



## ESTEID-kaardi sertifitseerimispoliitika

Versioon 4.0  
OID: 1.3.6.1.4.1.10015.1.1.4  
OID: 1.3.6.1.4.1.10015.1.2.4  
01.12.2014

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
01.12.2014	4.0	Parandatud dokumendi sõnastust ja vormindust. Täpsustatud käesoleva dokumendi sisu. Punktis 1.2 - lisatud uued mõisted E-residendi digi-ID ja ID-1 vorm. Punktis 1.6 - muudetud SK ja PPA kontaktandmed. Punktis 2.1.2 ja 2.1.3 - muudetud registreerimiskeskuse ja PPA kohustusi. Punktis 2.4.2 - muudetud tühistusnimekirjade avaldamise sagedust. Punktis 4.6.1 - muudetud sertifikaadi kehtetuks tunnistamise volitusi. Punktis 6.1.2.1 - muudetud kliendi võtmete moodustamise kirjeldust. Punktis 6.1.2.3 - täiendatud kliendi isikliku võtme aktiveerimise reegleid.
01.09.2012	3.3	Lisatud 2011. aasta ID-kaardi ja EL-kaardi sertifikaatide vahetamine. Punkt 1.2 - täiendatud terminoloogiat. Punkt 2.1.2 – täiendatud registreerimiskeskuse kohustusi. Punkt 4.2.5 – muudetud sertifikaatide uuendamist ja vahetamist.
01.01.2011	3.2	Lisatud uus dokument – elamislokaart ja sellega seotud toimingud. Punkt 4.2.1 – täpsustatud Digi-ID sertifikaaditaotluste esitamist. Punkt 4.2.3 – muudetud sertifikaatide aktiveerimist, sertifikaadid aktiveeritakse kohe kliendi juuresolekul. Punkt 4.2.5 – täpsustatud sertifikaatide uuendamist ning toimingute lubatust erinevate dokumentide korral. Punkt 6.1.2.1 – täpsustatud kliendi võtmete loomist.
01.10.2010	3.1	Lisatud Digitaalsele isikutunnistusele kehtestatud nõuded ning dokumendile omistatud 2 OID väärtust.
01.01.2010	2.2	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 .....	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.....	10
2.1.3.	PPA kohustused .....	10
2.1.4.	Nõuded kliendile.....	10
2.1.5.	Nõuded huvitatud isikule.....	10
2.1.6.	Nõuded kataloogiteenusele .....	11
2.2.	Vastutus .....	11
2.2.1.	SK vastutus.....	11
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 .....	12
2.4.1.	SK informatsiooni avaldamine .....	12
2.4.2.	Avaldamise sagedus .....	12
2.4.3.	Juurdepääsureeglid .....	12
2.4.4.	Kataloogiteenus .....	12
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 .....	13
3.3.	Eraldusnimi .....	13
4.	Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtjad .....	13
4.1.	Sertifikaaditaotluse esitamine .....	13
4.2.	Sertifikaaditaotluse menetlemine .....	13
4.2.1.	Otsuse tegemine.....	13
4.2.2.	Sertifikaadi väljastamine.....	14
4.2.3.	ID-kaardi, EL-kaardi ja Digi-ID väljastamine, sertifikaatide aktiveerimine.....	14
4.2.4.	Sertifikaadi kontroll ja tõestamine .....	14



---

4.2.5.	Sertifikaadi uuendamine ja vahetamine.....	14
4.3.	Sertifikaadi kehtetuks tunnistamine ja kehtivuse peatamine.....	15
4.4.	Sertifikaatide kehtivuse peatamine .....	15
4.5.	Sertifikaadi kehtivuse peatamise lõpetamine .....	15
4.6.	Sertifikaadi kehtetuks tunnistamine .....	15
4.6.1.	Sertifikaadi kehtetuks tunnistamise volitused.....	15
4.6.2.	Sertifikaadi kehtetuks tunnistamise taotluse esitamine.....	15
4.6.3.	Sertifikaadi kehtetuks tunnistamise menetlus.....	16
4.6.4.	Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus.....	16
4.7.	Protseduurid jälgitavuse tagamiseks .....	16
4.8.	Tegutsemise eriolukorras.....	16
4.9.	Sertifitseerimise osutaja töö lõpetamine.....	16
5.	Füüsilised ja organisatsioonilised turbemeetmed .....	16
5.1.	Turbehaldus .....	16
5.2.	Füüsilised turbemeetmed .....	16
5.2.1.	SK füüsiline pääsukontroll .....	16
5.2.2.	Muud nõuded. ID-kaartide, EL-kaartide ja Digi-ID hoiustamine .....	16
5.3.	Nõuded tööprotseduuridele.....	16
5.4.	Personali turbenõuded.....	17
6.	Tehnilised turbenõuded .....	17
6.1.	Võtmehaldus .....	17
6.1.1.	SK kinnitusvõtmed.....	17
6.1.2.	Kliendi võtmed .....	17
6.2.	Süsteemiturve .....	18
6.3.	Sertifitseerimise osutamiseks kasutatavate tehniliste vahendite kirjeldus.....	18
6.4.	Sertifitseerimise osutamisel tekkinud andmete säilitamine ja kaitse .....	18
7.	Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid.....	18
8.	Sertifitseerimispoliitika haldus.....	18
9.	Viidatud ja seonduvad dokumendid .....	18

## 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 toodud.

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.
ID-1 vorm	Formaat vastavalt standardile ISO/IEC 7810.
Isikutunnistusele, elamisloakaardile digitaalsele 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
SM	EV Siseministeerium
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 1.3.6.1.4.1.10015.1.1.4**
- **Digi-ID-l 1.3.6.1.4.1.10015.1.2.4**

OID tunnuscode lisatakse käesoleva CP alusel väljastatavasse sertifikaati.

CP tunnuscode 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 ja EL-kaardi puhul 1.2 – Digi-ID puhul
CP versiooni tunnus	4

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 prefektuuride kodakondsus- ja migratsioonibüroode teenindustes ning EV välisesindustes (edaspidi PPA klienditeeninduspunkt), mille täpne loetelu ja lahtiolekuajad viidatakse PPA koduleheküljel [www.politsei.ee](http://www.politsei.ee) ja SK koduleheküljel [www.sk.ee](http://www.sk.ee).

ID-kaartidega, EL-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 protseduurireegleid, 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 ja EL-kaardi tellimusi ja edastab neid TRÜB-ile;
- edastab ID-kaarte ja EL-kaarte klienditeeninduspunktidele;
- väljastab isikustatud ID-kaardi või EL-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 ja EL-kaardi tellimusi;
- isikustab ID-kaardi või EL-kaardi;
- moodustab ID-kaardi võtmed 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.
- toodab ID-kaardi, EL-kaardi ja 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 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 kodakondsus- ja migratsiooniosakond

Pärnu mnt 139,  
15060 Tallinn  
Info: +372 612 3000  
Faks: +372 612 3009  
E-post: [teenindus@politsei.ee](mailto:teenindus@politsei.ee)

PPA abiliin ID-kaardiga, EL-kaardiga ja Digi-ID-ga seotud probleemide lahendamiseks ja SK klienditeeninduspunktide töötajate nõustamiseks tööpäevadel kella 09.00-17.00: telefon +372 612 3000.

Kontaktandmete muutumisel teavitatakse sellest koheselt 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](mailto: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:

- sertifitseerimisteenus osutamine on kooskõlas AS Sertifitseerimiskeskuse sertifitseerimispõhimõtetega;
- sertifitseerimisteenus 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 sertifitseerimisteenus 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 sertifitseerimisteenus 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, EL-kaardi või Digi-ID aktiveerides sinna laetud sertifikaadid;
- tagama esmase nõustamise ja abistamise ID-kaardi, EL-kaardi ja Digi-ID käsitlemisel;
- vastu võtma kliendi taotlusi Digi-ID (v.a E-residendi digi-ID) asendus PIN-koodide määramiseks;
- vastu võtma taotlusi ID-kaardi ja EL-kaardi sertifikaatide vahetamiseks.

### 2.1.2.2. SK klienditeeninduspunkti kohustused

Vt CPS p.2.1.2.1.

SK klienditeeninduspunkt peab vastu võtma taotlusi:

- Kuni 2010. aasta lõpuni väljastatud ID-kaardi sertifikaatide uuendamiseks ja vahetamiseks;
- ID-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);
- EL-kaardi sertifikaatide kehtivuse peatamiseks, kehtivuse peatamise lõpetamiseks ja kehtetuks tunnistamiseks ja asendus PIN-koodide määramiseks.

### 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 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.

## 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 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 või EL-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 isikut tõendavatel dokumentidel" [2].

## **4. Sertifitseerimisteenuse 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 allkirjastab selle. Allkirjastatud 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 täielikkust.

#### **4.2.1. Otsuse tegemine**

Vt CPS p.4.2.1.

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

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

Digi-ID positiivse otsuse korral koostab PPA Digi-ID-l olevale võtmepaarile vastavad sertifikaaditaotlused digitaalset allkirja ja isikusamasuse kontrolli võimaldava sertifikaadi väljastamiseks ja saadab need SK-le.

ID-kaardile, EL-kaardile või Digi-ID-le 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, EL-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, 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 koheselt 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 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 ja vahetamine

ID-kaardi kehtivaid või aegunud sertifikaate saab asendada uuesti genereeritud võtmepaari põhjal väljastatud sertifikaatidega.

Juhul, kui sertifikaadid asendatakse kaardil kasutaja seni kehtinud sertifikaatide alusel kehtivusaja pikendamise eesmärgil, on tegemist uuendamisega.

Juhul, kui sertifikaadid asendatakse kaardil PPA või SK klienditeeninduspunkti töötaja poolt, on tegemist sertifikaatide vahetamisega kaardil.

Uuendada saab sertifikaate ainult ID-kaartidel, mis on väljastatud kuni 31.12.2006. EL-kaardi ja Digi-ID sertifikaatide uuendamist ei toimu.

Kehtetuks tunnistatud ja kaardi kehtivusajaga võrdselt kehtivaid sertifikaate ei saa uuendada. 2007. aastast kuni 2011. aasta lõpuni välja antud ID-kaardi ja EL-kaardi sertifikaate saab vahetada. Digi-ID ja alates 2012. aastal välja antavate EL-kaartide ja ID-kaartide kehtetuks tunnistatud sertifikaadid asendatakse uue Digi-ID, EL-kaardi või ID-kaardi väljastamisega.

---

### **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.

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 andmed.

### **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 Isikut tõendavate dokumentide seaduse alusel [6].

#### **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, 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 Dokumendi kiibis isikustamise ajal kasutades kiibi võtme genereerimise funktsionaalsust ning ID-kaardi sertifikaatide uuendamisel PPA või SK klienditeeninduspunktis või SK koduleheküljel olevas rakenduses ning uute sertifikaatide laadimisel kaardile. 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)
- [2] Sertifikaadid Eesti Vabariigi isikut tõendavatel dokumentidel
- [3] Digitaalallkirja seadus, <https://www.riigiteataja.ee/akt/114032014012> (Redaktsiooni jõustumise kp 01.07.2014)
- [4] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
- [5] Isikutunnistusele, elamisloakaardile ja digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimused
- [6] Isikutõendavate dokumentide seadus, <https://www.riigiteataja.ee/akt/121032014011> (Redaktsiooni jõustumise kp 01.05.2014)

Seotud õigusaktid:



- 
- Isikuandmete kaitse seadus, <https://www.riigiteataja.ee/akt/114032014031> (Redaktsiooni jõustumise kp 01.07.2014)