AS Sertifitseerimiskeskus – Digi-ID sertifitseerimispoliitika

Tõlge AS Sertifitseerimiskeskuse originaaldokumendile "AS Sertifitseerimiskeskus – Certificate Policy for Digi-ID"

Versioon 6.0

OID: 1.3.6.1.4.1.10015.1.2

Kehtiv alates 01.11.2016

Versiooni ajalugu

Kuupäev	Versioon	Muudatused
01.11.2016	6.0	Sertifitseerimispoliitika on ümber kujundatud vastavalt standardile IETF RFC 3647 [7] ja määrusele eIDAS [2].
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 SK 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; Punkt 4.2.2 – Sertifikaadi väljastamine; Punkt 4.2.3 – ID-kaardi, EL-kaardi ja digi-ID väljastamine, sertifikaatide aktiveerimine; Punkt 4.2.5 – Sertifikaadi uuendamine ja vahetamine.
01.12.2014	4.0	Parandatud dokumendi sõnastust ja vormindust. Täpsustatud käesoleva dokumendi sisu. Punkt 1.2 – lisatud uued terminid E-residendi digi-ID ja ID-1 vorm. Punkt 1.6 – muudetud SK ja PPA kontaktandmed. Punktid 2.1.2 ja 2.1.3 – muudetud registreerimiskeskuse ja PPA kohustusi. Punkt 2.4.2 – muudetud tühistusnimekirjade avaldamise sagedust. Punkt 4.6.1 – muudetud sertifikaadi kehtetuks tunnistamise volitusi. Punkt 6.1.2.1 – muudetud kliendi võtmete moodustamise kirjeldust. Punkt 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 sertifikaatide 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 võtmete loomist.
01.10.2010	3.1	Lisatud digitaalsele isikutunnistusele kehtestatud nõuded ning dokumendile omistatud 2 OID väärtust.
01.01.2010	2.2	Organisatsioonilised muudatused: KMA on nüüd PPA (Politsei- ja Piirivalveamet); uuendatud PPA ja SK aadressid
28.08.2009	2.1	Ühildatud SK uuendatud CPS-iga. Keelelised parandused. Muudetud punkti 1.5.1 – täpsustatud on rollide jaotust erinevate organisatsioonide vahel. Muudetud punkti 4.2.3 – sertifikaadid aktiveeritakse 1 tunni jooksul alates ID-kaardi väljastamisest.
19.06.2006	2.0	Muudatused vastavalt ID-kaardi uuele lepingule.

17.10.2002	1.2	Ühildatud 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 – Digi-ID sertifitseerimispoliitika“ (edaspidi CP), määrab kindlaks menetlus- ja tegevusnõuded, mida Sertifitseerimiskeskus (edaspidi SK) järgib ja mille järgimist ta nõuab üksustelt Eesti Vabariigis väljastatud digitaalsete isikut tõendavate dokumentide ning e-elamisloakaartide sertifikaatide (edaspidi koos Digi-ID) väljastamisel ja haldamisel. Sertifikaadid võimaldavad elektroonilist allkirjastamist ja identifitseerimist füüsilistel isikutel.
Sertifikaadid on alati paarides: iga digi-ID 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 digi-ID-l on üks lukust avamise kood (PUK). Ühel isikul saab korraga olla ainult üks kehtiv digi-ID. Digi-ID on füüsiliselt ID-1 vormis, vastab standardile ISO/IEC 7816 [1] ja ID-kaardi dokumentatsioonile [18].

Digi-ID sertifikaatide väljastamine ja haldamine põhineb määrusel (EL) nr 910/2014 [2], 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 [4]), ja normitud sertifitseerimispoliitikale, mis nõuab turvalist krüptograafilist seadet (NCP+) (standardist ETSI EN 319 411-1 [3]).

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

Digi-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.

Digi-ID isikutuvastamist võimaldavate sertifikaatide väljastamine ja haldamine põhineb poliitika NCP+ nõuetel: normitud sertifitseerimispoliitika, mis nõuab turvalist krüptograafilist seadet.

Käesolevas CP-s kirjeldatud digi-ID 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“ [5] ja ESTEID-kaardi sertifitseerimispoliitika [6]. Nimetatud dokumentide ümberkujundamine standardi IETF RFC 3647 [7] kohaselt ja käesoleva CP jõustamine ei muuda oluliselt vastavate sertifitseerimisteenuste osutamist.

IETF RFC 3647 [7] 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 standardites ETSI EN 319 411-1 [3] ja ETSI EN 319 411-2 [4].

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 [3] punkti 5.3 ja standardit ETSI EN 319 411-2 [4].

Käesoleva dokumendi nimi on on “AS Sertifitseerimiskeskus – digi-ID

sertifitseerimispoliitika". Käesoleva CP tunnuskood on OID: 1.3.6.1.4.1.10015.1.2

OID on koostatud vastavalt järgnevale tabelile.

Parameeter	**Viide OID-is**
Interneti tunnus	1.3.6.1
Eraettevõtte tunnus	4
Eraettevõtteid haldava IANA poolt registreeritud ettevõtte tunnus	1
IANA registris SK-le antud tunnus	10015
Sertifitseerimisteenuse tunnus	1.2

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

- ETSI EN 319 411-2 [4] 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 digi-ID isikutuvastamist võimaldavad sertifikaadid PEAVAD sisaldama järgmiste

- poliitikate OID-e: ETSI EN 319 411-1 [3] 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. Avaliku võtme infrastruktuuri pooled

Vaadake standardi ETSI EN 319 411-1 [3] punkti 5.4 ja standardit ETSI EN 319 411-2 [4].

1.3.1. Sertifitseerimisasutused

Sätted puuduvad.

1.3.2. Registreerimisasutused

Registreerimisasutused on sätestatud isikut tõendavate dokumentide seaduse 3. peatükis (edaspidi „ITDS“ [9]).

MÄRKUS. Politsei- ja Piirivalveameti ja Välisministeerium VÕIVAD esineda dokumendis 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 digi-ID üleandmine;
- neid nimetatakse koos PPA-ks, kui nad esindavad ITDS-i [9] kohaselt Eesti Vabariiki dokumentide väljastaja rollis, nt isikute esialgse tuvastamise või otsuste tegemise ajal nende digi-ID taotlemise kõlblikkuse kohta.

1.3.3. Kliendid

Klient on käesoleva CP alusel väljastatud sertifikaadi subjekt.

Klient saab olla ainult ITDS-i [9] 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 valmistaja valmistab kaardid tehases ette ja tagab RA büroos tehnilise keskkonna isikustamiseks.

1.4. Sertifikaadi kasutamine

Vaadake standardi ETSI EN 319 411-1 [3] punkti 5.5 ja standardit ETSI EN 319 411-2 [4].

1.4.1. Sertifikaadi sobivad kasutusviisid

Kliendi sertifikaadid on mõeldud järgmisteks otstarveteks:

Kvalifitseeritud elektroonilise allkirja sertifikaat on mõeldud

järgmiseks:

- ITDS-i [2] nõuetele vastavate kvalifitseeritud elektroonilise allkirjade andmine .

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 eesmärkidel:

- 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 või kasutada kvalifitseeritud elektrooniliste allkirjade andmiseks, mis vastavad määrusele eIDAS [2].

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

1.5.2. Kontaktisik

Ärijuht

E-post: info@sk.ee

1.5.3. CPS-i sobivust poliitikaga määrav isik

Sätted puuduvad.

1.5.4. CPS-i heakskiitmise kord

Käesoleva CP tähendust mittemuutvad muudatused, nagu õigekirjavigade parandamine, tõlkimine ja kontaktandmete ajakohastamine, dokumenteeritakse 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 valmistajaga.

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

1.6. Definitsioonid ja lühendid

1.6.1. Terminoloogia

Käesolevas CP-s kasutatakse termineid alljärgnevas tähenduses.

Termin	Definitsioon
AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted	Põhimõtted, mida SK rakendab usaldusteenuse osutamisel.
Autentimine	Isiku unikaalne tuvastamine tema väidetava identiteedi kontrollimise teel.
Kaardi valmistaja	Valmistab digi-ID-kaardid tehases ette ja tagab RA büroos tehnilise keskkonna isikustamiseks.
Sertifikaat	Avalik võti koos muu teabega, mis on määratud sertifikaadi profiilis [11], mis on tänu sertifitseerimisasutuse poolt väljastatud isikliku võtmega 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 kogukonnas ja/või avaliku infrastruktuuri poolte rakendustes koos üldiste turbenõuetega.
Sertifitseerimispõhimõtted	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.
Sertifikaadi tühistusnime-kiri	Kehtetute (tühistatud, 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.
Digi-ID	Digitaalne isikutunnistus
Krüpteerimine	Teabe töötlemise meetod, mis muudab teabe loetamatuks neile, kellel ei ole vajalikke oskusi või õigusi.
ID-1	Vorm, millega on määratletud isikutunnistuste füüsilised omadused vastavalt standardile ISO/IEC 7816 [1].
Terviklus	Massiivi omadus: teavet ei ole pärast massiivi loomist muudetud.
Objekti identifikaator	Objekti unikaalseks nimetamiseks kasutatav identifikaator (OID).
Isikuandmete fail	Digi-ID 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 digitaalallkirjade loomiseks ja/või selliste andmete või failide dekrüpteerimiseks, mis krüpteeriti vastava avaliku võtmega.
Avalik võti	Võtmepaari võti, mida vastava isikliku võtme omanik võib avalikkusele avaldada ja mida huvitatud isik kasutab selleks, et kinnitada omaniku vastava isikliku võtmega loodud digitaalallkirju ja/või krüpteerida teateid, et neid saaks dekrüpteerida ainult 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 on välja andnud kvalifitseeritud usaldusteenuste osutaja ja mis vastab määruse eIDAS [2] lisas I kehtestatud 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	Turvaline allkirja andmise vahend, mis vastab määruses eIDAS [2] kehtestatud nõuetele.
Huvitatud isik	Isik, kes toetub sertifikaadis sisalduvale teabele.
Registreerimisasutus	Üksus, mis vastutab sertifikaadi kasutaja identifitseerimise ja autentimise eest. Lisaks sellele võib registreerimisasutus võtta vastu sertifikaatide taotlusi, neid kontrollida ja/või edastada need 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 on avaliku teenusena väljastatud digi-ID sertifikaadid, kui tal on selleks seadusega kehtestatud õigus.
Subjekt	Käesolevas dokumendis on subjekt sama mis klient.
Tingimused	Dokument, mis kirjeldab kliendi sertifikaatide kasutamisega seotud kohustusi ja vastutust. Klient peab olema dokumendiga tuttav ja sertifikaatide kättesaamisel tingimustega nõustuma.

1.6.2. Lühendid

Lühend	Definitsioon
CA	Sertifitseerimisasutus
CP	Sertifitseerimispoliitika. Käesolev dokument on CP.
CPS	Sertifitseerimise põhimõtted
CRL	Sertifikaatide tühistusnimekiri
CSR	Sertifikaadi signeerimise taotlemine
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.
ITDS	Isikut tõendavate dokumentide seadus
OCSP	Sertifikaadi kehtivuse kontroll
OID	Objekti identifikaator, objekti identifitseerimise unikaalne kood
PKI	Avaliku võtme infrastruktuur
QSCD	Turvaline allkirja andmise vahend
RA	Registreerimisasutus
SK	AS Sertifitseerimiskeskus, sertifitseerimisteenuse osutaja
SK PS	AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted [10]

2. Avaldamine ja repositooriumi vastutus

Vaadake standardi ETSI EN 319 411-1 [3] punkti 6.1 ja standardit ETSI EN 319 411-2 [4].

2.1. Repositooriumid

SK TAGAB oma depositooriumi 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[11] ja tingimused [12] koos jõustumiskuupäevadega TULEB avaldada SK veebilehel https://sk.ee/repositoorium/ 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 kaartide valmistaja vahelistes lepingutes, VÕIB CPS-ist välja jätta.

CPS EI TOHI sisaldada PPA ega kaartide valmistaja 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 [3] punkti 6.2 ja standardit ETSI EN 319 411-2 [4].

3.1. Nimetamine

Sertifikaadi eraldusnimi PEAB vastama sertifikaadi profiilis [11] 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 kohaldata.

3.1.4. Erinevate nimevormide tõlgendamise reeglid

ITDS-i [9] kohaselt TULEB võõrtähed vajaduse korral kodeerida vastavalt ICAO ümberkirjutusreeglitele. E-posti aadresside loomise eeskirjad TULEB nimetada sertifikaadi profiili [11] 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 PPA poolt.

3.2.2. Organisatsiooni identiteedi autentimine

Ei kohaldata.

3.2.3. Üksikisiku identiteedi autentimine

Autentimise sooritab RA vastavalt ITDS-i [9] 3. peatükile.

3.2.4. Kontrollimata kliendiandmed

Kontrollimata kliendiandmeid EI TOHI sertifikaadis lubada.

3.2.5. Volituste kinnitamine

Kinnitamise sooritab RA vastavalt ITDS-le [9].

3.2.6. Koostoimivuse kriteeriumid

Sätted puuduvad.

3.3. Identifitseerimine ja autentimine uue võtme taotlemiseks

3.3.1. Identifitseerimine ja autentimine tavapäraseks võtmevahetuseks

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

3.3.2. Identifitseerimine ja autentimine võtmevahetuseks pärast tühistamist

Vaadake käesoleva CP punkti 3.2.

3.4. Identifitseerimine ja autentimine tühistamise taotlemiseks

Sätted puuduvad.

4. Sertifikaadi elutsükli tegevusnõuded

Vaadake standardi ETSI EN 319 411-1 [3] punkti 6.3 ja standardit ETSI EN 319 411-2 [4].

4.1. Sertifikaadi taotlemine

4.1.1. Kes saab sertifikaati taotleda

Isikute digi-ID taotlemise kõlblikkus on määratletud ITDS-is [9]. SK PEAB võtma CSR-e vastu ainult kaardi valmistajalt.

4.1.2. Registreerimisprotsess ja vastutus

Sertifikaadi taotlemise kõlblikkust puudutavate otsuste tegemise vastutus ja protsess on sätestatud ITDS-is [9].

Kaardi valmistaja vastutab digi-ID valmistamise ja kaardi initsialiseerimise eest püsivara ning visuaalse kujunduse õige versiooniga.

Positiivse otsuse korral PEAB PPA isikustama uue digi-ID, täitma isikuandmete faili, looma autentimiseks võtmepaarid ja kvalifitseeritud elektroonilise allkirja ning esitama CSR-ide paari kaardi valmistajale. Kaardi valmistaja edastab sertifikaaditaotluse SK-le.

PPA vastutab õigete isiku tuvastamise andmete (nimed, isikukoodid, kuupäevad) esitamise eest kaardi valmistajale. Kaart Valmistaja 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 [11] punktile 6.1, kui kliendil on uus nimi eelnevalt kasutamata
- aadressi loomine vastavalt sertifikaadi profiili [11] punktile 6.1, kui kliendile ei ole eelnevalt aadressi määratud.

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 [9] 3. peatükis kirjeldatud viisil.

PPA PEAB saatma sertifikaaditaotlused SK-le kaardi valmistaja kaudu.
SK PEAB võtma CSR-e vastu ainult kaardi valmistajalt. SK ja kaardi valmistaja PEAVAD kasutama isiku tuvastamise andmeid, mille esitab PPA.

4.2.2. Sertifikaaditaotluse 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. Sertifikaaditaotluse 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 poole avalik võti ja sertifikaadi kasutamine

Sätted puuduvad.

4.6. Sertifikaadi uuendamine

Ei ole

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 kehtetuks tunnistada.

Sertifikaadi võtmevahetuse VÕIB sooritada ainult esialgsel taotlemisel digi-ID tootmisvigade korral enne sertifikaatide vastuvõtmist. Sellisel juhul TULEB kirjutada vastavale digi-ID andmekandjale ainult viimane sertifikaatide paar, mis jääb kehtivaks. Kõik vigased või kasutamiskõlbmatud sertifikaadid TULEB kohe kehtetuks tunnistada.

4.7.1. Sertifikaadi võtmevahetuse asjaolud

Käesolevas CP-s käsitatakse korduvat digi-ID taotlust esialgse digi-ID taotlusena. Kui klient taotleb korduvat digi-ID-d, TULEB menetleda taotlust uue digi-ID taotlusena ja TULEB sooritada füüsiline autentimine.

Sertifikaadi võtmevahetus on lubatud järgmiseks:

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

Täiendavad sertifikaadi võtmevahetuse asjaolud TULEB leppida kokku PPA-ga. 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 digi-ID üleandmist kliendile, VÕIVAD võtmevahetuse protsessi algatada ainult klient ja kaardi valmistaja koos.

SK EI TOHI võtta vastu uue võtme taotlusi muudelt isikutelt peale kaardi valmistaja.

4.7.3. Sertifikaadi võtmevahetuse taotluste menetlemine

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

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

4.7.4. Kliendi teavitamine uue sertifikaadi väljastamisest

Sätted puuduvad.

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 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 digi-ID tootmisvigade korral enne sertifikaatide vastuvõtmist. Sellisel juhul TULEB kirjutada vastavale digi-ID andmekandjale ainult viimane sertifikaatide paar, mis jääb kehtivaks. Kõik vigased või kasutamiskõlbmatud sertifikaadid TULEB kohe kehtetuks tunnistada.

EPOLE

4.8.1. Sertifikaadi muutmise asjaolud

Sertifikaadi muutmine on lubatud järgmiseks:

- andmete muutmine, mis on jäädvustatud visuaalselt digi-ID-le 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.

Täiendavad sertifikaadi muutmise asjaolud TULEB leppida kokku PPA-ga. CP ja CPS TULEB muutuste kajastamiseks uuendada.

4.8.2. Kes võib sertifikaadi muutmist taotleda

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

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

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 digi-ID-le ja salvestatud isikuandmete faili, TULEB taotlust menetleda uue digi-ID taotlusena ning 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 digi-ID andmekandjale. Vanad sertifikaadid TULEB kohe kehtetuks tunnistada. Mõlemad digi-ID 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

Vaadake käesoleva CP punkti 4.4.3.

4.9. Sertifikaadi tühistamine ja peatamine

4.9.1. Tühistamise asjaolud

Sertifikaadi kehtetuks tunnistamise asjaolud TULEB sätestada ITDS-is [9] ja määruse eIDAS Eesti täiendusakti [19] artiklis 19.

4.9.2. Kes saab tühistamist taotleda

Sertifikaadi kehtetuks tunnistamise taotlemiseks kõlblikud üksused TULEB sätestada ITDS-is [9] ja määruse eIDAS Eesti täiendusakti [13] artiklis 19.

4.9.3. Sertifikaadi kehtetuks tunnistamise taotlemise kord

Sertifikaadi kehtetuks tunnistamise taotlemise kord TULEB sätestada ITDS-is [9] ja määruse eIDAS Eesti täiendusakti [20] artiklis

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 [13] 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 [13] artiklis 18.

Sertifikaadi kehtetuks tunnistamise taotlemise kord TULEB sätestada ITDS-is [9] ja määruse eIDAS Eesti täiendusakti [20] artiklis

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. [13].

4.9.19. Kehtivuse peatatuse lõpetamise kord

Sertifikaadi kehtivuse peatatuse lõpetamise kord TULEB sätestada määruse eIDAS Eesti täiendusakti [13] artiklis 18.

4.10. Sertifikaadi oleku kontrollimise teenused

4.10.1. Kasutusomadused

Sätted puuduvad.

4.10.2. Teenuse kättesaadavus

SK TAGAB sertifikaadi oleku kontrollimise teenuste kättesaadavuse 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 taastamise 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 [3] punkti 6.4 ja standardit ETSI EN 319 411-2 [4].

6. Tehniline turvakontroll

Vaadake standardi ETSI EN 319 411-1 [3] punkti 6.5 ja standardit ETSI EN 319 411-2 [4].

6.1. Võtmepaari loomine ja installeerimine

6.1.1. Võtmepaari loomine

Kliendi sertifikaadi võtmed TULEB luua QSCD abil ühes järgmistest rollidest:

- klient,

- PPA.

6.1.2. Isikliku võtme üleandmine kliendile

Sertifikaadi võtmed TULEB anda üle QSCD-l, mille PEAB kliendile üle andma PPA.

6.1.3. Avaliku võtme üleandmine sertifikaadi väljastajale

PPA PEAB andma avaliku võtme kaardi valmistajale üle, kasutades turvalist sidekanalit.

Kaardi valmistaja 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 [11] 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 [11] 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 digi-ID 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
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

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

6.4. Aktiveerimisandmed

6.4.1. Aktiveerimisandmete genereerimine ja installeerimine

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

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

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

Ühe digi-ID kõik PIN-koodid asendatakse 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.
- PPA.

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 [3] punkti 6.6 ja standardit ETSI EN 319 411-2 [4].

7.1. Sertifikaadi profiil

Sertifikaat PEAB vastama sertifikaadi profiilis [11] kirjeldatud profiilile.

7.2. CRL-i profiil

CRL PEAB vastama sertifikaadi profiilis [11] kirjeldatud profiilile.

7.3. OCSP profiil

OCSP vastused PEAVAD vastama sertifikaadi profiilis [11] kirjeldatud profiilile.

8. Vastavusaudit ja muud hindamised

Vaadake standardi ETSI EN 319 411-1 [3] punkti 6.7 ja standardit ETSI EN 319 411-2 [4].

9. Muud tegevus- ja õigusalased küsimused

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

Kaardi valmistaja 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 punkti 2.2.1, „Avaldamis- ja teavitamispoliitika“.

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 [2] – Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ,
- määruse eIDAS Eesti täiendusakt [13],
- isikut tõendavate dokumentide seadus [9],
- riigilõivuseadus [14],

- isikuandmete kaitse seadus [15],
- seonduvad Euroopa standardid:
  - ETSI EN 319 401 [16] Elektroonilised allkirjad ja infrastruktuurid (ESI); Üldised poliitikanõuded usaldusteenuse osutajatele,
  - ETSI EN 319 411-1 [3] Elektroonilised allkirjad ja infrastruktuurid (ESI); Poliitika- ja turvanõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 1. osa: Üldised nõuded,
  - ETSI EN 319 411-2 [4] Elektroonilised allkirjad ja infrastruktuurid (ESI); Üldised poliitikanõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 2. osa: Poliitikanõuded kvalifitseeritud sertifikaate väljastavatele sertifitseerimisasutustele,
  - EN 419 211 [17] Turvalise allkirja andmise vahendi kaitseprofiilid.

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 ISO/IEC 7816, 1.–4. osa, avaldatud aadressil http://iso.org/
2 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
3 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
4 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
5 väljastavatele sertifitseerimisasutustele AS Sertifitseerimiskeskus – sertifitseerimispõhimõtted (SP), avaldatud:
.6 https://www.sk.ee/repositoorium/CPS/ ESTEID-kaardi sertifitseerimispoliitika, avaldatud:
.7 https://www.sk.ee/repositoorium/CP/
. RFC 3647 – Palve kommenteerimiseks 3647, internet X.509 avaliku võtme infrastruktuur, sertifitseerimispoliitika ja -tavade
8 raamistik, avaldatud: https://www.ietf.org/rfc/rfc3647.txt
.9 ETSI koostamise eeskirjad (sätete väljendamise verbaalsed kujud)
1.0 Isikut tõendavate dokumentide seadus, RT I 1999, 25, 365,
.11 avaldatudhttps://www.riigiteataja.ee/en/eli/511042016001/consolide/current
. AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted, avaldatud: https://sk.ee/en/repository/sk-ps/
12 Sertifikaadi, CRL-i ja OCSP profiilid Eesti Vabariigi isikut tõendavatel dokumentidel, avaldatud:
. https://www.sk.ee/repositoorium/profiil/https://sk.ee/en/repository/profiles/
13 Eesti Vabariigi isikut tõendavate dokumentide sertifikaatide kasutustingimused, avaldatud:
.14 https://sk.ee/repositoorium/kasutustingimused// https://sk.ee/en/repository/conditions-for-use-of-certificates/;
.15 määruse eIDAS Eesti täiendusakt (2016-05, projekt)
.16 Riigilõivuseadus, avaldatud: https://www.riigiteataja.ee/en/eli/ee/519022016005/consolide/current
Isikuandmete kaitse seadus, 06.01.2016, avaldatud: https://www.riigiteataja.ee/en/eli/507032016001/consolide/current
ETSI EN 319 401 V2.1.1 (2016-02) Elektroonilised allkirjad ja infrastruktuurid (ESI); Üldised poliitikanõuded usaldusteenuse

.
17
.18
.19
.

. Providers
17 ETSI EN 419 211 Protection profiles for secure signature creation device
18 ID card documentation webpage: http://www.id.ee/index.php?id=35772
19 AS Sertifitseerimiskeskus - ESTEID-SK Certification Practice Statement, published: https://www.sk.ee/repositoorium/CPS/