AS Sertifitseerimiskeskus
Mobiil-ID sertifitseerimispoliitika

Versioon 2.0
OID: 1.3.6.1.4.1.10015.11.1.2
Kehtiv alates 16.12.2009

Versiooni info		
Kuupäev	**Versioon**	**Muudatused**
16.11.2009	2.0	Lisatud praktikast tingitud täiendused Mobiil-ID käivitamisel, keelelised korrektuurid
11.04.2007	1.0	Lõplik versioon
15.03.2007	0.9	Mustand

Nõuded digitaalset allkirjastamist ja digitaalset isikusamasuse kontrolli võimaldavate Mobiil-ID sertifikaatide väljastamiseks ja teenindamiseks.

1. Sissejuhatus

1.1. Ülevaade

Käesolev dokument (edaspidi CP) on reeglite kogum, mis määrab ära nõuded Mobiil-ID 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 digitaalsetele 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 mobiiltelefoniteenuse kasutamisele ka elektroonilises keskkonnas digitaalset isikusamasuse tõendamist ja digitaalset allkirjastamist
Sertifikaatide kasutustingimused	Dokument, mis sisaldab kohustusi ja vastutust Mobiil-ID SIM kaardi ja sellega seotud sertifikaatide kasutamisel. Klient peab Mobiili-ID SIM kaardi väljastamisel olema tutvunud ja aktsepteerima selles dokumendis toodud tingimusi.
Sertifikaaditaotlus	Kliendi poolt täidetav ning käsitsi allkirjastatav kirjalik avaldus Mobiil-ID teenuse avamiseks ja sertifikaatide saamiseks

1.3. Kasutatud lühendid

Vt CPS p.11.

Lühend	Definitsioon
MO	Elektroonilise side ettevõtja, kes osutab mobiiltelefoniteenust ja kellega on sõlmitud vastavad lepingud Mobiil-ID SIM kaardi väljastamiseks ja Mobiil-ID sertifikaatide järelteenindamiseks.

1.4. Sertifitseerimispoliitika identifitseerimine

Käesoleva CP tunnuskood on **OID: 1.3.6.1.4.1.10015.11.1.2**

CP tunnuskood 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	11.1
CP versiooni tunnus	2

Tabel 1. CP tunnuskoodi koostamine

1.5. Organisatsioon ja kasutusvaldkond

1.5.1. Sertifitseerimiskeskus (SK)

Vt CPS p.1.2.1.

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.

Taotluste vastuvõtmine Mobiil-ID sertifikaatide väljastamiseks, Mobiil-ID SIM kaartide väljastamine ning seotud sertifikaatide teenindamine (kehtivuse peatamine, kehtivuse peatatuse lõpetamine, kehtetuks tunnistamine 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 koduleheküljel.

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. Kasutaja

1.5.3.1. Klient

Vt CPS p.1.2.3.1.

Klient on füüsiline isik, kellele väljastatakse avaliku teenusena Mobiil-ID sertifikaate. Igal Kliendil võib olla kehtivas staatuses üks digitaalset isikutuvastamist ja üks digitaalset allkirjastamist võimaldav Mobiil-ID sertifikaat.

Klient on käesoleva CP alusel väljastatud sertifikaadi omanik.

Kliendi eraldusnimi sertifikaadis koostatakse vastavalt sertifikaadiprofiilile, mis on toodud käesoleva dokumendi punktis 7.1.

Kliendil peab olema võimalus enne Mobiil-ID lepingu sõlmimist tutvuda „Mobiil-ID sertifikaatide kasutustingimustega“ [3]

1.5.3.2. Huvitatud isik

Vt CPS p.1.2.3.2.

1.5.4. 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.

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 sertifitseerimispõhimõtetega;
- sertifitseerimisteenuse osutamine on kooskõlas käesoleva CPga.

SK kohustub täiendavalt:
- vastu võtma ja registreerima MO poolt esitatud sertifikaaditaotlusi ning väljastama neile vastavaid sertifikaate;
- pakkuma vastavat veebirakendust Mobiil-ID sertifikaatide aktiveerimiseks;
- vastu võtma, registreerima ja töötlema MO poolt esitatud sertifikaadi kehtivuse peatamise, kehtivuse peatatuse lõpetamise ja kehtetuks tunnistamise taotlusi ning 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 sertifikaatide väljastamiseks, peatamiseks, kehtivuse peatatuse lõpetamiseks ja kehtetuks tunnistamiseks ning kontrollima nende taotluste õigsust ja terviklikkust. Klienditeeninduspunkt kohustub kõikide nimetatud toimingute teostamisel kontrollima taotluse esitaja isikusamasust ja volitusi toimingu 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 sertifikaaditaotluse ja väljastama kliendile Mobiil-ID SIM kaardi;
- tagama esmase nõustamise ja abistamise Mobiil-ID SIM kaardi käsitlemisel ning Mobiil-ID 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. MO kohustused

MO kohustub:

- Mobiil-ID-ga 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 sertifikaatidega seotud taotlusi (väljastamis-, kehtivuse peatamis-, kehtivuse peatatuse lõpetamise ja kehtetuks tunnistamise 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. Nõuded kliendile

Vt CPS p.2.1.3.

Klient peab Mobiil-ID sertifikaaditaotluse esitamisel edastama MO klienditeeninduspunktile õige informatsiooni. Sertifikaati kantud isikuandmete muutumise korral on klient kohustatud teatama muutunud andmed MO klienditeeninduspunktile ja taotlema uued Mobiil-ID sertifikaadid.

2.1.5. Nõuded huvitatud isikule

Vt CPS p.2.1.4.

2.1.6. Nõuded kataloogiteenusele

Kataloogiteenust antud teenuse juures ei kasutata.

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 2.1.2.1 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 2.1.3 toodud ja teiste 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/eid/eid2007.crl

Kataloogiteenust antud teenuse juures ei kasutata.

2.4.2. Avaldamise sagedus

Sertifikaatide tühistusnimekirju avaldatakse iga 12 tunni järel.

2.4.3. Juurdepääsureeglid

Juurdepääs punktis 2.4.1 kirjeldatud informatsioonile üldkasutatavat andmesidevõrku kasutades on tasuta ning juurdepääsu ei piirata.

2.4.4. Kataloogiteenus

Kataloogiteenust antud teenuse juures ei kasutata.

2.5. Audit

Vt CPS p.2.5.

2.6. Konfidentsiaalsus

Vt CPS p.2.6.

3. Kliendi identifitseerimine

3.1. Kliendi isikusamasuse kontroll

Kliendi isikusamasust kontrollitakse vastavalt MO-ga kokku lepitud 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 käesoleva dokumendi punktile 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 MO klienditeeninduspunktis.

Klient täidab taotlusankeedi Mobiil-ID teenuse taotlemiseks ning allkirjastab selle. Allkirjastatud Mobiil-ID taotlus on käsitletav sertifikaaditaotlusena. Sertifikaaditaotluse esitamisele peab eelnema isikusamasuse tuvastamine vastavalt isikusamasuse kontrolli protseduurile (vt. punkt 3.1).

Sertifikaaditaotluse sisu ja esitamise kord peab minimaalselt olema kooskõlas digitaalallkirjaseadusega.

Sertifikaaditaotluse esitamisel klient nõustub „Mobiil-ID sertifikaatide kasutustingimustega“ [3].

Täiendavat informatsiooni saab MO veebilehtedelt ja http://www.sk.ee

4.2. Sertifikaaditaotluse menetlemine

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 MO. Sertifikaaditaotluse rahuldamise või mitterahuldamise otsuse langetamisel lähtutakse isikusamasuse kontrolli tulemustest, esitatud andmete õigsusest ja sellest, kas kliendil on vastavalt MO tegutsemispiirkonna õigusaktidele õigus saada Mobiil-ID sertifikaate.

Kliendi teavitamine otsusest toimub MO klienditeeninduspunktis kohapeal.

4.2.2. Sertifikaadi väljastamine

Mobiil-ID SIM kaardi tootja laeb kaardile genereeritud võtmepaari isiklikud võtmed ja edastab avalikud võtmed MO-le. SK väljastab peale MO poolt edastatud sertifikaaditaotluse andmete autentsuse ja terviklikkuse automatiseeritud kontrolli taotlusele vastavad sertifikaadid. Sertifikaadid väljastatakse isikule Mobiil-ID SIM kaardi väljastamisel.

SK poolt väljastatud sertifikaadid on aktiveerimata staatuses. Sertifikaate ei ole võimalik kasutada enne sertifikaatide aktiveerimist. Mobiil-ID sertifikaatide aktiveerimine toimub eraldiseisva protsessina (vt. p. 4.2.3).

Kehtivate sertifikaatidega Mobiil-ID SIM kaardile uute sertifikaatide taotlemisel väljastatakse isikule uus Mobiil-ID SIM kaart MO klienditeeninduspunktis.

4.2.3. Sertifikaadi aktiveerimine

Sertifikaatide aktiveerimiseks kasutab sertifikaadi omanik eraldiseisvat veebirakendust, mille eesmärk on isikusamasuse kontrolli tõhustamine. Sertifikaatide aktiveerimine veebirakenduses on võimalik ainult kasutades ID-kaarti.

Sertifikaate ei ole võimalik kasutada enne sertifikaatide aktiveerimisprotseduuri teostamist.

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 SIM kaardi väljastamisega MO klienditeeninduspunktis.

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 liitumislepingus olevate andmetega.

.
Sertifikaatide peatamise taotluse registreerimisel MO klienditeeninduspunktis ei märgita üles taotluse esitaja isikutuvastamisel kasutatud dokumendi andmed.

4.5. Sertifikaadi kehtivuse peatatuse lõpetamine

Vt CPS p.4.5.

Sertifikaatide kehtivuse peatatust on võimalik lõpetada MO klienditeeninduspunktis.

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

Sertifikaadi kehtivuse peatatuse lõpetamise taotlus peab sisaldama:

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

Lisaks võib MO sertifikaadi kehtetuks tunnistamise avalduse esitada ilma sertifikaadi omaniku osavõtuta järgmistel juhtudel:

- kliendi liitumisleping MO-ga lõpetatakse vastavalt MO üldtingimustele, kui klient on andnud selleks MO-le volituse;
- Mobiil-ID teenuse leping lõpetatakse numbri omaniku algatusel;
- klient teeb SIM kaardi vahetuse;
- klient vahetab sideteenuse pakkujat.

4.6.2. Sertifikaadi kehtetuks tunnistamise taotluse esitamine

Vt CPS p.4.6.2.

Sertifikaatide kehtetuks tunnistamine on võimalik MO klienditeeninduspunktis.

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

Sertifikaadi kehtetuks tunnistamise taotlus peab sisaldama:

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

MO 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.

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 kasutatakse RSA algoritmi võtmepikkusega vähemalt 1024 bitti. 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 poole uue Mobiil-ID SIM kaardi saamiseks.

6.1.2.4. Kliendi võtmete varundamine ja deponeerimine

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

6.2. Süsteemiturve

Vt CPS p.6.2.

6.3. Sertifitseerimisteenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus

Vt CPS p.6.3.

6.4. Sertifitseerimisteenuse osutamisel tekkinud andmete säilitamine ja kaitse

Vt CPS p.6.4.

7. Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid

7.1. Sertifikaadi profiil

SK väljastab X.509 versioon 3 sertifikaate vastavalt soovituslikus standardis RFC 3280 [4] toodud juhistele. Mobiil-ID väljastatavas sertifikaadis peavad vähemalt olema välja toodud järgmised andmed:

Väli	OID	Kirjeldus
Version		Sertifikaadi vormingu versiooninumber: V3
Serial number		Sertifikaadi järjekorra number, sertifitseerija poolt sertifikaadile antud unikaalne tunnusnumber
Signature Algorithm		Sertifikaadi signeerimisalgoritm:sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer		Sertifikaadi väljaandja andmed
id-at-countryName	2.5.4.6	Riigi tunnus: EE
id-atorganizationName	2.5.4.10	Sertifitseerija nimi SR-s: AS Sertifitseerimiskeskus
id-atorganizationalUnitName	2.5.4.11	Sertifitseerimisteenuste liik: Sertifitseerimisteenused
id-at-commonName	2.5.4.3	Sertifitseerija eraldusnimi: EID-SK 2007
Subject		Sertifikaadi omaniku andmed
id-at-serialNumber	2.5.4.5	Kliendi isikukood
id-at-givenName	2.5.4.42	Kliendi eesnimed
id-at-surname	2.5.4.4	Kliendi perekonnanimi
id-at-commonName	2.5.4.3	Sertifikaadi üldnimi kujul: <PEREKONNANIMI>,<EESNIMED>,<ISIKUKOOD>
id-atorganizationalUnitName	2.5.4.11	Sertifikaadi kasutusvaldkond Digitaalset isikutuvastust võimaldavas sertifikaadis: *mobile authentication* Digitaalallkirjastamist võimaldavas sertifikaadis: *mobile signature*
id-atorganizationName	2.5.4.10	Mobiilteenuseoperaatori nimi
id-at-countryName	2.5.4.6	Sertifikaadi taotluses märgitud isikukoodi välja andnud riigi kood vastavalt RFC 3280 toodud juhistele.
Valid from		Sertifikaadi kehtivuse algusaeg. Informatsioon kodeeritud vastavalt RFC 3280 toodud juhistele.
Valid to		Sertifikaadi kehtivuse lõppemise aeg. Informatsioon kodeeritud vastavalt RFC 3280 toodud juhistele. Üldjuhul sertifikaadi väljastamise aeg + 1825 päeva (5 aastat).
Public key		Avalik võti ASN.1 kujul koosneb vähemalt 1024 bitisest moodulist ja 3 baidisest eksponendist (65537)
Key Usage	2.5.29.15	Sertifikaadi põhikasutusala Digitaalset isikutuvastust võimaldavas sertifikaadis on seatud sellised võtmekasutust tähistavad atribuudid: *Digital Signature, Key Encipherment, Data Encipherment;* Digitaalallkirjastamist võimaldavas sertifikaadis on tähistatud ainult üks võtmekasutusala: *Non-Repudiation*
Extended Key Usage	2.5.29.37	Võtme laiendatud kasutusala. Kasutusel ainult digitaalset isikutuvastust võimaldavas sertifikaadis: Client Authentication (1.3.6.1.5.5.7.3.2)

		E-mail Protection (1.3.6.1.5.5.7.3.4)
Certificate Policies	2.5.29.32	Sertifitseerimispoliitika. Viide sertifikaadi väljastamisel lähtutud põhimõtetele. Viidatakse põhimõtete unikaalsele tunnusele - OID-le kui ka selle asukohale SK avalikul veebilehel: Policy Identifier= 1.3.6.1.4.1.10015.11.1.1.2 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/mid/
Authority Key Identifier	2.5.29.35	Sertifitseerija avaliku võtme räsi
Subject Key Identifier	2.5.29.14	Käesoleva sertifikaadi avaliku võtme räsi
CRL Distribution Points	2.5.29.31	http://www.sk.ee/crls/eid/eid2007.crl
Basic Constraints	2.5.29.19	Piirang, mis näitab sertifikaadi tüüpi (lõppkasutaja sertifikaat): *Subject Type=End Entity, Path Length Constraint=None*
1.3.6.1.5.5.7.1.3 id-pe-qcStatements	1.3.6.1.5.5.7.1.3	Kvalifitseeritud sertifikaadi tunnus. Laiendus, mis näitab, et sertifikaat on väljastatud vastavalt kvalifitseeritud sertifikaatidele sätestatud nõuetele (vt RFC 3739).
Thumbprint algorithm		Räsimisel kasutatakse sha1 algoritmi.
Thumbprint		Sertifikaadi räsi

7.2. Tühistusnimekirja (CRL-i) profiil

Tühistusnimekiri väljastatakse kaks korda päevas ja sisaldab nii peatatud kehtivusega kui ka kehtetuks tunnistatud sertifikaate. Nimekiri on koostatud vastavalt tühistusnimekirjade vormingule x.509 versioon 2 (vt RFC 3280) [4].

CRL komponent	OID	Viide RFC 3280	Märkused
CertificateList		5.1.1	
tBSCertList		5.1.1.1	vaata järgmist tabeli osa
signatureAlgorithm		5.1.1.2	Tühistusnimekirja allkirjastamise algoritm: sha1WithRSAEncryption
signatureValue		5.1.1.3	Signatuur
tBSCertList		5.1.2	
version		5.1.2.1	Tühistusnimekirja vormingu versioon: V2
signature		5.1.2.2	väärtus sõltub valitud algoritmist
Issuer		5.1.2.3	UTF8 kodeeritud CRL-i väljastaja eraldusnimi
id-at-countryName	2.5.4.6		EE
id-at-organizationName	2.5.4.10		AS Sertifitseerimiskeskus
id-atorganizationalUnitName	2.5.4.11		Sertifitseerimisteenused
id-at-commonName	2.5.4.3		EID-SK 2007
thisUpdate		5.1.2.4	Tühistusnimekirja väljastuskuupäev ja kellaaeg. UTC aeg kuni 2049-ni, hiljem

			kasutatakse siin GeneralisedTime
nextUpdate		5.1.2.5	Järgmise tühistusnimekirja väljastamise kuupäev. UTC aeg kuni 2049-ni, hiljem kasutatakse siin GeneralisedTime
revokedCertificates		5.1.2.6	Kehtetuks tunnistatud või peatatud kehtivusega sertifikaatide loetelu.
Revocation Date	2.5.29.24		Kehtivuse peatamise/kehtetuks tunnistamise kuupäev ja kellaaeg
Reason code	2.5.29.21		Põhjus (peatatud kehtivusega sertifikaatide puhul 6 – Certificate Hold)
Serial Number			Kehtetuks tunnistatud või peatatud kehtivusega sertifikaadi number
CRL Number	2.5.29.20	5.2.3	Järjekorra number, sertifitseerija poolt sertifikaadile antud unikaalne tunnusnumber
Authority Key Identifier	2.5.29.35	5.1.2.7	SK vastava avaliku võtme (millele vastavat privaatvõtit kasutati antud CRL-i signeerimiseks) identifikaator, mis on oluline SK sertifikaatide ahela loomiseks
Issiuing Distribution Point	2.5.29.28		Tühistusnimekirja levituspunkt

Väljal authorityKeyIdentifier esitatakse SK vastava avaliku võtme (millele vastavat privaatvõtit kasutati antud CRL-i signeerimiseks) identifikaator, mis on oluline SK sertifikaatide ahela loomiseks.

Väli CRL number on monotoonselt kasvav arv ning määrab konkreetse, SK poolt välja antud, CRL-i järjekorranumbri.

Samuti võib sertifitseerimisteenuse osutaja võimalusel kasutada ka CRL Entry laiendusi, järgides RFC 3280-s esitatud nõudeid ja soovitusi.

8. Sertifitseerimispoliitika haldus

Vt CPS p.8.

Käesolev CP ja viidatud dokumendid [1], [2], [4], [5] avaldatakse SK koduleheküljel ja dokument [3] avaldatakse SK ja MO koduleheküljel.

Kõik sisulised muudatused kooskõlastatakse MO-ga.

9. Viidatud ja seonduvad dokumendid

Viidatud dokumendid:

[1] AS Sertifitseerimiskeskus sertifitseerimispõhimõtted (CPS)
[2] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;
[3] Mobiil-ID 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] Eesti Vabariigi digitaalallkirja seadus, RT I 2000, 26, 150