MAANTEEAMET

Eesti
MSA sertifitseerimispoliitika arukale sõidumeerikule

Versioon 1.0
02.02.2020

MSA sertifitseerimispoliitika on saanud ERCA heakskiidu 13.01.2020.

Sisukord

1. Sissejuhatus

Käesolev dokument on Eesti ***MSA sertifitseerimispoliitika*** arukale sõidumeerikule.

MSA sertifitseerimispoliitika on nõutud ERCA, Euroopa juursertifitseerimise asutuse väljastatud ***ERCA poliitika*** alusel.

Hetkel kehtiv ***ERCA poliitika*** on avaldatud https://dtc.jrc.ec.europa.eu/:

- Arukas sõidumeerik – Euroopa juursertifikaatide poliitika ning sümmeetriliste võtmete infrastruktuuri poliitika, versioon 1.0, juuni 2018 [*Smart Tachograph - European Root Certificate Policy and Symmetric Key Infrastructure Policy, Version 1.0, June 2018*]

Euroopa Parlamendi ja nõukogu määrusega (EL) nr 165/2014 on võetud kasutusele teise põlvkonna digitaalne sõidumeerik ehk arukas sõidumeerik. Komisjoni rakendusmääruse (EL) 2016/799 lisas 1C sätestatakse arukate sõidumeerikute ja nende komponentide konstruktsiooni, katsetamise, paigaldamise, kasutamise ja parandamise tehnilised nõuded.

1.1 Kehtivus

See ***MSA sertifitseerimispoliitika*** kehtib alates selle heakskiitmisest ERCA-s. Poliitika kehtib kuni teavitatakse vastupidisest.

MSA sertifitseerimispoliitika kehtivus lõppeb, kui MSA lõpetab tegevuse või kui MSA annab teada, et ***MSA sertifitseerimispoliitika*** enam ei kehti, nt selle pärast, et jõustunud on ***MSA sertifitseerimispoliitika*** uus versioon.

1.2 Terminoloogia

Dokumendis tuleb sõnu „nõutav“, „peab“ ja „tuleb“, „ei tohi“, „peaks“ „ei peaks“, „soovitatav“, „võib“ ja „valikuline“ tõlgendada nii, nagu on kirjeldatud standardis RFC 2119.

Siin poliitikas kasutame peamiselt sõnu „peab“ ja „tuleb“.

ERCA poliitikas tähistab lühend CP komponendi isikustajat [*Component Personaliser*]. See on sama, mis Eestis kaardi isikustaja, kuna see on ainus komponent, mille valmistamine kuulub Eestis MSA vastutusse.

Dokumendis kasutatav terminoloogia:

ERCA	Euroopa juursertifitseerimise asutus [*European Root Certification Authority*]	
MSA	Liikmesriigi asutus [*Member State Authority*]	
CIA	Kaarte väljastav asutus [*Card Issuing Authority*]	

CP	Kaardi isikustaja [*Card Personaliser*] (komponendi isikustaja [*Component Personaliser*])	Selles ***MSA sertifitseerimispoliitikas*** käsitletakse ainult kaardi isikustajat
MSCA	Liikmesriigi sertifitseerimisasutus [*Member State Certification Authority*]	
CPS	Sertifitseerimistavad [*Certification Practice Statement*]	Vt RFC 3647
ERCA poliitika	Euroopa juursertifikaatide poliitika ning sümmeetriliste võtmete infrastruktuuri poliitika	
Vastavustabel	*[Compliance table]*	Tabel, kus on toodud kõik siin poliitikas sätestatud nõuded ning kuidas organisatsioonid neid järgivad.
Ei kohaldu	[*Not applicable*]	
VU	Sõidukiseade [*Vehicle Unit*]	Sõidukis olev sõidumeerik, mis salvestab autojuhi tegevusi, nagu juhtimis- ja puhkeaeg
HSM	Riistvaraline turvamoodul [*Hardware Security Module*]	Turvaline arvuti krüpteerimisvõtmete salvestamiseks ja haldamiseks
PKI	Avaliku võtme infrastruktuur [*Public Key Infrastructure*]	Krüpteerimisvõtmete krüpteerimiseks, identifitseerimiseks ja allkirjastamiseks kasutamise meetod
Intsident	Käesolevas dokumendis on intsident sama, mis turvaintsident	Turvaintsident on hoiatus, et sõidumeeriku süsteem võib olla ohus või on oht juba realiseerunud

1.3 Erand

Eesti MSA-ga ei ole seotud ükski sõidumeerikuid või liikumisandureid tootev CP, mistõttu ei ole ***MSA sertifitseerimispoliitikasse*** vaja kaasata tootjat puudutavaid regulatsioone.

1.4 MSA sertifitseerimispoliitika eesmärk

MSA sertifitseerimispoliitika eesmärk on aruka sõidumeeriku turvanõuete, st sõidumeerikukaartide väljastamiseks ja valmistamiseks vajalike turvanõuete kehtestamine Eestis. Arukas sõidumeerik on raskeveokites autojuhi tegevuste nagu juhtimis- ja puhkeaja salvestamiseks kasutatav kontrollseade.

Arukas sõidumeerik sisaldab kaitset vajavaid isikuandmeid ja turvakomponente. Süsteem on nii üles ehitatud, et ühes liikmesriigis toimuv turvaintsident, näiteks teatud krüptograafiliste võtmete ohtu sattumine, võib põhjustada olulist kahju tervele Euroopa süsteemile. Seetõttu peab sõidumeeriku kaartide ja seadmete väljastamisel ja valmistamisel olema tagatud vajalik turvalisus.

1.5 MSA sertifitseerimispoliitikaga seotud organisatsioonid

MSA sertifitseerimispoliitika puudutab järgmisi organisatsioone ning kehtestab neile nõuded ja rollid:

Organisatsioon ja roll	Teavet andev peatükk	Nõudeid sisaldav peatükk
MSA	1, 2	3, 4, 14, 15
CIA	1, 2, 3	5, 13, 14
CP	1, 2, 3	6, 8, 9 10, 11, 12, 13, 14
MSCA	1, 2, 3	7, 8, 9 10, 11, 12, 13, 14

2. Organisatsioonid, rollid ja vastutus

MSA sertifitseerimispoliitikas on sätestatud järgmised aruka sõidumeerikuga seotud rollid:

ERCA, Euroopa juursertifitseerimise asutus

CIA, kaarte väljastav asutus

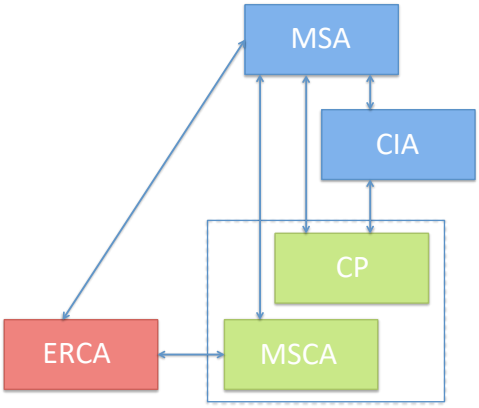
CP, kaardi isikustaja (komponendi isikustaja)

MSCA, liikmesriigi sertifitseerimisasutus

Määruses 2016/799 käsitletud võtmete haldamisega seoses on vastava määruse B osa 11. liite nõuetes CSM_53 kuni CSM_71 kirjeldatud kaht haldustasandit.

Euroopa tasandil vastutab Euroopa juursertifitseerimise asutus (ERCA) avalike ja privaatsete juurvõtmepaaride ning vastavate sertifikaatide ja sümmeetriliste peavõtmete loomise ja haldamise eest. ERCA väljastab liikmesriigi sertifitseerimisasutustele (MSCA-dele) sertifikaate ning jagab neile sümmeetrilisi peavõtmeid.

Liikmesriigi tasandil vastutavad MSCA-d aruka sõidumeeriku seadmete sertifikaatide väljastamise eest ning sümmeetriliste peavõtmete ning muude peavõtmetest tuletatud ja arukasse sõidumeerikusse paigaldatavate andmete jagamise eest. MSCA on ERCA-le alluv sertifitseerimisasutus. Rollide ülevaade:



2.1 Euroopa tasandi rollid ja vastutus

Euroopa Komisjoni kui ERCA eest vastutavat organit nimetatakse edaspidi *Euroopa asutuseks*.

Euroopa asutuse kontaktaadress on:

European Commission
DG MOVE - Directorate General for Mobility and Transport
Directorate C – Land
Unit C.1 – Road Transport
Rue J.-A. Demot, 24-28
B-1040 Bruxelles

Euroopa Komisjoni talitust, mille kohustus on ***ERCA poliitika*** rakendada ning liikmesriikidele võtmete sertifitseerimisteenust osutada, nimetatakse edaspidi ERCA-ks.

ERCA kontaktaadress on:

European Root Certification Authority
Head of the Cyber and Digital Citizens' Security Unit E3
Directorate E - Space, Security and Migration
DG JRC - Joint Research Centre (TP 361)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)

2.2 Eestis tegevuse eest vastutavad asutused

Eestis vastutab aruka sõidumeerikuga seonduva eest Maanteeamet ehk liikmesriigi asutus (**MSA**).

Maanteeamet
Teelise 4
10916, Tallinn

Eesti

https://www.mnt.ee/et

MSA on sisse seadnud järgmised kolm täidesaatvat organisatsiooni või rolli:

- **CIA**
- **CP**
- **MSCA**

CIA:
Vastutab sõidumeerikukaartide väljastamise eest; kaarte väljastav asutus (**CIA**).

Nimi ja aadress:

Maanteeamet
Teelise 4
10916 Tallinn
Eesti

https://www.mnt.ee/et

CP:
Vastutab sõidumeerikukaartide isikustamise ja jagamise eest; kaardi isikustaja (**CP**).

Nimi ja aadress:

CardPlus Group OY
Koskelontie 23 F
02920 Espoo
Soome

MSCA:
Vastutab sertifitseerimisteenuste, sealhulgas liikmesriikide juurvõtmete haldamise ning liikumisandurite andmete krüpteerimise eest; liikmesriigi sertifitseerimisasutus (**MSCA**).

Nimi ja aadress:

SK ID Solutions AS
Pärnu mnt 141
11314 Tallinn
Eesti

CP ja **MSCA** funktsioone ostetakse sisse asutuseväliselt töövõtjalt.

3. Liikmesriigi asutused, MSA

Iga liikmesriik loob liikmesriigi asutuse (MSA).

3.1 ERCA poliitika

MSA võib igal ajal esitada Euroopa asutusele ***ERCA poliitika*** muutmise ettepanekuid.

3.2 MSA sertifitseerimispoliitika

Iga liikmesriigi asutus kehtestab ***MSA sertifitseerimispoliitika*** ja dokumenteerib seda kooskõlas ***ERCA poliitika*** kõigi kohalduvate nõuetega.

3.3 ERCA heakskiidetav ingliskeelne MSA sertifitseerimispoliitika

3.3.1 *MSA sertifitseerimispoliitika heakskiitmine*

MSA peab tegema ***MSA sertifitseerimispoliitika*** ERCA-le kättesaadavaks.

ERCA peab kontrollima ***MSA sertifitseerimispoliitika*** vastavust käesolevas dokumendis sätestatud nõuetele. MSA peab vastama asjakohaselt kõikidele ERCA kommentaaridele. Kontrolli eesmärk on võrreldavate turvatasemete tagamine igas liikmesriigis.

ERCA peab viitamise eesmärgil arhiveerima ***MSA sertifitseerimispoliitika*** ning vastava kontrolliaruande.

3.3.2 *MSA sertifitseerimispoliitika sidusrühmadele*

Pärast ERCA heakskiitu peab MSA tegema oma ***MSA sertifitseerimispoliitika*** kättesaadavaks kõigile sidusrühmadele, sealhulgas oma riigi MSCA-le ja CP-le.

3.3.3 *ERCA sertifitseerimisteenused*

ERCA-l tuleb osutada võtmete sertifitseerimise teenust MSA-ga seotud MSCA-le ainult siis, kui ***MSA sertifitseerimispoliitika*** kontroll annab piisavalt alust hinnata, et ***ERCA poliitikaga*** kehtestatud nõudeid täidetakse.

ERCA võtmete sertifitseerimisteenuste jätkuv osutamine MSCA-le sõltub MSA auditiaruannete õigeaegsest esitamisest (vt ***ERCA poliitika*** punkti 8.1), mis näitab, et MSCA täidab jätkuvalt oma kohustusi vastavalt heakskiidetud ***MSA sertifitseerimispoliitikas*** sätestatule.

3.4 Poliitika muutmise kord (MSA)

3.4.1 *Vastutus muudatuste eest*

MSA vastutab poliitika ja selle muutmise eest.

ERCA poliitika muutmisel võib muuta ka ***MSA sertifitseerimispoliitikat.***

3.4.2 *Muutmist puudutav teave*

MSA sertifitseerimispoliitikat võib muuta ainult asjakohaste rollide ja organisatsioonidega, st CIA, CP ja MSCA-ga, kirjalikult konsulteerides, välja arvatud vähetähtsate redaktsiooniliste muudatuste puhul. Teatavaks tuleb teha ajavahemik, mille jooksul uus ***MSA sertifitseerimispoliitika*** kehtima hakkab.

3.4.3 *MSA sertifitseerimispoliitika edastamine ERCA-le heakskiitmiseks*

ERCA peab andma heakskiidu kõigile ***MSA sertifitseerimispoliitikas*** tehtavatele muudatustele. MSA saadab ERCA-le heakskiitmiseks iga uuendatud ***MSA sertifitseerimispoliitika***.

3.5 MSCA määramine

MSA peab määrama MSCA, mis rakendab ***MSA sertifitseerimispoliitikat*** ja osutab seejuures CP-le võtme sertifitseerimise ja jagamise teenuseid. MSCA peab tegutsema liikmesriigi nimel.

3.6 Sertifikaadi tühistamine

MSA-l on õigus taotleda ***MSA sertifitseerimispoliitika*** punktis 2.2 nimetatud ja MSCA-le väljastatud sertifikaatide tühistamist

3.7 Intsidentidega tegelemine

MSA peab teavitama ERCA-d igasugusest võtmete avalikukstulekuga seotud intsidendist.

MSA peab korraldama järeluurimise, tuvastama juurpõhjused ja võtma parandusmeetmeid.

MSA uurimiste tulemused tuleb teha teatavaks ERCA-le.

3.8 Kaebused

MSA tegeleb CP ja MSCA osutatavate teenustega seoses CIA-lt saadud kaebustega.

MSA tegeleb MSCA osutatavate teenustega seoses CP-lt saadud kaebustega.

MSA tegeleb ERCA osutatavate teenustega seoses CP-lt ja MSCA-lt saadud kaebustega.

4. Vastavusaudit ja heakskiit

4.1 Organisatsioonide ja rollide heakskiitmine

MSA võib anda heakskiidu CIA-le enne, kui sel lubatakse tegevust alustada.

MSA peab andma heakskiidu CP-le ja MSCA-le enne, kui neil lubatakse tegevust alustada.

MSA peab andma heakskiidu MSCA CPS-le enne, kui MSCA-l lubatakse tegevust alustada.

MSA peab andma heakskiidu CP CPS-le enne, kui CP-l lubatakse tegevust alustada.

4.1.1 *Tegevuse heakskiitmine (MSCA, CP ja CIA)*

Enne kui MSCA, CP ja CIA alustavad tegevust, peab MSA korraldama tegevuse alustamisele eelneva hindamise, et tõendada, kas organisatsioon suudab tegutseda kooskõlas ***MSA sertifitseerimispoliitika*** nõuetega ning MSCA puhul ka CPS-ga. Vastavusaudit on kohustuslik.

4.1.2 *MSCA ja CP CPS-i heakskiitmine*

MSA peab tagama, et MSCA ning CP CPS-id vastavad ***MSA sertifitseerimispoliitikale***.

4.2 Vastavusauditi ulatus ja sagedus

MSA võib teha CIA-le täieliku ja ametliku vastavusauditi.

MSA peab tegema MSCA-le ja CP-le täieliku ja ametliku vastavusauditi.

Vastavusaudit peab tuvastama, kas ***MSA sertifitseerimispoliitikas*** ning MSCA puhul CPS-is kirjeldatud organisatsiooni ja rolli puudutavad nõuded on täidetud.

MSA peab tegema esimese vastavusauditi 12 kuu jooksul MSCA, CP ja CIA tegevuse alustamisest.

Kui vastavusauditiga puudusi ei tuvastata, tuleb järgmine vastavusaudit korraldada 24 kuu jooksul.

Kui vastavusauditiga tuvastatakse puudus, tuleb 12 kuu jooksul teha järelaudit, et kontrollida, kas puudused on kõrvaldatud.

4.3 Hindaja (audiitori) identiteet/kvalifikatsioon

Vastavusauditi teeb sõltumatu audiitor.

MSA peab määrama ja heaks kiitma vastavusauditit korraldava isiku.

MSA peab registreerima auditeid korraldavate isikute nimed.

Audiitorid peavad vastama järgmistele nõuetele:

- eetiline käitumine: usaldusväärsus, samaväärne kohtlemine, konfidentsiaalsus suhtluses auditeeritava organisatsiooniga ning selle teabe ja andmete käsitlemisel;
- õiglane ja erapooletu esitlus: auditi tulemused, järeldused ja aruanded on õiged ning kirjeldavad täpselt auditi ajal tehtud toiminguid;
- professionaalsus: audiitor on asjatundlik ja professionaalselt väga pädev ning kasutab tõhusalt enda kogemusi, mis on saadud põhjaliku praktika käigus infotehnoloogia, PKI (avaliku võtme infrastruktuuri) ning seotud tehniliste normide ja standardite valdkonnas.

Audiitoril peavad olema põhjalikud teadmised ning soovitavalt akrediteering järgmistes valdkondades:

- infosüsteemi turvaauditi korraldamine;
- andmekaitse regulatsioonid (privaatsus);
- PKI ja krüptograafilised tehnoloogiad;
- PKI tarkavara toimimine;
- asjakohased Euroopa Komisjoni poliitikad ja määrused.

4.3.1 *Hindaja ning hinnatava isiku vaheline suhe*

Audiitor peab olema auditeeritavast organisatsioonist sõltumatu ega tohi olla sellega seotud.

4.4 Vastavusauditiga kaetud valdkonnad

Vastavusauditiga kontrollitakse vastavust ***MSA sertifitseerimispoliitikale.*** Auditeerida tuleb MSCA CPS-i ning organisatsiooni dokumenteeritud seotud protseduure ja tehnikaid.

Vastavusaudit peab hõlmama MSCA CPS-is ning muudes MSCA ja CP dokumentides kirjeldatud tehniliste, menetluslike ja personali tavade rakendamist, millele on viidatud vastavustabelis.

Mõned valdkonnad, millele vastavusauditites keskendutakse:

- identimine ja autentimine;
- tööfunktsioonid/teenused;
- füüsilised, menetluslikud ja personali turvakontrollid;
- tehnilised turvakontrollid.

Vastavusauditiga tuleb hinnata süsteemi logisid / auditi logisid, et teha kindlaks, kas auditeeritava organisatsiooni süsteemides on turvanõrkusi.

Kindlaks tehtud (võimalikke) nõrkusi peavad maandama hinnatav roll ja organisatsioon.

Vastavusauditit, sealhulgas hinnangut ning võimalikke nõrkusi, tuleb kajastada ja dokumenteerida auditiaruandes.

4.5 Puuduse tõttu rakendatavad meetmed

Kui audiitor avastab puudusi, peab auditeeritud organisatsioon ja roll (MSCA, CP ja CIA) viivitamatult võtma parandusmeetmeid.

Parandusmeetmetest tuleb teavitada audiitorit, kes meetmed heaks kiidab.

Pärast parandusmeetmete võtmist tuleb 12 kuu jooksul korraldada järelaudit.

4.6 Tulemustest teavitamine

Audiitor teavitab auditeeritud organisatsiooni (MSCA, CP ja CIA) ning MSA-d kõikidest vastavusauditi tulemustest.

4.6.1 *ERCA-le esitatav auditiaruanne*

MSA peab saatma ERCA-le auditi tulemuste kohta auditiaruande. Aruandes peab olema välja toodud vähemalt avastatud kõrvalekallete hulk ning iga kõrvalekalde olemus.

ERCA peab avaldama auditiaruande kättesaamiskuupäeva oma veebilehel. MSA peab esitama ERCA-le taotluse alusel vastavusauditi kõik tulemused.

5. Sõidumeerikukaartide väljastamine (CIA)

Siin peatükis on sätestatud CIA-le kehtivad nõuded.

5.1 Vastavustabel

CIA-l peab olema vastavustabel, kus kirjeldatakse, kuidas CIA ***MSA sertifitseerimispoliitikas*** sätestatud nõudeid järgib, viitega juhtdokumentidele.

5.2 MSA-le esitatavad kaebused

CIA kaebused CP ja MSCA osutatud teenuste kohta esitatakse menetlemiseks MSA-le.

5.3 CIA vastavuse auditeerimine

CIA-d võib auditeerida (vt 4. peatükk).

CIA peab andma oma valdused, personali, süsteemi ja dokumentatsiooni jms vastavusauditi käsutusse.

Kui audiitor avastab puudusi, peab CIA viivitamatult võtma parandusmeetmeid.

Parandusmeetmetest tuleb teavitada audiitorit, kes need heaks kiidab.

5.4 Sõidumeeriku kaartide väljastamine

CIA peab tagama, et juhikaardi kasutajate isikud tuvastatakse sõidumeerikukaardi taotlemisel.

CIA tuvastab kõigi teiste sõidumeerikukaartide vastutava osapoole (omaniku). Seda tuleb CIA-l teha taotlusprotsessi ajal.

CIA peab tagama, et kaardi sertifikaadi/sertifikaatide kehtivuskuupäev on sama, mis sõidumeerikukaardi kehtivuse alguskuupäevaga vastavalt elementaarfaili identifikaatorite kodeeringule.

CIA peab kontrollima, et enne sõidumeerikukaardi uuesti väljastamist on sõidumeerikukaardi eest vastutav osapool registreerinud, et kaart on varastatud või kadunud.

CIA peab tagama, et uuesti väljastatud sõidumeerikukaarti ei anta üle enne, kui olemasolev sõidumeerikukaart on antud CIA-le või registreeritud varastatuks või kadunuks.

5.5 Teave sõidumeerikukaardi taotlejale

CIA peab teavitama taotlejat aruka sõidumeeriku kaartide omamise ja kasutamise eeskirjadest.

5.6 Sõidumeerikukaartide käsitlemine

CIA peab sõidumeerikukaarte turvaliselt käsitlema ja säilitama.

CIA-l peab olema riketega kaartide käsitlemise kord.

5.7 Sõidumeerikukaartide kasutuskõlbmatuks muutmine

CP muudab sõidumeerikukaardid kasutuskõlbmatuks turvalisel viisil elektrooniliselt või füüsiliselt. CP hävitab kaardi nii, et sertifikaatide või võtmete ohtu sattumine oleks kindlalt välistatud (näiteks kiibi pooleks lõikamisega).

5.8 Teabevahetus CP-ga

CIA peab veenduma, et CP on saanud kätte sõidumeerikukaartide taotlused ning väljastama kättesaadud sõidumeerikukaartide kohta kviitungi.

Kui CIA avastab, et mõni sõidumeerikukaart on CP ja CIA vahelise transpordi käigus kaduma läinud, peab CIA teavitama CP-d kaardi kadumisest kui intsidendist. CP saadab uue sõidumeerikukaardi.

5.9 Teabevahetus teiste osapooltega

CIA peab tegema sõidumeerikukaarte puudutava teabe kättesaadavaks asjakohastele osapooltele nagu:

- kontrolliasutused (Eestis ja teistes liikmesriikides);
- MSA;
- Euroopa Liidu Komisjonile (ERCA).

CIA peab tegema vajaliku sõidumeerikuid puudutava teabe kättesaadavaks teistele riikidele (TACHOnet jms).

CIA peab tagama teistele osapooltele antavate sõidumeerikukaartide teabe tervikluse ja konfidentsiaalsuse.

CIA peab edastama neile saadetud (leitud, ära võetud) juhikaardid kaardi väljastanud CIA-le.

5.10 Logimine, andmete säilitamine ja arhiveerimine

CIA peab säilitama sõidumeerikukaartide kohta kõik vajalikud andmed ja vähemalt

- sõidumeerikukaardi numbri, seose vastutava isikuga ning staatuse

CIA peab arhiveerima sõidumeerikukaarte puudutava teabe määramatuks ajaks.

CIA peab tagama arhiveeritud teabe kättesaadavuse, tervikluse ja konfidentsiaalsuse.

CIA peab tegema teabe MSA-le vastava taotluse alusel kättesaadavaks.

5.11 Üldised turvanõuded

CIA-l peavad olema vajalikud kirjalikud dokumendid ja praktikad, et tagada tööde vastavus ***MSA sertifitseerimispoliitikale***.

CIA-l peavad olema määratletud rollid ja vastutus. Kogu personalil peab olema asjakohane pädevus ja väljaõpe. Ühelgi isikul ei või olla rohkem kui üks turvakriitiline roll, et ei tekiks huvide konflikti.

Kriitilisi süsteeme ja andmeid tuleb kaitsta volituseta juurdepääsu eest juurdepääsukontrolli süsteemidega ning ligipääsu täpse tuvastamisega (isikutasandil).

Süsteemile juurdepääsu ja kriitiliste süsteemide kasutamist tuleb kontrollida asjakohase teabe kogumise ja analüüsimisega. Nimetatud teavet tuleb kaitsta moonutamise eest. Nimetatud teave tuleb esitada taotluse alusel MSA-le.

6. Kaardi isikustaja (CP)

6.1 Vastavustabel

CP-l peab olema vastavustabel, kus kirjeldatakse, kuidas CP ***MSA sertifitseerimispoliitikas*** sätestatud nõudeid järgib, viitega juhtdokumentidele.

6.2 Vastutus

Komponendi isikustajad vastutavad selle eest, et seadmetel on asjakohased võtmed ja sertifikaadid.

- Juhi- ja töökojakaartide CP:
  - tagab kahe kaardivõtmepaari loomise vastastikuseks autentimiseks ja allkirjastamiseks;
  - teeb MSCA_Card’iga sertifikaadi rakendamise toimingu;
  - teeb KM-WC ja KDSRC rakendamise (ainult töökojakaartidele);
  - tagab kaardis võtmete ja sertifikaatide olemasolu, et neid saaks kasutada vastastikuseks autentimiseks ja allkirjastamiseks, MoS-VU ühendamiseks, DSRC-andmeside dekrüpteerimiseks ning andmete autentsuse kinnitamiseks (ainult töökojakaartidele).

- Ettevõtte- ja kontrollikaartide CP:
  - tagab kaardi võtmepaari loomise vastastikuseks autentimiseks;
  - teeb MSCA_Card’iga sertifikaadi rakendamise toimingu;
  - teeb KDSRC rakendamise (ainult kontrollikaartidele);
  - tagab kaardis võtmete ja sertifikaatide olemasolu, et neid saaks kasutada vastastikuseks autentimiseks, DSRC-andmeside dekrüpteerimiseks ning andmete autentsuse kinnitamiseks (ainult kontrollikaartidele).

6.3 CP sertifitseerimistava

CP peab ***MSA sertifitseerimispoliitika*** rakendamist dokumenteerima CPS-s (sertifitseerimistavades). CP peab tegema CPS-i MSA-le kättesaadavaks.

Vastava taotluse esitamisel peab CP tegema enda CPS-i kättesaadavaks ka ERCA-le.

6.4 MSA-le esitatavad kaebused

CP kaebused MSCA osutatud teenuste kohta esitatakse menetlemiseks MSA-le.

6.5 CP vastavuse auditeerimine

CP-d tuleb auditeerida (vt 4. peatükk).

CP peab andma oma valdused, personali, süsteemi ja dokumentatsiooni jms vastavusauditi käsutusse.

Kui audiitor avastab puudusi, peab auditeeritud organisatsioon viivitamatult võtma parandusmeetmeid.

Parandusmeetmetest tuleb teavitada audiitorit, kes need heaks kiidab.

6.6 Äriteabe konfidentsiaalsus

CP peab käsitlema konfidentsiaalsete andmetena vähemalt järgmisi andmeid:

- privaatvõtmeid;
- sümmeetrilisi peavõtmeid.

Konfidentsiaalset teavet ei tohi avalikustada, välja arvatud siis, kui selleks on õiguslik kohustus.

6.7 Kaardi kaotus

Kui CP avastab sõidumeerikukaardi kadumise enne kaardi saatmist Eestisse, tuleb kaardi kadumisest teavitada CIA-d ja MSCA-d ning CP saadab uue kaardi.

6.8 Sõidumeerikukaartide kasutuskõlbmatuks muutmine

CP muudab sõidumeerikukaardid kasutuskõlbmatuks turvalisel viisil elektrooniliselt või füüsiliselt. CP hävitab kaardi selliselt, et sertifikaatide või võtmete ohtu sattumine oleks kindlalt välistatud (näiteks kiibi pooleks lõikamisega).

7. Liikmesriigi sertifitseerimisasutus, MSCA

MSCA peab tegutsema kooskõlas ERCA CP, ***MSA sertifitseerimispoliitika*** ning enda CPS-ga.

7.1 Vastavustabel

MSCA-l peab olema vastavustabel, kus kirjeldatakse, kuidas MSCA järgib ***MSA sertifitseerimispoliitikas*** sätestatud nõudeid, viitega juhtdokumentidele.

Vastavustabeli peab koostama lisaks CPS-le.

7.2 MSCA sertifitseerimistavad

CP peab ***MSA sertifitseerimispoliitika*** rakendamist dokumenteerima CPS-s (sertifitseerimistavades). CP peab tegema CPS-i MSA-le kättesaadavaks.

MSCA peab CPS-i tegema kättesaadavaks oma klientidele, st CP-le, vastavalt vajadusele.

Taotluse alusel peab MSCA tegema enda CPS-i kättesaadavaks ka ERCA-le.

7.3 Tegevustoimikud

MSCA peab pidama enda tegevuse kohta nõuetekohast toimikut, et tõendada ***MSA sertifitseerimispoliitika*** ja CPS-i järgimist.

Taotluse alusel peab MSCA tegema toimikud kättesaadavaks MSA-le ja/või ERCA-le.

7.4 MSCA vastavuse auditeerimine

MSCA-d tuleb auditeerida (vt 4. peatükk).

MSCA peab andma oma valdused, personali, süsteemi ja dokumentatsiooni jms vastavusauditi käsutusse.

Kui audiitor avastab puudusi, peab auditeeritud organisatsioon viivitamatult võtma parandusmeetmeid.

Parandusmeetmetest tuleb teavitada audiitorit, kes need heaks kiidab.

7.5 Avaldamise ja säilitamise kohustused

7.5.1 *Sertifikaatide hoidlad*

MSCA peab vastutama kõigi seadmete sertifikaatide (kaardi sertifikaatide) hoidlas säilitamise eest.

Hoidla ei tohi olla avalik.

7.5.2 *Sertifikaatide staatus*

MSCA peab vastava taotluse saamisel tegema sertifikaate puudutava teabe kättesaadavaks asjakohastele osapooltele nagu:

- kontrollasutustele (Eestis ja teistes liikmesriikides);

- MSA-le;
- Euroopa Liidu Komisjonile (ERCA).

7.6 Äriteabe konfidentsiaalsus

MSCA peab käsitlema konfidentsiaalse teabena vähemalt järgmisi andmeid:

- privaatvõtmeid;
- sümmeetrilisi peavõtmeid;
- auditi logisid / süsteemi logifaile; st kõik MSCA tarkvaras toimunud olulised turvasündmused tuleb varustada automaatselt ajatempliga ning salvestada süsteemi logifailides;
- PKI haldamist puudutavat üksikasjalikku dokumentatsiooni.

Konfidentsiaalset teavet ei tohi avalikustada, välja arvatud siis, kui selleks on õiguslik kohustus.

7.7 Sertifikaatide ja võtmete tühistamine

MSCA-l on õigus taotleda endale väljastatud sertifikaatide tühistamist.

7.8 Üldised turvanõuded

MSCA privaatvõtmeid ei tohi eksportida ega säilitada üheski muus süsteemis peale MSCA süsteemide.

MSCA peab asjakohaselt turvatud vahenditega edastama sümmeetrilised peavõtmed, nendest saadud võtmed või peavõtmetega krüpteeritud andmed CP-le üksnes rakendusmääruse (EL) 2016/799 IC lisa 11. liites sätestatud võtmete ja andmete edastamise eesmärgi täitmiseks.

Seadmevõtmed tuleb luua, edastada ja sisestada seadmesse selliselt, et säiliks võtmete konfidentsiaalsus ja terviklus. Sellel eesmärgil on nõutud, et:

- kogu varustuse kasutusea jooksul järgitakse varustuse ühiste turvalisuse sertifitseerimise kriteeriumide alusel sätestatud ettekirjutusi;
- kui seadme privaatvõtme loomine ei toimu seadmesiseselt, siis luuakse privaatvõti sellise HSM-i sees, mis vastab ERCA poliitika punktis 6.2 toodud nõuetele;
- kui seadme sümmeetrilise võtme loomine ei toimu seadmesiseselt, siis luuakse sümmeetriline võti sellise HSM-i sees, mis vastab ERCA poliitika punktis 6.2 toodud nõuetele;
- privaatvõtmed ja sümmeetrilised võtmed sisestatakse seadmesse füüsiliselt turvalises keskkonnas;
- kui seade suudab luua privaatvõtmeid ja sümmeetrilisi võtmeid, siis kaitseb võtmete loomist seadme turvasertifikaat, mis tagab, et kasutatakse avalikke ning asjakohaseid krüptograafilisi võtme genereerimise algoritme.

7.9 Sertifikaatide kasutus

MSCA_Card sertifikaate tuleb kasutada MSCA_Card väljastatud kaardisertifikaatide kinnitamiseks.

Card_MA sertifikaate tuleb kasutada vastastikuseks autentimiseks ning kaardi ja VU seansivõtme ühildamiseks.

Card_Sign sertifikaate tuleb kasutada kaardist allalaetud andmete autentsuse ja tervikluse kontrollimiseks. Card_Sign privaatvõtit võib kasutada ainult kaardist allalaetud andmete allkirjastamiseks.

KM-WC tuleb anda CP-le töökojakaartidesse paigaldamiseks.

(KDSRC-d kasutab MSCA VU võtmete tuletamiseks DSRC turvalisuse tagamisel.)

KDSRC-d tuleb kasutada kontrolli- ja töökojakaartides, et tuletada VU DSRC-võtmeid, mis on vajalikud VU DSRC-i autentsuse ja tervikluse dešifreerimiseks ja kontrollimiseks.

8. Identimine ja autentimine (ERCA poliitika 3. peatükk)

MSCA peab järgima ***ERCA poliitika*** 3. peatükis sätestatud nõudeid.

8.1 Organisatsiooni identiteedi autentimine

MSCA peab oma CPS-is sätestama organisatsiooni identiteedi autentimise korra.

8.2 Üksikisiku identiteedi autentimine

MSCA peab oma CPS-is sätestama üksikisiku identiteedi autentimise korra.

9. Sertifitseerimist ja võtmeid puudutavad nõuded (ERCA poliitika 4. peatükk)

CP ja MSCA peavad järgima ***ERCA poliitika*** 4. peatükis sätestatud nõudeid.

10. Seade, haldus ja tegevuskontroll (ERCA poliitika 5. peatükk)

CP ja MSCA peavad järgima ***ERCA poliitika*** 5. peatükis sätestatud nõudeid.

10.1 CP ja MSCA

10.1.1 *Riskijuhtimine*

CP-l ja MSCA-l peab olema kirjalik riskijuhtimise kord. Riskianalüüsi tuleb teha ja uuendada vähemalt iga 12 kuu järel või enne oluliste muudatuste tegemist.

10.1.2 *Muutmiskord*

CP-l ja MSCA-l peab olema kirjalik muudatuste tegemise kord. Muudatuste tegemise kord peab hõlmama teabevahetust MSA-ga.

10.1.3 *Andmete säilitamine*

MSCA peab säilitama isikustamisandmeid nii kaua, kuni neid isikustamiseks vaja läheb ning kuni vajalikud andmed on edastatud CP-le.

MSCA peab kustutama sertifitseerimistaotluse, kui isikustamisprotsess on lõppenud ning CP on saanud kätte vajalikud andmed.

ERCA, MSCA ja CP esindajate andmed on ainsad MSCA süsteemis töödeldavad või säilitatavad isikuandmed.

Andmeid käsitletakse vastavalt isikuandmete kaitse üldmäärusele (EL) 2016/679.

10.1.4 *Arhiveerimine*

MSCA ja CP peavad tegema kindlaks, milliseid andmeid ja kui kauaks arhiveerida. MSCA ja CP peavad andma asjakohase taotluse alusel arhiveeritud andmed MSA-le.

11. Tehniline turvakontroll (ERCA poliitika 6. peatükk)

CP ja MSCA peavad järgima ERCA poliitika 6. peatükis sätestatud nõudeid.

12. Sertifikaatide, CRL-i ja OCSP profiilid (ERCA poliitika 7. peatükk)

CP ja MSCA peavad järgima ERCA poliitika 7. peatükis sätestatud nõudeid.

13. Talitluspidevuse kavandamine ja intsidentidega tegelemine (CP ja MSCA)

13.1 Talitluspidevuse kava

MSCA-l ja CP-l peab intsidentide ja õnnetuste mõju vältimiseks ja vähendamiseks olema põhjalikult dokumenteeritud talitluspidevuse kava. Kava peab käsitlema:

- võtmete ohtu sattumist;
- andmekadu (vargus, tulekahju, riist- või tarkvaravead, jms);
- muid liike süsteemivigu.

13.2 Võtmete ohtu sattumine

CP ja MSCA peavad konkreetselt kirjeldama, milliseid meetmeid tuleb rakendada, kui MSCA privaatvõti või liikumisanduri võti ohtu satub või arvatakse olevat ohtu sattunud.

Sellistel juhtudel peavad CP ja MSCA viivitamatult teavitama MSA-d ja ERCA-d.

Kui kaardi võtmed satuvad ohtu ning see avastatakse enne kaardi kasutajale saatmist, ei tohi kaarti kasutajale saata.

13.2.1 *Erinõuded võtmete ohtu sattumise korral*

Privaatvõtme ohtu sattumine on turvaintsident, mida tuleb menetleda.

Kui MSCA privaatvõti ohtu satub või arvatakse olevat ohtu sattunud, teavitab MSCA intsidendist ERCA-d ning MSA-d ilma põhjendamatu viivituseta ning vähemalt **8 tunni** jooksul intsidendi avastamisest.

Intsidendi aruandes (teavituses) peab MSCA tooma välja ohu tekkimise asjaolud.

MSCA intsidendi uurimise tulemustest tuleb teavitada MSA-d ja ERCA-d.

13.3 Intsidentidega tegelemine

13.3.1 *Intsidentidega tegelemine*

Kõik tuvastatud intsidendid (turvaintsidendid) tuleb:

- salvestada
- teatavaks teha
- klassifitseerida
- neid tuleb uurida ja analüüsida
- neist tuleb raporteerida
- nende suhtes tuleb võtta parandus- ja ennetusmeetmeid.

CIA-l võib olla intsidentide (turvaintsidentide) käsitlemise protsess, kus on kirjeldatud kõike alates intsidentide raporteerimisest kuni teabe salvestamiseni ja parandus- ning vastumeetmeteni.

CP ja MSCA peavad kasutama kirjalikke intsidentide aruandeid.

CP-l ja MSCA-l peab olema kirjalik turvaintsidentide käsitlemise kord.

CP-l ja MSCA-l peab olema toimik (nimekiri) kõikidest turvaintsidentidest (intsidendi aruanded).

Intsidentidega tegelemine
MSCA ja CP peavad eraldama ressursse ja määrama vastutaja iga intsidendi uurimiseks ja analüüsiks ning seejärel esitlema tuvastatud juurpõhjuseid ning rakendama **parandus**meetmeid.

Intsidentide ennetamine

MSA, MSCA ja CP peavad koguma intsidentide kohta statistikat ning korraldama igal aastal dokumenteeritud juhtkonnakoosoleku, kus statistikat analüüsitakse. Koosoleku tulemusena koostatakse nimekiri meetmetest, mida rakendada tulevaste intsidentide **ennetamiseks**.

14. Organisatsioonide ja rollide lõpetamine

14.1 MSA

MSA peab tagama, et igal ajal töötab vähemalt üks MSCA (vt ***ERCA poliitika*** 5.8).

Kui CIA, CP või MSCA lõpetatakse, vastutab MSA asjakohaste osapoolte ning ERCA teavitamise eest.

MSA vastutab selle eest, et CIA, CP ja MSCA esitavad asjakohased arukat sõidumeerikut puudutavad andmed ja teabe arhiveerimiseks või muudavad andmed ja teabe kasutuskõlbmatuks. MSA vastutab arhiveerimise ja kasutuskõlbmatuks muutmise otsuse eest.

MSA vastutab otsuse eest esitada mis tahes kehtiva MSCA sertifikaadi tühistamise taotlus või kõigi MSCA sertifikaatide aeguda laskmise eest (vt ***ERCA poliitika*** 4.1.1.12).

MSA vastutab selle eest, et kõik privaatsed MS juurvõtmed muudetakse kasutuskõlbmatuks ning MS avalikud juurvõtmed arhiveeritakse.

14.2 CIA

CIA-l tuleb teha MSA ja teiste osapooltega koostööd, et lõpetamine oleks korrektne ja tõhus.

14.3 MSCA ja CP

MSCA-l ja CP-l tuleb teha MSA ja teiste osapooltega koostööd, et lõpetamine oleks korrektne ja tõhus.

MSCA ja CP peavad järgima MSA lõpetamisele kehtestatud nõudeid ja otsust selle kohta, millised andmed ja teave edastada MSA-le või muudetakse kasutuskõlbmatuks.

MSCA peab turvalisel viisil hävitama kõigi tema valduses olevate sümmeetriliste peavõtmete koopiad (vt ***ERCA poliitika*** 4.2.12).

15. Muudatuste ajalugu

Kuupäev	Versioon	Kommentaar	Isik
09.01.2019	0.1	MSA esitas versiooni ülevaatamiseks	Tiit Poll
17.01.2019	0.1	MSCA poolt üle vaadatud	Kai Tooming
17.01.2019	0.2	MSA esitas versiooni teistkordseks ülevaatamiseks	Tiit Poll
18.01.2019	0.2	MSCA poolt üle vaadatud	Kai Tooming
29.01.2019	0.2	Lõplik versioon esitatud ERCA-le	Tiit Poll
01.03.2019	0.2	ERCA heakskiit saadud	Michel Chiaramello
10.12.2019	0.3	MSA poolt uuendatud CP ja MSCA kontaktid	Tiit Poll
11.12.2019	1.0	Lõplik versioon esitatud ERCA-le	Tiit Poll
13.01.2020	1.0	ERCA heakskiit saadud	Michel Chiaramello