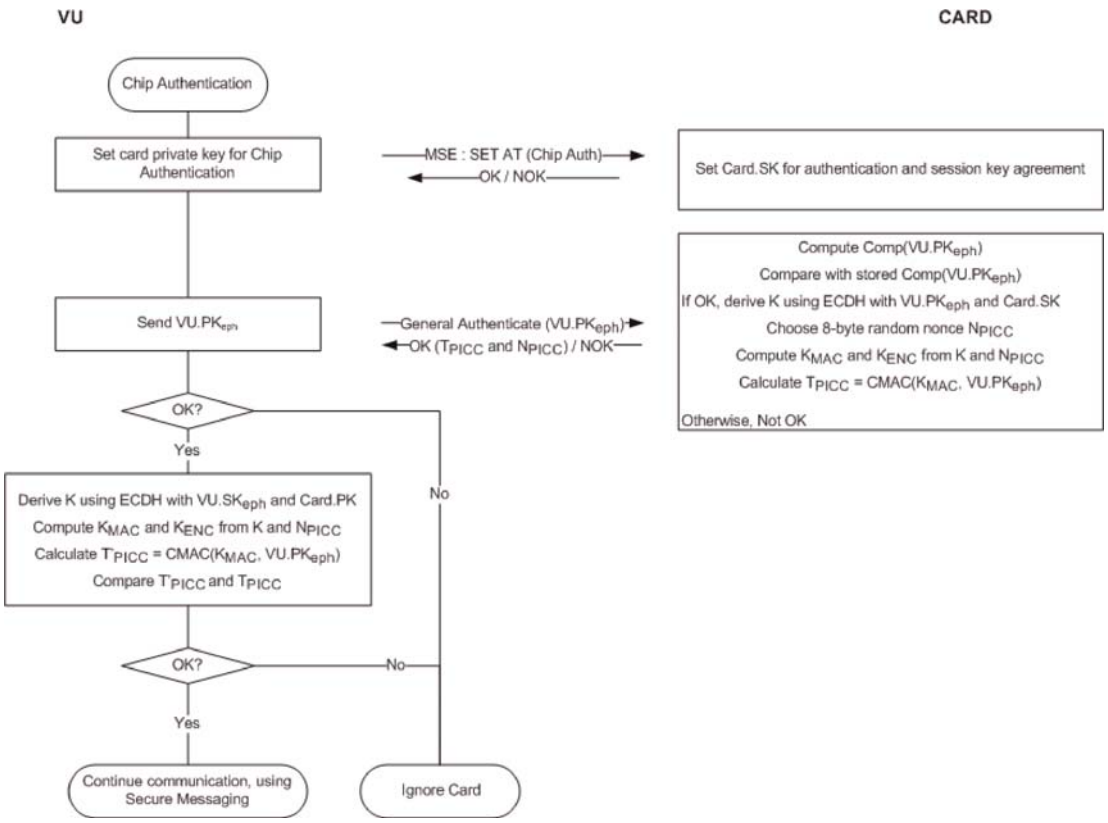
▼B

10.4. **Sirun todentaminen ja tilapäisestä avaimesta sopiminen**

CSM_175 Ajoneuvoyksikköjen ja korttien on käytettävä kaaviossa 7 kuvattua sirun todentamisprotokollaa, jolla kortti todennetaan ajoneuvoyksikölle. Sirun todentamisen avulla ajoneuvoyksikkö voi selkeästi todentaa kortin aitouden.

Kaavio 7

Sirun todentaminen ja tilapäisestä avaimesta sopiminen



CSM_176 Ajoneuvoyksikön ja kortin on suoritettava seuraavat vaiheet:

1. Ajoneuvoyksikkö aloittaa sirun todentamisprosessin lähettämällä MSE: Set AT -komennon, jolla ilmaistaan ’sirun todennus käyttäen ECDH-algoritmia, minkä tuloksena on tilapäinen AES-avaimen pituus, joka on sidoksissa kortin Card_MA-avainparin avainkokoon, kuten CSM_50 alakohdassa on määritelty’. Ajoneuvoyksikön on määritettävä kortin avainparin avainkoko kortin varmenteesta.

2. Ajoneuvoyksikkö lähettää kortille sen lyhytaikaisen avainparin julkisen pisteen $VU.PK_{eph}$. Kuten edellä CSM_164 alakohdassa on selitetty, ajoneuvoyksikkö loi tämän lyhytaikaisen avainparin ennen ajoneuvoyksikön varmenneketjun todentamista. Ajoneuvoyksikkö lähetti lyhytaikaisen julkisen avaimen $Comp(VU.PK_{eph})$ tunnisteen kortille, joka tallensi sen.

▼B

3. Kortti laskee avaimen Comp($VU.PK_{eph}$) avaimesta $VU.PK_{eph}$ ja vertaa sitä avaimen Comp($VU.PK_{eph}$) tallennettuun arvoon.

4. Kortti laskee salatun K:n arvon käyttäen ECDH-algoritmia yhdessä kortin pysyvän yksityisen avaimen ja ajoneuvoyksikön lyhytaikaisen julkisen avaimen kanssa.

5. Kortti valitsee satunnaisen 8-tavuisen nonce-luvun N_{PICC} ja luo sen perusteella K:n arvosta kaksi tilapäistä AES-avainta K_{MAC} ja K_{ENC}. Ks. CSM_179 alakohta.

6. Kortti laskee K_{MAC}-avainta käyttäen todennustunnisteen ajoneuvoyksikön lyhytaikaisen julkisen avaimen tunnisteesta: T_{PICC} = CMAC(K_{MAC}, $VU.PK_{eph}$). Kortti lähettää ajoneuvoyksikölle tunnisteet N_{PICC} ja T_{PICC}.

7. Ajoneuvoyksikkö laskee saman salatun K:n arvon kuin kortti laski vaiheessa 4 käyttäen ECDH-algoritmia yhdessä kortin pysyvän julkisen avaimen ja ajoneuvoyksikön lyhytaikaisen yksityisen avaimen kanssa.

8. Ajoneuvoyksikkö luo K:n sekä tunnisteen N_{PICC} arvosta kaksi tilapäistä avainta K_{MAC} ja K_{ENC}; ks. CSM_179 alakohta.

9. Ajoneuvoyksikkö todentaa todennustunnisteen T_{PICC}.

CSM_177 Edellä vaiheessa 3 kortin on laskettava avain Comp(VU.PKeph) julkisen pisteen x-koordinaatiksi avaimessa VU.PKeph.

CSM_178 Edellä vaiheissa 4 ja 7 kortin ja ajoneuvoyksikön on käytettävä viitteessä TR-03111 määriteltyä ECKA-EG-algoritmia.

CSM_179 Edellä vaiheissa 5 ja 8 kortin ja ajoneuvoyksikön on käytettävä tilapäisten AES-avainten luomiseen avaimen johtamisfunktiota siten, kuin viitteessä TR-03111 on määritelty, seuraavin tarkennuksin ja muutoksin:

— Laskurin arvo on ‘00 00 00 01’ K_{ENC}-avaimen osalta ja ‘00 00 00 02’ K_{MAC}-avaimen osalta.

— Vapaaehtoista nonce-lukua *r* on käytettävä ja sen on vastattava tunnistetta N_{PICC}.

— 128-bittisten AES-avainten luomiseen on käytettävä hajautusalgoritmia SHA-256.

— 192-bittisten AES-avainten luomiseen on käytettävä hajautusalgoritmia SHA-384.

— 256-bittisten AES-avainten luomiseen on käytettävä hajautusalgoritmia SHA-512.

Tilapäisten avainten pituuden (ts. pituuden, johon hash katkaistaan) on oltava sidoksissa Card_MA-avainparin pituuteen, kuten CSM_50 alakohdassa on määritelty.

▼B

CSM_180 Edellä vaiheissa 6 ja 9 kortin ja ajoneuvoyksikön on käytettävä AES-algoritmia CMAC-käyttötilassa, kuten viitteessä SP 800-38B määritelty. T_{PICC}-tunnisteen pituuden on oltava sidoksissa tilapäisten AES-avainten pituuteen, kuten CSM_50 alakohdassa on määritelty.

10.5. **Salattu sanomanvälitys**

10.5.1 *Yleistä*

CSM_181 Kaikki komennot ja vastaukset, joita ajoneuvoyksikön ja ajopiirturikortin välillä vaihdetaan onnistuneesta sirun todennuksesta lähtien käyttöjakson päättymiseen saakka, on suojattava salatulla sanomanvälityksellä (SM).

CSM_182 Lukuun ottamatta sellaisen tiedoston lukemista, jossa on käyttöehto SM-R-ENC-MAC-G2 (ks. lisäyksessä 2 oleva 4 kohta), salattua sanomanvälitystä on käytettävä todentamisen vaativassa käyttötilassa (authentication-only mode). Tässä käyttötilassa kaikkiin komentoihin ja vastauksiin lisätään salauksen tarkistussumma (eli MAC-koodi) sanoman aitouden ja eheyden varmistamiseksi.

CSM_183 Kun tietoja luetaan tiedostosta, jossa on käyttöehto SM-R-ENC-MAC-G2, salattua sanomanvälitystä on käytettävä käyttötilassa, joka edellyttää salauksen ja sen jälkeen todennuksen (encrypt-then-authenticate mode), mikä tarkoittaa, että vastauksen sisältävä data salataan ensin sanoman luottamuksellisuuden varmistamiseksi, minkä jälkeen muotoillusta salatusta datasta lasketaan MAC-koodi aitouden ja eheyden varmistamiseksi.

CSM_184 Salatussa sanomanvälityksessä on käytettävä viitteessä AES määriteltyä AES-salausta sekä tilapäisiä avaimia K_{MAC} ja K_{ENC}, joista on sovittu sirun todentamisen aikana.

CSM_185 Lähetysvaihelaskurina (SSC) on käytettävä etumerkitöntä kokonaislukua toistohyökkäysten estämiseksi. Lähetysvaihelaskurin koon on vastattava AES-salauksen lohkokokoa (128 bittiä). Lähetysvaihelaskurin on oltava MSB-first-muodossa. Lähetysvaihelaskuri alkaa nollasta (ts. ‘00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’), kun salattu sanomanvälitys aloitetaan. Lähetysvaihelaskurin arvoa on lisättävä aina ennen komennon tai vastauksen tietoyksikön (APDU) luomista, mikä tarkoittaa, että koska laskurin aloitusarvo salatussa sanomanvälitysjaksossa on 0, sen arvo ensimmäisessä komennossa on 1. Lähetysvaihelaskurin arvo ensimmäisessä vastauksessa on 2.

CSM_186 Sanoman salaamiseen on käytettävä K_{ENC}-avainta ja AES-algoritmia ISO 10116 -standardissa määritellyssä salauslohkoja ketjuttavassa käyttötilassa (CBC), missä limitysparametri m = 1 ja alustusvektori SV = E(K_{ENC}, SSC) (ts. K_{ENC}-avaimella salattu lähetysvaihelaskurin arvo).

CSM_187 Sanoman todentamiseen on käytettävä K_{MAC}-avainta ja AES-algoritmia CMAC-käyttötilassa siten kuin viitteessä SP 800-38B on määritelty. MAC-koodin pituuden on oltava sidoksissa tilapäisten AES-avainten pituuteen, kuten CSM_50 alakohdassa on määritelty. Lähetysvaihelaskuri on sisällytettävä MAC-koodiin liittämällä se koodin alkuun ennen datasähkeen todentamista.

▼B

10.5.2 *Salatun sanomanvälityksen rakenne*

CSM_188 Salatussa sanomanvälityksessä on hyödynnettävä ainoastaan salatun sanomanvälityksen dataobjekteja (ks. ISO 7816-4), jotka luetellaan Taulukko 5. Näitä dataobjekteja on käytettävä sanomassa aina taulukossa määritellyssä järjestyksessä.

Taulukko 5

Salatun sanomanvälityksen dataobjektit

Dataobjektin nimi	Tuntomerkki	Esiintyminen pakollinen [(M)andatory], ehdollinen [(C)onditional] tai kielletty [(F)orbidden]	
		komennoissa	vastauksissa
Koodaamaton data, jota ei ole BER-TLV-koodattu	‘81’	C	C
Koodaamaton data, joka on BER-TLV-koodattu, lukuun ottamatta salatun sanomanvälityksen dataobjekteja	‘B3’	C	C
Täytetyn sisällön osoitin ja kryptogrammi, koodaamaton data, jota ei ole BER-TLV-koodattu	‘87’	C	C
Suojattu Le	‘97’	C	F
Suorittamisen tila	‘99’	F	M
Salauksen tarkistussumma	‘8E’	M	M

Huomautus: Kuten lisäyksessä 2 on määritelty, ajopiirturikortit voivat tukea READ BINARY- ja UPDATE BINARY -komentoja, joissa on pariton INS-tavu (‘B1’ edustaa ‘D7’). Näitä komentovariantteja tarvitaan yli 32 768 tavun tiedostojen lukemiseen ja päivittämiseen. Jos tällaista varianttia käytetään, on käytettävä dataobjektia, jonka tuntomerkki on ‘B3’, sellaisen dataobjektin sijaan, jonka tuntomerkki on ‘81’. Ks. lisätietoa lisäyksessä 2.

CSM_189 Kaikki salatun sanomanvälityksen dataobjektit on DER TLV -koodattava siten kuin ISO 8825-1 -standardissa on määritelty. Tällaisen koodauksen tuloksena on seuraavanlainen tuntomerkki-pituus-sisältö-rakenne (TLV):

Tuntomerkki: Tuntomerkki on koodattu yhteen tai kahteen tavuun ja ilmoittaa sisällön.

Pituus: Pituus on koodattu etumerkittömänä kokonaislukuna yhteen, kahteen tai kolmeen tavuun, jolloin enimmäispituus on 65 535 tavua. Tavujen vähimmäismäärää on käytettävä.

Sisältö: Sisältö on koodattu nollaan tai useampaan tavuun.

CSM_190 Salatulla sanomanvälityksellä suojatut tietoyksiköt on luotava seuraavasti:

— Komennon ylätunniste on sisällytettävä MAC-koodin laskentaan, jolloin luokkaa osoittavassa CLA-tavussa on käytettävä arvoa ‘0C’.

▼B

— Kuten lisäyksessä 2 on määritelty, kaikkien INS-tavujen on oltava parillisia, lukuun ottamatta mahdollisesti READ BINARY- ja UPDATE BINARY -komentojen parittomia INS-tavuja.

— Lc:n todellinen arvo muokataan muotoon Lc' salatun sanomanvälityksen käytön jälkeen.

— Datakentän on koostuttava salatun sanomanvälityksen dataobjekteista.

— Uusi Le-tavu on asetettava suojatun komennon tietoyksikössä arvoon ‘00’. Tarvittaessa dataobjekti ‘97’ on sisällytettävä datakenttään Le:n alkuperäisen arvon ilmaisemiseksi.

CSM_191 Salattava dataobjekti on täytettävä ISO 7816-4 -standardin mukaisesti käyttämällä täytetyn sisällön osoitinta ‘01’. MAC-koodin laskemiseksi jokainen dataobjekti tietoyksikössä on lisäksi erikseen täytettävä ISO 7816-4 -standardin mukaisesti.

Huomautus: Salatussa sanomanvälityksessä täyttö on suoritettava aina salatun sanomanvälityksen kerroksessa eikä CMAC- tai CBC-algoritmeilla.

Yhteenveto ja esimerkit

Komennon tietoyksiköllä, johon sovelletaan salattua sanomanvälitystä, on seuraava rakenne riippuen vastaavan suojaamattoman komennon tapauksesta (DO tarkoittaa dataobjektia):

Tapaus 1	CLA INS P1 P2 || Lc' || DO ‘8E’ || Le
Tapaus 2	CLA INS P1 P2 || Lc' || DO ‘97’ || DO‘8E’ || Le
Tapaus 3 (parillinen INS-tavu)	CLA INS P1 P2 || Lc' || DO ‘81’ || DO‘8E’ || Le
Tapaus 3 (pariton INS-tavu):	CLA INS P1 P2 || Lc' || DO ‘B3’ || DO‘8E’ || Le
Tapaus 4 (parillinen INS-tavu):	CLA INS P1 P2 || Lc' || DO ‘81’ || DO‘97’ || DO‘8E’ || Le
Tapaus 4 (pariton INS-tavu):	CLA INS P1 P2 || Lc' || DO ‘B3’ || DO‘97’ || DO‘8E’ || Le

missä Le = ‘00’ tai ‘00 00’ riippuen siitä, onko käytössä lyhyitä pituuskenttiä vai laajennettuja pituuskenttiä; ks. ISO 7816-4.

Vastauksen tietoyksiköllä, johon sovelletaan salattua sanomanvälitystä, on seuraava rakenne riippuen vastaavan suojaamattoman vastauksen tapauksesta:

Tapaus 1 tai 3:	DO ‘99’ || DO ‘8E’ || SW1SW2
Tapaus 2 tai 4 (parillinen INS-tavu) salauksella:	DO ‘81’ || DO ‘99’ || DO ‘8E’ || SW1SW2
Tapaus 2 tai 4 (parillinen INS-tavu) ilman salausta:	DO ‘87’ || DO ‘99’ || DO ‘8E’ || SW1SW2
Tapaus 2 tai 4 (pariton INS-tavu) ilman salausta:	DO ‘B3’ || DO ‘99’ || DO ‘8E’ || SW1SW2

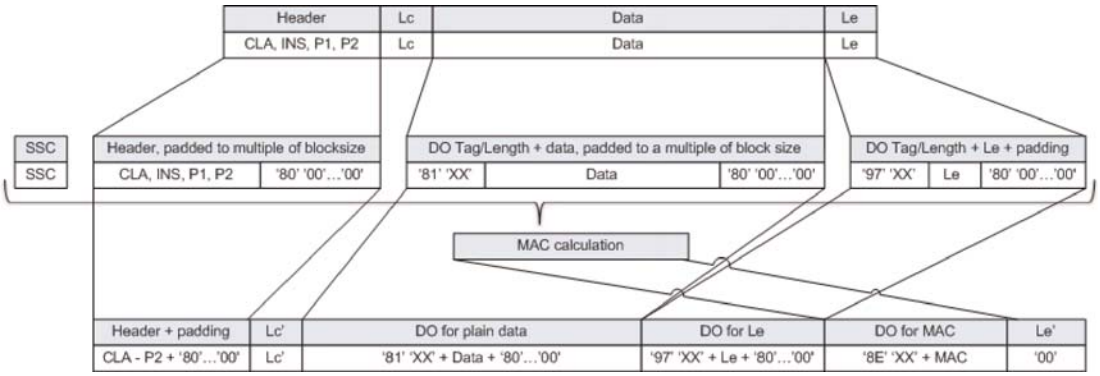
Huomautus: Tapauksia 2 tai 4 (pariton INS-tavu), joissa on salaus, ei milloinkaan käytetä ajoneuvoyksikön ja kortin väliseen viestintään.

▼B

Jäljempänä esitetään kolme esimerkkiä tietoyksiköiden muunnoksista komennoissa, joissa on parillinen INS-koodi. Kaaviossa 8 esitetään todennettu tapauksen 4 komennon tietoyksikkö, kaaviossa 9 esitetään todennettu tapauksen 2 tai 4 vastauksen tietoyksikkö ja kaaviossa 10 esitetään salattu ja todennettu tapauksen 2 tai 4 vastauksen tietoyksikkö.

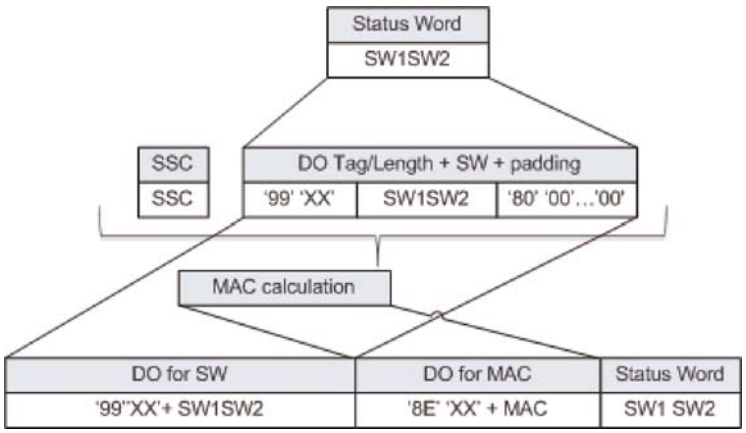
Kaavio 8

Todennetun tapauksen 4 komennon tietoyksikön muunnos



Kaavio 9

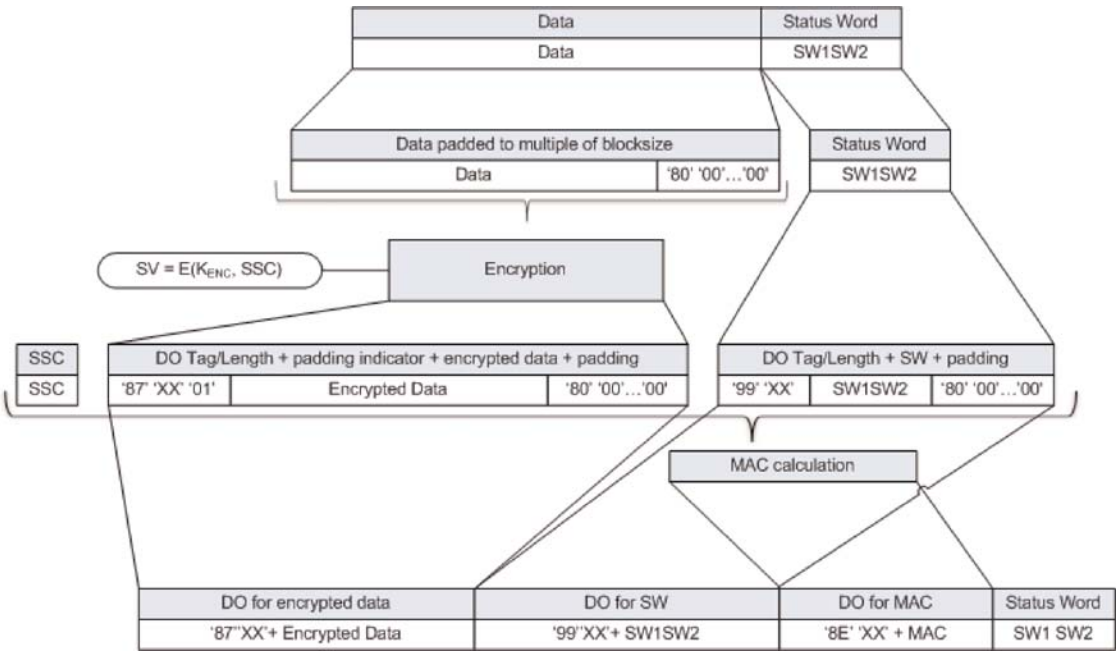
Todennetun tapauksen 1 tai 3 vastauksen tietoyksikön muunnos



▼B

Kaavio 10

Salatun ja todennetun tapauksen 2 tai 4 vastauksen tietoyksikön muunnos



10.5.3 *Salatun sanomanvälitysjakson lopettaminen*

CSM_192 Ajoneuvoyksikön on lopetettava käynnissä oleva salattu sanomanvälitysjakso ainoastaan silloin, jos jokin seuraavista ehdoista täyttyy:

— Se vastaanottaa salaamattoman vastauksen tietoyksikön.

— Se havaitsee virheen salatun sanomanvälityksen vastauksen tietoyksikössä:

  — Odotettu salatun sanomanvälityksen dataobjekti puuttuu, dataobjektien järjestys on virheellinen tai mukana on tuntematon dataobjekti.

  — Salatun sanomanvälityksen dataobjekti on virheellinen, esim. MAC-arvo tai TLV-rakenne on virheellinen tai täytön osoitin tuntomerkissä ‘87’ ei ole ‘01’.

— Kortti lähettää tilaa osoittavan tavun, jonka mukaan se on havainnut salatun sanomanvälityksen virheen (ks. CSM_194 alakohta).

— Komentojen ja niihin liittyvien vastausten enimmäismäärä käynnissä olevassa jaksossa täyttyy. Valmistajan on määriteltävä tämä enimmäismäärä tietyn ajoneuvoyksikön osalta ottaen huomioon käytettyjen varusteiden turvallisuusvaatimukset ja siten, että salatun sanomanvälityksen komentojen ja niihin liittyvien vastausten enimmäisarvo käyttöjaksoa kohden on 240.

▼B

CSM_193 Ajopiirturikortin on lopetettava käynnissä oleva salattu sanomanvälitysjakso ainoastaan silloin, jos jokin seuraavista ehdoista täyttyy:

— Se vastaanottaa salaamattoman komennon tietoyksikön.

— Se havaitsee virheen salatun sanomanvälityksen komennon tietoyksikössä:

— Odotettu salatun sanomanvälityksen dataobjekti puuttuu, dataobjektien järjestys on virheellinen tai mukana on tuntematon dataobjekti.

— Salatun sanomanvälityksen dataobjekti on virheellinen, esim. MAC-arvo tai TLV-rakenne on virheellinen.

— Sen virta katkeaa tai se asetetaan alkutilaan.

— Ajoneuvoyksikkö valitsee sovelluksen kortilla.

— Ajoneuvoyksikkö aloittaa ajoneuvoyksikön todentamisprosessin.

— Komentojen ja niihin liittyvien vastausten enimmäismäärä käynnissä olevassa jaksossa täyttyy. Valmistajan on määriteltävä tämä enimmäismäärä tietyn kortin osalta ottaen huomioon käytettyjen varusteiden turvallisuusvaatimukset ja siten, että salatun sanomanvälityksen komentojen ja niihin liittyvien vastausten enimmäisarvo käyttöjaksoa kohden on 240.

CSM_194 Ajopiirturikortti käsittelee salattua sanomanvälitystä koskevia virheitä seuraavasti:

— Jos komennon tietoyksiköstä puuttuu joitakin odotettuja salatun sanomanvälityksen dataobjekteja, dataobjektien järjestys on virheellinen tai mukana on tuntemattomia dataobjekteja, ajopiirturikortin on vastattava tilaa osoittavilla tavuilla ‘69 87’.

— Jos salatun sanomanvälityksen dataobjekti komennon tietoyksikössä on virheellinen, ajopiirturikortin on vastattava tilaa osoittavilla tavuilla ‘69 88’.

Tällöin tilaa osoittavat tavut on lähetettävä takaisin ilman salattua sanomanvälitystä.

CSM_195 Jos ajoneuvoyksikön ja ajopiirturikortin välinen salattu sanomanvälitysjakso lopetetaan, ajoneuvoyksikön ja ajopiirturikortin on

— tuhottava suojatusti tallennetut tilapäiset avaimet

— aloitettava välittömästi uusi salattu sanomanvälitysjakso siten kuin 10.2–10.5 kohdassa on kuvattu.

CSM_196 Jos ajoneuvoyksikkö päättää jostain syystä aloittaa uudelleen molemminpuolisen todentamisen asetetun kortin kanssa, prosessi alkaa kortin varmenneketjun todentamisella, joka kuvataan 10.2 kohdassa, ja jatkuu 10.2–10.5 kohdassa kuvatulla tavalla.

▼B

11. AJONEUVOYKSIKÖN JA ULKOISEN GNSS-LAITTEISTON KYTKEMINEN, MOLEMMINPUOLINEN TODENTAMINEN JA SALATTU SANOMANVÄLITYS

11.1. **Yleistä**

CSM_197 GNSS-laitteisto, jonka avulla ajoneuvoyksikkö määrittää sijaintinsa, voi olla sisäinen (ts. asennettu kiinteästi ajoneuvoyksikön kuoren sisälle) tai ulkoinen moduuli. Ensimmäisessä tapauksessa GNSS-laitteiston ja ajoneuvoyksikön välistä sisäistä viestintää ei tarvitse standardoida eikä tämän luvun vaatimuksia sovelleta. Jälkimmäisessä tapauksessa ajoneuvoyksikön ja ulkoisen GNSS-laitteiston välinen viestintä on standardoitava ja suojattava siten kuin tässä luvussa kuvataan.

CSM_198 Ajoneuvoyksikön ja ulkoisen GNSS-laitteiston välinen salattu viestintä on toteutettava samoin kuin ajoneuvoyksikön ja ajopiirturikortin välinen salattu viestintä siten, että ulkoinen GNSS-laitteisto (EGF, external GNSS facility) ottaa kortin roolin. Ulkoisen GNSS-laitteiston on täytettävä kaikki 10 luvussa mainitut ajopiirturikortteja koskevat vaatimukset ottaen huomioon tässä luvussa esitetyt poikkeukset, selvennykset ja lisäykset. Etenkin molemminpuolinen varmenneketjun todentaminen, ajoneuvoyksikön todentaminen sekä sirun todentaminen on suoritettava siten kuin 11.3 ja 11.4 kohdassa on kuvattu.

CSM_199 Ajoneuvoyksikön ja ulkoisen GNSS-laitteiston välinen viestintä eroaa ajoneuvoyksikön ja kortin välisestä viestinnästä siten, että ajoneuvoyksikkö ja ulkoinen GNSS-laitteisto on kytkettävä yhteen korjaamossa, ennen kuin ne voivat jakaa GNSS-tietoja tavanomaisen toiminnan aikana. Kytkemisprosessi on kuvattu 11.2 kohdassa.

CSM_200 Ajoneuvoyksikön ja ulkoisen GNSS-laitteiston välisessä viestinnässä on käytettävä ISO 7816-4- ja ISO 7816-8 -standardeihin perustuvia APDU-komentoja ja -vastauksia. Näiden tietoyksiköiden (APDU) täsmällinen rakenne on määritelty tämän liitteen lisäyksessä 2.

11.2. **Ajoneuvoyksikön kytkeminen ulkoiseen GNSS-laitteistoon**

CSM_201 Korjaamon on hoidettava ajoneuvoyksikön kytkeminen ulkoiseen GNSS-laitteistoon. Kytkemisen jälkeen ajoneuvoyksikön ja ulkoisen GNSS-laitteiston on kyettävä viestimään tavanomaisen toiminnan aikana.

CSM_202 Ajoneuvoyksikön kytkemisen ulkoiseen GNSS-laitteistoon on oltava mahdollista vain silloin, kun ajoneuvoyksikkö on kalibrointitilassa. Ajoneuvoyksikkö aloittaa kytkemisen.

CSM_203 Korjaamo voi kytkeä ajoneuvoyksikön uudelleen toiseen tai samaan ulkoiseen GNSS-laitteistoon milloin tahansa. Uudelleenkytkemisen aikana ajoneuvoyksikön on tuhottava suojatusti olemassa oleva EGF_MA-varmenne muististaan ja tallennettava sen ulkoisen GNSS-laitteiston EGF_MA-varmenne, johon se kytketään.

CSM_204 Korjaamo voi kytkeä ulkoisen GNSS-laitteiston uudelleen toiseen tai samaan ajoneuvoyksikköön milloin tahansa. Uudelleenliittämisen aikana ulkoisen GNSS-laitteiston on tuhottava suojatusti olemassa oleva VU_MA-varmenne muististaan ja tallennettava sen ajoneuvoyksikön VU_MA-varmenne, johon se kytketään.

▼B

11.3. **Molemminpuolinen varmenneketjun todentaminen**

11.3.1 *Yleistä*

CSM_205 Ajoneuvoyksikön ja ulkoisen GNSS-laitteiston molemminpuolinen varmenneketjun todentaminen on suoritettava ainoastaan silloin, kun korjaamo kytkee ajoneuvoyksikön ulkoiseen GNSS-laitteistoon. Kun ajoneuvoyksikkö on kytketty ulkoiseen GNSS-laitteistoon, niiden tavanomaisen toiminnan aikana ei todenneta mitään varmenteita. Sen sijaan ajoneuvoyksikön ja ulkoisen GNSS-laitteiston on luotettava kytkemisen aikana tallennettuihin varmenteisiin sen jälkeen, kun näiden varmenteiden voimassaoloaika on tarkistettu. Ajoneuvoyksikkö ja ulkoinen GNSS-laitteisto eivät saa luottaa mihinkään muihin varmenteisiin, kun niiden välinen viestintä suojataan tavanomaisen toiminnan aikana.

11.3.2 *Ajoneuvoyksikön ja ulkoisen GNSS-laitteiston kytkemisen aikana*

CSM_206 Kun ajoneuvoyksikkö kytketään ulkoiseen GNSS-laitteistoon, ajoneuvoyksikön on käytettävä kaaviossa 4 (10.2.1 kohta) kuvattua protokollaa ulkoisen GNSS-laitteiston varmenneketjun todentamiseen.

Huomautuksia kaavioon 4 tässä yhteydessä:

— Tässä lisäyksessä ei käsitellä viestinnän hallintaa. Ulkoinen GNSS-laitteisto ei kuitenkaan ole älykäs kortti, minkä vuoksi ajoneuvoyksikkö ei todennäköisesti lähetä Reset-komentoa aloittaakseen viestinnän eikä vastaanota ATR-signaalia.

— Kaaviossa mainittuja kortin varmenteita ja julkisia avaimia on tulkittava samoin kuin ulkoisen GNSS-laitteiston varmenteita ja julkisia avaimia molemminpuolisen todentamisen yhteydessä. Edellä 9.1.6 kohdassa näistä käytetään nimitystä EGF_MA.

— Kaaviossa mainittuja Card.CA-nimisiä varmenteita ja julkisia avaimia on tulkittava samoin kuin jäsenvaltion varmenneviranomaisen varmenteita ja julkisia avaimia ulkoisen GNSS-laitteiston varmenteiden allekirjoittamisen yhteydessä. Edellä 9.1.3 kohdassa näistä käytetään nimitystä MSCA_VU-EGF.

— Kaaviossa mainittua Card.CA.EUR-varmennetta on tulkittava samoin kuin eurooppalaista juurivarmennetta, joka ilmoitetaan MSCA_VU-EGF-varmenteen varmenneviranomaisen viitteessä (CAR).

— Kaaviossa mainittua Card.Link-varmennetta on tulkittava samoin kuin mahdollista ulkoisen GNSS-laitteiston linkkivarmennetta. Kuten edellä 9.1.2 kohdassa on määritelty, tämä on uuden eurooppalaisen juuriavainparin linkkivarmenne, jonka ERCA on luonut ja allekirjoittanut edellisellä eurooppalaisella yksityisellä avaimella.

— Card.Link.EUR-varmenne on eurooppalainen juurivarmenne, joka ilmoitetaan Card.Link-varmenteen varmenneviranomaisen viitteessä (CAR).

— Viitteen `cardExtendedSerialNumber`sijaan ajoneuvoyksikön on luettava viite `sensorGNSSserialNumber`EF-tiedoston ICC-tiedoista.

— Ajopiirturikortin sovellustunnisteen (AID) sijaan ajoneuvoyksikön on valittava ulkoisen GNSS-laitteiston sovellustunniste.

— ’Korttia ei hyväksytä’ (Ignore Card) on tulkittava samoin kuin ’Ulkoista GNSS-laitteistoa ei hyväksytä’ (Ignore EGF).

▼B

CSM_207 Kun ajoneuvoyksikkö on todentanut EGF_MA-varmenteen, sen on tallennettava kyseinen varmenne tavanomaisen toiminnan aikana tapahtuvaa käyttö varten; ks. 11.3.3 kohta.

CSM_208 Kun ulkoinen GNSS-laitteisto kytketään ajoneuvoyksikköön, ulkoisen GNSS-laitteiston on käytettävä kaaviossa 5 (10.2.2 kohta) kuvattua protokollaa ajoneuvoyksikön varmenneketjun todentamiseen.

Huomautuksia kaavioon 5 tässä yhteydessä:

— Ajoneuvoyksikön on luotava uusi lyhytaikainen avainpari käyttäen ulkoisen GNSS-laitteiston varmenteessa olevia domain-parametreja.

— Kaaviossa mainittuja VU-nimisiä varmenteita ja julkisia avaimia käytetään molemminpuoliseen todentamiseen. Edellä 9.1.4 kohdassa näistä käytetään nimitystä VU_MA.

— Kaaviossa mainittuja VU.CA-nimisiä varmenteita ja julkisia avaimia käytetään ajoneuvoyksikön ja ulkoisen GNSS-laitteiston varmenteiden allekirjoittamiseen. Edellä 9.1.3 kohdassa näistä käytetään nimitystä MSCA_VU-EGF.

— Kaaviossa mainittu VU.CA.EUR-varmenne on eurooppalainen juurivarmenne, joka ilmoitetaan VU.CA-varmenteen varmenneviranomaisen viitteessä (CAR).

— Kaaviossa mainittu VU.Link-varmenne on mahdollinen ajoneuvoyksikön linkkivarmenne. Kuten edellä 9.1.2 kohdassa on määritelty, tämä on uuden eurooppalaisen juuriavainparin linkkivarmenne, jonka ERCA on luonut ja allekirjoittanut edellisellä eurooppalaisella yksityisellä avaimella.

— VU.Link.EUR-varmenne on eurooppalainen juurivarmenne, joka ilmoitetaan VU.Link-varmenteen varmenneviranomaisen viitteessä (CAR).

CSM_209 Poiketen CSM_167 alakohdan vaatimuksesta ulkoisen GNSS-laitteiston on käytettävä GNSS-aikaa minkä tahansa esitetyn varmenteen voimassaoloajan todentamiseen.

CSM_210 Kun ulkoinen GNSS-laitteisto on todentanut VU_MA-varmenteen, sen on tallennettava kyseinen varmenne tavanomaisen toiminnan aikana tapahtuvaa käyttö varten; ks. 11.3.3 kohta.

11.3.3 *Tavanomaisen toiminnan aikana*

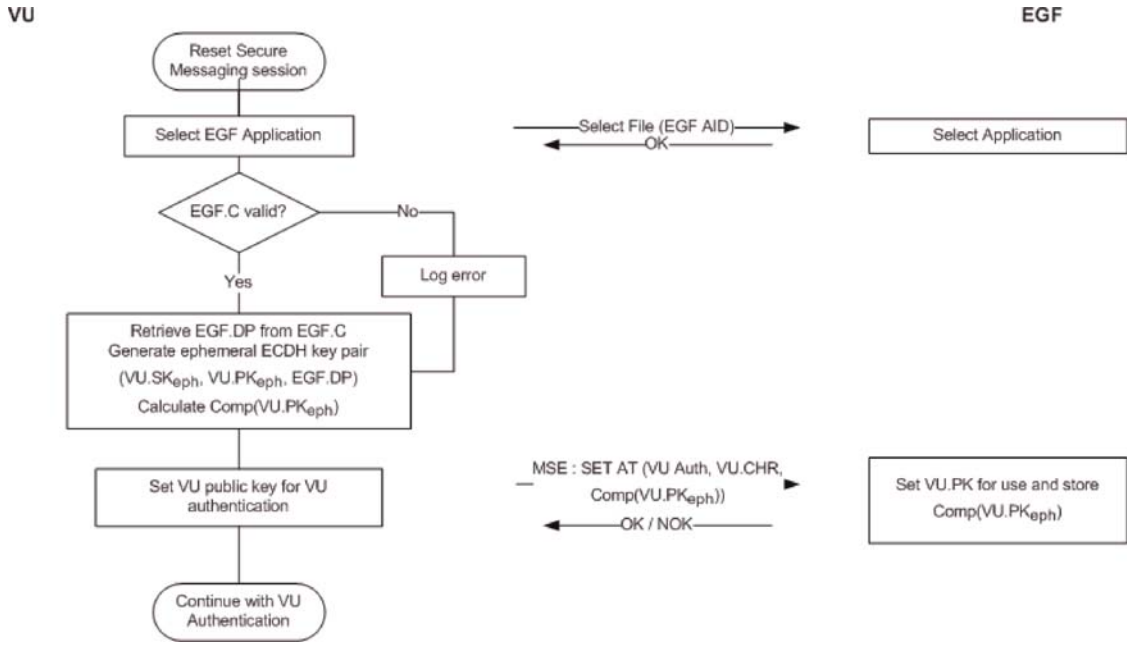
CSM_211 Tavanomaisen toiminnan aikana ajoneuvoyksikön ja ulkoisen GNSS-laitteiston on käytettävä kaaviossa 11 kuvattua protokollaa tallennettujen EGF_MA- ja VU_MA-varmenteiden voimassaoloajan todentamiseen sekä julkisen avaimen VU_MA asentamiseen myöhempää ajoneuvoyksikön todentamista varten. Tavanomaisen toiminnan aikana ei suoriteta muuta varmenneketjujen molemminpuolista todentamista.

On huomattava, että kaavio 11 koostuu pääasiassa kaaviossa 4 ja kaaviossa 5 esitetyistä ensimmäisistä vaiheista. Jälleen on otettava huomioon, että ulkoinen GNSS-laitteisto ei ole älykäs kortti, minkä vuoksi ajoneuvoyksikkö ei todennäköisesti lähetä Reset-komentoa aloittaakseen viestinnän eikä vastaanota ATR-signaalia. Tätä ei kuitenkaan käsitellä tässä lisäyksessä.

▼B

Kaavio 11

Varmenteen voimassaoloajan molemminpuolinen todentaminen ajoneuvoyksikön ja ulkoisen GNSS-laitteiston välisen tavanomaisen toiminnan aikana



CSM_212 Kuten kaaviossa 11 esitetään, ajoneuvoyksikön on kirjattava virhe, jos EGF_MA-varmenne on vanhentunut. Molemminpuolinen todentaminen, avaimesta sopiminen ja myöhempi viestintä salatun sanomanvälityksen kautta etenevät kuitenkin tavanomaisesti.

11.4. **Ajoneuvoyksikön todentaminen, sirun todentaminen ja tilapäisestä avaimesta sopiminen**

CSM_213 Ajoneuvoyksikön todentaminen, sirun todentaminen ja tilapäisestä avaimesta sopiminen ajoneuvoyksikön ja ulkoisen GNSS-laitteiston välillä on suoritettava kytkemisen aikana sekä silloin, kun salattu sanomanvälitysjakso aloitetaan uudelleen tavanomaisen toiminnan aikana. Ajoneuvoyksikön ja ulkoisen GNSS-laitteiston on suoritettava 10.3 ja 10.4 kohdassa kuvatut prosessit. Kaikkia näiden kohtien vaatimuksia on sovellettava.

11.5. **Salattu sanomanvälitys**

CSM_214 Kaikki komennot ja vastaukset, joita ajoneuvoyksikön ja ulkoisen GNSS-laitteiston välillä vaihdetaan onnistuneesta sirun todennuksesta lähtien käyttöjakson päättymiseen saakka, on suojattava salatulla sanomanvälityksellä todentamisen vaativassa käyttötilassa (authentication-only mode). Kaikkia 10.5 kohdan vaatimuksia on sovellettava.

CSM_215 Jos ajoneuvoyksikön ja ulkoisen GNSS-laitteiston välinen salattu sanomanvälitysjakso lopetetaan, ajoneuvoyksikön on aloitettava välittömästi uusi salattu sanomanvälitysjakso siten kuin 11.3.3 ja 11.4 kohdassa on kuvattu.

12. AJONEUVOYKSIKÖN JA LIIKETUNNISTIMEN LIITTÄMINEN SEKÄ VIESTINTÄ

12.1. **Yleistä**

CSM_216 Ajoneuvoyksikön ja liiketunnistimen on viestittävä siten, että ne käyttävät ISO 16844-3 -standardissa määriteltyä rajapintaprotokollaa liittämisen ja tavanomaisen toiminnan aikana tässä luvussa ja 9.2.1 kohdassa mainituin muutoksin.

▼B

Huomautus: Tämän luvun lukijoiden oletetaan tuntevan ISO 16844-3 -standardin sisältö.

12.2. **Ajoneuvoyksikön ja liiketunnistimen liittäminen eri sukupolvien avaimilla**

Kuten edellä 9.2.1 kohdassa on selitetty, liiketunnistimen pääavain ja kaikki siihen liittyvät avaimet korvataan säännöllisesti. Sen vuoksi korjaamokorteissa voi olla jopa kolme liiketunnistimeen liittyvää (peräkkäisten avainsukupolvien) AES-avainta K_{M-WC}. Vastaavasti liiketunnistimissa olevia tietoja on voitu salata kolmella erilaisella AES-salausjärjestelmällä (jotka perustuvat liiketunnistimen pääavaimen K_M peräkkäisiin sukupolviin). Ajoneuvoyksikkö sisältää ainoastaan yhden liiketunnistimeen liittyvän avaimen K_{M-VU}.

CSM_217 Toisen sukupolven ajoneuvoyksikkö on liitettävä toisen sukupolven liiketunnistimeen seuraavasti (vertaa ISO 16844-3 -standardissa esitettyyn taulukkoon 6):

1. Toisen sukupolven korjaamokortti asetetaan ajoneuvoyksikköön, joka liitetään liiketunnistimeen.

2. Ajoneuvoyksikkö lukee kaikki saatavilla olevat K_{M-WC}-avaimet korjaamokortilta, tarkistaa avainten versionumerot ja valitsee sen, joka vastaa ajoneuvoyksikön K_{M-VU}-avaimen versionumeroa. Jos korjaamokortilla ei ole sopivaa K_{M-WC}-avainta, ajoneuvoyksikkö lopettaa liittämisprosessin ja näyttää asianmukaisen virheilmoituksen korjaamokortin haltijalle.

3. Ajoneuvoyksikkö laskee liiketunnistimen pääavaimen K_M avaimista K_{M-VU} ja K_{M-WC} ja laskee tunnistusavaimen K_{ID} avaimesta K_M, kuten 9.2.1 kohdassa on määritelty.

4. Ajoneuvoyksikkö lähettää komennon, jolla aloitetaan liittäminen liiketunnistimeen ISO 16844-3 -standardin mukaisesti, ja salaa liiketunnistimelta vastaanottamansa sarjanumeron tunnistusavaimella K_{ID}. Ajoneuvoyksikkö lähettää salatun sarjanumeron takaisin liiketunnistimelle.

5. Liiketunnistin vertaa salattua sarjanumeroa peräkkäin jokaiseen sarjanumeron salaukseen, joita sen hallussa on. Jos se löytää osuman, ajoneuvoyksikkö on todennettu. Liiketunnistin tarkistaa ajoneuvoyksikön käyttämän K_{ID}-avaimen sukupolven ja lähettää takaisin liittämisavaimensa vastaavan salatun version (ts. joka on salattu käyttäen saman sukupolven K_M-avainta).

6. Ajoneuvoyksikkö avaa liittämisavaimen salauksen käyttämällä K_M-avainta, luo tilapäisen K_S-avaimen, salaa sen liittämisavaimella ja lähettää lopputuloksen liiketunnistimelle. Liiketunnistin avaa K_S-avaimen salauksen.

7. Ajoneuvoyksikkö kokoaa liittämistiedot siten kuin ISO 16844-3 -standardissa on määritelty, salaa tiedot liittämisavaimella ja lähettää lopputuloksen liiketunnistimelle. Liiketunnistin avaa liittämistietojen salauksen.

8. Liiketunnistin salaa vastaanotetut liittämistiedot vastaanotetulla K_S-avaimella ja lähettää tiedot takaisin ajoneuvoyksikölle. Ajoneuvoyksikkö todentaa, että liittämistiedot ovat samat tiedot, jotka ajoneuvoyksikkö lähetti liiketunnistimelle edellisessä vaiheessa. Jos näin on, tämä

▼B

osoittaa, että liiketunnistin käytti samaa K_S-avainta kuin ajoneuvoyksikkö ja lähetti vaiheessa 5 liittämisavaimen, joka oli salattu oikean sukupolven K_M-avaimella. Siten liiketunnistin on todennettu.

On syytä huomata, että vaiheet 2 ja 5 eroavat ISO 16844-3 -standardin vakioprosessista, kun taas muut vaiheet ovat vakiomuotoisia.

Esimerkki: Oletetaan, että liittäminen suoritetaan ERCA (3) -varmenteen voimassaoloajan ensimmäisenä vuonna; ks. 9.2.1.2 kohdassa oleva kaavio 2. Lisäksi:

— Oletetaan, että liiketunnistin myönnettiin ERCA (1) -varmenteen voimassaoloajan viimeisenä vuonna. Se sisältää tällöin seuraavat avaimet ja tiedot:

  — N_s[1]: sen sarjanumero, joka on salattu ensimmäisen sukupolven K_{ID}-avaimella,

  — N_s[2]: sen sarjanumero, joka on salattu toisen sukupolven K_{ID}-avaimella,

  — N_s[3]: sen sarjanumero, joka on salattu kolmannen sukupolven K_{ID}-avaimella,

  — K_P[1]: sen ensimmäisen sukupolven liittämisavain ([1]), joka on salattu ensimmäisen sukupolven K_M-avaimella,

  — K_P[2]: sen toisen sukupolven liittämisavain, joka on salattu toisen sukupolven K_M-avaimella,

  — K_P[3]: sen kolmannen sukupolven liittämisavain, joka on salattu kolmannen sukupolven K_M-avaimella.

— Oletetaan, että korjaamokortti myönnettiin ERCA (3) -varmenteen voimassaoloajan ensimmäisenä vuonna. Tällöin se sisältää toisen ja kolmannen sukupolven $K_{M\text{-}WC}$-avaimen.

— Oletetaan, että ajoneuvoyksikkö on toisen sukupolven ajoneuvoyksikkö, joka sisältää toisen sukupolven $K_{M\text{-}VU}$-avaimen.

Tällöin vaiheet 2–5 suoritetaan seuraavasti:

— Vaihe 2: Ajoneuvoyksikkö lukee toisen ja kolmannen sukupolven $K_{M\text{-}WC}$-avaimet korjaamokortilta ja tarkistaa niiden versionumerot.

— Vaihe 3: Ajoneuvoyksikkö yhdistää toisen sukupolven $K_{M\text{-}WC}$-avaimen sen omaan $K_{M\text{-}VU}$-avaimeen ja laskee avaimet K_M ja K_{ID}.

— Vaihe 4: Ajoneuvoyksikkö salaa liiketunnistimelta vastaanottamansa sarjanumeron K_{ID}-avaimella.

— Vaihe 5: Liiketunnistin vertaa vastaanotettua dataa sarjanumeroon N_s[1] eikä löydä osumaa. Seuraavaksi se vertaa dataa sarjanumeroon N_s[2] ja löytää osuman. Se päättelee, että ajoneuvoyksikkö on toisen sukupolven ajoneuvoyksikkö, ja lähettää sen vuoksi takaisin K_P[2]-avaimen.

([1]) On syytä huomata, että ensimmäisen, toisen ja kolmannen sukupolven liittämisavaimet voivat tosiasiassa olla sama avain tai ne voivat olla kolme erilaista ja eripituista avainta, kuten CSM_117 alakohdassa on selitetty.

▼B

12.3. **Ajoneuvoyksikön ja liiketunnistimen liittäminen sekä viestintä AES-avaimilla**

CSM_218 Kuten 9.2.1 kohdassa olevassa Taulukko 3 on määritelty, kaikkien (toisen sukupolven) ajoneuvoyksikön ja liiketunnistimen liittämiseen sekä myöhempään viestintään käytettävien avainten on oltava AES-avaimia eikä kaksinkertaisia TDES-avaimia, kuten ISO 16844-3 -standardissa on määritelty. Näiden AES-avainten pituus voi olla 128, 192 tai 256 bittiä. AES-avainten lohkokoko on 16 tavua, joten salatun sanoman pituuden on oltava 16 tavun kerrannainen verrattuna TDES-avainten 8 tavuun. Lisäksi joitakin näitä sanomia käytetään AES-avainten kuljettamiseen, ja näiden avainten pituus voi olla 128, 192 tai 256 bittiä. Sen vuoksi ISO 16844-3 -standardissa olevassa taulukossa 5 esitettyä datatavujen komentokohtaista lukumäärää muutetaan Taulukko 6 esitetyn mukaisesti.

Taulukko 6

Salaamattomien ja salattujen datatavujen komentokohtainen lukumäärä siten kuin ISO 16844-3 -standardissa on määritelty

Komento	Pyyntö/ vastaus	Tiedon kuvaus	Salaamattomien datatavujen lukumäärä ISO 16844-3 -standardin mukaan	Salaamattomien AES-avainta käyttävien datatavujen lukumäärä	Salattujen datatavujen lukumäärä, kun käytetään AES-avaimia, joiden pituus on		
					128 bittiä	192	256
10	pyyntö	Todentamistiedot + tiedostonumero	8	8	16	16	16
11	vastaus	Todentamistiedot + tiedoston sisältö	16 tai 32 riippuen tiedostosta	16 tai 32 riippuen tiedostosta	16 / 32	16 / 32	16 / 32
41	pyyntö	Liiketunnistimen sarjanumero	8	8	16	16	16
41	vastaus	Liittämisavain	16	16 / 24 / 32	16	32	32
42	pyyntö	Tilapäinen avain	16	16 / 24 / 32	16	32	32
43	pyyntö	Liittämistiedot	24	24	32	32	32
50	vastaus	Liittämistiedot	24	24	32	32	32
70	pyyntö	Todentamistiedot	8	8	16	16	16
80	vastaus	Liiketunnistimen laskurin arvo + todentamistiedot	8	8	16	16	16

CSM_219 Liittämistiedot, jotka lähetetään komennoissa 43 (ajoneuvoyksikön pyyntö) ja 50 (liiketunnistimen vastaus), on koottava siten kuin ISO 16844-3 -standardin 7.6.10 kohdassa on määritelty, lukuun ottamatta sitä, että liittämistietojen salauskaaviossa on käytettävä AES-algoritmia TDES-algoritmin sijaan, jolloin tuloksena on kaksi AES-salausta, ja CSM_220 alakohdassa määritelty täyttö on valittava siten, että se sopii AES-salauksen lohkokokoon. Salaukseen on käytettävä avainta K'_P, joka luodaan seuraavasti:

— jos liittämisavaimen K_P pituus on 16 tavua: $K'_P = K_P$ XOR $(N_s||N_s)$

▼B

— jos liittämisavaimen K_P pituus on 24 tavua: $K'_p = K_P$ XOR $(N_s||N_s||N_s)$

— jos liittämisavaimen K_P pituus on 32 tavua: $K'_p = K_P$ XOR $(N_s||N_s||N_s||N_s)$

missä N_s on liiketunnistimen 8-tavuinen sarjanumero.

CSM_220 Jos salaamattoman datan pituus (AES-avaimia käyttäen) ei ole 16 tavun kerrannainen, on käytettävä ISO 9797-1 -standardissa määriteltyä täyttömenetelmää 2.

Huomautus: ISO 16844-3 -standardissa salaamattomien datatavujen lukumäärä on aina kahdeksan kerrannainen, joten TDES-avaimia käytettäessä täyttö ei ole tarpeen. ISO 16844-3 -standardissa annettua datan ja sanomien määritelmää ei muuteta tämän lisäyksen tässä osassa, minkä vuoksi täyttö on välttämätöntä.

CSM_221 Komennossa 11 ja tilanteessa, jossa on salattava useampi kuin yksi datalohko, on käytettävä ISO 10116 -standardissa määriteltyä salauslohkoja ketjuttavaa käyttötilaa, missä limitysparametri $m = 1$. Alustusvektorin (IV) on oltava seuraavanlainen:

— Komennon 11 osalta: ISO 16844-3 -standardin 7.6.3.3 kohdassa määritelty 8-tavuinen todennuslohko, joka on täytetty käyttäen ISO 9797-1 -standardissa määriteltyä täyttömenetelmää 2; ks. myös ISO 16844-3 -standardin 7.6.5 ja 7.6.6 kohta.

— Kaikkien muiden komentojen osalta, kun siirretään yli 16 tavua, siten kuin Taulukko 6 on määritelty: ‘00’ {16} (ts. 16 tavua ja binaariarvo 0).

Huomautus: Kuten ISO 16844-3 -standardin 7.6.5 ja 7.6.6 kohdassa on esitetty, silloin kun liiketunnistin salaa tiedostoja komennon 11 sisällyttämistä varten,

— todennuslohkoa käytetään alustusvektorina, kun tiedostot salataan CBC-käyttötilassa

— todennuslohko salataan ja sisällytetään ensimmäisen lohkona dataan, joka lähetetään ajoneuvoyksikölle.

12.4. **Ajoneuvoyksikön ja liiketunnistimen liittäminen eri sukupolvien laitteissa**

CSM_222 Kuten edellä 9.2.1 kohdassa on selitetty, toisen sukupolven liiketunnistin voi sisältää liittämistietojen TDES-salauksen (joka on määritelty tämän lisäyksen osassa A), mikä mahdollistaa liiketunnistimen liittämisen ensimmäisen sukupolven ajoneuvoyksikköön. Tässä tapauksessa ensimmäisen sukupolven ajoneuvoyksikkö on liitettävä toisen sukupolven liiketunnistimeen siten kuin tämän lisäyksen osassa A ja ISO 16844-3 -standardissa on kuvattu. Liittämisprosessissa voidaan käyttää joko ensimmäisen tai toisen sukupolven korjaamokorttia.

Huomautuksia:

— Toisen sukupolven ajoneuvoyksikköä ei voida liittää ensimmäisen sukupolven liiketunnistimeen.

▼B

— Toisen sukupolven ajoneuvoyksikköä ei voida kytkeä liiketunnistimeen ensimmäisen sukupolven korjaamokortilla.

13. DSRC-TIEDONSIIRRON KAUTTA TAPAHTUVAN ETÄVIESTINNÄN TIETOTURVA

13.1. **Yleistä**

Kuten lisäyksessä 14 on määritelty, ajoneuvoyksikkö luo säännöllisesti ajopiirturin etäseurantatietoja (RTM, Remote Tachograph Monitoring) ja lähettää niitä sisäiseen tai ulkoiseen etäviestintälaitteistoon (RCF, Remote Communication Facility). Etäviestintälaitteisto vastaa näiden tietojen lähettämisestä etäkyselylaitteeseen lisäyksessä 14 kuvatun DSRC-rajapinnan kautta. Lisäyksessä 1 täsmennetään, että RTM-tiedot on ketjutettu seuraavista:

Salatut ajopiirturin hyötykuormatiedot salaamattomien ajopiirturin hyötykuormatietojen salaus

DSRC-tietoturvadata kuvataan jäljempänä

Salaamattomien ajopiirturin hyötykuormatietojen muoto määritellään lisäyksessä 1 ja kuvataan tarkemmin lisäyksessä 14. Tässä kohdassa kuvataan DSRC-tietoturvadatan rakennetta; muodollinen eritelmä annetaan lisäyksessä 1.

CSM_223 Salaamaton data `tachographPayload`, jonka ajoneuvoyksikkö lähettää etäviestintälaitteistoon (jos etäviestintälaitteisto ei ole ajoneuvoyksikön sisäinen laite) tai joka siirretään ajoneuvoyksiköstä etäkyselylaitteeseen DSRC-rajapinnan kautta (jos etäviestintälaitteisto on ajoneuvoyksikön sisäinen laite), on suojattava käyttötilassa, joka edellyttää salauksen ja sen jälkeen todennuksen (encrypt-then-authenticate mode), mikä tarkoittaa, että ajopiirturin hyötykuormatiedot salataan ensin sanoman luottamuksellisuuden varmistamiseksi, minkä jälkeen lasketaan MAC-koodi tietojen aitouden ja eheyden varmistamiseksi.

CSM_224 DSRC-tietoturvadatan on koostuttava seuraavien dataelementtien ketjutuksesta seuraavassa järjestyksessä; ks. myös kaavio 12:

Current date time	ajoneuvoyksikön kuluva päivämäärä ja aika (datatyyppi `TimeReal`)
Counter	3-tavuinen laskuri, ks. CSM_225 alakohta
VU serial number	ajoneuvoyksikön sarjanumero (datatyyppi `VuSerialNumber`)
DSRC master key version number	sen DSRC-pääavaimen yksitavuinen versionumero, jonka perusteella ajoneuvoyksikkökohtaiset DSRC-avaimet on luotu, ks. 9.2.2 kohta
MAC	MAC-koodi lasketaan kaikista RTM-tietojen edellisistä tavuista.

CSM_225 DSRC-tietoturvadatan kolmetavuisen laskurin on oltava MSB-first-muodossa. Kun ajoneuvoyksikkö laskee RTM-tiedot ensimmäisen kerran sen käyttöönoton jälkeen, sen on asetettava laskurin arvoksi 0. Ajoneuvoyksikön on lisättävä laskuridatan arvoa yhdellä aina ennen seuraavien RTM-tietojen laskemista.

▼B

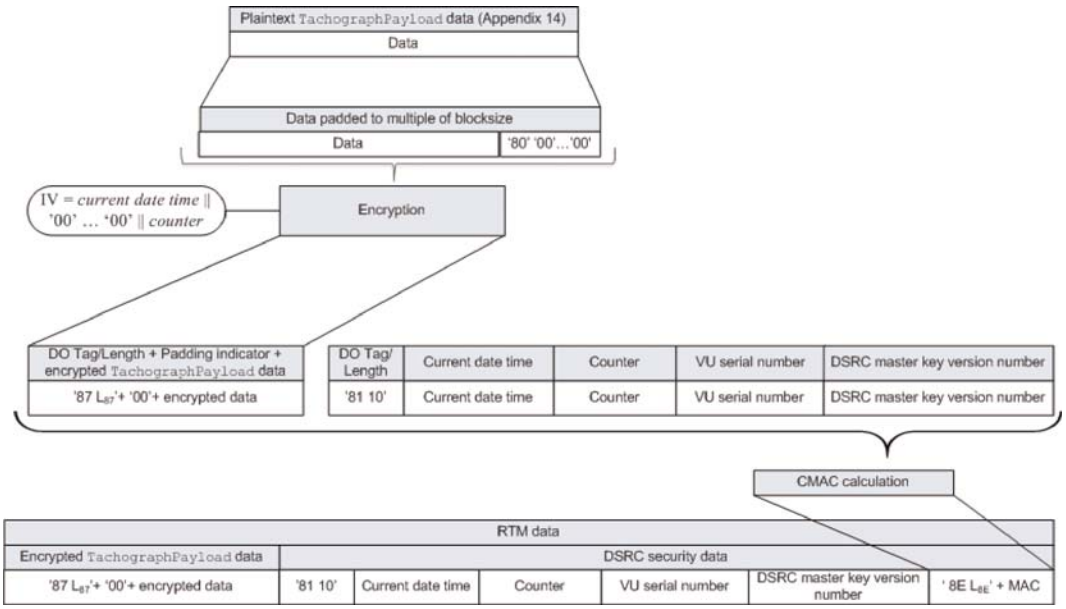
13.2. **Ajopiirturin hyötykuormatietojen salaus ja MAC-koodin luominen**

CSM_226 Kun ajoneuvoyksikkö vastaanottaa salaamattoman dataelementin, jonka datatyyppi on `TachographPayload`, kuten lisäyksessä 14 on kuvattu, sen on salattava nämä tiedot kaaviossa 12 esitetyllä tavalla: ajoneuvoyksikön DSRC-salausavainta $K_VU_{DSRC}_ENC$ (ks. 9.2.2 kohta) on käytettävä yhdessä AES-salauksen kanssa ISO 10116 -standardissa määritellyssä salauslohkoja ketjuttavassa käyttötilassa (CBC), missä limitysparametri $m = 1$. Alustusvektorin on oltava *IV = current date time* || '*00 00 00 00 00 00 00 00*' || *counter*, missä *current date time* ja *counter* määritellään CSM_224 alakohdassa. Salattavat tiedot on täytettävä ISO 9797-1 -standardissa määriteltyä täyttömenetelmää 2 käyttäen.

CSM_227 Ajoneuvoyksikön on laskettava MAC-koodi DSRC-tietoturvadatassa kaaviossa 12 esitetyllä tavalla: MAC-koodi lasketaan kaikista RTM-tietojen edellisistä tavuista DSRC-pääavaimen versionumeroon saakka, mukaan lukien kyseinen versionumero sekä dataobjektien tuntomerkit ja pituudet. Ajoneuvoyksikön on käytettävä DSRC-avaintaan avaimen $K_VU_{DSRC}_MAC$ (ks. 9.2.2 kohta) todentamiseen AES-algoritmin kanssa CMAC-käyttötilassa siten kuin viitteessä SP 800-38B on määritelty. MAC-koodin pituuden on oltava sidoksissa ajoneuvokohtaisten DSRC-avainten pituuteen, kuten CSM_50 alakohdassa on määritelty.

Kaavio 12

Ajopiirturin hyötykuormatietojen salaus ja MAC-koodin luominen



13.3. **Ajopiirturin hyötykuormatietojen todentaminen ja salauksen avaus**

CSM_228 Kun etäkyselylaite vastaanottaa ajoneuvoyksiköltä RTM-tietoja, sen on lähetettävä koko RTM-tietopaketti valvontakortille PROCESS DSRC MESSAGE -komennon datakenttään, kuten lisäyksessä 2 on kuvattu. Sen jälkeen:

▼B

1. Valvontakortin on tarkistettava DSRC-tietoturvadatassa oleva DSRC-pääavaimen versionumero. Jos valvontakortti ei tunne ilmoitettua DSRC-pääavainta, sen on lähetettävä takaisin lisäyksessä 2 määritelty virhe ja lopetettava prosessi.

2. Valvontakortin on luotava ilmoitetun DSRC-pääavaimen sekä DSRC-tietoturvadatassa olevan ajoneuvoyksikön sarjanumeron perusteella ajoneuvoyksikkökohtaiset DSRC-avaimet K_VU_{DSRC}_ENC ja K_VU_{DSRC}_MAC, kuten CSM_124 alakohdassa on määritelty.

3. Valvontakortin on käytettävä avainta K_VU_{DSRC}_MAC DSRC-tietoturvadatassa olevan MAC-koodin todentamiseen, kuten CSM_227 alakohdassa on määritelty. Jos MAC-koodi on virheellinen, valvontakortin on lähetettävä takaisin lisäyksessä 2 määritelty virhe ja lopetettava prosessi.

4. Valvontakortin on käytettävä avainta K_VU_{DSRC}_ENC salatun ajopiirturin hyötykuormatietojen salauksen avaamiseen, kuten CSM_226 alakohdassa on määritelty. Valvontakortin on poistettava täyttö ja lähetettävä etäkyselylaitteelle takaisin ajopiirturin hyötykuormatiedot, joiden salaus on avattu.

CSM_229 Toistohyökkäysten estämiseksi etäkyselylaitteen on todennettava RTM-tietojen tuoreus todentamalla, että *current date time* -arvo DSRC-tietoturvadatassa ei poikkea liikaa etäkyselylaitteen kuluvasta ajasta.

Huomautuksia:

— Tämä edellyttää, että etäkyselylaitteella on täsmällinen ja luotettava aikalähde.

— Koska lisäyksessä 14 edellytetään, että ajoneuvoyksikkö laskee uudet RTM-tiedot 60 sekunnin välein, ja ajoneuvoyksikön kello voi poiketa yhden minuutin todellisesta ajasta, RTM-tietojen tuoreuden alaraja on kaksi minuuttia. Vaadittu tietojen tuoreus riippuu myös etäkyselylaitteen kellon täsmällisyydestä.

CSM_230 Kun korjaamo todentaa ajoneuvoyksikön DSRC-tiedonsiirron asianmukaisen toiminnan, sen on lähetettävä ajoneuvoyksiköltä vastaanotettu koko RTM-tietopaketti korjaamokortille PROCESS DSRC MESSAGE -komennon datakenttään, kuten lisäyksessä 2 on kuvattu. Korjaamokortin on suoritettava kaikki CSM_228 alakohdassa mainitut tarkistukset ja toiminnot.

14. KOPIOITUJEN TIETOJEN ALLEKIRJOITTAMINEN JA ALLEKIRJOITUSTEN TODENTAMINEN

14.1. **Yleistä**

CSM_231 Tietojen kopioimiseen ulkoisille tietovälineille tarkoitettu älykäs laite (IDE-laite) tallentaa ajoneuvoyksiköltä tai kortilta yhden kopiointijakson aikana saadut tiedot yhteen fyysiseen tiedostoon. Tiedot voidaan tallentaa ulkoiselle tietovälineelle (ESM). Tiedosto sisältää datalohkojen digitaaliset allekirjoitukset siten kuin lisäyksessä 7 on määritelty. Tiedosto sisältää myös seuraavat varmenteet (ks. 9.1 kohta):

▼B

— Ajoneuvoyksikön tietojen kopiointi:

— VU_Sign-varmenne

— MSCA_VU-EGF-varmenne, joka sisältää VU_Sign-varmenteen todentamiseen käytettävän julkisen avaimen.

— Kortin tietojen kopiointi:

— Card_Sign-varmenne

— MSCA_Card-varmenne, joka sisältää Card_Sign-varmenteen todentamiseen käytettävän julkisen avaimen.

CSM_232 IDE-laitteen on saatava käyttöön seuraavat varmenteet:

— Jos IDE-laite käyttää valvontakorttia allekirjoituksen todentamiseen kaavion 13 mukaisesti, tarvittaessa linkkivarmenne, joka yhdistää viimeisimmän EUR-varmenteen siihen EUR-varmenteeseen, jonka voimassaoloaika edeltää sitä.

— Jos IDE-laite todentaa allekirjoituksen itse, sen on tuhottava kaikki voimassa olevat eurooppalaiset juurivarmenteet.

Huomautus: IDE-laitteen käyttämää menetelmää näiden varmenteiden palauttamiseksi ei käsitellä tässä lisäyksessä.

14.2. **Allekirjoituksen luominen**

CSM_233 Kopioitujen tietojen digitaalisten allekirjoitusten luomiseen on käytettävä viitteessä DSS määriteltyä ECDSA-allekirjoitusalgoritmia sekä ajoneuvoyksikön tai kortin avainkokoon sidoksissa olevaa hajautusalgoritmia, kuten CSM_50 alakohdassa on määritelty. Allekirjoituksen on oltava tekstimuodossa, kuten viitteessä TR-03111 on määritelty.

14.3. **Allekirjoituksen todentaminen**

CSM_234 IDE-laite voi todentaa kopioitujen tietojen allekirjoituksen itse tai käyttää tätä varten valvontakorttia. Jos IDE-laite käyttää valvontakorttia, allekirjoituksen todentaminen on suoritettava kaavion 13 mukaisesti. Jos IDE-laite todentaa allekirjoituksen itse, sen on todennettava kaikkien tiedoston varmenneketjun varmenteiden aitous ja voimassaoloaika, minkä lisäksi sen on todennettava tietojen allekirjoitus viitteessä DSS määriteltyä allekirjoituksen muodostamiskaaviota noudattaen.

Huomautuksia kaavioon 13:

— Analysoitavaa laitetta, joka allekirjoitti tiedot, kutsutaan lyhenteellä EQT.

— Kaaviossa mainittuja EQT-nimisiä varmenteita ja julkisia avaimia käytetään allekirjoittamiseen (ts. VU_Sign tai Card_Sign).

— Kaaviossa mainittuja EQT.CA-nimisiä varmenteita ja julkisia avaimia käytetään tarpeen mukaan ajoneuvoyksikön tai kortin varmenteiden allekirjoittamiseen.

— Kaaviossa mainittu EQT.CA.EUR-varmenne on eurooppalainen juurivarmenne, joka ilmoitetaan EQT.CA-varmenteen varmenneviranomaisen viitteessä (CAR).

▼B

— Kaaviossa mainittu EQT.Link-varmenne on mahdollinen laitteen linkkivarmenne. Kuten edellä 9.1.2 kohdassa on määritelty, tämä on uuden eurooppalaisen juuriavainparin linkkivarmenne, jonka ERCA on luonut ja allekirjoittanut edellisellä eurooppalaisella yksityisellä avaimella.

— EQT.Link.EUR-varmenne on eurooppalainen juurivarmenne, joka ilmoitetaan EQT.Link-varmenteen varmenneviranomaisen viitteessä (CAR).

CSM_235 Laskeakseen hash-tuloksen M, joka on lähetetty valvontakortille PSO:Hash-komennossa, IDE-laitteen on käytettävä sen ajoneuvoyksikön tai kortin avainkokoon sidoksissa olevaa hajautusalgoritmia, josta tiedot on kopioitu, kuten CSM_50 alakohdassa on määritelty.

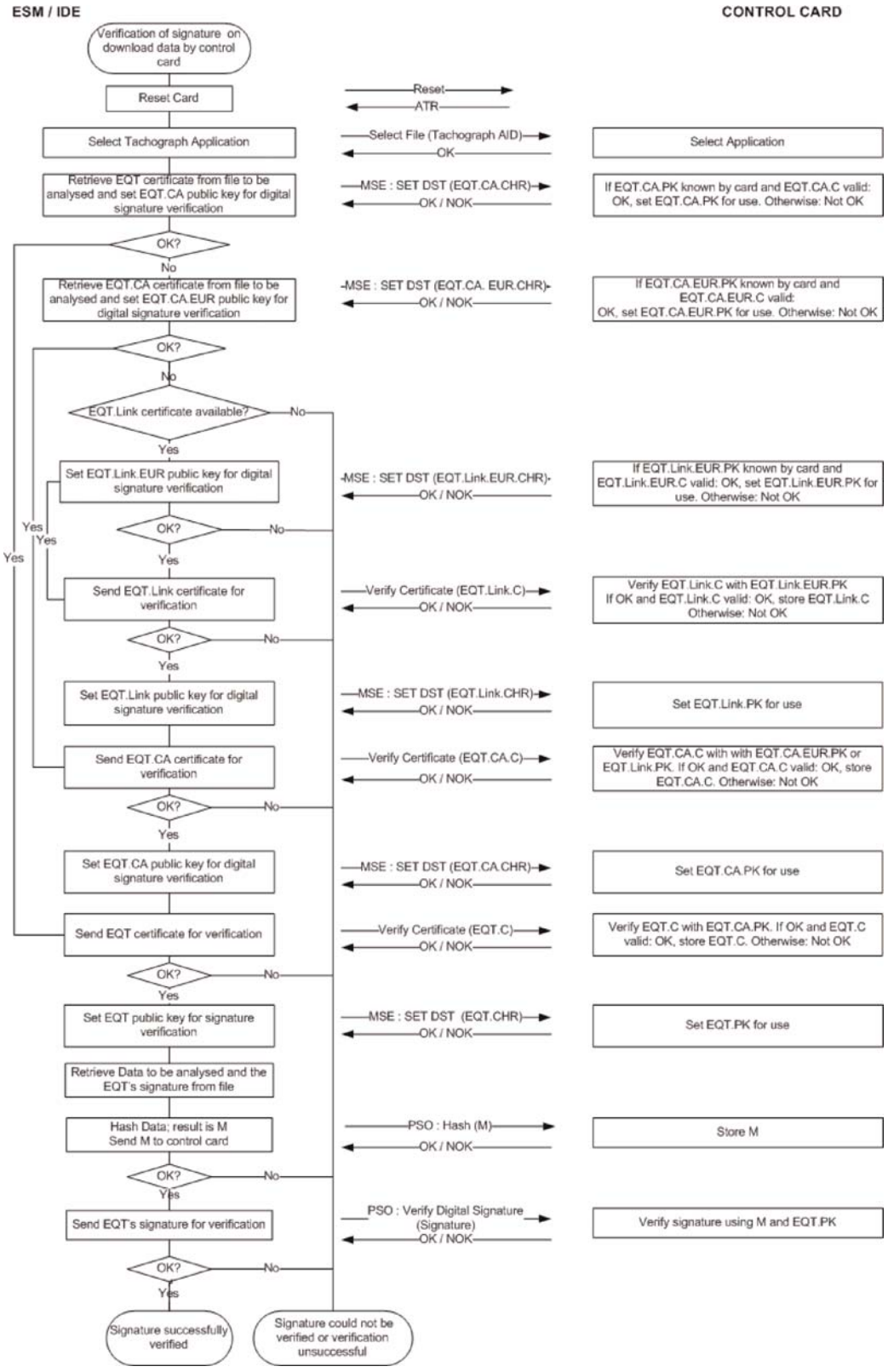
CSM_236 Laitteen allekirjoituksen todentamiseksi valvontakortin on noudatettava viitteessä DSS määriteltyä allekirjoituksen muodostamiskaaviota.

Huomautus: Tässä asiakirjassa ei määritellä suoritettavia toimintoja tilanteessa, jossa kopioitujen tietojen allekirjoitusta ei voida todentaa tai todennus epäonnistuu.

▼B

Kaavio 13

Kopioitujen tietojen allekirjoituksen todentamisprotokolla



▼B

Lisäys 12

MAAILMANLAAJUISEEN SATELLIITTINAVIGOINTIJÄRJESTELMÄÄN (GNSS) PERUSTUVA PAIKANTAMINEN

SISÄLLYSLUETTELO

1. JOHDANTO

1.1. Soveltamisala

1.2. Lyhenteet ja merkinnät

2. GNSS-VASTAANOTTIMEN ERITELMÄ

3. NMEA-LAUSEKKEET

4. AJONEUVOYKSIKKÖ, JOSSA ON ULKOINEN GNSS-LAITTEISTO

4.1. Kokoonpano

4.1.1 Pääasialliset osat ja rajapinnat

4.1.2 Ulkoisen GNSS-laitteiston tila toimintavaiheen päättyessä

4.2. Ulkoisen GNSS-laitteiston ja ajoneuvoyksikön välinen viestintä

4.2.1 Viestintäprotokolla

4.2.2 GNSS-tietojen suojattu välittäminen

4.2.3 Lue tietue -komennon rakenne

4.3. Ulkoisen GNSS-laitteiston kytkentä, molemminpuolinen todentaminen ja tilapäinen avaimesta sopiminen ajoneuvoyksikön kanssa

4.4. Virheenkäsittely

4.4.1 Virhe viestinnässä ulkoisen GNSS-laitteiston kanssa

4.4.2 Ulkoisen GNSS-laitteiston turvakomponentin fyysisen eheyden rikkominen

4.4.3 Sijaintitietojen puuttuminen GNSS-vastaanottimesta

4.4.4 Ulkoisen GNSS-laitteiston varmenteen voimassaoloajan päättyminen

5. AJONEUVOYKSIKKÖ ILMAN ULKOISTA GNSS-LAITTEISTOA

5.1. Kokoonpano

5.2. Virheenkäsittely

5.2.1 Sijaintitietojen puuttuminen GNSS-vastaanottimesta

6. GNSS-LAITTEISTON AIKOJEN PÄÄLLEKKÄISYYS -TAPAHTUMA

7. AJONEUVON LIIKERISTIRIITA

1. JOHDANTO

Tässä lisäyksessä annetaan teknisiä vaatimuksia ajoneuvoyksiköiden käyttämille GNSS-tiedoille, mukaan lukien menettelyt, joita on sovellettava paikannustietoja koskevan turvallisen ja virheettömän tiedonsiirron varmistamiseksi.

Näitä vaatimuksia koskevat asetuksen (EU) N:o 165/2014 pääasialliset artiklat ovat: ajoneuvon sijainnin kirjaamista tietyissä paikoissa vuorokautisen työjakson aikana koskeva 8 artikla, ITS-rajapintaa koskeva 10 artikla ja älykkäihin ajopiirtureihin liittyviä yksityiskohtaisia säännöksiä koskeva 11 artikla.

▼B

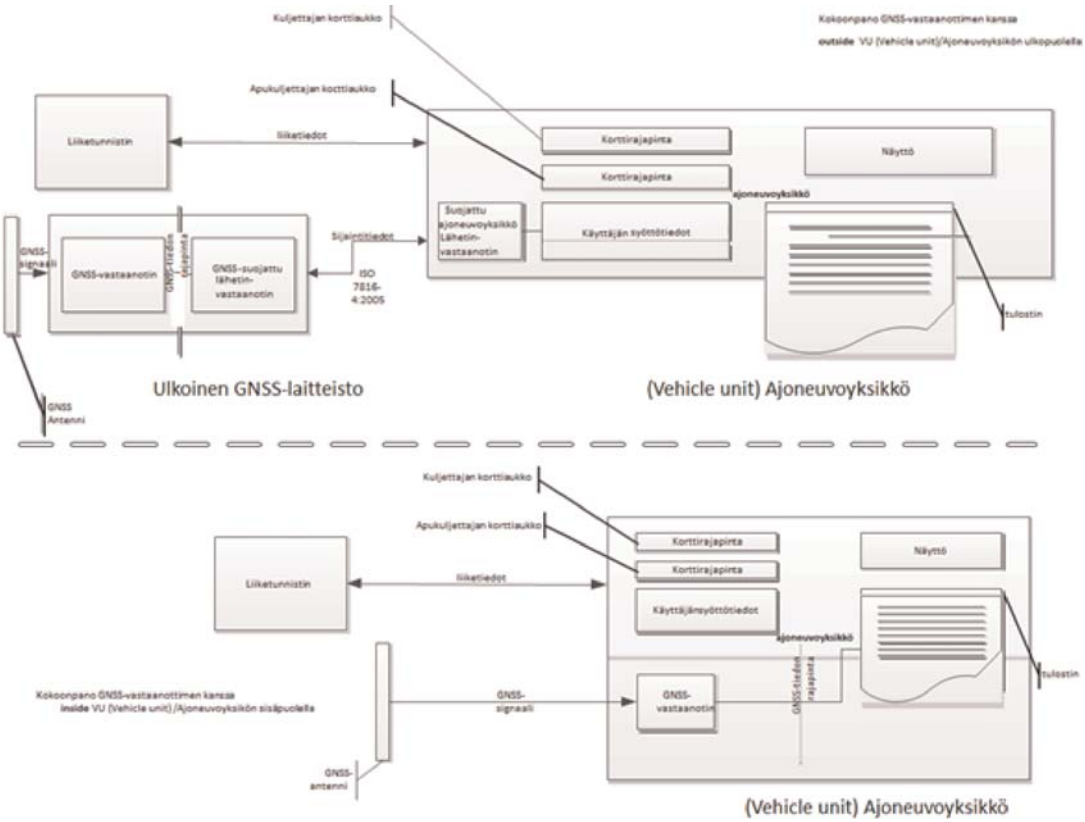
1.1. **Soveltamisala**

GNS_1 Ajoneuvoyksikön on kerättävä paikkatietoja ainakin yhdestä GNSS-järjestelmästä 8 artiklan täytäntöönpanon tukemiseksi.

Ajoneuvoyksikössä voi olla tai siitä voi puuttua ulkoinen GNSS-laitteisto, kuten kuvataan kuvassa 1:

Kuva 1

GNSS-vastaanottimen eri konfiguroinnit



1.2. **Lyhenteet ja merkinnät**

Tässä lisäyksessä käytetään seuraavia lyhenteitä:

DOP	(Dilution of Precision) Paikannuksen hyvyysluku (DOP-luku)
EGF	(Elementary File GNSS Facility) GNSS-laitteiston EF-tiedosto
EGNOS	(European Geostationary Navigation Overlay Service) Euroopan geostationaarinen navigointilisäjärjestelmä
GNSS	(Global Navigation Satellite System) Maailmanlaajuinen satelliittinavigointijärjestelmä
GSA	(GPS DOP and active satellites) GPS DOP-arvot ja aktiiviset satelliitit
HDOP	(Horizontal Dilution of Precision) Vaakasuuntainen paikannuksen hyvyysluku (HDOP-luku)
ICD	(Interface Control Document) Rajapinnan valvonta-asiakirja
NMEA	(National Marine Electronics Association) Kansallinen merielektroniikan yhdistys

▼B

PDOP (Position Dilution of Precision) 3D-paikannuksen hyvyysluku (PDOP-luku)

RMC (Recommended Minimum Specific) Suositeltu erityinen vähimmäismäärä

SIS (Signal in Space) Signaali avaruudessa

VDOP (Vertical Dilution of Precision) Korkeussuuntainen paikannuksen hyvyysluku (VDOP-luku)

VU (Vehicle unit) Ajoneuvoyksikkö

2. GNSS-VASTAANOTTIMEN ERITELMÄ

Riippumatta siitä, kuuluuko älykkään ajopiirturin kokoonpanoon ulkoinen GNSS-laitteisto, älykkään ajopiirturin tehokas toiminta edellyttää suojattujen ja luotettavien paikannustietojen tarjontaa. Sen vuoksi on aiheellista edellyttää, että se on yhteensopiva Galileo- ja EGNOS (European Geostationary Navigation Overlay Service) -ohjelmien tarjoamien palveluiden kanssa Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1285/2013 ([1]) mukaisesti. Galileo-ohjelman mukaisesti perustettu järjestelmä on riippumaton maailmanlaajuinen satelliittinavigointijärjestelmä ja EGNOS-ohjelman mukaisesti perustettu järjestelmä on alueellinen satelliittinavigointijärjestelmä, jolla parannetaan maailmanlaajuisen paikannusjärjestelmän (GPS) signaalin laatua.

GNS_2 Valmistajien on varmistettava, että älykkäiden ajopiirtureiden GNSS-vastaanottimet sopivat yhteen Galileo- ja EGNOS-järjestelmien tarjoamien paikannuspalveluiden kanssa. Valmistajat voivat lisäksi valita, että ne sopivat yhteen muiden satelliittinavigointijärjestelmien kanssa.

GNS_3 GNSS-vastaanottimen on voitava tukea Galileon avoimen palvelun todentamistoimintoja, kun Galileo-järjestelmä tarjoaa tällaisen palvelun ja kun GNSS-vastaanottimen valmistajat tukevat tätä. Jälkiasennusta ei kuitenkaan vaadita, kun on kyse älykkäistä ajopiirtureista, jotka on saatettu markkinoille ennen edellä tarkoitettujen edellytysten täyttymistä ja jotka eivät voi tukea Galileon avoimen palvelun todentamistoimintoja.

3. NMEA-LAUSEKKEET

Tässä kohdassa kuvataan älykkäiden ajopiirtureiden toiminnassa käytettäviä NMEA-standardin lausekkeita. Tämä kohta koskee älykkään ajopiirturin kokoonpanoa joko ulkoisen GNSS-laitteiston kanssa tai ilman sitä.

GNS_4 Paikannustiedot perustuvat NMEA-lausekkeeseen GNSS-tietojen suositellusta erityisestä vähimmäismäärästä (Recommended Minimum Specific GNSS Data), johon sisältyvät sijaintitiedot (leveys- ja pituusaste), aika UTC-muodossa (hhmmss.ss) ja nopeus maan päällä solmuissa sekä täydentävät arvot.

RMC-lausekkeen muoto on seuraava (kuten NMEA V4.1 -standardi):

([1]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 1285/2013, annettu 11 päivänä joulukuuta 2013, Euroopan satelliittinavigointijärjestelmien toteuttamisesta ja käytöstä sekä neuvoston asetuksen (EY) N:o 876/2002 ja Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 683/2008 kumoamisesta (EUVL L 347, 20.12.2013, s. 1).

▼B

Kuva 2

RMC-lausekkeen rakenne



1) Time (UTC)
2) Status, A = Valid position, V = Warning
3) Latitude
4) N or S
5) Longitude
6) E or W
7) Speed over ground in knots
8) Track made good, degrees true
9) Date, ddmmyy
10) Magnetic Variation, degrees
11) E or W
12) Checksum

Tila ilmoittaa, jos GNSS-signaali on saatavilla. Siihen saakka kun tilan arvoksi ei ole asetettu A, vastaanotettuja tietoja (esim. ajasta tai pituus-/leveysasteesta) ei voida käyttää ajoneuvon sijainnin kirjaamiseksi ajoneuvoyksikössä.

Sijainnin tarkkuus perustuu edellä mainittuun RMC-lausekkeen muotoon. Kentän 3 ja 5 ensimmäistä osaa (ensimmäiset kaksi numeroa) käytetään asteiden osoittamiseen. Muita käytetään osoittamaan minuutteja kolmen desimaalin tarkkuudella. Tarkkuus on siis 1/1 000 minuuttia tai 1/60 000 astetta (koska minuutti on 1/60 asteesta).

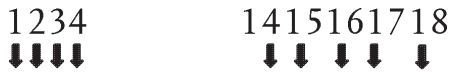
GNS_5 Ajoneuvoyksikön on säilytettävä ajoneuvoyksikön tietokannassa sijaintitiedot pituus- ja leveysasteista tarkkuudella 1/10 minuuttia tai 1/600 astetta, kuten kuvataan lisäyksessä 1 tyypin GeoCoordinates-paikkatiedoista.

Ajoneuvoyksikkö voi käyttää GPS DOP ja aktiiviset satelliitit (GSM-järjestelmäalue) -komentoa määrittämään ja kirjaamaan signaalin saatavuus ja tarkkuus. Erityisesti HDOP-lukua käytetään osoittamaan kirjatun sijaintitiedon tarkkuuden taso (ks. 4.2.2. kohta). Ajoneuvoyksikkö tallentaa vaakasuuntainen paikannuksen hyvyysluvun (HDOP-luku), joka lasketaan käytössä olevilla GNSS-järjestelmillä kerättyjen HDOP-lukujen minimistä.

GNSS System Id osoittaa, onko kyse GPS-, Glonass-, Galileo- tai Beidou-järjestelmästä tai satelliitteihin perustuvasta lisäjärjestelmästä (SBAS).

Kuva 3

GSA-lausekkeen rakenne



1) Valintatila
2) Tila
3) Sijainnin löytämiseen käytetyn ensimmäisen satelliitin ID
4) Sijainnin löytämiseen käytetyn toisen satelliitin ID

[...]

14) Sijainnin löytämiseen käytetyn 12. satelliitin ID
15) PDOP-luku metreissä
16) HDOP-luku metreissä
17) VDOP-luku metreissä
18) GNSS System Id
19) Tarkistussumma

▼B

Jossa tila (2) osoittaa, että sijainnin löytäminen ei ole käytettävissä (tila=1) tai sijainnin löytäminen on saatavilla 2D-paikannuksessa (tila=2) tai 3D-paikannuksessa (tila=3).

GNS_6 *GSA*-lauseke tallennetaan tietuenumerolla ‘06’.

GNS_7 NMEA-lausekkeiden (esim. RMC-, GSA- tai muut lausekkeet) maksimikoko, jota voidaan käyttää lukukomennon mitoitukseen, on 85 tavua (ks. taulukko 1).

4. AJONEUVOYKSIKKÖ, JOSSA ON ULKOINEN GNSS-LAITTEISTO

4.1. **Kokoonpano**

4.1.1 *Pääasialliset osat ja rajapinnat*

Tässä kokoonpanossa GNSS-vastaanotin on osa ulkoista GNSS-laitteistoa.

GNS_8 Ulkoisen GNSS-laitteiston on saatava virtansa erityisellä ajoneuvon rajapinnalla.

GNS_9 Ulkoisen GNSS-laitteiston on muodostuttava seuraavista osista (ks. kuva 4):

a) Kaupallisesta GNSS-vastaanottimesta, jolla tarjotaan sijaintitietoja GNSS-dataliitännän kautta. Esimerkiksi GNSS-dataliitäntä voi olla NMEA-standardi V4.10, jossa GNSS-vastaanotin toimii talker-laitteena ja se välittää NMEA-lausekkeet suojattuun GNSS-lähettimeen/vastaanottimeen, joka toimii 1 Hz taajuudella ennalta määritellylle NMEA-lausekkeiden sarjalle, johon on sisällyttävä ainakin RMC- ja GSA-lausekkeet. GNSS-dataliitännän soveltaminen on ulkoisen GNSS-laitteiston valmistajien valittavissa.

b) Lähetin/vastaanotinyksikkö (suojattu GNSS-lähetin/vastaanotin), joka pystyy tukemaan standardia ISO/IEC 7816-4:2013 (ks. 4.2.1 kohta) viestintään ajoneuvoyksikön kanssa sekä tukemaan GNSS-dataliitäntää GNSS-vastaanottimeen. Yksikkö on varustettu muistilla, joka tallentaa GNSS-vastaanottimen ja ulkoisen GNSS-laitteiston tunnistetiedot.

c) Suljettu järjestelmä, jossa on laitteiston havainnointiin kajoamiseen tarkoitettu toiminto, ja johon sisältyy sekä GNSS-vastaanotin että suojattu GNSS-lähetin/vastaanotin. Laitteiston havainnointiin kajoamiseen tarkoitettu toiminto käyttää tietoturvatoimenpiteitä, joita edellytetään älykkään ajopiirturin suojausprofiilissa.

d) Ajoneuvoon asennettu GNSS-antenni, joka on yhdistetty GNSS-vastaanottimeen kotelojärjestelmän kautta

GNS_10 Ulkoisella GNSS-laitteistolla on ainakin seuraavat ulkoiset rajapinnat:

a) rajapinta GNSS-antenniin, joka on asennettu ajoneuvon mastoon, jos käytetään ulkoista antennia

b) rajapinta ajoneuvoyksikköön.

GNS_11 Ajoneuvoyksikössä sen suojattu lähetin/vastaanotin on suojatun GNSS-lähettimen/vastaanottimen suojatun yhteyden toinen pää ja sen on tuettava standardia ISO/IEC 7816-4:2013, kun kyse on liitännästä ulkoiseen GNSS-laitteistoon.

▼B

GNS_12 Ajoneuvoyksikön on tuettava viestinnän fyysiseen siirtoon ulkoisen GNSS-laitteiston kanssa standardia ISO/IEC 7816-12:2005 tai muuta standardia, joka voi tukea standardia ISO/IEC 7816-4:2013. (ks. 4.2.1 kohta).

4.1.2 *Ulkoisen GNSS-laitteiston tila toimintavaiheen päättyessä*

GNS_13 Ulkoisen GNSS-laitteiston on tallennettava seuraavat arvot suojatun GNSS-lähettimen/vastaanottimen pysyvään muistiin, kun sen toimintavaihe päättyy:

— EGF_MA-avainpari ja vastaava varmenne

— MSCA_VU-EGF-varmenne, joka sisältää EGF_MA-varmenteen todentamiseen käytettävän julkisen avaimen MSCA_VU-EGF.PK

— EUR-varmenne, joka sisältää MSCA_VU-EGF-varmenteen todentamiseen käytettävän julkisen avaimen EUR.PK

— EUR-varmenne, jonka voimassaoloaika edeltää MSCA_VU-EGF-varmenteen todentamiseen käytettävän EUR-varmenteen voimassaoloaikaa (jos sellainen on)

— näiden kahden EUR-varmenteen yhdistävä linkkivarmenne (jos sellainen on)

— ulkoisen GNSS-laitteiston sarjanumero pitkässä muodossa

— GNSS-laitteiston käyttöjärjestelmän tunniste

— ulkoisen GNSS-laitteiston tyyppihyväksyntänumero

— ulkoisen GNSS-moduulin turvakomponentin tunniste.

4.2. **Ulkoisen GNSS-laitteiston ja ajoneuvoyksikön välinen viestintä**

4.2.1 *Viestintäprotokolla*

GNS_14 Ulkoisen GNSS-laitteiston ja ajoneuvoyksikön välisen viestintäprotokollan on tuettava kolmea tehtävää:

1. GNSS-tietojen kerääminen ja jakelu (esim. sijainti, ajoitus, nopeus),

2. Ulkoisen GNSS-laitteiston konfiguraatiotietojen kerääminen,

3. Hallintaprotokolla, jolla tuetaan ulkoisen GNSS-laitteiston ja ajoneuvoyksikön välistä kytkentää, molemminpuolista todentamista ja tilapäistä avaimesta sopimista.

GNS_15 Viestintäprotokolla perustuu standardiin ISO/IEC 7816-4:2013, jossa ajoneuvoyksikön suojattu lähetin/vastaanotin on isäntä ja suojattu GNSS-lähetin/vastaanotin renki. Ulkoisen GNSS-laitteiston ja ajoneuvoyksikön välinen fyysinen liitäntä perustuu standardiin ISO/IEC 7816-12:2005 tai muuhun standardiin joka voi tukea standardia ISO/IEC 7816-4:2013.

▼B

GNS_16 Viestintäprotokollassa ei tueta laajennettuja pituuskenttiä.

GNS_17 ISO 7816 -standardin viestintäprotokollaksi (sekä *-4:2013 että *-12:2005) ulkoisen GNSS-laitteiston ja ajoneuvoyksikön välillä asetetaan T=1.

GNS_18 Kun kyse on toiminnoista 1) GNSS-tietojen kerääminen ja jakelu ja 2) ulkoisen GNSS-laitteiston konfiguraatiotietojen kerääminen sekä 3) hallintaprotokolla, suojattu GNSS lähetin/vastaanotin simuloi älykorttia tiedostojärjestelmärakenteella, joka koostuu MF-tiedostosta, DF-tiedostosta ja sovellustunnisteesta, joka määritetään lisäyksen 1 6.2 kappaleessa (‘FF 44 54 45 47 4D’) sekä kolmesta perustiedostosta, jotka sisältävät varmenteet ja yhdestä perustiedostosta (EF.EGF), jonka tiedostotunniste on ‘2F2F’, kuten kuvataan taulukossa 1.

GNS_19 Suojatun GNSS-lähettimen/vastaanottimen on tallennettava GNSS-vastaanottimesta tulevat tiedot ja EF-EGF-tiedoston konfigurointi. Tämä on lineaarinen, vaihtuvamittainen tiedosto, jonka tunniste vastaa arvoa ‘2F2F’ heksadesimaalimuodossa.

GNS_20 Suojatun GNSS-lähettimen/vastaanottimen on käytettävä datan tallentamiseen muistia, joka voi suorittaa vähintään 20 miljoonaa tietojen kirjoittamisen ja lukemisen sykliä. Tämän näkökohdan lisäksi suojatun GNSS-lähettimen/vastaanottimen sisäisestä suunnittelusta ja toteutuksesta vastaavat maahantuojat.

Tietueiden numeroiden ja datan kartoitus esitetään taulukossa 1. Huom: neljälle satelliittijärjestelmälle ja satelliitteihin perustuvalle lisäjärjestelmälle on olemassa neljä GSA-lauseketta.

GNS_21 Tiedostorakenne esitetään taulukossa 1. Lisätietoja käyttöedellytyksistä (ALW, NEV, SM-MAC), ks. lisäys 2 3.5 kohta.

Taulukko 1

▼C2

Tiedostorakenne

		Luoton käytön edellytykset		
Tiedosto	Tiedoston tunniste	Lue	Päivitä	Salattu
MF	3F00			
EF.ICC	0002	ALW	NEV (by VU)	Ei
DF GNSS Facility	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 (by VU)	Ei

▼C2

Tiedosto/Dataelementti	Tiedostonumero	Koko (tavua)		Oletusarvot
		Min.	Maks.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS Facility		*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:n RMC-lauseke	”01”	85	85	
NMEA:n GSA-lauseke 1	”02”	85	85	
NMEA:n GSA-lauseke 2	”03”	85	85	
NMEA:n GSA-lauseke 3	”04”	85	85	
NMEA:n GSA-lauseke 4	”05”	85	85	
NMEA:n GSA-lauseke 5	”06”	85	85	
Ulkoisen GNSS-laitteiston sarjanumero pitkässä muodossa, jonka määritelmä lisäyksessä 1 on SensorGNSSSerialNumber.	”07”	8	8	
GNSS-lähettimen/vastaanottimen käyttöjärjestelmän tunniste, jonka määritelmä lisäyksessä 1 on SensorOSIdentifier.	”08”	2	2	
Ulkoisen GNSS-laitteiston tyyppihyväksyntänumero, jonka määritelmä lisäyksessä 1 on SensorExternalGNSSApprovalNumber.	”09”	16	16	
Ulkoisen GNSS-laitteiston turvakomponentin tunniste, jonka määritelmä lisäyksessä 1 on SensorExternalGNSSSCIdentifier.	”10”	8	8	
RFU (Reserved for Future Use) Varattu myöhempään käyttöön	”11”–”FD”			

▼B

4.2.2 *GNSS-tietojen suojattu välittäminen*

GNS_22 GNSS-sijaintitietojen suojattu välittäminen sallitaan ainoastaan seuraavissa olosuhteissa:

1. Kytkemisprosessi on saatettu päätökseen lisäyksessä 11 kuvatulla tavalla. Yhteiset turvamekanismit.

▼B

2. Määräajoin tehtävä molemminpuolinen todentaminen ja tilapäisestä avaimesta sopiminen ajoneuvoyksikön ja GNSS-laitteiston välillä kuvataan myös lisäyksessä 11. Yhteiset turvamekanismit on pantu täytäntöön ilmoitetulla tiheydellä.

GNS_23 Jokaisena sekuntina T (jossa T on pienempi tai yhtä suuri arvo kuin 10), ellei suoriteta kytkentää tai molemminpuolista todentamista ja tilapäisestä avaimesta sopimista, ajoneuvoyksikkö hakee ulkoisesta GNSS-laitteistosta sijaintitiedot seuraavan datavirran perusteella:

1. Ajoneuvoyksikkö hakee sijaintitiedot ulkoisesta GNSS-laitteistoista yhdessä paikannuksen hyvyyslukujen kanssa (GSA NMEA -lausekkeesta). Suojattu ajoneuvoyksikön lähetin/vastaanotin käyttää ISO/IEC 7816-4:2013 SELECT ja READ RECORD(S) -komentoja salatun sanomanvälityksen todentamisen vaativassa käyttötilassa (authentication-only mode), kuten tämä kuvataan lisäyksessä 11 olevassa 11.5 kappaleessa, ja tiedoston tunniste on ”2F2F” sekä RECORD-numero (tietuenumero) on ”01” RMC NMEA -lausekkeen ja ‘02’,‘03’,‘04’,‘05’,‘06’ GSA NMEA -lausekkeen osalta.

2. Viimeisin vastaanotettu sijaintitieto tallennetaan EF-tiedostoon yhdessä tunnisteen ‘2F2F’ ja taulukossa 1 kuvattujen tietueiden kanssa suojattuun GNSS-lähettimeen/vastaanottimeen, kun suojattu GNSS-lähetin/vastaanotin ottaa vastaan NMEA-tietoja vähintään 1 Hz taajuudella GNSS-vastaanottimesta GNSS-dataliitännän kautta.

3. Suojattu GNSS-lähetin/vastaanotin lähettää vastauksen ajoneuvoyksikön suojattuun lähettimeen/vastaanottimeen käyttämällä tietoyksikön vastausviestiä salatulla sanomanvälityksellä todentamisen vaativassa käyttötilassa, kuten lisäyksessä 11 olevassa 11.5 kohdassa kuvataan.

4. Ajoneuvoyksikön suojattu lähetin/vastaanotin tarkistaa saadun vastuksen aitouden ja eheyden. Jos saadaan positiivinen tulos, sijaintitiedot siirretään ajoneuvoyksikön prosessoriin GNSS-dataliitännän kautta.

5. Ajoneuvoyksikön prosessori tarkistaa vastaanotetun datan ja ottaa talteen tiedot (esim. leveysaste, pituusaste, aika) RMC NMEA -lausekkeesta. RMC NMEA -lauseke sisältää tiedot siitä, ovatko sijaintitiedot voimassa. Jos ne eivät ole voimassa, paikkatietoja ei ole vielä saatavilla ja sitä ei voida käyttää tallentamaan ajoneuvon sijaintia. Jos ne ovat voimassa, ajoneuvoyksikön prosessori ottaa talteen HDOP-arvot GSA NMEA -lausekkeista ja laskee keskiarvon käytettävissä olevista satelliittijärjestelmistä (kun sijainnin löytämistoiminto on käytettävissä).

6. Ajoneuvoyksikön prosessori tallentaa vastaanotetut ja käsitellyt tiedot, kuten ajoneuvoyksikköön liittyvän leveys- ja pituusasteen, ajan ja nopeuden muodossa, joka määritetään lisäyksen 1 tietohakemistossa GeoCoordinates-paikkatiedoiksi yhdessä HDOP-arvon kanssa, joka lasketaan käytettävissä olevista GNSS-järjestelmistä kerätyistä HDOP-vähimmäisarvoista.

▼B

4.2.3 *Lue tietue -komennon rakenne*

Tässä kohdassa kuvataan yksityiskohtaisesti lue tietue -komennon (Read Record) rakennetta. Salattu sanomanvälitys (todentamisen vaativassa käyttötilassa) lisätään, kuten lisäyksessä 11 (Yhteiset turvamekanismit) kuvataan.

GNS_24 Komento tukee salattua sanomanvälitystä todentamisen vaativassa käyttötilassa, ks. lisäys 11.

GNS_25 Komentoviesti

Tavu	Pituus	Arvo	Kuvaus
CLA (komennon luokan ilmaiseva tavu)	1	‘0Ch’	Salattua sanomanvälitystä pyydetään
INS (käskytavu)	1	‘B2h’	Lue tietue
P1	1	‘XXh’	Tietuenumero (‘00’ viittaa nykyiseen tietueeseen)
P2	1	‘04h’	Lue tietue, kun tietuenumeroksi on ilmoitettu P1
Le	1	‘XXh’	Vastauksena odotettavan datan pituus. Luettavien tavujen määrä.

GNS_26 Tietueesta, jonka viittauksena on P1, tulee nykyinen tietue.

Tavu	Pituus	Arvo	Kuvaus
#1-#X	X	‘XX..XXh’	Tiedot luettu
SW	2	‘XXXXh’	Tilaa osoittavat tavut (SW1,SW2)

— Jos komennon suorittaminen onnistui, suojattu GNSS-lähetin/vastaanotin vastaa ‘**9000**’.

— Jos käytettävä tiedosto ei ole tietuepohjainen, suojattu GNSS-lähetin/vastaanotin vastaa ‘**6981**’.

— Jos komentoa käytetään yhdessä tietuenumero P1 = ‘00’ kanssa, mutta käytössä ei ole EF-tiedostoa, suojattu GNSS-lähetin/vastaanotin vastaa ‘**6986**’ (komento ei ole sallittu).

— Jos tietuetta ei löydy, suojattu GNSS-lähetin/vastaanotin vastaa ‘**6A 83**’.

— Jos ulkoinen GNSS-laitteisto havannoi, että laitteeseen on kajottu, se vastaa ‘**66 90**’.

GNS_27 Suojattu GNSS-lähetin/vastaanotin tukee seuraavia ajopiirturin sukupolven 2 komentoja, jotka eritellään lisäyksessä 2:

Komento	Viite
Select	Lisäys 2 kohta 3.5.1
Read Binary	Lisäys 2 kohta 3.5.2
Get Challenge	Lisäys 2 kohta 3.5.4
PSO: Verify Certificate	Lisäys 2 kohta 3.5.7
External Authenticate	Lisäys 2 kohta 3.5.9
General Authenticate	Lisäys 2 kohta 3.5.10
MSE:SET	Lisäys 2 kohta 3.5.11

▼B

4.3. **Ulkoisen GNSS-laitteiston kytkentä, molemminpuolinen todentaminen ja tilapäinen avaimesta sopiminen ajoneuvoyksikön kanssa**

Ulkoisen GNSS-laitteiston kytkentää, molemminpuolista todentamista ja tilapäistä avaimesta sopimista ajoneuvoyksikön kanssa kuvataan lisäyksessä 11. Yhteiset turvamekanismit, 11 kappale.

4.4. **Virheenkäsittely**

Tässä kohdassa kuvataan, miten ajoneuvoyksikkö vastaa ulkoisen GNSS-laitteiston mahdollisiin virhetilanteisiin ja tallentaa ne.

4.4.1 *Virhe viestinnässä ulkoisen GNSS-laitteiston kanssa*

GNS_28 Jos ajoneuvoyksikkö ei pysty viestimään siihen kytketyn ulkoisen GNSS-laitteiston kanssa yli 20 peräkkäisen minuutin ajan, ajoneuvoyksikkö luo ja kirjaa tapahtuman tyyppiä EventFaultType, ja enum-arvoksi asetetaan ‘53’H *Ulkoisen GNSS-laitteiston viestintävika* ja aikaleimaksi kuluva aika. Tapahtuma luodaan ainoastaan, jos seuraavat kaksi edellytystä täytetään: a) älykäs ajopiirturi ei ole kalibrointitilassa ja b) ajoneuvo on liikkeessä. Tässä yhteydessä virhe viestinnässä syntyy, kun ajoneuvoyksikön suojattu lähetin/vastaanottaja ei saa vastausviestiä pyynnön sisältävän viestin jälkeen, kuten 4.2 kohdassa kuvataan.

4.4.2 *Ulkoisen GNSS-laitteiston turvakomponentin fyysisen eheyden rikkominen*

GNS_29 Jos ulkoinen GNSS-laitteisto on rikottu, suojattu GNSS-lähetin/vastaanotin poistaa kaiken sen muistin, myös salatun materiaalin. Kuten GNS_25:n ja GNS_26:n osalta kuvataan, ajoneuvoyksikkö havaitsee siihen kajoamisen, jos vastauksen tila on ‘6690’. Ajoneuvoyksikkö luo silloin tapahtuman tyyppiä EventFaultType ja enum-arvo on *‘55’H GNSS-laitteiston havainnointiin kajoaminen*.

4.4.3 *Sijaintitietojen puuttuminen GNSS-vastaanottimesta*

GNS_30 Jos suojattu GNSS-lähetin/vastaanotin ei saa dataa GNSS-vastaanottimesta yli kolmen peräkkäisen tunnin ajan, suojattu GNSS-lähetin/vastaanotin luo vastausviestin READ RECORD (lue tietue) -käskylle, RECORD-numero (tietuenumero) on ‘01’ ja 12 tavun tietokenttä asetetaan arvoon 0xFF. Saatuaan tämän vastausviestin, jonka tietokentällä on tämä arvo, ajoneuvoyksikkö luo ja tallentaa tapahtuman tyyppiä EventFaultType, enum-arvo ‘52’H *ulkoisen GNSS-vastaanottimen vika*, jolloin aikaleima vastaa nykyistä ajan arvoa ainoastaan, jos seuraavat kaksi ehtoa täytetään: a) älykäs ajopiirturi ei ole kalibrointitilassa ja b) ajoneuvo on liikkeessä.

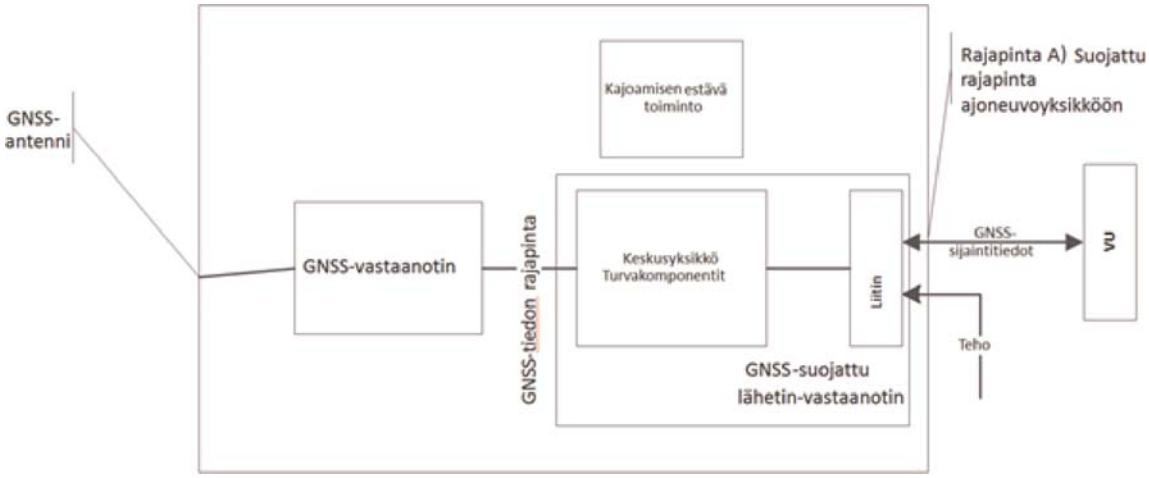
4.4.4 *Ulkoisen GNSS-laitteiston varmenteen voimassaoloajan päättyminen*

GNS_31 Jos ajoneuvoyksikkö havaitsee, että molemminpuolista todentamista varten käytetty EGF-varmenne ei ole enää voimassa, ajoneuvoyksikkö luo ja tallentaa tallennuslaitteiston vian tyyppiä typeEventFaultType ja enum-arvo on *‘56’H Ulkoisen GNSS-laitteiston varmenteen voimassaoloajan päättyminen*, jonka aikaleima vastaa nykyistä ajan arvoa. Ajoneuvo käyttää silti edelleen vastaanotettuja GNSS-sijaintitietoja.

▼B

Kuva 4

Kaavio ulkoisesta GNSS-laitteistosta



5. AJONEUVOYKSIKKÖ ILMAN ULKOISTA GNSS-LAITTEISTOA

5.1. **Kokoonpano**

Tässä kokoonpanossa GNSS-vastaanotin on ajoneuvoyksikön sisäpuolella, kuten kuvassa 1 esitetään.

GNS_32 GNSS-vastaanotin toimii talker-laitteena ja välittää NMEA-lausekkeet ajoneuvoyksikön prosessiin, joka toimii listener-laitteena ja jonka taajuus on 1/10 Hz tai nopeampi edeltä määritellyille NMEA-lausekkeiden sarjalle, johon on sisällyttävä ainakin RMC- ja GSA-lausekkeet.

GNS_33 Ulkoinen GNSS-antenni asennetaan ajoneuvoon tai sisäinen GNSS-antenni liitetään ajoneuvoyksikköön.

5.2. **Virheenkäsittely**

5.2.1 *Sijaintitietojen puuttuminen GNSS-vastaanottimesta*

GNS_34 Jos ajoneuvoyksikkö ei saa dataa GNSS-vastaanottimesta yli kolmen peräkkäisen tunnin ajan, ajoneuvoyksikkö luo ja tallentaa tapahtuman tyyppiä EventFaultType, enum-arvo ‘51’H *ulkoisen GNSS-vastaanottimen vika*, jolloin aikaleima vastaa nykyistä ajan arvoa ainoastaan, jos seuraavat kaksi ehtoa täytetään: a) älykäs ajopiirturi ei ole kalibrointitilassa ja b) ajoneuvo on liikkeessä.

6. GNSS-LAITTEISTON AIKOJEN PÄÄLLEKKÄISYYS -TAPAHTUMA

Jos ajoneuvoyksikkö havaitsee yli minuutin kestoisen poikkeaman ajoneuvoyksikön ajanmittaustoiminnon ja GNSS-vastaanottimesta peräisin olevan ajan välillä, ajoneuvoyksikkö luo ja tallentaa tapahtuman tyyppiä EventFaultType, enum-arvo *‘0B’H Aikojen päällekkäisyys (GNSS-laitteiston/ajoneuvoyksikön sisäinen kello)*. Tämä tapahtuma tallennetaan yhdessä ajoneuvoyksikön sisäisen kellon arvon kanssa ja yhdessä automaattisen ajansäädön kanssa. Kun aikojen päällekkäisyys -tapahtuma on syntynyt, ajoneuvoyksikkö ei tarkista aikaeroa seuraavaan 12 tuntiin. Tämä tapahtuma ei synny tapauksissa, joissa GNSS-vastaanotin ei havainnoinut mitään kelvollista GNSS-signaalia edellisen 30 päivän aikana. Kun GNSS-vastaanottimen sijaintitiedot ovat jälleen saatavilla, aika säädetään automaattisesti.

▼B

7. AJONEUVON LIIKERISTIRIITA

GNS_35 Ajoneuvoyksikön on luotava ja kirjattava ajoneuvon liikeristiriita -tapahtuma (ks. tämän liitteen vaatimus 84), jossa aikaleima vastaa nykyistä ajan arvoa, jos liiketunnistimesta lasketut liiketiedot ovat ristiriidassa sisäisestä GNSS-vastaanottimesta tai ulkoisesta GNSS-vastaanottimesta laskettujen liiketietojen kanssa. Tällaisten ristiriitojen havaitsemiseksi käytetään näiden lähteiden välisten nopeuserojen mediaaniarvoa, kuten jäljempänä määritetään:

— korkeintaan 10 sekunnin välein lasketaan GNSS-järjestelmän arvioiman ajoneuvon nopeuden ja liiketunnistimen arvioiman ajoneuvon nopeuden välisen eron absoluuttinen arvo,

— kaikkia laskettuja arvoja aikaikkunassa, johon sisältyvät viimeiset viisi liikeminuuttia, käytetään laskemaan mediaaniarvo,

— mediaaniarvo lasketaan keskiarvona 80 prosenttia jäljellä olevista arvoista sen jälkeen kuin korkeimmat arvot on poistettu (absoluuttisina arvoina).

Ajoneuvon liikeristiriita -tapahtuma syntyy, jos mediaaniarvo ylittää 10 km/t viiden keskeytymättömän minuutin ajan ajoneuvon ollessa liikkeessä. Muita ajoneuvon liiketunnistuksen riippumattomia lähteitä voidaan mahdollisesti käyttää, jotta ajopiirturiin kajoaminen voidaan havaita luotettavammin. (Huom: viimeisen viiden minuutin mediaaniarvoa sovelletaan mittauksen ääriarvoihin ja hetkellisiin arvoihin liittyvien riskien vähentämiseksi). Tämä tapahtuma ei saa syntyä seuraavissa olosuhteissa: a) lautta-/junakuljetuksen aikana, b) kun GNSS-vastaanottimen sijaintitietoja ei ole saatavilla ja c) kalibrointitilassa.

▼B

Lisäys 13

ITS-RAJAPINTA

SISÄLLYSLUETTELO

1. JOHDANTO

2. SOVELTAMISALA

2.1. Lyhenteet, määritelmät ja merkinnät

3. VIITATUT ASETUKSET JA STANDARDIT

4. RAJAPINNAN TOIMINTAPERIAATTEET

4.1. Ennakkoedellytykset tiedonsiirrolle ITS-rajapinnan avulla

4.1.1 ITS-rajapinnan avulla toimitettavat tiedot

4.1.2 Tietojen sisältö

4.1.3 ITS-sovellukset

4.2. Yhteysteknologia

4.3. PIN-varmentaminen

4.4. Viestin muoto

4.5. Kuljettajan suostumus

4.6. Vakiotietojen hakeminen

4.7. Henkilötietojen hakeminen

4.8. Tapahtumiin ja vikoihin liittyvien tietojen hakeminen

1. JOHDANTO

Tässä lisäyksessä määritellään suunnitelma ja menettelyt, joiden avulla otetaan käyttöön ITS-rajapinta asetuksen (EU) N:o 165/2014 (*asetus*) 10 artiklan vaatimusten mukaisesti.

Asetuksessa määritellään, että ajoneuvojen ajopiirturit voidaan varustaa standardien mukaisilla rajapinnoilla, jotka mahdollistavat sen, että ajopiirturin kirjaamia tai tuottamia tietoja voidaan käyttää normaalitilassa ulkoisessa laitteessa, edellyttäen että seuraavat edellytykset täyttyvät:

a) rajapinta ei vaikuta ajopiirturin tietojen aitouteen eikä eheyteen

b) rajapinta on 11 artiklan yksityiskohtaisten säännösten mukainen

c) rajapintaan yhdistetyllä ulkoisella laitteella pääsee tarkastelemaan henkilötietoja ja paikannustietoja vain, jos kuljettajalta, jota tiedot koskevat, on saatu siihen todennettavissa oleva suostumus.

2. SOVELTAMISALA

Tässä lisäyksessä määritellään, miten ulkoisissa laitteissa olevilla sovelluksilla voidaan saada Bluetooth®-yhteyden kautta tietoja (*tiedot*) ajopiirturista.

Tämän rajapinnan avulla saatavilla olevat *tiedot* kuvataan tämän asiakirjan liitteessä 1. Rajapinta ei estä muiden rajapintojen ottamista käyttöön (esim. CAN-väyläliitännän kautta) ajoneuvoyksikön tietojen siirtämiseksi muihin ajoneuvon käsittely-yksikköihin.

▼B

Tässä lisäyksessä määritellään

— ITS-rajapinnan kautta saatavilla olevat *tiedot*

— tietojen siirtämiseen käytettävä Bluetooth®-profiili

— kysely- ja latausmenettelyt ja toimenpiteiden järjestys

— ajopiirturin ja ulkoisen laitteen yhdistämismekanismi

— ajajan käytettävissä oleva suostumusmekanismi.

Selvyyden vuoksi, tässä liitteessä ei määritellä

— *tietojen* keräämisen suorittamista ja hallintaa ajoneuvoyksikössä (se määritellään muualla *asetuksessa* tai muutoin se kuuluu tuotesuunnittelua koskevaan toimintoon)

— ulkoisessa laitteessa olevaan sovellukseen kerättävien tietojen esitystapaa

— tietoturvasäännöksiä Bluetooth®-protokollan lisäksi (kuten salaus) *tietojen* sisällön osalta (ne määritellään muualla asetuksessa [liite 10 Yhteiset suojamekanismit])

— ITS-rajapinnassa käytettäviä Bluetooth®-protokollia.

2.1. **Lyhenteet, määritelmät ja merkinnät**

Tässä lisäyksessä käytetään seuraavia nimenomaisesti tätä lisäystä koskevia lyhenteitä ja määritelmiä:

yhteys	tiedonvaihto pääyksikön (eli ajopiirturin) ja ulkoisen yksikön välillä ITS-rajapinnan avulla Bluetooth®-protokollan kautta
tiedot	liitteessä 1 tarkoitetut tiedot
asetus	asetus (EU) N:o 165/2014, annettu 4 päivänä helmikuuta 2014, tieliikenteessä käytettävistä ajopiirtureista, tieliikenteen valvontalaitteista annetun neuvoston asetuksen (ETY) N:o 3821/85 kumoamisesta sekä tieliikenteen sosiaalilainsäädännön yhdenmukaistamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 561/2006 muuttamisesta
BR	(Basic Rate) Perusliittymä
EDR	(Enhanced Data Rate) Kehittynyt tiedonsiirtonopeus
GNSS	(Global Navigation Satellite System) Maailmanlaajuinen satelliittinavigointijärjestelmä
IRK	(Identity Resolution Key) Henkilöllisyyden selvitysavain
ITS	(Intelligent Transport System) Älykäs liikennejärjestelmä
LE	(Low Energy) Matala energia
PIN	(Personal Identification Number) PIN-koodi; Henkilökohtainen tunnusluku
PUC	(Personal Unblocking Code) Henkilökohtainen avauskoodi, PUK-koodi
SID	(Service Identifier) Palvelun tunniste
SPP	(Serial Port Profile) Sarjaporttiprofiili

▼B

SSP (Secure Simple Pairing) Suojattu yksinkertainen yhdistäminen

TRTP (Transfer Request Parameter) Lähetyspyynnön parametri

TREP (Transfer Response Parameter) Lähetyspyyntöä koskevan vastauksen parametri

VU (Vehicle Unit) Ajoneuvoyksikkö

3. VIITATUT ASETUKSET JA STANDARDIT

Tässä lisäyksessä annettu eritelmä koskee kaikkia seuraavia asetuksia ja standardeja tai niiden osia ja on riippuvainen niistä. Merkitykselliset standardit tai standardien merkitykselliset lausekkeet yksilöidään tämän lisäyksen lausekkeissa. Ristiriitatapauksissa tämän lisäyksen lausekkeita sovelletaan ensisijaisina.

Tässä lisäyksessä viitataan seuraaviin asetuksiin ja standardeihin:

— Euroopan parlamentin ja neuvoston asetus (EU) N:o 165/2014, annettu 4 päivänä helmikuuta 2014, tieliikenteessä käytettävistä ajopiirtureista, tieliikenteen valvontalaitteista annetun neuvoston asetuksen (ETY) N:o 3821/85 kumoamisesta sekä tieliikenteen sosiaalilainsäädännön yhdenmukaistamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 561/2006 muuttamisesta

— Euroopan parlamentin ja neuvoston asetus (EY) N:o 561/2006, annettu 15 päivänä maaliskuuta 2006, tieliikenteen sosiaalilainsäädännön yhdenmukaistamisesta ja neuvoston asetusten (ETY) N:o 3821/85 ja (EY) N:o 2135/98 muuttamisesta sekä neuvoston asetuksen (ETY) N:o 3820/85 kumoamisesta

— ISO 16844 – 4: Road vehicles – Tachograph systems – Part 4: Can interface

— ISO 16844 – 7: Road vehicles – Tachograph systems – Part 7: Parameters

— Bluetooth® – Serial Port Profile – V1.2

— Bluetooth® – perusversio 4.2

— NMEA 0183 V4.1 protocol.

4. RAJAPINNAN TOIMINTAPERIAATTEET

4.1. **Ennakkoedellytykset tiedonsiirrolle ITS-rajapinnan avulla**

Ajoneuvoyksikkö on vastuussa ajoneuvoyksikköön tallennettavien tietojen päivittämisestä ja ylläpidosta, eikä ITS-rajapinta osallistu siihen. Tämän toteuttamiseen tarvittavat keinot ovat ajoneuvoyksikön sisäisiä, ne määritellään muualla asetuksessa eivätkä ne kuulu tähän lisäykseen.

4.1.1 *ITS-rajapinnan avulla toimitettavat tiedot*

Ajoneuvoyksikkö on vastuussa ITS-rajapinnan avulla saatavilla olevien tietojen päivittämisestä ajoneuvoyksikköä koskevissa menettelyissä määriteltävällä tiheydellä, eikä ITS-rajapinta osallistu siihen. Ajoneuvoyksikön tietoja käytetään *tietojen* täydentämisen ja päivittämisen perustana, ja sen toteuttamiseen tarvittavat keinot määritellään muualla *asetuksessa* tai jos kyseisiä eritelmiä ei ole, se kuuluu tuotesuunnitteluun eikä se kuulu tähän lisäykseen.

▼B

4.1.2 *Tietojen sisältö*

Tietojen sisältö määritellään tämän lisäyksen liitteessä 1.

4.1.3 *ITS-sovellukset*

ITS-sovelluksissa käytetään ITS-rajapinnan avulla saataville annettuja tietoja esimerkiksi parantamaan kuljettajan toimintojen hallintaa asetuksen mukaisesti, havaitsemaan mahdolliset ajopiirturin viat tai käyttämään GNSS-tietoja. Sovellusten eritelmät eivät kuulu tämän lisäyksen soveltamisalaan.

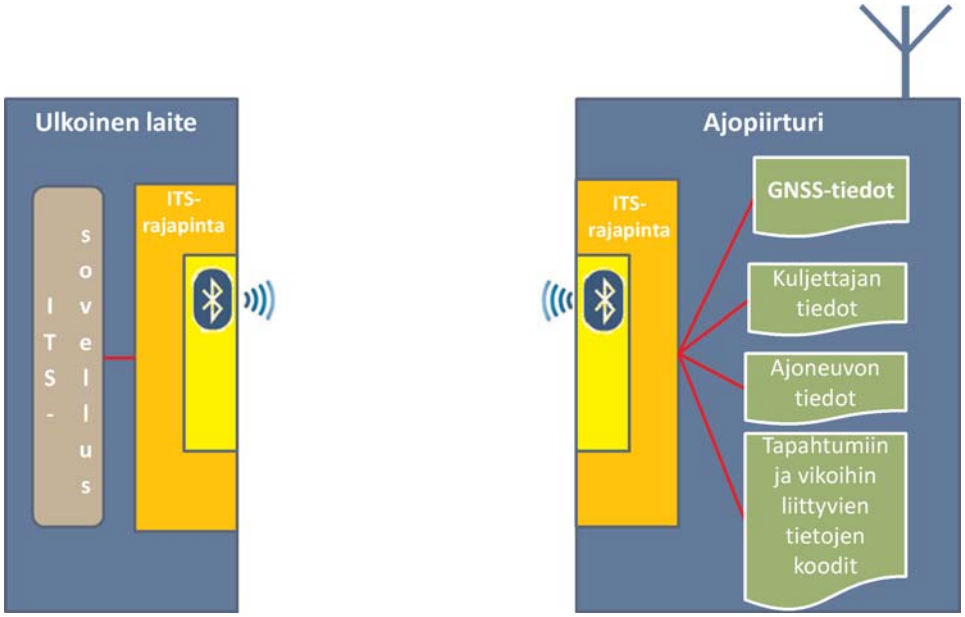
4.2. **Yhteysteknologia**

Tietoja vaihdetaan ITS-rajapintaa käyttämällä yhteensopivan Bluetooth®-rajapinnan version 4.2 tai uudempien versioiden avulla. Bluetooth® toimii ilman toimilupaa toimivalla ISM-kaistalla (teollinen, tieteellinen ja lääketieteellinen) taajuudella 2,4–2,485 GHz. Bluetooth® 4.2 tarjoaa entistä paremman yksityisyys- ja suojamekanismit ja lisää tiedonsiirtojen nopeutta ja luotettavuutta. Näitä eritelmiä varten käytetään luokan 2 Bluetooth®-radiota, jonka kantoalue on enintään 10 metriä. Lisätietoa Bluetooth® 4.2 -versiosta on saatavilla sivustolla www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Yhteys luodaan yhteyslaitteilla sen jälkeen, kun yhdistämisprosessi on saatettu loppuun valtuutetulla laitteella. Koska Bluetooth® käyttää isäntä-/oheismallia ohjaamaan sitä, milloin ja mihin laitteet voivat lähettää tietoja, ajopiirturilla on isännän tehtävä ja ulkoinen laite on oheislaite.

Kun ulkoinen laite tulee ajoneuvoyksikön kantoalueelle ensimmäisen kerran, Bluetooth®-yhdistämisprosessi voidaan aloittaa (katso myös liite 2). Laitteet jakavat osoitteensa, nimensä ja profiilinsa ja yhteisen salaisen avaimen, jonka avulla ne voivat muodostaa yhteyden toisiinsa milloin tahansa, kun ne ovat jatkossa yhdessä. Kun tämä vaihe on saatettu loppuun, ulkoinen laite on luotettava, ja se pystyy tekemään pyyntöjä tietojen lataamiseksi ajopiirturista. Bluetooth®-rajapinnan käyttämien salausmekanismien lisäksi ei ole tarkoitus lisätä muita. Jos lisäsuojausmekanismeja kuitenkin tarvitaan, se tehdään liitteen 10 Yhteiset suojamekanismit mukaisesti.

Seuraavassa kuvassa kuvataan yleinen yhteysperiaate:



▼B

Bluetooth®-yhteyden SPP-profiilia (sarjaporttiprofiili) käytetään siirtämään tietoja ajoneuvoyksiköstä ulkoiseen laitteeseen.

4.3. **PIN-varmentaminen**

Turvallisuussyistä ajoneuvoyksikkö käyttää PIN-koodin varmennusjärjestelmää erillään Bluetooth-yhdistämisestä. Jokaisen ajoneuvoyksikön on voitava luoda varmentamista varten vähintään neljästä luvusta koostuvia PIN-koodeja. Aina, kun ulkoinen laite yhdistetään ajoneuvoyksikköön, laitteen on annettava oikea PIN-koodi ennen kuin se saa mitään tietoja.

Oikean PIN-koodin antamisen jälkeen laite asetetaan hyväksyttyjen laitteiden luetteloon. Hyväksyttyjen laitteiden luetteloon tallennetaan vähintään 64 tiettyyn ajoneuvoyksikköön yhdistettyä laitetta.

Jos laite antaa väärän PIN-koodin kolme kertaa peräkkäin, se asetetaan väliaikaisesti kiellettyjen laitteiden luetteloon. Kun laite on kiellettyjen laitteiden luettelossa, kaikki sen uudet yritykset hylätään. Aina, kun laite antaa väärän PIN-koodin jälleen kolme kertaa peräkkäin, sen kieltoaika pitenee (katso taulukko 1). Oikean PIN-koodin antaminen nollaa kiellon keston ja yritysten määrän. Liitteessä 2 olevassa kuvassa 1 esitetään PIN-koodin validointiyritysten järjestystä koskeva kaavio.

Taulukko 1

Kiellon kesto riippuu väärän PIN-koodin peräkkäisten antamiskertojen määrästä

Peräkkäisten väärien koodien määrä	Kiellon kesto
3	30 sekuntia
6	5 minuuttia
9	1 tunti
12	24 tuntia
15	Pysyvä

Väärän PIN-koodin antaminen 15 kertaa peräkkäin johtaa ITS-yksikön asettamiseen pysyvästi kiellettyjen laitteiden luetteloon. Pysyvä kielto voidaan kumota vain oikean PUK-koodin antamisella.

PUK-koodi muodostuu kahdeksasta luvusta, ja valmistaja toimittaa sen ajoneuvoyksikön mukana. Väärän PUK-koodin antaminen kymmenen kertaa peräkkäin asettaa ITS-yksikön peruuttamattomasti kiellettyjen laitteiden luetteloon.

Valmistaja voi tarjota mahdollisuuden PIN-koodin vaihtamiseen suoraan ajoneuvoyksikön avulla, mutta PUK-koodia ei voi muuttaa. Tarvittaessa PIN-koodin muuttaminen edellyttää nykyisen PIN-koodin antamista suoraan ajoneuvoyksikköön.

Lisäksi kaikki sallittujen laitteiden luetteloon tallennetut laitteet säilytetään siihen asti, että käyttäjä poistaa ne manuaalisesti (esim. ajoneuvoyksikön käyttöliittymän avulla tai muulla keinoin). Siten kadotetut tai varastetut ITS-yksiköt voidaan poistaa sallittujen laitteiden luettelosta. Lisäksi kaikki ITS-yksiköt, jotka poistuvat Bluetooth-yhteyden kantoalueelta yli 24 tunniksi, poistetaan automaattisesti ajoneuvoyksikön sallittujen laitteiden luettelosta, ja niiden on annettava jälleen oikea PIN-koodi, kun yhteys muodostetaan uudelleen.

▼B

Ajoneuvoyksikön rajapinnan ja ajoneuvoyksikön välisten viestien muotoa ei anneta, vaan se jätetään valmistajan päätettäväksi. Kyseisen valmistajan on kuitenkin varmistettava, että ITS-yksikön ja ajoneuvoyksikön rajapinnan välistä viestimuotoa noudatetaan (katso ASN.1-eritelmät).

Kaikkiin tietopyyntöihin vastataan siten lähettäjän tunnusten asianmukaisella todentamisella ennen minkäänlaista käsittelyä. Liitteessä 2 olevassa kuvassa 2 esitetään tämän menettelyn järjestyskaavio. Kaikki kiellettyjen laitteiden luetteloon asetetut laitteet hylätään automaattisesti, ja kaikki laitteet, jotka eivät ole kiellettyjen eivätkä sallittujen laitteiden luettelossa, saavat PIN-pyynnön, joka niiden on täytettävä ennen tietopyynnön lähettämistä.

4.4. **Viestin muoto**

Kaikkien ITS-yksikön ja ajoneuvoyksikön rajapinnan välillä kulkevien viestien muoto perustuu rakenteeseen, jossa on kolme osaa: ylätunniste, jossa on kohdetavu (TGT), lähdetavu (SRC) ja pituustavu (LEN),

datakenttä, jossa on palvelun tunnistetavu (SID) sekä vaihteleva määrä datatavuja (enintään 255).

Tarkistussummatavu on kaikkien viestin sisältämien tavujen, paitsi itse CS-tavun, yhden bitin ryhmissä laskettu summa modulo 256 (jakojäännös, joka syntyy, kun kyseinen summa jaetaan luvulla 256).

Viesti on Big Endian -muodossa.

Taulukko 2

Yleinen viestimuoto

Ylätunniste			Datakenttä					Tarkistussumma
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 tavua			Enintään 255 tavua					1 tavu

Ylätunniste

TGT ja SRC: viestin kohdelaitteen (TGT) ja lähdelaitteen (SRC) tunnisteet. Ajoneuvoyksikön rajapinnan oletustunniste on ”EE”. Tätä tunnistetta ei voida muuttaa. ITS-yksikön oletustunniste on ”A0” yhteysjakson ensimmäisessä viestissä. Ajoneuvoyksikkö osoittaa sitten ITS-yksikölle yksilöllisen tunnisteen ja ilmoittaa sille tämän tunnisteen tulevissa viesteissä käyttöjakson aikana.

LEN-tavussa otetaan huomioon vain datakentän osa ”DATA” (katso taulukko 2), ja neljä ensimmäistä tavua aiheutuu käytännöstä.

Ajoneuvoyksikkö vahvistaa viestin lähettäjän varmennuksen tarkastamalla oman tunnisteluettelonsa vertaamalla Bluetooth-tietoihin ja tarkastamalla, että annetulla tunnisteella luetteloitu ITS-yksikkö on parhaillaan Bluetooth-yhteyden kantoalueella.

Datakenttä

Palvelun tunnisteen (SID) lisäksi datakentässä on myös muita muuttujia: lähetyspyynnön parametri (TRTP) ja laskuritavut.

▼B

Jos siirrettävät tiedot ovat pidempiä kuin yhdessä viestissä saatavilla oleva tila, ne jaetaan useisiin osaviesteihin. Jokaisessa osaviestissä on sama ylätunniste ja SID, mutta niissä on 2-tavuinen laskuri, juokseva laskuri (CC) ja enimmäislaskuri (CM) osoittamaan osaviestin numero. Jotta virheiden tarkistamista ja viestin keskeyttämistä koskevat toiminnot olisivat mahdollisia, vastaanottava laite kuittaa jokaisen osaviestin. Vastaanottava laite voi joko hyväksyä kyseisen osaviestin, pyytää sen lähettämistä uudelleen, pyytää lähettävää laitetta aloittamaan koko viestin uudelleen tai keskeyttää viestin lähetyksen kokonaan.

Jos CC- ja CM-laskureita ei käytetä, niiden arvoksi annetaan 0xFF.

Esimerkkinä seuraava viesti

YLÄTUNNISTE	SID	TRTP	CC	CM	DATA	CS
3 tavua	Enemmän kuin 255 tavua					1 tavu

Lähetetään sellaisenaan.

YLÄTUNNISTE	SID	TRTP	01	n	DATA	CS
3 tavua	255 tavua					1 tavu

YLÄTUNNISTE	SID	TRTP	02	n	DATA	CS
3 tavua	255 tavua					1 tavu

…

YLÄTUNNISTE	SID	TRTP	N	N	DATA	CS
3 tavua	Enintään 255 tavua					1 tavu

Taulukossa 3 esitetään viestit, joita ajoneuvoyksikkö ja ITS-yksikkö voivat vaihtaa. Kunkin parametrin sisältö annetaan heksadesimaaliarvona. Taulukossa ei esitetä selkeyden vuoksi CC- ja CM-laskureita, katso edellä täydellinen malli.

Taulukko 3

Viestin yksityiskohtainen sisältö

Viesti	Ylätunniste			DATA			Tarkistus-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)	

▼B

Viesti	Ylätunniste			DATA			Tarkistus-summa
	TGT	SRC	LEN	SID	TRTP	DATA	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Aika	
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		
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Data	
DataUnavailable							
Tietoja ei saatavilla	*ITSID*	EE	02	0A	TREP	10	
Henkilötietoja ei jaettu	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Yleinen hylkäys	*ITSID*	EE	02	0B	SID Req	10	
Palvelua ei tueta	*ITSID*	EE	02	0B	SID Req	11	
Osatoimintoa ei tueta	*ITSID*	EE	02	0B	SID Req	12	
Väärä viestin pituus	*ITSID*	EE	02	0B	SID Req	13	
Väärät ehdot tai virhe pyynnön rakenteessa	*ITSID*	EE	02	0B	SID Req	22	
Pyyntö alueen ulkopuolella	*ITSID*	EE	02	0B	SID Req	31	
Vastausta odotetaan	*ITSID*	EE	02	0B	SID Req	78	
ITSID ei täsmää	*ITSID*	EE	02	0B	SID Req	FC	
ITSID:tä ei löydy	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Ajoneuvoyksikön rajapinta lähettää tämän viestin, jos ITS-yksikkö, joka ei ole kiellettyjen eikä sallittujen laitteiden luettelossa, lähettää tietopyynnön.

▼B

SendITSID (SID 02)

Ajoneuvoyksikön rajapinta lähettää tämän viestin aina, kun uusi laite lähettää pyynnön. Kyseinen laite käyttää oletustunnistetta ”A0” ennen kuin sille osoitetaan yksilöllinen tunniste yhteyttä varten.

SendPIN (SID 03)

ITS-yksikkö lähettää tämän viestin, jotta ajoneuvoyksikkö asettaa sen sallittujen laitteiden luetteloon. Tämän viestin sisältö on 4 INTEGER koodien 0 ja 9 välillä..

PairingResult (SID 04)

Ajoneuvoyksikön rajapinta lähettää tämän viestin ilmoittaakseen ITS-yksikölle, oliko sen lähettämä PIN-koodi oikein. Tämän viestin sisältö on BOOLEAN ja arvo ”True”, jos PIN-koodi oli oikein, ja ”False”, jos se ei ollut.

SendPUC (SID 05)

ITS-yksikkö lähettää tämän viestin, jotta ajoneuvoyksikkö poistaa sen kiellettyjen laitteiden luettelosta. Tämän viestin sisältö on 8 INTEGER koodien 0 ja 9 välillä.

BanLiftingResult (SID 06)

Ajoneuvoyksikkö lähettää tämän viestin ilmoittaakseen ITS-yksikölle, oliko sen lähettämä PUK-koodi oikein. Tämän viestin sisältö on BOOLEAN ja arvo ”True”, jos PUK-koodi oli oikein, ja ”False”, jos se ei ollut.

RequestRejected (SID 07)

Ajoneuvoyksikön rajapinta lähettää tämän viestin vastauksena kaikkiin viesteihin kiellettyjen laitteiden luettelossa olevalta ITS-yksiköltä, lukuun ottamatta viestiä ”SendPUC”. Viestissä on aika, jonka ITS-yksikkö on vielä kiellettyjen laitteiden luettelossa, ja sen jälkeen liitteessä 3 määritetty järjestysmuoto ”Aika”.

RequestData (SID 08)

ITS-yksikkö lähettää tämän viestin tietojen käyttöoikeudesta. Yhden tavun TRTP-parametri (Transfer Request Parameter) ilmoittaa pyydettyjen tietojen tyypin. Tietoja on useaa eri tyyppiä:

— standardTachData (TRTP 01): muiksi kuin henkilötiedoiksi luokitellut ajopiirturista saatavilla olevat tiedot.

— personalTachData (TRTP 02): henkilötiedoiksi luokitellut ajopiirturista saatavilla olevat tiedot.

— gnssData (TRTP 03): GNSS-tiedot, aina henkilötietoja.

— standardEventData (TRTP 04): muuksi kuin henkilötiedoiksi luokitellut tallennetut tapahtumatiedot.

— personalEventData (TRTP 05): henkilötiedoiksi luokitellut tallennetut tapahtumatiedot.

— standardFaultData (TRTP 06): muiksi kuin henkilötiedoiksi luokitellut tallennetut viat.

— manufacturerData (TRTP 07): valmistajan saataville antamat tiedot.

▼B

Katso tämän lisäyksen liitteestä 3 lisätietoja kunkin tietotyypin sisällöstä.

Katso lisäyksestä 12 lisätietoja GNSS-tietojen muodosta ja sisällöstä.

Katso liitteestä IB ja IC lisätietoja tapahtumatietojen koodeista ja vioista.

RequestAccepted (SID 09)

Ajoneuvoyksikön rajapinta lähettää tämän viestin, jos ITS-yksikön viesti ”RequestData” on hyväksytty. Viestissä on 1-tavuinen TREP, joka on asianomaiseen RequestData-viestiin liittyvä TRTP-tavu, sekä kaikki pyydetyn tyypin tiedot.

DataUnavailable (SID 0A)

Ajoneuvoyksikön rajapinta lähettää tämän viestin, jos jostakin syystä pyydettyjä tietoja ei ole saatavilla lähetettäväksi hyväksyttyjen laitteiden luettelossa olevaan ITS-yksikköön. Viestissä on 1-tavuinen TREP, joka on pyydettyjen tietojen TRTP, ja taulukossa 3 esitetty 1-tavuinen virhekoodi. Käytettävissä on seuraavat koodit:

— Tietoja ei saatavilla (10): Ajoneuvoyksikön rajapinta ei pääse käsiksi ajoneuvoyksikön tietoihin määrittelemättömästä syystä.

— Henkilötietoja ei jaettu (11): ITS-yksikkö yrittää hakea henkilötietoja, kun niitä ei ole jaettu.

NegativeAnswer (SID 0B)

Ajoneuvoyksikkö lähettää nämä viestit, jos pyyntöä ei voida täyttää jostakin muusta syystä kuin siitä, että tietoja ei ole saatavilla. Nämä viestit johtuvat tavallisesti huonosta pyyntimuodosta (pituus, SID, ITSID jne.) mutta eivät pelkästään siitä. Datakentän TRTP:ssä on pyynnön SID. Datakentässä on kielteisen vastauksen syyn määrittävä koodi. Käytettävissä on seuraavat koodit:

— Yleinen hylkääminen (koodi: 10)

— Toimintoa ei voida suorittaa syystä, jota ei ilmoiteta jäljempänä eikä osassa (anna osan *DataUnavailable* numero).

— Palvelua ei tueta (koodi: 11)

— Pyydetty SID ei ymmärrettävä.

— Osatoimintoa ei tueta (koodi: 12)

— Pyydetty TRTP ei ymmärrettävä. Se voi esimerkiksi puuttua tai se on hyväksyttyjen arvojen ulkopuolella.

— Väärä viestin pituus (koodi: 13)

— Vastaanotetun viestin pituus väärä (LEN-tavu ja kyseessä olevan viestin pituus eivät täsmää).

— Väärät ehdot tai virhe pyynnön rakenteessa (koodi: 22)

— Pyydetty palvelu ei ole toimintavalmiudessa tai pyynnön esittäneen viestin osien järjestys on väärä.

— Pyyntö alueen ulkopuolella (koodi: 33)

▼B

— Pyynnön parametritietue (datakenttä) ei oikeanlainen.

— Vastausta odotetaan (koodi: 78)

— Pyydettyä toimintoa ei ehditä suorittaa ajoissa, eikä ajoneuvoyksikkö ole valmis vastaanottamaan uutta pyyntöä.

— *ITSID* ei täsmää (koodi: FB)

— SRC *ITSID* ei vastaa liitettyä laitetta Bluetooth-tietojen vertailun perusteella.

— *ITSID*:tä ei löydy (koodi: FC)

— SRC *ITSID* ei liity mihinkään laitteeseen.

Liitteessä 3 olevan ASN.1-koodin riveillä 1–72 (**FormatMessageModule**) määritellään viestimuoto sellaisena kuin se on kuvattuna taulukossa 3. Viestien sisällöstä annetaan lisätietoja jäljempänä.

4.5. **Kuljettajan suostumus**

Kaikki saatavilla olevat tiedot luokitellaan joko vakiotiedoiksi tai henkilötiedoiksi. Henkilötiedot ovat saatavilla vain, jos kuljettaja on antanut suostumuksensa ja hyväksynyt sen, että hänen henkilötietonsa voidaan välittää ajoneuvon verkosta kolmannen osapuolen sovelluksiin.

Kuljettajan suostumus annetaan, kun kyseinen ajoneuvossa aikaisemmin käyttämätön kuljettajakortti tai korjaamokortti asetetaan paikalleen ensimmäisen kerran ja kuljettajaa pyydetään antamaan suostumuksensa ajopiirturin henkilötietojen välittämiseen valinnaisen ITS-rajapinnan avulla (katso myös liitteessä I C oleva 3.6.2 kohta)

Suostumuksen tila (käytössä / ei käytössä) tallennetaan ajopiirturin muistiin.

Jos kuljettajia on monta, vain suostumuksensa antaneiden kuljettajien henkilötiedot jaetaan ITS-rajapinnassa. Jos ajoneuvossa on esimerkiksi kaksi kuljettajaa, ja vain ensimmäinen kuljettaja on hyväksynyt henkilötietojensa jakamisen, toista kuljettajaa koskevia henkilötietoja ei jaeta.

4.6. **Vakiotietojen hakeminen**

Liitteessä 2 olevassa kuvassa 3 esitetään ITS-yksikön vakiotietojen saamisesta lähettämän hyväksyttävän pyynnön järjestyskaaviot. ITS-yksikkö on asetettu asianmukaisesti hyväksyttyjen laitteiden luetteloon, eikä se pyydä henkilötietoja, joten lisävarmennusta ei tarvita. Kaavioissa oletetaan, että liitteessä 2 olevassa kuvassa 2 esitettyä asianmukaista menettelyä on noudatettu. Ne voidaan rinnastaa kuvan 2 harmaaseen laatikkoon *REQUEST TREATMENT*.

Saatavilla olevista tiedoista vakiotiedoiksi katsotaan seuraavat:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Henkilötietojen hakeminen**

Liitteessä 2 olevassa kuvassa 4 esitetään henkilötietojen saamista koskevan pyynnön käsittelyn järjestyskaavio. Kuten aikaisemmin todettiin, ajoneuvoyksikkö lähettää henkilötietoja vain, jos kuljettaja on antanut siihen yksiselitteisen suostumuksensa (katso myös 4.5). Muussa tapauksessa pyyntö on hylättävä automaattisesti.

▼B

Saatavilla olevista tiedoista henkilötiedoiksi katsotaan seuraavat:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Tapahtumiin ja vikoihin liittyvien tietojen hakeminen**

ITS-yksiköt voivat pyytää tapahtumista tietoja, jotka sisältävät luettelon kaikista odottamattomista tapahtumista. Nämä tiedot katsotaan joko vakiotiedoiksi tai henkilötiedoiksi, katso liite 3. Kunkin tapahtuman sisältö on tämän lisäyksen liitteessä 1 tarkoitettujen asiakirjojen mukainen.

▼B

LIITE 1

LUETTELO ITS-RAJAPINNAN AVULLA SAATAVILLA OLEVISTA TIEDOISTA

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
SpeedAuthorised	Vehicle Unit	**not personal**
TachographCardSlot1	Driver Card	**not personal**
TachographCardSlot2	Driver Card	**not personal**
Driver1Name	Driver Card	personal
Driver2Name	Driver Card	personal

▼B

Data	Source	Data classification (personal/ not 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
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

▼B

Data	Source	Data classification (personal/ not 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) KULJETTAJAN SUOSTUMUKSEN JÄLKEEN SAATAVILLA OLEVAT JATKUVAT GNSS-TIEDOT

Katso lisäys 12 – GNSS

3) ILMAN KULJETTAJAN SUOSTUMUSTA SAATAVILLA OLEVAT TAPAHTUMAKOODIT

Tapahtuma	Tallennussäännöt	Kustakin tapahtumasta kirjattavat tiedot
Ei-voimassa olevan kortin asettaminen laitteeseen	— 10 viimeisintä tapahtumaa	— tapahtuman päivämäärä ja aika — kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja tapahtuman luoneen kortin sukupolvi — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Korttiristiriita	— 10 viimeisintä tapahtumaa	— tapahtuman alkamispäivämäärä ja -aika — tapahtuman päättymispäivämäärä ja -aika — kunkin kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja ristiriidan aiheuttaneiden kunkin kortin sukupolvi
Edellistä kortin käyttöjaksoa ei lopetettu oikein	— 10 viimeisintä tapahtumaa	— päivämäärä ja aika, jolloin kortti asetettiin paikoilleen — kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi — viimeisimmän käyttöjakson tiedot sellaisina kuin ne ovat luettavissa kortilta: — päivämäärä ja aika, jolloin kortti asetettiin paikoilleen — rekisteritunnus, jäsenvaltio, jossa ajoneuvo on rekisteröity ja ajoneuvoyksikön sukupolvi

▼B

Tapahtuma	Tallennussäännöt	Kustakin tapahtumasta kirjattavat tiedot
Keskeytynyt virransyöttö (2)	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika — tapahtuman päättymispäivämäärä ja -aika — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja kortin luominen — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Virhe yhteydessä etäviestintälaitteistoon	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika — tapahtuman päättymispäivämäärä ja -aika — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja kortin luominen — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Sijaintitietojen puuttuminen GNSS-vastaanottimesta	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika — tapahtuman päättymispäivämäärä ja -aika — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja kortin luominen — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Virhe liikedatassa	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika — tapahtuman päättymispäivämäärä ja -aika — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja kortin luominen — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Ajoneuvon liikeristiriita	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika — tapahtuman päättymispäivämäärä ja -aika — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja kortin luominen — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Tietoturvan murtoyritys	10 viimeisintä kutakin tyyppiä edustavaa tapahtumaa	— tapahtuman alkamispäivämäärä ja -aika — tapahtuman päättymispäivämäärä ja -aika (jos tieto on oleellinen) — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja kortin luominen — tapahtuman tyyppi

▼B

Tapahtuma	Tallennussäännöt	Kustakin tapahtumasta kirjattavat tiedot
Aikojen päällekkäisyys	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— valvontalaitteen päivämäärä ja aika — GNSS-laitteiston päivämäärä ja aika — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja kortin luominen — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä

4) KULJETTAJAN SUOSTUMUKSEN NOJALLA SAATAVILLA OLEVAT TAPAHTUMAKOODIT

Tapahtuma	Tallennussäännöt	Kustakin tapahtumasta kirjattavat tiedot
Ajo ilman asianmukaista korttia	— pisimpään kestänyt tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui — viisi pisimpään kestänyttä tapahtumaa viimeisen 365 vuorokauden aikana	— tapahtuman alkamispäivämäärä ja -aika — tapahtuman päättymispäivämäärä ja -aika — tapahtuman alkaessa ja/tai päättyessä paikoilleen asetetun kortin korttityyppi, numero, kortin myöntänyt jäsenvaltio ja kortin luominen — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Kortin paikoilleen asettaminen ajon aikana	— viimeinen tapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui	— tapahtuman päivämäärä ja aika — kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä
Ylinopeus (1)	— vakavin ylinopeustapahtuma kultakin niistä 10 viimeisimmästä päivästä, jolloin tapahtumia sattui (eli tapahtuma, johon liittyy korkein keskinopeus) — viisi vakavinta tapahtumaa viimeisten 365 vuorokauden ajalta — ensimmäinen tapahtuma, joka sattui viimeksi suoritetun kalibroinnin jälkeen	— tapahtuman alkamispäivämäärä ja -aika — tapahtuman päättymispäivämäärä ja -aika — suurin tapahtuman kestäessä mitattu nopeus — tapahtuman kestäessä mitattujen nopeuslukemien aritmeettinen keskiarvo — kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja kuljettajakortin sukupolvi (tarvittaessa) — kyseisenä päivänä sattuneiden vastaavien tapahtumien lukumäärä

5) ILMAN KULJETTAJAN SUOSTUMUSTA SAATAVILLA OLEVAT VIKATIETOKOODIT

Vikatapahtumat	Tallennussäännöt	Kustakin viasta kirjattavat tiedot
Korttivika	— 10 viimeisintä kuljettajakortin vikatapahtumaa	— päivämäärä ja aika, jolloin vikatapahtuma alkoi — päivämäärä ja aika, jolloin vikatapahtuma päättyi — kortin tyyppi, numero, kortin myöntänyt jäsenvaltio ja sen sukupolvi
Valvontalaiteviat	— 10 viimeisintä kutakin tyyppiä edustavaa vikatapahtumaa — ensimmäinen vikatapahtuma, joka sattui viimeksi suoritetun kalibroinnin jälkeen	— päivämäärä ja aika, jolloin vikatapahtuma alkoi — päivämäärä ja aika, jolloin vikatapahtuma päättyi — vian tyyppi — vikatapahtuman alkaessa ja/tai päättyessä paikoilleen asetettujen korttien tyyppi, numero ja ne myöntänyt jäsenvaltio sekä niiden sukupolvi

▼B

Tämä vikatapahtuma syntyy, kun jokin seuraavista vioista ilmenee laitteen ollessa muussa kuin kalibrointitilassa:

— vika ajoneuvoyksikön sisällä

— vika tulostimessa

— vika näytössä

— tietojen kopiointiin liittyvä vika

— vika tunnistimessa

— GNSS-vastaanottimeen tai ulkoiseen GNSS-laitteistoon liittyvä vika

— etäviestintälaitteistoon liittyvä vika.

6) VALMISTAJAA KOSKEVAT TAPAHTUMAT JA ILMAN KULJETTAJAN SUOSTUMUSTA SAATAVILLA OLEVAT VIAT

Tapahtuma tai vika	Tallennussäännöt	Kustakin tapahtumasta kirjattavat tiedot
Valmistaja määrittelee	Valmistaja määrittelee	Valmistaja määrittelee

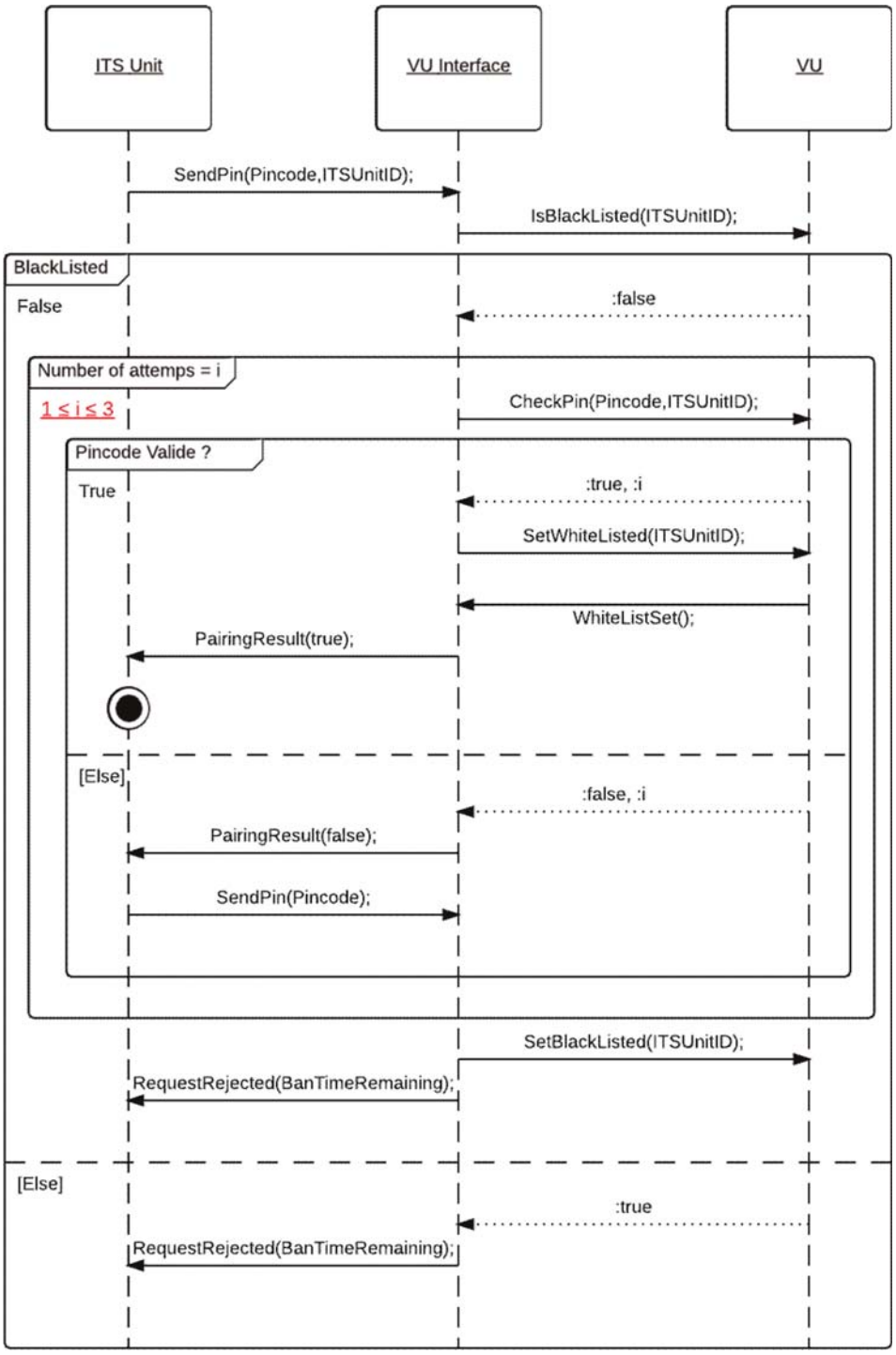
▼B

LIITE 2

ITS-YKSIKÖN KANSSA VAIHDETTAVIEN VIESTIEN JÄRJESTYSKAAVIOT

Kuva 1

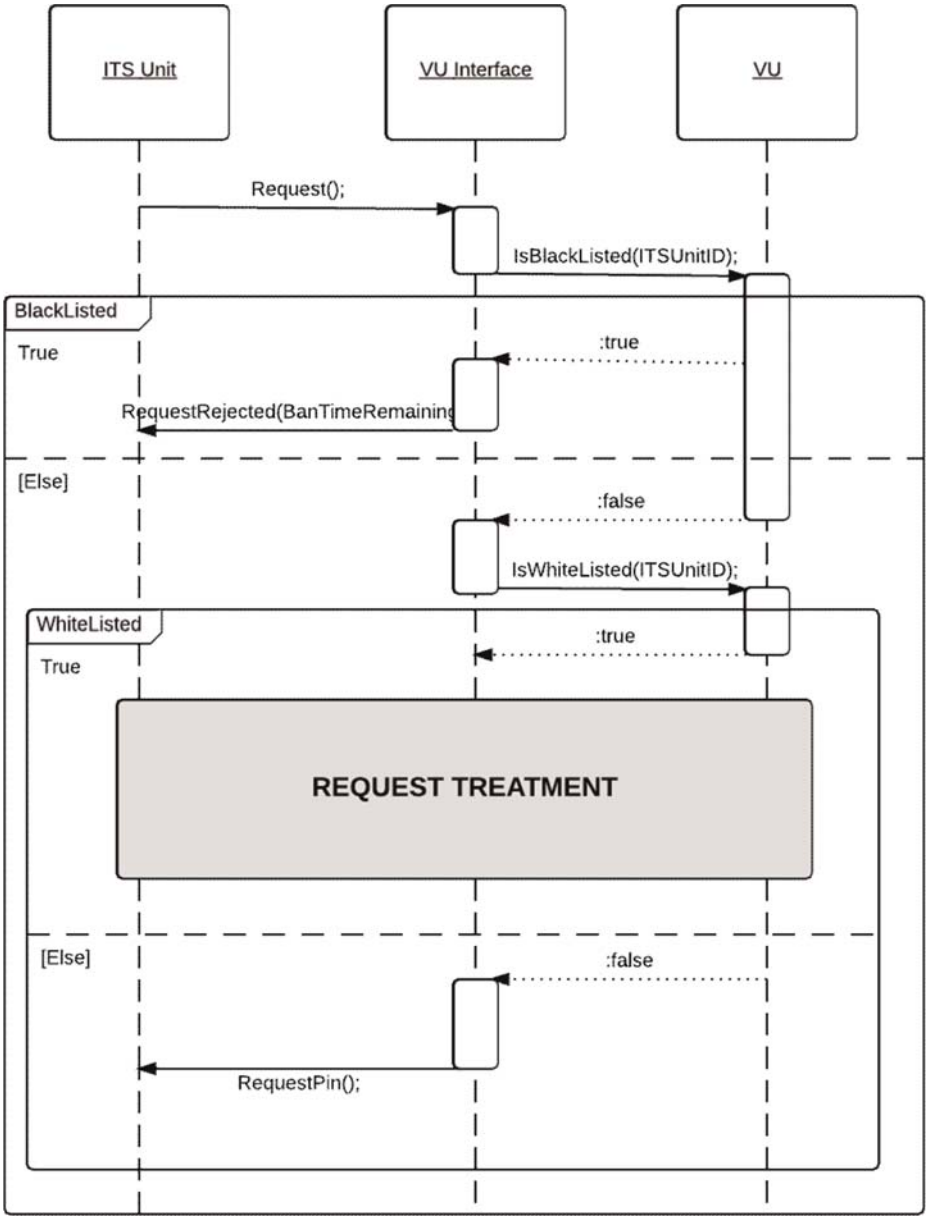
PIN-koodin validointiyrityksen järjestyskaavio



▼B

Kuva 2

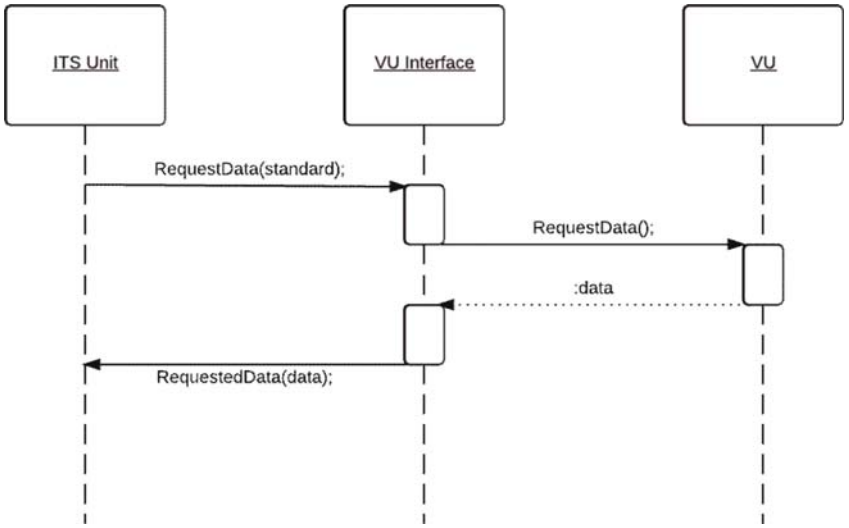
ITS-yksikön varmennuksen tarkistamista koskeva järjestyskaavio



▼B

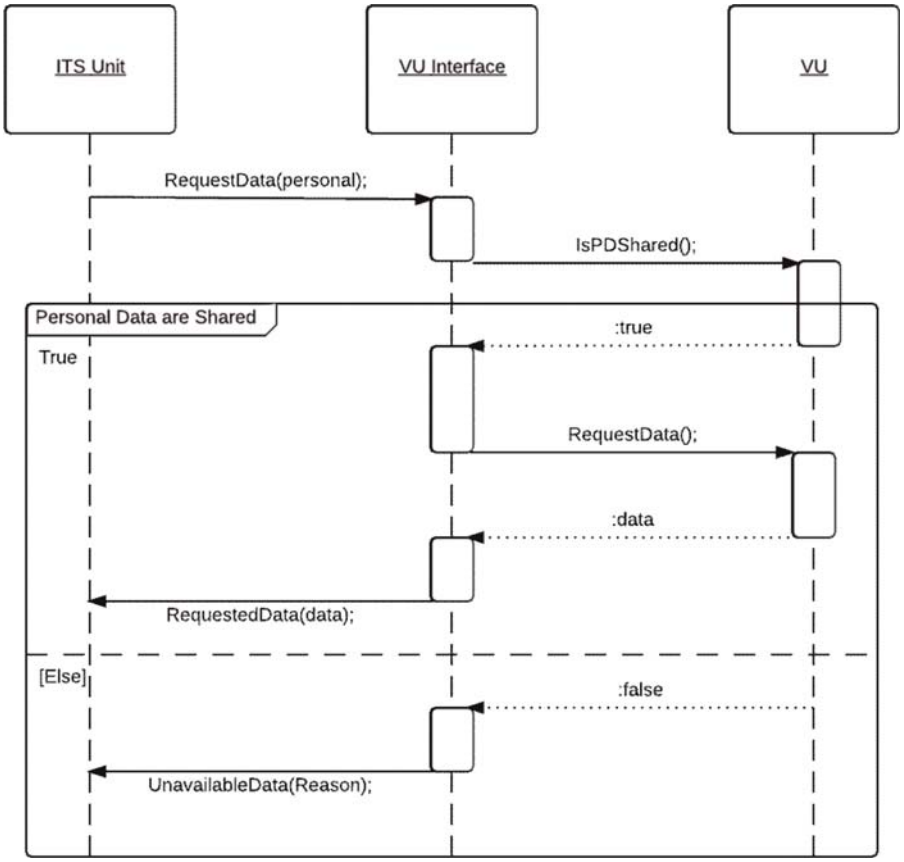
Kuva 3

Muuksi kuin henkilötiedoiksi luokiteltujen tietojen saamista koskevien pyyntöjen käsittelyn järjestyskaavio



Kuva 4

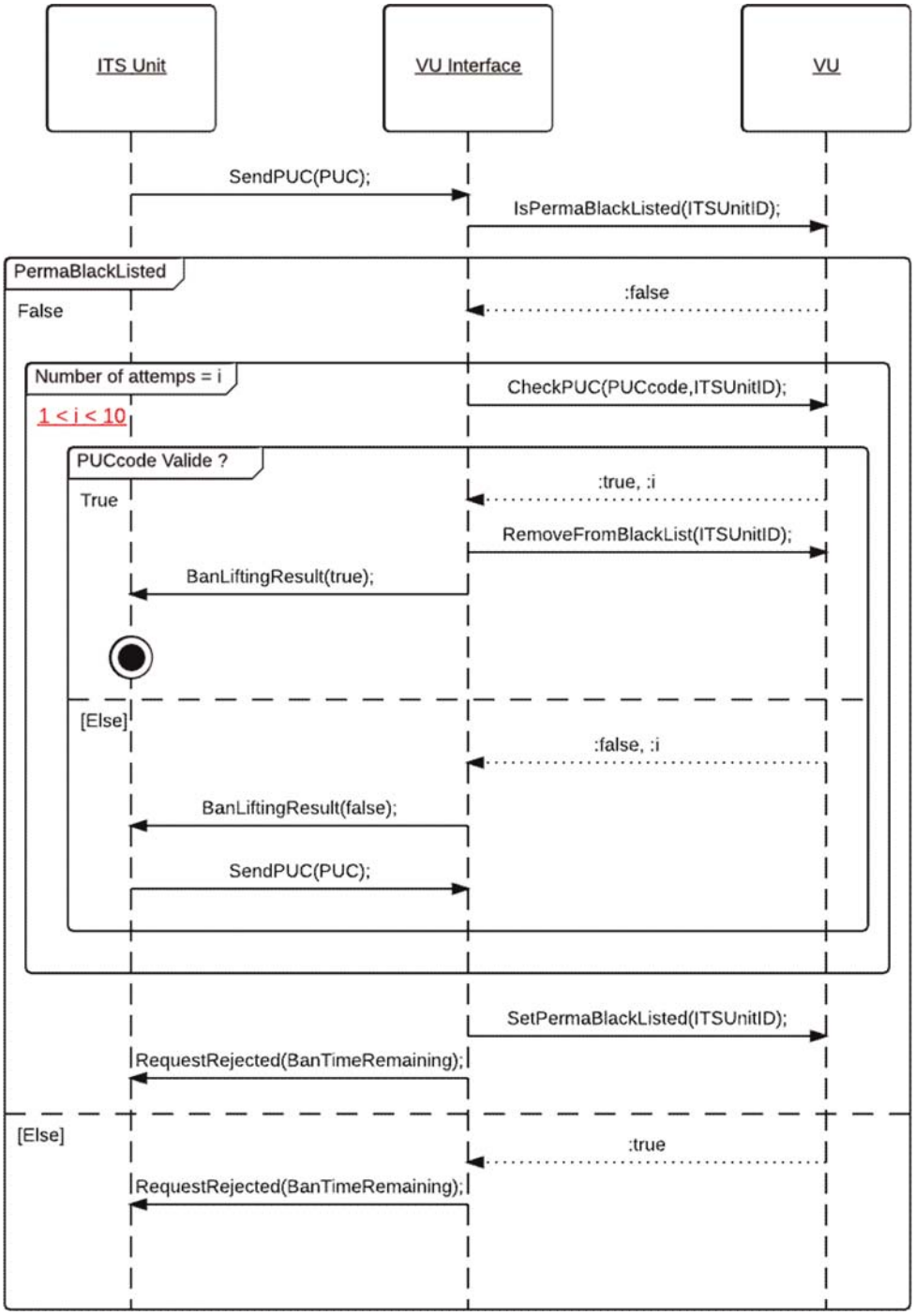
Henkilötiedoiksi luokiteltujen tietojen saamista koskevien pyyntöjen käsittelyn järjestyskaavio



▼B

Kuva 5

PUK-koodin validointiyrityksen järjestyskaavio (sama)



▼B

LIITE 3

ASN.1 SPECIFICATIONS

```
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,
```

▼B

```
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
```

▼B

```
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
```

▼B

```
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—

```

▼B

```
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{
```

▼B

```
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
```

▼B

```
                                                    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--
```

▼B

```
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
```

▼B

```
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,
```

▼B

```
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,
```

▼B

```
537                     numberOfSimilarEvent INTEGER
538             }
539
540             PositionDataError ::= SEQUENCE{
541                     beginDate GeneralizedTime,
542                     endDate GeneralizedTime,
543                     carsdType SEQUENCE OF UTF8String,
544                     cardsNumber SEQUENCE OF INTEGER,
545                     issuingMemberState SEQUENCE OF NationAlpha,
546                     cardsGeneration SEQUENCE OF INTEGER,
547                     numberOfSimilarEvent INTEGER
548             }
549
550             MotionDataError ::= SEQUENCE{
551                     beginDate GeneralizedTime,
552                     endDate GeneralizedTime,
553                     carsdType SEQUENCE OF UTF8String,
554                     cardsNumber SEQUENCE OF INTEGER,
555                     issuingMemberState SEQUENCE OF NationAlpha,
556                     cardsGeneration SEQUENCE OF INTEGER,
557                     numberOfSimilarEvent INTEGER
558             }
559
560             VehicleMotionConflict ::= SEQUENCE{
561                     beginDate GeneralizedTime,
562                     endDate GeneralizedTime,
563                     carsdType SEQUENCE OF UTF8String,
564                     cardsNumber SEQUENCE OF INTEGER,
565                     issuingMemberState SEQUENCE OF NationAlpha,
566                     cardsGeneration SEQUENCE OF INTEGER,
567                     numberOfSimilarEvent INTEGER
568             }
569
570             SecurityBreachAttempt ::= SEQUENCE{
571                     beginDate GeneralizedTime,
572                     endDate GeneralizedTime OPTIONAL,
573                     carsdType SEQUENCE OF UTF8String,
574                     cardsNumber SEQUENCE OF INTEGER,
575                     issuingMemberState SEQUENCE OF NationAlpha,
576                     numberOfSimilarEvent INTEGER,
577                     typeOfEvent SecurityBreachEvent
578             }
579
580
581             TimeConflict ::= SEQUENCE{
582                     beginDate GeneralizedTime,
583                     endDate GeneralizedTime,
584                     carsdType SEQUENCE OF UTF8String,
585                     cardsNumber SEQUENCE OF INTEGER,
586                     issuingMemberState SEQUENCE OF NationAlpha,
587                     cardsGeneration SEQUENCE OF INTEGER,
588                     numberOfSimilarEvent INTEGER
589             }
590
591             ---------------
592             --FAULTS LIST--
593             ---------------
594
595             CardFault ::= SEQUENCE{
```

▼B

```
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
```

▼B

Lisäys 14

ETÄYHTEYSTOIMINTO

SISÄLLYSLUETTELO

1 JOHDANTO

2 SOVELTAMISALA

3 LYHENTEET, MÄÄRITELMÄT JA MERKINNÄT

4 TOIMINTASKENAARIOT

4.1 Yleistä

4.1.1 5,8 GHz:n DSRC-rajapinnan kautta tapahtuvan tiedonsiirron ennakkoedellytykset

4.1.2 Profiili 1 a: käsin suunnattavan tai väliaikaisesti tienvarteen asennetun ja suunnatun etäyhteytenä toteutetun varhaisen havaitsemisen lukijan avulla

4.1.3 Profiili 1 b: ajoneuvoon asennetun ja suunnatun etäyhteytenä toteutetun varhaisen havaitsemisen lukijan (RECDR-lukija) avulla

4.2 Turvallisuus/eheys

5 ETÄYHTEYSTOIMINNON SUUNNITTELU JA PROTOKOLLAT

5.1 Suunnittelu

5.2 Työnkulku

5.2.1 Toiminnot

5.2.2 DSRC-yhteyden kautta saatujen tietojen tulkinta

5.3 Fyysisen DSRC-rajapinnan parametrit etäyhteyttä varten

5.3.1 Sijaintia koskevat rajoitteet

5.3.2 Vastaanotto- ja lähetysyhteyksien parametrit

5.3.3 Antennin suunnittelu

5.4 DSRC-protokollan vaatimukset ajopiirturin etäseurantaa varten

5.4.1 Yleistä

5.4.2 Komennot

5.4.3 Kyselykomentosarja

5.4.4 Tietorakenteet

5.4.5 RtmData-elementit, suoritetut toiminnot ja määritelmät

5.4.6 Tiedonsiirtomekanismi

5.4.7 DSRC-tapahtuman yksityiskohtainen kuvaus

5.4.8 DSRC-testitapahtuman kuvaus

5.5 Direktiivin 2015/71/EY tukeminen

5.5.1 Yleistä

5.5.2 Komennot

▼B

5.5.3 Kyselykomentosarja

5.5.4 Tietorakenteet

5.5.5 OWS-datan DSRC-tapahtuman ASN.1-moduuli

5.5.6 OwsData-elementit, suoritetut toiminnot ja määritelmät

5.5.7 Tiedonsiirtomekanismit

5.6 Ajoneuvoyksikön DSRC-laitteen ja ajoneuvoyksikön välinen tiedonsiirto

5.6.1 Fyysinen yhteys ja rajapinnat

5.6.2 Sovellusprotokolla

5.7 Virheenkäsittely

5.7.1 Tietojen kirjaaminen ja viestintä ajoneuvoyksikön DSRC-laitteessa

5.7.2 Langattoman yhteyden virheet

6 ETÄYHTEYSTOIMINNON KÄYTTÖÖNOTTOON JA MÄÄRÄAIKAISTARKASTUKSIIN LIITTYVÄT TESTIT

6.1 Yleistä

6.2 ECHO

6.3 Testit suojattujen tietojen sisällön validoimiseksi

1 JOHDANTO

Tässä lisäyksessä määritellään suunnittelu ja noudatettavat menettelyt asetuksen (EU) N:o 165/2014, jäljempänä ’asetus’, 9 artiklassa edellytetyn etäyhteystoiminnon, jäljempänä ’yhteys’, suorittamiseksi.

DSC_1 Asetuksen (EU) N:o 165/2014 mukaan ajopiirturi on varustettava etäyhteystoiminnolla, jonka avulla toimivaltaisten valvontaviranomaisten edustajat voivat lukea ajopiirturin tietoja ohi ajavista ajoneuvoista käyttäen etäkyselylaitteistoa (etäyhteytenä toteutetun varhaisen havaitsemisen lukija [REDCR]), erityisesti langatonta kyselylaitteistoa, joka käyttää CEN 5.8 GHz:n lyhyen kantaman DSRC-tiedonsiirron (DSRC) rajapintoja.

On tärkeää ymmärtää, että tämä toiminto on tarkoitettu vain esisuodattimeksi, jolla valitaan tarkemmin tarkastettavat ajoneuvot, eikä se korvaa asetuksen (EU) N:o 165/2014 säännöksissä määriteltyä muodollista tarkastusprosessia. Ks. kyseisen asetuksen johdanto-osan 9 kohta, jonka mukaan ajopiirturin ja valvontaviranomaisten välisellä etäyhteydellä tienvarsitarkastuksia varten helpotetaan kohdennettuja tienvarsitarkastuksia.

DSC_2 *Tiedot* vaihdetaan *yhteydellä*, joka on tämän lisäyksen mukainen 5,8 GHz:n langatonta DSRC-yhteyttä käyttävä langaton yhteys, joka on testattu standardin EN 300 674-1 asianmukaisten parametrien mukaan {Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication

▼B

(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)}.

DSC_3 *Yhteys* viestintälaitteistoon luodaan ainoastaan toimivaltaisen valvontaviranomaisten laitteista lähetetystä pyynnöstä käyttäen vaatimusten mukaisia radioyhteyksiä (*varhaiseen havaitsemiseen tarkoitettu etäyhteyslukija (REDCR)*).

DSC_4 *Tiedot* on suojattava niiden eheyden varmistamiseksi.

DSC_5 *Yhteyden* kautta saatuja tietoja saavat käyttää ainoastaan valvontaviranomaiset, joilla on valtuudet tarkastaa asetukseen (EY) N:o 561/2006 ja asetukseen N:o 165/2014 kohdistuvia rikkomuksia, ja korjaamot siltä osin kuin se on tarpeen ajopiirturin moitteettoman toiminnan varmistamiseksi.

DSC_6 *Yhteyden* aikana voidaan vaihtaa ainoastaan sellaisia *tietoja*, jotka ovat tarpeellisia kohdennettujen tienvarsitarkastusten suorittamiseksi ajoneuvoille, joiden ajopiirturia on mahdollisesti manipuloitu tai käytetty väärin.

DSC_7 Tietojen eheys ja turvallisuus varmistetaan suojaamalla ajoneuvoyksikössä olevat *tiedot* ja siirtämällä vain suojattuja hyötytietoja ja suojaukseen liittyviä tietoja (ks. 5.4.4 jakso) langattomalla 5,8 GHz:n DSRC-etäyhteydellä, mikä tarkoittaa, että vain toimivaltaisten valvontaviranomaisten valtuutetuilla henkilöillä on välineet ymmärtää *yhteyden* avulla siirrettyjä tietoja ja todentaa niiden aitous. Ks. lisäys 11 ”Yhteiset turvamekanismit”.

DSC_8 *Tiedoissa* on oltava aikaleima, josta käy ilmi niiden viimeisimmän päivityksen ajankohta.

DSC_9 Turvatietojen sisältö saa olla ainoastaan toimivaltaisten valvontaviranomaisten sekä niiden osapuolien tiedossa ja hallinnassa, joiden kanssa ne jakavat näitä tietoja, eikä siihen sovelleta tämän lisäyksen aiheena olevaa *yhteyttä* koskevia säännöksiä, paitsi kun *yhteys* edellyttää turvatietopaketin siirtämistä jokaisen hyötytietopaketin kanssa.

DSC_10 Samaa rakennetta ja laitteistoa on voitava käyttää muiden tietokäsitteiden (kuten ajoneuvossa punnitsemisen) hankkimiseen tässä määriteltyä rakennetta käyttäen.

DSC_11 Selvyyden vuoksi huomautetaan, että asetuksen (EU) N:o 165/2014 säännösten (7 artikla) mukaisesti kuljettajan henkilöllisyyttä koskevia tietoja ei siirretä *yhteyden* avulla.

2 SOVELTAMISALA

Tässä lisäyksessä määritellään, miten toimivaltaisten valvontaviranomaisten edustajat käyttävät määriteltyä 5,8 GHz:n langatonta DSRC-yhteyttä saadakseen etäyhteyden avulla kohdennetusta ajoneuvosta tietoja (*tiedot*), jotka osoittavat, että kohteena oleva ajoneuvo saattaa rikkoa

▼B

asetusta (EU) N:o 165/2014 ja että sen pysäyttämistä lähempää tarkastusta varten olisi harkittava kohdennetusti.

Asetuksessa (EU) N:o 165/2014 edellytetään, että kerätyt tiedot on rajoitettava sellaisiin tietoihin tai niihin liittyviin tietoihin, joilla tunnistetaan mahdollinen rikkomus asetuksen (EU) N:o 165/2014 9 artiklan määritelmän mukaisesti.

Tässä skenaariossa yhteyteen käytettävissä oleva aika on rajallinen, koska *yhteys* on kohdennettu ja sen kantama on lyhyt. Lisäksi toimivaltaiset valvontaviranomaiset voivat käyttää samaa ajopiirturin etäseurannan (Remote Tachograph Monitoring, RTM) yhteyttä myös muihin sovelluksiin (kuten direktiivissä (EU) 2015/719/EY määriteltyihin raskaiden hyötyajoneuvojen suurimpiin sallittuihin painoihin ja mittoihin), ja tällaiset toimenpiteet voivat olla erillisiä tai peräkkäisiä toimivaltaisten valvontaviranomaisten harkinnan mukaan.

Tässä lisäyksessä määritellään

— *yhteyttä* varten käytettävät viestintälaitteet, menettelyt ja protokollat

— standardit ja asetukset, joita radiolaitteiden on noudatettava

— *tietojen* esittäminen *viestintälaitteistolle*

— kysely- ja latausmenettelyt ja toimenpiteiden järjestys

— siirrettävät *tiedot*

— *yhteyden* avulla siirrettyjen *tietojen* mahdollinen tulkinta

— *yhteyteen* liittyviä turvatietoja koskevat säännökset

— toimivaltaisten valvontaviranomaisten mahdollisuutta käyttää *tietoja*

— miten *varhaiseen havaitsemiseen tarkoitettu etäyhteyslukija* voi pyytää erilaisia rahtia ja ajoneuvoja koskevia tietokäsitteitä.

Selvyyden vuoksi todettakoon, että tässä lisäyksessä ei määritellä

— *tietojen* keräämistä ja hallintaa ajoneuvoyksikössä (joka riippuu tuotesuunnittelusta, ellei sitä määritellä muualla asetuksessa (EU) N:o 165/2014

— muotoa, jossa kerätyt tiedot esitetään toimivaltaisten valvontaviranomaisten edustajalle, eikä perusteita, joita toimivaltaiset valvontaviranomaiset käyttävät päättäessään, mitä ajoneuvoja pysäytetään (nämä seikat riippuvat tuotesuunnittelusta, ellei niitä määritellä muualla asetuksessa (EU) N:o 165/2014 tai toimivaltaisten valvontaviranomaisten toimintapoliittisella päätöksellä); selvyyden vuoksi todettakoon, että *yhteyden* avulla ainoastaan saatetaan *tiedot* toimivaltaisten valvontaviranomaisten saataville, jotta nämä voivat tehdä tietoon perustuvia päätöksiä

▼B

— *tietojen* sisältöä koskevia tietoturvasäännöksiä, kuten salausta (ne määritellään lisäyksessä 11 ”Yhteiset turvamekanismit”)

— ajopiirturin etäseurannan lisäksi muiden saman rakenteen ja saman laitteiston avulla saatavien tietokäsitteiden yksityiskohtia

— ajoneuvoyksikön ja ajoneuvoyksikön DSRC-laitteen välisen toiminnan ja hallinnan yksityiskohtia eikä ajoneuvoyksikön DSRC-laitteen sisäistä toiminta (lukuun ottamatta *tietojen* toimittamista varhaiseen havaitsemiseen tarkoitetun etäyhteyslukijan (REDCR) pyynnöstä).

3 LYHENTEET, MÄÄRITELMÄT JA MERKINNÄT

Tässä lisäyksessä käytetään seuraavia nimenomaisesti tätä lisäystä koskevia lyhenteitä ja määritelmiä:

Antenni	Radiolähettimen tai -vastaanottimen yhteydessä käytettävä sähköinen laite, joka muuntaa sähkövirran radioaalloiksi ja päinvastoin. Antennin toimiessa radiolähetin syöttää radiotaajuudella värähtelevän sähkövirran antennin liittimiin ja antenni säteilee sähkövirrasta saatavan energian sähkömagneettisina aaltoina (radioaaltoina). Vastaanotettaessa antenni sieppaa osan sähkömagneettisen aallon energiasta ja tuottaa siitä pienen jännitteen liittimiinsä, jotka johtavat sen vastaanottimeen, jossa jännite vahvistetaan.
Yhteys	Tietojen vaihtaminen DSRC-REDCR-lukijan ja ajoneuvon DSRC-laitteen välillä 5 kohdan mukaisesti isäntä-renki-periaatteella tietojen saamiseksi.
Tiedot	Ennalta määritetyssä muodossa esitettävät suojatut tiedot (ks. 5.4.4 jakso), joita *DSRC-REDCR-lukija* pyytää ja jotka *ajoneuvon DSRC-laite* toimittaa sille jäljempänä 5 jaksossa määritellyn 5,8 GHz:n DSRC-yhteyden avulla.
Asetus (EU) N:o 165/2014	Euroopan parlamentin ja neuvoston asetus (EU) N:o 165/2014, annettu 4 päivänä helmikuuta 2014, tieliikenteessä käytettävistä ajopiirtureista, tieliikenteen valvontalaitteista annetun neuvoston asetuksen (ETY) N:o 3821/85 kumoamisesta sekä

▼B

	tieliikenteen sosiaalilainsäädännön yhdenmukaistamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 561/2006 muuttamisesta.
AID	(Application Identifier) Sovellustunniste
BLE	Bluetooth Low Energy
BST	(Beacon Service Table) Lähettimen palvelutaulukko
CIWD	(Card insertion while driving) Kortin syöttäminen ajon aikana
CRC	(Cyclic redundancy check) Syklinen redundanssitarkistus
DSC (n)	(identifier of a requirement for a specific DSRC appendix) Vaaditun tietyn DSRC-lisäyksen tunniste
DSRC	(Dedicated Short Range Communication) Lyhyen kantaman DSRC-tiedonsiirto
DSRC-REDCR	(DSRC – Remote Early Detection Communication Reader) DSRC-tiedonsiirtoa käyttävä varhaiseen havaitsemiseen tarkoitettu etäyhteyslukija
DSRC-VU	(DSRC – Vehicle Unit) Ajoneuvoyksikön DSRC-laite. Tämä on liitteessä 1 C määritelty ”varhaiseen havaitsemiseen tarkoitettu etäyhteyslaite”.
DWVC	(Driving without valid card) Ajaminen ilman voimassa olevaa korttia
EID	(Element Identifier) Osan tunniste
LLC	(Logical Link Control) Looginen siirtotien ohjaus
LPDU	(LLC Protocol Data Unit) LLC-siirtoyhteyskäytännön datayksikkö
OWS	(Onboard Weighing System) Ajoneuvon sisäinen punnitusjärjestelmä
PDU	(Protocol Data Unit) Siirtoyhteyskäytännön datayksikkö
REDCR	(Remote early detection communication reader) Varhaiseen havaitsemiseen tarkoitettu etäyhteyslukija. Tämä on liitteessä 1 C määritelty ”varhaiseen havaitsemiseen tarkoitettu etäyhteyslukulaite”.
RTM	(Remote Tachograph Monitoring) Ajopiirturin etäseuranta
SM-REDCR	(Security Module-Remote early detection communication reader) Varhaiseen havaitsemiseen tarkoitetun etäyhteyslukijan turvamoduuli
TARV	Säänneltyjen ajoneuvojen telemaattiset sovellukset (ISO 15638 -standardisarja)

▼B

VU	(Vehicle unit) Ajoneuvoyksikkö
VUPM	(Vehicle Unit Payload Memory) Ajoneuvoyksikön hyötykuormamuisti
VUSM	(Vehicle Unit Security Module) Ajoneuvoyksikön turvamoduuli
VST	(Vehicle Service Table) Ajoneuvon palvelutaulukko
WIM	(Weigh in motion) Punnitseminen liikkeessä
WOB	(Weigh on board) Ajoneuvossa tapahtuva punnitseminen

Tässä lisäyksessä annettu eritelmä koskee kaikkia seuraavia asetuksia ja standardeja tai niiden osia ja on riippuvainen niistä. Merkitykselliset standardit tai standardien merkitykselliset lausekkeet yksilöidään tämän lisäyksen lausekkeissa. Ristiriitatapauksissa tämän lisäyksen lausekkeita sovelletaan ensisijaisina. Ristiriitatapauksissa, joiden suhteen tässä lisäyksessä ei ole selvästi määritelty eritelmää, sovelletaan ensisijaisesti suosituksen ERC 70-03 mukaista toimintaa (testattuna standardin EN 200 674-1 asianmukaisten parametrien mukaan) ja sen jälkeen laskevassa järjestyksessä standardeja EN 12795, EN 12253, EN 12834 ja standardin EN 13372 6.2, 6.3, 6.4 ja 7.1 kohtaa.

Tässä lisäyksessä viitataan seuraaviin asetuksiin ja standardeihin:

[1] Euroopan parlamentin ja neuvoston asetus (EU) N:o 165/2014, annettu 4 päivänä helmikuuta 2014, tieliikenteessä käytettävistä ajopiirtureista, tieliikenteen valvontalaitteista annetun neuvoston asetuksen (ETY) N:o 3821/85 kumoamisesta sekä tieliikenteen sosiaalilainsäädännön yhdenmukaistamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 561/2006 muuttamisesta. 561/2006 muuttamisesta.

[2] Euroopan parlamentin ja neuvoston asetus (EY) N:o 561/2006, annettu 15 päivänä maaliskuuta 2006, tieliikenteen sosiaalilainsäädännön yhdenmukaistamisesta ja neuvoston asetusten (ETY) N:o 3821/85 ja (EY) N:o 2135/98 muuttamisesta sekä neuvoston asetuksen (ETY) N:o 3820/85 kumoamisesta (ETA:n kannalta merkityksellinen teksti).

[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).

[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).

[6] EN 12253 Road transport and traffic telematics – Dedicated short-range communication – Physical layer using microwave at 5.8 GHz.

▼B

[7] EN 12795 Road transport and traffic telematics – Dedicated short-range communication – Data link layer: medium access and logical link control.

[8] EN 12834 Road transport and traffic telematics – Dedicated short-range communication – Application layer.

[9] EN 13372 Road transport and traffic telematics – Dedicated short-range communication – Profiles for RTTT applications

[10] ISO 14906 Electronic fee collection – Application interface definition for dedicated short – range communication

4 TOIMINTASKENAARIOT

4.1 **Yleistä**

Asetuksessa (EU) 165/2014 säädetään erityisistä ja kontrolloiduista skenaarioista, joissa *yhteyttä* käytetään.

Tuetut skenaariot ovat seuraavat:

”Communication Profile 1: Roadside inspection using a short range wireless communication Remote Early Detection Communication Reader instigating a physical roadside inspection (master-:-slave)

Reader Profile 1a: via a hand aimed or temporary roadside mounted and aimed Remote Early Detection Communication

Reader Profile 1b: via a vehicle mounted and directed Remote Early Detection Communication Reader”.

4.1.1 *5,8 GHz:n DSRC-rajapinnan kautta tapahtuvan tiedonsiirron ennakkoedellytykset*

HUOM. Ennakkoedellytysten asiayhteyden ymmärtämiseksi viitataan jäljempänä olevaan kaavioon 14.3.

4.1.1.1 Ajoneuvoyksikössä olevat tiedot

DSC_12 Ajoneuvoyksikkö vastaa ajoneuvoyksikössä tallennettavien tietojen päivittämisestä 60 sekunnin välein ja niiden ylläpitämisestä DSRC-yhteystoiminnon osallistumatta tähän mitenkään. Keino, jolla tämä toteutetaan, on ajoneuvoyksikön sisäinen, ja se määritellään liitteessä 1 C olevassa 3.19 kohdassa ”*Etäyhteys kohdennettuja tienvarsitarkastuksia varten*”, eikä sitä siksi määritellä tässä lisäyksessä.

4.1.1.2 Ajoneuvoyksikön DSRC-laitteeseen toimitettavat tiedot

DSC_13 Ajoneuvoyksikkö vastaa DSRC-ajopiirturitietojen (*tiedot*) päivittämisestä aina, kun ajoneuvoyksikköön tallennetut tiedot päivitetään 4.1.1.1 kohdassa (DSC_12) määritellyin väliajoin DSRC-yhteystoiminnon osallistumatta tähän mitenkään.

DSC_14 Ajoneuvoyksikön tietoja käytetään *tietojen* täydentämiseen ja päivittämiseen. Keino, jolla tämä toteutetaan, eritellään liitteessä 1 C olevassa 3.19 kohdassa ”*Etäyhteys kohdennettuja tienvarsitarkastuksia varten*”, tai jos tällaista eritelmää ei ole, se riippuu tuotteen suunnittelusta, eikä sitä eritellä tässä lisäyksessä. Ajoneuvoyksikön DSRC-laitteen ja ajoneuvoyksikön välisen yhteyden suunnittelusta ks. 5.6 jakso.

▼B

4.1.1.3 Tietojen sisältö

DSC_15 *Tietojen* sisällön ja muodon on oltava sellaiset, että kun tietojen salaus on avattu, niiden rakenteen sekä muodon, jossa ne asetetaan saataville, on oltava tämän lisäyksen 5.4.4 jakson (Tietorakenteet) mukaisia.

4.1.1.4 Tietojen esitystapa

DSC_16 *Tiedot*, jotka on päivitetty tiheästi 4.1.1.1 kohdassa määriteltyjen menettelyjen mukaisesti, on suojattava ennen niiden esittämistä *ajoneuvoyksikön DSRC-laitteelle* ja esitettävä suojattuna tietokäsitteen arvona, joka tallennetaan väliaikaisesti *ajoneuvoyksikön DSRC-laitteelle tietojen* senhetkisenä versiona. Nämä tiedot siirretään *ajoneuvoyksikön turvamoduulista* DSRC-toiminnon *ajoneuvoyksikön hyötykuormamuistiin*. *Ajoneuvoyksikön turvamoduuli* ja *ajoneuvoyksikön hyötykuormamuisti* ovat toimintoja eivätkä välttämättä fyysisiä yksikköjä. Se fyysinen ilmentymismuoto, jolla nämä toiminnot suoritetaan, riippuu tuotesuunnittelusta, ellei sitä eritellä muualla asetuksessa (EU) N:o 165/2014.165 2014.

4.1.1.5 Tietoturvadata

DSC_17 Tietoturvadata *(securityData)*, joka koostuu tiedoista, jotka REDCR-lukija tarvitsee kyetäkseen avaamaan *tietojen* salauksen, on toimitettava tavalla, joka määritellään lisäyksessä 11 ”Yhteiset turvamekanismit” ja esitettävä tietokäsitteen arvona, joka tallennetaan väliaikaisesti *ajoneuvoyksikön DSRC-laitteelle securityData*-datan sen hetkisenä versiona tämän lisäyksen 5.4.4 jaksossa määritellyssä muodossa.

4.1.1.6 DSRC-rajapinnan kautta siirrettävissä olevat ajoneuvoyksikön hyötykuormamuistin tiedot

DSC_18 Tietokäsite, jonka on kaikkina aikoina oltava saatavilla ajoneuvoyksikön hyötykuormamuistissa siirtämistä varten *REDCR-lukijan* pyynnöstä, määritellään 4.4.5 jaksossa täydellisten ASN.1-moduulieritelmien osalta.

Yleistä yhteysprofiilista 1

Tämä profiili kattaa käyttötapauksen, jossa toimivaltaisten valvontaviranomaisten edustaja käyttää lyhyen kantaman etäyhteytenä toteutetun varhaisen havaitsemisen lukijaa (suosituksen ERC 70-03 mukaisesti käytettävät ja standardin EN 300 674-1 asianmukaisten parametrien mukaan testatut 5,8 GHz:n DSRC-rajapinnat 5 jakson mukaisesti) (*REDCR-lukija*) tunnistaakseen etäyhteyden avulla ajoneuvon, joka saattaa rikkoa asetusta (EU) N:o 165/2014. Kun ajoneuvo on tunnistettu, kyselylaitteistoa käyttävä toimivaltaisten valvontaviranomaisten edustaja päättää, pysäytetäänkö ajoneuvo.

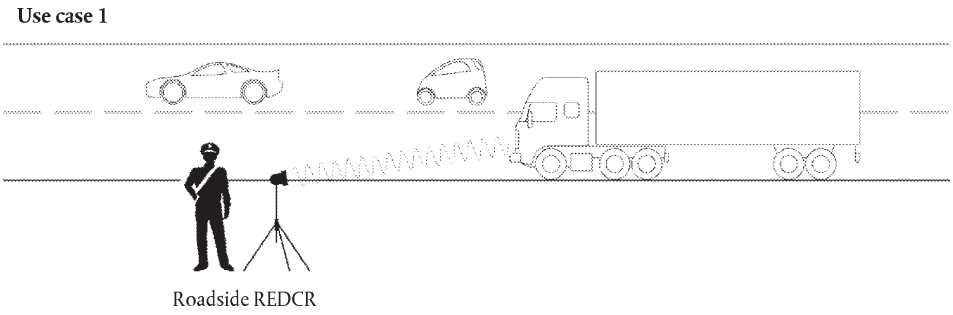
4.1.2 *Profiili 1 a: käsin suunnattavan tai väliaikaisesti tienvarteen asennetun ja suunnatun etäyhteytenä toteutetun varhaisen havaitsemisen lukijan avulla*

Tässä käyttötapauksessa toimivaltaisten valvontaviranomaisten edustaja on sijoittunut tienvarteen ja suuntaa kädessä pidettävän, jalustalle asennetun tai vastaavan kannettavan *REDCR-lukijan* tienvarresta kohti kohteena olevan ajoneuvon tuulilasin keskipistettä. Kysely tehdään suosituksen ERC 70-03 mukaisesti käytettävien ja standardin EN 300 674-1 asianmukaisten parametrien mukaan testattujen 5,8 GHz:n DSRC-rajapintojen avulla 5 jakson mukaisesti. Ks. kaavio 14.1 (käyttötapaus 1)

▼B

Kaavio 14.1

Tienvarressa suoritettava kysely 5,8 GHz:n DSRC-yhteyden avulla

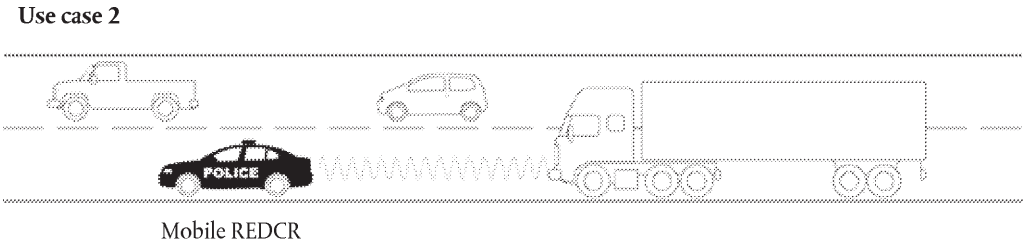


4.1.3 *Profiili 1 b: ajoneuvoon asennetun ja suunnatun etäyhteytenä toteutetun varhaisen havaitsemisen lukijan (RECDR-lukija) avulla*

Tässä käyttötapauksessa toimivaltaisten valvontaviranomaisten edustaja sijaitsee liikkuvassa ajoneuvossa ja joko suuntaa kädessä pidettävän kannettavan *REDCR-lukijan* ajoneuvosta kohti kohteena olevan ajoneuvon tuulilasin keskipistettä tai *REDCR-lukija* on asennettu ajoneuvoon siten, että se osoittaa kohti kohteena olevan ajoneuvon tuulilasin keskipistettä, kun etäyhteytenä toteutetun varhaisen havaitsemisen lukija on tietyssä asennossa kohteena olevaan ajoneuvoon nähden (esimerkiksi suoraan sen edessä liikennevirrassa). Kysely tehdään suosituksen ERC 70-03 mukaisesti käytettävien ja standardin EN 300 674-1 asianmukaisten parametrien mukaan testattujen 5,8 GHz:n DSRC-rajapintojen avulla 5 jakson mukaisesti. Ks. kaavio 14.2 (käyttötapaus 2).

Kaavio 14.2

Ajoneuvosta suoritettava kysely 5,8 GHz:n DSRC-yhteyden avulla



4.2 **Turvallisuus/eheys**

Jotta olisi mahdollista tarkastaa etäyhteyden avulla ladattujen tietojen aitous ja eheys, suojatut *tiedot* tarkistetaan ja niiden salaus avataan lisäyksen 11 (Yhteiset turvamekanismit) mukaisesti.

5 ETÄYHTEYSTOIMINNON SUUNNITTELU JA PROTOKOLLAT

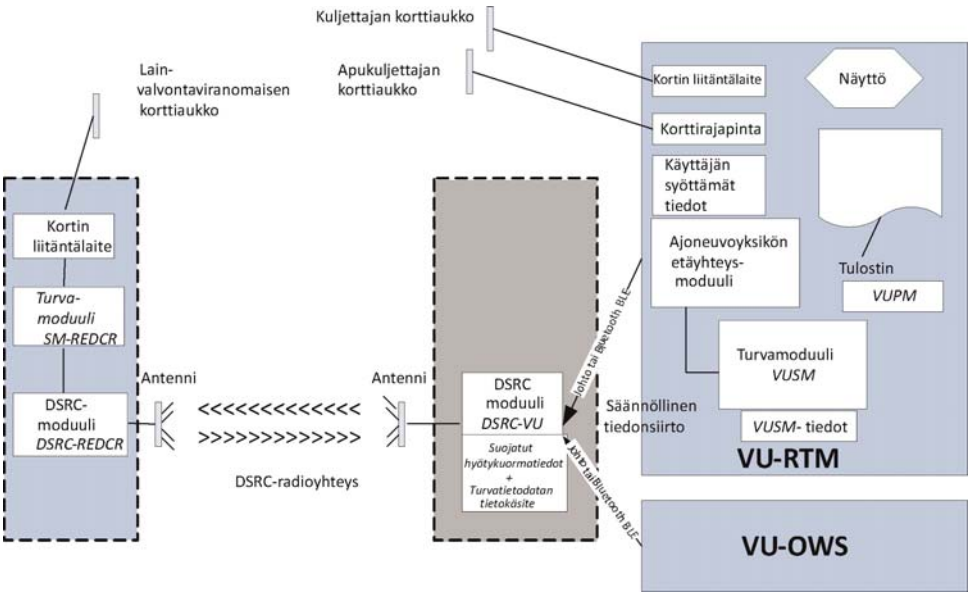
5.1 **Suunnittelu**

Älykkään ajopiirturin etäyhteystoiminnon suunnittelu kuvataan kaaviossa 14.3.

▼B

Kaavio 14.3

Etäyhteystoiminnon suunnittelu



DSC_19 Seuraavat toiminnot sijaitsevat ajoneuvoyksikössä:

— Turvamoduuli (*VUSM*). Tämä ajoneuvoyksikön toiminto suojaa *tiedot*, jotka lähetetään *ajoneuvoyksikön DSRC-laitteesta* etäyhteyden välityksellä toimivaltaisten valvontaviranomaisten edustajalle.

— Suojatut tiedot tallennetaan ajoneuvoyksikön turvamoduulin muistiin. Ajoneuvoyksikkö salaa ja täydentää edellä 4.1.1.1 kohdassa (DSC_12) määritellyin väliajoin ajoneuvoyksikön DSRC-laitteen muistissa olevan RTMData-tietokäsitteen (joka koostuu hyötykuormatiedoista ja jäljempänä tässä lisäyksessä määritellyistä suojausta koskevien tietokäsitteiden arvoista). Turvamoduulin toiminta määritellään asetuksessa lisäyksessä 11 ”Yhteiset turvamekanismit”, ja se kuuluu tämän lisäyksen soveltamisalaan ainoastaan sikäli, että sen on toimitettava päivityksiä ajoneuvoyksikön yhteyslaitteeseen aina, kun ajoneuvon turvamoduulin tiedot muuttuvat.

— Ajoneuvoyksikön ja ajoneuvon DSRC-laitteen välinen yhteys voi olla kaapeliyhteys tai Bluetooth Low Energy (BLE) -yhteys, ja ajoneuvon DSRC-laite voi sijaita fyysisesti antennin yhteydessä ajoneuvon tuulilasissa, ajoneuvon sisällä tai jossain näiden paikkojen välissä.

— Ajoneuvon DSRC-laitteella on oltava kaikkina aikoina luotettava virranlähde. Se, miten laite saa virtansa, on suunnitteluun liittyvä päätös.

— Ajoneuvon DSRC-laitteen muistin on oltava haihtumaton, jotta se säilyttää tiedot ajoneuvoyksikön DSRC-laitteessa silloinkin, kun ajoneuvon virta on kytketty pois päältä.

— Jos ajoneuvoyksikön ja ajoneuvon DSRC-laitteen välinen yhteys muodostetaan BLE-yhteyden avulla ja virtalähteenä on latautumaton akku, ajoneuvon DSRC-laitteen virtalähde on vaihdettava jokaisen määräaikaisen tarkastuksen yhteydessä, ja ajoneuvon DSRC-laitteen valmistaja vastaa siitä,

▼B

että virtalähde on riittävä kestääkseen määräaikaisten tarkastusten väliajan ja mahdollistaa REDCR-lukijan normaalin tietojen saannin koko tämän ajan vioittumatta ja keskeytyksettä.

— Ajoneuvoyksikön RTM-datan hyötykuormamuisti (*VUPM*) Tämä ajoneuvoyksikön toiminto vastaa *tietojen* toimittamisesta ja päivittämisestä. *Tietojen* sisältö. (”TachographPayload”) määritellään jäljempänä 5.4.4/5.4.5 jaksossa ja päivitetään 4.1.1.1 (DSC_12) kohdassa määritellyin väliajoin.

— Ajoneuvoyksikön DSRC-laite. Tämä toiminto, antenniin sisällytettynä tai kytkettynä ja yhteydessä ajoneuvoyksikköön kaapeli- tai langattoman yhteyden (BLE) avulla, säilyttää sen hetkiset tiedot (*VUPM-data*) ja hallinnoi vastausta 5,8 GHz:n DSRC-yhteyden kautta tehtävään kyselyyn. DSRC-laitteen kytkemistä irti tai sen toiminnan häiritsemistä ajoneuvon normaalin käytön aikana pidetään asetuksen (EU) N:o 165/2014 rikkomisena.

— REDCR-lukijan turvamoduuli (*SM-REDCR)* on toiminto, jota käytetään ajoneuvoyksiköstä peräisin olevan datan salauksen avaamiseen ja sen eheyden tarkistamiseen. Keino, jolla tämä toteutetaan, määritellään lisäyksessä 11 ”Yhteiset turvamekanismit”, eikä sitä määritellä tässä lisäyksessä.

— REDCR-lukijan DSRC-toiminto (*DSRC-REDCR-lukija*) muodostuu 5,8 GHz:n lähetin-vastaanottimesta ja siihen liittyvästä laitteistosta ja ohjelmistosta, jotka hallinnoivat *yhteyttä ajoneuvon DSRC-laitteeseen* tämän lisäyksen mukaisesti.

— *DSRC-REDCR-lukija* lähettää kyselyn kohteena olevan *ajoneuvoyksikön DSRC-laitteelle* ja saa *tiedot* (kohteena olevan ajoneuvon sen hetkisen *VUPM-datan*) DSRC-yhteyden kautta sekä käsittelee ja tallentaa saadut tiedot *SM-REDCR*-turvamoduuliinsa.

— *Ajoneuvoyksikön DSRC-laitteen* antenni (antenni) on sijoitettava paikkaan, jossa ajoneuvon ja tienpuoleisen antennin välinen DSCR-yhteys on optimaalinen (yleensä ajoneuvon tuulilasin keskikohta tai sen lähellä noin 1,5-2,2 metrin korkeudessa). Kevyissä ajoneuvoissa antenni on asianmukaista asentaa tuulilasin yläosaan.

— Antennin edessä tai lähellä ei saa olla esineitä (esim. nimikilpiä, tarroja, heijastuksenestokalvoja, aurinkolippoja, lepoasennossa olevia tuulilasinpyyhkimiä), jotka voivat häiritä yhteyttä.

— Antenni on asennettava niin, että sen keskiakseli on suurin piirtein samansuuntainen tienpinnan kanssa.

▼B

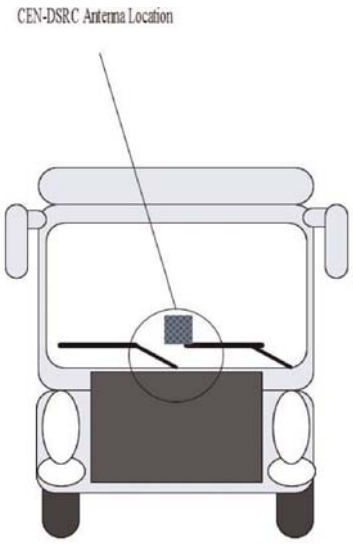
DSC_20 Antennin ja yhteyden on toimittava suosituksen ERC 70-03 mukaisesti testattuna standardin EN 300 674-1 asianmukaisten parametrien mukaan 5 jakson mukaisesti. Antennissa ja yhteydessä voidaan käyttää ECC:n raportissa 228 kuvattuja häiriönlieventämistekniikoita, esimerkiksi suodattimia 5,8 GHz:n CEN-DSRC-yhteydessä.

DSC_21 DSRC-antenni on liitettävä ajoneuvoyksikön DSRC-laitteeseen joko suorasti tuulilasiin tai sen lähelle asennetussa moduulissa tai nimenomaisella johdolla, jonka rakenne tekee laittomasta irti kytkemisestä vaikeaa. Antennin kytkemistä irti tai sen toiminnan häiritsemistä pidetään asetuksen (EU) N:o 165/2014 rikkomisena. Antennin tahallista häirintää tai muuta sen toimintakyvyn alentamista pidetään asetuksen (EU) N:o 165/2014 rikkomisena.

DSC_22 Antennin muotoa ei määritellä, vaan se päätetään kaupallisin perustein, mutta ajoneuvoyksikön asennetun DSRC-laitteen on täytettävä jäljempänä 5 jaksossa määritellyt ohjeidenmukaisuuden vaatimukset. Antenni on sijoitettava kohdassa DSC_19 määritellyllä ja kaaviossa 14.4 esitetyllä tavalla (ympyrä), ja sen on tuettava tehokkaasti 4.1.2 ja 4.1.3 kohdassa kuvattuja käyttötapauksia.

Kaavio 14.4

Esimerkki 5,8 GHz:n DSRC-antennin sijoittamisesta säänneltyjen ajoneuvojen tuulilasiin



REDCR-lukijan ja sen antennin muoto voi vaihdella lukijan ominaisuuksien (jalustalle asennettu, kädessä pidettävä, ajoneuvoon asennettu jne.) sekä toimivaltaisten valvontaviranomaisten edustajan soveltaman toimintatavan mukaan.

Näyttö- ja/tai ilmoitustoimintoa käytetään etäyhteystoiminnon tulosten esittämiseksi toimivaltaisten valvontaviranomaisten edustajalle. Näyttötoiminto voidaan toteuttaa kuvaruudulla, tulosteena, äänimerkkinä tai tällaisten ilmoitusten yhdistelmänä. Tällaisen näyttö- ja/tai ilmoitustoiminnon muoto riippuu toimivaltaisten valvontaviranomaisten edustajien vaatimuksesta ja laitesuunnittelusta, eikä sitä määritellä tässä lisäyksessä.

▼B

DSC_23 *REDCR-lukijan* suunnittelu ja muoto riippuvat kaupallisesta suunnittelusta, suosituksen ERC 70-03 rajoissa, sekä tässä lisäyksessä (5.3.2 jakso) määritellyistä suunnittelua ja suorituskykyä koskevista eritelmistä. Näin markkinoille annetaan mahdollisimman suuri toimintavara suunnitella ja tarjota laitteita, jotka kattavat minkä tahansa toimivaltaisen valvontaviranomaisen erityiset kyselyskenaariot.

DSC_24 *Ajoneuvoyksikön DSRC-laitteen* suunnittelu ja muoto ja sen sijoittaminen ajoneuvoyksikön sisä- tai ulkopuolelle riippuu kaupallisesta suunnittelusta, suosituksen ERC 70-03 rajoissa, sekä tässä lisäyksessä (5.3.2 jakso) ja tässä lausekkeessa (5.1) annetuista suunnittelua ja suorituskykyä koskevista eritelmistä.

DSC_25 *Ajoneuvoyksikön DSRC-laitteen* on kuitenkin kyettävä kohtuullisesti ottamaan vastaan muista älykkäistä ajoneuvolaitteista tulevia tietokäsitteiden arvoja avoimen teollisuusstandardin mukaisten yhteyden ja protokollien avulla (esimerkiksi ajoneuvon sisäisestä punnituslaitteistosta), mikäli tällaiset tietokäsitteet on identifioitu ainutkertaisilla ja tunnetuilla sovellustunnisteilla/tiedostonimillä, ja tällaisten protokollien käyttöä koskevat ohjeet on asetettava Euroopan komission sekä asiaan kuuluvien laitteiden valmistajien saataville maksutta.

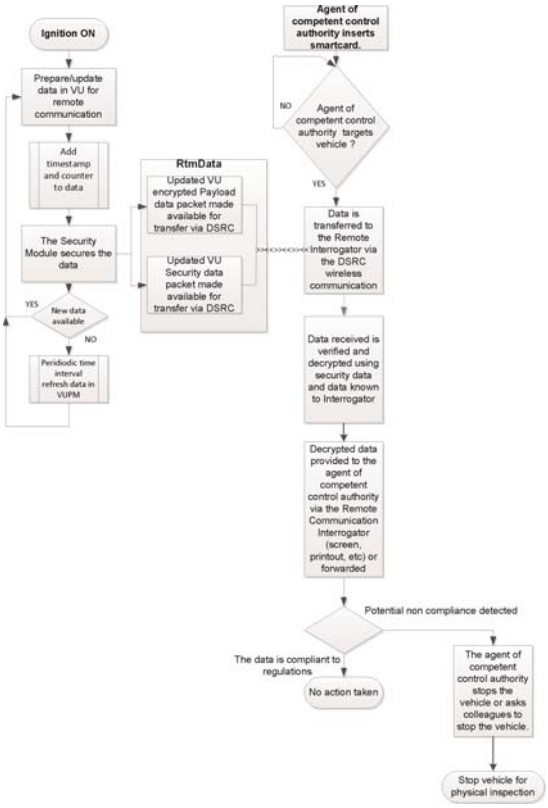
5.2 **Työnkulku**

5.2.1 *Toiminnot*

Toimintojen työnkulku esitetään kaaviossa 14.5. (NOTE: not to be translated)

Kaavio 14.5

Etäyhteystoiminnon työnkulku



▼B

Vaiheet kuvataan seuraavassa:

a. Kun ajoneuvo on käytössä (sytytysvirta on kytketty päälle), ajopiirturi toimittaa tietoja ajoneuvoyksikön toiminnolle. Ajoneuvoyksikön toiminto valmistelee *tiedot* etäyhteystoimintoa varten (salattuina) ja päivittää *ajoneuvoyksikön DSRC-laitteen* muistissa olevan *VUPM-datan* (4.1.1.1–4.1.1.2 kohdan mukaisesti). Kerättyjen *tietojen* muodon on oltava jäljempänä olevien 5.4.4–5.4.5 kohdan mukainen.

b. Aina kun *tiedot* päivitetään, tietoturvadatakäsitteessä määritelty aikaleima on päivitettävä.

c. *VUSM*-toiminto suojaa tiedot lisäyksessä 11 määriteltyjen menettelyjen mukaisesti.

d. Aina kun *tiedot* päivitetään (ks. 4.1.1.1–4.1.1.2 kohta), *tiedot* on siirrettävä *ajoneuvoyksikön DSRC-laitteeseen*, jossa se korvaa aiemmat tiedot, niin että päivitetyt sen hetkiset tiedot (*tiedot*) ovat aina toimitettavissa, jos *REDCR-lukija* lähettää kyselyn. Kun ajoneuvoyksikkö toimittaa *tiedot* ajoneuvoyksikön DSRC-laitteelle, niiden on oltava tunnistettavissa tiedostonimen *RTMData* tai sovellustunnisteen (ApplicationID) ja attribuuttitunnisteiden avulla.

e. Jos toimivaltaisten valvontaviranomaisten edustaja haluaa kohdentaa tarkastuksen tiettyyn ajoneuvoon ja kerätä *tiedot* kohteena olevasta ajoneuvosta, toimivaltaisten valvontaviranomaisten edustajan on ensin syötettävä älykorttinsa *REDCR-lukijaan*, jotta *yhteys* voidaan luoda ja *REDCR-lukijan turvamoduuli* voi todentaa sen aitouden ja avata tietojen salauksen.

f. Toimivaltaisen valvontaviranomaisen edustaja suuntaa tämän jälkeen lukijan ajoneuvoon ja pyytää tietoja etäyhteyden avulla. *REDCR-lukija* avaa 5,8 GHz:n DSRC-rajapinnan avulla istunnon kohdennetun ajoneuvon *ajoneuvoyksikön DSRC-laitteen* kanssa ja pyytää *tietoja*. *Tiedot* siirretään *REDCR-lukijaan* langattoman viestintäjärjestelmän avulla DSRC-attribuuttina käyttäen GET-sovelluspalvelua 5.4 jakson mukaisesti. Attribuutti sisältää salatut hyötytietojen arvot ja DSRC-turvatietodatan.

g. *REDCR*-laite analysoi tiedot, ja ne toimitetaan toimivaltaisen valvontaviranomaisen edustajalle.

h. Toimivaltaisen valvontaviranomaisen edustaja käyttää tietoja apuna päättäessään, pysäyttääkö hän ajoneuvon tarkempaa tarkastusta varten vai pyytääkö hän jotain muuta toimivaltaisen valvontaviranomaisen edustajaa pysäyttämään ajoneuvon.

5.2.2 *DSRC-yhteyden kautta saatujen tietojen tulkinta*

DSC_26 5,8 GHz:n rajapinnan kautta saatujen tietojen on kuljetettava jäljempänä 5.4.4 ja 5.4.5 kohdassa määritelty merkitys ja vain tämä merkitys, ja ne on ymmärrettävä kyseisissä kohdissa määriteltyjen tavoitteiden rajoissa. Asetuksen N:o (EU) 165/2014 säännösten mukaisesti *tietoja* saa käyttää vain merkityksellisten tietojen toimittamiseksi toimivaltaiselle valvontaviranomaiselle, jotta tämä voi päättää, mitkä ajoneuvot olisi

▼B

pysäytettävä fyysistä tarkastusta varten, ja tämän jälkeen ne on poistettava asetuksen N:o (EU) 165/2014 9 artiklan mukaisesti.

5.3 **Fyysisen DSRC-rajapinnan parametrit etäyhteyttä varten**

5.3.1 *Sijaintia koskevat rajoitteet*

DSC_27 Ajoneuvojen etäkyselyä 5,8 GHz:n DSRC-rajapinnan avulla ei tule käyttää 200 metrin säteellä toimintakykyisestä 5,8 GHz.n DSRC-majakasta.

5.3.2 *Vastaanotto- ja lähetysyhteyksien parametrit*

DSC_28 Ajopiirturin etäseurantaan käytettävän laitteiston on oltava suosituksen ERC 70-03 ja jäljempänä taulukoissa 14.1 ja 14.2 määriteltyjen parametrien mukainen ja toimittava niiden mukaisesti.

DSC_29 Jotta varmistetaan yhteensopivuus muiden standardoitujen 5,8 GHz:n DSRC-järjestelmien toiminnallisten parametrien kanssa, ajopiirturin etäseurantaan käytettävän laitteiston on lisäksi oltava standardien EN 12253 ja EN 13372 parametrien mukainen.

Nimittäin:

Taulukko 14.1

▼C2

Vastaanottoyhteyden parametrit

Parametrin numero (Item No.)	Parametri	Arvo (Arvot)	Huomautus
D1	Satelliittimaayhteyksien kantoaaltotaajuudet	REDCR-lukija voi käyttää neljää vaihtoehtoa: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Sisältyy suositukseen ERC 70–03. Tienvarsijärjestelmän täytäntöönpanija voi valita kantoaaltotaajuudet ja ajoneuvoyksikön DSRC-laitteen ei tarvitse tietää niitä. (Yhdenmukainen standardien EN 12253, EN 13372 kanssa)
D1a (*)	Kantoaaltotaajuuden toleranssi	5 ππμ:n puitteissa	(Yhdenmukainen standardin EN 12253 kanssa)
D2 (*)	Tienvarsiyksikön (REDCR-lukija) lähettimen spektrimaski	Sisältyy suositukseen ERC 70–03. REDCR-lukija on luokkaan B,C kuuluva laite standardin EN 12253 mukaisesti. Tähän liitteeseen ei sisälly muuta erityistä vaatimusta	Parametri, jota käytetään häiriöiden valvomiseen kyselylaitteiden välillä lähialueella (kuten määritellään standardeissa EN 12253 ja EN 13372).
D3	Ajoneuvoon asetetun laitteen (ajoneuvoyksikön DSRC-laite) vähimmäistaajuusalue	5,795–5.815,GHz	(Yhdenmukainen standardin EN 12253 kanssa)
D4 (*)	Suurin EIRP-teho	Sisältyy suositukseen ERC 70–03 (ilman lupaa) ja kansallisiin säännöksiin. Korkeintaan +33 dBm	(Yhdenmukainen standardin EN 12253 kanssa)

▼C2

Parametrin numero (Item No.)	Parametri	Arvo (Arvot)	Huomautus
D4a	Kulmikas EIRP-maski	Kyselylaitteen suunnittelijan ilmoittaman ja julkaiseman eritelmän mukaisesti	(Yhdenmukainen standardin EN 12253 kanssa)
D5	Polarisaatio	Vastapäiväinen, ympyränmuotoinen	(Yhdenmukainen standardin EN 12253 kanssa)
D5a	Ristipolarisaatio	XPD: Keskilinjalla: RSU (REDCR-lukija) t ≥ 15 δB Ajoneuvoon asetetun laitteen (ajoneuvoyksikön DSRC-laite) r ≥ 10 δB -3 dB alue: Tievarsiyksikkö (REDCR-lukija) t ≥ 10 δB Ajoneuvoon asetetun laitteen (ajoneuvoyksikön DSRC-laite) r ≥ 6 δB	(Yhdenmukainen standardin EN 12253 kanssa)
D6 (*)	Modulaatio	Amplitudimodulaatio kahdella tasolla	(Yhdenmukainen standardin EN 12253 kanssa)
D6a (*)	Modulaatioindeksi	0,5 ... 0,9	(Yhdenmukainen standardin EN 12253 kanssa)
D6b	Silmäkuvio	≥ 90 % (aika) / ≥ 85 % (amplitudi)	
D7 (*)	Datan koodaus	FM0 Bitti ”1” muuttuu ainoastaan bittivälin alussa ja lopussa. Bitti ”0” muuttuu myös bittivälin keskellä verrattuna ”1”-bittiin.	(Yhdenmukainen standardin EN 12253 kanssa)
D8 (*)	Bittinopeus	500 kBit/s	(Yhdenmukainen standardin EN 12253 kanssa)
D8a	Bittikellon toleranssi	parempi kuin 100 ppm	(Yhdenmukainen standardin EN 12253 kanssa)
D9 (*)	Bittivirhesuhde (B.E.R) kommunikoinnissa	≤ 10^{-6} jos ajoneuvoon asetetun laitteen (ajoneuvoyksikön DSRC-laite) tulosignaaliteho on välillä [D11a–D11b].	(Yhdenmukainen standardin EN 12253 kanssa)
D10	Ajastin (wake-up trigger), joka herättää ajoneuvoon asetetun laitteen (ajoneuvoyksikön DSRC-laite)	Ajoneuvoon asetettu laite (ajoneuvoyksikön DSRC-laite) herää vastaanotettuaan vähintään 11 oktetin kehyksen (mukaan lukien alustus).	Herätystä varten ei tarvita erityistä rakennetta. Ajoneuvoyksikön DSRC-laite voi herätä vastaanotettuaan alle 11 oktetin kehyksen (Yhdenmukainen standardin EN 12253 kanssa)
D10a	Aloitusajan enimmäisarvo	≤ 5 ms	(Yhdenmukainen standardin EN 12253 kanssa)
D11	Viestintävyöhyke	Alue, jonka sisällä saavutetaan parametrin D9a mukainen bittivirhesuhde	(Yhdenmukainen standardin EN 12253 kanssa)
D11a (*)	Tehoraja viestinnälle (ylempi).	-24dBm	(Yhdenmukainen standardin EN 12253 kanssa)

▼C2

Parametrin numero (Item No.)	Parametri	Arvo (Arvot)	Huomautus
D11b (*)	Tehoraja viestinnälle (alempi).	Tulosignaaliteho: -43 dBm (keskilinjalla) -41 dBm (-45° – +45° puitteissa, joka vastaa tienpinnan kanssa yhdensuuntaista pitkittäistä tasoa, kun ajoneuvoyksikön DSRC-laite asennetaan myöhemmin ajoneuvoon (suuntakulma))	(Yhdenmukainen standardin EN 12253 kanssa) Laajennettu vaatimus korkeintaan ± 45° vaakakulmille tässä lisäyksessä määriteltyjen käyttötapausten vuoksi.
D12 (*)	Ajoneuvoyksikön DSRC-laitteen tehon katkaisun taso	-60 dBm	(Yhdenmukainen standardin EN 12253 kanssa)
D13	Alustus (preamble)	Alustus on pakollinen.	(Yhdenmukainen standardin EN 12253 kanssa)
D13a	Alustuksen pituus ja rakenne	16 bittiä ± 1 bitti FM0-koodattuna bittinä ”1”	(Yhdenmukainen standardin EN 12253 kanssa)
D13b	Alustuksen aaltomuoto	Matalan ja korkean tason vaihtuva sarja, jonka pulssin pituus on 2 μs. Aaltotaajuus annetaan parametrissa D8a	(Yhdenmukainen standardin EN 12253 kanssa)
D13c	Ylimääräiset bitit	(REDCR-lukija) voi lähettää enintään 8 bittiä lopputunnuksen jälkeen. Ajoneuvoon asetetun laitteen (ajoneuvoyksikön DSRC-laite) ei tarvitse ottaa näitä ylimääräisiä bittejä huomioon.	(Yhdenmukainen standardin EN 12253 kanssa)

(*) – Lähetysyhteyden parametri, johon sovelletaan vaatimustenmukaisuuden testausta standardin EN 300 674–1 asiaankuuluvan parametritestauksen mukaisesti.

▼B

Taulukko 14.2

▼C2

Lähetysyhteyden parametrit

Parametrin numero (Item No.)	Parametri	Arvo (Arvot)	Huomautus
U1 (*)	Apukantoaallon taajuudet	Ajoneuvoon asetettu laite (ajoneuvoyksikön DSRC-laite) tukee taajuutta 1,5 MHz ja 2,0 MHz Tienvarsiyksikkö (REDCR-lukija) tukee taajuutta 1,5 MHz tai 2.0 MHz tai kumpaakin. U1-0: 1,5 MHz U1-1: 2,0 MHz	Apukantoaallon taajuuden valinta (1,5 MHz tai 2,0 MHz) valitusta standardin EN 13372 profiilista riippuen.
U1a (*)	Apukantoaallon toleranssi	seuraavan puitteissa 0.1%	(Yhdenmukainen standardin EN 12253 kanssa)
U1b	Sivukaistojen käyttö	Samat tiedot kummallakin sivukaistalla	(Yhdenmukainen standardin EN 12253 kanssa)
U2 (*)	Ajoneuvoon asetetun laitteen (ajoneuvoyksikön DSRC-laite) lähettimen spektrimaski	Standardin EN 12253 mukaisesti 1) Teho kaistan ulkopuolella (out band power): ks. ETSI EN 300674–1	(Yhdenmukainen standardin EN 12253 kanssa)

▼C2

Parametrin numero (Item No.)	Parametri	Arvo (Arvot)	Huomautus
		2) Teho kaistan sisäpuolella (in band power): [U4a] dBm 500 kHz:ssä 3) Lähetys millä tahansa muulla lähetyskanavalla: U2(3)-1 = -35 dBm 500 kHz:ssä	
U4a (*)	Suurin EIRP-teho – yksisivukaistainen (Maximum Single Side Band E.I.R.P.) (keskilinjalla)	Kaksi vaihtoehtoa: U4a-0: -14 dBm U4a-1: -21 dBm	Laitteen suunnittelijan ilmoitetun ja julkaistun eritelmän mukaisesti
U4b (*)	Suurin EIRP-teho – yksisivukaistainen (35^0)	Kaksi vaihtoehtoa: Ei sovelleta -17dBm	Laitteen suunnittelijan ilmoitetun ja julkaistun eritelmän mukaisesti
U5	Polarisaatio	Vastapäiväinen, ympyränmuotoinen	(Yhdenmukainen standardin EN 12253 kanssa)
U5a	Ristipolarisaatio	XPD: Keskilinjalla: Tienvarsiyksikkö (REDCR-lukija) r 15 δB Ajoneuvoon asetettu laite (ajoneuvoyksikön DSRC-laite) t 10 δB -3 dB: Tienvarsiyksikkö (REDCR-lukija) r 10 δB Ajoneuvoon asetettu laite (ajoneuvoyksikön DSRC-laite) t 6 δB	(Yhdenmukainen standardin EN 12253 kanssa)
U6	Apukantoaallon modulaatio	2-PSK Koodattu data synkronoidaan apukantoaallon kanssa: koodatun datan muuntaminen tapahtuu samaan aikaan apukantoaallon muuntamisen kanssa.	(Yhdenmukainen standardin EN 12253 kanssa)
U6b	Käyttöjakso	Käyttöjakso: 50 % ± α, α ≤ 5 %	(Yhdenmukainen standardin EN 12253 kanssa)
U6c	Kantoaallon modulointi	Moduloidun apukantoaallon monistaminen kantoaallon kanssa	(Yhdenmukainen standardin EN 12253 kanssa)
U7 (*)	Datan koodaus	NRZI (Ei muutosta bitin ”1” alussa, muutos bitin ”0” alussa, ei muutosta bitissä)	(Yhdenmukainen standardin EN 12253 kanssa)
U8 (*)	Bittinopeus	250 kbit/s	(Yhdenmukainen standardin EN 12253 kanssa)
U8a	Bittikellon toleranssi	Seuraavan puitteissa: 100 ππμ	(Yhdenmukainen standardin EN 12253 kanssa)
U9	Viestinnän bittivirhesuhde	$\leq 10^{-6}$	(Yhdenmukainen standardin EN 12253 kanssa)

▼C2

Parametrin numero (Item No.)	Parametri	Arvo (Arvot)	Huomautus
U11	Viestintävyöhyke	Alue, jonka sisällä ajoneuvoyksikön DSRC-laite sijaitsee siten, että REDCR-lukija vastaanottaa sen lähetyksiä ja bittivirhesuhde on pienempi kuin parametrissa U9a.	(Yhdenmukainen standardin EN 12253 kanssa)
U12a (*)	Muuntovahvistus (alaraja)	1 dB kummallekin sivukaistalle Kulman laajuus: ympyräsymmetrinen keskilinjan ja ± 35° välissä sekä	
		-45° – +45° puitteissa, joka vastaa tienpinnan kanssa yhdensuuntaista pitkittäistä tasoa, kun ajoneuvoyksikön DSRC-laite asennetaan myöhemmin ajoneuvoon (suuntakulma)	Suurempi kuin määritelty arvoalue korkeintaan ± 45° vaakakulmille, kun otetaan huomioon tässä lisäyksessä määritellyt käyttötapaukset.
U12b (*)	Muuntovahvistus (yläraja)	10 dB kummallekin sivukaistalle	Vähempi kuin määritelty arvoalue kullekin sivukaistalle ympyräkartion sisällä, joka sijaitsee keskiakselin ympärillä, jolla on ± 45° avautumiskulma
U13	Alustus (preamble)	Alustus on pakollinen.	(Yhdenmukainen standardin EN 12253 kanssa)
U13a	Alustus (preamble) Pituus ja merkkijono	32–36 µs, pelkästään apukantoaallolla moduloitu, sen jälkeen 8 bittiä NRZ-koodauksen tilassa ”0” bittiä.	(Yhdenmukainen standardin EN 12253 kanssa)
U13b	Ylimääräiset bitit	Ajoneuvoyksikön DSRC-laite voi lähettää enintään 8 bittiä lopputunnuksen jälkeen. Tienvarsiyksikön (REDCR-lukija) ei tarvitse ottaa näitä ylimääräisiä bittejä huomioon.	(Yhdenmukainen standardin EN 12253 kanssa)

(*) – Lähetysyhteyden parametri, johon sovelletaan vaatimustenmukaisuuden testausta standardin EN 300 674–1 asiaankuuluvan parametritestauksen mukaisesti.

▼B

5.3.3 *Antennin suunnittelu*

5.3.3.1 REDCR-lukijan antenni

DSC_30 *REDCR-lukijan* antennin suunnittelu, joka määräytyy kaupallisen päätöksen mukaan 5.3.2 kohdassa määritellyissä rajoissa, mukautetaan optimoimaan *DSRC-REDCR-lukijan* lukukyky siinä tarkoituksessa ja niissä lukuolosuhteissa, joissa *REDCR-lukija* on suunniteltu toimimaan.

5.3.3.2 Ajoneuvoyksikön antenni

DSC_31 Ajoneuvoyksikön DSRC-laitteen antennin suunnittelu, joka määräytyy kaupallisen päätöksen mukaan 5.3.2 jaksossa määritellyissä rajoissa, mukautetaan optimoimaan DSRC-REDCR-lukijan lukukyky siinä tarkoituksessa ja niissä lukuolosuhteissa, joissa REDCR-lukija on suunniteltu toimimaan.

▼B

DSC_32 Ajoneuvoyksikön antenni kiinnitetään ajoneuvon etutuulilasiin tai sen lähelle edellä 5.1 jakson mukaisesti.

DSC_33 Korjaamon testausympäristössä (ks. 6.3 jakso) edellä olevan 5.1 jakson mukaisesti kiinnitetyn ajoneuvoyksikön DSRC-laitteen antennin on luotava onnistunut vakiomuotoinen testausyhteys ja suoritettava onnistunut tässä lisäyksessä määritelty RTM-tietojen siirto 2–10 metrin etäisyydeltä yli 99 prosentin onnistumisprosentilla keskiarvona yli 1 000 kyselystä.

5.4 **DSRC-protokollan vaatimukset ajopiirturin etäseurantaa varten**

5.4.1 *Yleistä*

DSC_34 *Tietojen* lataamiseen 5,8 GHz:n DSRC-rajapinnan kautta käytettävässä siirtoprotokollassa on noudatettava seuraavia vaiheita. Tässä jaksossa kuvataan siirron kulku ihanteellisissa olosuhteissa ilman uudelleenlähetyksiä tai yhteyskatkoksia.

HUOM. Alustusvaiheen (vaihe 1) tarkoituksena on luoda yhteys *REDCR-lukijan* ja sellaisten ajoneuvojen DSRC-laitteiden välille, jotka ovat siirtyneet 5,8 GHz:n (isäntä-renki) DSRC-siirtotilaan mutta eivät vielä luoneet yhteyttä *REDCR-lukijaan*, sekä ilmoittaa sovellusprosessit.

— **Vaihe 1** Alustus. *REDCR-lukija* lähettää kehyksen, joka sisältää ”lähettimen palvelutaulukon” (BST), jossa on sovellustunnisteet (AID) sen tukemassa palveluluettelossa. RTM-sovelluksessa tämä on yksinkertaisesti palvelu, jonka AID-arvo = 2 (Freight&Fleet). *Ajoneuvoyksikön DSRC-laite* arvioi saadun BST:n ja vastaa (ks. jäljempänä) luettelolla Freight&Fleet-alueella tuettujen sovellusten luettelolla tai jättää vastaamatta, jos mitään sovelluksia ei tueta. Jos *REDCR-lukija* ei tarjoa arvoa AID=2, ajoneuvoyksikön DSRC-laite ei vastaa sille.

— **Vaihe 2** *Ajoneuvoyksikön DSRC-laite* lähettää kehyksen, joka sisältää pyynnön yksityisen ikkunan osoittamisesta.

— **Vaihe 3** *REDCR-lukija* lähettää kehyksen, joka sisältää pyynnön yksityisen ikkunan osoittamisesta.

— **Vaihe 4** *Ajoneuvoyksikön DSRC-laite* käyttää osoitettua yksityistä ikkunaa ja lähettää kehyksen, joka sisältää sen ajoneuvon palvelutaulukon (VST). VST sisältää luettelon kaikista tämän *ajoneuvoyksikön DSRC-laitteen* AID=2-kehyksessä tukemista eri sovellusilmentymistä. Eri ilmentymät on yksilöitävä erikseen tuotettavilla osien tunnisteilla (EID), joista jokaiseen liittyy sovelluskontekstitunnus-parametrin arvo, joka ilmaisee sovelluksen ja tuetun standardin.

— **Vaihe 5** Seuraavaksi *REDCR-lukija* analysoi tarjotun VST:n ja joko päättää yhteyden (RELEASE), koska se ei ole kiinnostunut mistään, mitä VST tarjoaa (eli se saa VST:n sellaisesta *ajoneuvoyksikön DSRC-laitteesta*, joka ei tue RTM-tapahtumaa), tai, jos se saa asianmukaisen VST:n, käynnistää sovellusilmentymän.

▼B

— **Vaihe 6** Tämän aikaan saamiseksi REDCR-lukijan lähettää kehyksen, joka sisältää komennon noutaa RTM-data ja joka yksilöi RTM-sovellusilmentymän yksilöimällä sitä vastaavan tunnisteen (jonka ajoneuvoyksikön DSRC-laite on yksilöinyt VST:ssä), ja osoittaa yksityisen ikkunan.

— **Vaihe 7** *Ajoneuvoyksikön DSRC-laite* käyttää nyt osoitettua yksityistä ikkunaa ja lähettää kehyksen, joka sisältää VST:ssä ilmoitettua RTM-sovellusilmentymää vastaavan osoitteellisen tunnisteen, ja tämän jälkeen *RtmData*-attribuutin (hyötytieto-osa + turvatieto-osa).

— **Vaihe 8** Jos pyyntö koskee useita palveluja, arvo ‘n’ vaihtuu seuraavaksi palvelun viitenumeroksi ja prosessi toistetaan.

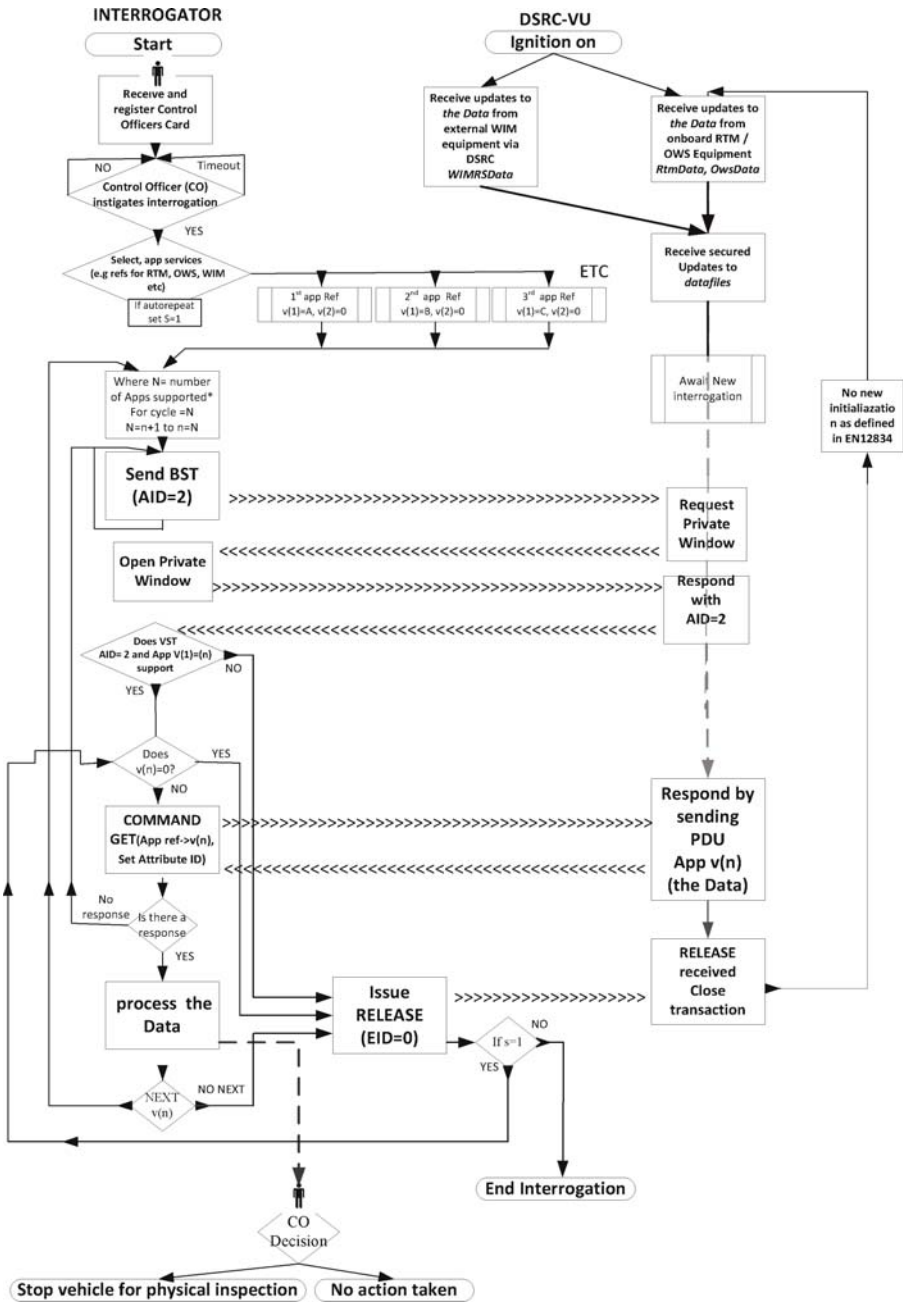
— **Vaihe 9** *REDCR-lukija* vahvistaa tietojen vastaanoton lähettämällä kehyksen, joka sisältää RELEASE-komennon *ajoneuvoyksikön DSRC-laitteelle* istunnon päättämiseksi, TAI, jos se ei pysty vahvistamaan LPDU-datayksikön vastaanoton onnistumista, palaa vaiheeseen 6.

Kaaviossa 14.6 esitetään tapahtumaprotokolla kuvana.

▼B

Kaavio 14.6

Vuokaavio ajopiirturin etäseurannasta 5,8 GHz:n DSRC-yhteyden avulla



5.4.2 *Komennot*

DSC_35 Seuraavat komennot ovat ainoat RTM-tapahtumassa käytettävät toiminnot:

— **INITIALISATION.request**: RECDR-lukijan lähetyksen muodossa antama komento, jossa määritellään REDCR-lukijan tukemat sovellukset.

— **INITIALISATION.response**: Ajoneuvoyksikön DSRC-laitteen antama vastaus, jolla vahvistetaan yhteyden muodostaminen ja joka sisältää luettelon tuetuista sovelluksista ja niiden ominaisuuksista sekä tiedot siitä, miten ne osoitetaan (EID).

▼B

— **GET.request**: *REDCR-lukijan ajoneuvoyksikön DSRC-laitteelle* antama komento, jolla yksilöidään osoitettava sovellusilmentymä VST:stä saadun määritellyn EID:n avulla ja käsketään *ajoneuvoyksikön DSRC-laitetta* lähettämään valittu attribuutti tai attribuutit *tietojen* mukana. GET-komennon tarkoituksena on, että *REDCR-lukija* saa *tiedot ajoneuvoyksikön DSRC-laitteelta*.

— **GET.response**: Ajoneuvoyksikön DSRC-laitteen antama vastaus, joka sisältää pyydetyt *tiedot*.

— **ACTION.request ECHO**: Komento, jolla käsketään *ajoneuvoyksikön DSRC-laitteen* lähettää tiedot *ajoneuvoyksikön DSRC-laitteelta* takaisin *REDCR-lukijaan*. ECHO-komennon tarkoituksena on antaa korjaamoille tai tyyppihyväksyntätestauslaitoksille mahdollisuus testata DSRC-yhteyden toimivuus ilman tietoturvavaltuuksia.

— **ACTION**.response ECHO: Ajoneuvoyksikön vastaus ECHO-komentoon.

— **EVENT_REPORT.request** RELEASE: Komento, joka kertoo *ajoneuvoyksikön DSRC-laitteelle*, että tapahtuma on päättynyt. RELEASE-komennon tarkoituksena on päättää istunto *ajoneuvoyksilön DSRC-laitteen* kanssa. Saatuaan RELEASE-komennon *ajoneuvoyksikön DSRC-laite* ei enää vastaa uusiin kyselyihin sen hetkisen yhteyden aikana. On syytä huomata, että standardin EN 12834 mukaan ajoneuvoyksikön DSRC-laite ei ota yhteyttä kahdesti samaan kyselylaitteeseen, ellei se ole ollut pois yhteystilasta 255 sekunnin ajan tai kyselylaitteen lähettimen tunniste vaihtuu.

▼C2

5.4.3 *Kyselykomentosarja*

DSC_36 Komento- ja vastaussarjan näkökulmasta tapahtuma voidaan kuvata seuraavasti:

Sarja	Lähettäjä		Vastaanottaja	Kuvaus	Toiminto
1	REDCR	>	DSRC-VU	Viestintäyhteyden aloittaminen – Pyyntö	REDCR lähettää BST:n
2	*DSRC-VU*	>	*REDCR*	*Viestintäyhteyden aloittaminen – Vastaus*	*Jos BST tukee AID = 2:a, DSRC-VU pyytää yksityisen ikkunan*
3	REDCR	>	DSRC-VU	Yksityisen ikkunan osoittaminen	Lähettää yksityisen ikkunan osoituksen sisältävän kehyksen
4	*DSRC-VU*	>	*REDCR*	*VST:n lähetys*	*Lähettää VST:n sisältävän kehyksen*
5	REDCR	>	DSRC-VU	Erityisen EID:n attribuuttiin sialtyviä tietoja koskevan GET.request-komennon lähetys	
6	*DSRC-VU*	>	*REDCR*	*GET.response-komennon lähetys pyydetyn erityisen EID:n attribuutin kanssa*	*Lähettää attribuutin (RTMData, OWSData...) erityistä EID:a koskevien tietojen kanssa*

▼C2

Sarja	Lähettäjä		Vastaanottaja	Kuvaus	Toiminto
7	REDCR	>	DSRC-VU	Muuta attribuuttia koskevan GET.request-tietopyynnön lähetys (soveltuvin osin)	
8	*DSRC-VU*	>	*REDCR*	*GET.response-komennon lähetys pyydetyn attribuutin kanssa*	*Lähettää attribuutin erityistä EID:a koskevien tietojen kanssa*
9	REDCR	>	DSRC-VU	Tietojen onnistunut vastaanotto	Lähettää RELEASE-komennon, joka päättää tapahtuman
10	*DSRC-VU*			*Tapahtuman päättäminen*	

Esimerkki tapahtumasarjasta ja vaihdettujen kehysten sisällöistä määritellään lausekkeissa 5.4.7 ja 5.4.8.

▼B

5.4.4 *Tietorakenteet*

DSC_37 Kun *tiedot* siirretään 5,8 GHz:n DSRC-rajapinnan kautta, niiden semanttisen rakenteen on oltava tässä lisäyksessä kuvatun mukainen. Näiden tietojen rakenne määritellään tässä lausekkeessa.

DSC_38 Hyötykuormatiedot (RTM-data) muodostuvat seuraavien dataelementtien ketjutuksesta:

1. EncryptedTachographPayload-data, joka on TachographPayload-datan 5.4.5 jaksossa määritelty ASN.1-standardin mukainen salaus. Salausmenetelmä on kuvattu lisäyksessä 11.

2. DSRCSecurityData, joka määritellään lisäyksessä 11.

DSC_39 RTM-data osoitetaan RTM-attribuuttina=1 ja siirretään RTM-säiliössä=10.

DSC_40 RTM-kontekstitunnus tuetun TARV-standardisarjan osan (RTM vastaa osaa 9).

ASN.1-moduulin mukainen DSRC-datan määritelmä RTM-sovelluksessa on seuraava:

▼B

```
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)
```

▼B

```
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-elementit, suoritetut toiminnot ja määritelmät*

DSC_41 Tietoyksikköjen arvot, jotka ajoneuvoyksikkö laskee ja joita käytetään ajoneuvoyksikön DSRC-laitteessa olevien suojattujen tietojen päivittämiseen, lasketaan taulukossa 14.3 määriteltyjen sääntöjen mukaisesti:

Taulukko 14.3

▼C2

RtmData-elementit, suoritetut toiminnot ja määritelmät

(1) RTM-datan rakenne	(2) Ajoneuvoyksikön suorittama toiminto		(3) ASN.1-tietojen määrittely
RTM1 **Ajoneuvon rekisterikilpi**	Ajoneuvoyksikkö asettaa RTM1- tietoelementin *tp15638VehicleRegistrationPlate* arvon datatyypin *VehicleRegistrationIdentification* tallennetun arvon perusteella, kuten määritetään lisäyksessä 1 *VehicleRegistrationIdentification*	Ajoneuvon rekisteröintikilpi ilmaistaan merkkijonona	`tp15638VehicleRegstrationPlate LPN, --Ajoneuvon rekisteröintikilpi on peräisin standardista ISO 14906 standardissa EN 15509 määritetyn rajoituksen huomioon ottaen, mikä on SARJA, johon sisältyy maakoodi, jota seuraa aakkostunnus ja sen jälkeen kilven numero; siihen sisältyy aina 14 oktettia (johon kuuluu täytenollia), joten standardissa EN 15509 rekisterikilven numeron pituus on aina 17 oktettia, joista 14 on "todellisen" kilven numeroa.`
RTM2 **Ylinopeustapaus (Speeding Event)**	Ajoneuvoyksikkö asettaa loogisen arvon datatyypille RTM2 tp15638SpeedingEvent. Ajoneuvoyksikkö laskee muuttujan tp15638SpeedingEvent arvon ajoneuvoyksikköön rekisteröityjen ylinopeustapausten lukumäärästä 10 viimeisimmältä päivältä, jolloin tapahtumia sattui, kuten liitteessä 1 C määritetään.	1 (TRUE) – osoittaanopeuksiin liittyvät epäsään nöllisyydet 10 viimeisimmältä päivältä, jolloin tapahtumia sattui	`tp15638speedingEvent BOOLEAN,`

▼C2

(1) RTM-datan rakenne	(2) Ajoneuvoyksikön suorittama toiminto		(3) ASN.1-tietojen määrittely
	Jos edellisen 10 päivän aikana on ainakin yksi tp15638SpeedingEvent -tapahtuma, muuttujan tp15638SpeedingEvent arvoksi asetetaan TRUE. MUUSSA TAPAUKSESSA, jos edellisen 10 päivän aikana ei ole yhtään tapahtumaa, muuttujan tp15638SpeedingEvent arvoksi asetetaan FALSE.		

RTM3
 	
Ajo ilman voimassa olevaa korttia (Driving Without Valid Card)
	Ajoneuvoyksikkö asettaa loogisen arvon datatyypille RTM3
	
	tp15638DrivingWithoutValidCard.
	
	Ajoneuvoyksikkö asettaa loogisen arvon ”True” muuttujalle tp15638DrivingWithoutValidCard, jos ajoneuvoyksikön tietoihin on kirjattu edellisen 10 päivän ajalta ainakin yksi tapahtuma tyyppiä ”Ajo ilman asianmukaista korttia”, kuten liitteessä 1 C määritetään.
	
	MUUSSA TAPAUKSESSA, jos edellisten 10 päivän aikana ei ole yhtään tapahtumaa, muuttujan tp15638DrivingWithoutValidCard arvoksi asetetaan FALSE.
		1 (TRUE) = osoittaa,että korttia on käytetty väärin	`tp15638DrivingWithoutValidCard`
			
			`BOOLEAN,`

RTM4 **Voimassa oleva kuljettajakortti (Valid Driver Card)**	Ajoneuvoyksikkö asettaa loogisen arvon datatyypille RTM4 tp15638DriverCard ajoneuvoyksikköön kirjatun datan perusteella ja lisäyksen 1 määritelmän mukaisesti. Jos mitään voimassa olevaa korttia ei ole, ajoneuvoyksikkö asettaa muuttujaksi TRUE MUUSSA TAPAUKSESSA, jos on voimassa oleva kuljettajakortti, ajoneuvoyksikkö asettaa muuttujaksi FALSE	0 (FALSE) = osoittaa voimassa olevan kuljettajakortin	`tp15638DriverCard` `BOOLEAN,`
RTM5 **Kortin paikoilleen asettaminen ajon aikana (Card Insertion while Driving)**	Ajoneuvoyksikkö asettaa loogisen arvon datatyypille RTM5 Ajoneuvoyksikkö asettaa arvon TRUE muuttujalle tp15638CardInsertion, jos ajoneuvoyksikkö on kirjannut edellisten 10 päivän ajalta ainakin yhden tapahtuman tyyppiä ”Kortin paikoilleen asettaminen ajon aikana”, liitteen 1 C määritelmän perusteella. MUUSSA TAPAUKSESSA, jos edellisten 10 päivän aikana ei ole yhtään tapahtumaa, muuttujan tp15638CardInsertion arvoksi asetetaan FALSE.	1 (TRUE) = osoittaa, että kortti on asetettu paikoilleen ajon aikana10 viimeisimmän päivän aikana, jolloin tapauksia sattui	`tp15638CardInsertion` `BOOLEAN,`
RTM6 **Virhe liikedatassa (Motion Data Error)**	Ajoneuvoyksikkö asettaa loogisen arvon datatyypille RTM6 Ajoneuvoyksikkö asettaa arvon TRUE muuttujalle tp15638MotionDataError, jos ajoneuvoyksikkö on kirjannut edellisten 10 päivän ajalta ainakin yhden tapahtuman tyyppiä ”Virhe liikedatassa”, liitteen 1 C määritelmän mukaisesti. MUUSSA TAPAUKSESSA, jos edellisten 10 päivän aikana ei ole yhtään tapahtumaa, muuttujan tp15638MotionDataError arvoksi asetetaan FALSE.	1 (TRUE) = osoittaa virheen liikedatassa 10 viimeisimmän päivän aikana, jolloin tapauksia sattui	`tp15638motionDataError` `BOOLEAN,`

▼C2

(1) RTM-datan rakenne	(2) Ajoneuvoyksikön suorittama toiminto		(3) ASN.1-tietojen määrittely
RTM7 **Ajoneuvon liikeristiriita (Vehicle Motion Conflict)**	Ajoneuvoyksikkö asettaa loogisen arvon datatyypille RTM7 Ajoneuvoyksikkö asettaa arvon TRUE muuttujalle tp15638vehicleMotionConflict, jos ajoneuvoyksikkö on kirjannut edellisten 10 päivän ajalta ainakin yhden tapahtuman tyyppiä ”Ajoneuvon liikeristiriita” (arvo ”0A”H). MUUSSA TAPAUKSESSA, jos edellisten 10 päivän aikana ei ole yhtään tapahtumaa, muuttujan tp15638vehicleMotionConflict arvoksi asetetaan FALSE.	1 (TRUE) = osoittaaliikeristiriidan 10 viimeisimmän päivän aikana, jolloin tapauksia sattui	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Toinen kuljettajakortti (2nd Driver Card)**	Ajoneuvoyksikkö asettaa loogisen arvon datatyypille RTM8 liitteen 1 C perusteella (”kuljettajan päivittäiseen toimintaan liittyvät tiedot” CREW ja CO-DRIVER). Jos ajoneuvoyksikössä on toinen voimassa oleva kuljettajakortti, ajoneuvoyksikkö asettaa muuttujaksi TRUE MUUSSA TAPAUKSESSA, jos ajoneuvoyksikössä ei ole toista voimassa olevaa kuljettajakorttia, ajoneuvoyksikkö asettaa muuttujaksi FALSE	1 (TRUE) = osoittaa, että toinen kuljettajakortti on asennettu	`tp156382ndDriverCard` `BOOLEAN,`
RTM9 **Nykyinen toiminta (Current Activity)**	Ajoneuvoyksikkö asettaa loogisen arvon datatyypille RTM9. Jos nykyinen toiminta kirjataan ajoneuvoyksikössä muuksi toiminnaksi kuin ”DRIVING”, siten kuin liitteessä 1 C määritellään, ajoneuvoyksikkö asettaa muuttujaksi TRUE MUUSSA TAPAUKSESSA, jos nykyinen toiminta ei ole kirjattu ajoneuvoyksikössä toiminnaksi ”DRIVING”, ajoneuvoyksikkö asettaa muuttujaksi FALSE	1 (TRUE) = muu toiminta valittu; 0 (FALSE) = DRIVING valittu	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Edellinen käyttöjakso lopetettu (Last Session Closed)**	Ajoneuvoyksikkö asettaa loogisen arvon datatyypille RTM10. Jos edellistä käyttöjaksoa ei lopetettu oikein liitteessä 1C määritetyllä tavalla, ajoneuvoyksikkö asettaa muuttujaksi TRUE. MUUSSA TAPAUKSESSA, jos edellinen käyttöjakso lopetettiin oikein, ajoneuvoyksikkö asettaa muuttujaksi FALSE	1 (TRUE) = ei ole lopetettu oikein 0 (FALSE) = on lopetettu oikein	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Virransyötön keskeytyminen (Power Supply Interruption)**	Ajoneuvoyksikkö luo kokonaislukuarvon datatyypille RTM11. Ajoneuvoyksikkö asettaa arvon muuttujalle tp15638PowerSupplyInterruption, joka vastaa pisintä virransyötön keskeytymistä, asetuksen (EU) N:o 165/2014 9 artiklan tyypin ”virtakatkos” (”Power supply interruption”) mukaisesti, kuten liitteessä 1C määritetään.	Virransyötön keskeytymisten määrä 10 viimeisimmän päivän aikana, jolloin tapauksia sattui	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

▼C2

(1) RTM-datan rakenne	(2) Ajoneuvoyksikön suorittama toiminto		(3) ASN.1-tietojen määrittely
	MUUSSA TAPAUKSESSA, jos 10 viimeisimmän päivän aikana, jolloin tapauksia sattui, ei ole ollut virransyötön keskeytymistä koskevia tapauksia, kokonaislukuarvoksi asetetaan 0.		
RTM12 **Vika tunnistimessa (Sensor Fault)**	Ajoneuvoyksikkö luo kokonaislukuarvon datatyypille RTM12. Ajoneuvoyksikkö asettaa muuttujalle sensorFault arvoksi — 1 jos tapahtuma tyyppiä ”35”H, vika tunnistimessa (Sensor fault) on kirjattu edellisten 10 päivän aikana, — 2 jos tapahtuma tyyppiä GNSS-vastaanottimen vika (GNSS receiver fault) (joko sisäinen tai ulkoinen, ja enum-arvo on ”51”H tai ”52”H) on kirjattu edellisten 10 päivän aikana. — 3 jos tapahtuma tyyppiä ”53”H, ulkoisen GNSS-laitteiston viestintävika (”53”H External GNSS communication fault), on kirjattu 10 viimeisimmän päivän aikana, jolloin tapauksia sattui. — 4 Jos sekä vika tunnistimessa (Sensor Fault) ja GNSS-vastaanottimen vika (GNSS receiver fault) on kirjattu 10 viimeisimmän päivän aikana, jolloin tapauksia sattui — 5 Jos sekä vika tunnistimessa (Sensor Fault) ja ulkoisen GNSS-laitteiston viestintävika (External GNSS communication fault) on kirjattu 10 viimeisimmän päivän aikana, jolloin tapauksia sattui — 6 Jos sekä GNSS-vastaanottimen vika (GNSS receiver fault) ja ulkoisen GNSS-laitteiston viestintävika (External GNSS communication fault) on kirjattu 10 viimeisimmän päivän aikana, jolloin tapauksia sattui — 7 Jos kaikki kolme tunnistinvikaa on kirjattu 10 viimeisimmän päivän aikana, jolloin tapauksia sattui MUUSSA TAPAUKSESSA se asettaa arvon 0, jos mitään tapahtumaa ei ole kirjattu 10 viimeisimmän päivän aikana	— tunnistinvika yksi oktetti datatermistön mukaisesti	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Ajan asetus (Time Adjustment)**	Ajoneuvoyksikkö luo kokonaislukuarvon (timeReal lisäyksessä 1) datatyypille RTM13 ajan asetukseen liittyvien tietojen olemassaolon perusteella, liitteen 1 C määritelmän mukaisesti. Ajoneuvoyksikkö asettaa arvon ajankohtaan, jolloin sattui viimeisin ajan asetustietoa (”Time Adjustment”) koskeva tapahtuma. MUUSSA TAPAUKSESSA, jos mitään ”Time Adjustment” -tapahtumaa, siten kuin se määritellään liitteessä 1 C, ei ole ajoneuvoyksikön tiedoissa, se asettaa arvoksi 0	Viimeisimmän ajan asetustiedon ajankohta	`tp15638TimeAdjustment` `INTEGER(0..4294967295),`
RTM14 **Tietoturvan murtoyritys (Security Breach Attempt)**	Ajoneuvoyksikkö luo kokonaislukuarvon (timeReal lisäyksessä 1) datatyypille RTM14 tietoturvan murtoyrityksen olemassaolon perusteella siten kuin se määritellään liitteessä 1 C. Ajoneuvoyksikkö asettaa sen kirjaaman viimeisimmän tietoturvan murtoyrityksen ajankohdan arvon.	Viimeisimmän tietoturvan murtoyrityksen ajankohta — Oletusarvo = 0x00FF	`tp15638LatestBreachAttempt` `INTEGER(0..4294967295),`

▼C2

(1) RTM-datan rakenne	(2) Ajoneuvoyksikön suorittama toiminto		(3) ASN.1-tietojen määrittely
	MUUSSA TAPAUKSESSA, jos mitään ”tietoturvan murtoyritys” -tapahtumaa, siten kuin se määritellään liitteessä 1 C, ei ole ajoneuvoyksikön tiedoissa, se asettaa arvoksi 0x00FF		
RTM15 **Viimeisin kalibrointi (Last Calibration)**	Ajoneuvoyksikkö asettaa kokonaislukuarvon (timeReal lisäyksessä 1) datatyypille RTM15 viimeisimpien kalibrointitietojen perusteella, kuten määritetään liitteessä 1 C. Ajoneuvoyksikkö asettaa sen kirjaamien viimeisimmän kahden kalibroinnin (RTM15 ja RTM16) ajankohdan arvot, jotka on kirjattu VuCalibrationData -tietoihin, kuten määritetään lisäyksessä 1. Ajoneuvoyksikkö asettaa RTM15:n arvon viimeisimmän kalibrointitiedon timeReal -arvon perusteella.	Viimeisimpään kalibrointiin liittyvien tietojen aika	`tp15638LastCalibrationData` `INTEGER(0..4294967295),`
RTM16 **Viimeistä edellinen kalibrointi (Previous Calibration)**	Ajoneuvoyksikkö luo kokonaislukuarvon (timeReal lisäyksessä 1) datatyypille RTM16 viimeistä kalibrointia edeltävän kalibroinnin tietojen perusteella MUUSSA TAPAUKSESSA, jos viimeistä edeltävää kalibrointia ei ole, ajoneuvoyksikkö asettaa RTM16:n arvoksi 0.	Viimeistä edeltävän kalibroinnintiedot	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Ajopiirturin yhdistämispäivä (Date Tachograph Connected)**	Ajoneuvoyksikkö luo kokonaislukuarvon (timeReal lisäyksessä 1) datatyypille RTM17. Ajoneuvoyksikkö asettaa arvoksi ajoneuvoyksikön ensiasennuksen ajankohdan. Ajoneuvoyksikkö ottaa nämä tiedot vuCalibrationRecords -tietuesarjan VuCalibrationData -tietueista (lisäys 1), jolloin CalibrationPurpose-muuttuja on: ”03”H	Ajopiirturin yhdistämispäivä	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Nykyinen nopeus (Current Speed)**	Ajoneuvoyksikkö luo kokonaislukuarvon datatyypille RTM18. Ajoneuvoyksikkö asettaa datatyypin RTM16 arvoksi viimeisimmän kirjatun nykyistä nopeutta koskevan tiedon RtmData:n viimeisimmän päivityksen ajankohtana.	Viimeisin kirjattu nykyistä nopeutta koskeva tieto	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Aikaleima (TimeStamp)**	Ajoneuvoyksikkö luo kokonaislukuarvon (timeReal lisäyksessä 1) datatyypille RTM17. Ajoneuvoyksikkö asettaa datatyypin RTM19 arvoksi RtmData:n arvon viimeisimmän päivityksen ajankohtana.	Tämänhetkisen TachographPayload-tietueen aikaleima	`tp15638Timestamp` `INTEGER(0..4294967295),`

▼B

5.4.6 *Tiedonsiirtomekanismi*

DSC_42 REDCR-lukija pyytää alustusvaiheen jälkeen aiemmin määritellyt hyötykuormatiedot, jotka *ajoneuvoyksikön DSRC-laite* sitten siirtää osoitetussa ikkunassa. REDCR-lukija käyttää GET-komentoa tietojen noutamiseen.

▼B

DSC_43 Kaikissa DSRC-vaihdoissa tiedot on koodattava pakkaukseen tarkoitettujen koodaussääntöjen (PER) mukaisesti.

5.4.7 *DSRC-tapahtuman yksityiskohtainen kuvaus*

DSC_44 Alustus suoritetaan lausekkeiden DSC_44–DSC_48 ja taulukoiden14.4–14.9 mukaisesti. Alustusvaiheessa REDCR-lukija aloittaa BST:n (lähettimen palvelutaulukko) sisältävän kehyksen lähettämisen standardin EN 12834 sekä standardin EN 13372, 6.2, 6.3, 6.4 ja 7.1 kohdan mukaisesti seuraavassa taulukossa 14.4 määritellyin asetuksin.

Taulukko 14.4

▼C2

Alustus – BST-kehyksen asetukset

Kenttä	Asetukset
Yhteyden tunniste	Lähetyksen osoite
BeaconId	Standardin EN 12834 mukaisesti
Aika	Standardin EN 12834 mukaisesti
Profiili	Ei liittymää, käytä 0 tai 1
MandApplications	Ei laajennusta, ei EID:tä, ei parametriä, AID = 2 Freight&Fleet
NonMandApplications	Ei ole
ProfileList	Ei laajennusta, profiilien määrä luettelossa = 0
Fragmentoinnin indikaattori (Fragmentation header)	Ei fragmentointia
Siirtokerroksen (2. kerros) asetukset (Layer 2 settings)	Komennon PDU (Command PDU), käyttöliittymäkomento (UI command)

▼B

Käytännön esimerkki taulukossa 14.4 määritellyistä asetuksista sekä bittikoodauksista esitetään seuraavassa taulukossa 14.5.

Taulukko 14.5

▼C2

Alustus – esimerkki BST-kehyksen sisällöstä

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
1	Erote (FLAG)	0111 1110	Alkuerote (Start flag)
2	Lähetyksen tunnus (broadcast IC)	1111 1111	Lähetyksen osoite (broadcast address)
3	MAC-koodin ohjauskenttä (MAC Control Field)	1010 0000	Komennon PDU (Command PDU)
4	LLC-ohjauskenttä (LLC Control field)	0000 0011	Käyttöliittymäkomento (UI command)

▼C2

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
5	Fragmentoinnin indikaattori (Fragmentation header)	1xxx x001	Ei fragmentointia
6	BST	1000	Alustuspyyntö (initialisation request)
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	Ei-pakollisia sovelluksia (NonMand applications) ei ole
		xxx	Valmistajan tunniste (manufacturer Identifier)
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27 bitin tunniste, valmistajan saatavilla
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32 bitin UNIX-reaaliaikainen
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	Ei liittymää. Esimerkkiprofiili 0
17	MandApplications SEQUENCE (SIZE(0..127,...)) OF {	0000 0001	Ei liittymää, pakollisten sovellusten (mandApplications) lukumäärä = 1
18	SEQUENCE {		
	OPTION indicator	0	EID puuttuu
	OPTION indicator	0	Parametri puuttuu
	AID DSRCApplicationEntityID}}	00 0010	Ei liittymää. AID = 2 Freight&Fleet

▼C2

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
19	ProfileList SEQUENCE (0..127,...) OF Profile}	0000 0000	Ei laajennusta, profiilien määrä luettelossa = 0
20	FCS	xxxx xxxx	Kehyspohjainen varmiste (frame check sequence)
21		xxxx xxxx	
22	Erote	0111 1110	Loppuerote (end flag)

▼B

DSC_45 Ottaessaan vastaan BST:tä *ajoneuvoyksikön DSRC-laite* pyytää osoittamaan standardissa EN 12795 ja standardin EN 13372 7.1.1 kohdassa määritellyn yksityisen ikkunan ilman erityisiä RTM-asetuksia. Taulukossa 14.6 on esimerkki bittikoodauksesta.

Taulukko 14.6

▼C2

Alustus – Yksityisen ikkunan osoittamispyynnön kehyksen sisältö

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
1	Erote (FLAG)	0111 1110	Alkuerote (Start flag)
2	Yksityinen LID	xxxx xxxx	Tietyn ajoneuvoyksikön DSRC-laitteen yhteysosoite
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-koodin ohjauskenttä (MAC Control field)	0110 0000	Yksityistä ikkunaa koskeva pyyntö (Private window request)
7	FCS	xxxx xxxx	Kehyspohjainen varmiste (frame check sequence)
8		xxxx xxxx	
9	Erote (flag)	0111 1110	Loppuerote (end flag)

▼B

DSC_46 Tämän jälkeen REDCR-lukija vastaa osoittamalla standardissa EN 12795 ja standardin EN 13372 7.1 kohdassa määritellyn yksityisen ikkunan ilman erityisiä RTM-asetuksia.

Taulukossa 14.7 on esimerkki bittikoodauksesta.

Taulukko 14.7

▼C2

Alustus – Yksityisen ikkunan osoittamisen kehyksen sisältö

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
1	Erote (FLAG)	0111 1110	Alkuerote (start flag)
2	Yksityinen LID	xxxx xxxx	Tietyn ajoneuvoyksikön DSRC-laitteen yhteysosoite
3		xxxx xxxx	

▼C2

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-koodin ohjauskenttä (MAC Control field)	0010 s000	Yksityisen ikkunan osoittaminen (Private window allocation)
7	FCS	xxxx xxxx	Kehyspohjainen varmiste (frame check sequence)
8		xxxx xxxx	
9	Erote (flag)	0111 1110	Loppuerote (end flag)

▼B

DSC_47 Ottaessaan vastaan yksityisen ikkunan osoittamisen *ajoneuvoyksikön DSRC-laite* lähettää standardin EN 12834 sekä standardin EN 13372, 6.2, 6.3, 6.4 ja 7.1 kohdan mukaisen ajoneuvon palvelutaulukkonsa (VST) taulukossa 14.8 määritellyin asetuksin käyttäen osoitettua siirtoikkunaa.

Taulukko 14.8

▼C2

Alustus – VST-kehyksen asetukset

Kenttä	Asetukset
Yksityinen LID	Standardin EN 12834 mukaisesti
VST-parametrit	Fill = 0, sen jälkeen kukin tuettu sovellus: EID löytyy, parametri löytyy, AID = 2, EID sellainen kuin ajoneuvoon asetettu laite sen tuottaa
Parametri	Ei liittymää, sisältää RTM-kontekstitunnuksen
ObeConfiguration	Vapaaehtoinen kenttä ObeStatus voi löytyä, mutta REDCR-lukija ei käytä sitä
Fragmentoinnin indikaattori (Fragmentation header)	Ei fragmentointia
Siirtokerroksen (2. kerros) asetukset (Layer 2 settings)	Komennon PDU (Command PDU), käyttöliittymäkomento (UI command)

▼B

DSC_48 *Ajoneuvoyksikön DSRC-laitteen* on tuettava ”Freight and Fleet” -sovellusta, joka on yksilöity sovellustunnisteella ‘2’. Muita sovellustunnisteita voidaan tukea, mutta niitä ei saa olla tässä VST:ssä, koska BST edellyttää vain arvoa AID=2. ”Applications”-kenttä sisältää luettelon *ajoneuvoyksikön DSRC-laitteen* tuetuista sovelluksista. Kunkin tuetun sovellusilmentymän osalta annetaan viite asiaan kuuluvaan standardiin. Viite muodostuu Rtm Context -tunnuksesta, joka koostuu OLIOTUNNISTEESTA, joka edustaa kyseistä standardia, sen osaa (RTM:n osalta 9) ja mahdollisesti sen versiota, sekä ajoneuvoyksikön tuottamasta EID:stä, joka liittyy kyseiseen sovellukseen.

Käytännön esimerkki taulukossa 14.8 määritellyistä asetuksista sekä bittikoodauksista esitetään taulukossa 14.9.

▼B

Taulukko 14.9

▼C2

Alustus – esimerkki VST-kehyksen sisällöstä

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
1	Erote (FLAG)	0111 1110	Alkuerote (start flag)
2	Yksityinen LID	xxxx xxxx	Tietyn ajoneuvoyksikön DSRC-laitteen yhteysosoite
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-koodin ohjauskenttä (MAC Control field)	1100 0000	Komennon PDU (Command PDU)
7	LLC-ohjauskenttä (LLC Control field)	0000 0011	Käyttöliittymäkomento
8	Fragmentoinnin indikaattori (Fragmentation header)	1xxx x001	Ei fragmentointia
9	VST SEQUENCE {	1001	Alustuksen vastaus
	Fill BIT STRING (SIZE(4))	0000	Ei käytetä ja arvoksi asetaan 0
10	Profile INTEGER (0..127,...) Applications SEQUENCE OF {	0000 0000	Ei liittymää. Esimerkkiprofiili 0
11		0000 0001	Ei liittymää, 1 sovellus
12	SEQUENCE {		
	OPTION indicator	1	EID löytyy
	OPTION indicator	1	Parametri löytyy
	AID DSRCApplicationEntityID	00 0010	Ei liittymää. AID = 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Määritetty ajoneuvoon asetetussa laitteessa ja tunnistaa sovelluksen esiintymän.
14	Parameter Container {	0000 0010	Ei liittymää, säilön valinta = 02, oktettijono
15		0000 1000	Ei liittymää, RTM-kontekstitunnuksen pituus = 8

▼C2

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
16	Rtm-ContextMark::= SEQUENCE {	0000 0110	Tuetun standardin, osan ja version oliotunniste. Esimerkki: ISO (1) standardi (0) TARV (15638) osa 9 (9) versio 1 (1). Ensimmäinen oktetti on 06H, joka on oliotunniste, toinen oktetti on 06H, joka on pituus. Seuraavat 6 oktettia koodaavat esimerkkinä olevaa oliotunnistetta Huomaa, että löytyy ainoastaan yksi osa (valinnainen RtmCommProfile-osa on jätetty pois)
17	StandardIdentifier standardIdentifier	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 ei löydy
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Ajoneuvoyksikön DSRC-laitteen valmistajan tunniste siten, kuin se määritellään rekisterissä ISO 14816
27		xxxx xxxx	
28	FCS	xxxx xxxx	Kehyspohjainen varmiste (frame check sequence)
29		xxxx xxxx	
30	Flag	0111 1110	Loppuerote (end flag)

▼B

DCS_49 Tämän jälkeen REDCR-lukija lukee tiedot antamalla GET-komennon, joka vastaa standardin EN 13372 6.2, 6.3 ja 6.4 kohdassa ja standardissa EN 12834 määriteltyä GET-komentoa, taulukossa 14.10 määritellyin asetuksin.

Taulukko 14.10

▼C2

Esitys – GET-pyynnön kehyksen asetukset

Kenttä	Asetukset
Herätinlaitteen tunniste (Invoker Identifier) (IID)	Ei ole
Yhteyden tunniste (Link Identifier) (LID)	Tietyn ajoneuvoyksikön DSRC-laitteen yhteysosoite
Ketjutus (chaining)	Ei
Osan tunniste (EID)	Kuten ajoneuvojen palvelutaulukossa määritetään Ei liittymää.

▼C2

Kenttä	Asetukset
Pääsytiedot	Ei
AttributeIdList	Ei liittymää, 1 ominaisuus (attribute), AttributeID = 1 (RtmData)
Fragmentointi	Ei
Siirtokerroksen (2. kerros) asetukset (Layer 2 settings)	Komennon PDU (Command PDU), kerätty ACn -komento (Polled ACn command)

▼B

Taulukossa 14.11 on esimerkki RTM-datan lukemisesta.

Taulukko 14.11

▼C2

Esitys – Esimerkki GET-pyynnön kehyksestä

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
1	Erote (FLAG)	0111 1110	Alkuerote (start flag)
2	Yksityinen LID	xxxx xxxx	Tietyn ajoneuvoyksikön DSRC-laitteen yhteysosoite
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-koodin ohjauskenttä (MAC Control field)	1010 s000	Komennon PDU (Command PDU)
7	LLC-ohjauskenttä (LLC Control field)	n111 0111	Kerätty ACn-komento, n-bittiä
8	Fragmentoinnin indikaattori (Fragmentation header)	1xxx x001	Ei fragmentointia
9	Get.request SEQUENCE {	0110	GET-pyyntö
	OPTION indicator	0	Pääsytiedot puuttuvat
	OPTION indicator	0	IID puuttuu
	OPTION indicator	1	AttributeIdList löytyy
	Fill BIT STRING(SIZE(1))	0	Asetettu arvoon 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	RTM-sovelluksen EID, kuten ajoneuvojen palvelutaulukossa määritetään Ei liittymää.
11	AttributeIdList SEQUENCE OF { AttributeId}}	0000 0001	Ei liittymää, ominaisuuksien määrä = 1
12		0000 0001	AttributeId = 1, RtmData. Ei liittymää.
13	FCS	xxxx xxxx	Kehyspohjainen varmiste (frame check sequence)
14		xxxx xxxx	
15	Flag	0111 1110	Loppuerote (end flag)

▼B

DSC_50 Ottaessaan vastaan GET-pyynnön *ajoneuvoyksikön DSRC-laite* lähettää pyydetyt tiedot sisältävän GET-vastauksen, joka vastaa standardin EN 13372 6.2, 6.3 ja 6.4 kohdassa ja standardissa EN 12834 määriteltyä GET-vastausta, taulukossa 14.12 määritellyin asetuksin.

Taulukko 14.12

▼C2

Esitys – GET-vastauksen kehyksen asetukset

Kenttä	Asetukset
Herätinlaitteen tunniste (Invoker Identifier) (IID)	Ei ole
Yhteyden tunniste (Link Identifier) (LID)	Standardin EN 12834 mukaisesti
Ketjutus (chaining)	Ei
Osan tunniste (EID)	Kuten ajoneuvojen palvelutaulukossa määritetään
Pääsytiedot	Ei
Fragmentointi	Ei
Siirtokerroksen (2. kerros) asetukset (Layer 2 settings)	Vastauksen PDU (Response PDU), vastaus käytettävissä ja hyväksytty komento, ACn -komento

▼B

Taulukossa 14.13 esitetään esimerkki RTM-datan lukemisesta.

Taulukko 14.13

▼C2

Esittäminen – Esimerkki vastauskehyksen sisällöstä

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
1	Erote (FLAG)	0111 1110	Alkuerote (start flag)
2	Yksityinen LID	xxxx xxxx	Tietyn ajoneuvoyksikön DSRC-laitteen yhteysosoite
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-koodin ohjauskenttä (MAC Control field)	1101 0000	Vastauksen PDU (Response PDU)
7	LLC-ohjauskenttä (LLC Control field)	n111 0111	Vastaus käytettävissä, ACn -komento n-bittiä
8	LLC-tilan kenttä (LLC status field)	0000 0000	Vastaus käytettävissä ja hyväksytty komento
9	Fragmentoinnin indikaattori (Fragmentation header)	1xxx x001	Ei fragmentointia
10	Get.response SEQUENCE {	0111	GET RESPONSE

▼C2

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
	OPTION indicator	0	IID puuttuu
	OPTION indicator	1	Ominaisuuksia koskeva luettelo (Attribute List) löytyy
	OPTION indicator	0	Palautteen tilaa ei ole
	Fill BIT STRING(SIZE(1))	0	Ei käytössä
11	EID INTEGER(0..127,…)	xxxx xxxx	Vastaus RTM-sovelluksesta. Ei liittymää.
12	AttributeList SEQUENCE OF {	0000 0001	Ei liittymää, ominaisuuksien määrä = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Ei liittymää, AttributeID = 1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Ei liittymää, Säilön valinta = 1010.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Kehyspohjainen varmiste (frame check sequence)
n+2		xxxx xxxx	
n+3	Erote	0111 1110	Loppuerote (end flag)

▼B

DSC_51 Tämän jälkeen REDCR-lukija sulkee yhteyden antamalla EVENT_REPORT, RELEASE -komennon, joka vastaa standardin EN 13372 6.2, 6.3 ja 6.4 kohtaa sekä standardin EN 12834 7.3.8 kohtaa, ilman erityisiä RTM-asetuksia. Taulukossa 14.14 on esimerkki RELEASE-komennon bittikoodauksesta.

Taulukko 14.14

▼C2

Päättäminen. EVENT_REPORT Release -kehyksen sisältö

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
1	Erote (FLAG)	0111 1110	Alkuerote (start flag)
2	Yksityinen LID	xxxx xxxx	Tietyn ajoneuvoyksikön DSRC-laitteen yhteysosoite
3		xxxx xxxx	
4		xxxx xxxx	

▼C2

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
5		xxxx xxxx	
6	MAC-koodin ohjauskenttä	1000 s000	Kehys sisältää LPDU-komennon
7	LLC-ohjauskenttä (LLC Control field)	0000 0011	Käyttöliittymäkomento
8	Fragmentoinnin indikaattori (Fragmentation header)	1xxx x001	Ei fragmentointia
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Pääsytiedot puuttuvat
	OPTION indicator	0	Tapahtuman parametrit puuttuvat
	OPTION indicator	0	IID puuttuu
	Mode BOOLEAN	0	Vastausta ei odoteta
10	EID INTEGER (0..127,…)	0000 0000	Ei laajennusta, EID = 0 (järjestelmä)
11	EventType INTEGER (0..127,…)}	0000 0000	Tapahtuman tyyppi 0 = Release
12	FCS	xxxx xxxx	Kehyspohjainen varmiste
13		xxxx xxxx	
14	Erote	0111 1110	Loppuerote (end flag)

▼B

DSC_52 *Ajoneuvoyksikön DSRC-laitteen* ei oleteta vastaavan Release-komentoon. Tämän jälkeen yhteys päätetään.

5.4.8 *DSRC-testitapahtuman kuvaus*

DSC_53 Valtuutettujen henkilöiden, joilla on pääsy turvamenettelyihin, on suoritettava lisäyksessä 11 määritellyt täysimittaiset testit, joihin sisältyy tietojen suojaaminen, edellä määriteltyä normaalia GET-komentoa käyttäen.

DSC_54 Käyttöönoton ja määräaikaistarkastusten yhteydessä tehtävät testit, jotka edellyttävät salauksen avaamista ja avattujen tietojen sisällön ymmärtämistä, on suoritettava lisäyksen 11 ”Yhteiset turvamekanismit” ja lisäyksen 9 ”Vaadittavien vähimmäistestien tyyppihyväksyntäluettelo” mukaisesti.

Perustavanlaatuinen DSRC-yhteys voidaan kuitenkin testata ECHO-komennolla. Tällaisia testejä saatetaan vaatia käyttöönoton tai määräaikaistarkastusten yhteydessä tai muutoin toimivaltaisen valvontaviranomaisen tai asetuksen (EU) N:o 165/2014 niin edellyttäessä (ks. jäljempänä 6 jakso).

▼B

DSC_55 Tämän perusyhteystestin suorittamiseksi REDCR-lukija antaa ECHO-komennon istunnon aikana eli sen jälkeen, kun alustusvaihe on saatu onnistuneesti päätökseen. Vuorovaikutuksen järjestys on samanlainen kuin kyselyssä:

— Vaihe 1 *REDCR-lukija* lähettää ”lähettimen palvelutaulukon” (BST), jossa on sovellustunnisteet (AID) sen tukemassa palveluluettelossa. RTM-sovelluksissa tämä on yksinkertaisesti palvelu, jonka AID-arvo = 2.

Ajoneuvoyksikön DSRC-laite arvioi saamansa BST:n, ja jos se havaitsee BST:n pyytävän Freight&Fleet-palvelua (AID = 2), *ajoneuvoyksikön DSRC-laite* vastaa. Jos *REDCR-lukija* ei tarjoa arvoa AID=2, *ajoneuvoyksikön DSRC-laite* sulkee tapahtumansa *REDCR-lukijan* kanssa.

— Vaihe 2 *Ajoneuvoyksikön DSRC-laite* lähettää pyynnön yksityisen ikkunan osoittamisesta.

— Vaihe 3 REDCR-lukija lähettää yksityisen ikkunan osoittamisen.

— Vaihe 4 *Ajoneuvoyksikön DSRC-laite* käyttää osoitettua yksityistä ikkunaa ja lähettää ajoneuvon palvelutaulukon (VST). VST sisältää luettelon kaikista tämän *ajoneuvoyksikön DSRC-laitteen* AID=2-kehyksessä tukemista eri sovellusilmentymistä. Eri ilmentymät on yksilöitävä ainutkertaisilla osien tunnisteilla (EID), joista jokaiseen liittyy parametrin arvo, joka ilmaisee tuetun sovellusilmentymän.

— Vaihe 5 Seuraavaksi *REDCR-lukija* analysoi tarjotun VST:n ja joko päättää yhteyden (RELEASE), koska se ei ole kiinnostunut mistään, mitä VST tarjoaa (eli se saa VST:n sellaisen *ajoneuvoyksikön DSRC-laitteesta*, joka ei ole RTM-ajoneuvoyksikkö), tai, jos se saa asianmukaisen VST:n, käynnistää sovellusilmentymän.

— Vaihe 6 *REDCR-lukija* antaa komennon (ECHO) kyseessä olevalla *ajoneuvoyksikön DSRC-laitteelle* ja osoittaa yksityisen ikkunan.

— Vaihe 7 *Ajoneuvoyksikön DSRC-laite* käyttää nyt osoitettua yksityistä ikkunaa ja lähettää ECHO vastauskehyksen.

Seuraavissa taulukoissa esitetään käytännön esimerkki ECHO-vaihtoistunnosta.

DSC_56 Alustus suoritetaan 5.4.7 jakson (DSC_44–DSC_48) ja taulukkojen 14.4–14.9 mukaisesti.

DSC_57 Tämän jälkeen REDCR-lukija antaa standardin ISO 14906 mukaisen, 100 tavua sisältävän ACTION, ECHO -komennon ilman erityisiä RTM-asetuksia. Taulukossa 14.15 esitetään REDCR-lukijan lähettämän kehyksen sisältö.

▼B

Taulukko 14.15

▼C2

Esimerkki ACTION, ECHO-pyynnön kehyksestä

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
1	Erote (FLAG)	0111 1110	Alkuerote (Start flag)
2	Yksityinen LID	xxxx xxxx	Tietyn ajoneuvoyksikön DSRC-laitteen yhteysosoite
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-koodin ohjauskenttä	1010 s000	Komennon PDU (Command PDU)
7	LLC-ohjauskenttä (LLC Control field)	n111 0111	Kerätty ACn-komento, n-bittiä
8	Fragmentoinnin indikaattori (Fragmentation header)	1xxx x001	Ei fragmentointia
9	ACTION.request SEQUENCE {	0000	Toimintoa (action) koskeva pyyntö (ECHO)
	OPTION indicator	0	Pääsytiedot puuttuvat
	OPTION indicator	1	Toiminnon parametri (action parameter) löytyy
	OPTION indicator	0	IID puuttuu
	Mode BOOLEAN	1	Vastausta odotetaan
10	EID INTEGER (0..127,…)	0000 0000	Ei laajennusta, EID = 0 (järjestelmä)
11	EID INTEGER (0..127,…)	0000 1111	Ei laajennusta, pyyntö toimintotyypille (action type) ECHO
12	ActionParameter CONTAINER {	0000 0010	Ei liittymää, säiliön valinta = 2
13		0110 0100	Ei liittymää. Merkkijonon pituus = 100 oktettia
14		xxxx xxxx	Takaisin lähetetyt tiedot (echo)
…		…	
113	}}	xxxx xxxx	
114614	FCS	xxxx xxxx	Kehyspohjainen varmiste (frame check sequence)
115715		xxxx xxxx	
116816	Erote (flag)	0111 1110	Loppuerote (end flag)

▼B

DSC_58 Saadessaan ECHO-pyynnön *ajoneuvoyksikön DSRC-laite* lähettää 100-tavuisen ECHO-vastauksen heijastamalla saadun komennon standardin ISO 14906 mukaisesti ilman erityisiä RTM-asetuksia. Taulukossa 14.16 esitetään esimerkki bittitason koodauksesta.

Taulukko 14.16

▼C2

Esimerkki ACTION, ECHO-vastauksen kehyksestä

Oktetti nro	Määrite/Kenttä	Bittejä oktetissa	Kuvaus
1	Erote (FLAG)	0111 1110	Alkuerote (start flag)
2	Yksityinen LID	xxxx xxxx	Tietyn ajoneuvoyksikön yhteysosoite
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-koodin ohjauskenttä (MAC Control field)	1101 0000	Vastauksen PDU (Response PDU)
7	LLC-ohjauskenttä (LLC Control field)	n111 0111	ACn-komento, n-bittiä
8	LLC-tilan kenttä (LLC status field)	0000 0000	Vastaus käytettävissä
9	Fragmentoinnin indikaattori (Fragmentation header)	1xxx x001	Ei fragmentointia
10	ACTION.response SEQUENCE {	0001	ACTION vastaus (ECHO)
	OPTION indicator	0	IID puuttuu
	OPTION indicator	1	Vastauksen parametri (response parameter) löytyy
	OPTION indicator	0	Palautteen tilaa ei ole
	Fill BIT STRING (SIZE (1))	0	Ei käytössä
11	EID INTEGER (0..127,…)	0000 0000	Ei laajennusta, EID = 0 (järjestelmä)
12	ResponseParameter CONTAINER {	0000 0010	Ei liittymää, säiliön valinta = 2
13		0110 0100	Ei liittymää. Merkkijonon pituus = 100 oktettia
14		xxxx xxxx	Takaisin lähetetyt tiedot (echo)
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Kehyspohjainen varmiste (frame check sequence)
115		xxxx xxxx	
116	Erote (flag)	0111 1110	Loppuerote (end flag)

▼B

5.5 **Direktiivin 2015/71/EY tukeminen**

5.5.1 *Yleistä*

DSC_59 Raskaiden hyötyajoneuvojen suurimmista sallituista painoista ja mitoista annetun direktiivin 2015/719/EY tukemiseksi ajoneuvon sisäisen punnitusjärjestelmän (OWS) tietojen lataamiseksi 5,8 GHz:n rajapintayhteyden avulla käytetään samaa tapahtumaprotokollaa kuin RTM-datan yhteydessä (ks. 5.4.1 jakso). Ainoa ero on se, että TARV-standardiin liittyvä oliotunniste koskee standardin ISO 15638 ajoneuvon sisäisiä punnitusjärjestelmiä koskevaa osaa 20.

5.5.2 *Komennot*

DSC_60 OWS-tapahtumassa käytetään samoja komentoja kuin RTM-tapahtumassa.

5.5.3 *Kyselykomentosarja*

DSC_61 OWS-datan kyselykomentosarja on sama kuin RTM-datan kyselykomentosarja.

5.5.4 *Tietorakenteet*

DSC_62 Hyötykuormatiedot (OWS-data) koostuvat seuraavien dataelementtien ketjutuksesta:

1. EncryptedOwsPayload-data, joka on OwsPayload -datan 5.5.5 jaksossa määritelty ASN.1-standardin mukainen salaus. Salausmenetelmä on sama kuin RtmData-tietoja varten hyväksytty salausmenetelmä, joka määritellään lisäyksessä 11.

2. DSRCSecurityData, joka lasketaan samoilla algoritmeilla kuin RtmData ja joka määritellään lisäyksessä 11.

▼B

5.5.5 *OWS-datan DSRC-tapahtuman ASN.1-moduuli*

DSC_63. ASN.1-moduulin mukainen DSRC-datan määritelmä RTM-sovelluksessa on seuraava:

```
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
```

▼B

5.5.6 *OwsData-elementit, suoritetut toiminnot ja määritelmät*

OwsData-elementit on määritelty siten, että ne tukevat raskaiden hyötyajoneuvojen suurimmista sallituista painoista ja mitoista annettua direktiiviä 2015/719/EY. Niiden merkitys on seuraava:

— recordedWeight tarkoittaa raskaan hyötyajoneuvon mitattua kokonaispainoa 10 kg:n tarkkuudella standardin EN ISO 14906 mukaisesti. Esimerkiksi arvo 2 500 tarkoittaa 25 tonnin painoa.

— axlesConfiguration tarkoittaa raskaan hyötyajoneuvon akselijärjestelmää akselien lukumääränä. Kokoonpano määritellään 20-bittisellä bittimaskilla (laajennettu standardista EN ISO 14906).

2-bittinen bittimaski edustaa akselin järjestelmää seuraavassa muodossa:

— Arvo 00B tarkoittaa, että arvoa ei ole saatavilla, koska ajoneuvossa ei ole akselikuormitusta keräävää laitteistoa.

— Arvo 01B tarkoittaa, että akselia ei ole.

— Arvo 10B tarkoittaa, että akseli on olemassa ja kuormitus on laskettu ja kerätty ja se toimitetaan axlesRecordedWeight-kentässä.

— Arvo 11B on varattu tulevaan käyttöön.

Viimeiset neljä bittiä on varattu tulevaan käyttöön.

Akselien määrä										
Vetoyksikön akselien määrä			Perävaunun akselien määrä							
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	Varattu tulevaan käyttöön (4 bittiä)

— axlesRecordedWeight merkitsee kutakin akselia kohden kirjattua ominaispainoa 10 kg:n tarkkuudella. Kutakin akselia kohden käytetään kaksi tavua. Esimerkiksi arvo 150 tarkoittaa 1 500 kg:n painoa.

Muut datatyypit määritellään 5.4.5 jaksossa.

5.5.7 *Tiedonsiirtomekanismit*

DSC_64 OWS-datan tiedonsiirtomekanismi kyselylaitteen ja ajoneuvon DSRC-laitteen välillä on sama kuin RTM-datan tiedonsiirtomekanismi (ks. 5.4.6 jakso).

DSC_65 Enimmäispainoja koskevat tiedot keräävän alustan ja DSRC-laitteen välinen tiedonsiirto perustuu 5.6 jaksossa määriteltyihin fyysiseen yhteyteen, rajapintoihin ja protokollaan.

5.6 **Ajoneuvoyksikön DSRC-laitteen ja ajoneuvoyksikön välinen tiedonsiirto**

5.6.1 *Fyysinen yhteys ja rajapinnat*

DSC_66 *Ajoneuvoyksikön* ja *ajoneuvoyksikön DSRC-laitteen* välinen yhteys voidaan toteuttaa joko fyysisellä johdolla tai Bluetooth v4.0 BLE -tekniikkaan perustuvalla lyhyen kantaman langattomalla yhteydellä.

▼B

DSC_67 Riippumatta valitusta fyysisestä yhteydestä ja rajapinnasta seuraavien vaatimusten on täytyttävä:

DSC_68 a) Jotta ajoneuvoyksikön ja ajoneuvoyksikön DSRC-laitteen ja myös sen eri erien toimituksiin voidaan käyttää eri toimittajia, ajoneuvoyksikön ja ajoneuvoyksikön DSRC-laitteen välisen yhteyden on oltava avoimen standardin mukainen yhteys. Ajoneuvoyksikkö on liitettävä ajoneuvoyksikön DSRC-laitteeseen joko

i) vähintään 2 metriä pitkällä kiinteällä johdolla käyttäen suoraa DIN 41612 H11 -liitintä – ajoneuvoyksikön DSRC-laitteesta 11-nastainen hyväksytty urosliitin, joka sopii ajoneuvoyksikön laitteen samanlaiseen DIN/ISO-hyväksyttyyn naarasliittimeen, tai

ii) Bluetooth Low Energy (BLE) -yhteydellä, tai

iii) standardien ISO 11898 tai SAE J1939 mukaisella yhteydellä.

DSC_69 b) Ajoneuvoyksikön ja ajoneuvoyksikön DSRC-laitteen välisten rajapintojen ja yhteyden määritelmän on tuettava 5.6.2 jaksossa määriteltyjä sovellusprotokollakäskyjä.

DSC_70 c) Ajoneuvoyksikön ja ajoneuvoyksikön DSRC-laitteen on tuettava yhteyden kautta tapahtuvan tiedonsiirron toimintaa suorituskyvyn ja virransyötön osalta.

5.6.2 *Sovellusprotokolla*

DSC_71 Ajoneuvoyksikön etäviestintälaitteiston ja ajoneuvoyksikön DSRC-laitteen välinen sovellusprotokolla vastaa etäviestintätietojen säännöllisestä siirtämisestä ajoneuvoyksiköstä DSRC-laitteeseen.

DSC_72 Tärkeimmät komennot ovat seuraavat:

1. Yhteyden alustus – pyyntö

2. Yhteyden alustus – vastaus

3. Lähetetään tietoja, joissa on RTM-sovelluksen tunniste ja RTM-datan mukaan määritellyt hyötykuormatiedot

4. Tietojen vastaanottoilmoitus

5. Yhteyden päättäminen – pyyntö

6. Yhteyden päättäminen – vastaus

DSC_73 In ASN1.0-standardin mukaan edelliset komennot voidaan määritellä seuraavasti:

▼B

```
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 Komentojen ja parametrien kuvaus on seuraava:

— `RCDT-Communication Link Initialization – Request` -komentoa käytetään yhteyden alustukseen. Ajoneuvoyksikkö lähettää komennon ajoneuvoyksikön DSRC-laitteelle. Ajoneuvo asettaa LinkIdentifier-parametrin ja viestittää sen ajoneuvoyksikön DSRC-laitteelle tietyn yhteyden jäljittämiseksi.

(*Huom:* tällä on tarkoitus tukea tulevia yhteyksiä ja muita sovelluksia/moduuleja, kuten ajoneuvossa tapahtuvaa punnitusta).

— `RCDT-Communication Link Initialization – Response` on komento, jota ajoneuvoyksikön DSRC-laite käyttää vastatakseen yhteyden alustusta koskevaan pyyntöön. Ajoneuvoyksikön DSRC-laite lähettää komennon ajoneuvoyksikölle. Komento ilmoittaa alustuksen tuloksen joko vastauksena = 1 (onnistui) tai = 0 (epäonnistui).

DSC_75 Yhteyden alustus tehdään vasta asennuksen, kalibroinnin ja moottorin/ajoneuvoyksikön käynnistämisen jälkeen.

▼B

— RCDT-Send Data- komennon avulla ajoneuvoyksikkö lähettää allekirjoitetut RCDTData-tiedot (eli *etäyhteystiedot*) ajoneuvoyksikön DSRC-laitteelle. Tiedot lähetetään 60 sekunnin välein. DataTransactionId-parametri yksilöi kunkin tiedonsiirron. Myös LinkIdentifier-parametria käytetään sen varmistamiseen, että asianomainen yhteys on oikea.

— RCDT-Data Acknowledgment- komento lähetetään ajoneuvoyksikön DSRC-laitteelle, jotta se antaa palautetta ajoneuvoyksikölle RCDT-Send Data- komennolla lähetettyjen, DataTransactionId-parametrilla yksilöityjen tietojen vastaanottamisesta. Vastausparametri on = 1 (onnistui) tai = 0 (epäonnistui). Jos ajoneuvoyksikkö saa enemmän kuin kolme vastausta, joiden parametri = 0 tai jos se ei saa RCDT Data Acknowledgment -vastausta tietystä aiemmin lähetetystä RCDT-Send Data -komennosta, johon liittyi tietty DataTransactionId-parametri, ajoneuvoyksikkö tuottaa ja kirjaa tapahtuman.

— RCDT-Communication Link Termination request on komento, jonka ajoneuvoyksikkö lähettää ajoneuvoyksikön DSRC-laitteelle yhteyden päättämiseksi tietyn LinkIdentifier-parametrin osalta.

DSC_76 Kun ajoneuvoyksikön DSRC-laite tai ajoneuvoyksikkö käynnistetään uudelleen, kaikki olemassa olevat viestintäyhteydet on poistettava, koska ajoneuvoyksikön äkillinen sulkeminen saattaa aiheuttaa ”jäljellä roikkuvia” yhteyksiä.

— RCDT-Communication Link Termination – Response on komento, jonka ajoneuvoyksikön DSRC-laite lähettää ajoneuvoyksikölle vahvistaakseen ajoneuvoyksikön pyynnön yhteyden päättämisestä tietyn LinkIdentifier-parametrin osalta.

5.7 **Virheenkäsittely**

5.7.1 *Tietojen kirjaaminen ja viestintä ajoneuvoyksikön DSRC-laitteessa*

DSC_77 *VUSM*-toiminto toimittaa jo suojatut *tiedot ajoneuvoyksikön DSRC-laitteelle*. *VUSM*-toiminto tarkistaa, että *ajoneuvoyksikön DSRC-laitteeseen* kirjatut tiedot on kirjattu asianmukaisesti. *Ajoneuvoyksiköstä ajoneuvoyksikön DSRC-laitteelle* suoritettavan tiedonsiirron yhteydessä tapahtuvien mahdollisten virheiden kirjaus ja raportointi kirjataan EventFaultType-tyypillä ja enum-arvolla, joksi on asetettu ‘62’H Remote Communication Facility -yhteysvirhe, sekä aikaleimalla.

DSC_78 *Ajoneuvoyksikkö* ylläpitää yksilöllisellä nimellä merkittyä ja tarkastajien helposti tunnistettavissa olevaa tiedostoa ”ajoneuvoyksikön sisäisen viestinnän virheiden” kirjaamista varten.

DSC_79 Jos VUPM-toiminto yrittää saada ajoneuvoyksikön tietoja turvamoduulista (siirtääkseen ne ajoneuvoyksikön DSRC-laitteelle) tässä onnistumatta, se kirjaa virheen EventFaultType-tyypillä ja enum-arvolla, joksi on asetettu *‘62’H Remote Communication Facility* -yhteysvirhe, sekä aikaleimalla. Yhteysvirhe havaitaan,

▼B

kun `RCDT Data Acknowledgment`- viestiä ei saada siihen liittyvistä `RCDT Send Data`- tiedoista (eli joilla on sama DataTransactionId-parametri `Send Data- ja Acknowledgment`- viesteissä) vähintään kolmella peräkkäisellä kerralla.

5.7.2 *Langattoman yhteyden virheet*

DSC_80 Yhteysvirheiden käsittelyn on oltava asiaan liittyvien DSRC-standardien eli standardien EN 300 674-1, EN 12253, EN 12795, EN 12834 sekä standardin EN 13372 asianmukaisten parametrien mukaista.

5.7.2.1 *Salaus- ja allekirjoitusvirheet*

DSC_81 Salaus- ja allekirjoitusvirheet käsitellään lisäyksen 11 ”Yhteiset turvamekanismit” mukaisesti, eivätkä ne sisälly mihinkään DSRC-tiedonsiirtoon liittyviin virheilmoituksiin.

5.7.2.2 *Virheiden kirjaaminen*

DSRC-media on dynaaminen langaton yhteys ympäristössä, jolle ovat tyypillisiä epävarmat ilmakehän ja häiriöolosuhteet varsinkin tähän sovellukseen liittyvissä ”kannettavan REDCR-lukijan” ja ”liikkuvan ajoneuvon” yhdistelmissä. Tästä syystä on tarpeen erottaa toisistaan ”lukemisen epäonnistuminen” ja ”virhe”. Langattoman rajapinnan kautta suoritettavissa tapahtumissa lukemahäiriöt ovat tavallisia, ja niiden seurauksena on tavallisesti uusi yritys, eli BST lähetetään uudelleen ja komentosarja toistetaan, mikä useimmiten johtaa onnistuneeseen viestintäyhteyteen ja tiedonsiirtoon, ellei kohteena oleva ajoneuvo siirry kantaman ulkopuolelle uudelleenlähetyksen vaatimana aikana. (”Onnistunut” ”lukeminen” saattaa edellyttää useita yrityksiä.)

Lukemisen epäonnistuminen saattaa johtua siitä, että antenneja ole liitetty asianmukaisesti pariksi (”suuntausvirhe”); siitä, että toinen antenneista on varjossa – tämä voi olla tietoista, mutta myös toisen ajoneuvon fyysisen läsnäolon aiheuttamaa; etenkin 5,8 GHz:n WIFI-verkkojen tai muiden julkisten langattomien yhteyksien aiheuttamista radiotaajuuksisista häiriöistä; tai tutkainterferenssistä, vaikeista ilmakehän olosuhteista tai yksinkertaisesti siirtymisestä DSRC-yhteyden kantaman ulkopuolelle. Yksittäisiä lukemahäiriötapauksia ei voida niiden luonteen vuoksi kirjata, koska viestintää ei yksinkertaisesti tapahtunut.

Jos toimivaltaisen valvontaviranomaisen edustaja kuitenkin kohdentaa etäyhteyden tiettyyn ajoneuvoon ja yrittää tehdä kyselyn sen *ajoneuvoyksikön DSRC-laitteelta*, mutta tiedonsiirto ei onnistu, tämän virheen syynä saattaa olla tietoinen laitteisiin kajoaminen, ja tästä syystä toimivaltaisen valvontaviranomaisen edustajalla on oltava keino kirjata virhe ja ilmoittaa kauempana tienvarressa oleville kollegoille mahdollisesta rikkomisesta. Näin kollegat voivat pysäyttää ajoneuvon ja suorittaa fyysisen tarkastuksen. Koska onnistunutta viestintää ei kuitenkaan ole tapahtunut, ajoneuvoyksikön DSRC-laite ei voi antaa virhettä koskevia tietoja. Tästä syystä tällaisen raportoinnin on oltava REDCR-lukulaitteiden suunnitteluun sisältyvä toiminto.

”Lukemisen epäonnistuminen” on teknisesti eri asia kuin ”virhe”. Tässä yhteydessä ”virheellä” tarkoitetaan väärän arvon saamista.

▼B

Ajoneuvoyksikön DSRC-laitteeseen siirrettävät tiedot toimitetaan jo suojattuina, ja siksi tietojen toimittajan on varmennettava ne (ks. 5.4 jakso).

Tämän jälkeen radiorajapinnan kautta siirrettävät tiedot tarkistetaan syklisillä redundanssitarkastuksilla viestinnän tasolla. Jos syklinen redundanssitarkastus vahvistaa tiedot, ne ovat oikeelliset. Jos syklinen redundanssitarkastus ei vahvista tietoja, ne lähetetään uudelleen. Sen todennäköisyys, että virheelliset tiedot läpäisisivät syklisen redundanssitarkastuksen, on niin pieni, että se voidaan jättää huomiotta.

Jos syklinen redundanssitarkastus ei vahvista tietoja eikä niiden uudelleenlähettämiseen ja vastaanottamiseen ole aikaa, tuloksena ei ole virhe, vaan tietyn tyyppisen lukemahäiriön ilmentymä.

Ainoat merkitykselliset ”häiriötiedot”, jotka voidaan kirjata, koskevat niiden tapahtumien onnistuneiden alustusten määrää, jotka eivät johda onnistuneeseen tiedonsiirtoon REDCR-lukijaan.

DSC_82 Tästä syystä *REDCR-lukija* kirjaa, aikaleimalla varustettuna, kuinka monta kertaa DSRC-kyselyjen alustusvaiheet ovat onnistuneet, mutta tapahtuma päättyi ennen kuin REDCR-lukija pystyi onnistuneesti noutamaan *tiedot*. Näiden tietojen on oltava toimivaltaisen tarkastusviranomaisen saatavilla, ja ne tallennetaan REDCR-laitteen muistiin. Se, miten tämä toteutetaan, riippuu tuotesuunnittelusta tai toimivaltaisen valvontaviranomaisen eritelmästä.

Ainoat merkitykselliset ”virhetiedot”, jotka voidaan kirjata, koskevat niiden tapausten määrää, joissa REDCR-lukija ei onnistu avaamaan vastaan otettujen *tietojen* salausta. On kuitenkin huomattava, että tämä liittyy vain REDCR-ohjelmiston tehokkuuteen. Tiedot voivat olla teknisesti salattuja, mutta semanttisesti merkityksettömiä.

DSC_83 Tästä syystä REDCR-lukija kirjaa, aikaleimalla varustettuna, kuinka monta kertaa se on onnistumatta yrittänyt avata DSRC-rajapinnan kautta saatujen tietojen salauksen.

6 ETÄYHTEYSTOIMINNON KÄYTTÖÖNOTTOON JA MÄÄRÄAIKAISTARKASTUKSIIN LIITTYVÄT TESTIT

6.1 **Yleistä**

DSC_84 Etäyhteystoimintoa varten on määrätty kahdentyyppisiä testejä:

1) ECHO-testi, jolla validoidaan langaton viestintäkanava *DSRC-REDCR-lukija*>>-:-<*ajoneuvoyksikön DSRC-laite.*

2) Päästä päähän -turvallisuustesti, jolla varmistetaan, että korjaamokortilla on pääsy ajoneuvoyksikön luomien ja langattoman viestintäkanavan kautta siirrettyjen salattujen ja allekirjoitettujen tietojen sisältöön.

6.2 **ECHO**

Tämä lauseke sisältää nimenomaisia säännöksiä, joiden tarkoituksena on testata ainoastaan, että yhteys DSRC-REDCR-lukija>>-:-<ajoneuvoyksikön DSRC-laite toimii.

▼B

ECHO-komennon tarkoituksena on antaa korjaamoille tai tyyppihyväksyntätestauslaitoksille mahdollisuus testata DSRC-yhteyden toimivuus ilman tietoturvavaltuuksia. Näin ollen testaajan laitteen tarvitsee vain pystyä alustamaan DSRC-yhteys (lähettämällä BST, jonka AID=2) ja sen jälkeen lähettämään ECHO-komento sekä, mikäli DSRC-yhteys toimii, ottamaan vastaan ECHO-vastaus. Ks. lähemmin 5.4.8 jakso. Mikäli se saa tämän vastauksen moitteettomasti, DSRC-yhteyden (*DSRC-REDCR-lukija*>>-:-<*ajoneuvoyksikön DSRC-laite*) asianmukainen toimivuus voidaan vahvistaa.

6.3 **Testit suojattujen tietojen sisällön validoimiseksi**

DSC_85 Tämä testi suoritetaan tietojen päästä päähän ulottuvan suojauksen validoimiseksi. Tähän testiin tarvitaan DSRC-testilukija. DSRC-testilukija suorittaa saman toiminnon ja sitä käytetään samoin eritelmin kuin lainvalvontaviranomaisten käyttämää lukijaa. Ainoana erona on, että DSRC-testilukijan käyttäjän varmennukseen käytetään korjaamokorttia eikä valvontakorttia. Testi voidaan suorittaa älykkään ajopiirturin alustavan aktivoinnin jälkeen tai kalibrointimenettelyn päätteeksi. Aktivoinnin jälkeen ajoneuvoyksikön on tuotettava suojatut varhaista havaitsemista koskevat tiedot ja viestittävä ne ajoneuvoyksikön DSRC-laitteelle.

DSC_86 Korjaamohenkilöstön on sijoitettava DSRC-testilukija 2–10 metrin etäisyydelle ajoneuvon eteen.

DSC_87 Tämän jälkeen korjaamohenkilöstö syöttää korjaamokortin DSRC-testilukijaan tehdäkseen varhaista havaitsemista koskevien tietojen kyselypyynnön ajoneuvoyksikölle. Onnistuneen kyselyn jälkeen korjaamohenkilöstöllä on pääsy vastaanotettuihin tietoihin, jotta se voi varmistaa, että niiden eheys on validoitu onnistuneesti ja että ne on salattu.

▼B

Lisäys 15

SIIRTYMINEN: ERI SUKUPOLVIEN LAITTEIDEN RINNAKKAISEN KÄYTÖN HALLINTA

SISÄLLYSLUETTELO

1. MÄÄRITELMÄT

2. YLEISET SÄÄNNÖKSET

2.1. Yhteenveto siirtymisestä

2.2. Ajoneuvoyksikköjen ja korttien yhteentoimivuus

2.3. Ajoneuvoyksikköjen ja liiketunnistimien yhteentoimivuus

2.4. Ajoneuvoyksikköjen, ajopiirturikorttien ja tietojen kopiointilaitteiden yhteentoimivuus

2.4.1 Kortin tietojen suora kopiointi IDE-laitteella

2.4.2 Kortin tietojen kopiointi ajoneuvoyksikön kautta

2.4.3 Ajoneuvoyksikön tietojen kopiointi

2.5. Ajoneuvoyksikköjen ja kalibrointilaitteiden yhteentoimivuus

3. TÄRKEIMMÄT VAIHEET ENNEN KÄYTTÖÖNOTTOPÄIVÄMÄÄRÄÄ

4. KÄYTTÖÖNOTTOPÄIVÄMÄÄRÄN JÄLKEEN SOVELLETTAVAT SÄÄNNÖKSET

1. MÄÄRITELMÄT

Tässä lisäyksessä tarkoitetaan

’älykkäällä ajopiirturijärjestelmällä’ tässä liitteessä määriteltyä järjestelmää (1 luku, määritelmä bbb)

’ensimmäisen sukupolven ajopiirturijärjestelmällä’ tässä asetuksessa määriteltyä järjestelmää (2 artikla, määritelmä 1)

’toisen sukupolven ajopiirturijärjestelmällä’ tässä asetuksessa määriteltyä järjestelmää (2 artikla, määritelmä 7)

’käyttöönottopäivämäärällä’ tässä liitteessä määriteltyä päivämäärää (1 luku, määritelmä ccc)

’IDE-laitteella’ (Intelligent dedicated equipment) tietojen kopioimiseen ulkoisille tietovälineille tarkoitettua laitetta, joka on määritelty tämän liitteen lisäyksessä 7.

2. YLEISET SÄÄNNÖKSET

2.1. **Yhteenveto siirtymisestä**

Tämän liitteen johdanto-osassa esitetään yhteenveto siirtymisestä ensimmäisen sukupolven ajopiirturijärjestelmästä toisen sukupolven ajopiirturijärjestelmään.

Johdanto-osan säännösten lisäksi todetaan seuraavaa:

— Ensimmäisen sukupolven liiketunnistimet eivät ole yhteentoimivia toisen sukupolven ajoneuvoyksikköjen kanssa.

— Toisen sukupolven liiketunnistimia aletaan asentaa ajoneuvoihin samaan aikaan kuin toisen sukupolven ajoneuvoyksikköjä.

▼B

— Tietojen kopiointi- ja kalibrointilaitteita on kehitettävä valvontalaitteiden ja ajopiirturikorttien molempien sukupolvien käytön tukemiseksi.

2.2. **Ajoneuvoyksikköjen ja korttien yhteentoimivuus**

Ensimmäisen sukupolven ajopiirturikortit ovat yhteentoimivia ensimmäisen sukupolven ajoneuvoyksikköjen kanssa (tämän asetuksen liitteen 1 B mukaisesti), ja toisen sukupolven ajopiirturikortit ovat yhteentoimivia toisen sukupolven ajoneuvoyksikköjen kanssa (tämän asetuksen liitteen 1 C mukaisesti). Lisäksi sovelletaan alla olevia vaatimuksia.

MIG_001 Vaatimusten MIG_004 ja MIG_005 mukaisia tilanteita lukuun ottamatta ensimmäisen sukupolven ajopiirturikortteja voidaan käyttää toisen sukupolven ajoneuvoyksiköissä niiden voimassaoloajan päättymiseen asti. Niiden haltija voi kuitenkin pyytää niiden korvaamista toisen sukupolven ajopiirturikorteilla heti, kun näitä on saatavilla.

MIG_002 Toisen sukupolven ajoneuvoyksiköissä voidaan käyttää mitä tahansa paikalleen asetettua, voimassa olevaa ensimmäisen sukupolven kuljettaja-, valvonta- ja yrityskorttia.

MIG_003 Tämä mahdollisuus voidaan poistaa tällaisista ajoneuvoyksiköistä pysyvästi korjaamolla, minkä jälkeen niissä ei voida enää käyttää ensimmäisen sukupolven ajopiirturikortteja. Tämä on mahdollista vasta sen jälkeen, kun Euroopan komissio on käynnistänyt menettelyn, jonka tarkoituksena on pyytää korjaamoita tekemään näin, esimerkiksi ajopiirturin määräaikaistarkastuksen yhteydessä.

MIG_004 Toisen sukupolven ajoneuvoyksiköissä voidaan käyttää vain toisen sukupolven korjaamokortteja.

MIG_005 Toisen sukupolven ajoneuvoyksiköt ottavat toimintatilan määrittämisessä huomioon vain paikalleen asetettujen, voimassa olevien korttien tyypin niiden sukupolvesta riippumatta.

MIG_006 Mitä tahansa voimassa olevaa toisen sukupolven ajopiirturikorttia voidaan käyttää ensimmäisen sukupolven ajoneuvoyksiköissä samalla tavalla kuin samantyyppistä ensimmäisen sukupolven ajopiirturikorttia.

2.3. **Ajoneuvoyksikköjen ja liiketunnistimien yhteentoimivuus**

Ensimmäisen sukupolven liiketunnistimet ovat yhteentoimivia ensimmäisen sukupolven ajoneuvoyksikköjen kanssa, ja toisen sukupolven liiketunnistimet ovat yhteentoimivia toisen sukupolven ajoneuvoyksikköjen kanssa. Lisäksi sovelletaan alla olevia vaatimuksia.

MIG_007 Toisen sukupolven ajoneuvoyksikköjä ei voida liittää ensimmäisen sukupolven liiketunnistimiin eikä käyttää niiden kanssa.

MIG_008 Toisen sukupolven liiketunnistimia voidaan liittää vain toisen sukupolven ajoneuvoyksikköihin tai kummankin sukupolven ajoneuvoyksikköihin ja käyttää niiden kanssa.

2.4. **Ajoneuvoyksikköjen, ajopiirturikorttien ja tietojen kopiointilaitteiden yhteentoimivuus**

MIG_009 Tietojen kopiointilaitteita voidaan käyttää vain yhden sukupolven tai molempien sukupolvien ajoneuvoyksikköjen ja ajopiirturikorttien kanssa.

▼B

2.4.1 *Kortin tietojen suora kopiointi IDE-laitteella*

MIG_010 Tiedot kopioidaan IDE-laitteella kortinlukijaan asetetuilta yhden sukupolven ajopiirturikorteilta kyseisen sukupolven turvallisuusmekanismeja ja tietojen kopiointiprotokollaa käyttäen. Kopioidut tiedot ovat kyseiselle sukupolvelle määritetyssä muodossa.

MIG_011 Jotta myös muut kuin EU:n valvontaviranomaiset voivat valvoa kuljettajia, toisen sukupolven kuljettajakorttien (ja korjaamokorttien) tietoja voidaan kopioida samalla tavalla kuin ensimmäisen sukupolven kuljettajakorttien (ja korjaamokorttien). Kopioitavat tiedot ovat

— allekirjoittamattomat EF-tiedostot, `IC` ja `ICC`

— allekirjoittamattomat EF-tiedostot (ensimmäinen sukupolvi), `Card_Certificate` ja `CA_Certificate`

— ensimmäisen sukupolven kortin kopiointiprotokollan edellyttämät muut sovellustietoja sisältävät (`TACHO` DF -tiedoston alaiset) EF-tiedostot. Tiedot suojataan digitaalisella allekirjoituksella ensimmäisen sukupolven turvallisuusmekanismien mukaisesti.

Kopioitaviin tietoihin eivät kuulu sovellustietoja sisältävät EF-tiedostot, joita on vain toisen sukupolven kuljettajakorteilla (ja korjaamokorteilla) (`TACHO_G2` DF -tiedoston alaiset sovellustietoja sisältävät EF-tiedostot).

2.4.2 *Kortin tietojen kopiointi ajoneuvoyksikön kautta*

MIG_012 Tiedot kopioidaan ensimmäisen sukupolven ajoneuvoyksikköön asetetulta toisen sukupolven kortilta ensimmäisen sukupolven tietojen kopiointiprotokollaa käyttäen. Kortti vastaa ajoneuvoyksikön komentoihin samalla tavalla kuin ensimmäisen sukupolven kortti, ja kopioidut tiedot ovat samassa muodossa kuin ensimmäisen sukupolven kortilta kopioidut tiedot.

MIG_013 Tiedot kopioidaan toisen sukupolven ajoneuvoyksikköön asetetulta ensimmäisen sukupolven kortilta tämän liitteen lisäyksessä 7 määriteltyä tietojen kopiointiprotokollaa käyttäen. Ajoneuvoyksikkö lähettää komentoja kortille samalla tavalla kuin ensimmäisen sukupolven ajoneuvoyksikkö, ja kopioidut tiedot ovat ensimmäisen sukupolven korteille määritetyssä muodossa.

2.4.3 *Ajoneuvoyksikön tietojen kopiointi*

MIG_014 Tiedot kopioidaan toisen sukupolven ajoneuvoyksiköstä toisen sukupolven turvallisuusmekanismeja ja tämän liitteen lisäyksessä 7 määriteltyä tietojen kopiointiprotokollaa käyttäen.

MIG_015 Jotta myös muut kuin EU:n valvontaviranomaiset voivat valvoa kuljettajia ja muut kuin EU:n korjaamot kopioida tietoja ajoneuvoyksiköistä, toisen sukupolven ajoneuvoyksikköjen tietoja voidaan vapaavalintaisesti kopioida myös ensimmäisen sukupolven turvallisuusmekanismeja ja ensimmäisen sukupolven tietojen kopiointiprotokollaa käyttäen. Kopioidut tiedot ovat samassa muodossa kuin ensimmäisen sukupolven ajoneuvoyksiköstä kopioidut tiedot. Tämä mahdollisuus on valittavissa valikon komentojen avulla.

▼B

2.5. **Ajoneuvoyksikköjen ja kalibrointilaitteiden yhteentoimivuus**

MIG_016 Kalibrointilaitteilla pystytään kalibroimaan kummankin sukupolven ajopiirturit kyseisen sukupolven kalibrointiprotokollaa käyttäen. Kalibrointilaitetta voidaan käyttää vain yhden sukupolven ajopiirturin tai molempien sukupolvien ajopiirturien kanssa.

3. TÄRKEIMMÄT VAIHEET ENNEN KÄYTTÖÖNOTTOPÄIVÄMÄÄRÄÄ

MIG_017 Testiavaimet ja -varmenteet tulevat valmistajien saataville viimeistään **30 kuukautta** ennen käyttöönottopäivämäärää.

MIG_018 Valmistajien mahdollisesti pyytämät yhteentoimivuustestit voidaan aloittaa viimeistään **15 kuukautta** ennen käyttöönottopäivämäärää.

MIG_019 Viralliset avaimet ja varmenteet tulevat valmistajien saataville viimeistään **12 kuukautta** ennen käyttöönottopäivämäärää.

MIG_020 Jäsenvaltiot voivat myöntää toisen sukupolven korjaamokortteja viimeistään **3 kuukautta** ennen käyttöönottopäivämäärää.

MIG_021 Jäsenvaltiot voivat myöntää kaikentyyppisiä toisen sukupolven ajopiirturikortteja viimeistään **1 kuukausi ennen käyttöönottopäivämäärää**.

4. KÄYTTÖÖNOTTOPÄIVÄMÄÄRÄN JÄLKEEN SOVELLETTAVAT SÄÄNNÖKSET

MIG_022 Käyttöönottopäivämäärän jälkeen jäsenvaltiot voivat myöntää vain toisen sukupolven ajopiirturikortteja.

MIG_023 Ajoneuvoyksikköjen ja liiketunnistimien valmistajat saavat valmistaa ensimmäisen sukupolven ajoneuvoyksikköjä ja liiketunnistimia niin kauan kuin niitä on käytössä, jotta vialliset osat voidaan korvata.

MIG_024 Ajoneuvoyksikköjen ja liiketunnistimien valmistajat voivat pyytää jo tyyppihyväksyttyjen ensimmäisen sukupolven ajoneuvoyksikkö- ja liiketunnistintyyppien tyyppihyväksynnän jatkamista ja saada sen.

▼B

Lisäys 16

MUUNNIN M1- JA N1-LUOKAN AJONEUVOJA VARTEN

SISÄLLYSLUETTELO

1. LYHENTEET JA VIITEASIAKIRJAT

1.1. Lyhenteet

1.2. Vertailustandardit

2. MUUNTIMEN YLEISET OMINAISUUDET JA TOIMINNOT

2.1. Muuntimen yleiskuvaus

2.2. Toiminnot

2.3. Turvallisuus

3. VALVONTALAITTEITA KOSKEVAT VAATIMUKSET MUUNTIMEN OLLESSA ASENNETTUNA

4. MUUNTIMEN RAKENNETTA JA TOIMINTOJA KOSKEVAT VAATIMUKSET

4.1. Rajapinta saapuvien nopeuspulssien kanssa ja niiden muuntaminen

4.2. Saapuvien pulssien tuottaminen sulautetulle liiketunnistimelle

4.3. Sulautettu liiketunnistin

4.4. Turvallisuusvaatimukset

4.5. Suorituskykyä koskevat tiedot

4.6. Materiaalit

4.7. Merkinnät

5. VALVONTALAITTEIDEN ASENNUS MUUNNINTA KÄYTETTÄESSÄ

5.1. Asennus

5.2. Sinetöinti

6. TARKASTUKSET, MÄÄRÄAIKAISTARKASTUKSET JA KORJAUKSET

6.1. Määräaikaistarkastukset

7. VALVONTALAITTEIDEN TYYPPIHYVÄKSYNTÄ MUUNNINTA KÄYTETTÄESSÄ

7.1. Yleistä

7.2. Toiminnallisuustodistus

1. LYHENTEET JA VIITEASIAKIRJAT

1.1. **Lyhenteet**

TBD (To Be Defined) Päätetään myöhemmin

VU (Vehicle unit) Ajoneuvoyksikkö

1.2. **Vertailustandardit**

ISO16844-3 Road vehicles – Tachograph systems – Part 3: Motion sensor interface

2. MUUNTIMEN YLEISET OMINAISUUDET JA TOIMINNOT

2.1. **Muuntimen yleiskuvaus**

ADA_001 Muunnin toimittaa siihen yhdistetylle ajoneuvoyksikölle turvatut liiketiedot, jotka kuvaavat jatkuvasti ajoneuvon nopeutta ja kuljettua matkaa.

Muunnin on tarkoitettu ainoastaan sellaisiin ajoneuvoihin, jotka on varustettava valvontalaitteella tämän asetuksen mukaisesti.

▼B

Se on asennettava ja sitä on käytettävä vain niissä ajoneuvotyypeissä, jotka on määritelty liitteen IC määritelmässä yy) 'muunnin', jos ei ole mekaanisesti mahdollista asentaa muun tyyppistä olemassa olevaa liiketunnistinta, joka on muutoin tämän liitteen ja sen lisäysten 1–16 määräysten mukainen.

Muunninta ei saa liittää mekaanisesti ajoneuvon liikkuvaan osaan, vaan se on yhdistettävä nopeus/etäisyysimpulsseihin, joita integroidut tunnistimet tai vaihtoehtoiset liitännät synnyttävät.

ADA_002 Muuntimen koteloon on asennettava (tämän liitteen IC 8 luvun "Valvontalaitteiden ja ajopiirturikorttien tyyppihyväksyntä" määräysten mukaisesti) tyyppihyväksytty liiketunnistin. Kotelossa on oltava myös pulssimuunnin, joka muuntaa saapuvat pulssit sulautetulle liiketunnistimelle. Sulautettu liiketunnistin on yhdistettävä ajoneuvoyksikköön, niin että ajoneuvoyksikön ja muuntimen rajapinta täyttää standardin ISO16844-3 vaatimukset.

2.2. **Toiminnot**

ADA_003 Muuntimessa on oltava seuraavat toiminnot:

— rajapinta saapuvien nopeuspulssien kanssa ja niiden muuntaminen,

— saapuvien pulssien tuottaminen sulautetulle liiketunnistimelle,

— kaikki sulautetun liiketunnistimen toiminnot, turvatun liikedatan tuottaminen ajoneuvoyksikölle.

2.3. **Turvallisuus**

ADA_004 Muuntimen ei tule olla turvasertifioitu tämän liitteen lisäyksessä 10 määritellyn liiketunnistimia koskevan yleisen tietoturvatavoitteen mukaisesti. Sen sijaan sovelletaan tämän lisäyksen 4.4 kohdassa määriteltyjä tietoturvavaatimuksia.

3. VALVONTALAITTEITA KOSKEVAT VAATIMUKSET MUUNTIMEN OLLESSA ASENNETTUNA

Seuraavien lukujen vaatimuksissa kerrotaan miten tämän liitteen vaatimukset on ymmärrettävä muunninta käytettäessä. Asiaankuuluvat liitteen IC vaatimusten numerot ilmoitetaan suluissa.

ADA_005 Muuntimella varustetun ajoneuvon valvontalaitteiden on täytettävä kaikki tämän liitteen määräykset, ellei tässä lisäyksessä toisin määrätä.

ADA_006 Jos muunnin on asennettu, valvontalaitteet käsittävät johdot, muuntimen (liiketunnistin mukaan luettuna) ja ajoneuvoyksikön [01].

ADA_007 Valvontalaitteiden tapahtumien ja/tai vikojen havaitsemistoimintoa muutetaan seuraavasti:

— ajoneuvoyksikkö synnyttää "keskeytynyt virransyöttö" -tapahtuman, kun laite on muussa kuin kalibrointitilassa ja sulautetun liiketunnistimen virransyöttö keskeytyy yli 200 millisekunnin ajaksi [79]

▼B

— ajoneuvoyksikkö synnyttää ”virhe liiketiedoissa” -tapahtuman, kun sulautetun liiketunnistimen ja ajoneuvoyksikön välinen normaali datavirta keskeytyy ja/tai kun sulautetun liiketunnistimen ja ajoneuvoyksikön välisen tiedonsiirron eheydessä tai autenttisuudessa ilmenee virhe [83]

— ajoneuvoyksikkö synnyttää ”tietoturvan murtoyritys” -tapahtuman muussa tapauksessa, joka vaikuttaa sulautetun liiketunnistimen tietoturvaan laitteen ollessa muussa kuin kalibrointitilassa [85]

— ajoneuvoyksikkö synnyttää ”valvontalaitteen vika” -tapahtuman laitteen ollessa muussa kuin kalibrointitilassa, jos sulautetussa liiketunnistimessa esiintyy jokin vika [88].

ADA_008 Muuntimen viat, jotka valvontalaite voi havaita, ovat niitä, jotka liittyvät sulautettuun liiketunnistimeen [88].

ADA_009 Ajoneuvoyksikön kalibrointitoiminnon avulla on voitava liittää sulautettu liiketunnistin automaattisesti ajoneuvoyksikköön [202, 204].

4. MUUNTIMEN RAKENNETTA JA TOIMINTOJA KOSKEVAT VAATIMUKSET

4.1. **Rajapinta saapuvien nopeuspulssien kanssa ja niiden muuntaminen**

ADA_011 Muuntimen tuloliitäntä hyväksyy taajuuspulsseja, jotka kuvaavat ajoneuvon nopeutta ja kuljettua etäisyyttä. Saapuvien pulssien sähköiset ominaisuudet ovat seuraavat: *Valmistaja määrittelee.* Säädöt, joita voivat suorittaa vain muuntimen valmistaja ja muuntimen asennuksen suorittava hyväksytty korjaamo, mahdollistavat tarvittaessa muuntimen oikeanlaisen tuloliitännän ajoneuvoon.

ADA_012 Muuntimen tuloliitännällä on voitava tarvittaessa kertoa tai jakaa saapuvien nopeuspulssien taajuuspulsseja kiinteällä kertoimella ja mukauttaa signaali kerroinalueeseen k, joka on määritelty tässä liitteessä (4 000-25 000 pulssia/km). Kiinteän kertoimen voivat ohjelmoida ainoastaan muuntimen valmistaja ja muuntimen asennuksen suorittava hyväksytty korjaamo.

4.2. **Saapuvien pulssien tuottaminen sulautetulle liiketunnistimelle**

ADA_013 Saapuvat pulssit, joita on mahdollisesti mukautettu edellä mainitulla tavalla, on tuotettava sulautetulle liiketunnistimelle niin, että liiketunnistin havaitsee jokaisen tulevan pulssin.

4.3. **Sulautettu liiketunnistin**

ADA_014 Tuotetut pulssit stimuloivat sulautettua liiketunnistinta, ja niiden avulla se muodostaa tarkasti liikedataa, joka kuvastaa ajoneuvon liikettä aivan kuin se olisi liitetty mekaanisesti ajoneuvon liikkuvaan osaan.

ADA_015 Ajoneuvo käyttää sulautetun liiketunnistimen tunnistetietoja muuntimen tunnistamiseen [95].

▼B

ADA_016 Sulautettuun liiketunnistimeen tallennettujen asennustietojen katsotaan edustavan muuntimen asennustietoja [122].

4.4. **Turvallisuusvaatimukset**

ADA_017 Muuntimen kotelo on suunniteltava niin, ettei sitä voida avata. Se on sinetöitävä, niin että yritykset käsitellä sitä epäasianmukaisesti voidaan havaita helposti (esim. silmämääräisessä tarkastuksessa, ks. ADA_035). Sinetteihin sovelletaan samoja vaatimuksia kuin liiketunnistimen sinetteihin [398–406].

ADA_018 Sulautetun liiketunnistimen poistaminen muuntimesta ei saa olla mahdollista ilman muuntimen kotelon sinetin (sinettien) rikkomista tai tunnistimen ja muuntimen kotelon välisen sinetin rikkomista (ks. ADA_034).

ADA_019 Muuntimella on varmistettava, että liiketietoja voidaan käsitellä ja johtaa vain muuntimen tulosta.

4.5. **Suorituskykyä koskevat tiedot**

ADA_020 Muuntimen on oltava täysin toimiva valmistajan määrittämällä lämpötila-alueella.

ADA_021 Muuntimen on oltava täysin toimiva kosteusalueella 10–90 prosenttia [214].

ADA_022 Muuntimen on oltava suojattu ylijännitettä, väärää napaisuutta ja oikosulkuja vastaan [216].

ADA_023 Muuntimen on

— reagoitava magneettikenttään, joka häiritsee ajoneuvon liikkeiden havainnointia; siinä tapauksessa ajoneuvoyksikkö tallentaa ja säilyttää tunnistinvian [88]; tai

— sisällettävä tuntoelin, joka on suojattu magneettikentiltä tai joka ei reagoi magneettikenttiin [217].

ADA_024 Muuntimen on oltava sähkömagneettista yhteensopivuutta koskevan kansainvälisen säännön UN ECE R10 mukainen ja suojattu staattisen sähkön aiheuttamilta purkauksilta ja jännitepiikeiltä [218].

4.6. **Materiaalit**

ADA_025 Muuntimen on täytettävä suojausluokka *(valmistaja määrittelee asennuskohdasta riippuen*) [220, 221].

ADA_026 Muuntimen kotelon on oltava väriltään keltainen.

4.7. **Merkinnät**

ADA_027 Muuntimeen on kiinnitettävä arvokilpi, jossa annetaan seuraavat tiedot:

— muuntimen valmistajan nimi ja osoite,

— valmistajan osanumero sekä muuntimen valmistusvuosi,

— muuntimen tyyppihyväksyntämerkki tai muuntimen sisältävän valvontalaitteen tyyppihyväksyntämerkki,

— muuntimen asennuspäivä,

▼B

— sen ajoneuvon valmistenumero, johon muunnin on asennettu.

ADA_028 Arvokilvessä on oltava myös seuraavat tiedot (jos niitä ei voida lukea suoraan sulautetun liiketunnistimen ulkopuolelta):

— sulautetun liiketunnistimen valmistaja,

— valmistajan osanumero sekä sulautetun liiketunnistimen valmistusvuosi,

— sulautetun liiketunnistimen tyyppihyväksyntämerkki.

5. VALVONTALAITTEIDEN ASENNUS MUUNNINTA KÄYTETTÄESSÄ

5.1. **Asennus**

ADA_029 Ajoneuvoihin asennettavia muuntimia saavat asentaa ainoastaan ajoneuvojen valmistajat tai hyväksytyt korjaamot, jotka on valtuutettu asentamaan, aktivoimaan ja kalibroimaan digitaalisia ja älykkäitä ajopiirtureita.

ADA_030 Muuntimen asentavan hyväksytyn korjaamon on säädettävä tuloliitäntä ja valittava (tarvittaessa) tulosignaalin jakosuhde.

ADA_031 Muuntimen asentavan hyväksytyn korjaamon on sinetöitävä muuntimen kotelo.

ADA_032 Muunnin on asennettava mahdollisimman lähelle sitä ajoneuvon osaa, joka tuottaa sen tulopulssit.

ADA_033 Muuntimen virtaa syöttävien johtojen on oltava punaisia (positiivinen napa) ja mustia (maa).

5.2. **Sinetöinti**

ADA_034 Seuraavia sinetöintivaatimuksia on noudatettava:

— muuntimen kotelo on sinetöitävä (ks. ADA_017),

— sulautetun tunnistimen kotelo on sinetöitävä muuntimen koteloon, paitsi jos on mahdotonta poistaa tunnistin muuntimen kotelosta rikkomatta muuntimen kotelon sinettiä (sinettejä) (ks. ADA_018),

— muuntimen kotelo on sinetöitävä ajoneuvoon,

— muuntimen ja siihen saapuvia pulsseja synnyttävän laitteen välinen kytkentä on sinetöitävä molemmista päistä (siinä määrin kuin tämä on kohtuudella mahdollista).

6. TARKASTUKSET, MÄÄRÄAIKAISTARKASTUKSET JA KORJAUKSET

6.1. **Määräaikaistarkastukset**

ADA_035 Käytettäessä muunninta jokaisessa valvontalaitteen määräaikaistarkastuksessa (määräaikaistarkastus merkitsee liitteen 1C vaatimusten [409–413] noudattamista) tarkastetaan,

— että muuntimessa on asianmukainen tyyppihyväksyntämerkintä,

— että muuntimen ja sen liitäntöjen sinetit ovat koskemattomat,

▼B

— että muunnin on asennettu asennuskilvessä ilmoitetulla tavalla,

— että muunnin on asennettu muuntimen ja/tai ajoneuvon valmistajan määrittelemällä tavalla,

— että muuntimen asentaminen tarkastettavaan ajoneuvoon on sallittua.

ADA_036 Nämä tarkastukset käsittävät sinettien kalibroinnin ja vaihtamisen näiden kunnosta riippumatta.

7. VALVONTALAITTEIDEN TYYPPIHYVÄKSYNTÄ MUUNNINTA KÄYTETTÄESSÄ

7.1. **Yleistä**

ADA_037 Valvontalaite on tyyppihyväksytettävä täydellisenä muuntimen kanssa [425].

ADA_038 Muuntimelle voidaan tehdä oma tyyppihyväksyntä tai tyyppihyväksyntä valvontalaitteen osana.

ADA_039 Tällaisen tyyppihyväksynnän on sisällettävä toiminnalliset testit, joissa käytetään muunninta. Jokaisen testin myönteiset tulokset todetaan asiaankuuluvassa todistuksessa [426].

7.2. **Toiminnallisuustodistus**

ADA_040 Muuntimen valmistajalle toimitetaan muuntimen tai valvontalaitteen, muunnin mukaan luettuna, toiminnallisuustodistus vasta sitten, kun seuraavat vähimmäisvaatimukset täyttävät toiminnalliset testit on läpäisty hyväksytysti.

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
1.	**Hallinnollinen tarkastus**		
1.1	Asiakirjat	Muuntimen kirjallisen aineiston oikeellisuus	
2.	**Silmämääräinen tarkastus**		
2.1.	Muuntimen yhtäpitävyys kirjallisen aineiston kanssa		
2.2.	Muuntimen tunniste / merkinnät		ADA_027, ADA_028
2.3	Muuntimen materiaalit		[219–223] ADA_026
2.4.	Tiivisteet		ADA_017, ADA_018, ADA_034
3.	**Toiminnalliset testit**		
3.1	Nopeuspulssien tuottaminen sulautetulle liiketunnistimelle		ADA_013

▼B

Nro	Testi	Kuvaus	Vaatimukset, joihin testi liittyy
3.2	Rajapinta saapuvien nopeuspulssien kanssa ja niiden muuntaminen		ADA_011, ADA_012
3.3	Liikkeen mittauksen tarkkuus		[30–35], [217]
4.	**Ympäristötestit**		
4.1	Valmistajan testitulokset	Valmistajan ympäristötestien tulokset.	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Sähkömagneettinen yhteensopivuus**		
5.1	Laitteen tuottama säteily ja magneettinen vastaanottavuus	Varmennetaan direktiivin 2006/28/EY vaatimusten noudattaminen	ADA_024
5.2	Valmistajan testitulokset	Valmistajan ympäristötestien tulokset.	ADA_024

▼C1

LIITE II

TYYPPIHYVÄKSYNTÄMERKKI JA -TODISTUS

I. TYYPPIHYVÄKSYNTÄMERKKI

1. Tyyppihyväksyntämerkki muodostuu

a) suorakulmiosta, jonka sisälle on sijoitettu pieni ”e” kirjain ja sen jäljessä tyyppihyväksynnän antaneen maan tunnusnumero tai -kirjain seuraavien tunnusten mukaisesti:

Belgia	6,
Bulgaria	34,
Tšekki	8,
Tanska	18,
Saksa	1,
Viro	29,
Irlanti	24,
Kreikka	23,
Espanja	9,
Ranska	2,
Kroatia	25,
Italia	3,
Kypros	CY,
Latvia	32,
Liettua	36,
Luxemburg	13,
Unkari	7,
Malta	MT,
Alankomaat	4,
Itävalta	12,
Puola	20,
Portugali	21,
Romania	19,
Slovenia	26,
Slovakia	27,
Suomi	17,
Ruotsi	5,
Yhdistynyt kuningaskunta	11,

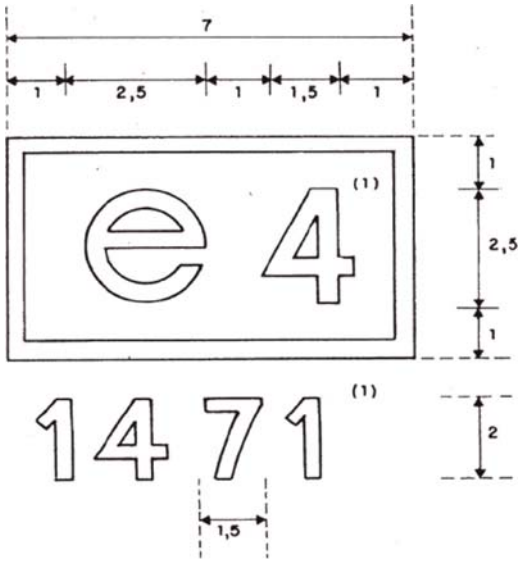
ja

b) valvontalaitteen tai piirturilevyn prototyypille laaditun tyyppihyväksyntätodistuksen numeroa tai ajopiirturikortin numeroa vastaava hyväksyntänumero sijoitettuna johonkin tämän suorakulmion vieressä olevaan kohtaan.

▼C1

2. Tyyppihyväksyntämerkki on oltava jokaisen valvontalaitteen arvokilvessä, jokaisessa piirturilevyssä ja jokaisessa ajopiirturikortissa. Se on merkittävä pysyvästi, ja se on aina oltava helposti luettavissa.

3. Seuraavassa piirretyn hyväksyntämerkin mitat ([1]) on ilmaistu millimetreinä, ja nämä mitat ovat vähimmäismitat. Mittojen väliset suhteet on säilytettävä.



([1]) Luvut ainoastaan ohjeellisia.

▼C1

II. ANALOGISTEN AJOPIIRTUREIDEN TYYPPIHYVÄKSYNTÄTODISTUS

Tyyppihyväksynnän antaneen jäsenvaltion on annettava hakijalle jäljempänä esitetyn mallin mukainen tyyppihyväksyntätodistus. Ilmoittaessaan muille jäsenvaltioille annetuista tyyppihyväksynnöistä tai tarvittaessa niiden peruuttamisista jäsenvaltion on käytettävä tämän todistuksen jäljennöksiä.

TYYPPIHYVÄKSYNTÄTODISTUS

Toimivaltaisen viranomaisen nimi .....

Ilmoitus koskee ([1]):

— valvontalaitetyypin tyyppihyväksyntää

— valvontalaitetyypin tyyppihyväksynnän peruuttamista

— mallipiirturilevyn hyväksyntää

— mallipiirturilevyn hyväksynnän peruuttamista

Tyyppihyväksyntänumero:

.....

1. Tavaramerkki tai kauppanimi .....

2. Tyypin tai mallin nimi .....

3. Valmistajan nimi .....

4. Valmistajan osoite .....

5. Päivä, jona hakemus tyyppihyväksyntää varten on esitetty .....

6. Tutkimuslaitos .....

7. Testausselosteen päiväys ja numero(t) .....

8. Hyväksymispäivä .....

9. Tyyppihyväksynnän peruuttamispäivä .....

10. Valvontalaitetyyppi tai -tyypit, jossa/joissa levy on tarkoitettu käytettäväksi

11. Paikka .....

12. Päivämäärä .....

13. Liitteenä seuraavat kuvailevat asiakirjat .....

14. Huomautuksia (myös tiedot mahdollisten sinettien sijainnista)

(allekirjoitus)

([1]) Tarpeeton viivataan yli.

▼C1

III. TYYPPIHYVÄKSYNTÄTODISTUS DIGITAALISILLE AJOPIIRTUREILLE

Tyyppihyväksynnän antaneen jäsenvaltion on annettava hakijalle jäljempänä esitetyn mallin mukainen tyyppihyväksyntätodistus. Ilmoittaessaan muille jäsenvaltioille annetuista tyyppihyväksynnöistä tai tarvittaessa niiden peruuttamisista jäsenvaltion on käytettävä tämän todistuksen jäljennöksiä.

TYYPPIHYVÄKSYNTÄTODISTUS DIGITAALISILLE AJOPIIRTUREILLE

Toimivaltaisen viranomaisen nimi .....

Ilmoitus koskee ([1]):

☐ tyyppihyväksyntää, joka koskee:

☐ tyyppihyväksynnän peruuttamista, joka koskee:

☐ valvontalaitemallia

☐ valvontalaitteen osaa ([2])

☐ kuljettajakorttia

☐ korjaamokorttia

☐ yrityskorttia

☐ valvontakorttia

Tyyppihyväksyntänumero:

.....

1. Tuotenimi tai tavaramerkki .....
2. Mallinimi .....
3. Valmistajan nimi .....
4. Valmistajan osoite .....
5. Päivä, jona tyyppihyväksyntähakemus on esitetty .....
6. Tutkimuslaitos (-laitokset) .....
7. Testausselosteen päiväys ja numero .....
8. Hyväksymispäivä .....
9. Tyyppihyväksynnän peruuttamispäivä .....
10. Ne valvontalaitte(id)en osien mallit, joiden kanssa käytettäväksi kyseinen osa on tarkoitettu
11. Paikka .....
12. Päivämäärä .....
13. Liitteenä seuraavat kuvailevat asiakirjat .....
14. Huomautuksia (myös tiedot mahdollisten sinettien sijainnista)

(allekirjoitus)

([1]) Merkitään rasti asianomaisiin kohtiin.
([2]) Yksilöidään ilmoituksen kohteena oleva osa.

▼C1

IV. TYYPPIHYVÄKSYNTÄTODISTUS ÄLYKKÄILLE AJOPIIRTUREILLE

Tyyppihyväksynnän antaneen jäsenvaltion on annettava hakijalle jäljempänä esitetyn mallin mukainen tyyppihyväksyntätodistus. Ilmoittaessaan muille jäsenvaltioille annetuista tyyppihyväksynnöistä tai tarvittaessa niiden peruuttamisista jäsenvaltion on käytettävä tämän todistuksen jäljennöksiä.

TYYPPIHYVÄKSYNTÄTODISTUS ÄLYKKÄILLE AJOPIIRTUREILLE

Toimivaltaisen viranomaisen nimi .....

Ilmoitus koskee ([1]):

☐ tyyppihyväksyntää, joka koskee:

☐ tyyppihyväksynnän peruuttamista, joka koskee:

☐ valvontalaitemallia

☐ valvontalaitteen osaa ([2])

☐ kuljettajakorttia

☐ korjaamokorttia

☐ yrityskorttia

☐ valvontakorttia

Tyyppihyväksyntänumero:

.....

1. Tuotenimi tai tavaramerkki .....
2. Mallinimi .....
3. Valmistajan nimi .....
4. Valmistajan osoite .....
5. Päivä, jona tyyppihyväksyntähakemus on esitetty .....
6. a) Toiminnallisuustodistuksen testilaboratorio .....
   b) Turvallisuustodistuksen testilaboratorio .....
   c) Yhteentoimivuustodistuksen testilaboratorio .....
7. a) Toiminnallisuustodistuksen päiväys ja numero .....
   b) Turvallisuustodistuksen päiväys ja numero .....
   c) Yhteentoimivuustodistuksen päiväys ja numero .....
8. Hyväksymispäivä .....
9. Tyyppihyväksynnän peruuttamispäivä .....
10. Ne valvontalaitte(id)en osien mallit, joiden kanssa käytettäväksi kyseinen osa on tarkoitettu
11. Paikka .....
12. Päivämäärä .....
13. Liitteenä seuraavat kuvailevat asiakirjat .....
14. Huomautuksia (myös tiedot mahdollisten sinettien sijainnista)

(allekirjoitus)

([1]) Merkitään rasti asianomaisiin kohtiin.
([2]) Yksilöidään ilmoituksen kohteena oleva osa.