

ESTEID sertifitseerimispoliitika

Versioon 2.0

OID: 1.3.6.1.4.1.10015.1.1.2.0

Nõuded Eesti Vabariigi siseriiklikule isikutunnistusele digitaalkirja ja isikutuvastust võimaldavate sertifikaatide väljastamiseks ja teenindamiseks.

Versioonid ja muudatused:

Versioon	Kuupäev	Kommentaariid
1.1	10.11.2001	PROJEKT
1.2	17.10.2002	Ühitatud SK CPS-iga. Lisatud sertifikaadi uuendamist, ID-kaardi aktiveerimiskoodide muutmist käsitlev temaatika.
2.0	19.06.2006	Muudatused vastavalt uuele lepingustruktuurile.

Sisukord

SISUKORD.....	2
SISSEJUHATUS.....	4
ÜLEVAADE.....	4
KASUTATUD TERMINOLOOGIA.....	4
KASUTATUD LÜHENDID.....	4
SERTIFITSEERIMISPOLIITIKA IDENTIFITSEERIMINE.....	5
ORGANISATSIOON JA KASUTUSVALDKOND.....	5
<i>Sertifitseerimiskeskus (SK)</i>	5
<u>1.1.1 SK registreerimiskeskus</u>	<u>5</u>
<i>KMA</i>	6
<i>Kaardi isikustaja – TRÜB</i>	6
<i>Kasutaja</i>	6
<i>Sertifikaatide kasutusvaldkond</i>	6
KONTAKTANDMED.....	7
ÜLDTINGIMUSED.....	8
KOHUSTUSED JA NÕUDED.....	8
<i>SK kohustused</i>	8
<i>Registreerimiskeskuse kohustused</i>	8
<i>KMA kohustused</i>	9
<i>Nõuded kliendile</i>	9
<i>Nõuded huvitatud isikule</i>	9
<i>Nõuded kataloogiteenusele</i>	9
VASTUTUS.....	9
<i>SK vastutus</i>	9
<i>Registreerimiskeskuse vastutus</i>	10
<i>KMA vastutus</i>	10
<i>Vastutuse piirid</i>	10
VAIDLUSTE LAHENDAMINE.....	10
INFORMATSIOONI AVALDAMINE JA KATALOOGITEENUS.....	10
<i>SK informatsiooni avaldamine</i>	10
<i>Avaldamise sagedus</i>	10
<i>Juurdepääsureeglid</i>	10
<i>Kataloogiteenus</i>	10
AUDIT.....	11
KONFIDENTSIAALSUS.....	11
KLIENDI IDENTIFITSEERIMINE.....	11
KLIENDI ISIKUSAMASUSE KONTROLL.....	11
SERTIFIKAADI TAOTLEJA AVALIKULE VÕTMELE VASTAVAISIKLIKU VÕTME TÕENDAMISE KORD.....	11
ERALDUSNIMI.....	11
SERTIFITSEERIMISTEENUSE OSUTAMINE.	
SERTIFITSEERIMISMENETLUSE KORD JA TÄHTAJAD.....	11
SERTIFIKAADITAOTLUSE ESITAMINE.....	11
<u>1.2 SERTIFIKAADITAOTLUSE MENETLEMINE</u>	<u>11</u>
<i>Otsuse tegemine</i>	12

<i>Sertifikaadi väljastamine</i>	12
<i>ID-kaardi väljastamine. Sertifikaatide aktiveerimine.</i>	12
<i>Sertifikaadi kontroll ja tõestamine.</i>	12
<i>Sertifikaadi uuendamine.</i>	12
SERTIFIKAADI KEHTETUKS TUNNISTAMISE JA PEATAMISE TAOTLUSED.....	13
SERTIFIKAATIDE PEATAMINE.....	13
SERTIFIKAADI PEATATUSELÕPETAMINE.....	13
SERTIFIKAADI KEHTETUKS TUNNISTAMINE.....	13
<i>Sertifikaadi kehtetuks tunnistamise volitused.</i>	13
<i>Sertifikaadi kehtetuks tunnistamise taotluse esitamine.</i>	13
<i>Sertifikaadi kehtetuks tunnistamise menetlus.</i>	13
<i>Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus.</i>	14
PROTSEDUURID JÄLGITAVUSE TAGAMISEKS.....	14
TEGUTSEMINE ERIOLUKORRAS.....	14
SERTIFITSEERIMISTEENUSE OSUTAJA TÖÖ LÕPETAMINE.....	14
FÜÜSILISED JA ORGANISATSIOONILISED TURBEMEETMED.....	14
TURBEHALDUS.....	14
FÜÜSILISED TURBEMEETMED.....	14
<i>SK füüsiline pääsukontroll.</i>	14
<i>Muud nõuded. ID-kaartide hoiustamine.</i>	14
NÕUDED TÖÖPROTSEDUURIDELE.....	14
PERSONALI TURBENÕUDED.....	14
TEHNILISED TURBENÕUDED.....	15
VÕTMEHALDUS.....	15
<i>SK kinnitusvõtmed.</i>	15
<i>Kliendi võtmed.</i>	15
SÜSTEEMITURVE.....	15
SERTIFITSEERIMISTEENUSE OSUTAMISEKS KASUTATAVATE TEHNILISTE VAHENDITE KIRJELDUS.....	16
SERTIFITSEERIMISTEENUSE OSUTAMISEL TEKKINUD ANDMETE SÄILITAMINE JA KAITSE.....	16
SERTIFIKAATIDE JA TÜHISTUSNIMEKIRJADE (CRLIDE) TEHNILISED PROFIILID.....	16
SERTIFITSEERIMISPOLIITIKA HALDUS.....	16
VIIDATUD JA SEONDUVAD DOKUMENDID.....	16

Sissejuhatus

Ülevaade

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

Käesolev CP rajaneb dokumendile „AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted versioon 2.0“ [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 vastulu 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 [4].

Kasutatud terminoloogia

Vt CPS p.10.

Termin	Definitsioon
Klienditeeninduspunkt	Käesoleva CP alusel toimiv SK ja/või KMA klienditeeninduspunkt sertifitseerimisega seotud teenuste osutamiseks, vt punkt 1.5.2.1
Isikutunnistuse sertifikaatide kasutustingimused	Dokument, mis sisaldab kliendi kohustusi ja vastutust ID-kaardi ja sellega seotud sertifikaatide kasutamisel. Klient peab ID-kaardi väljastamisel olema tutvunud ja aktsepteerima selles dokumendis toodud nõudeid.

Kasutatud lühendid

Vt CPS p.11.

Lühend	Definitsioon
KMA	Kodakondsus- ja –Migratsiooniamet
SM	Siseministerium
TRÜB	ID-kaardi plangi tootja ja isikustaja
SK	AS Sertifitseerimiskeskus, sertifitseerimisteenuse osutaja.

Sertifitseerimispoliitika identifitseerimine

Käesoleva CP tunnuskoode on **OID: 1.3.6.1.4.1.10015.1.1.2.0**

CP tunnuskoode on koostatud vastavalt järgnevale tabelile 1.

Parameeter	Viide OIDs
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	2.0

Tabel 1. CP tunnuskoode koostamine

Organisatsioon ja kasutusvaldkond

Sertifitseerimiskeskus (SK)

Vt CPS p.1.2.1.

TRÜB on Kodakondsus- ja Migratsiooniametile (edaspidi KMA) lepinguliselt delegeerinud ülesanded, mida kirjeldatakse punktis 1.3.3.

1.1.1 SK registreerimiskeskus

1.1.1.1 Klienditeeninduspunktid

Vt CPS p.1.2.2.1.

ID-kaartide taotluste vastuvõtmine ja ID-kaartide väljastamine toimub KMA regionaalosakondades ja büroodes ning Eesti välisesindustes (edaspidi KMA klienditeeninduspunkt), mille täpne loetelu ja lahtiolekuajad tuuakse ära KMA ja SK kodulehekülgedel.

ID-kaartidega seotud sertifikaatide teenindamine (sertifikaatide uuendamine, peatamine, peatuse lõpetamine, kehtetuks tunnistamine, asendus PIN määramine toimub KMA ja SK klienditeeninduspunktides, mille täpne loetelu ja lahtiolekuajad tuuakse ära KMA ja SK kodulehekülgedel.

1.1.1.2 Abiliin

Vt CPS p.1.2.2.2.

Abiliin kasutab isiku tuvastamiseks protseduurireegleid, mis on määratletud sisemiste dokumentidega.

Abiliin annab vajadusel täiendavalt ID-kaardiga seotud probleemide lahendamiseks tegeleva abiliini kontaktandmed.

KMA

KMA:

- edastab TRÜB-ile ID-kaardi tellimusi;
- edastab ID-kaarte klienditeeninduspunktidele.

KMA juhindub oma töös lepingus kokku lepitud ajalistest piirangutest.

KMA tagab turvalisuse enda kohustuste täitmisel sisemiste turbeprotseduuridega.

Kaardi isikustaja – TRÜB

TRÜB:

- võtab vastu ID-kaardi tellimusi;
- isikustab ID-kaardi;
- moodustab ID-kaardi võtmed ja taotleb nendele vastavad sertifikaadid;
- laeb sertifikaadid ID-kaardile;
- annab isikustatud ID-kaardid KMA-le üle.

TRÜB juhindub oma töös lepingus kokku lepitud ajalistest piirangutest.

TRÜB tagab turvalisuse enda kohustuste täitmisel sisemiste turbeprotseduuridega.

Kasutaja

1.1.1.3 Klient

Vt CPS p.1.2.3.1.

Klient on füüsiline isik, kellele väljastatakse avaliku teenusena sertifikaate, kui tal on selleks seadusjärgne õigus.

Klient on käesoleva CP alusel väljastatud sertifikaadi omanik.

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

Kliendil peab olema võimalus enne ID-kaardi väljastamist tutvuda isikutunnistuse sertifikaatide kasutustingimustega [5].

1.1.1.4 Huvitatud isik

Vt CPS p.1.2.3.2.

Sertifikaatide kasutusvaldkond

Vt CPS p.1.2.4.

Käesoleva 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.

Kontaktandmed

Vt CPS p.1.3.

SK

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/>

Abiliin

telefon 1777, (0) 630 4084

Klienditeeninduspunktid

Klienditeeninduspunktide kontaktandmed on toodud veebilehel <http://www.sk.ee> ja <http://www.mig.ee>.

KMA

Endla 13,
15179 Tallinn
Info: (372) 612 6979
Üldtel.: (372) 612 6901
Faks: (372) 631 3744
E-post: kma@mig.ee

KMA abiliin isikutunnistustega seotud probleemide lahendamiseks ja SK klienditeeninduspunktide töötajate nõustamiseks

Tasuta abiliin tööpäevadel kella 09.00-17.00: telefon 612 6970

Kontaktandmete muutumisel teavitatakse sellest koheselt SK koduleheküljel <http://www.sk.ee> ja KMA koduleheküljel <http://www.mig.ee>.

TRÜB

Trüb Baltic AS
Liivalaia 8
10118 Tallinn
Telefon +372 613 29 11
Faks +372 613 29 20
E-post info@trueb.ee

Üldtingimused

Kohustused ja nõuded

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 Trübist tulnud sertifikaaditaotlusi ja väljastama neile vastavaid sertifikaate;
- 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 töös lepingus kokkulepitud ajalistest piirangutest.

Registreerimiskeskuse kohustused

1.1.1.5 KMA klienditeeninduspunkti kohustused

Vt CPS p.2.1.2.1.

KMA klienditeeninduspunkt kohustub täiendavalt:

- väljastama kliendile ID-kaardi aktiveerides sinna laetud sertifikaadid;
- tagama esmase nõustamise ja abistamise ID-kaartide käsitlemisel.

1.1.1.6 SK klienditeeninduspunkti kohustused

SK klienditeeninduspunkt peab vastu võtma taotlusi sertifikaatide uuendamiseks, peatamiseks, peatamise 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.

SK klienditeeninduspunkt garanteerib oma töötajatele teenuse kvaliteetseks osutamiseks vajaliku koolituse.

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

1.1.1.7 Abiliini kohustused

Vt CPS p.2.1.2.2.

KMA kohustused

KMA kohustub:

- oma sertifitseerimissüsteemiga seotud infosüsteemi osas järgima käideldavuse ja turbenõudeid, mis vastavad vähemalt käesolevas poliitikas toodud nõuetele;
- tagama, et töötajatel, kes võtavad vastu ID-kaardi taotlusi ja/või on seotud sertifitseerimisteenust puudutava informatsiooniga, ei ole karistatust tahtlikult toimepandud kuriteo eest;
- edastama Eesti välisesindustele väljastamiseks ID-kaardid;
- tagama isikutunnistusi puudutava informatsiooni kättesaadavuse avalikus andmesidevõrgus aadressil <http://www.pass.ee>.

Nõuded kliendile

Vt CPS p.2.1.3.

Klient peab ID-kaardi taotluse esitamisel edastama KMA-le õige informatsiooni ning isikuandmete muutumise korral teatama õiged andmed KMA-le vastavalt kehtestatud õigusaktidele.

Nõuded huvitatud isikule

Vt CPS p.2.1.4.

Nõuded kataloogiteenusele

Vt CPS p.2.1.5.

Lisanõudeid kataloogiteenuse toimimiseks ette ei nähta.

Vastutus

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.

Registreerimiskeskuse vastutus

1.1.1.8 KMA klienditeeninduspunkti vastutus

Vt CPS p.2.2.2.1.

KMA klienditeeninduspunkt vastutab kõigi käesoleva CP punktis 2.1.2.1 toodud kohustuste täitmise eest.

1.1.1.9 SK klienditeeninduspunkti vastutus

Vt CPS p.2.2.2.1.

SK klienditeeninduspunkt vastutab kõigi käesoleva CP punktis 2.1.2.2 toodud kohustuste täitmise eest.

1.1.1.10 Abiliini vastutus

Vt CPS p.2.2.2.2.

Abiliin vastutab kõigi käesoleva CP punktis 2.1.2.3 toodud kohustuste täitmise eest.

KMA vastutus

KMA vastutab kõigi käesoleva CP punktis 2.1.3 toodud kohustuste täitmise eest.

Vastutuse piirid

Vt CPS p.2.2.3.

Vaidluste lahendamine

Vt CPS p.2.3.

Informatsiooni avaldamine ja kataloogiteenus

SK informatsiooni avaldamine

Vt CPS p.2.4.1.

Kehtiv tühistusnimekiri on kättesaadav kataloogiteenus kaudu ja aadressil <http://www.sk.ee/crls/>

Avaldamise sagedus

Vt CPS p.2.4.2.

Sertifikaatide tühistusnimekirju avaldatakse reeglina iga 12 tunni järel.

Juurdepääsureeglid

Vt CPS p.2.4.3.

Kataloogiteenus

Vt CPS p.2.4.4.

Audit

Vt CPS p.2.5.

Välisauditi tulemustest teatatakse kõikidele käesolevas CP-s punktis 1.5 toodud organisatsioonidele ja avaldatakse SK koduleheküljel.

Konfidentsiaalsus

Vt CPS p.2.6.

Kliendi identifitseerimine

Kliendi isikusamasuse kontroll

Kliendi isikusamasust kontrollitakse vastavalt kehtestatud õigusaktidele.

Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord

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

Eraldusnimi

Vt CPS p.3.3.

Kliendi eraldusnimi koostatakse vastavalt dokumendile “Sertifikaadid Eesti Vabariigi isikutunnistusel” [2].

Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtajad

Sertifikaaditaotluse esitamine

Vt CPS p.4.1.

Klient täidab taotlusankeedi ID-kaardi taotlemiseks ning allkirjastab selle. Allkirjastatud ID-kaardi taotlus on sertifikaaditaotluse koostamise aluseks.

Täiendavat informatsiooni saab veebilehtedelt <http://www.pass.ee>, <http://www.mig.ee> ja <http://www.sk.ee>.

1.2 Sertifikaaditaotluse menetlemine

ID-kaardi taotluse täpne läbivaatamise kord ja menetluse tähtajad on ära määratud vastavate õigusaktidega. Sertifikaaditaotluse menetlemisel kontrollitakse kliendi poolt esitatud andmete õigsust ja täielikkust.

Otsuse tegemine

Vt CPS p.4.2.1.

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

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

ID-kaardile uute sertifikaatide taotluse rahuldamise või mitterahuldamise otsustab SK.

Sertifikaadi väljastamine

SK väljastab peale TRÜB-i poolt edastatud sertifikaaditaotluse autentsuse ja terviklikkuse kontrolli taotlusele automaatselt vastavad sertifikaadid, mis laetakse TRÜB-is 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 KMA või SK klienditeeninduspunktis või SK koduleheküljel olevas rakenduses.

ID-kaardi väljastamine. Sertifikaatide aktiveerimine.

ID-kaart väljastatakse kliendile KMA klienditeeninduspunktis

Koos ID-kaardi väljastamisega aktiveerib KMA klienditeeninduspunkti ametnik ID-kaardile laetud sertifikaadid.

KMA klienditeeninduspunkti või Eesti välisesinduse ametnik annab kliendile üle ID-kaardi aktiveerimiskoodi sisaldava turvaümbriku (PIN-koodi ümbrik).

Klient (või kliendi seadusjärgne esindaja) allkirjastab ID-kaardi väljastamise akti-blanketi.

ID-kaardi sertifikaatide uuendamisel aktiveeritakse sertifikaadid koheselt peale nende laadimist kiipkaardile.

Sertifikaadi kontroll ja tõestamine

Vt CPS p.4.2.4.

Sertifikaadi uuendamine

Aegunud või tühistatud sertifikaate asendatakse uuesti genereeritud võtmepaari põhjal väljastatud sertifikaatidega.

Sertifikaadi kehtetuks tunnistamise ja peatamise taotlused

Vt CPS p.4.3.

Sertifikaatide peatamine

Vt CPS p.4.4.

Sertifikaatide peatamine on võimalik ka KMA klienditeeninduspunktis.

Taotluse esitaja tuvastatakse vastavalt kehtivatele õigusaktidele.

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

Sertifikaadi peatamise lõpetamine

Vt CPS p.4.5.

Sertifikaatide peatamise lõpetamine on võimalik ka KMA klienditeeninduspunktis.

Taotluse esitaja tuvastatakse vastavalt kehtivatele õigusaktidele.

Sertifikaadi peatamise lõpetamise taotlus peab sisaldama:

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

KMA klienditeeninduspunktis taotluse registreerimisel ei märgita üles taotluse esitaja isikutuvastamisel kasutatud dokumendi andmeid.

Sertifikaadi kehtetuks tunnistamine

Sertifikaadi kehtetuks tunnistamise volitused

Vt CPS p.4.6.1.

Sertifikaadi kehtetuks tunnistamise taotluse võib esitada KMA peale ID-kaardi tühistamist.

Sertifikaadi kehtetuks tunnistamise taotluse esitamine

Vt CPS p.4.6.2.

Sertifikaatide kehtetuks tunnistamine on võimalik ka KMA 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.

KMA klienditeeninduspunktis taotluse registreerimisel ei märgita üles taotluse esitaja isikutuvastamisel kasutatud dokumendi andmeid.

Sertifikaadi kehtetuks tunnistamise menetlus

Vt CPS p.4.6.3.

Sertifikaatide kehtetuks tunnistamise taotluse saab esitada ka KMA klienditeeninduspunktis.

Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus

Vt CPS p.4.6.4.

Protseduurid jälgitavuse tagamiseks

Vt CPS p.4.7.

Tegutsemine eriolukorras

Vt CPS p.4.8.

Sertifitseerimisteenuse osutaja töö lõpetamine

Vt CPS p.4.9.

Füüsilised ja organisatsioonilised turbemeetmed

Turbehaldus

Vt CPS p.5.1.

Füüsilised turbemeetmed

SK füüsiline pääsukontroll

Vt CPS p.5.2.1.

Muud nõuded. ID-kaartide hoiustamine

ID-kaarte hoiustatakse KMA klienditeeninduspunktis vastavalt kehtestatud sisemistele turvaeeskirjadele.

Asendus PIN-ümbrikke hoiustatakse KMA ja SK klienditeeninduspunktis vastavalt kehtestatud sisemistele turvaeeskirjadele.

Nõuded tööprotseduuridele

Vt CPS p.5.3.

Personali turbenõuded

Vt CPS p.5.4.

Tehnilised turbenõuded

Võtmehaldus

SK kinnitusvõtmed

Vt CPS p.6.1.1.

Kliendi võtmed

1.2.1.1 Kliendi võtmete moodustamine

Võtmete moodustamisel kasutatavad algoritmid, võtmepikkused ja teised parameetrid on toodud dokumendis „Sertifikaadid Eesti Vabariigi isikutunnistusel” [2].

Võtmed luuakse ID-kaardi isikustamise ajal ning sertifikaatide asendamisel KMA ja SK klienditeeninduspunktis 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.

1.2.1.2 Kliendi isikliku võtme ja aktiveerimiskoodide kaitse personaliseerimise käigus

KMA, SK ja TRÜB 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.

1.2.1.3 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 KMA või SK klienditeeninduspunkti poole asendus PIN-koodi ümbriku saamiseks.

1.2.1.4 Kliendi võtmete varundamine ja deponeerimine

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

Süsteemiturve

Vt CPS p.6.2.

Sertifitseerimisteenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus

Vt CPS p.6.3.

Sertifitseerimisteenuse osutamisel tekkinud andmete säilitamine ja kaitse

Vt CPS p.6.4.

Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid

Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid on toodud dokumendis „Sertifikaadid Eesti Vabariigi isikutunnistusel” [2].

Sertifitseerimispoliitika haldus

Vt CPS p.8.

Käesolev CP ja viidatud dokumendid [1] ning [2] avaldatakse SK koduleheküljel ja dokument [5] avaldatakse SK ja KMA koduleheküljel. Kõik muudatused kooskõlastatakse KMA ja TRÜB-ga.

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 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
- [5] Isikutunnistuse sertifikaatide kasutustingimused (ISKT)

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.