Asutuse sertifikaatide sertifitseerimispoliitika

Versioon 2.4

OID: 1.3.6.1.4.1.10015.7.1.2.4

Versioonid ja muudatused:

Versioon	Kuupäev	Kommentaarid
1.0	10.04.2002	Esimene versioon
1.1.	13.10.2006	Parandatud versioon
2.1	13.08.2009	Poliitika on viidud vastavusse Digitaalallkirja seadusest tulenevatele nõuetele. Eemaldatud „seadmesertifikaatide“ mõiste.
2.2	10.05.2010	Muudetud on punkte: 1.3.4 – ühte sertifikaati võib erinevaid kasutusvaldkondi (va digitaalse templi sertifikaati) 4.2.2 – kiipkaardi mõiste on asendatud turvalise allkirja andmise vahendiga
2.3	20.07.2012	Muudetud on punkte: 4.6.1 – lisatud sertifikaadi kehtetuks tunnistamise volitused.
2.4	28.09.2012	Muudetud punkte: 4.2.4 – kaotatud erinevus CPS’iga kinnituste andmisel

Sisukord

SISUKORD **3**

1 SISSEJUHATUS **5**

1.1 ÜLEVAADE 5
1.2 SERTIFITSEERIMISPOLIITIKA IDENTIFITSEERIMINE 5
1.3 ORGANISATSIOON JA KASUTUSVALDKOND 6
1.3.1 Sertifitseerimiskeskus (SK) *6*
1.3.2 SK registreerimiskeskus *6*
1.3.3 Kasutaja *6*
1.3.4 Sertifikaatide kasutusvaldkond *6*
1.4 KONTAKTANDMED 7

2 ÜLDTINGIMUSED **7**

2.1 KOHUSTUSED JA NÕUDED 7
2.1.1 Nõuded SK-le *7*
2.1.2 Nõuded registreerimiskeskusele *7*
2.1.3 Nõuded kliendile *8*
2.1.4 Nõuded huvitatud isikule *8*
2.1.5 Nõuded kataloogiteenusele *8*
2.2 VASTUTUS 8
2.2.1 SK vastutus *8*
2.2.2 Registreerimiskeskuse vastutus *8*
2.2.3 Vastutuse piirid *8*
2.3 VAIDLUSTE LAHENDAMINE 8
2.4 INFORMATSIOONI AVALDAMINE JA KATALOOGITEENUS 9
2.4.1 SK informatsiooni avaldamine *9*
2.4.2 Avaldamise sagedus *9*
2.4.3 Juurdepääsureeglid *9*
2.4.4 Kataloogiteenus *9*
2.5 AUDIT 9
2.6 KONFIDENTSIAALSUS 9

3 KLIENDI IDENTIFITSEERIMINE **9**

3.1 KLIENDI ISIKUSAMASUSE KONTROLL 9
3.2 SERTIFIKAADI TAOTLEJA AVALIKULE VÕTMELE VASTAVA ISIKLIKU VÕTME TÕENDAMISE KORD 9
3.3 ERALDUSNIMI 10

4 SERTIFITSEERIMISTEENUSE OSUTAMINE. SERTIFITSEERIMISMENETLUSE KORD JA TÄHTAJAD **10**

4.1 SERTIFIKAADITAOTLUSE ESITAMINE 10
4.2 SERTIFIKAADITAOTLUSE MENETLEMINE 10
4.2.1 Otsuse tegemine *10*
4.2.2 Sertifikaadi väljastamine *11*
4.2.3 Sertifikaatide üle arvestuse pidamise kord *11*

4.2.4 Sertifikaadi kontroll ja tõestamine *11*
4.2.5 Sertifikaadi uuendamine *12*
4.3 SERTIFIKAADI KEHTETUKS TUNNISTAMISE JA PEATAMISE TAOTLUSED 12
4.4 SERTIFIKAATIDE PEATAMINE 12
4.5 SERTIFIKAADI PEATATUSE LÕPETAMINE 12
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 14
4.9 SERTIFITSEERIMISTEENUSE OSUTAJA TÖÖ LÕPETAMINE 14

5 FÜÜSILISED JA ORGANISATSIOONILISED TURBEMEETMED 14

5.1 TURBEHALDUS 14
5.2 FÜÜSILISED TURBEMEETMED 14
5.2.1 SK füüsiline pääsukontroll *14*
5.3 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 15

7 SERTIFIKAATIDE JA TÜHISTUSNIMEKIRJADE (CRLIDE) TEHNILISED PROFIILID 15

7.1 SERTIFIKAATIDE PROFIIL 15
7.2 TÜHISTUSNIMEKIRJAD (CRL) 15

8 SERTIFITSEERIMISPOLIITIKA HALDUS 15

9 KASUTATUD TERMINOLOOGIA 16

10 KASUTATUD LÜHENDID 16

11 VIIDATUD JA SEONDUVAD DOKUMENDID 16

1 Sissejuhatus

1.1 Ülevaade

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

Käesolev CP rajaneb dokumendile „AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted“ [1], mis on registreeritud sertifitseerimisteenuse osutajate 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.

Asutuse sertifikaatide **erivormid** on veebiserveri sertifikaadid ja digitaalse templi sertifikaadid DAS mõistes. Täpsem kirjeldus on toodud käesoleva CP punktis 1.3.4.

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

1.2 Sertifitseerimispoliitika identifitseerimine

Käesoleva CP tunnuskood on **OID: 1.3.6.1.4.1.10015.7.1.2.4**

CP tunnuskood on koostatud vastavalt järgnevale tabelile 1.

Parameeter	Viide OIDis
Interneti tunnus	1.3.6.1
Ettevõtte tunnus	4
Ettevõtteid haldava IANA poolt registreeritud ettevõtte tunnus	1
IANA registris ASile Sertifitseerimiskeskus antud tunnus	10015
Sertifitseerimisteenuse tunnus	7.1
CP versiooni tunnus	2.4

Tabel 1. CP tunnuskoodi koostamine

1.3 Organisatsioon ja kasutusvaldkond

1.3.1 Sertifitseerimiskeskus (SK)

Vt CPS p.1.2.1.

1.3.2 SK registreerimiskeskus

1.3.2.1 SK klienditeeninduspunkt

SK klienditeeninduspunktiks on Sertifitseerimiskeskus AS ise.

1.3.2.2 Abiliin

Abiliini teenus käesoleva CP raames puudub.

1.3.3 Kasutaja

1.3.3.1 Klient

Vt CPS p.1.2.3.1.

Käesoleva CP alusel väljastatakse sertifikaate juriidilisest isikust klientidele.

Klient on käesoleva CP alusel väljastatud sertifikaadi omanik.

Ühele kliendile võib anda välja mitu asutuse sertifikaati.

1.3.3.2 Huvitatud isik

Vt CPS p.1.2.3.2.

1.3.4 Sertifikaatide kasutusvaldkond

Vt CPS p.1.2.4.
Käesoleva CP alusel väljastatakse sertifikaate juriidilistele isikutele piiramata kasutusvaldkonnaga. Käesolev CP seab erinõuded järgmiste sertifikaatide väljastamisele:

- **Veebiserveri sertifikaat** - HTTPS serverile antav sertifikaat tõestamaks veebiserveri omaniku autentsust;
- **Digitaalse templi sertifikaat** - kasutatakse tõendamaks digitaalse dokumendi terviklust ning omaniku seost sellise dokumendiga.

Digitaalse templi sertifikaati saab kasutada vastavalt DAS-le [3].

Erinevaid kasutusvaldkondi võib kokku panna ühte sertifikaati. Teiste kasutusvaldkondadega ei tohi kokku panna digitaalse templi sertifikaate.

Kokkuleppel kliendiga on lubatud väljastada sertifikaadi profiilis määratlemata kasutusvaldkondadega spetsiifilisi sertifikaate.

1.4 Kontaktandmed

Vt CPS p.1.3.

2 Üldtingimused

2.1 Kohustused ja nõuded

2.1.1 Nõuded SK-le

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 Kliendi sertifikaaditaotlused üle elektroonse turvalise andmesidekanali;
- 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 kehtetuks tunnistama kõik väljastatud sertifikaadid;
- 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 Nõuded registreerimiskeskusele

2.1.2.1 Nõuded SK klienditeeninduspunktile

Klienditeeninduspunkt peab vastu võtma taotlusi sertifikaatide väljastamiseks, peatamiseks, peatatuse lõpetamiseks ja kehtetuks tunnistamiseks ning kontrollima nende avalduste õigsust ja terviklikkust. Klienditeeninduspunkti töötaja kohustub

kõikide nimetatud toimingute teostamisel kontrollima taotluse esitaja isikusamasust ja volitusi toimingu teostamiseks.

2.1.2.2 Nõuded abiliinile

Abiliin puudub.

2.1.3 Nõuded kliendile

Vt CPS p.2.1.3.
Klient peab olema registreeritud juriidiline isik, kes ei ole asukohamaa seaduste kohaselt pankrotis või likvideerimisel, tema tegevus ei ole peatatud või muus sellesarnases seisukorras.
Klient peab järgima SK poolt käesolevas CP-s kehtestatud tingimusi ja protseduure.
Klient on kohustatud esitama SK-le õigeid ja täielikke andmeid ning informeerima viivitamatult SK-d andmete muutumisest.
Klient peab nõustuma „Asutuse sertifikaatide kasutustingimustega“ (ASKT).

2.1.4 Nõuded huvitatud isikule

Vt CPS p.2.1.4.

2.1.5 Nõuded kataloogiteenusele

Vt CPS p.2.1.5.

2.2 Vastutus

2.2.1 SK vastutus

SK on vastutav kõigi punktis 2.1.1 ja 2.1.5 toodud kohustuste täitmise eest Eesti Vabariigis kehtivates õigusaktides nõutud piirides.

2.2.2 Registreerimiskeskuse vastutus

2.2.2.1 Klienditeeninduspunkti vastutus

.
Klienditeeninduspunkt vastutab kõigi punktis 2.1.2.1 toodud kohustuste täitmise eest.

2.2.2.2 Abiliini vastutus

Abiliin puudub.

2.2.3 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/.

2.4.2 Avaldamise sagedus

Vt CPS p.2.4.2.

Tühistusnimekirja uuendatakse regulaarselt iga 12 tunni järel.

2.4.3 Juurdepääsureeglid

Vt CPS p.2.4.3.

2.4.4 Kataloogiteenus

Vt CPS p.2.4.4.
Kataloogis sisalduvad ka kehtetud sertifikaadid.

2.5 Audit

Vt CPS p.2.5.

2.6 Konfidentsiaalsus

Vt CPS p.2.6.

3 Kliendi identifitseerimine

3.1 Kliendi isikusamasuse kontroll

Asutuse sertifikaadi taotluse menetlemise käigus kontrollitakse:

- Kliendi registreeritust vastavalt asukohariigi õigusaktidele;.
- Kliendi esindaja isikusamasust;
- Kliendi esindaja volitusi kliendi nimel sertifikaadi taotlemiseks

3.2 Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord

Asutuse sertifikaadi taotlemiseks esitab klient SK-le elektrooniliselt sertifikaadi signeerimistaotluse (CSR – *Certificate Signing Request*), mis sisaldab taotleja avalikku võtit ning mis on signeeritud vastava isikliku võtmega. Signeerimistaotluse kooskõlalisuse korral saab SK eeldada, et vastav isiklik võti on taotleja valduses.

Juhul kui SK on kliendilt saanud volituse genereerida temale avalik ja isiklik võti, on kooskõlalisus tagatud SK siseprotseduuridega ning klient ei pea esitama SK-le elektrooniliselt sertifikaadi signeerimistaotlust (CSR - *Certificate Signing Request)*.

3.3 Eraldusnimi

Vt CPS p.3.3.
Sertifikaadi eraldusnimi koostatakse vastavalt dokumendile "Asutuse sertifikaatide profiil" [2].

Veebiserveri sertifikaatide puhul eraldusnime unikaalsust ei tagata.

Veebiserveri sertifikaadi eraldusnime omistamisel lähtutakse kliendi seadme domeeninime ja/või IP-aadressi seotusest kliendiga juhul, kui seade on kättesaadav üldkasutatava arvutivõrgu kaudu.

Digitaalse templi sertifikaadi eraldusnime omistamisel lähtutakse kliendi asukohamaa registrisse kantud nimest.

4 Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtajad

4.1 Sertifikaaditaotluse esitamine

Vt CPS p.4.1.
Sertifikaaditaotlus esitatakse SK-le elektrooniliselt kujul, mis võimaldab kontrollida kliendi esindaja isikusamasust. Taotlus sisaldab lisaks kliendi andmetele PKCS#10 [7] vormingus signeeritud sertifikaaditaotlust (CSR-i) või taotletava sertifikaadi eraldusnime ja kehtivusaega.

Kui klient soovib digitaalset templit CSR alusel, siis kinnitab kliendi esindaja taotluse vormil, et sertifikaadi haldamiseks kasutatakse turvalist allkirja andmise vahendit.

4.2 Sertifikaaditaotluse menetlemine

Sertifikaaditaotlus menetletakse 5 tööpäeva jooksul peale selle laekumist SK-sse. Sertifikaaditaotluse menetlemisel kontrollitakse kliendi poolt esitatud andmete õigsust ja täielikkust.

4.2.1 Otsuse tegemine

Sertifikaaditaotluse avalduse rahuldamise või mitterahuldamise otsustab SK. Otsuse tegemisel SK kontrollib:

- Kliendi isikusamasust (sh juriidilise isiku registreeritust vastavalt asukohariigi õigusaktidele);
- Kliendi esindaja isikusamasust
- Kliendi esindaja volitusi kliendi nimel sertifikaadi taotlemiseks ja/või tühistamiseks
- Kliendi poolt esitatud andmete õigsust ja täielikkust
- Kas kliendil on vastavalt Eesti Vabariigi õigusaktidele ja/või käesolevale CP-le õigus saada sertifikaat

Digitaalse templi taotluse puhul kontrollitakse täiendavalt sertifikaadi eraldusnime unikaalsust.

Veebiserveri sertifikaadi taotluse puhul kontrollitakse täiendavalt kliendi seadme domeeninime ja/või IP-aadressi seotusest kliendiga juhul, kui seade on kättesaadav üldkasutatava arvutivõrgu kaudu.

SK lähtub otsuse tegemisel eelpool toodud kontrollide tulemustest ning omab õigust keelduda sertifikaadi väljastamisest.

4.2.2 Sertifikaadi väljastamine

Vt CPS p.4.2.2.
Sertifikaat (või viide sellele) saadetakse kliendile tema kontaktandmetes märgitud elektronposti aadressile. Hiljemalt 1 tunni möödudes avaldatakse sertifikaat SK avalikus kataloogis.

SK poolt väljastatavale turvalisele allkirja andmise vahendile (sh kiipkaart) väljastatavale asutuse sertifikaadile peab klient järele tulema klienditeeninduspunkti.

Turvalisel allkirja andmise vahendil väljastatava digitaalse templi sertifikaadi väljastamisel kontrollib klienditeeninduspunkti töötaja kliendi esindaja isikusamasust kliendi isikut tõendava dokumendi alusel ning tema volitusi sertifikaadi kätte saamiseks

Kliendi esindaja kinnitab oma allkirjaga aktil, et on digitaalse templi sertifikaadi kätte saanud ning tutvunud käesoleva CP ja „Asutuse sertifikaatide kasutustingimustega".

4.2.3 Sertifikaatide üle arvestuse pidamise kord

Vt CPS p.4.2.3.
Kataloogile juurdepääsu ei piirata.

4.2.4 Sertifikaadi kontroll ja tõestamine

Vt CPS p.4.2.4.

4.2.5 Sertifikaadi uuendamine

Vt CPS p.4.2.5.
4 nädalat enne sertifikaadi kehtivuse lõppu saadab SK kliendile elektronposti teel kontaktaadressile teate sertifikaatide kehtivuse peatse lõppemise kohta.

Käesoleva CP mõistes sertifikaatide uuendamist ei toimu ja klient peab taotlema uued sertifikaadid.

4.3 Sertifikaadi kehtetuks tunnistamise ja peatamise taotlused

VT CPS p 4.3

Asutuse sertifikaate ei saa peatada, välja arvatud digitaalse templi sertifikaadid.

Digitaalse templi sertifikaatide kehtetuks tunnistamiseks ja peatamiseks peab kliendi seaduslik esindaja või sertifikaaditaotluses näidatud volitatud isik esitama kirjaliku või digitaalallkirjaga allkirjastatud vastavasisulise avalduse SK-le.

4.4 Sertifikaatide peatamine

Asutuse sertifikaate ei saa peatada, välja arvatud digitaalse templi sertifikaadid.

Digitaalse templi sertifikaati saab peatada SK klienditeeninduspunktis. VT CPS p 4.4.

Digitaalse templi sertifikaat peatatakse kohe pärast sertifikaadi kehtivuse peatamise nõude seaduslikkuse kontrollimist ning peatatud sertifikaadi andmed kehtivuse peatamise kohta kantakse SK poolt peetavasse sertifikaatide andmebaasi.

4.5 Sertifikaadi peatatuse lõpetamine

VT CPS p 4.5.

Asutuse sertifikaate ei saa peatada ega peatatust lõpetada, välja arvatud digitaalse templi sertifikaadid.

Digitaalse templi sertifikaadi peatatuse lõpetamiseks tuleb kliendi esindajal esitada kirjalik avaldus kliendteeninduspunkti või edastada kliendi esindaja digitaalallkirjaga allkirjastatud avaldus SK-sse kontaktandmetes toodud aadressile.

Digitaalse templi sertifikaadi peatatus lõpetatakse kohe pärast sertifikaadi kehtivuse peatatuse lõpetamise nõude seaduslikkuse kontrollimist ning andmed sertifikaadi peatatuse lõpetamise kohta kantakse SK poolt peetavasse sertifikaatide andmebaasi.

4.6 Sertifikaadi kehtetuks tunnistamine

4.6.1 Sertifikaadi kehtetuks tunnistamise volitused

Vt CPS p.4.6.1.

SK võib täiendavalt sertifikaadi kehtetuks tunnistada alljärgnevatel põhjustel:

- Vastavalt ASKT-le [6];
- Klient teatab, et esialgne sertifikaadi taotlus ei olnud volitatud ja Klient ei taotle tagasiulatuvalt volitust;
- SK saab piisavad tõendid, et Kliendi salajane võti (mis vastab sertifikaadi avalikule võtmele) on väljunud Kliendi kontrolli alt või on tekkinud selline oht või seda sertifikaati on muul viisil väärkasutatud;
- SK saab teate või on muul viisil teada saanud, et Klient on rikkunud ühte või mitut ASKT [6] järgset olulist kohustust;
- SK saab teate või on muul viisil teada saanud, mis tahes asjaolust, mis viitab sellele, et sertifikaadi domeeninime ja/või IP-aadressi kasutus ei ole enam õiguslik (näiteks kohus on tühistanud Kliendi õiguse kasutada domeeninime mis on sertifikaadis, asjakohane suhe registri ja domeeni omaniku vahel on lõpetatud);
- SK saab teate või on muul viisil teada saanud olulisest muutusest sertifikaadis sisalduva teabe kohta;
- SK määrab ainuotsusega, et sertifikaat ei ole väljastatud käesoleva CP või CPS-i alusel;
- SK tuvastab, et mingid sertifikaati kantud andmed ei ole õiged, välja arvatud organizationalUnitName väli, kui see olemas on;
- SK lõpetab tegevuse mis tahes põhjusel ja ei ole organiseerinud teist sertifitseerimisteenuse pakkujat sertifikaatide tühistusteenust pakkuma;
- On tekkinud kahtlus, et SK salajane võti, mida kasutati sertifikaadi väljastamiseks, on väljunud SK kontrolli alt.

4.6.2 Sertifikaadi kehtetuks tunnistamise avalduse esitamine

Vt CPS p.4.6.2.

Sertifikaadi kehtetuks tunnistamise avalduse võib allkirjastada ka digitaalallkirjaga ja edastada kontaktandmetes toodud SK meiliaadressile.

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.

5.3 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

Juhul kui SK on kliendilt saanud volituse genereerida tema avalik ja isiklik võti, tagab SK, et võtmeid ei kasutata enne kliendile kätte andmist ja võtmetest ei tehta koopiaid.

Klient vastutab täielikult oma salajase võtme säilimise ja kasutamise turvalisuse eest.

Kui klient genereerib ise oma digitaalse templi võtmepaari, siis peab ta tagama isikliku võtme haldamise turvalises allkirja andmise vahendis.

Kliendi isikliku võtme aktiveerimine võib toimuda turvalises allkirja andmise vahendis ilma igakordse aktiveerimiskoodi sisestamiseta.

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

VT CPS p 7.1.

Asutuse sertifikaadid kehtivad kuni **1125 päeva** (3 aastat ja 30 päeva).

Sertifikaatide täpne profiil on toodud dokumendis “Asutuse sertifikaatide profiil” [2].

7.2 Tühistusnimekirjad (CRL)

VT CPS p 7.2.

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

Tühistusnimekirja täpne profiil on toodud dokumendis “Asutuse sertifikaatide profiil” [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

9 Kasutatud terminoloogia

Vt CPS p.10.
Turvaline allkirja andmise vahend – vaata Digitaalallkirja seadus [3].

10 Kasutatud lühendid

Vt CPS p.11.

Lühend	Definitsioon
CSR	Sertifikaadi signeerimistaotlus
ASKT	Asutuse sertifikaatide kasutamise tingimused
SK	AS Sertifitseerimiskeskus

11 Viidatud ja seonduvad dokumendid

Viidatud dokumendid:

[1] AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtted (CPS)
[2] Asutuse sertifikaatide profiil
[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
[6] Asutuse sertifikaatide kasutamise tingimused. AS Sertifitseerimiskeskus.
[7] PKCS#10 – Certification Request Syntax Standard. http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/