



ESTEID-kaardi sertifitseerimispoliitika

Versioon 5.0

OID: 1.3.6.1.4.1.10015.1.1

OID: 1.3.6.1.4.1.10015.1.2

25.01.2016

Nõuded Eesti Vabariigi (edaspidi EV) poolt välja antavale ID-1 vormis isikutunnistusele (edaspidi ID-kaart), elamisloakaardile (edaspidi EL-kaart) ja digitaalsele isikutunnistusele (edaspidi Digi-ID) digitaalallkirja ja digitaalse isikusamasuse kontrolli võimaldavate sertifikaatide väljastamiseks ja teenindamiseks.

Versiooni info		
Kuupäev	Versioon	Muudatused
25.01.2016	5.0	<p>Punkt 1.2 - muudetud kasutatud terminoloogiat</p> <p>Punkt 1.3 - muudetud kasutatud lühendite nimekirja.</p> <p>Punkt 1.4 - muudetud sertifitseerimispoliitika identifitseerimist</p> <p>Punkt 1.5.2 - muudetud SK registreerimiskeskuse tegevuse kirjeldust.</p> <p>Punkt 1.5.3 - muudetud PPA tegevuse kirjeldust.</p> <p>Punkt 1.5.4 - muudetud TRÜBi tegevuse kirjeldust.</p> <p>Punkt 1.6 - muudetud PPA kontaktandmed.</p> <p>Punkt 2.1.1 - muudetud SK kohustuste kirjeldust.</p> <p>Punkt 2.1.2.1 - muudetud PPA klienditeeninduspunkti kohustuste kirjeldust.</p> <p>Punkt 2.1.3 - muudetud PPA kohustuste kirjeldust.</p> <p>Punkt 2.1.4 - muudetud nõudeid kliendile.</p> <p>Punkt 2.5 - muudetud auditi kirjeldust.</p> <p>Punkt 3.1 - muudetud kliendi isikusamasuse kontrolli.</p> <p>Punkt 4.1 - muudetud sertifikaaditaotluse esitamist.</p> <p>Punkt 4.2.1 - muudetud otsuse tegemist.</p> <p>Punkt 4.4 - muudetud sertifikaatide kehtivuse peatamist.</p> <p>Punkt 4.5 - muudetud sertifikaadi kehtivuse peatamise lõpetamist.</p> <p>Punkt 4.6.2 - muudetud sertifikaadi kehtetuks tunnistamise taotluse esitamist.</p> <p>Punkt 6.1.2.1 - muudetud kliendi võtmete moodustamist.</p> <p>Punkt 9 - uuendatud viidatud ja seonduvate dokumentide nimekirja.</p> <p>Seoses sertifikaatide uuendamise ja vahetamise muudatustega on uuendatud järgmised punktid:</p> <p>Punkt 2.1.2.2 - SK klienditeeninduspunkti kohustused;</p> <p>Punkt 3.2 - Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord;</p> <p>Punkt 4.2.2 - Sertifikaadi väljastamine;</p> <p>Punkt 4.2.3 - ID-kaardi, EL-kaardi ja Digi-ID väljastamine, sertifikaatide aktiveerimine;</p> <p>Punkt 4.2.5 - Sertifikaadi uuendamine ja vahetamine.</p>
01.12.2014	4.0	<p>Parandatud dokumendi sõnastust ja vormindust.</p> <p>Täpsustatud käesoleva dokumendi sisu.</p>



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



Sisukord

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



4.3.	Sertifikaadi kehtetuks tunnistamine ja kehtivuse peatamine	14
4.4.	Sertifikaatide kehtivuse peatamine	14
4.5.	Sertifikaadi kehtivuse peatamise lõpetamine	14
4.6.	Sertifikaadi kehtetuks tunnistamine	14
4.6.1.	Sertifikaadi kehtetuks tunnistamise volitused	14
4.6.2.	Sertifikaadi kehtetuks tunnistamise taotluse esitamine	15
4.6.3.	Sertifikaadi kehtetuks tunnistamise menetlus	15
4.6.4.	Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus	15
4.7.	Protseduurid jälgitavuse tagamiseks	15
4.8.	Tegutsemise eriolukorras	15
4.9.	Sertifitseerimiseenuse osutaja töö lõpetamine	15
5.	Füüsilised ja organisatsioonilised turbemeetmed	15
5.1.	Turbehaldus	15
5.2.	Füüsilised turbemeetmed	15
5.2.1.	SK füüsiline pääsukontroll	15
5.2.2.	Muud nõuded. ID-kaartide, EL-kaartide ja Digi-ID hoiustamine	15
5.3.	Nõuded tööprotseduuridele	15
5.4.	Personali turbenõuded	16
6.	Tehnilised turbenõuded	16
6.1.	Võtmehaldus	16
6.1.1.	SK kinnitusvõtmed	16
6.1.2.	Kliendi võtmed	16
6.2.	Süsteemiturve	16
6.3.	Sertifitseerimiseenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus	17
6.4.	Sertifitseerimiseenuse osutamisel tekkinud andmete säilitamine ja kaitse	17
7.	Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid	17
8.	Sertifitseerimispoliitika haldus	17
9.	Viidatud ja seonduvad dokumendid	17

1. Sissejuhatus

1.1. Ülevaade

Käesolev dokument (edaspidi sertifitseerimispoliitika, CP) on reeglite kogum, mis määrab peamised tööpõhimõtted ja -kontseptsioonid ID-kaardile, EL-kaardile ja Digi-ID-le 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
ID-kaart	Isikutunnistus on Eesti kodaniku ja Eestis püsivalt elava Euroopa Liidu kodaniku kohustuslik isikut tõendav dokument.
EL-kaart	Elamisloakaart on Eestis kehtiva elamisloa või elamisõiguse alusel püsivalt elava välismaalase kohustuslik isikut tõendav dokument, mida väljastatakse aastast 2011.
Digi-ID	Digitaalne isikutunnistus on ID-kaardiga analoogiline kiipkaart, millega saab elektroonilises keskkonnas oma isikut tuvastada ja anda digitaalset allkirja.
E-residendi digi-ID	Digitaalne isikutunnistus, mis on väljastatud isikule, kellel puudub õigus või vajadus taotleda Eesti Vabariigi isikutunnistust või elamisloakaarti.
Dokument	ID-kaart, EL-kaart, Digi-ID või E-residendi digi-ID.
ID-1 vorm	Formaat vastavalt standardile ISO/IEC 7810.
Isikutunnistusele, elamisloakaardile ja digitaalsetele isikutunnistusele väljastatavate sertifikaatide kasutustingimused	Dokument, mis sisaldab Kliendi kohustusi ja vastutust ID-kaardi või EL-kaardi või Digi-ID-ga ning nendega seotud sertifikaatide kasutamisel. Klient peab ID-kaardi või EL-kaardi või Digi-ID väljastamisel olema tutvunud ja aktsepteerima selles dokumendis toodud tingimusi.

1.3. Kasutatud lühendid

Lühend	Definitsioon
PPA	EV Politsei- ja Piirivalveamet



TRÜB	TRÜB AG – ID-kaardi, EL-kaardi ja Digi-ID plangi tootja ning ID-kaardi ja EL-kaardi isikustaja
SK	AS Sertifitseerimiskeskus – sertifitseerimisteenuse osutaja
STO	Sertifitseerimise Registris registreeritud sertifitseerimisteenuse osutaja

1.4. Sertifitseerimispoliitika identifitseerimine

Käesoleva CP tunnuscode on **OID**:

- **ID-kaardil ja EL-kaardil 1.3.6.1.4.1.10015.1.1**
- **Digi-ID-l 1.3.6.1.4.1.10015.1.2**

OID tunnuscode lisatakse käesoleva CP alusel väljastatavasse sertifikaati.

CP tunnuscode on koostatud vastavalt järgnevale tabelile 1.

Parameeter	Viide OIDs
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 ja EL-kaardi puhul 1.2 – Digi-ID puhul

Tabel 1. CP tunnuscode koostamine

1.5. Organisatsioon ja kasutusvaldkond

1.5.1. Sertifitseerimiskeskus (SK)

Vt CPS p.1.2.1.

Sertifikaadid väljastatakse ID-kaardile, EL-kaardile või Digi-ID-le. ID-kaardi, EL-kaardi ja Digi-ID väljastamise eest vastutab PPA. PPA-l on TRÜB-ga leping ID-kaardi, EL-kaardi ja Digi-ID plankide tootmiseks, ID-kaartide ja EL-kaartide isikustamiseks ja ID-kaardile, EL-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, EL-kaartide ja Digi-ID taotluste vastuvõtmine ning ID-kaartide, EL-kaartide ja Digi-ID väljastamine toimub PPA teenindustes ning EV välisesindustes (edaspidi PPA klienditeeninduspunkt), mille täpne loetelu ja lahtiolekuajad viidatakse PPA koduleheküljel www.politsei.ee ja SK koduleheküljel www.sk.ee.

ID-kaartidega, EL-kaartidega ja Digi-ID-ga seotud sertifikaatide teenindamine (sertifikaatide, kehtivuse peatamine, kehtivuse peatamise lõpetamine, kehtetuks tunnistamine, asendus PIN-koodide määramine v.a e-residendi Digi-ID) toimub PPA ja/või SK klienditeeninduspunktides. ID-kaartidega, EL-kaartidega ja Digi-ID-ga

seotud sertifikaatide vahetamine toimub PPA klienditeeninduspunktides või avalikus andmesidevõrgus olevas rakenduses.

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, EL-kaardi ja Digi-ID-ga seotud probleemide lahendamisel.

1.5.3. PPA

PPA:

- võtab vastu ID-kaardi, EL-kaardi ja Digi-ID taotlusi ning positiivse otsuse korral vormistab tellimuse, mille edastab TRÜB-ile (v.a Digi-ID, mida isikustab PPA);
- väljastab isikustatud ID-kaardi, EL-kaardi või Digi-ID kliendile;
- isikustab Digi-ID, taotleb sellele vastavad sertifikaadid ja laeb need kaardile.

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 ja EL-kaardi tellimusi;
- toodab ID-kaardi, EL-kaardi ja Digi-ID plangi;
- isikustab ID-kaardi või EL-kaardi PPA poolt edastatud tellimuste alusel;
- moodustab kaardil ID-kaardi või EL-kaardi võtmed ning taotleb nendele vastavad sertifikaadid;
- laeb sertifikaadid ID-kaardile või EL-kaardile;
- annab isikustatud ID-kaardid ja EL-kaardid PPA-le üle;
- moodustab kaardil 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 või EL-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 isikut tõendavatel dokumentidel”.

Kliendil peab olema võimalus enne ID-kaardi või EL-kaardi ja Digi-ID väljastamist tutvuda „Isikutunnistusele, elamisloakaardile 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: info@sk.ee
<http://www.sk.ee>

Abiliin

telefon 1777, +372 677 377

Klienditeeninduspunktid

Klienditeeninduspunktide kontaktandmed on viidatud SK ja PPA kodulehekülgedel.

PPA

Pärnu mnt 139,
15060 Tallinn
Info: +372 612 3000
Faks: +372 612 3009
E-post: info@politsei.ee
<http://www.politsei.ee>

PPA abiliin ID-kaardiga, EL-kaardiga ja Digi-ID-ga seotud probleemide lahendamiseks ja SK klienditeeninduspunktide töötajate nõustamiseks igapäevaselt kella 08.00-19.00: telefon +372 612 3000.

Kontaktandmete muutumisel teavitatakse sellest kohe SK ja PPA kodulehekülgedel.

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 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 EV 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 (v.a EV välisesindus) kohustub täiendavalt:

- väljastama kliendile ID-kaardi, EL-kaardi või Digi-ID aktiveerides sinna laetud sertifikaadid;
- tagama esmase nõustamise ja abistamise ID-kaardi, EL-kaardi ja Digi-ID käsitlemisel;
- vastu võtma taotlusi ID-kaardi, EL-kaardi ja Digi-ID sertifikaatide vahetamiseks;
- vastu võtma taotlusi ID-kaardi ja EL-kaardi sertifikaatide kehtivuse peatamiseks, kehtivuse peatamise lõpetamiseks, kehtetuks tunnistamiseks ja asendus PIN-koodide määramiseks;
- vastu võtma taotlusi Digi-ID sertifikaatide kehtivuse peatamiseks, kehtivuse peatamise lõpetamiseks, kehtetuks tunnistamiseks ja asendus PIN-koodide määramiseks (v.a E-residendi digi-ID).

2.1.2.2. SK klienditeeninduspunkti kohustused

Vt CPS p.2.1.2.1.

SK klienditeeninduspunkt peab vastu võtma taotlusi:

- ID-kaardi ja EL-kaardi sertifikaatide kehtivuse peatamiseks, kehtivuse peatamise lõpetamiseks, kehtetuks tunnistamiseks ja asendus PIN-koodide määramiseks;
- Digi-ID sertifikaatide kehtivuse peatamiseks, kehtivuse peatamise lõpetamiseks, kehtetuks tunnistamiseks ja asendus PIN-koodide määramiseks (v.a E-residendi digi-ID).

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 on välja toodud vastava andmekogu pidamise põhimääruses;
- tagama, et PPA klienditeeninduspunkti töötajatel ei ole karistatust tahtlikult toimepandud kuriteo eest;
- tagama ID-kaardi, EL-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, EL-kaardi või Digi-ID taotluse esitamisel edastama PPA-le õige informatsiooni ning isikuandmete muutumise korral teatama õiged andmed PPA-le vastavalt kehtestatud õigusaktidele.

Klient ei vastuta sertifikaatide peatamise ajal tehtud toimingute eest. Juhul kui Klient sertifikaatide peatamise lõpetab, vastutab Klient ainuisikuliselt ning täies ulatuses sertifikaatidega tehtud digitaalsest isikusamasuse kontrollimisest ja antud digitaalallkirjadest tulenevate tagajärgede eest ajal, mil sertifikaadid olid peatatud olekus. Kui Kliendil on kahtlus, et Dokument on sertifikaatide peatamise ajal väljunud Kliendi kontrolli alt, peab Klient sertifikaadid kehtetuks tunnistama.

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 EV-s 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 tühistusnimekiri on kättesaadav aadressil <http://www.sk.ee/crls>

2.4.2. Avaldamise sagedus

Vt CPS p.2.4.2.

Sertifikaatide tühistusnimekirju uuendatakse ja avaldatakse regulaarselt mitte harvemini kui 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 tulemused avaldatakse SK koduleheküljel ja edastatakse STO registri vastutavale töötajale.

2.6. Konfidentsiaalsus

Vt CPS p.2.6.

3. Kliendi identifitseerimine

3.1. Kliendi isikusamasuse kontroll

Kliendi isikusamasust kontrollitakse vastavalt kehtestatud õigusaktidele ja siseselt kehtestatud turvaeeskirjadele isikusamasuse kontrollimiseks.

3.2. Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord

Käesoleva CP alusel väljastatakse sertifikaate TRÜB-i poolt ID-kaardi või EL-kaardi isikustamise käigus või Digi-ID plangi tootmise käigus Kliendile moodustatud avalikele võtmetele. Samuti väljastatakse sertifikaate ID-kaardi, EL-kaardi ja Digi-ID sertifikaatide vahetamisel. Sertifikaadid väljastatakse ainult kaardi poolt moodustatud avalikele võtmetele.

3.3. Eraldusnimi

Vt CPS p.3.3.

Kliendi eraldusnimi koostatakse vastavalt dokumendile “Sertifikaadid Eesti Vabariigi isikut tõendavatel dokumentidel” [2].

4. Sertifitseerimiseenuse osutamine. Sertifitseerimismenetluse kord ja tähtajad

4.1. Sertifikaaditaotluse esitamine

Vt CPS p.4.1.

Klient täidab taotlusankeedi ID-kaardi, EL-kaardi või Digi-ID taotlemiseks ning kinnitab selles esitatud andmete õigsust. Kinnitatud ID-kaardi, EL-kaardi või Digi-ID taotlus on sertifikaaditaotluse koostamise aluseks.

Täiendavat informatsiooni saab SK ja PPA kodulehekülgedelt.



4.2. Sertifikaaditaotluse menetlemine

ID-kaardi, EL-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 terviklikkust.

4.2.1. Otsuse tegemine

Vt CPS p.4.2.1.

ID-kaardi, EL-kaardi või Digi-ID taotluse rahuldamise või mitterahuldamise otsustab PPA.

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

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, EL-kaardile või PPA-s Digi-ID-le. Ebakorrektned sertifikaaditaotlused lükatakse tagasi ning sellest teavitatakse taotluse esitanud osapoolt.

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

ID-kaardi, EL-kaardi või Digi-ID sertifikaatide vahetamisel väljastatakse uued sertifikaadid kaardile PPA klienditeeninduspunktis või avalikus andmesidevõrgus olevas rakenduses, kui rakenduse poolt on elektrooniliselt tõendatud Kliendi tahteavaldus sertifikaatide vahetamiseks.

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

ID-kaart, EL-kaart ja Digi-ID väljastatakse kliendile PPA klienditeeninduspunktis. PPA klienditeeninduspunkti töötaja edastab ID-kaardile, EL-kaardile või Digi-ID-le laetud sertifikaatide aktiveerimistaotluse SK-le. ID-kaardi, EL-kaardi ja Digi-ID sertifikaadid aktiveerib SK kohealt ning edastab PPA klienditeeninduspunkti töötajale aktiveerimistaotluse täitmise tulemuse.

Aktiveerimistaotluse positiivse tulemuse puhul annab PPA klienditeeninduspunkti töötaja kliendile üle ID-kaardi, EL-kaardi või Digi-ID ning sertifikaatide aktiveerimiskoodi sisaldava turvaümbriku (PIN-koodi ümbrik).

Klient (või kliendi seadusjärgne esindaja) allkirjastab ID-kaardi, EL-kaardi või Digi-ID väljastamise akti, kinnitades ühtlasi ka tutvumist „Isikutunnistusele, elamisloakaardile ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimustega“[5].

ID-kaardi, EL-kaardi ja Digi-ID sertifikaatide vahetamisel aktiveeritakse sertifikaadid kohealt peale nende laadimist kiipkaardile.

4.2.4. Sertifikaadi kontroll ja tõestamine

Vt CPS p.4.2.4.

4.2.5. Sertifikaadi uuendamine ja vahetamine

ID-kaardi, EL-kaardi ja Digi-ID sertifikaate saab asendada uuesti väljastatud sertifikaatidega, st sertifikaatide vahetamisega. Uute sertifikaatide kehtivusaja lõpp on sama vahetatavate sertifikaatide kehtivusajaga.

Sertifikaate on võimalik asendada alljärgnevatel viisidel:

- sertifikaadid asendatakse kaardil olemasoleva võtmepaari põhjal;
- sertifikaadid asendatakse kaardil uuesti genereeritud võtmepaari põhjal.

Sertifikaatide vahetamist on võimalik läbi viia nii PPA klienditeeninduspunktis kui ka avalikus andmesidevõrgus olevas rakenduses.

Sertifikaatide uuendamist kehtivusaja pikendamise eesmärgil ei toimu. Aegunud sertifikaatide puhul tuleb Dokument asendada uuega.

4.3. Sertifikaadi kehtetuks tunnistamine ja kehtivuse peatamine

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 ja siseselt kehtestatud turvaeeskirjadele isikusamasuse kontrollimiseks.

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 ja siseselt kehtestatud turvaeeskirjadele isikusamasuse kontrollimiseks.

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 andmed.

4.6. Sertifikaadi kehtetuks tunnistamine

4.6.1. Sertifikaadi kehtetuks tunnistamise volitused

Sertifikaadi kehtetuks tunnistamise taotluse võib esitada PPA Isikut tõendavate dokumentide seaduse alusel [6].

4.6.2. Sertifikaadi kehtetuks tunnistamise taotluse esitamine

Sertifikaatide kehtetuks tunnistamisel lähtutakse Isikut tõendavate dokumentide seaduses [6] reguleeritud isikut tõendava dokumendi kehtetuks tunnistamise sätetest ja korrast.

4.6.3. Sertifikaadi kehtetuks tunnistamise menetlus

Sertifikaatide kehtetuks tunnistamisel lähtutakse Isikut tõendavate dokumentide seaduses [6] reguleeritud isikut tõendava dokumendi kehtetuks tunnistamise sätetest ja korrast.

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, EL-kaartide ja Digi-ID hoiustamine

ID-kaarte, EL-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 isikut tõendavatel dokumentidel” [2].

Võtmed luuakse alati Dokumendi kiibis ja 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, EL-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, EL-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. Asendus PIN-koode ei väljastata E-residendi digi-ID kaardile.

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 isikut tõendavatel dokumentidel” [2].

8. Sertifitseerimispoliitika haldus

Vt CPS p.8.

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

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

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

9. Viidatud ja seonduvad dokumendid

Viidatud dokumendid:

- [1] AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtted (CPS), avaldatud: <https://www.sk.ee/repositoorium/CPS/>;
- [2] Sertifikaadid Eesti Vabariigi isikut tõendavatel dokumentidel, AS Sertifitseerimiskeskus, avaldatud: <https://www.sk.ee/repositoorium/kasutustingimused/>;
- [3] Digitaalalkirja seadus, avaldatud: <https://www.riigiteataja.ee/akt/114032014012&leiaKehtiv>;
- [4] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, <https://www.ietf.org/rfc/rfc2527.txt>;
- [5] Isikutunnistusele, elamisloakaardile ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimused, avaldatud: <https://www.sk.ee/repositoorium/kasutustingimused/>;
- [6] Isikutõendavate dokumentide seadus, avaldatud: <https://www.riigiteataja.ee/akt/123032015016&leiaKehtiv>;

Seotud õigusaktid:

- Isikuandmete kaitse seadus, avaldatud: <https://www.riigiteataja.ee/akt/112072014051&leiaKehtiv>.