Eesti riiklik CA poliitika

Digitaalse sõidumeeriku süsteemile

Eesti Riiklik Autoregistrikeskus (ARK)
Estonian Motor Vehicle Registration Centre

Versioon

Visand Versioon 0.1	03.01.2005	ARK poolt alustatud põhi	
Visand Versioon 0.2	07.01.2005	Juhtkirja märkused ja kommentaarid	Jüri Voore Tarmo Milva SK
Visand Versioon 0.3	15.01.2005	Ver.0.3 parandused kinnitatud …	ARK
Visand Versioon 0.4	03.02.2005	Korrektuurid (parandused) : Ristviidete numeratsioon muudetud Võrdlustabel 19 lisatud	Jüri Voore Tarmo Milva SK
Visand Versioon 0.4	18.02.2005	Visandi versioon 1.0 kinnitamiseks ja tõlge vormindatud	Jüri Voore SK
Visand Versioon 0.5	24.03.2005	Teksti muudatused vastavalt Review Findings letter G07-TRVA/JB7jb/(2005)D76468 of 15.03.2005	ARK SK
Kinnitatud versioon 1.0	06.04.2005	Kinnitatud “Digital Tachograph Root Certification Authority” poolt 06.04.2005	

Sisukord

1 Sissejuhatus

Käesolev dokument on Riiklik CA poliitika Eesti Digitaalse Sõidumeeriku Süsteemile.

See Riiklik CA poliitika on kooskõlas

- Sõidumeeriku Süsteemi nõukogu määrus, 2135/98
- Komisjoni määrus 1360/2002
- "Guideline and Template National CA policy "
- "Common Security Guidelines"

Dokumendis kasutatud lühendid on täpsustatud selles dokumendis, peatükis 2.2.

1.1 Vastutav asutus

Vastutav asutus Riiklikus CA poliitikas on liikmesriigi institutsioon, MSA, Eesti Riiklik Autoregistrikeskus, mis täitab ka CIA rolli.

MSA määrab lepinguga AS Sertifitseerimiskeskuse tegevuse MSCA ja CSP rollis.

AS Sertifitseerimiskeskus tegutseb varadega, mis on seotud digitaalse sõidumeeriku süsteemiga, järgneval aadressil :

AS Sertifitseerimiskeskus

Pärnu mnt. 12

10148 Tallinn

Eesti.

MSCA ja CIA võivad teha alltöövõtulepinguid allettevõtjatega (Service Agencies). Teenindus esinduste kasutus ei vähenda MSA üldisi vastutusi nendele protsessidele.

Eesti Riiklik Autoregistrikeskuse klienditeenindus punktidega (RA) on tagatud regionaalne töö üle Eesti.

RA teenindus on täpsustatud teenuse osutamise kirjelduses (PS).

CSP-le määratud Service Agency on AS Sertifitseerimiskeskus, mis on täpsustatud teenuse osutamise kirjelduses (PS).

Kaardi personaliseerimise asutuse (CPO) funktsioonid sooritatakse :

Trüb Baltic AS

Liivalaia 8

10118 Tallinn

Estonia

Nagu nad on kirjeldatud CPO teenuse osutamise kirjelduses (PS).

1.2 Kinnitamine

Riiklik CA Poliitika kinnitatud:

Digital Tachograph Root Certification Authority
Traceability and Vulnerability Assessment Unit
European Commission
Joint Research Centre, Ispra Establishment (TP.360)
Via E. Fermi, 1
I-21020 Ispra (VA)
Italy
6. aprill 2005.a.

1.3 Kättesaadavus ja kontaktid

Riiklik CA poliitika on avalikult kättesaadav aadressilt http://www.ark.ee

Küsimused Riikliku CA poliitika asjus peaks adresseerima:

Eesti Riiklik Autoregistrikeskus
Mäepealse 19
12618 Tallinn
Eesti

Riikliku CA poliitika kontakt detailid

Dokumendi nimi:	Eesti Riiklik CA Poliitika Digitaalse Sõidumeeriku süsteemile
Dokumendi identsus:	EstNCAPolicy.pdf

2 Sõnaseletuste loend/Definitsioonid ja lühendid

2.1 Sõnaseletuste loend/Definitsioonid

CA Poliitika: kordade kogum, mis määrab ära võtmete, sertifikaatide ja seadmete kasutamise ulatuse kasutajatele ja taotlejatele, koos kindlate turvanõuetega.
Kaart/Sõidumeeriku kaart: Mikroskeemiga varustatud kaart, mis selles poliitikas vastab ka terminitele ”**IC-Card**” ja ”**Smart Card**”.
Kaardi kasutaja: Isik või asutus, kes kasutab Sõidumeeriku kaarti. Kaasa arvatud autojuhid, ettevõtte esindajad, töökoja töötajad ja järelvalve asutuse töötajad.
Sertifikaat: üldiselt on sertifikaat teksti struktuur, mis on seotud digitaalse allkirjaga, mida kasutatakse väljastaja poolt, et kinnitada informatsiooni

õigsust ning samuti, et sertifitseeritud avaliku võtme haldaja suudaks tõestada väljastatud privaatvõtmete õigsust.
Sertifitseerimisasutuse süsteem (CAS): infosüsteem, kus sertifikaadid väljastatakse allkirjastatud sertifikaadi (kasutaja) andmete poolt koos CA privaatse allkirjastamise võtmega.
Sertifitseerimise teenuse osutamise kirjeldus (CPS): sertifitseerimis-asutuse, mis tegeleb sertifikaatide väljastamisega, teenuse osutamise kirjeldus ja on seotud tegeliku CA poliitikaga. CPS on selles poliitikas asendatud teenuse osutamise kirjeldusega (PS), sest sellele on laiem ulatus ning seob samuti võtmed, sertifikaadid ja seadmed.
Vahendid: Sõidumeeriku süsteemis eksisteerivad järgmised vahendid: Sõidumeeriku kaardid, VU (vehicle units) ja liikumisandurid (Motion Sensors).
Tootja/Varustuse tootja: Sõidumeeriku varustuse tootjad. Selles poliitikas, suuremalt osalt mõeldakse VU ja liikumisanduri tootjaid, kuna neil on märgatav osa süsteemis.
Liikumisanduri võti: Sümmeetriline võti, mida kasutatakse liikumisanduri ja VU jaoks, et kindlustada mõlemapoolset äratundmist (tuvastust).
Teenuse osutamise kirjeldus (PS). Turvaliste teenuste osutamise kirjeldus, mis on rakendatud sõidumeeriku protsessides. PS on võrreldav standardse PKI CPS dokumendiga.
Isiklik võti: Asümmeetrilise võtme privaat osa, mida kasutatakse avaliku võtme krüptimiseks. Isiklikku võtit kasutatakse tavaliselt digitaalse allkirjaga allkirjastamiseks või teadete dekrüptimiseks. Samuti nimetatakse seda salavõtmeks.
Avalik võti: Asümmeetrilise võtmepaari avalik osa, mida kasutatakse avaliku võtme krüptimiseks. Avalikku võtit kasutatakse tavaliselt digitaalallkirjade kinnitamiseks või isikliku võtme omaniku teadete krüptimiseks.
RSA võtmed: RSA (Rivest, Shamir, Adelmann) on krüptograafiline algoritm, mida kasutatakse asümmeetrilistel (PKI) võtmetel Sõidumeeriku süsteemis.
Service Agency: Üksus, mis täidab ülesandeid MSCA või CPO nimel, allettevõtja.
Sõidumeeriku kaardid/Kaardid: Kasutusel on neli erinevat tüüpi kiibiga kaarti, mida kasutatakse Sõidumeeriku süsteemis: autojuhikaart, tööandja kaart, töökoja kaart ja kontrollija kaart.
Kasutaja: Kasutajad on seadmete kasutajad ja kas **kaardi omanikud** või Vehicle units/Motion Sensors tootjad. Kõik kasutajad on üheselt identifitseeritavad isikud.

Selles dokumendis:
Allkirjastatud: kui see poliitika vajab allkirjastamist, siis tehakse seda turvalise ning kontrollitava digitaalse allkirjaga.
Kirjutatud: see poliika peab olema kirjalik, et kõik sellega seotud osapooled saaksid vajadusel sellest informatsiooni.

2.2 Lühendite nimekiri

CA Certification Authority (sertifitseerimise asutus)
CAS Certification Authority System (sertifitseerimisasutuse süsteem)
CIA Card Issuing Authority (kaardiväljastamise asutus)
CC Common Criteria (tava kriteerium)
CP Card Personalisation service (kaardi personaliseerimise teenus)
CPO Card personalising organization (kaardi personaliseerimise asutus)
CPS Certification Practice Statement (sertifitseerimise teenuse osutamise kirjeldus)
CSP Certificate Service Provider (sertifitseerimise teenuse pakkuja)
DB Database (andmebaas - AB)
ERCA European Root CA (Euroopa Root CA)
HSM Hardware Security Module (riistvaraline turvamoodul)
ISSO Information System Security Officer (andmeturbe töötaja)
ITSEC Information Technology Security Evaluation Criteria (IT turvalisuse hindamise kriteeriumid)
KG Key Generation (võtme genereerimine)
MS Member State of Tachograph System (sõidumeeriku süsteemi liikmesriik)
MSA Member State Authority (liikmesriiki esindav asutus)
MSCA Member State CA (liikmesriigi CA)
PIN Personal Identification Number (personaalne identifitseerimise number)
PKI Public Key Infrastructure (avaliku võtme infrastruktuur)
PS Practice Statement (teenuse osutamise kirjeldus)
RA Registration Authority (registreerimisasutus)
RSA A specific Public key algorithm (teatud avaliku võtme algoritm)
SA System Administrator (süsteemi administraator)
VU Vehicle Unit (sõiduk)
VUP VU personalizing organization (sõiduki personaliseerimise asutus)

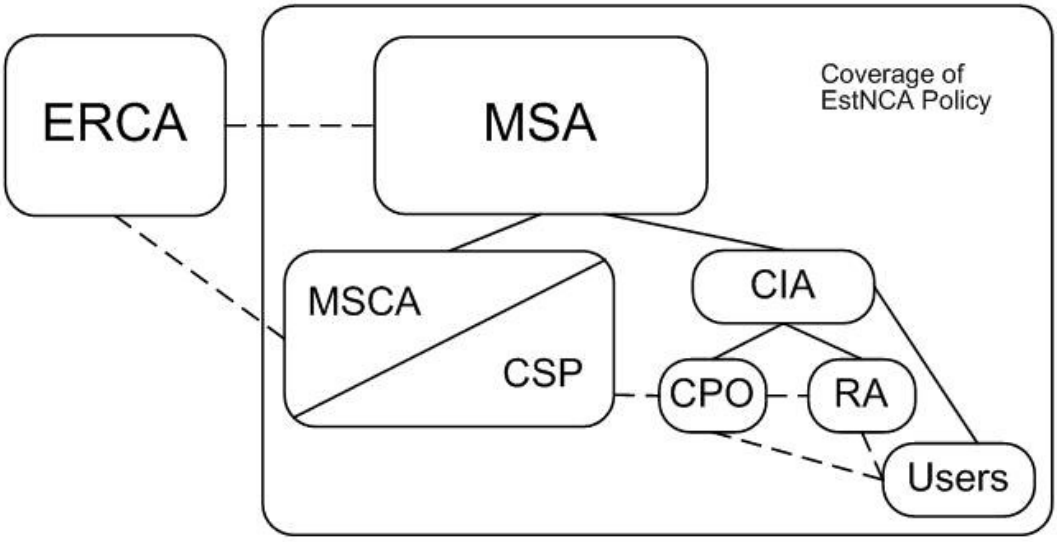
3 Käsitlusala ja rakendatavus

See Riiklik CA poliitika on kehtiv ainult Digitaalse Sõidumeeriku süsteemile.

MSCA poolt väljastatud kaardid ja sertifikaadid on kasutuses ainult Digitaalse Sõidumeeriku süsteemis.

4 Üldised sätted

See osa sisaldab sätteid MSA, CIA, RA, MSCA, CSP, CPO, CP, Service Agencies ja kasutajate kohustuste kohta.



Hierarhia, suhted ja andmete voog Riiklikus Sõidumeeriku Süsteemis

Pildil kasutatud lühendid ja sümbolid:

ERCA	European Root CA (Euroopa Root CA)
MSA	Member State Authority (Liikmesriigi asutus)
MSCA	Member State CA (Liikmesriigi CA)
CSP	Certificate Service Provider (Sertifitseerimisteenuse pakkuja)
CIA	Card Issuing Authority (Kaardi väljastamise asutus)
CPO	Card Personalising Organization (Kaardi personaliseerimise asutus)
CP	Card Personalisation service (Kaardi personaliseerimine)
RA	Registration Authority of CIA (CIA poolne registreerimisasutus)
_____	Responsibility hierarchy (Vastutuse hierarhia)
_ _ _ _ _ _ _ _	Data, information or card flow (andmete, informatsiooni või kaardi liikumine)

4.1 Kohustused

See osa sisaldab sätteid, millega määratakse kohustused alljärgnevatele

- MSA
- MSCA
- CIA
- CSP
- RA
- CPO
- Kasutajad (Kaardi omanikud)

- Service Agencies

4.1.1 MSA kohustused

Vastavalt NCA poliitikale on MSA-l järgmised kohustused:

a) Hoida Riiklikku CA poliitikat
b) Ametisse nimetada MSCA ja CIA;
c) Auditeerida CSP, CPO ja RA;
d) Kinnitada MSCA, CSP, CPO, CP ja RA kirjeldused teenuse osutamiseks;
e) Teavitada määratud osapooli ja Service Agencies sellest poliitikast;
f) Saada kinnitus ERCA-lt sellele poliitikale.

4.1.2 MSCA kohustused

a) Järgida Riiklikku CA poliitikat;
b) Avaldada MSCA teenuse osutamise kirjeldus (MSCA PS), mis sisaldab viidet Riiklikule CA poliitikale ja on kinnitatud MSA poolt;
c) Üle vaadata, et ERCA Root Policy nõudmised saaks realiseeritud MSCA sertifikaadi taotlemisel;
d) Omada piisavat organisatsioonilisi ja majanduslikke vahendeid, et tegutseda kindlalt vastavalt selles poliitikas kehtestatud nõuetele, eriti aga kanda usaldusega seotud riski, mis on kirjeldatud punktis 5.

MSCA tagab, et kõik MSCA määratud nõudmised, mis on selles poliitikas kirjeldatud, on rakendatud.

MSCA-l on vastutus, et selles poliitikas kirjeldatud protseduurid vastaksid nõudmistele ka juhul kui tehnilised lahendused on sõlmitud allettevõtjaga (Service Agency (CSP)). MSCA vastutab, et Service Agency tegutseks vastavalt sellele Riiklikule CA poliitikale ja PS'le.

4.1.3 CIA kohustused

a) Tagada, et taotluse protsessist edastatakse korrekne ja asjakohane kasutaja informatsioon CPO-le.
b) Teavitada selle poliitika nõuetest kasutajaid, mis on seotud süsteemi kasutusega.
c) Omada piisavat organisatsioonilisi ja majanduslikke vahendeid, et tegutseda kindlalt vastavalt selles poliitikas kehtestatud nõuetele, eriti aga kanda usaldusega seotud riski, mis on kirjeldatud punktis 5.

4.1.4 CSP kohustused

- Tagada, et korrektsed sertifikaadid oleks edastatud CP-le;
- Hoida MSCA privaatvõtme konfidentsiaalsust;
- Järgida seda Riiklikku CA poliitikat;
- Avaldada CSP teenuse osutamise kirjelduse (CSP PS), mis sisaldab viidet sellele Riiklikule CA poliitikale ja on kinnitatud MSA poolt.

4.1.5 CPO kohustused

Määratud CPO peab:

- Järgima seda Riiklikku CA poliitikat
- Avaldama CSP teenuse osutamise kirjelduse (CSP PS), mis sisaldab viidet sellele Riiklikule CA poliitikale ja on kinnitatud MSA poolt.
- Tagama, et kõik nõudmised, mis selles poliitikas on kirjeldatud, oleks rakendatud.

CPO-l on vastutus, et selles poliitikas kirjeldatud protseduurid vastavad nõudmistele.

4.1.6 RA kohustused

Määratud RA peab:

a) Tagama, et korrektsed ja asjakohased taotluse andmed oleks edastatud CIA-le ja CPO-le
b) Teavitama kasutajaid nõuetest, mis on seotud selle poliitikaga ja Sõidumeeriku süsteemi kasutamisega..

4.1.7 Service Agency kohustused

Service Agency-tel, kui nad pakuvad teenuseid selle poliitika raames, on kohustused MSA-le, vastavalt lepingu tingimustes kirjeldatule. Hoolimata nendest tingimustest jääb MSA-le täielik vastutus kogu Sõidumeeriku süsteemi üle, mis on kajastatud selles dokumendis.

4.1.8 Kaardiomaniku kohustused

CIA kohustab läbi tingimuste (vaata punkti 10.2.2) kasutajat täitma järgmisi kohustusi:

4.1.8.1 Kõikide kaartide tüübid

a) täpsed ja lõplikud andmed oleks edastatud RA-le ja CIA-le, vastavalt selle poliitika nõudmistele, eriti mis on seotud registreerimisega;
b) võtmeid ja sertifikaate kasutatakse ainult Sõidumeeriku süsteemis;
c) kaarte kasutatakse ainult Sõidumeeriku süsteemis;

d) eeldatud on mõistlik hoolitsus, et vältida lubamatut juurdepääsu seadme privaatvõtmele ja kaardile;

e) kasutajal võib ainult eriolukorras ja kindlalt määratud ajal olla valduses rohkem kui üks kaart või kombinatsioon kaartidest;

f) kasutaja ei tohi kasutada vigastatud või aegunud kaarti;

g) kasutaja ei tohi võltsida või muuta kaarti mingil moel;

h) kasutaja peab viivitamatult teavitama CIA-d, kui enne sertfikaadi aegumise lõppu peaks juhtuma midagi alljärgnevat:

- seadme privaatvõti või kaart on kaotatud, varastatud või potensiaalselt ohustatud
- sertifikaadi sisu on muutunud või muutub ebatäpseks.

4.1.8.2 Autojuhikaart

a) Kasutajal võib olla ainult üks kehtiv autojuhikaart;
b) Kasutaja võib kasutada ainult enda võtit, sertifikaati ja kaarti;

4.1.8.3 Töökoja kaart

a) Kasutaja peab kaitsma enda PIN-koodi
b) Kaarti ei tohi viia väljaspoole töökoda, v.a. juhul kui see on vajalik seadistamiseks, kalibreerimiseks või paranduseks

4.1.9 VU tootjate kohustused (personaliseerimise rollis)

Pole Eestis momendil kasutusel.

4.1.10 Liikumisandurite tootjate kohustused (personaliseerimise rollis)

Pole Eestis kasutusel.

5 Vastutus

5.1 MSCA, CPO ja RA vastutused MSA-le ja CIA-le

MSCA, CPO ja RA vastutavad oma kohustuste täitmise eest, isegi kui mõned või kõik on sisseostetud SA-dest. Kui MSCA või CPO tahavad sõlmida allettevõtulepinguid, siis peavad nad ette teatama sellistest kavatsustest ja tagama MSA-le kõik võimalused, et MSA vastaks talle määratud kohustustele. RA-le ei ole lubatud sõlmida allettevõtulepinguid.

MSCA, CPO või RA on vastutavad kahjustuste eest oma kohustuste täitmisel ainult juhul kui on põhjustatud omast lohakusest. Kui asutus on käitunud vastavalt sellele poliitikale ja vastavale PS-le, siis seda ei võeta kui lohakust.

MSCA, CPO või RA ei kanna vastutust lõppkasutajate suhtes, vaid ainult MSA-le ja CIA-le.

Kogu vastutus lõppkasutajate suhtes on MSA-l või CIA-l.

5.2 MSA ja CIA vastutus lõppkasutajate ja osapoolte suhtes

MSA on vastutav regulatsiooni (EEC) nr. 3821/85, regulatsiooni (EC) nr. 2135/98 ja Annex IB rakendamise eest. Täpsemalt on mõeldud, et MSA vastutab, et:

a) Sertifikaat oleks valmistatud vastavalt seadusandlusele ja sellele poliitikale;

b) Sertifikaat sisaldaks kogu informatsiooni, mis on vajalik Sõidumeeriku sertifikaadil ajahetkel, mil ta on väljastatud, ja eriti kaardi omaniku andmeid, mis on antud taotlemisel.

CIA-l on vastutus kinnitada, et kaardivaldaja andmed sertifikaadil oleks vastavuses andmetega taotlusel.

MSA või CIA ei vastuta lõppkasutajatele ja osapooltele tekitatud kahjude eest, juhul kui:

1) Valed või puudulikud andmed on esitatud taotleja poolt, välja arvatud kui on tõestatud MSA või CIA poolne lohakus;

2) Sertifikaadi kasutamine väljaspool seadusandlusega määratud eesmärke;

3) On avalikustatud PIN-kood, välja arvatatud juhtudel, mis on tulenevad MSA või CIA tegudest;

4) Esineb VU talitlushäire, telekommunikatsioonide või sarnaste vahendite kasutamises, mis võib takistada sertifikaadi kasutamist Sõidumeeriku süsteemis.

MSA või CIA ei ole kunagi vastutav majanduslike kahjude või teiste mitte otseste kahjude osas lõppkasutajale, osapooltele või nendega seotud lepingulistele partneritele.

Sõidumeeriku kaardid, võtmed ja sertifikaadid on mõeldud kasutamiseks ainult Sõidumeeriku süsteemis. Kõik teised kasutatavad sertifikaadid on vastuolus selle poliitikaga ja sellega seosnevalt ei kanna MSA ega CIA mingit vastutust selliste rikkumiste suhtes.

5.3 Vastav seadusandlus

Kahjustuste eest vastutus määratakse vastavalt Eesti Vabariigi võlaõigus seadusele.

6 Tõlgendus ja jõustamine

6.1 Kehtiv seadus

Sertifikaadi poliitika sätted on kooskõlas Eesti seadustega.

7 Konfidentsiaalsus

Konfidentsiaalsus on piiratud vastavalt direktiivile 95/46/EC, Andmebaasi seadusele, Isikuandmete kaitse seadusele ja Liiklusregistri põhimäärusele, mis kaitseb isikuid isiklikuandmete valest töötlemisest.

7.1 Konfidentsiaalsena hoitav informatsioon

Kõik füüsiliste või juriidiliste isikute andmed, mis on MSCA, CPO, CIA või SA valduses ning mis ei esine väljastatud kaartidel või sertifikaatidel, on konfidentsiaalsed. Neid andmeid ei väljastata ilma kasutaja otsese loata ega (kui võimalik) ilma kasutaja tööandja või esindaja loata, väljaarvatud seadusega määratud juhtudel.

Kõik privaatsed ja salajased võtmed, mida kasutatakse ja käsitletakse MSCA või CP poolt selle poliitika raames, hoitakse konfidentsiaalsena.

Auditi märkused ja aruandeid ei tehta täies mahus avalikuks, välja arvatud seaduses määratud juhtudel.

7.2 Mitte konfidentsiaalsena hoitav informatsioon

Isikut tõendav või füüsilise või juriidilise isiku andmed, mis on esitatud kaardil ja sertifikaadil, ei ole konfidentsiaalne, väja arvatud seaduses või eri kokkuleppel määratud juhtudel.

8 Teenuse osutamise kirjeldus (PS)

MSCA, CIA, CSP, CPO, CP ja RA peavad esitama praktika ja protseduuride kohta kirjeldused, et nad täidavad kõiki nõudmisi, mis on kirjeldatud selles Riiklikus CA poliitikas. PS-id kiidab heaks MSA.

Konkreetsemalt öeldes:

a) PS peab tuvastama välisasutuste kohustused, mis toetavad MSCA ja CIA teenuseid, kaasaarvatud rakendatavad poliitikad ja tavad.

b) Praktika avaldus peab kättesaadav olema MSA-le, Sõidumeeriku süsteemi kasutajatele ja seotud osapooltele (nt. juhtimisasutustele);

   Ometi, pole MSCA/CIA-l üldiselt nõutav teha kõiki teenuse detaile avalikuks ja kättesaadavaks kasutajatele;

c) MSCA/CIA juhtkonnal on vastutus kindlaks teha, kas PS on korralikult realiseeritud;

d) MSCA/CIA peab määratlema PS-i ülevaatamise korra;

e) MSCA, CIA, CSP, CPO, CP ja RA peavad teatama muudatustest vastava teadaandega, mis kavatsetakse teha PS-is ning peavad järgneva heakskiiduga tegema ümbertöötatud PS-i koheselt kättesaadavaks.

9 Seadmete haldus

Sõidumeeriku süsteemis määratletud varustus:

- Sõidumeeriku kaardid
- Sõiduki osad
- Liikumisandurid

Arvestades seda, et sõidukeid ja liikumisandureid ei toodeta Eestis, siis selle poliitika osa katab ainult Sõidumeeriku kaarte.

Varustust käsitletakse ja hallatakse mitmete osade poolt:

- CIA (kaartide tühistamine, registri hooldamine);
- RA (vastu võtta avaldus, esitatud andmete kinnitamine, andmete registreerimine, registreerimiskaardi uuendamine, kaardi väljaandmine jne.);
- MSCA (Liikumisanduri võtmed);
- CPO (tellimuse töötlus);
- CP (visuaalne ja elektroniline personaliseerimine, võtmed);
- CSP (sertifikaadid).

MSA poolt läbi viimiseks järgnevad funktsioonid:

- Kvaliteedikontroll (liigi heakskiit). Tegeliku töö teeb SA, mis on määratud CP osale;
- PS kinnitamine.

CIA poolt läbi viimiseks järgnevad funktsioonid:

- Avaldused kaartidele;
- Avalduse heakskiitmise registreerimine;
- Andmete hoidmine (AB) ja registreeritud kaartide info olekule;
- CPO-sse edastavate personaliseerimise andmete järelvalve;
- Infovahetus teiste liikmesriikidega;
- Kaotatud ja leitud kaartidega käsitlemine.

MSCA poolt läbi viimiseks järgnevad funktsioonid:

- Eesti jaoks MSCA võtmete genereerimine ja kasutajaliidese haldamine ERCA sertifikaadi protsessi juures.

CSP poolt läbi viimiseks järgnevad funktsioonid:

- Kaartide jaoks sertifikaatide genereerimine vastavalt CP tellimustele;
- Väljastatud sertifikaatide hoidmine andmebaasis (AB);
- Hoidma MSCA võtmete turvalisust.

CP poolt läbi viimiseks järgnevad funktsioonid:

- Kvaliteedikontroll (testkaardi näidised);
- Liikumisanduri võtme turvalisuse hoidmine;
- Sertifikaadi taotluse saatmine CSP-le;
- Võtme ja sertifikaadi sisestamine;

- Kaartide personaliseerimine;
- Kaartide toimetamine määratud kohtadesse
- Töökoja jaoks kaartide ja PIN-koodide jaotamine määratud kohtadesse

RA poolt läbi viimiseks järgnevad funktsioonid:

- Kasutaja registreerimine;
- Kaartide väljastamine kasutajatele;
- Võimalus kaardi funktsionaalsuse kontrollimiseks.

10 Sõidumeeriku kaardid

10.1 Kvaliteedikontroll – MSA/CP funktsioon

MSA/CP tagavad, et personaliseeritakse ainult vastavalt regulatsioonidele tüübikinnitatud kaarte.

10.2 Taotlus kaardile – CIA poolt käsitletud

CIA informeerib kasutajaid tingimustest ja nõudmistest, mis on seotud kaardi kasutamisega. See informatsioon on saadaval eesti ja inglise keeles.

Kasutaja peab nõustuma kaardi taotlemisel ja kätte saamisel nende tingimuste ja nõudmistega.

10.2.1 Kasutaja taotlus

Sõidumeeriku kaardi taotlejad peavad täitma CIA poolt määratud taotluse. Minimaalselt on vajalik korrektne informatsioon, et tuvastada kasutaja. Tööandjale töökoja- ja kontrollkaartide taotlemisel on samuti vaja täpsustada asutus.

Järgnev informatsioon on vajalik kaardi väljastamiseks. Juhul kui andmed pole saadud mujalt, on vajalik järgmised andmed:

- Nimi;
- Elukoht;
- Aadress
- E-maili aadress;

Juhikaardile:

- Juhiloa number;
- Sünnikuupäev ja -koht;
- Pilt ja allkiri;
- Isikukood;
- Eelmine / praegune juhikaardi number, kui on olemas;

- Eelimise /praeguse juhikaardi väljastaja.

Töökoja kaardile:

Töökoja kaarte väljastatakse ainult juriidilise isiku poolt taotlemisel füüsilisele isikule, kui täidetakse alljärgnevad tingimused:

- Nimi ja õiguslik seisund asutuses;
- Kaardikasutaja nimi (kaasaarvatud perekonnanimi, eesnimed ja isikukood);
- Kaardikasutaja pilt ja allkiri.

Kontrollija kaardile:

Kontrollija kaarte väljastatakse ainult juriidilise isiku poolt taotlemisel füüsilisele isikule, kui täidetakse alljärgnevad tingimused:

- Nimi ja õiguslik seisund asutuses;
- Kaardikasutaja nimi (kaasaarvatud perekonnanimi, eesnimed ja isikukood), vajalik on üksuse määramine;
- Kaardikasutaja pilt ja allkiri.

Tööandja kaardile:

Veofirmade sertifikaate väljastatakse firmale, mis hoiab või omab sõidukeid, millele on kohandatud digitaalne sõidumeerik, esindajatele, kui täidetakse alljärgnevad tingimused:

- Nimi ja õiguslik seisund asutuses;
- Kõik oluline olemasolev registreerimise informatsioon (nt. firma registreerimine), mis on seotud juriidilise isiku või asutusega ;
- Kasutaja seos juriidilise isiku või asutusega;
- Kaardikasutaja nimi (kaasaarvatud perekonnanimi, eesnimed ja isikukood), vajalik on üksuse määramine;
- Kaardikasutaja pilt ja allkiri.

10.2.2 Leping

Kaardi taotlemisel ja kätte saamisel peab taotleja tegema lepingu MSA-ga (või CIA-ga), mis sisaldab vähemalt:

- Kasutaja nõusolekut tingimuste ja nõudmiste kohta, seoses sõidumeeriku kaardi kasutamisega ja käsitlemisega;
- Kasutaja nõustub ja kinnitab, juhul kui ta ei ole CIA teavitanud vastupidisest, et alates kaardi kätte saamisest kuni selle kehtivuse lõpuni:

- Kasutaja ei luba volitamata isikutel juurdepääsu oma kaardile;
- Kogu kasutaja poolt CIA-le esitatud informatsioon, mis on asjakohane kaardile, on tõene;
- Kaarti kasutatakse kohusetundlikult pidevalt vastavalt kaardile kehtestatud piirangutele.

10.2.3 CIA poolsed tingimused - Juhikaardile

Autojuhikaart väljastatakse ainult isikutele, kellel on alaline elukoht taodeldavas riigis.

CIA kontrollib, et juhikaardi taotleja ei omaks kehtivaid autojuhikaarte Eestis või teistes liikmesriikides.

CIA kontrollib, et juhikaardi taotleja omaks kehtivat juhiluba ning vastavaid kategooriaid.

10.2.4 CIA poolsed tingimused – Töökoja kaardile

Töökojakaart väljastatakse ainult töökojale, mis omab kehtivat digitaalse sõidumeeriku töökoja luba.

10.2.5 CIA poolsed tingimused – Kontrollija kaardile

Kontrollija kaart väljastatakse ainult määratud ametlikele kontrollorganitele.

10.2.6 CIA poolsed tingumused – Tööandja kaardile

Tööandja kaart väljastatakse ainult veoseid tegevale firmale.

10.3 Kaartide kehtivusajad

Töökoja kaart kehtib mitte rohkem kui **üks** aasta kaardi väljastamisest.

Autojuhikaart kehtib mitte rohkem kui **viis** aastat kaardi väljastamisest.

Tööandja kaart kehtib mitte rohkem kui **viis** aastat kaardi väljastamisest.

Kontrollija kaart kehtib mitte rohkem kui **viis** aastat kaardi väljastamisest.

CIA töötab välja korra kasutaja teavitamiseks kehtivuse lõppemise kohta.

Uuendamise taotlemisel järgitakse korda, mis on kirjeldatud punktis 10.2.

10.4 Kaardi uuendamine – teostab CIA

Kasutaja taotleb kaardi uuendamist vähemalt **15 päeva** enne kaardi kehtivuse lõppu.

Kui see tingimus on täidetud, siis CIA väljastab uue kaardi kasutajale enne olemasoleva kaardi kehtivuse lõppu.

10.5 Kaardi vahetus – teostab CIA

Kui kasutaja vahetab alalist elukohta, siis ta võib taotleda oma kaardi vahetust. Kui olemasolev kaart on kehtiv, siis kasutaja peab tõendama ainult oma Eesti elukohta, et taotlus saaks heakskiidu.

RA peab uue kaardi kätte andmisel võtma enda valdusesse eelmise kaardi ning tagastama selle päritolu riigi CIA-sse.

Alalise elukoha vahetusega seotud kaardi vahetus peab üldiselt järgima reegleid 10.2 (uue kaardi taotlemiseks).

10.6 Kaotatud, varastatud, kahjustatud või tegevushäirega kaartide vahetus – teostab CIA

Kui kaart on kadunud või varastatud, siis kasutaja peab sellest teatama CIA-le. Kadunud kaardi leidmisest teatatakse CIA-le kasutaja või politsei poolt.

Varastatud ja kadunud kaardid lisatakse musta nimekirja, mis on kättesaadaval kõikidele liikmesriikidele.

Kahjustatud või tegevushäirega kaardid tagastatakse selle väljastanud CIA-le, kes visuaalselt ja elektrooniliselt tühistab kaardi ning lisab musta nimekirja.

Kui kaart on varastatud, kahjustatud või tegevushäirega, siis kasutaja peab taotlema asenduskaarti **7** päeva jooksul.

Arvestades, et kasutaja järgib ülaltoodud nõudeid, väljastab CIA asenduskaardi koos uute võtmetega ja sertifikaatidega 5 tööpäeva jooksul, kui on saadud täielik taotlus.

Asenduskaart saab sama kehtivusaja, mis originaalne kaart. Kui asenduskaardi kehtivus oleks vähem kui kolm kuud, siis CIA võib väljastada asenduskaardi asemel uuendatud kaardi.

10.7 Taotluse kinnitamine registreerimiseks – teostab CIA

CIA peab sisestama kinnitatud avaldused andmebaasi. Andmed tehakse kättesaadavaks CPO-le, kes kasutab neid sertifikaadi genereerimiseks ja kaardi personaliseerimiseks.

10.8 Kaardi personaliseerimine – teostab CPO

Kaardid on personaliseeritud nii visuaalselt kui elektrooniliselt. Isegi kui see teenus on teostatud Service Agent-i (CP) poolt, siis see ei vähenda CPO üldist vastutust.

10.8.1 Visuaalne personaliseerimine

Kaardid peab visuaalselt personaliseerima vastavalt Regulation Annex 1B, lõigule IV [REG-A]. Nimelt märkusele:

- kaardi omaniku foto peab olema kõigil väljastatud kaartidel: Juhikaardil, kontrollkaardil, töökojakaardil, tööandja kaardil.

10.8.2 Kasutaja andmete sissekanne

Andmed peab sisestama kaardile vastavalt Regulatsiooni 1360/2002, Annex 1B, appendix 2 [REG-A], reeglite TCS_403, TCS_408, TCS_413 ja TCS_418 struktuurile, vastavalt kaardi tüübile.

10.8.3 Võtme sissekanne

Privaatvõti sisestatakse kaardile, ilma et see lahkuks võtme genereerimise keskkonnast. See keskkond peab tagama, et ükski inimene, mis tahes tingimusel, ei saaks märkamata enda omandusse genereeritut privaatset võtit. Kui võimalik, siis võtmed genereeritakse otse kaardile või HSM-i poolt. Vaata samuti võtme haldamise punkti 12.2.

10.8.4 Sertifikadi sissekanne

Kasutaja sertifikaat sisestatakse kaardile enne tema väljastamist kasutajale.

10.8.5 Kvaliteedi kontroll

Dokumenteeritud korrad, et tagada: visuaalne informatsioon kasutaja kaartidel, elektrooniline informatsioon väljastatud kaartidele, sertifikaatide omavaheline vastavus ja samuti vastavus omanikuga. Kord kirjeldatakse CPO PS-is.

10.8.6 Väljastamata kaartide tühistamine (hävitamine)

Kõik kaardid, mis on kahjustatud või hävitatud (või mingil muul põhjusel lõpetamata või kätte andmata), peab personaliseerimise käigus füüsiliselt ja elektrooniliselt hävitama.

10.8.7 Kaardi registreerimine ja andmete hoidmine – teostab CPO ja CIA

CPO ja CIA jälgivad, et milline kaart ja kaardi number on väljastatud kasutajale. Kaardi number on määratud CIA poolt ja edastatud CPO-le. Andmed saadetakse CPO baasist CIA andmebaasi.

10.9 Kaartide väljastamine kasutajatele – teostab CP ja RA

a) Personaliseerimine peab olema ajastatud nii, et aeg oleks minimaalne, mis jääb kaardi personaliseemisest tema väljastamiseni kasutajale. Üle öö hoidmine nõuab turvalist hoidlat. Dokumenteeritud kord peab olema erandite tegemiseks. Kaasa arvatud häired tootmisprotsessis, tõrked kätte toimetamisel ja kaartide kaotamisel või vigastamisel.

b) Personaliseeritud kaardid peab koheselt toimetama kohta, kus need väljastatakse kasutajale, mis on samas kontrollitud ala.
c) Personaliseeritud kaardid hoitakse lahus veel personaliseerimata kaartidest.
d) Sõidumeeriku kaardid väljastatakse viisil, et oleks minimaalne kahjurisk.
e) Kaardi kätteandmisel kasutajale, kes ei ole kinnitatud kaardi taotlemisel, on vajalik tõendus kasutaja identiteedi (nt. nimi), kontrollimiseks füüsilise isikuga.

10.10 Autentsuse kood (PIN) – genereeritud CP poolt

See lõik kehtib ainult töökoja kaartidele.
Töökoja kaardid saavad PIN koodi, mida kasutatakse VU-le kaartide määramiseks (Regulation Annex 1B, App 10 [REG-A]: sõidumeeriku kaardid: 4.2.2)

PIN kood koosneb vähemalt neljast märgist (Regulation Annex 1B, App 10 [REG-A]: Vehicle Units:4.1.2).

10.11 PIN-i genereerimine

PIN koodid genereeritakse turvalises süsteemis ja on turvaliselt paigaldatud töökoja kaartidele ning otse-prinditud PIN-ümbrikusse. PIN koode ei hoita kunagi arvutisüsteemis viisil, mis lubaks ühendust PIN-i ja kasutaja vahel. PIN-i genereerimise süsteem peab vastama nõuetele ITSEC E3, CC EAL4 või samaväärse süsteemi kriteeriumitele.

10.12 PIN-i väljastamine

PIN koodid väljastatakse tavapostiga.
PIN koode ei väljastata koos vastavate kaartidega.

10.13 Kaardi kehtetuks tunnistamine – teostab CIA

Pidevalt peab olema võimalik kehtetuks tunnistada kaarte ja sellega seotud igat võtit. Kehtetuks tunnistamise otsuse peab tegema MSA või CIA, teostama peab CIA või tema SA.

CIA-sse tagastatud kaardid peab kehtetuks tunnistama.

Kaartide kehtetuks tunnistamine peab toimuma vastava seadmega ja nii, et kaardi funktsioonid ja võtmed saaks hävitatud. Kaardi peab samuti visuaalselt hävitama.

Kehtetuks tunnistatud kaardid registreeritakse kaartide andmebaasis ja number lisatakse musta nimekirja.

10.14 VU ja liikumisandurid

Antud hetkel Eestis ei rakendata, välja arvatud juhtudel kui tegemist on kahjustatud või vigastatud VU-ga. Töökojad peavad võimalusel väljastama andmed VU-st ja toimetama need firmale (veoseid tegevale). Juhul, kui see ei ole võimalik, siis kirjutab töökoda avalduse sellele firmale.

11 Võtmete haldus: Euroopa juurvõti,Liikmesriigi võtmed, liikumisanduri võtmed

See lõik sisaldab sätteid jägmiste haldamiste kohta:

- Euroopa juurvõti - ERCA avalik võti;
- Liikmesriigi võtmed, seal hulgas Liikmesriigi võtmepaar(id) allkirjastamiseks;
- Liikumisanduri võtmed.

ERCA avalikku võtit kasutatakse Liikmesriigi sertifikaatide kontrollimiseks. ERCA privaatvõtmega siin ei tegeleta, kuna seda ei väljastata ERCA-st.

Liikmesriigi võtmed on Liikmesriigi allakirjutamise võtmed ja samuti võib neid nimetada Liikmesriigi juurvõtmeteks.

Liikumisanduri võtmed on sümmeetrilised võtmed , mis paigaldatakse töökoja kaardile, VU-le ja liikumisandurile ühtseks äratundmiseks. MSCA saab liikumisanduri võtmed ERCA-lt, salvestab ja jagab neid CP-le.

Transpordi võtmed on RSA võtmepaarid, mida kasutatakse turvaliseks liikumisanduri võtmete üleviimiseks ERCA ja MSCA vahel.

Kui MSCA-l on vajadus teistele krüptovõtmetele, kui üleval loetletud, siis seda ei loeta kui sõidumeeriku süsteemi osa ja ei kajastata selles poliitikas.

Liikmesriigi võtmed ja transpordi võtmed genereeritakse sertifitseeritud HSM-is ja hoitakse füüsiliselt kõrge turvatasemega keskkonnas koos 24/7 turvakontrolliga, elektooniliste lukkudega ja videovalve süsteemiga.

11.1 ERCA avalik võti

MSCA hoiab ERCA avalikku võtit (EUR.PK) nii, et säiliks selle terviklikkus ja kättesaadavus igal ajal. Kui EUR.PK hoitakse CSP-s, siis kehtib sama reegel.

CPO peab tagama, et EUR.PK võti sisestatakse igale sõidumeeriku kaardile ja VU-le.

11.2 Liikmesriigi võtmed

Liikmesriigi võtmed on MSCA allkirjastamise võtmepaar(id), mida kasutatakse kõikide seadmete sertifikaatide allkirjastamiseks.

Võtmepaar sisaldab avalikku võtit (MS.PK) ja privaat või salajast võtit (MS.SK)

MSCA avalik võti sertifitseeritakse ERCA poolt, kuid on alati genereeritud MSCA enda poolt.

Liikmesriigi võtmeid ei tohi kasutada muudel eesmärkidel kui:

a) Sõidumeeriku kaardi sertifikaatide allkirjastamiseks

b) ERCA võtme sertifikaadi taotluse allkirjastamiseks, KCR, nagu on kirjeldatud Annex A [ERCA]

11.2.1 Liikmesriigi võtmete genereerimine

Liikmesriigi võtmepaari genereerimine toimub HSM-is, mis:

- Vastab FIPS 140-2 (või 140-1) 3 või kõrgema taseme nõudmistele [FIPS]; või
- Vastab CEN töögrupi kokkuleppe 14167-2 [CEN] nõudmistele; või
- On usaldusväärne süsteem, mis on vastavuses EAL 4 või kõrgemale tasemele vastavuses ISO 15408 [CC], E3 või kõrgemale ITSEC-is, või samaväärse turvatasemega kriteeriumitele. See peab olema turvalisuse eesmärk või kaitse profiil, mis vastab selles dokumendis esitatud nõudmistele, võttes aluseks riskianalüüsi ning arvestades füüsilise ja teiste mitte tehniliste turvameetmetega.

Tegelik kasutatav seade ja füüsilised turvanõuded on määratud ära **CSP PS-is**.

MSCA võtmepaari genereerimine peab nõudma vähemalt kolme inimese osalemist, kes on usaldatud isiku rollis MSCA-s või CSP-s.

Vähemalt üks nendest inimestest peab olema CAA rollis, kes on vastutav MSCA tegemistest.

Võtmed genereeritakse kasutades algoritmi, võtme pikkusega, mis on vastavuses EU direktiivile [REG] ja tehnilisele lisale [REG-A] (1024 bit RSA).

MSCA-l peab olema rohkem kui üks liikmesriigi võtmepaar koos seotud allkirjastamise sertifikaatidega, et tagada pidev töö.

11.2.2 Liikmesriigi võtmete kehtivuse aeg

Liikmesriigi privaatvõtme EST.SK kasutusaeg on **2** aastat vastava avaliku võtme sertifikaadi väljastamisest ning ei tohi kasutada mitte mingil eesmärgil pärsat kehtivuse lõppu.

Kuna ERCA allkirjastamine on rohkemale kui ühele liikmesriigi võtmepaarile, siis avalikul võtmel ei ole kehtivuse lõppu. Tegelik liikmesriigi avaliku võtme sertifikaatide kehtivus on määratud ja otsustatud ERCA Root Policy-s.

11.2.3 Liikmesriigi privaatvõtme hoidmine

Privaatvõtmeid peab hoidma ja töötlema kindlas kahjustuskindlas seadmes (HSM), mis:

- Vastab FIPS 140-2 (või 140-1) 3 või kõrgema taseme nõudmistele [FIPS]; või
- On usaldusväärne süsteem, mis on vastavuses EAL 4 või kõrgemale tasemele vastavuses ISO 15408 [CC], E3 või kõrgemale ITSEC-is, või samaväärse turvatasemega kriteeriumitele. See peab olema turvalisuse eesmärk või kaitse profiil, mis vastab selles dokumendis esitatud nõudmistele, võttes aluseks riskianalüüsi ning arvestades füüsilise ja teiste mitte tehniliste turvameetmetega.

MSCA privaat allkirjastamisvõtmele juurdepääsuks peab olema topelt kontroll. See tähendab, et ükski inimene ei saa üksi oma valdusesse selliseid õigusi, mis lubaks juurdepääsu keskkonda, kus on hoiul privaatvõtmed. See ei tähenda, et seadmete sertifikaatide allkirjastamise juures peaks olema topelt kontroll.

11.2.4 Liikmesriigi privaatvõtme varukoopia

Liikmesriigi privaat allkirjastamise võtmed võivad olla varundatud, kasutades võtme taastamise korda, mis vajab vähemalt topelt kontrolli. Kord peab olema kirjeldatud CSP PS-is. Lubatud on varundada privaatvõtmeid krüpteeritud formaadis, kui dekrüpteerimine nõuab HSM-i, siis vähemalt topelt kontroll ja nõudmised punktis 11.2.3 peavad olema täidetud. Siiski, kui MSCA-l on mitu võtmepaari vastavalt punktile 11.2.1, siis tegelikult varundamine ei ole vajalik.

11.2.5 Liikmesriigi privaatvõtme deponeerimine

Liikmesriigi privaatvõtmeid ei deponeerita.

11.2.6 Liikmesriigi võtmete ohustamine

Koostatakse kirjalik juhend, mis lisatakse CSP PS-ile, mis määrab meetmed, mida peavad tegema kasutajad ja turvalisuse eest vastutavad inimesed MSCA-s ja/või SA-s (CSP), kui liikmesriigi privaatvõti saab avalikuks või mingil teisel viisil arvestatava või kahtlustatava ohu alla.

Sellisel juhul peab MSCA vähemalt:

- Teavitama ilma viivituseta MSA-d, ERCA-d ja kõiki teisi MSCA-si.
- Alustab taasteplaani teostamisega, hoolimata võimalikust vastuse viivitusest ERCA-st

11.2.7 Liikmesriigi võtmete elu lõpp

MSCA-l peab olema tavad, et tagada alati kehtivate sertifitseeritud liikmesriigi allkirjastmise võtmepaari olemasolu.

Liikmesriigi allkirjastamise võtmepaari kasutamise lõpetamisel peab avaliku võtme arhiveerima ning privaatvõtme peab:

- Hävitama nii, et seda ei saaks taastada; või

- Sälitama sellisel kaitstud viisil, et oleks välistatud selle taaskasutamine.

11.3 Liikumisanduri võtmed

MSCA peab vajadusel taotlema liikumisanduri võtmeid Km, Km_{VU} ja Km_{WC} ERCA-st (regulatsiooni lisa 1B [REG-A]: 11:3.1.3).

MSCA peab edastama ainult töökoja võtme Km_{WC} CP-le, et see sisestataks töökoja kaardile.

MSCA ei tegele liikumisanduri peavõtmega Km või VU liikumisanduri võtmega Km_{WC} ja MSCA tagab, et neid ei kasutata muudel eesmärkidel ja need ei väljuks MSCA turvalisest keskkonnast.

CP võtab üle MSCA kohustused, et tagada töökoja võtme Km_{WC} sisestamine kõikidesse väljastatud töökoja kaartidesse (regulatsiooni lisa 1B [REG-A]; 11:3.1.3)

MSCA ja/või CP peab, hoidmise käigus, kasutamisel ja jagamisel, kaitsma liikumisanduri võtmeid kõrge füüsilise ja loogilise turvakontrolli tagamisega. Võtmeid peab hoidma ja töötlema kindlas kahjustuskindlas seadmes, mis:

- Vastab FIPS 140-2 (või 140-1) 3 või kõrgema taseme nõudmistele [FIPS]; või
- On usaldusväärne süsteem, mis on vastavuses EAL 4 või kõrgemale tasemele vastavuses ISO 15408 [CC], E3 või kõrgem ITSEC-is, või samaväärse turvataseme kriteeriumis. See peab olema turvalisuse eesmärk või kaitse profiil, mis vastab selles dokumendis esitatud nõudmistele, võttes aluseks riskianalüüsi ning arvestades füüsilise ja teiste mitte tehniliste turvameetmetega.

11.4 Võtmete transport

Kogu võtmete transport MSCA ja ERCA vahel peab kasutama vahendeid, meediat ja protokolle, mis on määratud ERCA Root Policy-s. Kui kasutatakse füüsilist meediat võtmete transportimiseks,siis MSA peab määrama volitatud inimese kandma seda meediat.

MSCA võtme sertifikaadi taotlemisel peab kasutama KCR protokolli, mis on kirjeldatud ERCA Root Policy lisas A [ERCA].

MSCA võtab vastu ERCA avaliku võtme levitamise formaadis, mis on kirjeldatud ERCA Root Policy lisas B [ERCA].

MSCA peab tagama, et KID ja võtmete moodulid, mis on saadetud ERCA-sse sertifitseerimiseks ja liikumisanduri võtme levitamiseks, on unikaalsed MSCA domeeni siseselt.

MSCA peab tagama, et privaatvõtmed jääksid HSM-i ja neid ei transporditaks sertifitseerimise käigus.

MSCA peab taotlema liikumisanduri võtit ERCA-lt, kasutades KDR protokolli, mis on kirjeldatud ERCA Root Policy lisas D [ERCA].

12 Seadmete võtmed (asümmeetrilised)

Seadmete võtmed on asümmeetrilised võtmed, mis genereeritakse kuskil väljastamise/tootmis protsessis ja on sertifitseeritud MSCA poolt sõidumeeriku seadmete jaoks:

- Sõidumeeriku kaartidele;
- VU-le (Ei kehti Eestis momendil ega ka mitte lähitulevikus).

Sümmeetrilised liikumisanduri võtmeid siin ei käsitleta.

12.1 Üldised CP/MSCA aspektid k.a. SA ja VU tootjad

Seadme (kaardi) käivitamine, võtme laadimine ja personaliseerimine peab olema teostatud füüsiliselt turvalises ning valvatud keskkonnas. Sisenemine sellele alale peab olema rangelt piiratud, kontrollitav inimese tasemel ja vähemalt kahe inimese kohalolek on vajalik toimingu teostamisel. Registreerima kõik sisestused ja tegemised süsteemis.

Delikaatseid andmed, mis on kasutusel võtme genereerimise süsteemis, ei tohi sellest väljuda, see oleks vastuolus selle poliitikaga.

Delikaatseid andmed, mis on kasutusel kaardi personaliseerimise süsteemis, ei tohi sellest väljuda, see oleks vastuolus selle poliitikaga.

Asutused (allettevõtjad, SA), mis tegelevad võtmete genereerimisega ja kaardi personaliseerimisega rohkem kui ühele Liikmesriigile, peavad tegema seda selgelt eraldatud protsessidena. Registreeritakse iga eraldi protsess ja sellega seotud MSA peab soovil omama sellele juurdepääsu.

MSCA/CPO/SA/VU tootjad: Registreerimine personaliseerimise süsteemis peab sisaldama viidet tellimusele ja nimekirja vastavate seadmete numbrite ja sertifikaatidega. Vastutav MSA peab omama juurdepääsu sellele registreerimisele (logile).

12.2 Seadme võtme genereermine

Võtmeid võib genereerida seadme tootja poolt või CP või MSCA poolt. (Annex 1B [REG-A], Appendix 11:3.1.1).

Isik, kes teostab võtme genereerimist peab tagama, et seadme võtmed genereeritakse turvaliselt ning seadme privaatvõti on hoitud saladuses.

Võtme genereerimine peab toimuma seadmega, mis:

- Vastab FIPS 140-2 (või 140-1) 3 või kõrgema taseme nõudmistele [FIPS]; või
- Vastab CEN töögrupi kokkuleppe 14167-2 [CEN] nõudmistele; või
- On usaldusväärne süsteem, mis on vastavuses EAL 4 või kõrgemale tasemele vastavuses ISO 15408 [CC], E3 või kõrgem ITSEC-is, või samaväärse turvataseme kriteeriumis. See peab olema turvalisuse

eesmärk või kaitse profiil, mis vastab selles dokumendis esitatud nõudmistele, võttes aluseks riskianalüüsi ning arvestades füüsilise ja teiste mitte tehniliste turvameetmetega.

Võtmeid genereeritakse RSA algoritmiga ning võtme pikkuseks on 1024biti (Annex 1B [REG-A], Appendix 11:2.1/3.2).

Genereerimise protseduur ja privaatvõtme hoidmine peab ennetama nende avalikustamist väljaspool loodud süsteemi. Lisaks peab see olema koheselt kustutatud süsteemist, kui see on sisestatud seadmesse.

CPO vastutus on võtta kasutusele vastavad meetmed, et tagada avaliku võtme unikaalsus oma haldusala siseselt, enne kui toimub sertifikaadiga sidumine.(See on oletatavalt tehtud kindlaks, et võtme genereermine on juhuslik oma loomuselt ja seega mitte unikaalse võtme genereerimise tõenäosus on üliväike.)

12.2.1 *Batch* võtmete genereermine

Krüptovõtme genereermist võib teha *batch* protsessina sertifikaadi taotlemise eel või otseses ühenduses sertifikaadi taotlusega.

Batch protsess peab toimuma eraldi oleva seadmel, mis vastab ülaltoodud turvanõuetele. Võti peab terviklikult olema kaitstud kuni sertifikaadi väljastamiseni.

12.2.2 Seadme võtme kehtivus

12.2.2.1 Võtmed kaartidel

Seadme privaatvõtme kasutamise aeg, mis on seotud väljastatud sertifikaadiga, selle poliitika raames, ei tohi kunagi ületada sertifikaadi kehtivuse lõppu.

12.2.2.2 VU

Ei kehti Eestis antud hetkel ega ka lähitulevikus.

12.2.3 Seadme privaatvõtme kaitsmine ja hoidmine - Kaardid

CP peab tagama, et kaardi privaatvõti oleks kaitstud (ja piiratud) kaardiga, mis on kätte antud kasutajale vastavalt selles politiikas kehtestatud kordadele.

Privaatvõtmetest ei hoita koopiaid kuskil mujal kui sõidumeeriku kaardil, kui just ei ole vajalik võtme genereerimisel ja seadme personaliseerimisel.

Mitte mingil juhul ei tohi kaardi privaatvõtit avalikustada või hoida väljaspool kaarti.

12.2.4 Seadme privaatvõtme kaitsmine ja hoidmine – VU-s

Ei kehti Eestis antud hetkel ega ka lähitulevikus.

12.2.5 Seadme privaatvõtme deponeerimine ja arhiveerimine

Seadme privaatvõtmeid ei deponeerita ega arhiveerita.

12.2.6 Seadme avaliku võtme arhiveerimine

Kõik sertifitseeritud avalikud võtmed arhiveeritakse CSP poolt, mis on MSCA poolt sertifitseeitud. Sertifitseeritud avalike võtmete kohta informatsioon võidakse hoida CP juures.

12.2.7 Seadme võtmete elu lõpp

Sõidumeeriku kasutamise lõpetamisel peab avaliku võtme arhiveerima ja privaatvõtme peab:

- Hävitama sellisel viisil, et seda ei oleks võimalik taastada, kui see on CIA võimaluses seda teha; või
- Säilitama sellisel viisil, et oleks kaitstud võimalus seda uuesti kasutusele võtta.

VU kasutamise lõpetamisel peab avaliku võtme arhiveerima ja privaatvõtme peab:

- Hävitama sellisel viisil, et seda ei oleks võimalik taastada; või
- Säilitama sellisel viisil, et oleks kaitstud võimalus seda uuesti kasutusele võtta.

13 Seadme sertifikaadi haldus

See osa kirjeldab sertifikaadi elutsüklit, samuti sisaldab registreerimise tegevust, sertifikaadi väljastamist, levitamist, kasutamist, uuendamist, tühistamist ja lõpetamist.

13.1 Andme sisestus

13.1.1 Sõidumeeriku kaardid

Kaardi omanikud ei taotle sertifikaate. Nende sertifikaadid väljastatakse vastavalt sõidumeeriku kaardi taotluselt saadud informatsioonile (lõik 10.2) ja samuti CIA registrist saadule. Sertifitseerimise jaoks avalik võti on eraldatud võtme genereermise protsessist.

CIA peab tagama, et sisestatud andmed sisaldaksid informatsiooni, mis osutaks *Certificate Holder Reference* (CHR) (viidet sertifikaadi valdajale) unikaalsust. MSCA peab kontrollima CHR unikaalsust oma haldusalas.

13.1.2 VU

Ei kehti Eestis antud hetkel ega ka lähitulevikus.

13.2 Sõidumeeriku kaardi sertifikaadid

13.2.1 Juhi sertifikaadid

Juhi sertifikaadid väljastatakse ainult kompetentsetele juhikaardi taotlejatele.

13.2.2 Töökoja sertifikaadid

Töökoja sertifikaadid väljastatakse ainult kompetentsetele töökoja kaardi taotlejatele.

13.2.3 Kontrollija sertifikaadid

Kontrollija sertifikaadid väljastatakse ainult kompetentsetele kontrollija kaardi taotlejatele.

13.2.4 Tööandja sertifikaadid

Veose firma sertifikaadid väljastatakse ainult kompetentsetele tööandja kaardi taotlejatele.

13.3 VU sertifikaadid

Ei kehti Eestis antud hetkel ega ka lähitulevikus.

13.4 Seadme sertifikaadi kehtivusaeg

Sertifikaadid ei kehti kauem kui vastav seade

- Juhi sertifikaat ei kehti kauem kui **5** aastat.
- Töökoja sertifikaat ei kehti kauem kui **1** aasta
- Kontrollija sertifikaat ei kehti kauem kui **5** aastat.
- Tööandja sertifikaat ei kehti kauem kui **5** aastat.

13.5 Seadme sertifikaadi väljastamine

MSCA peab tagama, et väljastab sertifikaate nii, et nende audentsus ja terviklikkus säiliksid. Sertifikaadi sisu on kirjeldatud regulatsiooni lisas 1B (Regulation Annex 1B [REG-A], appendix 11).

13.6 Seadme sertifikaadi uuendamine ja ajakohastamine

Vaata seadme haldust (lõik 9). Kuna sertifikaadid ja kaardid omavad sama kehtivuse aega, siis nendega tegeletakse ühtselt. VU sertifikaadid, kas ei oma kehtivuse lõppu või omavad väga pikka kehtivust, kuna on eeldatud, et seadme eluiga on lühem kui sertifikaadil.

13.7 Üldsusele avalikud seadmete sertifikaadid ja informatsioon

CIA peab tagama, et sertifikaadid saaksid kättesaadavad kasutajatele ja seotud osapooltele.

CIA peab tagama, et kõik tingimused ja nõudmised, samas ka CSP PS seosed, ning kõik muu seotud informatsioon tehtaks loetavaks kõikidele kasutajatele, seotud osapooltele ja määratud gruppidele.

13.8 Seadme sertifikaadi kasutus

Sõidumeeriku sertifikaate võib kasutada ainult sõidumeeriku süsteemis.

13.9 Seadme sertifikaatide tühistamine

Sertifikaate ei saa tühistada.

14 MSCA, CIA, CPO, CP, CSP ja RA informatsiooni turvalisuse haldus

Iga osapoole PS kirjeldab informatsiooni turvalisuse haldamist seoses selle riikliku CA poliitikaga.

Iga osapool omab enda dokumenteeritud informatsiooni turvapoliitikat. Osapooled on sõlminud informatsiooni turbe lepingu, mis katab detailselt üleüldisi osapoolte turvalisuse haldamist.

Iga osapool peab omandama informatsiooni turvalisuse haldamise süsteemi, mis on vastavuses BS7799 [ISO 17799] nõuetega. Ametlik sertifikaat ei ole vajalik.

Iga osapool peab tagama, et neil on pidevalt olemas personal, kes:

- On koolitatud sõidumeeriku süsteemi nende osa jaoks.
- Täidavad rolli, mis on kirjeldatud sõidumeeriku süsteemis
- On kontrollitud politsei või muu vastava asutuse poolt.

Iga osapool peab tagama, et hoiavad oma toimikutest arhiivi ja nad omavad poliitikat, mis määrab ära nende toimikute arhiveerimise perioodi.

15 MSCA ja CIA lõpetamine

15.1 Lõpetamine - MSA vastutus

MSCA või CIA lõpetamisel arvestatakse olukorraga, kus kõik MSCA või CIA-ga seotud teenused on lõplikult peatatud. See ei kehti juhul, kui teenus on edasi antud ühelt asutuselt teisele või kui MSCA teenus on edasi antud vanalt liikmesriigi võtmepaarilt uuele liikmesriigi võtmepaarile või ERCA

võtmele. See viitab situatsioonile, kui liikmesriik taganeb sõidumeeriku süsteemi kasutamisest või kui terve sõidumeeriku süsteem lõpetatakse.

MSA peab tagama alljärgnevate kohustuste täitmise.

Enne kui MSCA/CIA lõpetab oma teenused, siis peavad vähemalt järgmised protseduurid olema lõpetatud:

a) Teavitama kõik kasutajaid ja osapooli, kellega MSCA/CIA-l on lepingud või muud moodi seotud;
b) Peab teavitama avalikust vähemalt 3 kuud ette;
c) MSCA/CIA peab lõpetama kõik õigused, mis on antud allettevõtjatele, et täita MSCA/CIA rolli sertifikaatide väljastamisel;
d) MSCA/CIA peab võtma kasutusele vajalikud meetmed, et jätkuvalt säilitada ja jagada juurde pääsu arhiivi toimikutele, andes need soovi korral üle MSA-le.

15.2 CSP või CPO vastutuse üleandmine

CSP või CPO vastutuse üleandmine toimub juhul kui MSA otsustab määrata uued CSP või CPO endise asemele.

MSA vastutab, et vastutuste ja varade üleandmine toimub korrapäraselt.

Eelmine CSP peab üleandma uuele CSP-le kõik juurvõtmed vastavalt MSA poolt otsustatule.

Eelmine CSP peab hävitama kõik koopiad MSCA võtmetest.

16 Audit

MSA vastutab, et CPO-s ja CSP-s toimuksid auditeerimised.

16.1 Üksuse vastavuse auditi sagedus

Selle riikliku poliitika all tegutsevad CPO ja CSP peavad auditeerima oma vastavust sellele poliitikale vähemalt kord aastas. Auditeerimise aruanded peavad olema inglise keeles.

16.2 Auditi poolt kaetud teemad

Audit peab katma CPO/CSP/RA kohustused, mis on määratud § 5.3 ERCA-CP [ERCA].

Audit peab katma CPO/CSP/RA vastavust selle riikliku CA poliitikaga.

Audit arvestab samuti SA tegevust.

Audit koostab auditi aruande, mis määrab parendavad tegevused koos rakendamise graafikuga, mis on vajalik selle poliitika nõudmiste täitmiseks.

16.3 Kes peaks tegema auditit

MSA võib konsulteerida välise sertifitseerimise või akrediteerimise asutusega, et saada CPO/CP/CSP/RA PS heakskiitu, et tõsta seotud osapoolte rakendamise usaldust. Vastasel korral teostab auditi MSA.

16.4 Tegevused puuduste leidmisel

Kui auditi käigus on leitud puudused, siis MSA peab võtma kasutusele meetmed vastavalt tõsidusele.

16.5 Tulemuste teavitamine

Auditi aruande osad, vastavalt turvatasemele, peab tegema avalikuks vastavalt soovile. Tegelikku auditi aruannet ei tehta avalikuks, välja arvatud erandkorras. Inglise keelsed auditi aruanded saadetakse ERCA-le.

17 Riikliku CA poliitika protseduuride muudatused

17.1 Asjad, mida võib muuta teavitamiseta

Ainukesed muudatused, mida võib selles poliitikas teha teavitamiseta on:

a) trükivigade parandamine;
b) muutused kontaktides.

17.2 Teavitamisega muudatused

17.2.1 Teade

Sertifikaadi poliitikas võib teha muudatusi **90** päeva ette teatades.

Muudatused, mis on selle poliitika eest vastutava asutuse (MSA) otsustusala, mis materiaalselt **ei mõjuta** suuremat osa selle poliitika kasutajaid ja osapooli, võib teha **30** päevase ette teatamisega.

17.2.2 Kommenteerimise aeg

Seotud kasutajad võivad esitada kommentaare asutusele poliitika kohta **15** päeva jooksul teavituse ilmumisest.

17.2.3 Keda peab informeerima

Poliitikas toimunud muudatustest peab teavitama:

- ERCA
- MSCA ja CIA kaasa arvatud SA
- Kõik teised MSAd

17.2.4 Lõpliku muudatuste teavitamise aeg

Kui esitatud muudatus on tehtud kommentaaride tulemusena, siis teavitatakse sellest ette vähemalt **30** päeva enne muutuse jõustumist.

17.3 Muutused, mis vajavd uut Riikliku CA poliitika kinnitamist

Kui poliitika muutus on määratud MSA poolt, mis omab materiaalset seost suure osa selle poliitika kasutajatega, siis MSA peab saatma kontrollitud Riikliku CA poliitika **ERCA-sse** uuesti kinnitamiseks.

18 Viited

[REG] Council Requlation 3821/85 as amended by Council Regulation (EC) No 2135/98 of 24th September 1998

[REG-A] Annex I(B) to Council Regulation 2135/98 *Requirements for construction, testing, installation and inspection*

[BPM] Digital Tachograph Card Issuing Best Practice Manual. Card Issuing Group, 16 November 2001. (under construction), owned by the Commission

[CC] Common Criteria. ISO/IEC 15408 (1999): "Information technology - Security techniques - Evaluation criteria for IT security (parts 1 to 3)".

[CEN] CEN Workshop Agreement 14167-2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)

[ETSI 102 042] ETSI TS 102 042. Policy requirements for certification authorities issuing public key certificates

[FIPS] FIPS PUB 140-2 (May 25, 2001): "Security Requirements for Cryptographic Modules". Information Technology Laboratory, National Institute of Standards and Technology (NIST)

[ISO 17799] BS ISO/IEC 17799: 2000. Information technology -- Code of practice for information security management.

[CSG] Common Security Guideline, Card Issuing Project. (under construction), owed by the Commission

[ERCA] Digital Tachograph System European Root Policy version 2.0

Special Publication I.04.131

Vastavustabel ERCA poliitikale

See vastavustabel on seotud ERCA Root Policy [ERCA] lõigu 5.3 nõudmiste ja Eesti riikliku CA poliitikaga.

ERCA CP	EST CP	Remarks
§5.3.1	§1.1	CSP Practice Statement (PS) will identify the actual entities involved. PS will be made available to the ERCA.
§5.3.2	§11.2.1, §11.2.3, §11.3	CSP Practice Statement (PS) will identify actual (certified) HSM device to be used. PS will be made available to the ERCA
§5.3.3	§11 §11.2.1	CSP Practice Statement (PS) will identify actual physical security control systems used. PS will be made available to the ERCA
§5.3.4	§11.2.2	
§5.3.5	§11.2.1	
§5.3.6	§11.4	
§5.3.7	§11.4	
§5.3.8	§11.4	
§5.3.9	§11.4	
§5.3.10	§11.4	
§5.3.11	§11.2.7	
§5.3.12	§12.1, §12.2, §10.1	CP Practice Statement (PS) will identify actual (certified) HSM device to be used. PS will be made available to the ERCA CSP Practice Statement (PS) will identify actual (certified) card to be used. PS will be made available to the ERCA
§5.3.13	§7.1, §11.2.1, §12.2	
§5.3.14	§11.2.3, §12.2.2, §12.2.3	

ERCA CP	EST CP	Remarks
§5.3.15	§11.2.4	
5.3.16	§12.2	
§5.3.17	§11.2.5, §12.2.5	
§5.3.18	§11.3	
§5.3.19		Not applicable
§5.3.20		Not applicable
§5.3.21	§11.3	
§5.3.22	§4.1.9,	Not applicable
§5.3.23	§7.1, §11.3	
§5.3.24	§11.3	. Certification of actual device used will be made available to the ERCA
§5.3.25	§ 4.1.9	Estonian NCA policy will not support VU-manufacturers
§5.3.26	§11.2.1	
§5.3.27	§11.2	
§5.3.28	§11.2.3	
§5.3.29	§13.1.1	
§5.3.30	§12.2 §13.1.1	
§5.3.31	§10.6 §13.9	
§5.3.32	§13.4	
§5.3.33, §5.3.34		Not applicable, as no undefined validity certificates (required for service to VU manufacturers) are handled under the EST NCA policy.
§5.3.35	§10.2, §10.9	
§5.3.36	§11.2.6	
§5.3.37	§11.2.6	

ERCA CP	EST CP	Remarks
§5.3.38	§14	
§5.3.39	§14	
§5.3.40	§14	
§5.3.41	§15	
§5.3.42	§17	
§5.3.43	§16.1	
§5.3.44	§16.1	
§5.3.45	§16, §16.5	
§5.3.46	§16,2, §16.4	