



ESTEID sertifitseerimispoliitika

Versioon 3.1
OID: 1.3.6.1.4.1.10015.1.1.3.1
OID: 1.3.6.1.4.1.10015.1.2.3.1
01.10.2010

Nõuded Eesti Vabariigi siseriiklikule isikutunnistusele ja digitaalsele isikutunnistusele digitaalallkirja ja digitaalse isikusamasuse kontrolli võimaldavate sertifikaatide väljastamiseks ja teenindamiseks.

Versiooni info		
Kuupäev	Versioon	Muudatused
01.10.2010	3.1	Lisatud Digitaalsele isikutunnistusele kehtestatud nõuded ning dokumendile omistatud 2 OID väärtust.
01.01.2010	2.2	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 lepingustruktuurile.
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

Sisukord

1. Sissejuhatus	4
1.1. Ülevaade	4
1.2. Kasutatud terminoloogia	4
1.3. Kasutatud lühendid	4
1.4. Sertifitseerimispoliitika identifitseerimine	4
1.5. Organisatsioon ja kasutusvaldkond	5
1.5.1. Sertifitseerimiskeskus (SK)	5
1.5.2. SK registreerimiskeskus	5
1.5.3. PPA	6
1.5.4. TRÜB	6
1.5.5. Kasutaja	6
1.5.6. Sertifikaatide kasutusvaldkond	7
1.6. Kontaktandmed	7
2. Üldtingimused	8
2.1. Kohustused ja nõuded	8
2.1.1. SK kohustused	8
2.1.2. Registreerimiskeskuse kohustused	8
2.1.3. PPA kohustused	9
2.1.4. Nõuded kliendile	9
2.1.5. Nõuded huvitatud isikule	9
2.1.6. Nõuded kataloogiteenusele	9
2.2. Vastutus	9
2.2.1. SK vastutus	9
2.2.2. Registreerimiskeskuse vastutus	10
2.2.3. PPA vastutus	10
2.2.4. Vastutuse piirid	10
2.3. Vaidluste lahendamine	10
2.4. Informatsiooni avaldamine ja kataloogiteenus	10
2.4.1. SK informatsiooni avaldamine	10
2.4.2. Avaldamise sagedus	10
2.4.3. Juurdepääsureeglid	11
2.4.4. Kataloogiteenus	11
2.5. Audit	11
2.6. Konfidentsiaalsus	11
3. Kliendi identifitseerimine	11
3.1. Kliendi isikusamasuse kontroll	11
3.2. Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord	11
3.3. Eraldusnimi	11
4. Sertifitseerimisteenuse osutamine Sertifitseerimismenetluse kord ja tähtajad	11
4.1. Sertifikaaditaotluse esitamine	12
4.2. Sertifikaaditaotluse menetlemine	12
4.2.1. Otsuse tegemine	12
4.2.2. Sertifikaadi väljastamine	12
4.2.3. ID-kaardi ja Digi-ID väljastamine, sertifikaatide aktiveerimine	12
4.2.4. Sertifikaadi kontroll ja tõestamine	13
4.2.5. Sertifikaadi uuendamine	13



4.3.	Sertifikaadi kehtetuks tunnistamise ja kehtivuse peatamise taotlused	13
4.4.	Sertifikaatide kehtivuse peatamine	13
4.5.	Sertifikaadi kehtivuse peatamise lõpetamine.....	13
4.6.	Sertifikaadi kehtetuks tunnistamine	13
4.6.1.	Sertifikaadi kehtetuks tunnistamise volitused	13
4.6.2.	Sertifikaadi kehtetuks tunnistamise taotluse esitamine	14
4.6.3.	Sertifikaadi kehtetuks tunnistamise menetlus.....	14
4.6.4.	Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus	14
4.7.	Protseduurid jälgitavuse tagamiseks	14
4.8.	Tegutsemise eriolukorras.....	14
4.9.	Sertifitseerimiseenuse osutaja töö lõpetamine	14
5.	Füüsilised ja organisatsioonilised turbemeetmed	14
5.1.	Turbehaldus	14
5.2.	Füüsilised turbemeetmed.....	14
5.2.1.	SK füüsiline pääsukontroll	14
5.2.2.	Muud nõuded. ID-kaartide ja Digi-ID hoiustamine.....	15
5.3.	Nõuded tööprotseduuridele.....	15
5.4.	Personali turbenõuded	15
6.	Tehnilised turbenõuded.....	15
6.1.	Võtmehaldus	15
6.1.1.	SK kinnitusvõtmed	15
6.1.2.	Kliendi võtmed	15
6.2.	Süsteemiturve	16
6.3.	Sertifitseerimiseenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus.....	16
6.4.	Sertifitseerimiseenuse osutamisel tekkinud andmete säilitamine ja kaitse	16
7.	Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid.....	16
8.	Sertifitseerimispoliitika haldus	16
9.	Viidatud ja seonduvad dokumendid	16

1. Sissejuhatus

1.1. Ülevaade

Käesolev dokument (edaspidi sertifitseerimispoliitika, CP) on reeglite kogum, mis määrab peamised tööpõhimõtted ja -kontseptsioonid EstEID kaardi (edaspidi ID-kaart) ja digitaalse isikutunnistuse (edaspidi Digi-ID), sertifikaatide väljastamiseks vajaliku sertifitseerimisteenuse osutamiseks.

Käesolev CP rajaneb dokumendile „AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted“ [1] (edaspidi CPS), mis on registreeritud Sertifitseerimise Registris. CPS on aluseks sertifitseerimisteenuse osutamisel, käesolev CP täpsustab täiendavalt CPS-is toodud põhimõtteid.

Käesoleva CP ja CPS-i vastuolu korral tuleb ülimuslikuks pidada käesolevas CP-s toodut.

Käesolev CP laieneb ainult AS-i Sertifitseerimiskeskus poolt väljastatud digitaalsetele sertifikaatidele.

Käesolev CP koostamisel on kasutatud IETFi (*Internet Engineering Task Force*) soovitusliku dokumenti RFC 2527 [4].

1.2. Kasutatud terminoloogia

Termin	Definitsioon
Klienditeeninduspunkt	Käesoleva CP alusel toimiv SK ja/või PPA klienditeeninduspunkt sertifitseerimisega seotud teenuste osutamiseks, vt punkt 1.5.2.1
Isikutunnistusele ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimused	Dokument, mis sisaldab Kliendi kohustusi ja vastutust ID-kaardi või Digi-ID-ga ning nendega seotud sertifikaatide kasutamisel. Klient peab ID-kaardi või Digi-ID väljastamisel olema tutvunud ja aktsepteerima selles dokumendis toodud tingimusi.

1.3. Kasutatud lühendid

Lühend	Definitsioon
PPA	Eesti Vabariigi Politsei- ja Piirivalveamet
SM	Eesti Vabariigi Siseministerium
TRÜB	TRÜB AG, ID-kaardi ja Digi-ID plangi tootja ja ID-kaardi isikustaja
SK	AS Sertifitseerimiskeskus, sertifitseerimisteenuse osutaja
STO	Sertifitseerimise Registris registreeritud sertifitseerimisteenuse osutaja

1.4. Sertifitseerimispoliitika identifitseerimine

Käesoleva CP tunnuscode on **OID**:

- **ID-kaardil 1.3.6.1.4.1.10015.1.1.3.1**
- **Digi-ID-l 1.3.6.1.4.1.10015.1.2.3.1**

OID tunnuskood lisatakse käesoleva CP alusel väljastatavasse sertifikaati.

CP tunnuskood on koostatud vastavalt järgnevale tabelile 1.

Parameeter	Viide OIDis
Interneti tunnus	1.3.6.1
Eraettevõtte tunnus	4
Eraettevõtteid haldava IANA poolt registreeritud ettevõtte tunnus	1
IANA registris ASile Sertifitseerimiskeskus antud tunnus	10015
Sertifitseerimisteenuse tunnus	1.1 – ID-kaardi puhul 1.2 – Digi-ID puhul
CP versiooni tunnus	3.1

Tabel 1. CP tunnuskoodi koostamine

1.5. Organisatsioon ja kasutusvaldkond

1.5.1. Sertifitseerimiskeskus (SK)

Vt CPS p.1.2.1.

Sertifikaadid väljastatakse ID-kaardile või Digi-ID-le. ID-kaardi väljastamise eest vastutab PPA. PPA-l on TRÜB-ga leping ID-kaardi ja Digi-ID plankide tootmiseks, ID-kaartide isikustamiseks ja ID-kaardile ning Digi-ID-le kantavate sertifikaatide väljastamiseks ja teenindamiseks. TRÜB ja SK vahelise lepinguga osutab SK registreeritud STO-na sertifitseerimisteenust. Vastavalt TRÜB ja PPA vahelisele lepingule teostab PPA punktis 1.5.2 ja 1.5.3 kirjeldatud ülesandeid.

1.5.2. SK registreerimiskeskus

1.5.2.1. Klienditeeninduspunktid

Vt CPS p.1.2.2.1.

ID-kaartide ja Digi-ID taotluste vastuvõtmine ning ID-kaartide ja Digi-ID väljastamine toimub PPA Prefektuuride kodakondsus- ja migratsioonibüroode teenindustes ning Eesti Vabariigi välisesindustes (edaspidi PPA klienditeeninduspunkt), mille täpne loetelu ja lahtiolekuajad viidatakse PPA ja SK kodulehekülgedel.

ID-kaartidega ja Digi-ID-ga seotud sertifikaatide teenindamine (sertifikaatide uuendamine, kehtivuse peatamine, kehtivuse peatamise lõpetamine, kehtetuks tunnistamine, asendus PIN-koodide määramine) toimub PPA ja/või SK klienditeeninduspunktides. Digi-ID-le asendus PIN-koodide määramine toimub ainult PPA klienditeeninduspunktides. Klienditeeninduspunktide täpne loetelu ja lahtiolekuajad viidatakse PPA ja SK kodulehekülgedel.

1.5.2.2. Abiliin

Vt CPS p.1.2.2.2.

Abiliin kasutab isikusamasuse kontrolliks protseduureegleid, mis on määratletud sisemiste dokumentidega. Abiliin annab vajadusel täiendavalt infot ID-kaardi ja Digi-ID-ga seotud probleemide lahendamisel.

1.5.3. PPA

PPA:

- võtab vastu ID-kaardi tellimusi ja edastab neid TRÜB-ile;
- edastab ID-kaarte klienditeeninduspunktile;
- väljastab isikustatud ID-kaardi kliendile;
- võtab vastu Digi-ID tellimusi ja isikustab Digi-ID;
- taotleb Digi-ID võtmetele vastavad sertifikaadid;
- laeb sertifikaadid Digi-ID-le;
- väljastab isikustatud Digi-ID kliendile.

PPA juhindub oma töös lepingus kokku lepitud ajalistest piirangutest.

PPA tagab turvalisuse enda kohustuste täitmisel sisemiste turbeprotseduuridega.

1.5.4. TRÜB

TRÜB:

- võtab vastu ID-kaardi tellimusi;
- isikustab ID-kaardi;
- moodustab ID-kaardi võtmed ja taotleb nendele vastavad sertifikaadid;
- laeb sertifikaadid ID-kaardile;
- annab isikustatud ID-kaardid PPA-le üle.
- toodab Digi-ID plangi
- moodustab Digi-ID võtmed

TRÜB juhindub oma töös lepingus kokku lepitud ajalistest piirangutest.

TRÜB tagab turvalisuse enda kohustuste täitmisel sisemiste turbeprotseduuridega.

1.5.5. Kasutaja

1.5.5.1. Klient

Vt CPS p.1.2.3.1.

Klient on füüsiline isik, kellele väljastatakse avaliku teenusena ID-kaardi ja Digi-ID sertifikaate, kui tal on selleks seadusjärgne õigus.

Klient on käesoleva CP alusel väljastatud sertifikaadi omanik.

Kliendi eraldusnimi sertifikaadis koostatakse vastavalt sertifikaadiprofiilile, mis on toodud dokumendis „Sertifikaadid Eesti Vabariigi isikutunnistusel”.

Kliendil peab olema võimalus enne ID-kaardi ja Digi-ID väljastamist tutvuda „Isikutunnistusele ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimustega“ [5].

1.5.5.2. Huvitatud isik

Vt CPS p.1.2.3.2.

1.5.6. Sertifikaatide kasutusvaldkond

Vt CPS p.1.2.4.

Käesoleva CP alusel väljastatakse kahte tüüpi sertifikaate:

- a) sertifikaate digitaalseks allkirjastamiseks
- b) sertifikaate isiku digitaalseks isikusamasuse kontrolliks

Sertifikaate digitaalseks allkirjastamiseks saab kasutada digitaalseks allkirjastamiseks DAS [3] mõttes.

CP ei sea piiranguid sertifikaatide kasutamiseks erinevates tarkvararakendustes ega rakendusvaldkondades.

1.6. Kontaktandmed

Vt CPS p.1.3.

SK

AS Sertifitseerimiskeskus
Äriregistri kood 10747013
Pärnu mnt 141, 11314 Tallinn
Telefon +372 610 1880
Faks +372 610 1881
E-post: pki@sk.ee
<http://www.sk.ee>

Abiliin

telefon 1777, +372 677 377

Klienditeeninduspunktid

Klienditeeninduspunktide kontaktandmed on viidatud veebilehel <http://www.sk.ee> ja <http://www.politsei.ee>

PPA kodakondsus- ja migratsiooniosakond

Endla 13,
15179 Tallinn
Info: (372) 612 3000
Üldtel.: (372) 612 3300
Faks: (372) 612 3009
E-post: teeninduskeskus@politsei.ee

PPA abiliin ID-kaardi ja Digi-ID-ga seotud probleemide lahendamiseks ja SK klienditeeninduspunktide töötajate nõustamiseks tööpäevadel kella 09.00-17.00: telefon 612 3000.

Kontaktandmete muutumisel teavitatakse sellest koheselt SK koduleheküljel <http://www.sk.ee> ja PPA koduleheküljel <http://www.politsei.ee>

TRÜB

Trüb Baltic AS
Laki 5

10621 Tallinn
Telefon +372 658 11 30
Faks +372 658 11 39
E-post info@trueb.ee

2. Üldtingimused

2.1. Kohustused ja nõuded

2.1.1. SK kohustused

Vt CPS p.2.1.1.

SK tagab täiendavalt, et:

- sertifitseerimisteenuse osutamine on kooskõlas AS Sertifitseerimiskeskuse sertifitseerimispõhimõtetega;
- sertifitseerimisteenuse osutamine on kooskõlas käesoleva CPga.

SK kohustub täiendavalt:

- võtma vastu Trübist ja PPA-st tulnud sertifikaaditaotlusi ja väljastama neile vastavaid sertifikaate;
- osutama ööpäevaringset kataloogiteenust;
- tagama, et sertifitseerimisteenuse osutamisel kasutatavad kinnitusvõtmed oleksid riistvaraliste turvamoodulite abil kaitstud ning ei väljuks SK kontrolli alt;
- kinnitusvõtmete kontrolli alt väljumise korral peatama kõikide väljastatud sertifikaatide kehtivuse;
- tagama, et kõik aktiveeritud režiimis olevad kinnitusvõtmed asuvad Eesti Vabariigi territooriumil;
- tagama, et sertifitseerimisteenuse osutamisel kasutatavate kinnitusvõtmete aktiveerimine toimub jagatud kontrolli alusel;
- juhinduma töös lepingus kokkulepitud ajalistest piirangutest.

2.1.2. Registreerimiskeskuse kohustused

2.1.2.1. PPA klienditeeninduspunkti kohustused

Vt CPS p.2.1.2.1.

PPA klienditeeninduspunkt kohustub täiendavalt:

- väljastama kliendile ID-kaardi või Digi-ID aktiveerides sinna laetud sertifikaadid;
- tagama esmase nõustamise ja abistamise ID-kaardi ja Digi-ID käsitlemisel.

2.1.2.2. SK klienditeeninduspunkti kohustused

SK klienditeeninduspunkt peab vastu võtma taotlusi ID-kaardi sertifikaatide uuendamiseks, kehtivuse peatamiseks, kehtivuse peatamise lõpetamiseks, kehtetuks tunnistamiseks ja asendus PIN-koodide määramiseks ning Digi-ID sertifikaatide kehtivuse peatamiseks, kehtivuse peatamise lõpetamiseks ja kehtetuks tunnistamiseks. SK Klienditeeninduspunkt peab kontrollima esitatud taotluste õigsust ja terviklikkust. Klienditeeninduspunkt kohustub kõikide nimetatud toimingute teostamisel kontrollima taotluse esitaja isikusamasust ja volitusi toimingute teostamiseks.

SK klienditeeninduspunkt garanteerib oma töötajatele teenuse kvaliteetseks osutamiseks vajaliku koolituse.

SK klienditeeninduspunkti töötajal ei tohi olla karistatust tahtlikult toimepandud kuriteo eest.

2.1.2.3. Abiliini kohustused

Vt CPS p.2.1.2.2.

2.1.3. PPA kohustused

PPA kohustub:

- oma sertifitseerimissüsteemiga seotud infosüsteemi osas järgima käideldavuse ja turbenõudeid, mis vastavad vähemalt käesolevas CP-s toodud nõuetele;
- tagama, et töötajatel, kes võtavad vastu ID-kaardi ja Digi-ID taotlusi ja/või on seotud sertifitseerimisest puudutava informatsiooniga, ei ole karistatust tahtlikult toimepandud kuriteo eest;
- edastama välisesindusest saabunud taotlustele, positiivse otsuse korral, vormistatud ID-kaardid ja digitaalsed isikutunnistused ning edastama sertifikaadid aktiveerimisjärjekorda;
- tagama ID-kaardi ja Digi-ID puudutava informatsiooni kättesaadavuse avalikus andmesidevõrgus aadressil <http://www.politsei.ee>.

2.1.4. Nõuded kliendile

Vt CPS p.2.1.3.

Klient peab ID-kaardi või Digi-ID taotluse esitamisel edastama PPA-le õige informatsiooni ning isikuandmete muutumise korral teatama õiged andmed PPA-le vastavalt kehtestatud õigusaktidele.

2.1.5. Nõuded huvitatud isikule

Vt CPS p.2.1.4.

2.1.6. Nõuded kataloogiteenusele

Vt CPS p.2.1.5.

Lisanõudeid kataloogiteenuse toimimiseks ette ei nähta.

2.2. Vastutus

2.2.1. SK vastutus

Vt CPS p.2.2.1.

SK on vastutav kõigi käesoleva CP punktides 2.1.1 ja 2.1.2 toodud kohustuste täitmise eest Eesti Vabariigis kehtivates õigusaktides nõutud piirides.

2.2.2. Registreerimiskeskuse vastutus

2.2.2.1. PPA klienditeeninduspunkti vastutus

Vt CPS p.2.2.2.1.

PPA vastutab oma klienditeeninduspunkti kõigi käesoleva CP punktis 2.1.2.1 toodud kohustuste täitmise eest.

2.2.2.2. SK klienditeeninduspunkti vastutus

Vt CPS p.2.2.2.1.

SK vastutab oma klienditeeninduspunkti kõigi käesoleva CP punktis 2.1.2.2 toodud kohustuste täitmise eest.

2.2.2.3. Abiliini vastutus

Vt CPS p.2.2.2.2.

SK ja PPA vastutavad oma abiliini kõigi käesoleva CP punktis 2.1.2.3 toodud kohustuste täitmise eest.

2.2.3. PPA vastutus

PPA vastutab kõigi käesoleva CP punktis 2.1.3 toodud ja teiste käesolevas CP-s toodud tema kohustuste täitmise eest.

2.2.4. Vastutuse piirid

Vt CPS p.2.2.3.

2.3. Vaidluste lahendamine

Vt CPS p.2.3.

2.4. Informatsiooni avaldamine ja kataloogiteenus

2.4.1. SK informatsiooni avaldamine

Vt CPS p.2.4.1.

Kehtiv tühistusnimekirj on kättesaadav aadressil <http://www.sk.ee/crls>

2.4.2. Avaldamise sagedus

Vt CPS p.2.4.2.

Sertifikaatide tühistusnimekirju avaldatakse reeglina iga 12 tunni järel.

2.4.3. Juurdepääsureeglid

Vt CPS p.2.4.3.

2.4.4. Kataloogiteenus

Vt CPS p.2.4.4.

Käesoleva CP alusel väljastatud sertifikaadid avaldatakse aktiveerimisel avalikus kataloogis aadressil `ldap://ldap.sk.ee`.

Sertifikaatide kehtivuse peatamisel või kehtetuks tunnistamisel sertifikaadid kustutatakse kataloogist. Kehtivuse peatamise lõpetamisel sertifikaadid taasavaldatakse.

Aegunud sertifikaadid kustutatakse kataloogist aegumiskuupäevale järgneval päeval.

2.5. *Audit*

Vt CPS p.2.5.

Välisauditi tulemustest teatatakse kõikidele käesolevas CP-s punktis 1.5 toodud organisatsioonidele ja avaldatakse SK koduleheküljel.

2.6. *Konfidentsiaalsus*

Vt CPS p.2.6.

3. Kliendi identifitseerimine

3.1. *Kliendi isikusamasuse kontroll*

Kliendi isikusamasust kontrollitakse vastavalt kehtestatud õigusaktidele.

3.2. *Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord*

Käesoleva CP alusel väljastatakse sertifikaate TRÜB-i poolt ID-kaardi isikustamise käigus või Digi-ID plangi tootmise käigus Kliendile moodustatud avalikele võtmetele ja ID-kaardi sertifikaatide uuendamisel Kliendi poolt moodustatud avalikele võtmetele.

3.3. *Eraldusnimi*

Vt CPS p.3.3.

Kliendi eraldusnimi koostatakse vastavalt dokumendile “Sertifikaadid Eesti Vabariigi isikutunnistusel” [2].

4. Sertifitseerimiseenuse osutamine Sertifitseerimismenetluse kord ja tähtajad

4.1. *Sertifikaaditaotluse esitamine*

Vt CPS p.4.1.

Klient täidab taotlusankeedi ID-kaardi või Digi-ID taotlemiseks ning allkirjastab selle. Allkirjastatud ID-kaardi või Digi-ID taotlus on sertifikaaditaotluse koostamise aluseks.

Täiendavat informatsiooni saab veebilehtedelt <http://www.politsei.ee> ja <http://www.sk.ee>.

4.2. *Sertifikaaditaotluse menetlemine*

ID-kaardi ja Digi-ID taotluse täpne läbivaatamise kord ja menetluse tähtajad on ära määratud vastavate õigusaktidega. Sertifikaaditaotluse menetlemisel kontrollitakse kliendi poolt esitatud andmete õigsust ja täielikkust.

4.2.1. Otsuse tegemine

Vt CPS p.4.2.1.

ID-kaardi või Digi-ID taotluse rahuldamise või mitterahuldamise otsustab PPA. Kehtivate sertifikaatidega ID-kaardi või Digi-ID taotluse rahuldamise või mitterahuldamise otsuse langetamisel lähtutakse sellest, kas kliendil on vastavalt EV õigusaktidele õigus saada ID-kaarti või Digi-ID-d.

Positiivse otsuse korral moodustab TRÜB ID-kaardi puhul ja PPA Digi-ID puhul Kliendile võtmepaarid ning koostab neile vastavad sertifikaaditaotlused digitaalset allkirja ja isikusamasuse kontrolli võimaldava sertifikaadi väljastamiseks ja saadab need SK-le.

ID-kaardile uute sertifikaatide taotluse rahuldamise või mitterahuldamise otsustab SK.

4.2.2. Sertifikaadi väljastamine

SK väljastab peale TRÜB-i või PPA poolt edastatud sertifikaaditaotluse autentsuse ja terviklikkuse kontrolli taotlusele automaatselt vastavad sertifikaadid, mis laetakse TRÜB-is ID-kaardile või PPA-s Digi-ID-le.

Kõik väljastatud sertifikaadid on aktiveerimata olekus, st nad pole kätte saadavad punktis 2.1.6 viidatud avalikus kataloogis, vaid asuvad SK infosüsteemi suletud osas asuvas sertifikaatide andmebaasis.

Kehtivate sertifikaatidega ID-kaardile uute sertifikaatide taotlemisel väljastatakse uued sertifikaadid ID-kaardile PPA või SK klienditeeninduspunktis või SK koduleheküljel olevas rakenduses.

4.2.3. ID-kaardi ja Digi-ID väljastamine, sertifikaatide aktiveerimine

ID-kaart ja Digi-ID väljastatakse kliendile PPA klienditeeninduspunktis.

Koos ID-kaardi või Digi-ID väljastamisega edastab PPA klienditeeninduspunkti ametnik ID-kaardile või Digi-ID-le laetud sertifikaadid aktiveerimisjärjekorda. ID-kaardi ja Digi-ID sertifikaadid aktiveerib SK hiljemalt 1 tunni jooksul alates ID-kaardi või Digi-ID väljastamisest.

PPA klienditeeninduspunkti või Eesti välisesinduse ametnik annab kliendile üle ID-kaardi või Digi-ID aktiveerimiskoode sisaldava turvaümbriku (PIN-koodi ümbrik).

Klient (või kliendi seadusjärgne esindaja) allkirjastab ID-kaardi või Digi-ID väljastamise akti, kinnitades ühtlasi ka tutvumist sertifikaatide kasutustingimustega [5].

ID-kaardi sertifikaatide uuendamisel aktiveeritakse sertifikaadid koheselt peale nende laadimist kiipkaardile.

4.2.4. Sertifikaadi kontroll ja tõestamine

Vt CPS p.4.2.4.

4.2.5. Sertifikaadi uuendamine

ID-kaardi aegunud või kehtetuks tunnistatud sertifikaate asendatakse uuesti genereeritud võtmepaari põhjal väljastatud sertifikaatidega.

Digi-ID sertifikaatide uuendamist ei toimu. Aegunud või tühistatud Digi-ID sertifikaadid asendatakse uue Digi-ID väljastamisega.

4.3. Sertifikaadi kehtetuks tunnistamise ja kehtivuse peatamise taotlused

Vt CPS p.4.3.

4.4. Sertifikaatide kehtivuse peatamine

Vt CPS p.4.4.

Sertifikaatide kehtivuse peatamine on võimalik ka PPA klienditeeninduspunktis.

Taotluse esitaja isikusamasus kontrollitakse vastavalt kehtivatele õigusaktidele.

Taotluse registreerimisel PPA klienditeeninduspunktis märgitakse üles taotluse esitaja isikusamasuse kontrollil kasutatud dokumendi andmed.

4.5. Sertifikaadi kehtivuse peatamise lõpetamine

Vt CPS p.4.5.

Sertifikaatide kehtivuse peatamise lõpetamine on võimalik ka PPA klienditeeninduspunktis.

Taotluse esitaja isikusamasus kontrollitakse vastavalt kehtivatele õigusaktidele.

Sertifikaadi kehtivuse peatamise lõpetamise taotlus peab sisaldama:

- omaniku ja taotluse esitaja (kui erineb omanikust) eesnime ja perekonnanime;
- omaniku ja taotluse esitaja (kui erineb omanikust) isikukoodi;
- kehtivuse peatamise lõpetamise alust.

PPA klienditeeninduspunktis taotluse registreerimisel märgitakse üles taotluse esitaja isikusamasuse kontrollil kasutatud dokumendi andmeid.

4.6. Sertifikaadi kehtetuks tunnistamine

4.6.1. Sertifikaadi kehtetuks tunnistamise volitused

Vt CPS p.4.6.1.

Sertifikaadi kehtetuks tunnistamise taotluse võib esitada PPA peale ID-kaardi või Digi-ID kehtetuks tunnistamist.

4.6.2. Sertifikaadi kehtetuks tunnistamise taotluse esitamine

Vt CPS p.4.6.2.

Sertifikaatide kehtetuks tunnistamine on võimalik ka PPA klienditeeninduspunktis. Taotluse esitaja isikusamasus kontrollitakse vastavalt kehtivatele õigusaktidele.

Sertifikaadi kehtetuks tunnistamise taotlus peab sisaldama:

- omaniku ja taotluse esitaja (kui erineb omanikust) eesnime ja perekonnanime;
- omaniku ja taotluse esitaja (kui erineb omanikust) isikukoodi;
- kehtetuks tunnistamise põhjust.

PPA klienditeeninduspunktis taotluse registreerimisel märgitakse üles taotluse esitaja isikusamasuse kontrollil kasutatud dokumendi andmeid.

4.6.3. Sertifikaadi kehtetuks tunnistamise menetlus

Vt CPS p.4.6.3.

Sertifikaatide kehtetuks tunnistamise taotluse saab esitada ka PPA klienditeeninduspunktis.

4.6.4. Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus

Vt CPS p.4.6.4.

4.7. *Protseduurid jälgitavuse tagamiseks*

Vt CPS p.4.7.

4.8. *Tegutsemine eriolukorras*

Vt CPS p.4.8.

4.9. *Sertifitseerimisteenuse osutaja töö lõpetamine*

Vt CPS p.4.9.

5. Füüsilised ja organisatsioonilised turbemeetmed

5.1. *Turbehaldus*

Vt CPS p.5.1.

5.2. *Füüsilised turbemeetmed*

5.2.1. SK füüsiline pääsukontroll

Vt CPS p.5.2.1.

5.2.2. Muud nõuded. ID-kaartide ja Digi-ID hoiustamine

ID-kaarte ja Digi-ID-sid hoiustatakse PPA klienditeeninduspunktis vastavalt kehtestatud sisemistele turvaeeskirjadele.

Asendus PIN-ümbrikke hoiustatakse PPA ja SK klienditeeninduspunktis vastavalt kehtestatud sisemistele turvaeeskirjadele.

5.3. Nõuded tööprotseduuridele

Vt CPS p.5.3.

5.4. Personali turbenõuded

Vt CPS p.5.4.

6. Tehnilised turbenõuded

6.1. Võtmehaldus

6.1.1. SK kinnitusvõtmed

Vt CPS p.6.1.1.

6.1.2. Kliendi võtmed

6.1.2.1. Kliendi võtmete moodustamine

Võtmete moodustamisel kasutatavad algoritmid, võtmepikkused ja teised parameetrid on toodud dokumendis „Sertifikaadid Eesti Vabariigi isikutunnistusel” [2].

Võtmed luuakse ID-kaardi või Digi-ID isikustamise ajal ning ID-kaardi sertifikaatide asendamisel PPA ja SK klienditeeninduspunktis ja salvestatakse kaardi vastavasse turvaalasse. Loodud võtmeid ei ole võimalik kaardist eraldada ega taastada.

Kliendi võtmed on kaitstud ainult kliendile teadaolevate PIN koodidega ehk aktiveerimiskoodidega.

6.1.2.2. Kliendi isikliku võtme ja aktiveerimiskoodide kaitse isikustamise käigus

PPA, TRÜB ja SK tagavad kliendile genereeritud kliendi isikliku võtme ning aktiveerimiskoodide konfidentsiaalsuse ja mittekasutamise kuni võtmete salvestamiseks kasutatava ID-kaardi või Digi-ID ja võtmete aktiveerimiskoodide kliendile üleandmiseni.

Aktiveerimiskoodid trükitakse ühes eksemplaris otse turvaümbrikusse, mis edastatakse avamata kliendile.

6.1.2.3. Kliendi isikliku võtme aktiveerimine

Vt CPS p.6.1.2.3.

Kiipkaart lukustub kolme vale aktiveerimiskoodi (PIN-koodi) sisestamise järel. Kiipkaardi lahtiblokeerimiseks on võimalik kasutada kliendile üleantud ID-kaardi või Digi-ID PUK-koodi.

Kiipkaart lukustub täielikult kolme vale PUK-koodi sisestamisel.

PUK-koodi kadumisel või kiipkaardi täielikul lukustumisel tuleb pöörduda PPA või SK klienditeeninduspunkti poole asendus PIN-koodi ümbriku saamiseks.

6.1.2.4. Kliendi võtmete varundamine ja deponeerimine

Klientide isiklikest võtmetest ei salvestata varukoopiaid ja neid ei deponeerita mingil moel.

6.2. Süsteemiturve

Vt CPS p.6.2.

6.3. Sertifitseerimisteenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus

Vt CPS p.6.3.

6.4. Sertifitseerimisteenuse osutamisel tekkinud andmete säilitamine ja kaitse

Vt CPS p.6.4.

7. Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid

Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid on toodud dokumendis „Sertifikaadid Eesti Vabariigi isikutunnistusel“ [2].

8. Sertifitseerimispoliitika haldus

Vt CPS p.8.

Käesolev CP ja viidatud dokumendid AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtted (CPS) [1] ning Sertifikaadid Eesti Vabariigi isikutunnistusel [2] avaldatakse SK koduleheküljel.

Isikutunnistusele ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimused [5] avaldatakse SK ja PPA koduleheküljel.

Kõik muudatused CP-s kooskõlastatakse PPA-ga ja TRÜB-iga.

9. Viidatud ja seonduvad dokumendid

Viidatud dokumendid:

- [1] AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtted (CPS)
- [2] EVS 828:2009 „Sertifikaadid Eesti Vabariigi isikutunnistusel“



- [3] Eesti Vabariigi digitaalallkirja seadus, RT 1 2000, 26, 150.
- [4] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
- [5] Isikutunnistusele ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimused

Seotud õigusaktid:

- Isikut tõendavate dokumentide seadus, RT I 1999, 25, 365
- Isikuandmete kaitse seadus RT I 2007, 24, 127