EE Certification Centre Root CA sertifitseerimispoliitika

Versioon 2.0
OID: 1.3.6.1.4.1.10015.100.1
Kehtiv alates 17.12.2015

Nõuded AS Sertifitseerimiskeskus tipmise sertifitseerija poolt väljastatavate alamsertifitseerijate sertifikaatide väljastamiseks ja teenindamiseks.

Versiooni info		
Kuupäev	**Versioon**	**Muudatused**
17.12.2015	2.0	Muudetud punkti 1.3. Kasutatud lühendid Muudetud punkti 1.4. Sertifitseerimispoliitika identifitseerimine Täiendatud punkti 1.5.4. Sertifikaatide kasutusvaldkond Uuendatud punkti 1.6. Kontaktandmed Uuendatud punkti 2.4.1. SK informatsiooni avaldamine Muudetud punkti 2.4.4. Kataloogiteenus Muudetud punkti 3.1. Kliendi isikusamasuse kontroll Muudetud punkti 4.1. Sertifikaaditaotluse esitamine Muudetud punkti 4.2. Sertifikaaditaotluse menetlemine Muudetud punkti 4.2.2. Sertifikaadi väljastamine Muudetud punkti 6.1.2.1. Kliendi võtmete moodustamine Muudetud punkti 6.1.2.2. Kliendi isikliku võtme ja aktiveerimiskoodide kaitse personaliseerimise käigus Muudetud punkti 6.3. Sertifitseerimisteenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus Uuendatud punkti 9. Viidatud ja seonduvad dokumendid
01.10.2010	1.1	Esmane versioon

Sisukord

1. Sissejuhatus

1.1. Ülevaade

Käesolev dokument (edaspidi sertifitseerimispoliitika, CP) on reeglite kogum, mis määrab peamised tööpõhimõtted ja -kontseptsioonid AS Sertifitseerimiskeskus tipmise sertifitseerija poolt väljastatavate alamsertifitseerijate 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.

Käesolev CP laieneb ainult AS-i Sertifitseerimiskeskus tipmise sertifitseerija poolt väljastatud sertifikaatidele.

Käesoleva CP koostamisel on kasutatud IETFi (*Internet Engineering Task Force*) soovitusliku dokumenti RFC 2527 [3].

1.2. Kasutatud terminoloogia

Termin	Definitsioon

1.3. Kasutatud lühendid

Lühend	Definitsioon
SK	AS Sertifitseerimiskeskus, sertifitseerimisteenuse osutaja.
STO	Sertifitseerimise Registris registreeritud sertifitseerimisteenuse osutaja
DAS	Digitaalallkirja seadus
ECC	Elliptic Curve Cryptography

1.4. Sertifitseerimispoliitika identifitseerimine

Käesoleva CP tunnuskood on **OID: 1.3.6.1.4.1.10015.100.1**

OID tunnuskood lisatakse käesoleva CP alusel väljastatavasse sertifikaati.

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

Parameeter	Viide OIDis
IANA registris ASile Sertifitseerimiskeskus antud tunnus	10015
Sertifitseerimisteenuse tunnus	100.1

Tabel 1. CP tunnuskoodi koostamine

1.5. Organisatsioon ja kasutusvaldkond

1.5.1. Sertifitseerimiskeskus (SK)

Vt CPS p.1.2.1.

SK ei kasuta kolmandaid osapooli tipmise sertifitseerija poolt väljastatavate sertifikaatide väljastamiseks ja haldamiseks.

1.5.2. SK registreerimiskeskus

1.5.2.1. Klienditeeninduspunktid

Vt CPS p.1.2.2.1.

Klienditeeninduspunkt käesoleva CP raames puudub.

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 mõistes on klient ainult AS Sertifitseerimiskeskus, kes on käesoleva CP alusel väljastatud sertifikaadi omanik.

Samaaegselt võib kehtida rohkem kui üks tipmise sertifitseerija poolt väljastatud sertifikaat.

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 ainult AS Sertifitseerimiskeskuse alamsertifitseerijate sertifikaate ja teenindavaid sertifikaate.

CP ei sea piiranguid sertifikaatide kasutamiseks erinevates tarkvararakendustes ega rakendusvaldkondades.

1.6. Kontaktandmed

Vt CPS p.1.3.

SK

AS Sertifitseerimiskeskus
Äriregistri kood 10747013
Pärnu mnt 141, 11314 Tallinn
Telefon +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:

- 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.

2.1.2. Registreerimiskeskuse kohustused

2.1.2.1. Klienditeeninduspunkti kohustused

Klienditeeninduspunkt puudub.

2.1.2.2. Abiliini kohustused

Abiliin puudub.

2.1.3. Nõuded kliendile

Vt CPS p.2.1.3.

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 puudub.

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/repositoorium/CRL/

2.4.2. Avaldamise sagedus

Vt CPS p.2.4.2.

Sertifikaatide tühistusnimekirju avaldatakse reeglina iga 3 kuu 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 alamsertifitseerijate sertifikaadid, mis väljastavad või hakkavad väljastama lõppkasutajate sertifikaate, avaldatakse avalikus kataloogis aadressil ldap://ldap.sk.ee.

Sertifikaadi kehtetuks tunnistamisel sertifikaat kustutatakse kataloogist.
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

Kliendi esindajad ja nende volitused tipmise sertifitseerija võtmete moodustamiseks ja sertifikaadi väljastamiseks määratakse SK juhataja käskkirjaga. Käskkirjaga moodustatakse vähemalt 4 liikmeline komisjon, mida juhib juhataja poolt määratud komisjoni esimees. Võtmete moodustamise protseduuri juures viibiv sõltumatu audiitor kontrollib protseduuril osalevate isikute isikusamasust ning kas isikud on samad, kes käskkirjas märgitud.

3.2. Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord

Kliendi isikliku võtme kooskõlalisus tagatakse SK siseprotseduuridega. Protseduur viiakse läbi komisjoni kuuluvate isikute poolt ja välise sõltumatu audiitori esindaja juuresolekul.

3.3. Eraldusnimi

Vt CPS p.3.3.

Sertifikaadi eraldusnimi koostatakse vastavalt dokumendile “SK alam CA sertifikaadi ja tühistusnimekirja profiil” [2].

4. Sertifitseerimisteenuse osutamine Sertifitseerimismenetluse kord ja tähtajad

4.1. Sertifikaaditaotluse esitamine

Vt CPS p.4.1.

SK juhataja kinnitab oma käskkirjaga tipmise sertifitseerija võtmete loomise ja sertifikaadi väljastamise taotluse, määrates ära protseduuri läbi viivate isikute koosseisu ning protseduuri läbi viimise aja ja koha. Käskkirjas määratakse ära, et võtmete loomise ja sertifikaadi taotluse esitamise protseduur viiakse läbi minimaalselt 4 SK esindaja ja ühe välise sõltumatu audiitori esindaja juuresolekul.

Tipmise sertifitseerija sertifikaadi taotluse esitamise kord peab minimaalselt olema kooskõlas DAS-iga [4] ning lisaks järgnevate punktidega:

- Sertifikaaditaotlus peab sisaldama vähemalt järgnevaid punkte:
  - viide taotletava sertifikaadi sertifitseerimis-poliitikale;
  - märge selle kohta, kuidas toimub võtmepaari genereerimine;

4.2. Sertifikaaditaotluse menetlemine

Sertifikaaditaotluse töötlemise tähtaeg on määratletud punktis 4.1 sätestatud käskkirjaga.

Võtmed moodustatakse ja sertifikaadi taotlus koostatakse käskkirjas määratletud komisjoni ja välise audiitori juuresolekul käsitsi off-line toiminguna SK infosüsteemist. Läbi viidud protseduuri kohta koostatakse akt, milles on välja toodud protseduuri kulg ning väljastatud CA avalik võti ja võtme räsi. Akti allkirjastavad komisjoni liikmed ja sõltumatu väline audiitor. Väline sõltumatu audiitor kinnitab, et sertifikaadipäring on tehtud vastavalt loodud võtmetele.

4.2.1. Otsuse tegemine

Vt CPS p.4.2.1.

Otsustamist ei toimu, esitatud taotlus kuulub täitmisele.

4.2.2. Sertifikaadi väljastamine

Sertifikaat väljastatakse käskkirjas määratletud komisjoni juuresolekul käsitsi off-line toiminguna SK infosüsteemist. Väljastatud sertifikaat on kohe aktiivses staatuses. Läbi viidud protseduuri kohta koostatakse akt, milles on välja toodud protseduuri kulg ning väljastatud sertifikaat. Akti allkirjastavad komisjoni liikmed.

4.2.3. Sertifikaatide üle arvestuse pidamise kord

Vt CPS p.4.2.3.

4.2.4. Sertifikaadi kontroll ja tõestamine

Vt CPS p.4.2.4.

4.2.5. Sertifikaadi uuendamine

Sertifikaadi uuendamist ei toimu.

4.3. Sertifikaadi kehtetuks tunnistamise ja kehtivuse peatamise taotlused

Vt CPS p.4.3.

4.4. Sertifikaatide kehtivuse peatamine

Sertifikaadi kehtivuse peatamist ei toimu.

4.5. Sertifikaadi kehtivuse peatatuse lõpetamine

Sertifikaadi kehtivuse peatatuse lõpetamist ei toimu.

4.6. Sertifikaadi kehtetuks tunnistamine

4.6.1. Sertifikaadi kehtetuks tunnistamise volitused

Vt CPS p.4.6.1.

4.6.2. Sertifikaadi kehtetuks tunnistamise taotluse esitamine

Vt CPS p.4.6.2.

Sertifikaadi kehtetuks tunnistamise avaldus tuleb esitada allkirjastatult SK juhatajale.

4.6.3. Sertifikaadi kehtetuks tunnistamise menetlus

Vt CPS p.4.6.3.

Sertifikaatide kehtetuks tunnistamise taotluse saab esitada ainult SK juhatajale punktis 1.6 toodud kontaktaadressil. Viiakse läbi esitatud taotluse põhjendatuse kontroll esitatud tõendusmaterjalide põhjal ja muu kättesaadava info põhjal.

4.6.4. Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus

Vt CPS p.4.6.4.

Peale sertifikaadi kehtetuks tunnistamist väljastab SK kohe uue tühistusnimekirja, mis sisaldab kehtetuks tunnistatud sertifikaadi järjekorranumbrit.

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.

Võtmete loomisel rakendatakse jagatud vastutuse printsiipi, st. mitte keegi ei tea kõiki süsteemi käivitamiseks vajalikke paroole. Vajalikud kasutajate paroolid on jagatud vähemalt kaheks.

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.

Käesoleva poliitika alusel ei väljastata sertifikaate väiksemate võtmepaaride pikkusega kui RSA2048 bitti või ECC224 bitti. Konkreetse väljastatava CA võtme pikkus määratletakse vastava CA väljastamisel kehtivatele turvanõuetele.

6.1.2. Kliendi võtmed

6.1.2.1. Kliendi võtmete moodustamine

Võtmete moodustamisel kasutatavad algoritmid, võtmepikkused ja teised parameetrid on toodud dokumendis „SK alam CA sertifikaadi ja tühistusnimekirja profiil" [2].
Võtmed luuakse vastavalt juhendile, mis on kinnitatud SK juhataja käskkirjaga.

6.1.2.2. Kliendi isikliku võtme ja aktiveerimiskoodide kaitse personaliseerimise käigus

Vt CPS p.6.1.2.2

Kliendi isiklik võti on kaitstud FIPS140-2 Level 3 turvatasemega turvamooduliga.
Kõik aktiveerimiskoodid jagatakse vähemalt kaheks. Aktiveerimiskoodi määramise ajal on arvuti juures ainult antud aktiveerimiskoodi osa sisestaja, kes sisestab oma osa aktiveerimiskoodist ning kirjutab aktiveerimiskoodi osa kahele paberile ja ümbrikustab need.
Aktiveerimiskood peab olema vähemalt 12 sümbolit pikk, sisaldades suur- ja väiketähti, vähemalt üht numbrit ja üht sümbolit.
Aktiveerimiskoodi osa peab olema vähemalt 6 sümbolit pikk sisaldades suur- ja väiketähti, vähemalt üht numbrit ja üht sümbolit.
Aktiveerimiskoodid hoiustatakse erinevates turvalistes säilituskohtades.

6.1.2.3. Kliendi isikliku võtme aktiveerimine

Vt CPS p.6.1.2.3.

Võtmete aktiveerimine toimub jagatud kontrolli põhimõttel, kus aktiveerimiskoodid on jagatud vähemalt 2 isiku vahel välistamaks süsteemi käivitamist ühe isiku poolt.
Aktiveerimiskoodi osa sisestamisel on arvuti juures ainult antud aktiveerimiskoodi sisestav isik.
SK vastutab käesoleva CP mõistes kliendi isikliku võtme aktiveerimise turvalisuse eest.

6.1.2.4. Kliendi võtmete varundamine ja deponeerimine

Võtmete varundamist ja deponeerimist ei tehta.

6.2. Süsteemiturve

Vt CPS p.6.2.

6.3. Sertifitseerimisteenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus

Vt CPS p.6.3.

SK kasutab käesoleva CP alusel sertifitseerimisteenuste osutamiseks Safelayer Secure Communications S.A. KeyOne tarkvara.

6.4. Sertifitseerimisteenuse osutamisel tekkinud andmete säilitamine ja kaitse

Vt CPS p.6.4.

7. Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid

Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid on toodud dokumendis „SK alam CA sertifikaadi ja tühistusnimekirja profiil" [2].

8. Sertifitseerimispoliitika haldus

Vt CPS p.8.

Käesolev CP ja viidatud dokumendid AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtted (CPS) [1] ning „SK alam CA sertifikaadi ja tühistusnimekirja profiil " [2] avaldatakse SK koduleheküljel.

9. Viidatud ja seonduvad dokumendid

Viidatud dokumendid:

[1] AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtted (CPS), avaldatud: https://www.sk.ee/repositoorium/CPS/
[2] SK alam CA sertifikaadi ja tühistusnimekirja profiil, avaldatud: https://www.sk.ee/repositoorium/profiil/
[3] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, https://www.ietf.org/rfc/rfc2527.txt

[4] Digitaalallkirja seadus, avaldatud: https://www.riigiteataja.ee/akt/114032014012&leiaKehtiv;