



# AS Sertifitseerimiskeskus

## Mobiil-ID vormis digitaalse isikutunnistuse

### sertifitseerimispoliitika

Version 1.1  
OID: 1.3.6.1.4.1.10015.1.3.1.1  
Kehtiv alates 01.02.2011

Versiooni info		
Kuupäev	Versioon	Muudatused
01.02.2011	1.1	Lõplik versioon
11.01.2011	0.1	Mustand

Nõuded Eesti Vabariigi (edaspidi EV) poolt välja antavale Mobiil-ID vormis digitaalse isikutunnistusele (edaspidi Mobiil-ID) digitaalse isikusamasuse kontrolli võimaldavate sertifikaatide väljastamiseks ja teenindamiseks.

1.	Sissejuhatus.....	3
1.1.	Ülevaade .....	3
1.2.	Kasutatud terminoloogia.....	3
1.3.	Kasutatud lühendid.....	3
1.4.	Sertifitseerimispoliitika identifitseerimine .....	4
1.5.	Organisatsioon ja kasutusvaldkond.....	4
1.5.1.	Sertifitseerimiskeskus (SK).....	4
1.5.2.	Registreerimiskeskus.....	4
1.5.3.	PPA.....	5
1.5.4.	Kasutaja .....	5
1.5.5.	Sertifikaatide kasutusvaldkond .....	5
1.6.	Kontaktandmed .....	6
2.	Üldtingimused .....	6
2.1.	Kohustused ja nõuded.....	7
2.1.1.	SK kohustused.....	7
2.1.2.	Registreerimiskeskuse kohustused.....	7
2.1.3.	PPA kohustused.....	8
2.1.4.	MO kohustused.....	8
2.1.5.	Nõuded kliendile.....	9
2.1.6.	Nõuded huvitatud isikule .....	9
2.1.7.	Nõuded kataloogiteenusele .....	9
2.2.	Vastutus .....	9
2.2.1.	SK vastutus.....	9
2.2.2.	Registreerimiskeskuse vastutus.....	9
2.2.3.	MO vastutus.....	10
2.2.4.	PPA vastutus.....	10
2.2.5.	Vastutuse piirid.....	10

---

2.3.	Vaidluste lahendamine .....	10
2.4.	Informatsiooni avaldamine ja kataloogiteenus .....	10
2.4.1.	SK informatsiooni avaldamine.....	10
2.4.2.	Avaldamise sagedus .....	10
2.4.3.	Juurdepääsureeglid .....	10
2.4.4.	Kataloogiteenus.....	10
2.5.	Audit.....	10
2.6.	Konfidentsiaalsus.....	11
3.	Kliendi identifitseerimine .....	11
3.1.	Kliendi isikusamasuse kontroll.....	11
3.2.	Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord.....	11
3.3.	Eraldusnimi .....	11
4.	Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtajad. ....	11
4.1.	Sertifikaaditaotluse esitamine .....	11
4.2.	Sertifikaaditaotluse menetlemine.....	12
4.2.1.	Otsuse tegemine .....	12
4.2.2.	Sertifikaadi väljastamine.....	12
4.2.3.	Sertifikaadi aktiveerimine .....	12
4.2.4.	Sertifikaadi kontroll ja tõestamine .....	12
4.2.5.	Sertifikaadi uuendamine .....	12
4.3.	Sertifikaadi kehtetuks tunnistamise ja kehtivuse peatamise taotlused .....	12
4.4.	Sertifikaatide kehtivuse peatamine .....	13
4.5.	Sertifikaadi kehtivuse peatamise lõpetamine.....	13
4.6.	Sertifikaadi kehtetuks tunnistamine .....	13
4.6.1.	Sertifikaadi kehtetuks tunnistamise volitused .....	13
4.6.2.	Sertifikaadi kehtetuks tunnistamise taotluse esitamine.....	13
4.6.3.	Sertifikaadi kehtetuks tunnistamise menetlus.....	14
4.6.4.	Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus .....	14
4.7.	Protseduurid jälgitavuse tagamiseks .....	14
4.8.	Tegutsemise eriolukorras.....	14
4.9.	Sertifitseerimisteenuse osutaja töö lõpetamine.....	14
5.	Füüsilised ja organisatsioonilised turbemeetmed .....	14
5.1.	Turbehaldus .....	14
5.2.	Füüsilised turbemeetmed.....	14
5.2.1.	SK füüsiline pääsukontroll.....	14
5.2.2.	Muud nõuded. Mobiil-ID SIM kaartide hoiustamine.....	14
5.3.	Nõuded tööprotseduuridele .....	14
5.4.	Personali turbenõuded.....	14
6.	Tehnilised turbenõuded .....	15
6.1.	Võtmehaldus .....	15
6.1.1.	SK kinnitusvõtmed .....	15
6.1.2.	Kliendi võtmed.....	15
6.2.	Süsteemiturve.....	16
6.3.	Sertifitseerimisteenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus .....	16
6.4.	Sertifitseerimisteenuse osutamisel tekkinud andmete säilitamine ja kaitse.....	16
7.	Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid .....	16
8.	Sertifitseerimispoliitika haldus.....	16
9.	Viidatud ja seonduvad dokumendid .....	16

## 1. Sissejuhatus

### 1.1. Ülevaade

Käesolev dokument (edaspidi 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 toodud.

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

Käesolev CP koostamisel on kasutatud IETFi (*Internet Engineering Task Force*) soovitusliku 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 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 kliendi poolt täidetav ning digitaalselt allkirjastatav kirjalik avaldus Mobiil-ID sertifikaatide saamiseks.

### 1.3. Kasutatud lühendid

Vt CPS p.11.

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

Lühend	Definitsioon
	kehtivuse peatamiseks ja peatatuse lõpetamiseks.
PPA	EV Politsei- ja Piirivalveamet, Mobiil-ID väljaandja.
SK	AS Sertifitseerimiskeskus – sertifitseerimisteenuse osutaja
STO	Sertifitseerimise Registris registreeritud sertifitseerimisteenuse osutaja

## **1.4. Sertifitseerimispoliitika identifitseerimine**

Käesoleva CP tunnuscode on OID: 1.3.6.1.4.1.10015.1.3.1.1

CP tunnuscode 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	1.1

*Tabel 1. CP tunnuscode koostamine*

## **1.5. Organisatsioon ja kasutusvaldkond**

### **1.5.1. Sertifitseerimiskeskus (SK)**

Vt CPS p.1.2.1.

Sertifikaadid väljastatakse Mobiil-ID-le. 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 punktis 1.5.2 kirjeldatud kohustused.

### **1.5.2. Registreerimiskeskus**

#### **1.5.2.1. Klienditeeninduspunktid**

Vt CPS p.1.2.2.1.

Mobiil-ID SIM kaartide väljastamine ning Mobiil-ID sertifikaatide teenindamine (kehtivuse peatamine, kehtivuse peatatuse lõpetamine) ja Mobiil-ID SIM kaardiga seotud telefoni numbri muutmine toimub MO volitatud teeninduspunktides (edaspidi klienditeeninduspunkt), mille täpne loetelu ja lahtiolekuajad on viidatud SK koduleheküljel <http://www.sk.ee> ja MO kodulehekülgedel.

MO tagab turvalisuse enda kohustuste täitmisel sisemiste turbeprotseduuridega.

### **1.5.2.2. 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 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.

PPA tagab turvalisuse enda kohustuste täitmisel sisemiste turbeprotseduuridega.

### **1.5.4. Kasutaja**

#### **1.5.4.1. Klient**

Vt CPS p.1.2.3.1.

Klient on füüsiline isik, kellele väljastatakse avaliku teenusena sertifikaate, mis on seotud Mobiil-ID SIM kaardiga, kui tal on selleks seadusejärgne õigus. Igal Kliendil võib olla kehtivas staatuses üks digitaalset isikutuvastamist ja üks digitaalset allkirjastamist võimaldav Mobiil-ID SIM kaardiga seotud sertifikaat.

Klient on käesoleva CP alusel väljastatud sertifikaadi omanik.

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

Kliendil peab olema tutvunud enne Mobiil-ID sertifikaaditaotluse esitamist „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 DAS [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: pki@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 koheselt teavitama oma koduleheküljel.

### **PPA kodakondsus- ja migratsiooniosakond**

Endla 13,  
15179 Tallinn  
Infotelefon +372 612 3000  
Üldtelefon +372 612 3300  
Faks +372 612 3009  
E-post: [teeninduskeskus@politsei.ee](mailto:teeninduskeskus@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 - 17.00: 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 koheselt 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 AS Sertifitseerimiskeskuse sertifitseerimis põhimõtetega;
- sertifitseerimisteenuse osutamine on kooskõlas käesoleva CPga.

SK kohustub täiendavalt:

- vastu võtma ja registreerima MO poolt esitatud Mobiil-ID SIM kaardi väljastamise teatisi 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 töötlema MO poolt esitatud sertifikaadi kehtivuse peatamise, kehtivuse peatamise lõpetamise taotlusi ja PPA poolt esitatud kehtetuks tunnistamise taotlusi ning MO poolt esitatud Mobiil-ID SIM kaardiga seotud telefoni numbri muudatuse taotlusi;
- tagama, et sertifitseerimisteenuse osutamisel kasutatavad kinnitusvõtmed oleksid riistvaraliste turvamoodulite abil kaitstud ning ei väljuks SK kontrolli alt;
- kinnitusvõtmete kontrolli alt väljumise korral peatama kõikide väljastatud sertifikaatide kehtivuse;
- tagama, et kõik aktiveeritud režiimis olevad kinnitusvõtmed asuvad Eesti Vabariigi territooriumil;
- tagama, et sertifitseerimisteenuse osutamisel kasutatavate kinnitusvõtmete aktiveerimine toimub jagatud kontrolli alusel.

### **2.1.2. Registreerimiskeskuse kohustused**

#### **2.1.2.1. MO klienditeeninduspunkti kohustused**

Vt CPS p.2.1.2.1.

MO klienditeeninduspunkt peab vastu võtma taotlusi:

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

Klienditeeninduspunkt kohustub kõikide nimetatud toimingute teostamisel kontrollima:

- nende taotluste õigsust ja terviklikkust; ja
- taotluse esitaja isikusamasust ja volitusi toimingute teostamiseks.

MO klienditeeninduspunkt garanteerib oma töötajatele teenuse kvaliteetseks osutamiseks vajaliku koolituse.

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

MO klienditeeninduspunkt kohustub täiendavalt:

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

### **2.1.2.2. MO abiliini kohustused**

Vt CPS p.2.1.2.2.

### **2.1.3. 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;
- 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 osas järgima käideldavuse ja turbenõudeid, mis vastavad vähemalt käesolevas CP-s toodud nõuetele;
- veebipõhises taotluskeskkonnas järgima käideldavuse ja turbenõudeid, mis vastavad vähemalt käesolevas CP-s toodud nõuetele;
- 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 turbeprotseduuridega.

### **2.1.4. MO kohustused**

MO kohustub:

- Mobiil-ID teenuse osutamisega seotud infosüsteemi osas järgima käideldavuse ja turbenõudeid, mis vastavad vähemalt käesolevas CP-s toodud nõuetele;
- tagama turvalisuse enda kohustuste täitmisel sisemiste turbeprotseduuridega. 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 ja kehtivuse peatamise lõpetamise taotlused) ja/või on seotud sertifitseerimisteenust puudutava informatsiooniga, ei ole karistatust tahtlikult toimepandud kuriteo eest;



- tagama Mobiil-ID teenust puudutava informatsiooni kättesaadavuse avalikus andmesidevõrgus.

### **2.1.5. 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 või PPA-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.

### **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 Vabariigi 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 2.1.2.1 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 2.1.2.2 toodud kohustuste täitmise eest.

### **2.2.3. MO vastutus**

MO vastutab kõigi käesoleva CP punktis 2.1.4 toodud ja teiste CP-s toodud tema kohustuste täitmise eest.

### **2.2.4. PPA vastutus**

PPA vastutab kõigi käesoleva CP punktis 2.1.3 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 avaldatakse 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.

MO teostab kliendi isikusamasuse kontrolli vastavalt siseselt kehtestatud isikusamasuse kontrolli protseduurile.

### **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 isikutunnistusel“ [7].

## **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 täidab taotlusankeedi Mobiil-ID taotlemiseks ning allkirjastab selle digitaalselt. Allkirjastatud Mobiil-ID taotlus on käsitletav sertifikaaditaotlusena. Sertifikaaditaotluse esitamisele eelneb elektrooniline isikusamasuse kontrollimine.

Sertifikaaditaotluse sisu ja esitamise kord peab minimaalselt olema kooskõlas digitaalallkirjaseadusega.

Sertifikaaditaotluse esitamisel klient 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 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.

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 võimaldava sertifikaadi väljastamiseks.

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

### **4.2.2. Sertifikaadi väljastamine**

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

SK poolt väljastatud sertifikaadid on aktiveeritud staatuses.

### **4.2.3. Sertifikaadi aktiveerimine**

Sertifikaadid väljastatakse aktiveeritud staatuses.

### **4.2.4. Sertifikaadi kontroll ja tõestamine**

Vt CPS p.4.2.4.

### **4.2.5. Sertifikaadi uuendamine**

Sertifikaatide uuendamist ei toimu.

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

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

Vt CPS p.4.3.

---

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

Vt CPS p.4.4.

Sertifikaatide kehtivust on võimalik peatada:

- MO klienditeeninduspunktis;
- MO abiliinile helistades.

MO klienditeeninduspunktis ja helistades MO abiliinile 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 ei märgita üles taotluse esitaja isikutuvastamisel kasutatud dokumendi andmed.

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

Vt CPS p.4.5.

Sertifikaatide kehtivuse peatamist on võimalik lõpetada MO klienditeeninduspunktis.

Taotluse esitaja tuvastatakse vastavalt isikusamasuse kontrolli protseduurile (vt punkt 3.1).

Sertifikaadi kehtivuse peatamise lõpetamise taotlus peab sisaldama:

- avalduse esitaja eesnime ja perekonnanime;
- avalduse esitaja allkirja;
- peatatud kehtivusega sertifikaadi omaniku nime ja isikukoodi;
- kehtivuse peatamise lõpetamise alust.

Klienditeeninduspunktis taotluse registreerimisel märgitakse üles taotluse esitaja isikusamasuse kontrollil kasutatud dokumendi andmeid.

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

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

Vt CPS p.4.6.1.

Sertifikaadi kehtetuks tunnistamise taotluse võib esitada PPA peale Mobiil-ID kehtetuks tunnistamist.

##### **4.6.2. Sertifikaadi kehtetuks tunnistamise taotluse esitamine**

Vt CPS p.4.6.2.

Sertifikaatide kehtetuks tunnistamise taotluse esitamine on võimalik PPA veebipõhises taotluskeskkonnas. Taotluse esitaja isikusamasus kontrollitakse vastavalt kehtivatele õigusaktidele.

Sertifikaadi kehtetuks tunnistamise taotlus peab sisaldama:

- avalduse esitaja eesnime ja perekonnanime;
- avalduse esitaja allkirja;
- peatatud kehtivusega sertifikaadi omaniku nime ja isikukoodi;
- kehtetuks tunnistamise põhjust.

#### **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 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

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 isikutunnistusel”[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 volitusteta 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 avamata kliendile. 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 isikutunnistusel” [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 sertifitseerimis põhimõtted (CPS)
- [2] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;
- [3] Mobiil-ID vormis digitaalsele isikutunnistusele väljastatavate sertifikaatide kasutustingimused. AS Sertifitseerimiskeskus;
- [4] RFC 3280 – Request For Comments 3280, Internet X.509 Public Key Infrastructure / Certificate and Certificate Revocation List (CRL) Profile;
- [5] RFC 3739 – Request For Comments 3739. Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
- [6] Digitaalallkirja seadus, RT I 2000, 26, 150.





- [7] Sertifikaadid Eesti Vabariigi isikutunnistusel;
- [8] Isikut tõendavate dokumentide seadus, RT I 1999, 25, 365.