Mobiil-ID sertifitseerimispoliitika

Versioon 1.0

OID: 1.3.6.1.4.1.10015.11.1.1

Nõuded Eesti Vabariigi siseriiklikule digitaalallkirja ja isikutuvastust võimaldavate Mobiil-ID sertifikaatide väljastamiseks ja teenindamiseks.

Versioonid ja muudatused:

Versioon	Kuupäev	Kommentaarid
0.9	15.03.2007	Mustand
1.0	11.04.2007	Lõplik versioon

Sisukord

1 Sissejuhatus

1.1 Ülevaade

Käesolev dokument (edaspidi sertifitseerimispoliitika, CP) on reeglite kogum, mis määrab ära peamised tööpõhimõtted ja -kontseptsioonid Mobiil-ID kaardi sertifikaatide väljastamiseks vajaliku sertifitseerimisteenuse osutamiseks.

Käesolev CP rajaneb dokumendile „AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted versioon 2.0“ [1] (edaspidi CPS), mis on registreeritud sertifitseerimisteenuse osutajate riiklikus 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
Sertifikaatide kasutustingimused	Dokument, mis sisaldab Kliendi kohustusi ja vastutust Mobiil-ID kaardi ja sellega seotud sertifikaatide kasutamisel. Klient peab Mobiil-ID kaardi väljastamisel olema tutvunud ja aktsepteerima selles dokumendis toodud tingimusi.

1.3 Kasutatud lühendid

Vt CPS p.11.

Lühend	Definitsioon
SK	AS Sertifitseerimiskeskus, sertifitseerimisteenuse osutaja.
CP	Käesolev dokument – Mobiil-ID sertifitseerimispoliitika
CPS	AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted

MO	Mobiilioperaator, kellega on sõlmitud vastavad lepingud Mobiil-ID kaardi väljastamiseks ja teenindamiseks.

1.4 Sertifitseerimispoliitika identifitseerimine

Käesoleva CP tunnuskood on **OID: 1.3.6.1.4.1.10015.11.1.1**

CP tunnuskood 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	11
CP versiooni tunnus	1.1

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 punktides 1.5.2 ja **Error! Reference source not found.** kirjeldatud kohustused.

1.5.2 SK registreerimiskeskus

1.5.2.1 Klienditeeninduspunktid

Vt CPS p.1.2.2.1.

Mobiil-ID taotluste vastuvõtmine, SIM-kaartide väljastamine ning seotud sertifikaatide teenindamine (peatamine, peatatuse lõpetamine, kehtetuks tunnistamine) toimub MO teeninduspunktides (edaspidi klienditeeninduspunkt), mille täpne loetelu ja lahtiolekuajad on viidatud SK kodulehelt http://www.sk.ee ja MO kodulehekülgedel.

MO on vastutav kõikide Mobiil-ID kaartide tootmisega seotud operatsioonide ja protseduuride täitmise eest, sealhulgas Mobiil-ID kaardi turvalise võtme genereerimise eest.

MO tagab turvalisuse enda kohustuste täitmisel sisemiste turbeprotseduuridega.

1.5.2.2 Abiliin

Abiliin tegeleb klientide telefoniteenindusega ja võtab ööpäevaringselt klientidelt ning teistelt osapooltelt vastu taotlusi sertifikaatide peatamiseks, eelnevalt tuvastades isiku kasutades kliendi liitumislepingus olevaid andmeid.

Abiliin annab vajadusel täiendavalt infot Mobiil-ID kaardiga seotud probleemide lahendamisel.

Informatsiooni abiliini ja tema kontaktandmete kohta esitatakse SK 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, kui tal on selleks seadusjärgne õigus. Igal Kliendil on õigus saada üks Mobiil-ID sertifikaat.

Klient on käesoleva CP alusel väljastatud sertifikaadi omanik.

Kliendi eraldusnimi sertifikaadis koostatakse vastavalt sertifikaadiprofiilile, mis on toodud käesoleva dokumendi punktis 7.

Kliendil peab olema võimalus enne Mobiil-ID kaardi väljastamist 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 isiku digitaalseks tuvastamiseks
b) sertifikaate digitaalseks allkirjastamiseks

Digitaalallkirja kasutamine on reguleeritud kehtivate õigusaktidega.

CP ei sea piiranguid sertifikaatide kasutamiseks erinevates tarkvararakendustes ega rakendusvaldkondades.

1.6 Kontaktandmed

SK
Vt CPS p.1.3.

Abiliin
1777, +372 630 4084

MO

MO kontaktandmed on ära toodud SK veebilehel http://www.sk.ee. Kontaktandmete muutumisel on MO kohustatud sellest koheselt teavitama oma koduleheküljel.

Klienditeeninduspunktid

Klienditeeninduspunktide nimekiri ja kontaktandmed on viidatud SK veebilehel http://www.sk.ee. 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;
- vastu võtma, registreerima ja töötlema MO poolt esitatud sertifikaadi peatamis-, peatamise lõpetamise-, kehtetuks tunnistamise taotlusi ja Mobiil-ID 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 kohustub täiendavalt:

- väljastama kliendile Mobiil-ID kaardi aktiveerides teenuse ja edastades SK-le sertifikaaditaotluse;
- tagama esmase nõustamise ja abistamise Mobiil-ID kaardi käsitlemisel.

MO klienditeeninduspunkt peab vastu võtma taotlusi sertifikaatide uuendamiseks, peatamiseks, 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.

2.1.2.2 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, et töötajatel, kes võtavad vastu Mobiil-ID kaardiga seotud taotlusi (väljastamis-, peatamis-, tühistamis-, peatatuse lõpetamistaotlused ja sertifikaatide uuendamine) ja/või on seotud sertifitseerimisteenust puudutava informatsiooniga, ei ole karistatust tahtlikult toimepandud kuriteo eest;
- tagama Mobiil-ID kaarte puudutava informatsiooni kättesaadavuse avalikus andmesidevõrgus.

2.1.4 Nõuded kliendile

Vt CPS p.2.1.3.

Klient peab Mobiil-ID kaardi taotluse esitamisel edastama MO volitatud esindusele õige informatsiooni ning isikuandmete muutumise korral teatama õiged andmed rahvastikuregistrile ja MO volitatud esindusele vastavalt kehtestatud õigusaktidele.

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 ja 2.1.2 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 Abiliini vastutus

Vt CPS p.2.2.2.2.
SK ja MO vastutavad 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

Kehtiv tühistusnimekiri on kättesaadav aadressil http://www.sk.ee/crls/eid/eid2007.crl

2.4.2 Avaldamise sagedus

Sertifikaatide tühistusnimekirju avaldatakse reeglina 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.
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 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

4.1 Sertifikaaditaotluse esitamine

Vt CPS p.4.1.
Klient täidab taotlusankeedi Mobiil-ID kaardi taotlemiseks ning allkirjastab selle. Allkirjastatud Mobiil-ID kaardi taotlus on sertifikaaditaotluse koostamise aluseks.

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 kaardi taotluse rahuldamise või mitterahuldamise otsustab MO. Mobiil-ID kaardi taotluse rahuldamise või mitterahuldamise otsuse langetamisel lähtutakse sellest, kas kliendil on vastavalt MO tegutsemispiirkonna õigusaktidele õigus saada Mobiil-ID kaarti.

4.2.2 Sertifikaadi väljastamine

Mobiil-ID kaardi tootja laeb kaardile genereeritud võtmepaari salajased võtmed ja edastab avalikud võtmed MO-le, SK väljastab peale MO poolt edastatud sertifikaaditaotluse autentsuse ja terviklikkuse kontrolli taotlusele automaatselt vastavad sertifikaadid. Sertifikaat väljastatakse isikule Mobiil-ID kaardi väljastamisel.

Mobiil-ID kaardi väljastamisel klient nõustub Mobiil-ID sertifikaatide kasutustingimustega.

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

4.2.3 Sertifikaadi kontroll ja tõestamine

Vt CPS p.4.2.4.

4.2.4 Sertifikaadi uuendamine

Sertifikaatide uuendamist ei toimu. Aegunud või tühistatud sertifikaadid asendatakse uue Mobiil-ID kaardi väljastamisega.

4.3 Sertifikaadi kehtetuks tunnistamise ja peatamise taotlused

Vt CPS p.4.3.

4.4 Sertifikaatide peatamine

Vt CPS p.4.4.
Sertifikaatide peatamine toimub MO klienditeeninduspunktis või helistades abiliinile. Peataja isik tuvastatakse eelnevalt kasutades kliendi liitumislepingus olevaid andmeid.

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

4.5 Sertifikaadi peatatuse lõpetamine

Vt CPS p.4.5.
Sertifikaatide peatatuse lõpetamine on võimalik MO klienditeeninduspunktis.
Taotluse esitaja tuvastatakse vastavalt kehtivatele õigusaktidele.
Sertifikaadi peatatuse lõpetamise taotlus peab sisaldama:

- omaniku ja taotluse esitaja (kui erineb omanikust) eesnime ja perekonnanime;
- omaniku ja taotluse esitaja (kui erineb omanikust) isikukoodi;
- peatatuse lõpetamise alust.

MO klienditeeninduspunktis taotluse registreerimisel märgitakse üles taotluse esitaja isikutuvastamisel kasutatud dokumendi andmeid.

4.6 Sertifikaadi kehtetuks tunnistamine

4.6.1 Sertifikaadi kehtetuks tunnistamise volitused

Vt CPS p.4.6.1.
Sertifikaadi kehtetuks tunnistamise avalduse võib esitada MO ilma sertifikaadiomaniku osavõtuta järgmistel juhtdel:

- kliendi liitumisleping MO-ga lõpetatakse vastavalt MO üldtingimustele, kui klient on andnud selleks MO-le volituse;
- kliendi liitumisleping MO-ga lõpetatakse numbri omaniku algatusel;
- numbri omanik teeb kaardivahetuse;

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 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.

MO klienditeeninduspunktis taotluse registreerimisel märgitakse üles taotluse esitaja isikutuvastamisel kasutatud dokumendi andmeid.

4.6.3 Sertifikaadi kehtetuks tunnistamise menetlus

Vt CPS p.4.6.3.
Sertifikaatide kehtetuks tunnistamise taotluse saab esitada MO 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. Mobiil-ID kaartide hoiustamine

Mobiil-ID 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

6.1.2.1 Kliendi võtmete moodustamine

Võtmete moodustamisel kasutatakse RSA algoritmi võtmepikkusega 1024 bitti.

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

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

6.1.2.2 Kliendi isikliku võtme ja aktiveerimiskoodide kaitse

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

Aktiveerimiskoodid trükitakse ühes eksemplaris otse Mobiil-ID kaardi turvaalale, mis edastatakse avamata kliendile.

6.1.2.3 Kliendi salajaste võtmete kaitse

Vt CPS p.6.1.2.3.
Mobiil-ID salajaste võtmete kasutusfunktsioon lukustub kolme vale aktiveerimiskoodi (PIN-koodi) sisestamise järel. Funktsiooni lahtiblokeerimiseks on võimalik kasutada kliendile üleantud Mobiil-ID kaardi PUK-koodi.

Autentimis- ja allkirjastamisfunktsioonid lukustuvad üksteisest sõltumatult.

Funktsioon lukustub täielikult kolme vale PUK-koodi sisestamisel.

PUK-koodi kadumisel või kiipkaardi täielikul lukustumisel tuleb pöörduda MO klienditeeninduspunkti poole uue Mobiil-ID 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 toodud juhistele. Mobiil-ID väljastatavas sertifikaadis peavad vähemalt olema välja toodud järgmised andmed:

Väli	**OID**	**Kirjeldus**
Version		Sertifikaati formaadi tunnus: V3
Serial		Sertifikaadi järjekorra number, sertifitseerija poolt sertifikaadile antud unikaalne tunnusnumber
Issuer		
id-at-countryName	2.5.4.6	EE
id-at-organizationName	2.5.4.10	AS Sertifitseerimiskeskus
id-at-organizationalUnitName	2.5.4.11	Sertifitseerimisteenused
id-at-commonName	2.5.4.3	EID-SK 2007
Subject		
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	Kliendi unikaalne tunnus - üldnimi -kujul: <PEREKONNANIMI>,<EESNIMED>,<ISIKUKOOD>
id-at-organizationalUnitName	2.5.4.11	Digitaalset isikutuvastust võimaldavas sertifikaadis: mobile authentication Digitaalallkirjastamist võimaldavas sertifikaadis: mobile signature
id-at-organizationName	2.5.4.10	Mobiilteenuseoperaatori nimi
id-at-countryName	2.5.4.6	Sertifikaadi taotluses märgitud organisatsiooni asukoha riigi kood vastavalt RFC 3280 toodud juhistele.
Valid From		Sertifikaadi kehtivuse algusaeg. Informatsioon kodeeritud

Väli	OID	Kirjeldus
		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) või kui sertifikaadi taotlemisel esitatud dokumendi tähtaeg lõpeb enne seda aega, siis isikutuvastusel esitatud dokumendi kehtivusaja lõppu.
Public key		Avalik võti ASN.1 kujul koosneb 1024 bitisest moodulist ja 3 baidisest eksponendist (65537)
Public key algorithm	1.2.840.113549.1.1.1	Avaliku võtme krüptoalgoritm (RSA encryption).
Key Usage	2.5.29.15	Võtme kasutamisala. Digitaalset isikutuvastust võimaldavas sertifikaadis on seatud sellised võtmekasutust tähistavad attribuudid: 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 elektroonilist 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	2.5.29.3	Sertifitseerimispoliitika. Viide sertifikaadi väljastamisel lähtutud põhimõtetele. Viidatakse põhimõtete unikaalsele tunnusele - OID-le kui ka selle asukohale SK avalikul veebilehel: Policy Identifier= 1.3.6.1.4.1.10015.11.1.1.1 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
id-pe-qcStatements	1.3.6.1.5.5.7.1.3	Kvalifitseeritud sertifikaadi tunnus.

Väli	OID	Kirjeldus
		Laiendus, mis näitab, et sertifikaat on väljastatud vastavalt kvalifitseeritud sertifikaatidele sätestatud nõuetele (vt RFC 3739).
Thumbprint algorithm	1.2.840.113549. 1.1.5	Sertifikaadi räsi tüüp Räsimisel kasutatakse sha1 algoritmi.

7.2 Tühistusnimekirja (CRL-i) profiil

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

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	sha1WithRSAEncryption
signatureValue		5.1.1.3	signatuur
tBSCertList		5.1.2	
version		5.1.2.1	peab olema versioon 2
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-at-organizationalUnitName	2.5.4.11		Sertifitseerimisteenused
id-at-commonName	2.5.4.3		EID-SK 2007
thisUpdate		5.1.2.4	UTC aeg kuni 2049-ni, hiljem kasutatakse siin GeneralisedTime
nextUpdate		5.1.2.5	UTC aeg kuni 2049-ni, hiljem kasutatakse siin GeneralisedTime
revokedCertificates		5.1.2.6	
Invalidity Date	2.5.29.24		Peatamise/kehtetuks tunnistamise kuupäev
Reason code	2.5.29.21		Põhjus (peatatud sertifikaatide puhul „6”)
crlExtensions		5.1.2.7	
authorityKeyIdentifier			
CRL Number	2.5.29.20	5.2.3	Järjekorra number, sertifitseerija poolt sertifikaadile antud unikaalne tunnusnumber

Väljastatavad CRL-id peavad sisaldama kohustuslikult välju:
- Authority Key Identifier;
- CRL number.

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 STO 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] ning [2] avaldatakse SK koduleheküljel ja dokument [3] avaldatakse SK ja MO koduleheküljel.
Kõik muudatused kooskõlastatakse MO-ga

9 Viidatud ja seonduvad dokumendid

Viidatud dokumendid:

[1] AS-i 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

Seonduvad dokumendid:

- AS-i Sertifitseerimiskeskus infoturbepoliitika
- AS-i Sertifitseerimiskeskus käideldavuse strateegia ja poliitika
- AS-i Sertifitseerimiskeskus IT süsteemide taastamise poliitika