Seadmesertifikaatide sertifitseerimispoliitika

Versioon 1.1

OID: 1.3.6.1.4.1.10015.2.1.1.1

Versioonid ja muudatused:

Versioon	Kuupäev	Kommentaarid
1.0	10.04.2002	Esimene versioon
1.1.	13.10.2006	Parandatud versioon

Sisukord

1 Sissejuhatus

1.1 Ülevaade

Käesolev dokument (edaspidi sertifitseerimispoliitika, CP) on reeglite kogum, mis määrab ära peamised tööpõhimõtted ja -kontseptsioonid seadmesertifikaatide 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: 1.3.6.1.4.1.10015.2.1.1.1**

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	2.1
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.

1.3.2 SK registreerimiskeskus

1.3.2.1 SK klienditeeninduspunkt

SK klienditeeninduspunktiks on Sertifitseerimiskeskus AS ise.

1.3.2.2 Abiliin

Kuna käesoleva CP raames sertifikaatide peatamisteenus puudub, siis ei eksisteeri ka abiliini.

1.3.3 Kasutaja

1.3.3.1 Klient

Vt CPS p.1.2.3.1.

Käesoleva CP alusel väljastatakse sertifikaate klientidele, kes on juriidilised isikud.

Klient on käesoleva CP alusel väljastatud sertifikaadi omanik.

1.3.3.2 Huvitatud isik

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

1.3.4 Sertifikaatide kasutusvaldkond

Vt CPS p.1.2.4.
Käesoleva CP alusel väljastatakse sertifikaate, mida kasutatakse turvalise andmeside loomiseks seadmete (arvutite) vahel.

Seadmesertifikaate ei saa kasutada digitaalseks allkirjastamiseks DAS [3] mõttes.

1.4 Kontaktandmed

Vt CPS p.1.3.

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 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 Registreerimiskeskuse kohustused

2.1.2.1 SK klienditeeninduspunkti kohustused

Klienditeeninduspunkt peab vastu võtma taotlusi sertifikaatide väljastamiseks ja kehtetuks tunnistamiseks ning kontrollima nende avalduste õigsust ja terviklikkust. Klienditeeninduspunkt kohustub kõikide nimetatud toimingute teostamisel kontrollima taotluse esitaja isikusamasust ja volitusi toimingu teostamiseks.

2.1.2.2 Abiliini kohustused

Abiliin puudub.

2.1.3 Nõuded kliendile

Vt CPS p.2.1.3.

Klient peab järgima SK poolt käesolevas CP-s kehtestatud protseduure. Klient on kohustatud esitama SK-le õigeid ja täielikke andmeid ning informeerima viivitamatult SK-d andmete muutumisest.

2.1.4 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.

2.1.5 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

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/klass3/klass3.crl.

2.4.2 Avaldamise sagedus

Vt CPS p.2.4.2.

Uuendatud sertifikaatide tühistusnimekiri avaldatakse hiljemalt 10 minuti jooksul peale kehtetuks tunnistamise taotluse rahuldamist. 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.

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 ja tema poolt esitatud andmete kontrolli sätestab dokument „Seadmesertifikaatide kasutamise tingimused“ (SSKT) [6].

Seadmesertifikaadi taotluse menetlemise käigus kontrollitakse:

- Kliendi kui juriidilise isiku andmeid
- Seadme administraatori isikusamasust ning tema volitusi sertifikaadi taotlemiseks ja/või tühistamiseks
- Seadme domeeninime ja/või võrguaadressi seotust juriidilise isikuga juhul, kui seade on kättesaadav üldkasutatava arvutivõrgu kaudu

3.2 Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord

Klient esitab SK-le elektrooniliselt sertifikaadi signeerimistaotluse (CSR – *Certificate Signing Request*), mis sisaldab taotleja avalikku võtit ning mis on šifreeritud vastava

salajase võtmega. Sertifitseerimispäringu eduka dešifreerimise korral saab SK eeldada, et vastav isiklik võti on taotleja valduses.

3.3 Eraldusnimi

Vt CPS p.3.3.
Kliendi eraldusnimi koostatakse vastavalt dokumendile "Seadmesertifikaatide profiil" [2].

4 Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtajad

4.1 Sertifikaaditaotluse esitamine

Vt CPS p.4.1.
Sertifikaaditaotluse esitamine käib SK koduleheküljе kaudu. Klient täidab veebivormi oma kontaktandmetega ning saadab vormi kaudu ka eelgenereeritud sertifikaadi signeerimistaotluse (CSR-i). Andmete sisestamise järel väljastab veebisüsteem kliendikohase avaldusblanketi, mille klient välja trükib, allkirjastab ning saadab posti (ja telefaksi) teel SK-sse.

Käesolev CP näeb ette ka avalduse allkirjastamist digitaalselt vastavalt DAS-ile [3].

4.2 Sertifikaaditaotluse menetlemine

Sertifikaaditaotlus vaadatakse läbi peale kliendi poolt allkirjastatud avaldusblanketi laekumist SK-sse 2 tööpäeva jooksul. Sertifikaaditaotluse menetlemisel kontrollitakse kliendi poolt esitatud andmete õigsust ja täielikkust.

4.2.1 Otsuse tegemine

Sertifikaaditaotluse avalduse rahuldamise või mitterahuldamise otsustab SK. Oma otsuse tegemisel lähtub SK muuhulgas:

- Kliendi organisatsioonilisest staatusest
- Kliendi seadme domeeninime ja/või IP-aadressi seotusest organisatsiooniga juhul, kui seade on kättesaadav üldkasutatava arvutivõrgu kaudu
- Seadme administraatori isikust ja tema volitustest esindamaks Klienti

4.2.2 Sertifikaadi väljastamine

Vt CPS p.4.2.2.
Sertifikaat (või viide sellele) saadetakse kliendile tema kontaktandmetes märgitud elektronposti aadressile. Samal hetkel avaldatakse sertifikaat SK avalikus kataloogis.

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

Sertifikaadi kehtivust saab huvitatud isik kontrollida SK avaliku kataloogi ja seal leiduva tühistusnimekirja abil. SK ei väljasta seadmesertifikaatidel omapoolse esindaja poolt digitaalselt allkirjastatud kehtivustõendeid.

4.2.5 Sertifikaadi uuendamine

2 nädalat enne sertifikaadi kehtivuse lõppu saadab SK kliendile elektronposti teel vastavasisulise hoiatuse ning viite SK koduleheküljele, mis võimaldab taotleda uut sertifikaati.

Sertifikaadi uuendamine toimub ainult samale võtmepaarile ning nendele sertifikaatidele, mis ei ole kehtetuks tunnistatud. Muudel juhtumitel tuleb taotleda uut sertifikaati.

Sertifikaadi uuendamise taotlemine toimub SK kodulehekülje kaudu. SK rahuldab uuendustaotluse 2 tööpäeva jooksul alates sertifikaadi uuendustaotluse laekumisest SK infosüsteemi.

4.3 Sertifikaadi kehtetuks tunnistamise ja peatamise taotlused

Seadmesertifikaate peatada ei saa.

Seadmesertifikaatide kehtetuks tunnistamiseks peab sertifikaadi taotlemisel registreeritud taotlenud seadme administraator või juriidilise isiku seaduslik esindaja esitama kirjaliku taotluse SK-le.

4.4 Sertifikaatide peatamine

Seadmesertifikaate peatada ei saa.

4.5 Sertifikaadi peatatuse lõpetamine

Seadmesertifikaate peatada ei saa.

4.6 Sertifikaadi kehtetuks tunnistamine

4.6.1 Sertifikaadi kehtetuks tunnistamise volitused

Vt CPS p.4.6.1.
Vastavalt SSKT-le [6] võib sertifikaadi kehtetuks tunnistada ka SK.

4.6.2 Sertifikaadi kehtetuks tunnistamise avalduse esitamine

Sertifikaadi kehtetuks tunnistamiseks esitab klient allkirjastatud avalduse, mis sisaldab:

- avalduse esitaja nime;
- avalduse esitaja allkirja;
- kehtetuks tunnistatava sertifikaadi omaniku nime ja registrinumbrit;
- kehtetuks tunnistatava sertifikaadi väljastanud SK eraldusnime;
- sertifikaadi kehtetuks tunnistamise põhjust;
- vajadusel tõendusmaterjali sertifikaadi kehtetuks tunnistamise põhjuse asjaolude tõendamiseks.

Kehtetuks tunnistamise avalduse esitaja identifitseeritakse SK poolt.

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

Klient genereerib ise oma võtmepaari ning vastutab täielikult oma salajase võtme säilitamise ja kasutamise turvalisuse eest.

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

Seadmesertifikaadid kehtivad kuni **369 päeva** (1 aasta ja 4 päeva).

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

7.2 Tühistusnimekirjad (CRL)

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

Tühistusnimekirja täpne profiil on toodud dokumendis “Seadmesertifikaatide 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.9.

10 Kasutatud lühendid

Vt CPS p.10.

Lühend	Definitsioon
CSR	Sertifikaadi signeerimistaotlus
SSKT	Seadmesertifikaatide kasutamise tingimused

11 Viidatud ja seonduvad dokumendid

Viidatud dokumendid:

[1] AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtted (CPS)
[2] Seadmesertifikaatide 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] Seadmesertifikaatide kasutamise tingimused. AS Sertifitseerimiskeskus.

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.