ESTEID sertifitseerimispoliitika

Versioon 1.2

OID: 1.3.6.1.4.1.10015.1.1.1.1

Nõuded Eesti Vabariigi siseriiklikule isikutunnistusele digitaalallkirja ja isikutuvastust võimaldavate sertifikaatide väljastamiseks ja teenindamiseks

Versioonid ja muudatused:

Versioon	Kuupäev	Kommentaarid
1.1	10.11.2001	PROJEKT
1.2	17.10.2002	Ühitatud SK CPS-iga. Lisatud sertifikaadi uuendamist, ID-kaardi aktiveerimiskoodide muutmist käsitlev temaatika.

Sisukord

SISUKORD **2**

1 SISSEJUHATUS **4**

1.1 ÜLEVAADE 4
1.2 SERTIFITSEERIMISPÕHIMÕTETE IDENTIFITSEERIMINE 4
1.3 ORGANISATSIOON JA KASUTUSVALDKOND 5
1.3.1 Sertifitseerimiskeskus (SK) *5*
1.3.2 SK registreerimiskeskus *5*
1.3.3 EV Siseministeerium *5*
1.3.4 Kasutaja *6*
1.3.5 Sertifikaatide kasutusvaldkond *6*
1.4 KONTAKTANDMED 6

2 ÜLDTINGIMUSED **7**

2.1 KOHUSTUSED JA NÕUDED 7
2.1.1 SK kohustused *7*
2.1.2 Registreerimiskeskuse kohustused *8*
2.1.3 Siseministeeriumi kohustused *8*
2.1.4 Nõuded kliendile *9*
2.1.5 Nõuded huvitatud isikule *9*
2.1.6 Nõuded kataloogiteenusele *9*
2.2 VASTUTUS 9
2.2.1 SK vastutus *9*
2.2.2 Registreerimiskeskuse vastutus *9*
2.2.3 Siseministeeriumi vastutus *10*
2.2.4 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 10
2.7 OMANDIÕIGUSED 10

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 11

4.2.1 Otsuse tegemine *11*
4.2.2 Sertifikaadi väljastamine *12*
4.2.3 ID-kaardi väljastamine. Sertifikaatide aktiveerimine. *12*
4.2.4 Sertifikaadi kontroll ja tõestamine *12*
4.2.5 Sertifikaadi uuendamine *12*
4.3 SERTIFIKAADI KEHTETUKS TUNNISTAMISE JA PEATAMISE TAOTLUSED 13
4.4 SERTIFIKAATIDE PEATAMINE 13
4.5 SERTIFIKAADI PEATATUSE LÕPETAMINE 13
4.6 SERTIFIKAADI KEHTETUKS TUNNISTAMINE 13
4.6.1 Sertifikaadi kehtetuks tunnistamise volitused *13*
4.6.2 Sertifikaadi kehtetuks tunnistamise avalduse esitamine *13*
4.6.3 Sertifikaadi kehtetuks tunnistamise menetlus *13*
4.6.4 Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus *13*
4.7 PROTSEDUURID JÄLGITAVUSE TAGAMISEKS 13
4.8 TEGUTSEMINE ERIOLUKORRAS 13
4.9 SERTIFITSEERIMISTEENUSE OSUTAJA TÖÖ LÕPETAMINE 13

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. ID-kaartide transport ja hoiustamine *14*
5.3 NÕUDED TÖÖPROTSEDUURIDELE 14
5.4 PERSONALI TURBENÕUDED 14

6 TEHNILISED TURBENÕUDED 14

6.1 VÕTMEHALDUS 14
6.1.1 SK kinnitusvõtmed *14*
6.1.2 Kliendi võtmed *14*
6.2 SÜSTEEMITURVE 15
6.3 SERTIFITSEERIMISTEENUSE OSUTAMISEKS KASUTATAVATE TEHNILISTE VAHENDITE KIRJELDUS 15
6.4 SERTIFITSEERIMISTEENUSE OSUTAMISEL TEKKINUD ANDMETE SÄILITAMINE JA KAITSE 16

7 SERTIFIKAATIDE JA TÜHISTUSNIMEKIRJADE (CRLIDE) TEHNILISED PROFIILID 16

7.1 SERTIFIKAATIDE PROFIIL 16
7.1.1 Sertifikaatide loetelu ja otstarve *16*
7.2 TÜHISTUSNIMEKIRJAD (CRL) 16

8 SERTIFITSEERIMISPOLIITIKA HALDUS 17

9 KASUTATUD TERMINOLOOGIA 17

10 KASUTATUD LÜHENDID 17

11 VIIDATUD DOKUMENDID 17

1 Sissejuhatus

1.1 Ülevaade

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

Käesolev CP rajaneb dokumendile „AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted versioon 1.2“ [1], mis on registreeritud sertifitseerimisteenuse osutajate riiklikus registris. Need sertifitseerimispõhimõtted (edaspidi: 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 digitaalsetele sertifikaatidele.

Käesolev CP koostamisel on kasutatud IETFi (*Internet Engineering Task Force*) soovitusliku dokumenti RFC 2527 [5].

1.2 Sertifitseerimispoliitika identifitseerimine

Käesoleva CP tunnuskood on **OID: 1.3.6.1.4.1.10015.1.1.1.1**

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	1.1
CP versiooni tunnus	1.1

Tabel 1. CP tunnuskoodi koostamine

1.3 Organisatsioon ja kasutusvaldkond

1.3.1 Sertifitseerimiskeskus (SK)

Vt CPS p.1.2.1.

SK on Siseministeeriumile lepinguliselt delegeerinud ülesanded, mida kirjeldatakse punktis 1.3.3.

1.3.2 SK registreerimiskeskus

1.3.2.1 SK klienditeeninduspunkt

Vt CPS p.1.2.2.1.

SK klienditeeninduspunkt ei võta vastu sertifikaaditaotlusi (ID-kaardi taotlusi).

SK klienditeeninduspunkt lähtub oma töös SK ja Siseministeeriumi poolt kokkulepitud ajalistest piirangutest.

1.3.2.2 Abiliin

Vt CPS p.1.2.2.2.

Abiliin kasutab isiku tuvastamiseks protseduurireegleid, mis on määratletud sisemiste dokumentidega. Täiendavat informatsiooni saab veebilehelt http://www.pass.ee.

Abiliin annab täiendavalt vajadusel vastava abiliini kontaktandmed, kes tegeleb ID-kaardiga seotud probleemide lahendamisega.

1.3.3 EV Siseministeerium

Siseministeerium:

- võtab vastu ID-kaardi taotlusi kontrollib nende autentsust ja terviklikkust;
- hangib tootjalt klientidele edastatavate kiipkaartide toorikud (ID-kaardi toorikud);
- lisab kiipkaarditoorikutele visuaalsed kujunduselemendid ja turvaelemendid ning salvestab võtmete ja sertifikaatide vastuvõtmiseks vajaliku tarkvara ja andmestruktuurid;
- personaliseerib ID-kaardi kliendi info pealetrükkimise teel ja vastava andmestruktuuri loomise teel;
- loob kaartide aktiviseerimisinfo;
- genereerib võtmepaarid ning salvestab isiklike võtmete ainukesed koopiad kiipkaardile;
- salvestab kiipkaardile andmed kaardi omaniku kohta;

- genereerib ID kaardi taotluses esitatud andmete põhjal sertifikaaditaotlused ja edastab need sertifitseerijale;
- salvestab SK poolt vastusena saabunud sertifikaadid kiipkaardile;
- väljastab vastavalt Siseministeeriumis kehtestatud korras sätestatud juhtudel ID-kaarte.

Siseministeerium juhindub oma töös SK-ga kokku lepitud ajalistest piirangutest. Siseministeerium tagab sisemiste turbeprotseduuridega turvalisuse enda kohustuste täitmisel.

1.3.4 Kasutaja

1.3.4.1 Klient

Vt CPS p.1.2.3.1.

Klient on füüsiline isik, kellele väljastatakse avaliku teenusena sertifikaate, kui ta on Siseministeeriumi poolt määratud ID-kaardi omamisõigusega isik.

Klient on käesoleva CP alusel väljastatud sertifikaadi omanik.

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

1.3.4.2 Huvitatud isik

Vt CPS p.1.2.3.2.
Huvitatud isik peab lisaks olema eelnevalt tutvunud käesoleva CP-ga.

1.3.5 Sertifikaatide kasutusvaldkond

Vt CPS p.1.2.4.
Käesolev CP alusel väljastatakse kahte tüüpi sertifikaate:

a) sertifikaate digitaalseks allkirjastamiseks
b) sertifikaate isiku digitaalseks tuvastamiseks

Sertifikaate digitaalseks allkirjastamiseks saab kasutada digitaalseks allkirjastamiseks DAS [3] mõttes.

CP ei sea piiranguid sertifikaatide kasutamiseks erinevates tarkvararakendustes ega rakendusvaldkondades.

1.4 Kontaktandmed

Vt CPS p.1.3.

Sertifitseerimiskeskus
AS Sertifitseerimiskeskus
Äriregistri kood 10747013

Pärnu mnt 12, 10148 Tallinn
Telefon +372 610 1880
Faks +372 610 1881
E-post: pki@sk.ee
http://www.sk.ee/

tasuta abiliin: telefon 1777

Klienditeeninduspunktid

Klienditeeninduspunktide kontaktandmed on toodud veebilehel http://www.sk.ee.

Siseministeerium

EV Siseministeerium
Pikk 61, 15065 Tallinn
Telefon: +372 612 5007/008
Faks: +372 612 5087
E-post: sisemin@sisemin.gov.ee

Siseministeeriumi abiliin isikutunnistustega seotud probleemide lahendamiseks ja SK klienditeeninduspunktide töötajate nõustamiseks

tasuta abiliin: telefon 612 6970
Kontaktandmete muutumisel teavitatakse sellest koheselt SK koduleheküljel http://www.sk.ee .

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:

- võtma vastu ja rahuldama SM sertifikaaditaotlused üle elektroonse turvalise andmesidekanali kokkulepitud protokolli alusel;
- edastama SM-le andmed klienditeeninduspunktis väljastatud ja tagastatud ID-kaartide kohta;
- osutama ööpäevaringset kataloogiteenust;

- 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;
- juhinduma SM-ga kokkulepitud ajalistest piirangutest.

2.1.2 Registreerimiskeskuse kohustused

2.1.2.1 SK klienditeeninduspunkti kohustused

Vt CPS p.2.1.2.1.
Klienditeeninduspunkt kohustub täiendavalt:

- väljastama kliendile ID-kaardi, eelnevalt aktiveerides sinna laetud sertifikaadid;
- tagama esmase nõustamise ja abistamise ID-kaartide käsitlemisel;
- juhinduma töös SM ja SK poolt kokkulepitud ajalistest piirangutest.

2.1.2.2 Abiliini kohustused

Vt CPS p.2.1.2.2.

2.1.3 Siseministeeriumi kohustused

Siseministeerium kohustub:

- võtma klientidelt vastu taotlusi ID-kaardi ja sertifikaatide väljastamiseks ning kontrollib kliendi poolt edastatud andmete õigsust ja terviklikkust;
- tagama ID-kaartide personaliseerimise;
- oma sertifitseerimissüsteemiga seotud infosüsteemi osas järgima käideldavuse ja turbenõudeid, mis vastavad vähemalt käesolevas poliitikas toodud nõuetele;
- tagama, et töötajatel, kes võtavad vastu ID-kaardi avaldusi ja/või on seotud sertifitseerimisteenust puudutava informatsiooniga, ei ole karistatust tahtlikult toimepandud kuriteo eest;
- tagama ID-kaarti kasutamist puudutavate infovoldikute ja/või infomaterjali ning sertifikaatide kasutamise tingimuste kättesaadavuse;
- informeerima klienti avaldusele antud negatiivse otsuse puhul;
- esitama SK-le sertifikaatide väljastamiseks vajalikud autentsed ja terviklikud sertifikaaditaotlused;

- edastama SK-le ettevalmistatud ID-kaardid nende klienditeeninduspunktidesse toimetamiseks;
- väljastama Siseministeeriumis kehtestatud korras sätestatud juhtudel kliendile ID-kaardi, eelnevalt aktiveerides sinna laetud sertifikaadid
- tagama isikutunnistusi puudutava informatsiooni kättesaadavuse avalikus andmesidevõrgus aadressil http://www.pass.ee.

Siseministeerium juhindub oma töös oma ja SK-ga kokku lepitud ajalistest piirangutest.

2.1.4 Nõuded kliendile

Vt CPS p.2.1.3.
Klient peab järgima SK poolt käesolevas CPs kehtestatud protseduure.

Klient peab edastama Siseministeeriumile ID-kaardi taotluse esitamisel õiget informatsiooni ning isikuandmete muutumise korral teatab õiged andmed Siseministeeriumisse vastavalt kehtestatud reeglite kohaselt.

2.1.5 Nõuded huvitatud isikule

Vt CPS p.2.1.4.
Huvitatud isik peab arvestama sertifikaadi aktsepteerimisega seotud kohustuste ja riskidega, mis on toodud käesolevas CP-s.

2.1.6 Nõuded kataloogiteenusele

Vt CPS p.2.1.5.

2.2 Vastutus

2.2.1 SK vastutus

Vt CPS p.2.2.1.
SK on vastutav kõigi punktis 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 Klienditeeninduspunkti vastutus

Vt CPS p.2.2.2.1.
Klienditeeninduspunkt vastutab kõigi punktis 2.1.2.1 toodud kohustuste täitmise eest.

2.2.2.2 Abiliini vastutus

Vt CPS p.2.2.2.2.
Abiliin vastutab kõigi punktis 2.1.2.2 toodud kohustuste täitmise eest.

2.2.3 Siseministeeriumi vastutus

Siseministeerium vastutab kõigi punktis 2.1.3 toodud 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 kataloogiteenuse kaudu ja aadressil http://www.sk.ee/crls/esteid/crl.crl.

2.4.2 Avaldamise sagedus

Vt CPS p.2.4.2.

Sertifikaatide tühistusnimekirju avaldatakse reeglina 10 minuti jooksul peale peatamise esitamist või kehtetuks tunnistamise avalduse rahuldamist. Garanteeritud avaldamise sagedus on 12,5 tundi.

2.4.3 Juurdepääsureeglid

Vt CPS p.2.4.3.

2.4.4 Kataloogiteenus

Vt CPS p.2.4.4.

2.5 Audit

Vt CPS p.2.5.
Välisauditi tulemused avaldatakse SK koduleheküljel.

2.6 Konfidentsiaalsus

Vt CPS p.2.6.

2.7 Omandiõigused

AS Sertifitseerimiskeskus omab sertifitseerimisteenuse osutamisel kasutatavale tehnilisele terviklahendusele ja dokumentatsioonile kõiki õigusi, sealhulgas omandi- ja varalisi autoriõigusi.

3 Kliendi identifitseerimine

3.1 Kliendi isikusamasuse kontroll

Kliendi isikusamasust kontrollitakse vastavalt Siseministeeriumis kehtestatud protseduurireeglitele. Täiendavat informatsiooni saab veebilehelt http://www.pass.ee.

3.2 Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord

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

3.3 Eraldusnimi

Vt CPS p.3.3.
Kliendi eraldusnimi koostatakse vastavalt dokumendile "Sertifikaadid Eesti Vabariigi isikutunnistusel" [2].

4 Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtajad

4.1 Sertifikaaditaotluse esitamine

Vt CPS p.4.1.
Kui kliendil ei ole kehtivate sertifikaatidega ID-kaarti, siis taotluse sertifikaadi saamiseks esitab klient Siseministeeriumi allasutuse KMA regionaalosakonnas ID-kaardi avalduses, mille menetlemise reeglid määrab Siseministeerium.
Klient täidab KMA regionaalbüroos blanketi isikutunnistuse taotlemiseks ning allkirjastab selle. Allkirjastatud blankett isikutunnistuse taotlemiseks on sertifikaaditaotluse koostamise aluseks.

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

4.2 Sertifikaaditaotluse menetlemine

ID-kaardi taotluse avalduse täpne läbivaatamise kord ja töötlemise tähtajad on ära määratud Siseministeeriumis kehtestatud korra alusel. Sertifikaaditaotluse avalduse menetlemisel kontrollitakse kliendi poolt esitatud andmete õigsust ja täielikkust.

4.2.1 Otsuse tegemine

Vt CPS p.4.2.1.

ID-kaardi taotluse avalduse rahuldamise või mitterahuldamise otsustab Siseministeerium. Kehtivate sertifikaatidega ID-kaardile uute sertifikaatide taotluse avalduse rahuldamise või mitterahuldamise otsustab STO.

ID-kaardi taotluse avalduse rahuldamise või mitterahuldamise otsuse langetamisel lähtutakse sellest, kas kliendil on vastavalt EV õigusaktidele õigus saada ID-kaarti.

Positiivse otsuse korral moodustab Siseministeerium Kliendile võtmepaarid ning koostab neile vastavad sertifikaaditaotlused digitaalset allkirja ja isikutuvastust võimaldava sertifikaadi väljastamiseks ja saadab need SK-le.

4.2.2 Sertifikaadi väljastamine

SK väljastab automaatselt peale Siseministeeriumi poolt edastatud sertifikaaditaotluse autentsuse ja terviklikkuse kontrolli taotlusele vastavad sertifikaadid, mis laetakse Siseministeeriumis ID-kaardile.

Kõik väljastatud sertifikaadid on aktiveerimata olekus, st nad pole kätte saadavad punktis 2.1.6 viidatud avalikus kataloogis, vaid asuvad SK infosüsteemi suletud osas asuvas sertifikaatide andmebaasis.

Kehtivate sertifikaatidega ID-kaardile uute sertifikaatide taotlemisel väljastatakse uued sertifikaadid ID-kaardile klienditeeninduspunktis või SK koduleheküljel olevas rakenduses.

4.2.3 ID-kaardi väljastamine. Sertifikaatide aktiveerimine.

ID-kaardi väljastamine kliendile toimub SK klienditeeninduspunktis selle lahtiolekuaegadel.

Koos ID-kaardi väljastamisega aktiveerib SK klienditeeninduspunkti klienditeenindaja ID-kaardile laetud sertifikaadid.

SK klienditeeninduspunkti töötaja annab kliendile üle ID-kaardi aktiveerimiseks vajalikud aktiveerimiskoode sisaldava turvaümbriku.

Klient allkirjastab (alla 16 aastase puhul tema seaduslik esindaja) ID-kaardi väljastamise akti-blanketi.

Kehtivate sertifikaatidega ID-kaardile uute sertifikaatide laadimisel aktiveeritakse sertifikaadid koheselt peale nende laadimist kiipkaardile.

4.2.4 Sertifikaadi kontroll ja tõestamine

Vt CPS p.4.2.4.

4.2.5 Sertifikaadi uuendamine

ID-kaardi sertifikaate ei uuendata. Aegunud või tühistatud sertifikaate on võimalik asendada uuesti genereeritud võtmepaari põhjal väljastatud sertifikaatidega.

4.3 Sertifikaadi kehtetuks tunnistamise ja peatamise taotlused

Vt CPS p.4.3.

4.4 Sertifikaatide peatamine

Vt CPS p.4.4.

4.5 Sertifikaadi peatatuse lõpetamine

Vt CPS p.4.5.

4.6 Sertifikaadi kehtetuks tunnistamine

4.6.1 Sertifikaadi kehtetuks tunnistamise volitused

Vt CPS p.4.6.1.
Sertifikaadi kehtetuks tunnistamise avalduse võib esitada Siseministeeriumi esindaja peale ID-kaardi tühistamist või muu õigusaktides toodud isik.

4.6.2 Sertifikaadi kehtetuks tunnistamise avalduse esitamine

Vt CPS p.4.6.2.

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. ID-kaartide transport ja hoiustamine

ID-kaardi transport ja hoiustamine toimub pangakaartide transpordi ja hoiustamisega võrdsustatud turvatasemel.

ID-kaardi transport toimub relvastatud saatjaga.

ID-kaarte hoiustatakse SK klienditeeninduspunkti raudkapis.

5.3 Nõuded tööprotseduuridele

Vt CPS p.5.3.

5.4 Personali turbenõuded

Vt CPS p.5.4.

6 Tehnilised turbenõuded

6.1 Võtmehaldus

6.1.1 SK kinnitusvõtmed

Vt CPS p.6.1.1.

6.1.2 Kliendi võtmed

6.1.2.1 Kliendi võtmete moodustamine

Võtmete moodustamisel kasutatavad algoritmid, võtmepikkused ja teised parameetrid on toodud dokumendis “Sertifikaadid EV isikutunnistusel”.

Võtmed luuakse ID-kaardi personaliseerimise ajal ning sertifikaatide asendamisel Siseministeeriumis ja salvestatakse kaardi vastavasse turvaalasse. Loodud võtmeid ei ole võimalik kaardist eraldada ega taastada.

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

6.1.2.2 Kliendi isikliku võtme ja aktiveerimiskoodide kaitse personaliseerimise käigus

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

Aktiveerimiskoodid trükitakse ühes eksemplaris otse turvaümbrikusse, mis edastatakse avamata kliendile.

6.1.2.3 Kliendi salajase võtme aktiveerimine

Vt CPS p.6.1.2.3.
Kiipkaart lukustub kolme vale aktiveerimiskoodi (PIN-koodi) sisestamise järel.
Kiipkaardi lahtiblokeerimiseks on võimalik kasutada kliendile üleantud ID-kaardi PUK-koodi.
Kiipkaart lukustub täielikult kolme vale PUK-koodi sisestamisel.
PUK-koodi kadumisel või kiipkaardi täielikul lukustumisel tuleb pöörduda SK klienditeeninduspunkti poole.

6.1.2.4 Kliendi võtmete hävitamine

Sertifikaatide tühistamise või kehtivuse lõpu järel saab Siseministeerium ainult Siseministeeriumile teada oleva salakoodi abil kiipkaarti algväärtustada sellest kogu kasutajakohase informatsiooni kustutamise teel.
Kiipkaardi algväärtustamise järel ei ole sellest võtmete eraldamine võimalik.

6.1.2.5 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 Sertifikaatide profiil

7.1.1 Sertifikaatide loetelu ja otstarve

Isikutunnistusele kantakse kaks isikusertifikaati:
1) sertifikaat digitaalseks allkirjastamiseks
2) sertifikaat isiku digitaalseks tuvastamiseks

Sertifikaat isiku digitaalseks tuvastamiseks peab olema välja antud teenuse osutaja poolt, kes vastab Teede- ja Sideministeeriumi määruses "**Teenuse osutajate infosüsteemide auditeerimise kord**" esitatud nõuetele.

Sertifikaat digitaalseks allkirjastamiseks peab olema välja antud digitaalallkirja seaduses [3] esitatud nõuetele vastava sertifitseerimisteenuse osutaja poolt.

Sertifikaat isiku digitaalseks tuvastamiseks on ette nähtud selle omaniku autentimiseks mistahes elektroonilist isikutuvastust nõudvas suhtluses.

Sertifikaat digitaalseks allkirjastamiseks on selle omanikule ette nähtud digitaalallkirjade andmiseks Eesti Digitaalallkirja seaduse mõttes.

Isikutunnistusele kantud isikusertifikaadid kehtivad kuni **1100 päeva** (3 aastat ja 4 päeva), kuid mitte kauem isikutunnistuse kehtivuse lõpptähtajast.

Sertifikaatide täpne profiil on toodud dokumendis "Sertifikaadid Eesti Vabariigi isikutunnistusel" [2].

7.2 Tühistusnimekirjad (CRL)

Sertifikaatide tühistusnimekirja (*CRL*) formaadiks on x.509v2 (defineeritud RFC2459-s [4]).

Tühistusnimekirja täpne profiil on toodud dokumendis "Sertifikaadid Eesti Vabariigi isikutunnistusel" [2].

8 Sertifitseerimispoliitika haldus

Sertifitseerimispoliitika sisulist tähendust mitte muutvate paranduste puhul nagu õigekirjavigade parandamine, tõlkimine ja kontaktandmete ajakohastamine, tuleb muudatused dokumenteerida käesoleva dokumendi Muudatused - sektsioonis ning suurendada dokumendi versiooninumbri murdarvulist osa.

Sisuliste muudatuste puhul peab uus sertifitseerimispoliitika versioon olema eelnevatest selgelt eristatav. Uus versioon peab kandma ühe võrra suurendatud versiooninumbrit. Muudetud sertifitseerimispoliitika koos kehtima hakkamise päevaga, mis ei või olla varasem, kui 30 päeva avaldamisest, tuleb avaldada elektrooniliselt SK koduleheküljel

Kõik muudatused kooskõlastatakse Siseministeeriumiga.

9 Kasutatud terminoloogia

Vt CPS p.9.

10 Kasutatud lühendid

Vt CPS p.10.

Lühend	Definitsioon
KMA	Kodakondsus- ja –Migratsiooniamet
SM	Siseministeerium

11 Viidatud ja seonduvad dokumendid

Viidatud dokumendid:

[1] AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtted (CPS)
[2] Sertifikaadid Eesti Vabariigi isikutunnistusel
[3] Eesti Vabariigi digitaalallkirja seadus, RT 1 2000, 26, 150.
[4] RFC 2459 – Request For Comments 2459, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile; http://www.ietf.org/rfc
[5] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

Seonduvad dokumendid:

- AS-i Sertifitseerimiskeskus infoturbepoliitika
- AS-i Sertifitseerimiskeskus käideldavuse strateegia ja poliitika
- AS-i Sertifitseerimiskeskus IT süsteemide taastamise poliitika
- Andmekogude seadus, RT 1 1997, 28, 423
- Isikut tõendavate dokumentide seadus, RT 1 1999,25,365
- Isikuandmekaitse põhimõtted
- Isikuandmete kaitse seadus RT 1 1996, 48, 944.