AS Sertifitseerimiskeskus – ID-kaardi sertifitseerimispoliitika

Tõlge AS Sertifitseerimiskeskuse originaaldokumendile "AS Sertifitseerimiskeskus – Certificate Policy for ID card"

Versioon 6.0

OID: 1.3.6.1.4.1.10015.1.1

Kehtiv alates 01.11.2016

Versioonide ajalugu		
Kuupäev	**Versioon**	**Muudatused/uuendused/parandused**
01.11.2016	6.0	Sertifitseerimispoliitika on ümber kujundatud vastavalt standardile IETF RFC 3647 [3] ja määrusele eIDAS [9].
25.01.2016	5.0	Punkt 1.2 – muudetud kasutatud terminoloogiat. Punkt 1.3 – muudetud kasutatud lühendite nimekirja. Punkt 1.4 – muudetud sertifitseerimispoliitika identifitseerimist. Punkt 1.5.2 – muudetud registreerimiskeskuse tegevuse kirjeldust. Punkt 1.5.3 – muudetud PPA tegevuse kirjeldust. Punkt 1.5.4 – muudetud Trübi tegevuse kirjeldust. Punkt 1.6 – muudetud PPA kontaktandmed. Punkt 2.1.1 – muudetud SK kohustuste kirjeldust. Punkt 2.1.2.1 – muudetud PPA klienditeeninduspunkti kohustuste kirjeldust. Punkt 2.1.3 – muudetud PPA kohustuste kirjeldust. Punkt 2.1.4 – muudetud nõudeid kliendile. Punkt 2.5 – muudetud auditi kirjeldust. Punkt 3.1 – muudetud kliendi isikusamasuse kontrolli. Punkt 4.1 – muudetud sertifikaaditaotluse esitamist. Punkt 4.2.1 – muudetud otsuse tegemist. Punkt 4.4 – muudetud sertifikaatide kehtivuse peatamist. Punkt 4.5 – muudetud sertifikaadi kehtivuse peatatuse lõpetamist. Punkt 4.6.2 – muudetud sertifikaadi kehtetuks tunnistamise taotluse esitamist. Punkt 6.1.2.1 – muudetud kliendi võtmete moodustamist. Punkt 9 – uuendatud viidatud ja seonduvate dokumentide nimekirja. Seoses sertifikaatide uuendamise ja vahetamise muudatustega on uuendatud järgmised punktid: Punkt 2.1.2.2 – SK klienditeeninduspunkti kohustused; Punkt 3.2 – Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord;

01.12.2014	4.0	Muudetud dokumendi nimi. Parandatud dokumendi sõnastust ja vormindust. Täpsustatud käesoleva dokumendi sisu. Punkt 1.2 – täiendatud uute terminitega e-residendi digi-ID, ID-1 vorm. Punktis 1.6 – muudetud SK ja PPA kontaktandmed. Punktis 2.1.2 ja 2.1.3 – muudetud registreerimiskeskuse ja PPA kohustusi. Punktis 2.4.2 – muudetud tühistusnimekirjade avaldamise sagedust. Punktis 4.6.1 – muudetud sertifikaadi kehtetuks tunnistamise volitusi. Punktis 6.1.2.1 – muudetud kliendi võtmete moodustamise kirjeldust. Punktis 6.1.2.3 – täiendatud kliendi isikliku võtme aktiveerimise reegleid.
01.09.2012	3.3	Lisatud 2011. aasta ID-kaardi ja EL-kaardi sertifikaatide vahetamine. Punkt 1.2 – täiendatud terminoloogiat. Punkt 2.1.2 – täiendatud registreerimiskeskuse kohustusi. Punkt 4.2.5 – muudetud sertifikaadi uuendamist ja vahetamist
01.01.2011	3.2	Lisatud uus dokument – elamisloakaart ja sellega seotud toimingud. Punkt 4.2.1 – täpsustatud digi-ID sertifikaaditaotluste esitamist. Punkt 4.2.3 – muudetud sertifikaatide aktiveerimist, sertifikaadid aktiveeritakse kohe kliendi juuresolekul. Punkt 4.2.5 – täpsustatud sertifikaatide uuendamist ning toimingute lubatust erinevate dokumentide korral. Punkt 6.1.2.1 – täpsustatud kliendi võtmete loomist.
01.10.2010	3.1	Lisatud digitaalsele isikutunnistusele kehtestatud nõuded ning dokumendile omistatud 2 OID väärtust.
01.01.2010	2.2	Organisatsooni muudatused: Muudetud KMA – PPA ning PPA ja SK aadress.
28.08.2009	2.1	Ühildatud SK uuendatud CPS-iga. Keelelised korrektuurid. Muudetud punkti 1.5.1 – täpsustatud on rollide jaotust erinevare organisatsioonide vahel. Muudetud punkti 4.2.3 – sertifikaadid aktiveeritakse 1 tunni jooksul alates ID-kaardi väljastamisest.
19.06.2006	2.0	Muudatused vastavalt uuele ID-kaardi lepingu struktuurile.
17.10.2002	1.2	Ühitatud SK CPS-iga. Lisatud sertifikaadi uuendamist, ID-kaardi aktiveerimiskoodide muutmist käsitlev temaatika.
10.11.2001	1.1	Esmane versioon.

1. Sissejuhatus

1.1. Ülevaade

Käesolev dokument, edaspidi „AS Sertifitseerimiskeskus – ID-kaardi sertifitseerimispoliitika“ (edaspidi CP), määrab kindlaks menetlus- ja tegevusnõuded, mida Sertifitseerimiskeskus (edaspidi SK) järgib ja mille järgimist ta nõuab üksustelt Eesti Vabariigis väljastatud isikut tõendavate dokumentide ning elamisloakaardi sertifikaatide (edaspidi ID-kaart) väljastamisel ja haldamisel. Sertifikaadid võimaldavad elektroonilist allkirjastamist ja identifitseerimist füüsilistel isikutel. Sertifikaadid on alati paarides: iga ID-kaart sisaldab üht isikutuvastamist võimaldavat sertifikaati ja üht kvalifitseeritud elektroonilise
allkirja sertifikaati ning nende vastavaid isiklikke võtmeid. Iga isiklikku võtit kaitsevad eraldi aktiveerimisandmed (PIN-kood) ja igal ID-kaardil on üks lukust avamise kood (PUK). Ühel isikul saab korraga olla ainult üks kehtiv ID-kaart. ID-kaardid on füüsiliselt ID-1 vormis, vastab standardile ISO/IEC 7816 [17] ja ID-kaardi dokumentatsioonile [18].

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

> 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.**

ID-kaardi 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.

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

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

Kasutatavaid andmestruktuure ja sideprotokolle PEAB kirjeldama vajaduse korral ID-kaardi dokumentatsioonis [18].

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 ESTEID-kaardi 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 standardit ETSI EN 319 411-2 [5].

Käesoleva dokumendi nimi on „AS Sertifitseerimiskeskus – ID-kaardi

sertifitseerimispoliitika“. Käesoleva CP tunnuskood on OID: 1.3.6.1.4.1.10015.1.1

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	1.1

Klientidele väljastatud ID-kaardi 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)

Klientidele väljastatud ID-kaardi 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 standardit ETSI EN 319 411-2 [5].

1.3.1. Sertifitseerimisasutus

Sätted puuduvad.

1.3.2. Registreerimisasutused

Isikut tõendavate dokumentide seaduse (edaspidi ITDS [10]) kohaselt sätestatakse registreerimisasutused ITDS-i [10] 3. peatükis.

MÄRKUS. Politsei- ja Piirivalveameti ja Välisministeerium VÕIVAD esineda protsessis läbivalt mitmes rollis. Käesolevas CP-s eristatakse rolli alusel läbivalt järgmist:

- mõlemat asutust nimetatakse registreerimisasutuseks (RA), kui nad sooritavad tehnilisi toiminguid nagu silmast silma autentimine või ID-kaartide üleandmine;
- neid nimetatakse koos PPA-ks, kui nad esindavad ITDS-i [10] kohaselt Eesti Vabariiki dokumentide väljastaja rollis, nt isikute esialgse tuvastamise või otsuste tegemise ajal nende ID-kaardi taotlemise kõlblikkuse kohta.

1.3.3. Kliendid

Klient on käesoleva CP alusel väljastatud sertifikaadi subjekt.

Klient saab olla 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

Kaardi isikustaja on ID-kaardi valmistaja.

1.4. Sertifikaadi kasutamine

Vaadake standardi ETSI EN 319 411-1 [4] punkti 5.5 ja standardit ETSI EN 319 411-2 [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,
- krüpteerimine,
- 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 digi-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 PPA ja kaardi isikustajaga.

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.
Kaardi isikustaja	ID-kaartide valmistaja.
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.
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.
Eraldusnimi	Subjekti unikaalne nimi sertifikaatide infrastruktuuris.

Krüpteerimine	Teabe töötlemise meetod, mis muudab teabe loetamatuks neile, kellel ei ole vajalikke oskusi või õigusi.
ID-kaart	Identifitseerimisdokument, mis on Eesti kodaniku ja Eestis püsivalt elava Euroopa Liidu kodaniku kohustuslik isikut tõendav dokument.
ID-1	Vorm, millega on määratletud isikutunnistuste füüsilised omadused vastavalt standardile ISO/IEC 7816 [17].
Terviklus	Massiivi omadus: teavet ei ole pärast massiivi loomist muudetud.
Objekti identifikaator	Objekti unikaalseks nimetamiseks kasutatav identifikaator (OID).
Isikuandmete fail	ID-kaardi fail, mis sisaldab kliendi isikuandmeid.
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.
EL-kaart	Elamisloakaart on Eestis kehtiva elamisloa või elamisõiguse alusel püsivalt elava välismaalase kohustuslik isikut tõendav dokument, mida väljastatakse aastast 2011 ITDS-i [10] alusel õigustatud isikutele. Käesolevas dokumendis nimetatakse seda ID-kaardiks. Eesti elamisluba ei ole sama mis EL-i elamisluba.
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 ID-kaardi 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
CSR	Sertifikaadi signeerimise taotlemine
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]
OCSP	Sertifikaadi oleku võrguprotokoll
OID	Objekti identifikaator, objekti identifitseerimise unikaalne kood
PKI	Avaliku võtme infrastruktuur
QSCD	Kvalifitseeritud elektroonilise allkirja andmise vahend
RA	Registreerimisasutus
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] punkti 6.1 ja standardit ETSI EN 319 411-2 [5].

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 veebilehel https://sk.ee/en/repository vähemalt 30 päeva enne jõustumist.

2.2.2. Sertifitseerimispõhimõtetes avaldamata jäänud kirjed

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

CPS EI TOHI sisaldada PPA ega kaartide isikustaja 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

Isiklikud võtmed TULEB luua QSCD-l isikustamise ajal kaardi isikustaja poolt.

3.2.2. Organisatsiooni identiteedi autentimine

Ei kohaldata.

3.2.3. Üksikisiku identiteedi autentimine

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

Kinnitamise PEAB sooritama RA vastavalt ITDS-ile [10].

3.2.6. Koostoimivuse kriteeriumid

Sätted puuduvad.

3.3. Identifitseerimine ja autentimine võtmevahetuseks

3.3.1. Identifitseerimine ja autentimine tavapäraseks võtmevahetuseks

Klient TULEB tuvastada, ID-kaardi autentimissertifikaadi abil, mis vajab võtmevahetust, või vastavalt käesoleva CP punktile 3.2.

3.3.2. Identifitseerimine ja autentimine võtmevahetuseks pärast kehtetuks tunnistamist

Vaadake käesoleva CP punkti 3.2.

3.4. Identifitseerimine ja autentimine kehtetuks tunnistamise taotlemiseks

Sätted puuduvad.

4. Sertifikaadi elutsükli tegevusnõuded

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

4.1. Sertifikaadi taotlemine

4.1.1. Kes võib sertifikaaditaotluse esitada

Isikute ID-kaardi taotlemise kõlblikkus on määratletud ITDS-is [10]. SK PEAB CSR-e vastu võtma ainult kaardi isikustajalt.

4.1.2. Registreerimisprotsess ja vastutus

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

Positiivse otsuse korral PEAB PPA taotlema kaardi isikustajalt uue ID-kaardi.

Kaardi isikustaja kohustus on valmistada kaart, jäädvustada sellele visuaalsed elemendid, täita kaardil olev isikuandmete fail, luua autentimise ning kvalifitseeritud elektroonilise allkirja võtmepaarid ja esitada SK-le CSR-ide paar.

PPA vastutab õigete isiku tuvastamise andmete (nimed, isikukoodid, kuupäevad, pilt) esitamise eest kaardi isikustajale. Kaart Isikustaja ja SK kasutavad PPA esitatud väärtusi.

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 kliendil ei ole eelnevat aadressi.

SK vastutab arvepidamise eest määratud e-posti aadresside üle.

4.2. Sertifikaaditaotluse menetlemine

4.2.1. Identifitseerimis- ja autentimisfunktsioonide sooritamine

Kliendi identiteedi PEAB kinnitama PPA ITDS-i [10] 3. peatükis kirjeldatud viisil.

PPA PEAB saatma sertifikaaditaotlused SK-le kaardi isikustaja kaudu.

SK PEAB võtma vastu CSR-e ainult kaardi isikustajalt. SK ja kaardi isikustaja PEAVAD kasutama isiku tuvastamise andmeid, mille esitab PPA.

4.2.2. Sertifikaaditaotluste heakskiitmine või tagasilükkamine

CA PEAB keelduma sertifikaadi väljastamisest, kui sertifikaaditaotlus ei vasta kehtivate lepingutega kehtestatud tehnilistele nõuetele. Kui CSR-is sisalduvaid andmeid on vaja muuta, TULEB vastav muudatus kooskõlastada PPA-ga.

4.2.3. Sertifikaaditaotluste menetlemise aeg

Vastavalt kehtivatele seadustele ja lepingutele.

4.3. Sertifikaadi väljastamine

4.3.1. CA tegevused sertifikaadi väljastamisel

CA PEAB eraldama kliendile keskkonnas eesti.ee õige ja unikaalse e-posti aadressi. Selles etapis EI TOHI OCSP teenus anda vastust „HEA“ ja sertifikaati EI TOHI teha kataloogiteenuse kaudu kättesaadavaks.

4.3.2. Kliendi teavitamine sertifikaadi väljastamisest CA poolt

Sätted puuduvad.

4.4. Sertifikaadi vastuvõtmine

4.4.1. Käitumine sertifikaadi vastuvõtmisel

Sätted puuduvad.

4.4.2. Sertifikaadi avaldamine CA poolt

CA PEAB avaldama sertifikaadi kataloogiteenuse kaudu kohe pärast seda, kui klient on selle vastu võtnud, OCSP PEAB hakkama vastama „HEA“.

4.4.3. Sertifikaadi väljastamisest teatamine CA poolt teistele üksustele

Sätted puuduvad.

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 PEAB olema lubatud ainult kliendi õnnestunud isiklikul tuvastamisel füüsilise identiteedi kontrolli või digitaalsete autentimismeetodite abil.

Sertifikaadi võtmevahetuse ajal TULEB asendatavad sertifikaadid tunnistada kehtetuks.

Sertifikaadi võtmevahetuse VÕIB sooritada ainult esialgsel taotlemisel ID-kaardi tootmisvigade korral enne sertifikaatide vastuvõtmist. Sellisel juhul TULEB kirjutada vastavale kaardile ainult viimased sertifikaadid, mis jäävad kehtivaks. Kõik vigased või kasutamiskõlbmatud sertifikaadid TULEB kohe kehtetuks tunnistada.

4.7.1. Sertifikaadi võtmevahetuse asjaolud

Käesolevas CP-s käsitatakse korduva ID-kaardi taotlust esialgse ID-kaardi taotlusena. Kui klient taotleb korduvat ID-kaarti, TULEB taotlust menetleda uue ID-kaardi taotlusena ning TULEB sooritada füüsiline autentimine. Sertifikaadi

võtmevahetus on lubatud järgmiseks:

- aegunud või rikkis ID-kaardi asendamine;
- sertifikaatide ASN.1 kodeerimisvigade parandamine;
- SHA-1 allkirjade asendamine tugevama krüptograafiaga;
- kvaliteedikontrolli käigus avastatud tootmisvigade parandamine.

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

4.7.2. Kes võib uue avaliku võtme sertifitseerimist taotleda

Kui sertifikaadi asendamise vajadust ei avastata kvaliteedikontrolli ajal enne ID-kaardi üleandmist kliendile, VÕIVAD võtmevahetuse protsessi algatada ainult klient ja kaardi isikustaja koos. SK EI TOHI võtta vastu uue võtme taotlusi muudelt isikutelt peale kaardi isikustaja.

4.7.3. Sertifikaadi võtmevahetuse taotluste menetlemine

Kui uue võtme otstarve on asendada aegunud või rikkis ID-kaardi või taotleda korduvat ID-kaarti, on protsess sarnane esialgse väljastamisega.

Vastasel juhul TULEB menetleda sertifikaadi uue võtme taotlusi sertifikaadi muutmise taotlusi automaatselt turvaliste sidekanalite kaudu. Enne uute sertifikaatide väljastamist TULEB klient autentida isikliku võtme abil, mis vastab asendatavale kehtivale autentimissertifikaadile. Uued sertifikaadid TULEB kirjutada ID-kaardile. Vanad sertifikaadid TULEB kohe kehtetuks tunnistada. Mõlemad ID-kaardi sertifikaadid TULEB asendada samaaegselt.

4.7.4. Kliendi teavitamine uue sertifikaadi väljastamisest

Sätted puuduvad.

4.7.5. Käitumine uue võtmega sertifikaadi vastuvõtmisel

Sätted puuduvad.

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

Sätted puuduvad.

4.8. Sertifikaadi muutmine

Sertifikaadi muutmine PEAB olema lubatud ainult kliendi õnnestunud isiklikul tuvastamisel füüsilise identiteedi kontrolli või digitaalsete autentimismeetodite abil.

Sertifikaadi muutmise ajal TULEB asendatavad sertifikaadid tunnistada kehtetuks.

Sertifikaati VÕIB muuta ainult esialgsel taotlemisel ID-kaardi tootmisvigade korral enne sertifikaatide vastuvõtmist. Sellisel juhul TULEB kirjutada ID-kaardile ainult viimane sertifikaatide paar, mis jääb kehtivaks. Kõik vigased või kasutamiskõlbmatud sertifikaadid TULEB kohe kehtetuks tunnistada.

4.8.1. Sertifikaadi muutmise asjaolud

Sertifikaadi muutmine on lubatud järgmiseks:

- andmete muutmine, mis on jäädvustatud visuaalselt ID-kaardile ja salvestatud isikuandmete faili; e-
- posti aadresside muutmine, mis on kirjutatud autentimissertifikaadi subjekti lisanime väljale;
- sertifikaatide ASN.1 kodeerimisvigade parandamine;
- SHA-1 allkirjade asendamine tugevama krüptograafiaga;
- kvaliteedikontrolli käigus avastatud tootmisvigade parandamine.

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

Muutmisprotsessi VÕIVAD algatada klient ja kaardi isikustaja koos. Kui sertifikaadi asendamise vajadus avastatakse kvaliteedikontrolli ajal enne ID-kaardi üleandmist kliendile, VÕIB sertifikaadi muutmise sooritada CA-siseselt või seda võib taotleda PPA või isikustaja.

SK EI TOHI võtta vastu muutmise taotlusi muudelt isikutelt peale kaardi isikustaja.

4.8.3. Sertifikaadi muutmise taotluste menetlemine

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

Andmete muutmise korral, mis on jäädvustatud visuaalselt ID-kaardile ja salvestatud isikuandmete faili, TULEB taotlust menetleda uue ID-kaardi taotlusena ja TULEB sooritada füüsiline autentimine.

Vastasel juhul TULEB sertifikaadi muutmise taotlusi menetleda automaatselt turvaliste sidekanalite kaudu. Enne uute sertifikaatide väljastamist TULEB klient autentida isikliku võtme abil, mis vastab asendatavale kehtivale autentimissertifikaadile. Uued sertifikaadid TULEB kirjutada ID-kaardile. Vanad sertifikaadid TULEB kohe kehtetuks tunnistada. Mõlemad ID-kaardi sertifikaadid TULEB asendada samaaegselt.

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

Sätted puuduvad.

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.

.

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.

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.

Sätted

4.9.8. CRL-ide maksimaalne latentsusaeg

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

Sertifikaadi kehtivuse peatamise taotlemine PEAB olema võimalik telefoni teel 7 päeva nädalas ööpäev läbi. 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.

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] punkti 6.4 ja standardit ETSI EN 319 411-2 [5].

6. Tehniline turvakontroll

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

6.1. Võtmepaari loomine ja installeerimine

6.1.1. Võtmepaari loomine

Kliendi sertifikaadi võtmed TULEB luua QSCD abil ühes järgmistest rollidest:

- klient,
- kaardi isikustaja.

6.1.2. Isikliku võtme üleandmine kliendile

Sertifikaadi võtmed TULEB anda üle QSCD-l suletud ümbrikus, mille PEAB andma RA-le üle kaardi isikustaja. RA omakorda PEAB andma selle kliendile üle avamata kujul.

6.1.3. Avaliku võtme üleandmine sertifikaadi väljastajale

Kaardi isikustaja PEAB andma avaliku võtme CA-le üle, kasutades turvalist sidekanalit.

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

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

Isiklik võti TULEB luua QSCD-l.

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 ID-kaardi kaardilugejasse sisestamist.

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

Kliendi erinevatele võtmetele PEAB olema võimalik kehtestada erinevaid PIN-koode.

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

6.2.11. Krüptograafilise mooduli

Sätted

6.3. Võtmepaari haldamise muud aspektid

6.3.1. Avaliku võtme arhiveerimine

Sätted puuduvad.

6.3.2. Sertifikaadi ja võtmepaari kasutusaeg

Kliendi sertifikaadi kehtivusaeg EI TOHI ületada vastava ID-kaardi kehtivusaega, milleks see väljastati.

6.4. Aktiveerimisandmed

6.4.1. Aktiveerimisandmete genereerimine ja installeerimine

Esialgsed PIN-koodid PEAB looma kaardi isikustaja ja need TULEB lisada kliendile üleandmiseks eraldi suletud ümbrikku. Kaardi isikustaja EI TOHI PIN-koodide koopiaid säilitada.

Kaardi isikustaja PEAB tootma asendus-PIN-koode ja PEAB andma need RA-le üle suletud ümbrikes. PIN-koodide asendamise mehhanism PEAB välistama tehniliste vahenditega kogu protsessi jooksul võimaluse, et RA töötaja vaatab või salvestab asendus-PIN-koode.

RA PEAB väljastama kliendile asendus-PIN-koodid, kui PIN-koode on vaja asendada või uuendada. Ühe ID-

kaardi kõik PIN-koodid TULEB asendada korraga.

Enne asendus-PIN-koodide väljastamist PEAB RA kliendi autentima.

6.4.2. Aktiveerimisandmete kaitse

RA PEAB PIN-koodid kliendile isiklikult üle andma. RA 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] punkti 6.6 ja standardit ETSI EN 319 411-2 [5].

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] punkti 6.7 ja standardit ETSI EN 319 411-2 [5].

9. Muud tegevus- ja õigusalased küsimused

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

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

9.1.4. Muude teenuste tasud

Sätted

9.1.5.

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

SK omandab käesoleva CP intellektuaalomandi

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

Kaardi isikustaja 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 [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. ID-kaardi dokumentatsiooni veebileht: http://www.id.ee/index.php?id=35772
19. AS Sertifitseerimiskeskus – ESTEID-SK sertifitseerimispõhimõtted, avaldatud: https://sk.ee/en/repository/CPS/