AS Sertifitseerimiskeskus – Eesti Vabariigi Mobiil-ID sertifitseerimispoliitika

Tõlge AS Sertifitseerimiskeskuse originaaldokumendile "AS Sertifitseerimiskeskus – Certificate Policy for Mobile-ID of the Republic of Estonia"

Versioon 5.0

OID: 1.3.6.1.4.1.10015.1.3

Kehtiv alates 01.11.2016

Versioonide ajalugu		
Kuupäev	**Versioon**	**Muudatused**
01.11.2016	5.0	Sertifitseerimispoliitika on ümber kujundatud vastavalt standardile IETF RFC 3647 [3] ja määrusele eIDAS [9].
27.06.2016	4.0	Täiendatud punkt 1.4 Sertifitseerimispoliitika identifitseerimine. Täiendatud punkt 1.5.2.1 klienditeeninduspunktid. Täiendatud punkt 1.5.3 PPA. Täiendatud punkt 1.5.4.1 klient. Täiendatud punkt 2.1.1 SK kohustused. Täiendatud punkt 2.1.2 PPA kohustused. Täiendatud punkt 2.1.3 MO kohustused. Täiendatud punkt 2.1.4.1 MO klienditeeninduspunkti kohustused. Täiendatud punkt 2.1.5 klientide kohustused. Täiendatud punkt 4.1 Sertifikaaditaotluse esitamine. Täiendatud punkt 4.2 Sertifikaaditaotluse menetlemine. Täiendatud punkt 4.2.1 Otsuse tegemine. Täiendatud punkt 4.2.2 Sertifikaadi väljastamine. Täiendatud punkt 4.6.1 Sertifikaadi kehtetuks tunnistamise volitused. Täiendatud punkt 4.6.2 Sertifikaadi kehtetuks tunnistamise taotluse esitamine.
01.01.2016	3.0	Täiendatud punkt 1.2 Terminoloogia. Muudetud punkt 1.5 Organisatsioon ja kasutusvaldkond. Muudetud punkt 1.6 PPA kontaktandmed. Muudatused punktis 2.1 Kohustused. Täiendatud punkt 2.4.4 Kataloogiteenus. Muudetud punkt 3.1 Kliendi identifitseerimine. Muudetud punkt 3.3 Eraldusnimi. Muudetud punkt 4.1 Sertifikaaditaotluse esitamine. Muudatused punktis 4.2.4 Sertifikaadi uuendamine. Täiendatud punkt 4.4 Sertifikaatide kehtivuse peatamine. Muudetud punkt 4.5 Sertifikaadi kehtivuse peatatuse lõpetamine. Muudetud punkt 4.6 Sertifikaadi kehtetuks tunnistamine. Uuendatud punkt 9 Viidatud ja seonduvad dokumendid.
01.01.2015	2.0	Muudatused, mille eesmärk on viia käesolev sertifitseerimispoliitika kooskõlla isikut tõendavate dokumentide seadusega (RT I, 29.10.2014, 6) ja millega muudetakse Mobiil-ID väljastamise tingimusi.
01.02.2011	1.1	Lõppversioon.
11.01.2011	0.1	Esialgne projekt.

1. Sissejuhatus

1.1. Ülevaade

Käesolev dokument, edaspidi „AS Sertifitseerimiskeskus – Eesti Vabariigi Mobiil-ID sertifitseerimispoliitika“ (edaspidi CP), määrab kindlaks menetlus- ja tegevusnõuded, mida Sertifitseerimiskeskus (edaspidi SK) järgib ja mille järgimist ta nõuab üksustelt Eesti Vabariigis väljastatud Mobiil-ID vormis digitaalse isikutunnistuse sertifikaatide (edaspidi Mobiil-ID) väljastamisel ja haldamisel. Mobiil-ID väljastatakse füüsilisele isikule isikut tõendavate dokumentide seaduses nimetatud konkreetseks ajavahemikuks [10] ja see on seotud mobiiltelefoninumbriga. Mobiil-ID sisaldab seotud kvalifitseeritud elektroonilise allkirja andmise vahendit (SIM-kaarti) ja kaht sertifikaadipaari. Sertifikaadid võimaldavad elektroonilist allkirjastamist ja identifitseerimist füüsilistel isikutel. Sertifikaadid on alati paarides: iga Mobiil-ID sisaldab kaht sertifikaadipaari, mis koosnevad autentimissertifikaadist ja kvalifitseeritud elektroonilise allkirja sertifikaadist ning nende vastavatest isiklikest võtmetest. Iga isiklikku võtit kaitsevad aktiveerimisandmed (PIN-kood) ja igal Mobiil-ID-l on üks lukust avamise (PUK-kood). Ühel isikul saab korraga olla ainult üks kehtiv Mobiil-ID.

Mobiil-ID sertifikaatide väljastamine ja haldamine põhineb määrusel (EL) nr 910/2014 [9], millega kehtestatakse õiguslik raamistik elektroonilistele allkirjadele.

Käesolev dokument kirjeldab ainult poliitika piiranguid EL-i kvalifitseeritud sertifikaatidele, mis on väljastatud füüsilistele isikutele, kui isiklik võti ja
seonduv sertifikaat asuvad QSCD-l (QCP-n-qscd) (standardist ETSI EN 319 411-2 [5]), ja normitud sertifitseerimispoliitikale, mis nõuab turvalist
krüptograafilist seadet (NCP+) standardist ETSI EN 319 411-1 [4].

Käesolevas dokumendis tähendab „Sätted puuduvad“, et täiendavaid piiranguid ei ole kehtestatud ja et asjassepuutuvaid QCP-n-qscd ja NCP+ sätteid kohaldatakse otse.

Mobiil-ID sertifikaatide väljastamine ja haldamine põhineb poliitika QCP-n-qscd nõuetel: EL-i kvalifitseeritud sertifitseerimispoliitika, mis on väljastatud füüsilistele isikutele isikliku võtmega, mis on seotud QSCD-s sertifitseeritud avaliku võtmega.

Mobiil-ID isikutuvastamist võimaldavate sertifikaatide väljastamine ja haldamine põhineb poliitika NCP+ nõuetel: Normitud sertifikaat Poliitika, mis nõuab turvalist krüptograafilist seadet.

Käesolevas CP-s kirjeldatud Mobiil-ID kvalifitseeritud elektroonilise allkirja sertifikaatide sertifitseerimisteenus PEAB olema kvalifitseeritud usaldusteenus Eesti usaldusnimekirja kohaselt.

Vastuolude korral TULEB arvestada järgmisi dokumente järgmises järjekorras (ülimuslikud eespool):

- QCP-n-qscd,
- NCP+,
- käesole
- v CP,
  CPS.

Käesolevas CP-s on täielikult ümber kujundatud eelmine „AS Sertifitseerimiskeskus – sertifitseerimispõhimõtted“ [1] ja Mobiil-ID vormis digitaalse isikutunnistuse sertifitseerimispoliitika [2].
Nimetatud dokumentide ümberkujundamine standardi IETF RFC 3647 [3] kohaselt ja käesoleva CP jõustamine ei muuda oluliselt vastavate sertifitseerimisteenuste osutamist.

IETF RFC 3647 [3] ülesehituse säilitamiseks on käesolev CP jaotatud üheksaks osaks, seejuures on mittekohaldatavate jaotiste pealkirjade all märge **„Ei**

kohaldata“. Iga kõrgema taseme peatükk sisaldab viiteid asjakohastele jaotistele standardis ETSI EN 319 411-1 [4] ja ETSI EN 319 411-2 [5].

Käesolevas CP-s tuleb tõlgendada suurtähtedega kirjutatud modaalverbe ETSI koostamise eeskirjade [8] (sätete väljendamise verbaalsed kujud) punktis 3.2 kirjeldatud viisil.

Käesoleva CP punktis 1.6 nimetatud lühendid on kirjutatud käesolevas CP-s suurtähtedega.

1.2. Dokumendi nimi ja identifitseerimine

Vaadake standardi ETSI EN 319 411-1 [4] punkti 5.3 ja ETSI EN 319 411-2 [5].

Käesoleva dokumendi nimi on „AS Sertifitseerimiskeskus – Eesti Vabariigi Mobiil-ID sertifitseerimispoliitika“.

Käesoleva CP tunnuskood on OID: 1.3.6.1.4.1.10015.1.3

OID on koostatud vastavalt järgnevale tabelile.

Parameeter	**OID viide**
Interneti tunnus	1.3.6.1
Eraettevõtte tunnus	4
Eraettevõtteid haldava IANA poolt registreeritud ettevõtte tunnus	1
SK tunnus IANA registris	10015
Sertifitseerimisteenuse tunnus	1.3

Klientidele väljastatud Mobiil-ID kvalifitseeritud elektroonilise allkirja sertifikaat PEAB sisaldama järgmiste poliitikate OID-e:

- ETSI EN 319 411-2 [5] punkt 5.3 c) QCP-n-qscd puhul: 0.4.0.194112.1.2

  Itu-t(0) tuvastatud-organisatsioon(4) etsi(0) kvalifitseeritud-sertifikaatide-poliitikad(194112)

  poliitika-identifikaatorid(1) qcp-füüsiline-

- qscd (2) Käesolev CP.

Klientidele väljastatud Mobiil-ID isikutuvastamist võimaldavad sertifikaadid PEAVAD sisaldama järgmiste

- poliitikate OID-e: ETSI EN 319 411-1 [4] punkt 5.3 b) NCP+ puhul: 0.4.0.2042.1.2

  itu-t(0) tuvastatud-organisatsioon(4) etsi(0)

  muud-sertifikaatide-poliitikad(2042)

  poliitika-identifikaatorid(1)

- ncpplus (2) Käesolev CP.

1.3. Avalik infrastruktuur

Vaadake standardi ETSI EN 319 411-1 [4] punkti 5.4 ja ETSI EN 319 411-2 [5].

1.3.1. Sertifitseerimisasutus

Sätted puuduvad.

1.3.2. Registreerimisasutused

Politsei- ja Piirivalveamet (edaspidi PPA) ning mobiilside operaator (edaspidi MO) VÕIVAD
esineda dokumendis läbivalt mitmes rollis. Käesolevas CP-s eristatakse rolli alusel läbivalt järgmist:

- PPA-d ja MO-d koos nimetatakse registreerimisasutuseks (edaspidi RA), kui nad sooritavad tehnilisi toiminguid, mis ei ole konkreetse organisatsiooni suhtes spetsiifilised, nt kliendi autentimine.
- PPA-le ja MO-le viidatakse sõnaselgelt nende vastavate nimedega, kui nad sooritavad konkreetse organisatsiooniliigi jaoks spetsiifilisi toiminguid, nt kui MO väljastab kliendile QSCD nõuetele vastavad SIM-kaardid (edaspidi QSCD) või kui PPA esindab Eesti Vabariiki dokumentide väljastaja rollis vastavalt ITDS-ile [10] või isikute esialgse tuvastamise või otsuste tegemise ajal nende Mobiil-ID saamise kõlblikkuse kohta.

PPA-l ja MO-l on erinevad rollid, nende vastavaid kohustusi on kirjeldatud üksikasjalikumalt käesoleva dokumendi järgmistes punktides.

1.3.3. Kliendid

Klient on käesoleva CP alusel väljastatud sertifikaadi subjekt.

Klient PEAB olema ainult ITDS-i [10] alusel õigustatud füüsiline

isik.

1.3.4. Huvitatud isikud

Huvitatud isikud on sertifikaadi alusel otsuseid tegevad juriidilised või füüsilised isikud.

1.3.5. Teised pooled

SIM-kaardi valmistaja (edaspidi SCM) toodab QSCD, loob võtmepaarid ja laadib need QSCD-le.

MO seob kliendi konkreetse QSCD-ga ja väljastab QSCD kliendile.

Telekommunikatsiooniteenuse osutaja võimaldab sidet kliendi seadme ja QSCD vahel.

1.4. Sertifikaadi kasutamine

Vaadake standardi ETSI EN 319 411-1 [4] jaETSI EN 319 411-2 [5].
punkti 5.5

1.4.1. Sertifikaadi sobivad kasutusviisid

Kliendi sertifikaadid on mõeldud järgmisteks otstarveteks:

Kvalifitseeritud elektroonilise allkirja sertifikaat on mõeldud

järgmiseks:

- -kvalifitseeritud elektrooniliste allkirjade andmine vastavalt määrusele eIDAS [9].

Isikutuvastamist võimaldav sertifikaat on

- mõeldud järgmiseks:

  Autentimine,
- turvaline e-post.

CA isiklikke võtmeid EI TOHI kasutada muude sertifikaatide allkirjastamiseks peale järgmiste:

- QCP-n-qscd-le või NCP+-le vastavad kliendi sertifikaadid,
- OCSP vastuse kontrollimise
- sertifikaadid, tehnilisteks vajadusteks
  mõeldud sisesertifikaadid.

1.4.2. Sertifikaadi keelatud kasutusviisid

Käesoleva CP alusel väljastatud kliendi sertifikaate EI TOHI kasutada järgmistel otstarvetel:

- -ebaseaduslik tegevus (sh küberrünnakud ja katse rikkuda sertifikaati või Mobiil-ID-d), uute
- sertifikaatide väljastamine ja teave sertifikaatide kehtivuse kohta,
- kliendi isikliku võtme kasutamise võimaldamine teistele isikutele,
- elektrooniliseks allkirjastamiseks väljastatud sertifikaadi automaatse kasutamise võimaldamine,
- elektrooniliseks allkirjastamiseks väljastatud sertifikaadi kasutamine dokumentide allkirjastamiseks, millega võivad kaasneda soovimatud tagajärjed (sh selliste dokumentide allkirjastamine testimiseks).

Kliendi isikutuvastamist võimaldavat sertifikaati EI TOHI kasutada kvalifitseeritud elektrooniliste allkirjade andmiseks, mis vastavad määrusele eIDAS [9].

1.5. Poliitika haldamine

1.5.1. Dokumenti haldav organisatsioon

Käesolevat CP-d haldab SK.

AS Sertifitseerimiskeskus

Registrikood 10747013

Pärnu mnt 141, 11314 Tallinn

Tel +372 610 1880

Faks: +372 610 1881

E-post: info@sk.ee

http://www.sk.ee/en/

1.5.2. Kontaktisik

Ärijuht

E-post: info@sk.ee

1.5.3. CPS-i sobivust poliitikaga määrav isik

Sätted puuduvad.

1.5.4. CP heakskiitmise kord

Käesoleva CP sisulist tähendust mittemuutvate paranduste puhul, nagu õigekirjavigade parandamine, tõlkimine ja kontaktandmete ajakohastamine, TULEB muudatused dokumenteerida käesoleva dokumendi jaotises „Versioonid ja muudatused“.

Sellise juhul TULEB dokumendi versiooninumbri murdarvulist osa suurendada.

Sisuliste muudatuste puhul PEAB CP uus versioon olema eelnevatest selgelt eristatav ja seerianumbrit TULEB ühe võrra suurendada.

Muudetud CP koos jõustumiskuupäevaga, mis ei või olla varasem kui 30 päeva avaldamisest, TULEB avaldada elektrooniliselt SK kodulehel.

Kõik käesoleva CP muudatused TULEB kooskõlastada RA-ga.

Kõik muudatused PEAB kiitma heaks ärijuht ja muudetud CP PEAB jõustama tegevjuht.

1.6. Määratlused ja lühendid

1.6.1. Kasutatud terminoloogia

Käesolevas CP-s kasutatakse termineid alljärgnevas tähenduses.

Termin	Määratlus
AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted	Põhimõtted, mida SK rakendab usaldusteenuse osutamisel.
Autentimine	Isiku unikaalne tuvastamine tema väidetava identiteedi kontrollimise teel.
Sertifikaat	Kasutaja avalik võti koos muu teabega, mis on sätestatud sertifikaadi profiilis [6] ja mis on tänu selle väljastanud sertifitseerimisasutuse isikliku võtme abil šifreerimisele võltsimiskindel.
Sertifitseerimisasutus	SK struktuuri osa, mis vastutab elektrooniliste sertifikaatide ning sertifikaatide tühistusnimekirjade väljastamise ja kontrollimise eest oma elektroonilise allkirjaga.
Sertifikaadipaar	Sertifikaadipaar, mis sisaldab üht isikutuvastamist võimaldavat sertifikaati ja üht kvalifitseeritud elektroonilise allkirja sertifikaati.
Sertifitseerimispoliitika	Eeskirjad, mis näitavad konkreetse sertifikaadi rakendatavust mingis kindlas kogukonnas ja/või avalikus infrastruktuuris ühiste turvanõuetega.
Sertifitseerimis-põhimõtted	Üks mitmest dokumendist, mis kõik kokku moodustavad juhtimisraamistiku, mille alusel sertifikaate luuakse, väljastatakse, hallatakse ja kasutatakse.
Sertifikaadi profiil	Dokument, milles on määratud sertifikaadis sisalduv teave ja sertifikaadi miinimumnõuded.
Sertifikaat Tühistusnimekiri	Kehtetute (kehtetuks tunnistatud, kehtivus peatatud) sertifikaatide nimekiri.

Sertifitseerimisteenus	Sertifikaatide väljastamise, kehtivuse peatamise haldamise, kehtivuse peatatuse lõpetamise, kehtetuks tunnistamise, muutmise ja sertifikaatide võtmevahetusega seotud usaldusteenus.
Kataloogiteenus	Sertifikaatide kehtivuse teabe avaldamisega seotud usaldusteenus.
DigiDoc Service	SOAP-il põhinev veebiteenus, mille abil saab lisada e-teenusele või rakendusele hõlpsalt identifitseerimise, digitaalallkirja, allkirja identifitseerimise ja Mobiil-ID funktsionaalsuse.
Eraldusnimi	Subjekti nimi sertifikaatide infrastruktuuris, mis on iga kliendi jaoks unikaalne.
Krüpteerimine	Teabe töötlemise meetod, mis muudab teabe loetamatuks neile, kellel ei ole vajalikke oskusi või õigusi.
Terviklus	Massiivi omadus: teavet ei ole pärast massiivi loomist muudetud.
Mobiil-ID	Digitaalse isikutunnistuse vorm, mille elektroonilist identifitseerimist võimaldav sertifikaat ja elektroonilist allkirjastamist võimaldav sertifikaat on seotud mobiiltelefoni SIM-kaardiga.
Objekti identifikaator	Objekti unikaalseks nimetamiseks kasutatav identifikaator (OID).
PIN-kood	Autentimissertifikaadi ja kvalifitseeritud elektroonilise allkirja sertifikaadi aktiveerimiskood.
Isiklik võti	Võtmepaari võti, mida võtmepaari omanik hoiab salajas ja mida kasutatakse elektrooniliste allkirjade andmiseks ja/või selliste elektrooniliste dokumentide või failide dekrüpteerimiseks, mida krüpteeriti vastava avaliku võtmega.
Avalik võti	Võtmepaar, mida vastava isikliku võtme omanik võib avalikustada ja mida huvitatud isikud kasutavad selleks, et kontrollida omaniku vastava isikliku võtmega antud elektroonilisi allkirju ja/või krüpteerida teateid selliselt, et neid saaks dekrüpteerida vaid omaniku vastava isikliku võtmega.
PUK-kood	PIN-koodide lahtiblokeerimise koodid, kui need on pärast järjestikuste valede sisestuste lubatud arvu blokeeritud.
Kvalifitseeritud sertifikaat	Elektrooniliste allkirjade sertifikaat, mille väljastab usaldusteenuse osutaja ja mis vastab määruse eIDAS [9] määruse I lisas sätestatud nõuetele.
Kvalifitseeritud elektrooniline Allkiri	Täiustatud elektrooniline allkiri, mis luuakse kvalifitseeritud elektroonilise allkirja andmise vahendiga ja mis põhineb elektrooniliste allkirjade kvalifitseeritud sertifikaadil.
Kvalifitseeritud elektroonilise allkirja andmise vahend	Turvalise allkirja andmise vahend, mis vastab määruses eIDAS [9] sätestatud nõuetele.
Huvitatud isik	Üksus, mis kasutab sertifikaadis sisalduvat teavet.
Registreerimisasutus	Üksus, mis vastutab sertifikaatide subjektide identifitseerimise ja autentimise eest. Lisaks võib registreerimisasutus võtta vastu sertifikaatide taotlusi, kontrollida ja/või edastada neid sertifitseerimisasutusele.
Turvaline krüptograafiline seade	Seade, mis sisaldab kasutaja isiklikku võtit, kaitseb võtit ohtu sattumise eest ja sooritab kasutaja nimel allkirjastamis- või dekrüpteerimisfunktsioone.
Klient	Füüsiline isik, kellele väljastatakse Mobiil-ID sertifikaadid avaliku teenusena, kui tal on selleks seadusjärgne õigus.
Subjekt	Käesolevas dokumendis on subjekt sama mis klient.
Tingimused	Dokument, milles on kirjeldatud kliendi kohustusi ja vastutust seoses sertifikaatide kasutamisega. Sertifikaatide vastuvõtmisel peab klient olema tingimustega tutvunud ja nõustunud.

1.6.2. Lühendid

Lühend	Määratlus
CA	Sertifitseerimisasutus
CP	Sertifitseerimispoliitika. Käesolev dokument on CP.
CPS	Sertifitseerimispõhimõtted
CRL	Sertifikaatide tühistusnimekiri
eIDAS	Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014 [9] (23. juuli 2014) e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ.

ITDS	Isikut tõendavate dokumentide seadus [10]
MO	Mobiilside operaator
OCSP	Sertifikaadi oleku võrguprotokoll
OID	Objekti identifikaator, objekti identifitseerimise unikaalne kood
PPA	Politsei- ja Piirivalveamet
PKI	Avaliku võtme infrastruktuur
QSCD	Kvalifitseeritud elektroonilise allkirja andmise vahend
RA	Registreerimisasutus
SCM	SIM-kaardi valmistaja
SK	AS Sertifitseerimiskeskus, sertifitseerimisteenuse osutaja
SK PS	AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted [11]

2. Avaldamine ja repositooriumi vastutus

Vaadake standardi ETSI EN 319 411-1 [4] jaETSI EN 319 411-2 [5].
punkti 6.1

2.1. Repositooriumid

SK PEAB tagama oma repositooriumi kättesaadavuse 7 päeva nädalas ööpäev läbi; teenuse kättesaadavus on aastas minimaalselt 99% ja kavandatud seisakuaeg ei ületa iga-aastaselt 0,5%.

2.2. Sertifitseerimisteabe avaldamine

2.2.1. Avaldamis- ja teavitamispoliitika

Käesolev CP, sertifitseerimispõhimõtted [19], sertifikaadi profiil [6] ja tingimused [7] koos
jõustumiskuupäevadega TULEB avaldada SK vähemalt 30 päeva enne jõustumist.
veebilehelhttps://sk.ee/en/repository/

2.2.2. Sertifitseerimispõhimõtetes avaldamata jäänud kirjed

Teabe teenuse tasemete, tasude ja tehniliste üksikasjade kohta, mis on esitatud SK, PPA ning MO vahelistes lepingutes, VÕIB CPS-ist välja jätta.
CPS.

CPS ei TOHI hõlmata PPA ega MO sisekorda.

2.3. Avaldamise aeg ja sagedus

Sätted puuduvad.

2.4. Repositooriumide juurdepääsu kontrollimine

Sätted puuduvad.

3. Identifitseerimine ja autentimine

Vaadake standardi ETSI EN 319 411-1 [4] punkti 6.2 ja standardit ETSI EN 319 411-2 [5].

3.1. Nimetamine

Sertifikaadi eraldusnimi PEAB vastama sertifikaadi profiilis [6] kehtestatud tunnustele.

3.1.1. Nimede liigid

Sätted puuduvad.

3.1.2. Vajadus, et nimed oleksid tähendusega

Kõik sertifikaadi klienditeabejaotises sisalduvad väärtused PEAVAD olema tähendusega.

3.1.3. Klientide anonüümsus või pseudonüümsus

Ei ole lubatud.

3.1.4. Erinevate nimevormide tõlgendamise reeglid

ITDS-i [10] kohaselt TULEB võõrtähed vajaduse korral kodeerida vastavalt ICAO ümberkirjutusreeglitele. E-posti aadresside loomise eeskirjad TULEB nimetada sertifikaadi profiili [6] punktis 6.1.

3.1.5. Nimede unikaalsus

SK PEAB tagama, et erinevatele klientidele ei väljastata sertifikaate kokkulangeva üldnime (CN), seerianumbri ega e-posti aadressidega subjekti lisanime
(SAN) väljadel.

3.1.6. Kaubamärkide tunnustamine, autentimine ja roll

Ei kohaldata.

3.2. Identiteedi esialgne kinnitamine

3.2.1. Isikliku võtme omamise tõendamise meetod

MO PEAB sooritama kliendi autentimise ja väljastama kliendile QSCD.

Klient PEAB allkirjastama vastava avalduse ja kinnitama niiviisi väljastatud QSCD omandiõigust.

3.2.2. Organisatsiooni identiteedi autentimine

Ei kohaldata.

3.2.3. Üksikisiku identiteedi autentimine

Klientide autentimist sooritab RA järgmiselt. MO PEAB

sooritama kliendi autentimise kahel puhul:

- kui klient taotleb uut Mobiil-ID-d,
- kui kliendil on vaja asendada kehtiva Mobiil-ID QSCD (sertifikaadi võtmevahetus).

Mobiil-ID esialgsel taotlemisel PEAB MO autentima kliendi füüsilise kohaloleku kontrolli teel.

Kui kliendil on vaja asendada QSCD (sertifikaadi võtmevahetus), VÕIB MO autentida kliendi elektrooniliselt või füüsilise kohaloleku teel.

Mobiil-ID kasutamise kõlblikkuse kontrollimiseks PEAB PPA kliendi autentima. Elektrooniline autentimine PEAB OLEMA lubatud.

Elektroonilise autentimise võimaldamiseks peab kliendil olema kehtiv Eesti Vabariigi digitaalne isikutunnistus või Eesti Vabariigi isikutunnistus.

RA PEAB sooritama autentimise vastavalt ITDS-i [10] 3. peatükile.

3.2.4. Kontrollimata kliendiandmed

Kontrollimata kliendiandmeid EI TOHI sertifikaadis lubada.

3.2.5. Volituste kinnitamine

ITDS-i [10] kohaselt ei saa klient taotleda Mobiil-ID-d esindaja kaudu.

3.2.6. Koostoimivuse kriteeriumid

Sätted puuduvad.

3.3. Identifitseerimine ja autentimine võtmevahetuseks

3.3.1. Identifitseerimine ja autentimine tavapäraseks võtmevahetuseks

Sertifikaadi võtmevahetus asendab kehtiva Mobiil-ID puhul kliendi QSCD uuega.

Kliendi QSCD asendatakse, kui QSCD saab näiteks kahjustada või kui see on vaja asendada muudel põhjustel.

Võtmevahetuse taotlemise autentimise kirjeldust vaadake käesoleva CP punktist 3.2.3.

3.3.2. Identifitseerimine ja autentimine võtmevahetuseks pärast kehtetuks tunnistamist

Võtmevahetuse korral pärast kehtetuks tunnistamist TULEB kliendi identiteet kinnitada vastavalt käesoleva CP punktile 3.2.

3.4. Identifitseerimine ja autentimine kehtetuks tunnistamise taotlemiseks

Sätted puuduvad.

4. Sertifikaadi elutsükli tegevusnõuded

Vaadake standardi ETSI EN 319 411-1 [4] jaETSI EN 319 411-2 [5].
punkti 6.3

4.1. Sertifikaadi taotlemine

4.1.1. Kes võib sertifikaaditaotluse esitada

Sertifikaaditaotluse VÕIB esitada klient RA kaudu.

SK PEAB võtma sertifikaaditaotlusi vastu ainult RA-lt.

Sertifikaadi taotlemise protsess PEAB tagama, et kliendi valduses või kontrolli all on isiklik võti, mis on seotud sertifitseerimiseks esitatud avaliku võtmega.

4.1.2. Registreerimisprotsess ja vastutus

Sertifikaadi taotlemise kõlblikkust puudutavate otsuste tegemise vastutus ja protsess on sätestatud ITDS-i [10] 3. peatükis.

Kui klient taotleb uut Mobiil-ID-d, TULEB olemasolev Mobiil-ID lõpetada ja kliendile TULEB väljastada
uus Mobiil-ID.

Üks Mobiil-ID taotlemiseks vajalikke eeldusi on olemasolev ja kehtiv Eesti Vabariigi digitaalne isikutunnistus või Eesti Vabariigi isikutunnistus.

SK vastutab õige e-posti aadressi määramise eest
autentimissertifikaadile keskkonnas eesti.ee:

- eelmise korduskasutus, kui kliendile on aadress juba määratud
- eelnevalt kasutamata aadressi loomine vastavalt sertifikaadi profiili [6] punktile 6.1, kui kliendil on uus nimi
- eelnevalt kasutamata aadressi loomine. vastavalt sertifikaadi profiili [6] punktile 6.1, kui kliendile ei ole eelnevalt aadressi määratud.

CA vastutab arvepidamise eest määratud e-posti aadresside üle.

Registreerimisprotsess on järgmine.

- MO PEAB autentima kliendi käesoleva CP punktis 3.2.3 esitatud viisil.
- Õnnestunud autentimise korral PEAB klient allkirjastama MO-ga Mobiil-ID lepingu.
- MO PEAB väljastama kliendile QSCD ja selle CA-s isikustama. QSCD isikustamiseks esitab MO CA-le teavet, mis seob kliendi väljastatud QSCD-l olevate isiklike võtmetega ja vastavate avalike võtmega, mida CA kasutab sertifitseerimiseks.
- Klient PEAB taotlema sertifitseerimist PPA infosüsteemis. PPA PEAB autentima kliendi käesoleva CP punktis 3.2.3 esitatud viisil ja kontrollima kliendi Mobiil-ID kasutamise kõlblikkust vastavalt ITDS-ile [10].

4.2. Sertifikaaditaotluse menetlemine

4.2.1. Identifitseerimis- ja autentimisfunktsioonide sooritamine

Klient võib taotleda sertifitseerimist kahel võimalikul viisil:

- Kui klient taotleb uut Mobiil-ID-d, taotleb klient sertifitseerimist PPA infosüsteemis. PPA taotleb CA-s sertifitseerimist kliendi nimel.
- QSCD asendamisel (sertifikaadi võtmevahetus), taotleb MO CA-s sertifitseerimist kliendi nimel. Mõlemal juhul

autendib RA kliendi käesoleva CP punktis 3.2.3 esitatud viisil.

Õnnestunud autentimise korral VÕIB klient taotleda sertifitseerimist, allkirjastades vastava taotluse kas MO juures või PPA-s. SK PEAB

võtma sertifikaaditaotlusi vastu ainult RA-lt ja PEAB kasutama RA-st esitatud identifitseerimisandmeid.

4.2.2. Sertifikaaditaotluste heakskiitmine või tagasilükkamine

CA PEAB keelduma sertifikaadi väljastamisest, kui sertifikaaditaotlus ei vasta kehtivate lepingutega kehtestatud tehnilistele nõuetele.

Kui sertifikaaditaotluses sisalduvaid andmeid on vaja muuta, TULEB vastav muudatus kooskõlastada RA-ga. Kui CA keeldub

sertifikaati väljastamast, TULEB teavitada sertifitseerimist taotlenud üksust.

4.2.3. Sertifikaaditaotluste menetlemise aeg

Vastavalt kehtivatele seadustele ja lepingutele.

4.3. Sertifikaadi väljastamine

4.3.1. CA tegevused sertifikaadi väljastamisel

Sätted puuduvad.

4.3.2. Kliendi teavitamine sertifikaadi väljastamisest CA poolt

CA PEAB teavitama RA-d uue sertifikaadi väljastamisest kliendile. RA

PEAB teavitama klienti uue sertifikaadi väljastamisest.

4.4. Sertifikaadi vastuvõtmine

4.4.1. Käitumine sertifikaadi vastuvõtmisel

Kui klient taotleb uut Mobiil-ID-d, PEAVAD sertifikaadi vastuvõtuks olema täidetud järgmised tingimused: Klient on

- allkirjastanud PPA-s sertifitseerimistaotluse käesoleva CP punktis 4.2.1 esitatud viisil,
- CA on saanud PPA-lt vastava sertifitseerimistaotluse kätte.

Kui klient taotleb uut QSCD-d (sertifikaadi võtmevahetus), PEAVAD sertifikaadi vastuvõtuks olema täidetud järgmised

- tingimused: Klient on allkirjastanud MO juures sertifitseerimistaotluse käesoleva CP punktis 4.2.1 esitatud viisil,
- CA on saanud MO-lt vastava sertifitseerimistaotluse kätte.

4.4.2. Sertifikaadi avaldamine CA poolt

Sertifikaat TULEB teha kättesaadavaks kataloogiteenuse ja tarkvara DigiDoc Service [18] kaudu, OCSP PEAB hakkama vastama „HEA“.

4.4.3. Sertifikaadi väljastamisest teatamine CA poolt teistele üksustele

Väljastatud sertifikaatidest TULEB teavitada telekommunikatsiooniteenuse osutajat.

4.5. Võtmepaar ja sertifikaadi kasutamine

4.5.1. Kliendi isiklik võti ja sertifikaadi kasutamine

Sätted puuduvad.

4.5.2. Huvitatud isiku avalik võti ja sertifikaadi kasutamine

Sätted puuduvad.

4.6. Sertifikaadi uuendamine

Ei ole lubatud.

4.7. Sertifikaadi võtmevahetus

Sertifikaadi võtmevahetus asendab kehtiva Mobiil-ID puhul kliendi QSCD uuega. Käesolevas CP-s käsitatakse korduvaid Mobiil-ID taotlusi kehtiva Mobiil-ID ajal esialgsete uue Mobiil-ID taotlustena. Kui klient taotleb uut Mobiil-ID-d samal ajal, kui tal on kehtiv Mobiil-ID-leping, TULEB taotlust menetleda uue Mobiil-ID taotlusena ja olemasolev Mobiil-ID TULEB lõpetada.

4.7.1. Sertifikaadi võtmevahetuse asjaolud

Sertifikaadi võtmevahetust TULEB lubada ainult juhul, kui QSCD tuleb asendada kliendi hooletuse tõttu või kui QSCD on kahjustatud või kui see on vaja asendada muudel põhjustel.

Kui klient on kaotanud Mobiil-ID hooletuse tõttu, PEAB klient taotlema uut Mobiil-ID-d ja taotlust tuleb menetleda uue Mobiil-ID taotlusena käesoleva CP punktis 3.2.3 esitatud viisil.

4.7.2. Kes võib uue avaliku võtme sertifitseerimist taotleda

Võtmevahetuse protsessi VÕIVAD algatada ainult klient ja MO koos.

SK EI TOHI võtmevahetuse taotlusi võtta vastu muudelt isikutelt peale RA.

4.7.3. Sertifikaadi võtmevahetuse taotluste menetlemine

Sertifikaadi võtmevahetuse protsess on järgmine:

- MO PEAB autentima kliendi käesoleva CP punktis 3.2.3 esitatud viisil.
- Õnnestunud autentimise korral PEAB klient allkirjastama MO-ga lepingu.
- MO PEAB väljastama kliendile uue QSCD ja selle CA-s isikustama. QSCD isikustamiseks esitab MO CA-le teavet, mis seob kliendi väljastatud QSCD-l olevate isiklike võtmetega ja vastavate avalike võtmega, mida CA kasutab sertifitseerimiseks.
- MO PEAB taotlema CA-s sertifitseerimist kliendi nimel.

Väljastatud sertifikaatide kehtivusaeg EI TOHI ületada vastava Mobiil-ID kehtivusaega. Asendatud sertifikaadid

TULEB kohe kehtetuks tunnistada.

4.7.4. Kliendi teavitamine uue sertifikaadi väljastamisest

CA PEAB teavitama MO-d uue sertifikaadi väljastamisest kliendile. MO

PEAB teavitama klienti uue sertifikaadi väljastamisest.

4.7.5. Käitumine uue võtmega sertifikaadi vastuvõtmisel

Vaadake käesoleva CP punkti 4.4.1.

4.7.6. Uue võtmega sertifikaadi avaldamine CA poolt

Vaadake käesoleva CP punkti 4.4.2.

4.7.7. Sertifikaadi väljastamisest teatamine CA poolt teistele üksustele

Vaadake käesoleva CP punkti 4.4.3.

4.8. Sertifikaadi muutmine

Sertifikaadi muutmine PEAB olema lubatud ainult sertifitseerimisel esinevate vigade korral.

4.8.1. Sertifikaadi muutmise asjaolud

Sertifikaadi muutmine on lubatud järgmiseks:

- e-posti aadresside muutmine, mis on kirjutatud isikutuvastamist võimaldavate sertifikaatide subjekti
- lisanime väljale, sertifikaatide ASN.1 kodeerimisvigade parandamine,
- SHA-1 allkirjade asendamine tugevama krüptograafiaga.

Sertifikaadi muutmise täiendavad asjaolud TULEB leppida kokku PPA-ga ning CP ja CPS tuleb muutuste kajastamiseks uuendada.

4.8.2. Kes võib sertifikaadi muutmist taotleda

Sertifikaadi muutmise VÕIB sooritada CA siseselt või seda võib taotleda PPA.

4.8.3. Sertifikaadi muutmise taotluste menetlemine

CA PEAB menetlema sertifikaadi muutmise taotlusi ja ta ei ole kohustatud kliendiga selle üle läbi rääkima.

Sertifikaadid TULEB kohe kehtetuks tunnistada.

Viimati väljastatud sertifikaatide kehtivusaeg EI TOHI ületada vastava Mobiil-ID kehtivusaega.

4.8.4. Kliendi teavitamine uue sertifikaadi väljastamisest

Sätted puuduvad.

4.8.5. Käitumine muudetud sertifikaadi vastuvõtmisel

Sätted puuduvad.

4.8.6. Muudetud sertifikaadi avaldamine CA poolt

Vaadake käesoleva CP punkti 4.4.2.

4.8.7. Sertifikaadi väljastamisest teatamine CA poolt teistele üksustele

Vaadake käesoleva CP punkti 4.4.3.

4.9. Sertifikaadi kehtetuks tunnistamine ja kehtivuse peatamine

4.9.1. Kehtetuks tunnistamise asjaolud

Sertifikaadi kehtetuks tunnistamise asjaolud TULEB sätestada ITDS-is [10] ja määruse eIDAS Eesti täiendusakti [12] artiklis 19.

4.9.2. Kes võib kehtetuks tunnistamist taotleda

Sertifikaadi kehtetuks tunnistamise taotlemiseks kõlblikud üksused TULEB sätestada ITDS-is [10] ja määruse eIDAS Eesti täiendusakti [12] artiklis 19 sätestatud viisil.
.

4.9.3. Sertifikaadi kehtetuks tunnistamise taotlemise kord

Sertifikaadi kehtetuks tunnistamise taotlemise kord TULEB sätestada ITDS-is [10] ja määruse eIDAS Eesti täiendusakti [20]

artiklis 12.Sertifikaadi kehtetuks tunnistamist TULEB kohaldada ainult sertifikaadipaaridele.

Kui sertifikaadipaari üks sertifikaat tunnistatakse kehtetuks, tunnistatakse kehtetuks terve sertifikaadipaar. Muud sertifikaadipaarid VÕIVAD jääda kehtivaks.

Mobiil-ID kehtetuks tunnistamise korral tunnistatakse kehtetuks kõik seotud sertifikaadipaarid.

4.9.4. Kehtetuks tunnistamise taotlemise ajapikendus

Sätted puuduvad.

4.9.5. Aeg, mille jooksul CA peab kehtetuks tunnistamise taotlemist menetlema

Sätted puuduvad.

4.9.6. Kehtetuks tunnistamise kontrollimise nõuded huvitatud isikutele

Sätted puuduvad.

4.9.7. CRL-i väljastamise sagedus

Sätted puuduvad.

4.9.8. CRL-ide maksimaalne latentsusaeg

Sätted puuduvad.

4.9.9. Kehtetuks tunnistamise / oleku kontrollimise kättesaadavus veebis

Sätted puuduvad.

4.9.10. Kehtetuks tunnistamise veebis kontrollimise nõuded

Sätted puuduvad.

4.9.11. Kehtetuks tunnistamise teadete muud kättesaadavad vormid

Sätted puuduvad.

4.9.12. Võtme ohtu sattumisega seotud erinõuded

Sätted puuduvad.

4.9.13. Kehtivuse peatamise asjaolud

Sertifikaadi kehtivuse peatamise asjaolud TULEB sätestada määruse eIDAS Eesti täiendusakti [12] artiklis 17.

4.9.14. Kes võib kehtivuse peatamist taotleda

Sertifikaadi kehtivuse peatamist võivad taotleda kõik.

4.9.15. Kehtivuse peatamise taotlemise kord

Mobiil-ID kasutamist võimaldava telekommunikatsiooniteenuse peatamist PEAB olema võimalik taotleda telefoni teel 7 päeva nädalas ööpäev läbi. Telekommunikatsiooniteenuse peatamisega kaasneb Mobiil-ID kasutamise võimatus.

Sertifikaadi kehtivuse peatamise taotlemine PEAB olema CA-s võimalik. Sertifikaadi kehtivuse peatamist TULEB kohaldada ainult sertifikaadipaaridele. Kui sertifikaadipaari ühe sertifikaadi kehtivus tuleb peatada, peatatakse terve sertifikaadipaari kehtivus. Muud sertifikaadipaarid VÕIVAD jääda kehtivaks. Sertifikaadi kehtivuse peatamine PEAB jätma unikaalselt tuvastatava jälje.

4.9.16. Kehtivuse peatamise aja piirid

Piire ei ole.

4.9.17. Kehtivuse peatatuse lõpetamise asjaolud

Sertifikaadi kehtivuse peatatuse lõpetamise asjaolud TULEB sätestada määruse eIDAS Eesti täiendusakti [12] artiklis 18 sätestatud viisil.

Telekommunikatsiooniteenuse peatatust PEAB olema võimalik MO juures lõpetada. Kui telekommunikatsiooniteenuse peatatus lõpetatakse, on võimalik Mobiil-ID-d uuesti kasutada.

Kliendil PEAB olema võimalik taotleda sertifikaadi kehtivuse peatatuse lõpetamist MO juures juhul kui:

- kliendile on väljastatud QSCD, klient on allkirjastanud Mobiil-ID-lepingu ja sertifikaatide kehtivus on peatatud ning
- kliendi mobiiltelefoninumber muutub, kuid klient jätkab numbri ja Mobiil-ID kasutamist.

Sertifikaadi kehtivuse peatatust PEAB olema võimalik MO juures lõpetada. Sertifikaadi kehtivuse peatatuse lõpetamist TULEB kohaldada ainult sertifikaadipaaridele. Kui sertifikaadipaari ühe sertifikaadi kehtivuse peatatus tuleb lõpetada, lõpetatakse terve sertifikaadipaari kehtivuse peatatus.

4.9.18. Kes võib kehtivuse peatatuse lõpetamist taotleda

Üksused, mis võivad sertifikaadi kehtivuse peatatuse lõpetamist taotleda, TULEB sätestada määruse eIDAS Eesti täiendusakti artiklis 18 [12].

4.9.19. Kehtivuse peatatuse lõpetamise kord

Sertifikaadi kehtivuse peatatuse lõpetamise kord TULEB sätestada määruse eIDAS Eesti täiendusakti [12] artiklis 18.

4.10. Sertifikaadi staatuse kontrollimise teenused

4.10.1. Kasutusomadused

Sätted puuduvad.

4.10.2. Teenuse kättesaadavus

SK PEAB tagama oma sertifikaadi staatuse kontrollimise teenuste kättesaadavuse 7 päeva nädalas ööpäev läbi; teenuse kättesaadavus on aastas minimaalselt 99% ja kavandatud seisakuaeg ei ületa iga-aastaselt 0,5%.

4.10.3. Kasutusfunktsioonid

Sätted puuduvad.

4.11. Tellimuse lõppemine

Sätted puuduvad.

4.12. Deponeerimine ja taastamine

4.12.1. Deponeerimise ja taaste poliitika ning tavad

Ei ole lubatud.

4.12.2. Seansivõtme kapselduse ja taaste poliitika ning tavad

Ei kohaldata.

5. Vahendid, haldamine ja tegevuskontroll

Vaadake standardi ETSI EN 319 411-1 [4] jaETSI EN 319 411-2 [5].
punkti 6.4

6. Tehniline turvakontroll

Vaadake standardi ETSI EN 319 411-1 [4] jaETSI EN 319 411-2 [5].
punkti 6.5

6.1. Võtmepaari loomine ja installeerimine

6.1.1. Võtmepaari loomine

Isiklik võti TULEB luua QSCD-l või FIPS 140-2 3. tasandi sertifitseeritud HSM-is SIM-kaardi valmistamise protsessi käigus, mille järel tuleb TULEB võtmed kanda turvaliselt üle SIM-kaardile. Kui võtme loomiseks kasutatakse spetsiaalset turvamoodulit, TULEB isiklikud võtmed kustutada SIM-kaardi valmistaja infosüsteemist kohe pärast nende ülekandmist SIM-kaardile. Isiklikke võtmeid EI TOHI salvestada ülekande käigus mujale peale SIM-kaardi.

6.1.2. Isikliku võtme üleandmine kliendile

SCM PEAB valmistama isikustamata QSCD-sid ja looma isikustamata võtmepaare.

Isiklikud võtmed TULEB laadida QSCD-l, mis TULEB anda üle MO-le.

MO PEAB sooritama kliendi autentimise, isikustama QSCD ja väljastama kliendile QSCD vastavalt käesoleva CP punktile 4.1.2.

6.1.3. Avaliku võtme üleandmine sertifikaadi väljastajale

SCM PEAB valmistama isikustamata QSCD-sid ja looma isikustamata võtmepaare. Avalikud

võtmed TULEB anda üle MO-le.

MO omakorda PEAB andma avalikud võtmed registreerimiseks üle CA-le.

6.1.4. CA avaliku võtme üleandmine huvitatud isikutele

Sätted puuduvad.

6.1.5. Võtmete suurused

Lubatud võtmete suurused PEAVAD vastama sertifikaadi profiilis [6] kirjeldatule.

6.1.6. Avaliku võtme parameetrite genereerimine ja kvaliteedikontroll

Sätted puuduvad.

6.1.7. Võtme kasutuseesmärgid (X.509 v3 võtme kasutusala kohta)

Lubatud võtmete kasutamise lipud TULEB määrata vastavalt sertifikaadi profiilis [6] kirjeldatule.

6.2. Isikliku võtme kaitse ja krüptograafilise mooduli tehniline kontroll

6.2.1. Krüptograafilise mooduli standardid ja kontroll

Võtmed TULEB luua FIPS 140-2 (3. tasandi) sertifitseeritud seadmel.

6.2.2. Isikliku võtme (n m-ist) kontrollimine mitme inimese poolt

Sätted puuduvad.

6.2.3. Isikliku võtme deponeerimine

Sätted puuduvad.

6.2.4. Isikliku võtme varundamine

Sätted puuduvad.

6.2.5. Isikliku võtme arhiveerimine

Sätted puuduvad.

6.2.6. Isikliku võtme edastamine krüptograafilisse moodulisse ja sealt välja

Sätted puuduvad.

6.2.7. Isikliku võtme hoidmine krüptograafilises moodulis

Sätted puuduvad.

6.2.8. Isikliku võtme aktiveerimine

Kliendil TULEB paluda sisestada autentimissertifikaadi PIN-kood vähemalt üks kord pärast telefoni väljalülitamist. Kliendil TULEB paluda

sisestada kvalifitseeritud elektroonilise allkirja sertifikaadi PIN-kood enne iga toimingut,
mis tehakse vastava isikliku võtmega.

PEAB olema võimalik luua erinevaid PIN-koode erinevate sihtotstarvetega, nt PEAB olema võimalik luua erinevaid
PIN-koode vastavalt autentimissertifikaadi ja kvalifitseeritud elektroonilise allkirja sertifikaadi jaoks.

PIN-koodide pikkus PEAB olema vähemalt järgmine:

- autentimisvõti 4 numbrit,
- allkirjavõti 5 numbrit, PUK-kood

PEAB olema vähemalt 8 numbrit.

6.2.9. Isikliku võtme deaktiveerimine

Sätted puuduvad.

6.2.10. Isikliku võtme hävitamine

Sätted puuduvad.

6.2.11. Krüptograafilise mooduli hindamine

Sätted puuduvad.

6.3. Võtmepaari haldamise muud aspektid

6.3.1. Avaliku võtme arhiveerimine

Sätted puuduvad.

6.3.2. Sertifikaadi ja võtmepaari kasutusaeg

Kliendile väljastatud sertifikaatide kehtivusaeg EI TOHI ületada vastava Mobiil-ID kehtivusaega ja see peab vastama ITDS-ile [10].

6.4. Aktiveerimisandmed

6.4.1. Aktiveerimisandmete genereerimine ja installeerimine

Esialgsed aktiveerimisandmed PEAB looma SCM ja need TULEB anda kliendile üle varjatud kujul.

SCM EI TOHI PIN-koodide koopiaid säilitada.

6.4.2. Aktiveerimisandmete kaitse

PIN-koodid TULEB printida SIM-kaardi ümbrise plastosale turvakihi alla nii, et neid ei oleks võimalik turvaelementi kahjustamata lugeda, ja MO peab andma need üle kliendile.

Klient PEAB veenduma PIN-koode vastu võttes, et turvaelement ei ole kahjustatud.

MO EI TOHI PIN-koodide koopiaid säilitada.

6.4.3. Aktiveerimisandmete muud aspektid

Sätted puuduvad.

6.5. Arvuti turvakontroll

6.5.1. Arvuti tehnilised turvanõuded

Sätted puuduvad.

6.5.2. Arvuti turvalisuse hindamine

Sätted puuduvad.

6.6. Elutsükli tehniline kontroll

6.6.1. Süsteemiarenduse kontroll

Sätted puuduvad.

6.6.2. Turvahalduse kontroll

Sätted puuduvad.

6.6.3. Elutsükli turvakontroll

Sätted puuduvad.

6.7. Võrgu turvalisuse kontroll

Sätted puuduvad.

6.8. Ajatemplid

Sätted puuduvad.

7. Sertifikaadi, CRL-i ja OCSP profiilid

Vaadake standardi ETSI EN 319 411-1 [4] jaETSI EN 319 411-2 [5].
punkti 6.6

7.1. Sertifikaadi profiil

Sertifikaat PEAB vastama sertifikaadi profiilis [6] kirjeldatud profiilile.

7.2. CRL-i profiil

CRL PEAB vastama sertifikaadi profiilis [6] kirjeldatud profiilile.

7.3. OCSP profiil

OCSP vastused PEAVAD vastama sertifikaadi profiilis [6] kirjeldatud profiilile.

8. Vastavusaudit ja muud hindamised

Vaadake standardi ETSI EN 319 411-1 [4] jaETSI EN 319 411-2 [5].
punkti 6.7

9. Muud tegevus- ja õigusalased küsimused

Vaadake standardi ETSI EN 319 411-1 [4] jaETSI EN 319 411-2 [5].
punkti 6.8

9.1. Tasud

9.1.1. Sertifikaadi väljastamise ja uuendamise tasud

Sätted puuduvad.

9.1.2. Sertifikaadi juurdepääsu tasud

Sätted puuduvad.

9.1.3. Kehtetuks tunnistamise ja oleku kontrolli teabe juurdepääsu tasud

Sätted puuduvad.

9.1.4. Muude teenuste tasud

Sätted puuduvad.

9.1.5. Tagastamispoliitika

Sätted puuduvad.

9.2. Rahaline vastutus

9.2.1. Kindlustuskate

Sätted puuduvad.

9.2.2. Muud varad

Sätted puuduvad.

9.2.3. Kindlustus- ja garantiikaitse lõppüksustele

Sätted puuduvad.

9.3. Tegevusalase teabe konfidentsiaalsus

Sätted puuduvad.

9.4. Isikuandmete privaatsus

9.4.1. Privaatsusplaan

Sätted puuduvad.

9.4.2. Privaatsena käsitatav teave

Sätted puuduvad.

9.4.3. Privaatseks mittepeetav teave

Sätted puuduvad.

9.4.4. Isikliku teabe kaitsmiskohustus

Sätted puuduvad.

9.4.5. Teavitus ja nõusolek erateabe kasutamiseks

Sätted puuduvad.

9.4.6. Kohtu- või haldusmenetlusest tulenev avalikustamine

Sätted puuduvad.

9.4.7. Teised teabe avalikustamise asjaolud

Sätted puuduvad.

9.5. Intellektuaalomandi õigused

SK omandab käesoleva CP intellektuaalomandi õigused.

9.6. Kinnitused ja garantiid

9.6.1. CA kinnitused ja garantiid

CA töötaja EI TOHI olla karistatud tahtliku kuriteo toimepanemise eest.

9.6.2. RA kinnitused ja garantiid

RA töötaja EI TOHI olla karistatud tahtliku kuriteo toimepanemise eest.

9.6.3. Kliendi kinnitused ja garantiid

Sätted puuduvad.

9.6.4. Huvitatud isiku kinnitused ja garantiid

Huvitatud isik PEAB enne sertifikaadi kasutamist kontrollima sertifikaadi kehtivust, kasutades SK pakutavaid kehtivuskinnitusteenuseid.

Huvitatud isik PEAB arvestama sertifikaadis nimetatud piiranguid ja PEAB tagama selle, et vastuvõetav tehing vastab käesolevale CP-le.

9.6.5. Teiste poolte kinnitused ja garantiid

PPA töötaja EI TOHI olla karistatud tahtliku kuriteo toimepanemise eest.

MO töötaja EI TOHI olla karistatud tahtliku kuriteo toimepanemise eest.

9.7. Garantiidest lahtiütlemine

Sätted puuduvad.

9.8. Vastutuse piirangud

Sätted puuduvad.

9.9. Hüvitised

Sätted puuduvad.

9.10. Tähtaeg ja lõpetamine

9.10.1. Tähtaeg

Vaadake käesoleva CP avaldamise ja teavitamispoliitika punkti 2.2.1.

9.10.2. Lõpetamine

Käesolev CP PEAB jääma jõusse, kuni see asendatakse uue versiooniga või lõpetatakse CA lõpetamise tõttu või teenus lõpetatakse ja kõik sertifikaadid muutuvad seega kehtetuks.

9.10.3. Lõpetamise tagajärjed ja kehtima jäävad sätted

SK PEAB tegema teatavaks käesoleva CP lõpetamise tingimused ja tagajärjed.

9.11. Individuaalsed teated ja suhtlemine pooltega

Sätted puuduvad.

9.12. Muudatused

9.12.1. Muudatuste tegemise kord

Vaadake käesoleva CP punkti 1.5.4.

9.12.2. Teavitusmehhanism ja -aeg

Vaadake käesoleva CP punkti 1.5.4.

9.12.3. Asjaolud, mis nõuavad OID-i muutmist

OID PEAB muutuma, kui käesoleva CP rakendusala muutub või kasutusele tuleb uut liiki sertifikaat.

9.13. Vaidluste lahendamise sätted

Sätted puuduvad.

9.14. Kohaldatav õigus

Käesolevat CP-d reguleerib Euroopa Liidu ja Eesti seadusandlus.

9.15. Vastavus kohaldatava õigusega

SK PEAB tagama järgmiste nõuete täitmise:

- eIDAS [9] – Euroopa Parlamendi ja nõukogu 23. juuli 2014. a määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ,
- määruse eIDAS Eesti täiendusakt [12]
- isikut tõendavate dokumentide seadus [10],
- riigilõivuseadus [14],
- isikuandmete kaitse seadus [15],
- seonduvad Euroopa standardid:

- ETSI EN 319 401 Elektroonilised allkirjad ja infrastruktuurid (ESI); Üldised poliitikanõuded usaldusteenuse osutajatele [16],

ETSI EN 319 -411-1 Elektroonilised allkirjad ja infrastruktuurid (ESI); Poliitika- ja turvanõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 1. osa: Üldised nõuded [4],

ETSI EN 319 -411-2 Elektroonilised allkirjad ja infrastruktuurid (ESI); Poliitika- ja turvanõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 2. osa: Poliitikanõuded kvalifitseeritud sertifikaate väljastavatele sertifitseerimisasutustele [5],

EN 419 211 P-Turvalise allkirja andmise vahendi kaitseprofiilid [13].

9.16. Muud sätted

9.16.1. Kogu lepingu ulatus

Sätted puuduvad.

9.16.2. Loovutamine

Sätted puuduvad.

9.16.3. Sätete kehtivus

Sätted puuduvad.

9.16.4. Jõustamine (õigusabikulud ja õigustest loobumine)

Sätted puuduvad.

9.16.5. Vääramatu jõud

Sätted puuduvad.

9.17. Muud sätted

Ei ole lubatud.

10. Viidatud dokumendid

1. AS Sertifitseerimiskeskus – sertifitseerimispõhimõtted (CPS), avaldatud: https://sk.ee/en/repository/CPS/;
2. ESTEID-kaardi sertifitseerimispoliitika, avaldatud: https://sk.ee/en/repository/CP;
3. RFC 3647 – Palve kommenteerimiseks 3647, internet X.509 avaliku võtme infrastruktuur, sertifitseerimispoliitika ja -tavade raamistik, avaldatud: https://www.ietf.org/rfc/rfc3647.txt
4. ETSI EN 319 411-1 V1.1.1 (2016-02) Elektroonilised allkirjad ja infrastruktuurid (ESI); Poliitika- ja turvanõuded Sertifikaate väljastavatele usaldusteenuse osutajatele; 1. osa: Üldnõuded
5. ETSI EN 319 411-2 V2.1.1 (2016-02) Elektroonilised allkirjad ja infrastruktuurid (ESI); Poliitika- ja turvanõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 2. osa: Poliitikanõuded kvalifitseeritud sertifikaate väljastavatele sertifitseerimisasutustele
6. Sertifikaadi, CRL-i ja OCSP profiilid Eesti Vabariigi isikut tõendavatel dokumentidel, avaldatud: https://www.sk.ee/repositoorium/profiil/
7. Eesti Vabariigi isikut tõendavate dokumentide sertifikaatide kasutustingimused, avaldatud: https://sk.ee/repositoorium/kasutustingimused// ;
8. ETSI koostamise eeskirjad (sätete väljendamise verbaalsed kujud)
9. eIDAS – Euroopa Parlamendi ja nõukogu 23. juuli 2014. a määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ
10. Isikut tõendavate dokumentide seadus, RT I 1999, 25, 365, avaldatudhttps://www.riigiteataja.ee/en/eli/511042016001/consolide/current
11. AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted, avaldatud: https://sk.ee/en/repository/sk-ps/
12. määruse eIDAS Eesti täiendusakt (2016-05, projekt)
13. ETSI EN 419 211 Turvalise allkirja andmise vahendi kaitseprofiilid
14. Riigilõivuseadus, avaldatud: https://www.riigiteataja.ee/en/eli/ee/519022016005/consolide/current
15. Isikuandmete kaitse seadus, 06.01.2016, avaldatud: https://www.riigiteataja.ee/en/eli/507032016001/consolide/current
16. ETSI EN 319 401 V2.1.1 (2016-02) Elektroonilised allkirjad ja infrastruktuurid (ESI); Üldised poliitikanõuded usaldusteenuse osutajatele
17. ISO/IEC 7816, 1.–4. osa, avaldatud aadressil http://iso.org/
18. DigiDoc Servicehttps://sk.ee/en/services/validity-confirmation-services/digidoc-service/
19. AS Sertifitseerimiskeskus – ESTEID-SK sertifitseerimispõhimõtted, avaldatud::https://sk.ee/repositoorium/CPS/