



# AS Sertifitseerimiskeskus

## Mobiil-ID vormis digitaalse isikutunnistuse sertifitseerimispoliitika

Versioon 3.0  
OID: 1.3.6.1.4.1.10015.1.3.3  
Kehtiv alates 01.01.2016

Versiooni info		
Kuupäev	Versioon	Muudatused
01.01.2016	3.0	Täiendatud punkti 1.2 kasutatud terminoloogia. Muudetud punkti 1.5 organisatsioon ja kasutusvaldkond. Muudetud punkti 1.6 PPA kontaktandmed. Muudetud punkti 2.1 kohustused ja nõuded. Täiendatud punkti 2.4.4 kataloogiteenus. Muudetud punkti 3.1 kliendi isikusamasuse kontroll. Muudetud punkti 3.3 eraldusnimi. Muudetud punkti 4.1 sertifikaaditaotluse esitamine. Uuendatud punkti 4.2.4 sertifikaadi uuendamine. Täiendatud punkti 4.4 sertifikaatide kehtivuse peatamine. Muudetud punkti 4.5 sertifikaadi kehtivuse peatamise lõpetamine. Muudetud punkti 4.6 sertifikaadi kehtetuks tunnistamine. Uuendatud punkti 9 viidatud ja seonduvad dokumendid.
01.01.2015	2.0	Muudatuste eesmärk on viia käesolev sertifitseerimispoliitika kooskõlla isikut tõendavate dokumentide seaduse muudatustega (RT I, 29.10.2014, 6), millega muudetakse mobiil-ID väljastamise nõudeid ja tingimusi.
01.02.2011	1.1	Lõplik versioon
11.01.2011	0.1	Mustand

Nõuded Politsei- ja Piirivalveamet (edaspidi PPA) poolt välja antavale Mobiil-ID vormis digitaalsele isikutunnistusele (edaspidi Mobiil-ID) digitaalse isikusamasuse kontrolli võimaldavate sertifikaatide väljastamiseks ja teenindamiseks.

1. Sissejuhatus.....	4
1.1. Ülevaade .....	4
1.2. Kasutatud terminoloogia.....	4
1.3. Kasutatud lühendid .....	4
1.4. Sertifitseerimispoliitika identifitseerimine .....	5
1.5. Organisatsioon ja kasutusvaldkond .....	5
1.5.1. Sertifitseerimiskeskus (SK) .....	5
1.5.2. Registreerimiskeskus .....	5
1.5.3. PPA .....	6
1.5.4. Kasutaja .....	6
1.5.5. Sertifikaatide kasutusvaldkond .....	6
1.6. Kontaktandmed .....	7



2.	Üldtingimused.....	8
2.1.	Kohustused ja nõuded.....	8
2.1.1.	SK kohustused.....	8
2.1.2.	PPA kohustused.....	8
2.1.3.	MO kohustused.....	8
2.1.4.	Registreerimiskeskuse kohustused.....	9
2.1.5.	Nõuded kliendile.....	9
2.1.6.	Nõuded huvitatud isikule.....	10
2.1.7.	Nõuded kataloogiteenusele.....	10
2.2.	Vastutus.....	10
2.2.1.	SK vastutus.....	10
2.2.2.	Registreerimiskeskuse vastutus.....	10
2.2.3.	MO vastutus.....	11
2.2.4.	PPA vastutus.....	11
2.2.5.	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.	Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtjad.....	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.	Sertifikaadi kontroll ja tõestamine.....	13
4.2.4.	Sertifikaadi uuendamine.....	13
4.3.	Sertifikaadi kehtivuse peatamise ja kehtetuks tunnistamise taotlused.....	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.	Sertifitseerimisteenuse 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. Mobiil-ID SIM kaartide hoiustamine.....	16
5.3.	Nõuded tööprotseduuridele.....	16



---

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.....	17
6.3. Sertifitseerimisteenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus .....	17
6.4. Sertifitseerimisteenuse 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 CP) on reeglite kogum, mis määrab ära nõuded Mobiil-ID SIM kaardiga seotud sertifikaatide väljastamiseks ja teenindamiseks vajaliku sertifitseerimisteenuse osutamiseks.

Käesolev CP rajaneb dokumendile „AS Sertifitseerimiskeskus 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 vastuolu korral tuleb ülimuslikuks pidada käesolevas CP-s toodut.

Käesolev CP laieneb ainult AS-i Sertifitseerimiskeskus poolt väljastatud Mobiil-ID vormis digitaalse isikutunnistuse sertifikaatidele.

Käesoleva CP koostamisel on kasutatud IETFi (*Internet Engineering Task Force*) soovituslikku dokumenti RFC 2527 [2].

### 1.2. Kasutatud terminoloogia

Vt CPS p.10.

Termin	Definitsioon
Klienditeeninduspunkt	Käesoleva CP alusel toimiv mobiilioperaatori klienditeeninduspunkt, mis on volitatud Mobiil-ID-ga seotud teenuste osutamiseks, vt punkt 1.5.2.1.
Mobiil-ID	Politsei- ja Piirivalveameti poolt välja antav digitaalne isikutunnistus, mille digitaalset tuvastamist võimaldavad sertifikaadid ja digitaalset allkirjastamist võimaldavad sertifikaadid on seotud mobiiltelefoni SIM-kaardiga.
Mobiil-ID SIM kaart	Mobiiltelefoni SIM kaart, mis võimaldab lisaks tavapärase mobiilsideteenuse kasutamisele ka Mobiil-ID teenuse kasutamist ja millega seotakse kliendi isikuandmed.
Mobiil-ID teenus	Mobiilioperaatori poolt pakutav teenus, mis võimaldab kliendil elektroonilises keskkonnas digitaalset isikusamasuse kontrollimist ja digitaalset allkirjastamist.
Sertifikaaditaotlus	PPA veebipõhises taotluskeskkonnas digitaalselt allkirjastatav avaldus Mobiil-ID sertifikaatide saamiseks.
Turvaala	Kraabitav ala Mobiil-ID SIM kaardi ümbrisel, mille all asuvad Mobiil-ID aktiveerimiskoodid (PIN-koodid).

### 1.3. Kasutatud lühendid

Vt CPS p.11.

Lühend	Definitsioon
--------	--------------



Lühend	Definitsioon
MO	Elektroonilise side ettevõtja, kes osutab mobiilsideteenust ning Mobiil-ID teenust ning kellega on sõlmitud vastavad lepingud Mobiil-ID SIM kaardi väljastamiseks ja Mobiil-ID sertifikaatide kehtivuse peatamiseks.
PPA	Politsei- ja Piirivalveamet, Mobiil-ID väljaandja.
SK	AS Sertifitseerimiskeskus – STO.
STO	Sertifitseerimise Registris registreeritud sertifitseerimisteenuse osutaja.

## 1.4. Sertifitseerimispoliitika identifitseerimine

Käesoleva CP tunnuskoode on OID: 1.3.6.1.4.1.10015.1.3.3  
CP tunnuskoode on koostatud vastavalt järgnevale tabelile.

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	1.3
CP versiooni tunnus	3

Tabel 1. CP tunnuskoode koostamine

## 1.5. Organisatsioon ja kasutusvaldkond

### 1.5.1. Sertifitseerimiskeskus (SK)

Vt CPS p.1.2.1.

PPA ja SK vahelise lepinguga osutab SK registreeritud STO-na sertifitseerimisteenust. Mobiil-ID väljaandmise eest vastutab PPA. SK-l on leping MO-ga Mobiil-ID SIM kaartide väljastamiseks. SK on lepinguliselt delegeerinud MO-le punktides 1.5.2.1 ja 1.5.2.3 kirjeldatud kohustused.

### 1.5.2. Registreerimiskeskus

#### 1.5.2.1. Klienditeeninduspunktid

Vt CPS p.1.2.2.1.

Mobiil-ID SIM kaartide väljastamine ja teenindamine ning Mobiil-ID sertifikaatide teenindamine ja Mobiil-ID SIM kaardiga seotud telefoni numbri muutmise toimub MO volitatud teeninduspunktides (edaspidi klienditeeninduspunkt), mille täpsele loetelule ja lahtiolekuaegadele on viidatud SK koduleheküljel <http://www.sk.ee> ja MO-de kodulehekülgedel.

MO tagab turvalisuse enda kohustuste täitmisel sisemiste protseduuridega.

---

### 1.5.2.2. SK klienditeeninduspunkt

Vt CPS p.1.2.2.1.

SK klienditeeninduspunkt võtab vastu digitaalselt allkirjastatud avaldusi Mobiil-ID sertifikaatide kehtivuse peatamiseks ja kehtivuse peatatuse lõpetamiseks.

### 1.5.2.3. Abiliin

MO-d esindav telefoniteenindus, mis võtab ööpäevaringselt klientidelt ning teistelt osapooltelt vastu taotlusi sertifikaatide kehtivuse peatamiseks, eelnevalt tuvastades isiku vastavalt isikusamasuse kontrolli protseduuridele (vt punkt 3.1).

Abiliin annab vajadusel täiendavalt infot ja teostab toiminguid Mobiil-ID teenusega seotud probleemide lahendamisel.

Informatsiooni abiliini ja tema kontaktandmete kohta esitatakse MO koduleheküljel. Samas on toodud ära ka juhised abiliini poole pöördumiseks.

### 1.5.3. PPA

PPA

- Võtab vastu Mobiil-ID sertifikaaditaotlused, teeb otsuse sertifikaatide väljaandmiseks ja edastab sertifikaaditaotluse SK-le;
- Võtab vastu Mobiil-ID sertifikaadi kehtetuks tunnistamise taotlused, otsustab sertifikaatide kehtetuks tunnistamise ja edastab taotluse SK-le;
- Teeb otsuse sertifikaatide uuendamise osas ja edastab kirjaliku taotluse SK-le.

PPA tagab turvalisuse enda kohustuste täitmisel sisemiste protseduuridega.

### 1.5.4. Kasutaja

#### 1.5.4.1. Klient

Vt CPS p.1.2.3.1.

Klient on füüsiline isik, kellele väljastatakse avaliku teenusena Mobiil-ID SIM kaardiga seotud sertifikaate, kui tal on selleks seadusejärgne õigus. Igal Kliendil võib olla kehtivas staatuses üks Mobiil-ID SIM kaart koos sellega seotud sertifikaatidega.

Kliendi eraldusnimi sertifikaadis koostatakse vastavalt sertifikaadiprofiilile, mis on toodud dokumendis „Sertifikaadid Eesti Vabariigi isikut tõendavatel dokumentidel“ [7].

Klient peab tutvuma ja nõustuma enne Mobiil-ID sertifikaaditaotluse esitamist veebipõhises taotluskeskkonnas „Mobiil-ID vormis digitaalse isikutunnistuse väljastatavate sertifikaatide kasutustingimustega“ [3].

#### 1.5.4.2. Huvitatud isik

Vt CPS p.1.2.3.2.

### 1.5.5. 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 digitaalallkirja seaduse [6] 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](mailto:info@sk.ee)  
<http://www.sk.ee>

### **Abiliin**

Abiliini kohustusi täidab MO telefoniteenindus. Abiliini kontaktandmed on viidatud SK koduleheküljel <http://www.sk.ee> ja MO koduleheküljel.

### **MO**

MO kontaktandmed on viidatud SK koduleheküljel <http://www.sk.ee>. Kontaktandmete muutumisel on MO kohustatud sellest kohe teavitama oma koduleheküljel ja informeerima sellest muutmistest kohe ka SK-d.

### **PPA**

Pärnu mnt 139,  
15060 Tallinn  
Infotelefon +372 612 3000  
Faks +372 612 3009  
E-post: [info@politsei.ee](mailto:info@politsei.ee)  
<http://www.politsei.ee>

PPA abiliin Mobiil-ID taotlemise ja menetlemisega seotud probleemide lahendamiseks ja klienditeeninduspunktide töötajate nõustamiseks on avatud tööpäevadel kella 08.00 - 19.00: telefon +372 612 3000.

### **Klienditeeninduspunktid**

Klienditeeninduspunktide nimekiri ja kontaktandmed on viidatud SK koduleheküljel <http://www.sk.ee> ja MO koduleheküljel. Kontaktandmete muutumisel on MO kohustatud sellest kohe teavitama oma koduleheküljel.

## 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 SK sertifitseerimispõhimõtetega;
- sertifitseerimisteenuse osutamine on kooskõlas käesoleva CPga.

SK kohustub täiendavalt:

- vastu võtma ja registreerima MO poolt esitatud Mobiil-ID SIM kaardi väljastamise teatise ja registreerima MO poolt väljastatud Mobiil-ID SIM kaardiga seotud avalikud võtmed;
- vastu võtma ja registreerima PPA poolt esitatud sertifikaaditaotlusi ning väljastama neile vastavaid sertifikaate;
- vastu võtma, registreerima ja töötleva MO poolt esitatud sertifikaadi kehtivuse peatamise taotlusi ja PPA poolt esitatud kehtetuks tunnistamise taotlusi ning MO poolt esitatud Mobiil-ID SIM kaardiga seotud telefoninumbri muutmise taotlusi;
- vastu võtma ja registreerima PPA poolt kirjalikult esitatud sertifikaadi uuendamise taotlusi ning uuendama neile vastavalt sertifikaate.

#### 2.1.2. PPA kohustused

PPA kohustub:

- vastu võtma kliendi digitaalallkirjastatud taotlusi Mobiil-ID SIM kaardiga seotud sertifikaatide väljastamiseks;
- vastu võtma kliendi digitaalallkirjastatud taotlusi Mobiil-ID SIM kaardiga seotud sertifikaatide kehtetuks tunnistamiseks;
- vastu võtma SK-lt MO taotlusi Mobiil-ID SIM kaardiga seotud sertifikaatide kehtetuks tunnistamiseks;
- vastu võtma otsuseid sertifikaatide uuendamiseks;
- tagama kliendile kättesaadavuse teenust puudutavale infomaterjalile.

PPA on kohustatud kontrollima esitatud taotluste õigsust ja terviklikkust.

PPA peab kõikide toimingute teostamisel kontrollima taotluse esitaja isikusamasust ja volitusi toimingu teostamiseks vastavalt kehtestatud õigusaktidele.

PPA kohustub täiendavalt:

- sertifitseerimissüsteemiga seotud infosüsteemi (sealhulgas veebipõhine taotluskeskkond) osas järgima käesolevas CP-s toodud nõudeid;
- tagama, et töötajatel, kes on seotud sertifitseerimisteenust puudutava informatsiooniga, ei ole karistatust tahtlikult toimepandud kuriteo eest;
- tagama Mobiil-ID-d puudutava informatsiooni kättesaadavuse avalikus andmesidevõrgus aadressil <http://www.politsei.ee>;
- tagama turvalisuse enda kohustuste täitmisel sisemiste protseduuridega.

#### 2.1.3. MO kohustused



MO kohustub:

- Mobiil-ID teenuse osutamise seotud infosüsteemi osas järgima käesolevas CP-s toodud nõudeid;
- tagama turvalisuse enda kohustuste täitmisel sisemiste protseduuridega. MO on vastutav kõikide Mobiil-ID SIM kaartide tootmisega seotud operatsioonide ja protseduuride täitmise eest, sealhulgas Mobiil-ID SIM kaardi turvalise võtme genereerimise eest;
- tagama, et töötajatel, kes võtavad vastu Mobiil-ID SIM kaardi ja Mobiil-ID sertifikaatidega seotud taotlusi (kehtivuse peatamise taotlused) ja/või on seotud sertifitseerimisteenust puudutava informatsiooniga, ei ole karistatust tahtlikult toimepandud kuriteo eest;
- tagama Mobiil-ID teenust puudutava informatsiooni kättesaadavuse avalikus andmesidevõrgus.

## 2.1.4. Registreerimiskeskuse kohustused

### 2.1.4.1.MO klienditeeninduspunkti kohustused

Vt CPS p.2.1.2.1.

MO klienditeeninduspunkt peab vastu võtma taotlusi:

- Mobiil-ID SIM kaardi väljastamiseks;
- Mobiil-ID teenuse peatamiseks ja sulgemiseks;
- sertifikaatide kehtivuse peatamiseks;
- Mobiil-ID SIM kaardiga seotud telefoni numbri muudatuseks.

MO klienditeeninduspunkt kohustub täiendavalt:

- edastama SK-le väljastatud Mobiil-ID SIM kaardi taotluse;
- tagama esmase nõustamise Mobiil-ID SIM kaardi käsitlemisel, Mobiil-ID taotlemisel veebipõhises taotluskeskkonnas ning Mobiil-ID teenust toetavate e-teenuste kasutamisel;
- ette valmistama ja tagama kliendile kättesaadavuse teenust puudutavale infomaterjalile.

MO on kohustatud kontrollima esitatud taotluste õigsust ja terviklikkust.

MO peab kõikide toimingute teostamisel kontrollima taotluse esitaja isikusamasust ja volitusi toimingu teostamiseks vastavalt kehtestatud õigusaktidele ja sisemistele turbeprotseduuridele.

### 2.1.4.2.MO abiliini kohustused

Vt CPS p.2.1.2.2.

### 2.1.4.3.SK klienditeeninduspunkti kohustused

Vt CPS p.2.1.2.1.

SK klienditeeninduspunkt peab vastu võtma digitaalselt allkirjastatud taotlusi:

- Mobiil-ID sertifikaatide kehtivuse peatamiseks ja kehtivuse peatamise lõpetamiseks.

## 2.1.5. Nõuded kliendile

Vt CPS p.2.1.3.

Klient on kohustatud:

- Mobiil-ID SIM kaardi taotluse esitamisel edastama MO-le õiged isikuandmed;
- Mobiil-ID sertifikaaditaotluse esitamisel edastama PPA-le õiged isikuandmed;
- Isikuandmete muutumise korral PPA-d muutustest teavitama vastavalt kehtestatud õigusaktidele;
- Teavitama MO-d Mobiil-ID kasutamiskõlbmatuks muutmisest, kaotsi minekust või hävimisest vastavalt kehtestatud õigusaktidele.

Sertifikaati kantud isikuandmete muutumise korral on klient Mobiil-ID teenuse kasutamise jätkamiseks kohustatud taotlema uue Mobiil-ID SIM kaardi ja uued Mobiil-ID sertifikaadid.

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 digitaalallkirja(de)st tulenevate tagajärgede eest ajal, mil mobiilsideteenus ja/või sertifikaadid olid peatatud olekus. Kui Kliendil on kahtlus, et Dokument on mobiilsideteenuse ja/või sertifikaatide peatamise ajal väljunud Kliendi kontrolli alt, peab Klient sertifikaadid kehtetuks tunnistama.

#### 2.1.6. Nõuded huvitatud isikule

Vt CPS p.2.1.4.

#### 2.1.7. 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 toodud kohustuste täitmise eest Eesti Vabariigis kehtivates õigusaktides nõutud piirides.

### 2.2.2. Registreerimiskeskuse vastutus

#### 2.2.2.1.MO klienditeeninduspunkti vastutus

Vt CPS p.2.2.2.1.

MO vastutab oma volitatud klienditeeninduspunktide kõigi käesoleva CP punktis 2.1.4.1 toodud kohustuste täitmise eest.

#### 2.2.2.2.MO abiliini vastutus

Vt CPS p.2.2.2.2.



---

MO vastutab oma abiliini kõigi käesoleva CP punktis 2.1.4.2 toodud kohustuste täitmise eest.

#### 2.2.2.3. SK klienditeeninduspunkti vastutus

Vt CPS p.2.2.2.2.

SK vastutab oma klienditeeninduspunkti kõigi käesoleva CP punktis 2.1.4.3 toodud kohustuste täitmise eest.

#### 2.2.3. MO vastutus

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

#### 2.2.4. PPA vastutus

PPA vastutab kõigi käesoleva CP punktis 2.1.2 toodud ja teiste käesolevas CP-s toodud PPA kohustuste täitmise eest.

#### 2.2.5. 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.

## **2.6. Konfidentsiaalsus**

Vt CPS p.2.6.

# 3. Kliendi identifitseerimine

## **3.1. Kliendi isikusamasuse kontroll**

PPA teostab kliendi isikusamasuse kontrolli vastavalt kehtestatud õigusaktidele ja siseselt kehtestatud asjaomastele turvaeeskirjadele.

MO teostab kliendi isikusamasuse kontrolli vastavalt kehtestatud õigusaktidele ja siseselt kehtestatud asjaomastele turvaeeskirjadele.

SK teostab kliendi isikusamasuse vastavalt kehtivatele õigusaktidele ja siseselt kehtestatud asjaomastele turvaeeskirjadele.

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

Käesoleva CP alusel väljastatakse sertifikaate ainult MO poolt Kliendile moodustatud avalikele võtmetele.

## **3.3. Eraldusnimi**

Vt CPS p.3.3.

Kliendi eraldusnimi koostatakse vastavalt dokumendile „Sertifikaadid Eesti Vabariigi isikut tõendavatel dokumentidel“ [7].

SK tagab Kliendi eraldusnime kombinatsiooni unikaalsuse kliendi kohta.

# 4. Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtajad.

Käesolevas peatükis on esitatud sertifikaaditaotluse menetlemise kord ja tähtajad.

## **4.1. Sertifikaaditaotluse esitamine**

Vt CPS p.4.1.

Sertifikaaditaotluste esitamine on võimalik ainult PPA veebipõhises taotluskeskkonnas.

Klient kinnitab PPA veebipõhises taotluskeskkonnas Mobiil-ID taotlusankeedil esitatud andmete õigsust ning allkirjastab selle digitaalselt. Allkirjastatud Mobiil-ID taotlus on käsitletav sertifikaaditaotlusena. Sertifikaaditaotluse esitamisele eelneb elektrooniline isikusamasuse kontrollimine.

Sertifikaaditaotluse sisu ja esitamise kord peab olema kooskõlas digitaalallkirja seadusega [6].

Sertifikaaditaotluse esitamisel klient tutvub ja nõustub „Mobiil-ID vormis digitaalse isikutunnistusele väljastatavate sertifikaatide kasutustingimustega“ [3].

Täiendavat informatsiooni saab PPA veebilehelt <http://www.politsei.ee>.

## **4.2. Sertifikaaditaotluse menetlemine**

Mobiil-ID taotluse täpne läbivaatamise kord ja menetluse tähtjad 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.

Mobiil-ID sertifikaaditaotluse rahuldamise või mitterahuldamise otsustab PPA. Sertifikaaditaotluse rahuldamise või mitterahuldamise otsuse langetamisel lähtutakse isikusamasuse kontrolli tulemustest, esitatud andmete õigsusest ja sellest, kas kliendil on vastavalt Eesti Vabariigi õigusaktidele õigus saada Mobiil-ID.

Positiivse otsuse puhul saadab PPA SK-le sertifikaaditaotluse digitaalset allkirjastamist ja isikusamasuse kontrolli võimaldavate sertifikaatide väljastamiseks.

Sertifikaaditaotluse läbivaatamisel rakendatakse automatiseeritud kontrolli. Kliendi teavitamine otsusest toimub PPA veebipõhises taotluskeskkonnas.

### **4.2.2. Sertifikaadi väljastamine**

Mobiil-ID SIM kaardi tootja genereerib kaardile võtmepaari isiklikud võtmed ja edastab avalikud võtmed MO-le. MO edastab Mobiil-ID SIM kaardiga seotud avalikud võtmed SK-le. MO väljastab Mobiil-ID SIM kaardi kliendile ja edastab väljastatud Mobiil-ID SIM kaardi taotluse SK-le. Klient esitab PPA veebikeskkonnas sertifikaaditaotluse. SK väljastab peale PPA poolt edastatud sertifikaaditaotluse andmete autentsuse ja terviklikkuse automatiseeritud kontrolli taotlusele vastavad sertifikaadid.

### **4.2.3. Sertifikaadi kontroll ja tõestamine**

Vt CPS p.4.2.4.

### **4.2.4. Sertifikaadi uuendamine**

Sertifikaatide uuendamine toimub ainult PPA kirjaliku taotluse alusel.

Sertifikaadi uuendamisel tunnistatakse vana sertifikaat kehtetuks ning uus sertifikaat antakse välja vanale võtmele.

Aegunud või muul juhul kehtetuks tunnistatud sertifikaadid asendatakse uue Mobiil-ID väljaandmisega.

### **4.3. Sertifikaadi kehtivuse peatamise ja kehtetuks tunnistamise taotlused**

Vt CPS p.4.3.

### **4.4. Sertifikaatide kehtivuse peatamine**

Vt CPS p.4.4.

Mobiil-ID sertifikaatide väärkasutuse vältimiseks kasutatakse Mobiil-ID teenuse sulgemist. SK klienditeeninduspunktis sertifikaadid peatatakse.

Sertifikaatide kehtivust on võimalik peatada:

- MO klienditeeninduspunktis;
- MO abiliinile helistades;
- SK klienditeeninduspunktis.

MO klienditeeninduspunktis, helistades MO abiliinile ja SK klienditeeninduspunktis kehtivuse peatamise taotleja isik tuvastatakse vastavalt isikusamasuse kontrolli protseduurile (vt punkt 3.1). Andmeid võrreldakse Mobiil-ID teenuse liitumislepingus olevate andmetega.

Sertifikaatide peatamise taotluse registreerimisel MO klienditeeninduspunktis või MO abiliinil ei märgita üles taotluse esitaja isikutuvastamisel kasutatud dokumendi andmeid.

### **4.5. Sertifikaadi kehtivuse peatamise lõpetamine**

Vt CPS p.4.5.

Sertifikaatide kehtivuse peatamist on võimalik lõpetada SK klienditeeninduspunktis.

Taotluse esitaja isikusamasus kontrollitakse vastavalt kehtivatele õigusaktidele ja SK siseselt kehtestatud asjaomastele turvaeeskirjadele.

Sertifikaadi kehtivuse peatamise lõpetamise taotlus peab sisaldama:

- omaniku ja taotluse esitaja (kui taotluse esitaja ja omanik pole sama isik) eesnime ja perekonnanime;
- omaniku ja taotluse esitaja (kui taotluse esitaja ja omanik pole sama isik) isikukoodi;
- kehtivuse peatamise lõpetamise alust.

### **4.6. Sertifikaadi kehtetuks tunnistamine**

#### **4.6.1. Sertifikaadi kehtetuks tunnistamise volitused**

Vt CPS p.4.6.1.

Sertifikaadi kehtetuks tunnistamise taotluse võib SK-le esitada PPA.

---

#### 4.6.2. Sertifikaadi kehtetuks tunnistamise taotluse esitamine

Vt CPS p.4.6.2.

Sertifikaatide kehtetuks tunnistamise taotluse esitamine on võimalik Kliendil PPA veebipõhises taotluskeskkonnas. Taotluse esitaja isikusamasus kontrollitakse elektrooniliselt isikut tõendavasse dokumenti kantud autentimise sertifikaadi alusel.

Sertifikaadi kehtetuks tunnistamise taotlus peab sisaldama:

- avalduse esitaja eesnime ja perekonnanime;
- avalduse esitaja isikukoodi;
- kehtetuks tunnistamise põhjust.

Kliendil on võimalik MO klienditeeninduspunktis lõpetada Mobiil-ID leping või vahetada Mobiil-ID SIM kaart, mille käigus MO klienditeeninduspunkt peatab sertifikaadid ja edastab sertifikaatide kehtetuks tunnistamise taotluse PPA-le.

PPA võib esitada ka sertifikaadi kehtetuks tunnistamise taotluse isikut tõendavate dokumentide seaduse [8] alusel või seoses sertifikaadi uuendamise kirjaliku taotlusega.

#### 4.6.3. Sertifikaadi kehtetuks tunnistamise menetlus

Vt CPS p.4.6.3.

#### 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. Mobiil-ID SIM kaartide hoiustamine

Mobiil-ID SIM kaarte hoiustatakse MO klienditeeninduspunktis vastavalt kehtestatud sisemistele protseduuridele.

### **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

Vt CPS p.6.1.2.

##### 6.1.2.1. Kliendi võtmete moodustamine

Võtmete moodustamisel kasutatavad algoritmid, võtmepikkused ja teised parameetrid on toodud dokumendis „Sertifikaadid Eesti Vabariigi isikut tõendavatel dokumentidel”[7].

Mobiil-ID SIM kaardi tootja on kohustatud MO-le esitama koos Mobiil-ID SIM kaartide ja seonduvate avalike võtmetega kinnituse, et võtmed on genereeritud hea tava järgi ning on unikaalsed.

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

##### 6.1.2.2. Kliendi isikliku võtme ja aktiveerimiskoodide kaitse

MO ja Mobiil-ID SIM kaardi tootja tagavad kliendile genereeritud kliendi isikliku võtme ning aktiveerimiskoodide konfidentsiaalsuse ja mittekasutamise kuni võtmete salvestamiseks kasutatava Mobiil-ID SIM kaardi ja võtmete aktiveerimiskoodide kliendile üleandmiseni.

Aktiveerimiskoodid trükitakse ühes eksemplaris otse Mobiil-ID SIM kaardi Turvaalale, mis edastatakse kliendile avamata kujul. Kliendil on kohustus keelduda rikutud Turvaalaga Mobiil-ID SIM kaardi vastuvõtmisest.

##### 6.1.2.3. Kliendi isikliku võtme aktiveerimine

Mobiil-ID isiklike võtmete kasutusfunktsioon lukustub kolme vale aktiveerimiskoodi (PIN-koodi) sisestamise järel. Funktsiooni lahtiblokeerimiseks on võimalik kasutada kliendile üleantud Mobiil-ID SIM kaardi PUK-koodi.

Autentimis- ja allkirjastamisfunktsioonid lukustuvad üksteisest sõltumatult. Mobiil-ID funktsionaalsus lukustub täielikult kolme järjestikuse vale PUK-koodi sisestamisel.



PUK-koodi kadumisel või PUK-koodi lukustumisel tuleb pöörduda MO klienditeeninduspunkti uue Mobiil-ID SIM kaardi saamiseks ja PPA veebipõhisesse taotluskeskkonda uute sertifikaatide taotlemiseks.

#### 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” [7].

## 8. Sertifitseerimispoliitika haldus

Vt CPS p.8.

Käesolev CP ja viidatud dokumendid [1], [7] avaldatakse SK koduleheküljel ja dokument [3] avaldatakse SK, PPA ja MO koduleheküljel.

Kõik sisulised muudatused kooskõlastatakse PPA ja MO-ga.

## 9. Viidatud ja seonduvad dokumendid

Viidatud dokumendid:

- [1] AS Sertifitseerimiskeskus sertifitseerimispõhimõtted (CPS), avaldatud: <https://www.sk.ee/repositoorium/CPS/>
- [2] 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>;



- 
- [3] Mobiil-ID vormis digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimused, AS Sertifitseerimiskeskus, avaldatud: <https://www.sk.ee/repositoorium/kasutustingimused/>;
- [4] RFC 5280 – Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, <https://www.ietf.org/rfc/rfc5280.txt>;
- [5] RFC 3739 – Internet X.509 Public Key Infrastructure: Qualified Certificates Profile, <https://www.ietf.org/rfc/rfc3739.txt>;
- [6] Digitaalallkirja seadus, avaldatud: <https://www.riigiteataja.ee/akt/114032014012&leiaKehtiv>;
- [7] Sertifikaadid Eesti Vabariigi isikut tõendavatel dokumentidel, avaldatud: <https://www.sk.ee/repositoorium/profiil/>;
- [8] Isikut tõendavate dokumentide seadus, avaldatud: <https://www.riigiteataja.ee/akt/123032015016&leiaKehtiv>;

Seotud õigusaktid:

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