SK asutuse sertifikaatide sertifitseerimispoliitika

Versioon 3.0
OID: 1.3.6.1.4.1.10015.7.1.3
Kehtiv alates 13.02.2015

Versiooni info		
Kuupäev	**Versioon**	**Muudatused/täiendused**
13.01.2015	3.0	Kinnitatud versioon
14.11.2014	2.7	Versioon 3.0 mustand. Muudetud punkt 1.3.2 - täiendatud kasutatud lühendite nimekirja; Muudetud punkt 1.6 - uuendatud kontakt e-maili aadress; Muudetud punkt 4.2.1 - lisatud CAA kirje mittekäsitlemine sertifikaaditaotluse menetlemisel ja parandatud sertifikaaditaotluse menetlemise sõnastust dokumendi eestikeelses versioonis; Muudetud punkt 4.2.2 - täiendatud SSL-serveri sertifikaadi taotluse allkirjastajate nimekirja.
20.06.2014	2.6	Muudetud punkt 4.6.1 – täiendatud sertifikaadi kehtetuks tunnistamise volitusi; Muudetud punkt 8 - täiendatud sertifitseerimispoliitika haldust; Veebiserveri sertifikaadi mõiste on asendatud SSL serveri sertifikaadiga; Muudetud punkt 4.2.2 – täpsustatud nõuded sertifikaadi väljastamiseks igale sertifikaaditüübile eraldi. Väiksemad täpsustused/parandused vastavalt uutele RFC dokumentide versioonidele; restruktureerimine.
21.12.2012	2.5	Muudetud on punkt 2.4.4 – muudetud avalikus kataloogis sertifikaatide avaldamise reeglid.
28.09.2012	2.4	Muudetud on punkt 4.2.4 – kaotatud erinevus CPS'iga kinnituste andmisel.
20.07.2012	2.3	Muudetud on punkt 4.6.1 – lisatud sertifikaadi kehtetuks tunnistamise volitused.
10.05.2010	2.2	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.
13.08.2009	2.1	Poliitika on viidud vastavusse Digitaalallkirja seadusest tulenevatele nõuetele. Eemaldatud „seadmesertifikaatide" mõiste.
13.10.2006	1.1	Parandatud versioon
10.04.2002	1.0	Esmane versioon

1. Sissejuhatus

Nõuded AS Sertifitseerimiskeskus asutuse sertifitseerija poolt väljastatavate sertifikaatide väljastamiseks ja teenindamiseks.

1.1. Sisukord

1.2. Ülevaade

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

Käesolev CP rajaneb dokumendile „AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted“ [1] (edaspidi CPS), mis on registreeritud Sertifitseerimise Registris. CPS on aluseks sertifitseerimisteenuse osutamisel, käesolev CP täpsustab täiendavalt CPS-is toodud põhimõtteid.

Käesoleva CP ja CPS-i vastuolu korral tuleb ülimuslikuks pidada käesolevas CP-s toodut.

Asutuse sertifikaatide erivormid on SSL serveri sertifikaadid ja digitaalse templi sertifikaadid DAS [7] mõistes. Täpsem kirjeldus on toodud käesoleva CP punktis 1.5.4.

Käesolev CP koostamisel on kasutatud IETFi (*Internet Engineering Task Force*) soovitusliku dokumenti RFC 3647 [3].

1.3. Mõisted ja Lühendid

1.3.1. Mõisted

Vt CPS p.10

Mõiste	Kirjeldus
Objekti identifikaator	Unikaalne objekti tunnuskood (OID).
Sertifitseerija	Sertifikaate väljastav üksus.
Sertifitseerimispoliitika	Reeglid, millega nähakse ette, kuidas kasutavad sertifikaati teatavad kasutajarühmad või kuidas sertifikaati kohaldatakse teatavat laadi rakenduste puhul, ning ühised turbenõuded.
Sertifitseerimispõhimõtted	Sertifitseerija sertifikaatide väljastamise, haldamise, kehtetuks tunnistamise, uuendamise ja võtmete uuendamise hea tava kirjeldus.
Jagatud kontroll	Turvameede, millega tagatakse juurdepääs turvaobjektidele vaid kahe või enama võtmeisiku samaaegsel rakendamisel.

1.3.2. Kasutatud Lühendid

Vt CPS p.11

Lühend	Kirjeldus
CP	Sertifitseerimispoliitika (*Certification Policy*)
CPS	Sertifitseerimispõhimõtted (*Certification Practice Statement*)
CRL	Sertifikaatide tühistusnimekiri (*Certificate Revocation List*)
DAS	Eesti Vabariigi digitaalallkirja seadus
IANA	*Internet Assigned Numbers Authority* jaotab ülemaailmselt IP-aadresse, haldab domeeninimede süsteemi (DNS) juurtsooni ja määrab Internetis kasutatavaid sümboleid ja arvkoode.
OID	Objekti identifikaator, unikaalne objekti tunnuskood (*Object Identifier*)
SK	AS Sertifitseerimiskeskus, sertifitseerimisteenuse osutaja
CSR	Sertifikaadi signeerimistaotlus
DNS	(Domain Name System) Domeeni nimede süsteem, mille täpsema definitsiooni kirjeldab RFC 3467 (http://tools.ietf.org/html/rfc3467)
ASKT	Asutuse sertifikaatide kasutustingimused
CAA kirje	(CAA - The Certification Authority Authorization) sertifitseerimisteenuse osutaja autoriseerimine - DNS ressursikirje tüüp, mis näitab, millised sertifitseerimisteenuse osutajad on volitatud väljastama sertifikaate sellele domeeniaadressile. Viide allikale: RFC 6844 (http:tools.ietf.org/html/rfc6844).

1.4. Dokumendi pealkiri ja versioon

1.4.1. Sertifitseerimispoliitika identifitseerimine

Dokumendi nimetus: SK asutuse sertifikaatide sertifitseerimispoliitika.

Käesoleva CP tunnuskood on OID: 1.3.6.1.4.1.10015.7.1.3

CP tunnuskood on koostatud vastavalt järgnevale tabelile 1.

Parameeter	OID viide
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	7.1
CP versiooni tunnus	3

1.5. Organisatsioon ja kasutusvaldkond

1.5.1. Sertifitseerimiskeskus (SK)

Vt CPS p.1.2.1.

1.5.2. SK registreerimiskeskus

1.5.2.1. Klienditeeninduspunktid

Vt CPS p.1.2.2.1.

SK klienditeeninduspunktiks on Sertifitseerimiskeskus AS ise.

1.5.2.2. Abiliin

Vt CPS p.1.2.2.2.

Abiliini teenus käesoleva CP raames puudub.

1.5.3. Kasutaja

1.5.3.1. 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.

1.5.3.2. Huvitatud isik

Vt CPS p.1.2.3.2.

1.5.4. Sertifikaatide kasutusvaldkond

Vt CPS p.1.2.4.

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

- **SSL serveri sertifikaat** - SSL serverile (HTTPS, IMAPS, FTPS jt) antav sertifikaat tõestamaks SSL serveri omaniku autentsust;

- **Digitaalse templi sertifikaat** - kasutatakse tõendamaks digitaalse dokumendi terviklust ning omaniku seost sellise dokumendiga.

Digitaalse templi sertifikaati saab kasutada vastavalt DAS-le [7].

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.

1.6. Kontaktandmed

Vt CPS p. 1.3.

AS Sertifitseerimiskeskus
Äriregistri kood 10747013
Pärnu mnt 141, 11314 Tallinn
Tel +372 610 1880
Faks +372 610 1881
E-post: info@sk.ee
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 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. Klienditeeninduspunkti kohustused

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. Abiliini kohustused

Abiliin puudub.

2.1.3. Nõuded kliendile

Vt CPS p.2.1.3.

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) [5].

2.1.4. Nõuded huvitatud isikule

Vt CPS p.2.1.4.

2.1.5. Nõuded kataloogiteenusele

Vt CPS p.2.1.5.

Lisanõudeid kataloogiteenuse toimimiseks ette ei nähta.

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. 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.

SK vastutab täiendavalt tipmise sertifitseerija isiklike võtmete salastatuse ja sertifikaatide võimaliku väärkasutuse eest.

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 aadressil http://www.sk.ee/repository/crls

2.4.2. Avaldamise sagedus

Vt CPS p.2.4.2.

Sertifikaatide tühistusnimekirja uuendatakse ja avaldatakse regulaarselt mitte harvemini kui iga 12 tunni järel.

2.4.3. Juurdepääsureeglid

Vt CPS p.2.4.3.

2.4.4. Kataloogiteenus

Vt CPS p.2.4.4.

Käesoleva CP alusel väljastatud sertifikaadid avaldatakse aktiveerimisel avalikus kataloogis aadressil ldap://ldap.sk.ee.

Sertifikaadi kehtivuse peatamisel või kehtetuks tunnistamisel sertifikaat kustutatakse kataloogist. Kehtivuse peatatuse lõpetamisel sertifikaat taasavaldatakse.

Aegunud sertifikaadid kustutatakse kataloogist aegumiskuupäevale järgneval päeval.

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 “SK asutuse sertifikaatide ja tühistusnimekirja profiil” [2].

SSL serveri sertifikaatide puhul eraldusnime unikaalsust ei tagata.

SSL serveri sertifikaadi eraldusnime omistamisel lähtutakse kliendi seadme domeeninime ja/või IP-aadressi seotusest kliendiga, seejuures nimi peab olema avaliku DNS'iga lahendatav ning IPv4 või IPv6 aadress ei tohi olla IANA poolt märgitud kui 'reserved'.

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 [6] 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

Vt CPS p.4.2.1.

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.

SSL serveri sertifikaadi eraldusnime omistamisel lähtutakse kliendi seadme domeeninime ja/või IP-aadressi seotusest kliendiga. Sertifikaadi eraldusnimi peab olema avaliku DNS teenuse poolt lahendatav ning IPv4 või IPv6 aadress ei tohi olla Internet Assigned Numbers Authority poolt märgitud kui 'reserved'.
SSL serveri sertifikaadi väljastamisel SK ei kontrolli CAA kirjet.

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.

Digitaalse templi sertifikaadi väljastamiseks juriidiline isik:

- peab olema registreeritud Eestis;
- peab olema leitav Eesti Äriregistrist;
- ei tohi olla pankrotis või likvideerimisel, tema tegevus tohi olla peatatud või muus sellesarnases seisukorras.

Digitaalse templi sertifikaadi taotluse peab DAS [7] mõistes digitaalselt allkirjastama asutuse allkirjaõiguslik isik või tema digiallkirjaga volitatud isik.

SSL serveri sertifikaadi väljastamiseks juriidiline isik:

- peab olema registreeritud Eestis, Lätis, Leedus, Soomes või Rootsis ja leitav Euroopa Äriregistrist;
- ei tohi olla asukohamaa seaduste kohaselt pankrotis või likvideerimisel, tema tegevus ei tohi olla peatatud või muus sellesarnases seisukorras.

Lisaks, SSL serveri sertifikaadi väljastamiseks:

- peavad IANA registrist olema leitavad domeeni registreerinud Registripidaja andmed;
- peab domeen olema registreeritud vastava riigi Registripidaja registris;
- peab sertifikaaditaotluse digitaalselt allkirjastama Registripidaja registris märgitud domeeni halduskontakt või asutuse allkirjaõiguslik isik.

Juhul, kui domeeni haldajal ei ole DAS [7] mõistes digiallkirjastamise võimalust, on SK-l õigus rakendada lisakontrolle sertifikaadi väljastamiseks.

Kõigi teiste asutuste sertifikaatide puhul juriidiline isik:

- peab olema registreeritud Eestis, Lätis, Leedus, Soomes või Rootsis ja leitav Euroopa Äriregistrist;
- ei tohi olla asukohamaa seaduste kohaselt pankrotis või likvideerimisel, tema tegevus ei tohi olla peatatud või muus sellesarnases seisukorras.

Sertifikaadi taotluse peab DAS [7] mõistes digiallkirjastama asutuse allkirjaõiguslik isik või tema digiallkirjaga volitatud isik. Juhul, kui allkirjaõiguslikul isikul ei ole DAS mõistes digiallkirjastamise võimalust, on SK-l õigus rakendada lisakontrolle sertifikaadi väljastamiseks.

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 väljastatavale asutuse sertifikaadile peab klient järele tulema klienditeeninduspunkti.

Turvalisel allkirja andmise vahendil väljastatava digitaalse templi sertifikaadi väljastamisel kontrollib klienditeeninduspunkti töötaja Kliendi esindaja isikusamasust isikut tõendava dokumendi alusel ning tema volitusi sertifikaadi kätte saamiseks. Kliendi esindaja peab olema volitatud Kliendi allkirjaõigusliku ja sertifikaadi taotluse allkirjastanud isiku poolt.

Kliendi esindaja kinnitab oma allkirjaga, et on sertifikaadi kätte saanud ning tutvunud käesoleva CP ja „Asutuse sertifikaatide kasutustingimustega“ (ASKT) [5].

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

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 kehtivuse 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 kehtivuse 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 kehtivuse 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 klienditeeninduspunkti 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-l on õigus täiendavalt sertifikaat kehtetuks tunnistada alljärgnevatel põhjustel:

- Vastavalt „Asutuse sertifikaatide kasutustingimustele“ (ASKT) [5];
- Klient teatab, et esialgne sertifikaadi taotlus ei olnud volitatud ja Klient ei anna 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 „Asutuse sertifikaatide kasutustingimuste” (ASKT) [5] 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;
- SK saab teada, et sertifikaati on kasutatud kuriteo toimepanemiseks, nagu näiteks arvutikelmus, nuhkvara, pahavara ja arvutiviiruse levitamine jne.

4.6.2. Sertifikaadi kehtetuks tunnistamise taotluse 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 CRL-ide tehnilised profiilid

7.1. Sertifikaatide profiil

Vt CPS p.7.1.

Asutuse sertifikaadid kehtivad kuni 1125 päeva (3 aastat ja 30 päeva), välja arvatud B4B profiili sertifikaadid, mis kehtivad kuni 1855 päeva (5 aastat ja 30 päeva).

Sertifikaatide täpne profiil on toodud dokumendis “SK asutuse sertifikaatide ja tühistusnimekirja profiil” [2].

7.2. Tühistusnimekirjad (CRL)

Vt CPS p.7.2.

Sertifikaatide tühistusnimekirja (CRL) formaadiks on x.509v2 (defineeritud RFC5280-s [4]).

Tühistusnimekirja täpne profiil on toodud dokumendis “SK asutuse sertifikaatide ja tühistusnimekirja profiil” [2].

8. Sertifitseerimispoliitika haldus

Vt CPS p.8.

Käesolev CP ja viidatud dokumendid AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtted [1] ning „SK asutuse sertifikaatide ja tühistusnimekirja profiil” [2] avaldatakse SK koduleheküljel.

Sertifitseerimispoliitika sisulist tähendust mitte muutvate paranduste puhul nagu õigekirjavigade parandamine, tõlkimine ja kontaktandmete ajakohastamine, tuleb muudatused dokumenteerida käesoleva dokumendi versiooni info 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.

Sertifitseerimispoliitika sisuliseks muutmiseks teeb SK muudatusettepaneku, mille täistekst avalikustatakse elektrooniliselt SK koduleheküljel, 90 päeva enne muudetud sertifitseerimispoliitika planeeritavat kehtima hakkamist.

Pärast muudatusettepaneku elektroonilist avaldamist, on Kliendil võimalik esitada 30 päeva jooksul muudatusettepanekule põhjendatuid kommentaare, millele järgneb maksimaalselt 30 päevane muudatusettepanekule esitatud kommentaaride analüüs. 60 päeva pärast, alates muudatusettepaneku elektroonilisest avaldamisest, avalikustatakse uus sertifitseerimispoliitika versioon elektrooniliselt SK koduleheküljel või võetakse muudatusettepanek tagasi.

9. Viidatud ja seonduvad dokumendid

[1] AS Sertifitseerimiskeskus, sertifitseerimispõhimõtted;

[2] SK asutuse sertifikaatide ja tühistusnimekirja profiil;

[3] RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;

[4] RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[5] Asutuse sertifikaatide kasutustingimused. AS Sertifitseerimiskeskus;

[6] PKCS#10 – Certification Request Syntax Standard. http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs10-certification-request-syntax-standard.htm;

[7] Eesti Vabariigi digitaalallkirja seadus, RT I 2000, 26, 150