AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted CPS

Versioon 1.1

OID: 1.3.6.1.4.1.10015.1.1.1

31.08.2001

Versioonid ja muudatused:

Versioon	Kuupäev	Kommentaarid
1.0	31.08.2001	

Sisukord

1

Sissejuhatus

AS'i Sertifitseerimiskeskus (edaspidi SK) on asutatud 16 veebruaril 2001. a. Aktsiaseltsi omanikeks on võrdse 25% suuruse osalusega Hansapank, Eesti Ühispank, AS Eesti Telefon ja AS EMT. AS'I Sertifitseerimiskeskus põhitegevusalaks on digitaalallkirja kasutuselevõtuks vajalike sertifitseerimis- ja sellega seotud teiste teenuste osutamine, mis võimaldavad igapäevaelus turvalist ja tõendatud elektroonilist kommunikatsiooni nii riigiasutuste kui äriettevõtetega.

AS Sertifitseerimiskeskus missiooniks on kindlustada kliente täiesti usaldusväärse sertifitseerimisteenusega vastavalt EV õigusaktidele, olla andmekaitse alal üks turvalisemaid asutusi Eestis ning kasutada tipptehnoloogiaid lähtudes konkreetsest vajadusest ja majanduslikust aspektist.

Tehnilise teadmusbaasi ja avaliku arvamuse kujundamisel on märkimisväärne omanike tugi ja positsioon. Äsja alustanud firmana ei ole me seotud ajaloost külge jäänud protseduurireeglitega ega vana tehnoloogiaga.

1.1 Ülevaade

Käesolev dokument (edaspidi CPS) kirjeldab AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtteid ning sertifitseerimisteenuse osutamisel kasutatavaid protseduure.

Käesolev sertifitseerimispoliitika laieneb ainult ASi Sertifitseerimiskeskus poolt väljastatud digitaalsetele sertifikaatidele.

Käesolev CPS on aluseks erinevate sertifitseerimispoliitikate koostamiseks ja nendele vastavate sertifitseerimisteenuste pakkumiseks AS Sertifitseerimiskeskuses.

Käesolev CPS koostamisel on kasutatud IETFi (*Internet Engineering Task Force*) soovitusliku dokumenti RFC 2527..

1.2 Sertifitseerimispõhimõtete identifitseerimine

Käesoleva CPSi tunnuskood on **OID: 1.3.6.1.4.1.10015.1**

CPSi 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

Parameeter	Viide OIDis
Sertifitseerimisteenuse tunnus	1
CPS versiooni tunnus	1.1

Tabel 1. CPS tunnuskoodi koostamine

Käesolevale CPSile viidatakse AS Sertifitseerimiskeskuse tipmise sertifitseerija sertifikaadi sertifitseerimispoliitika laienduses.

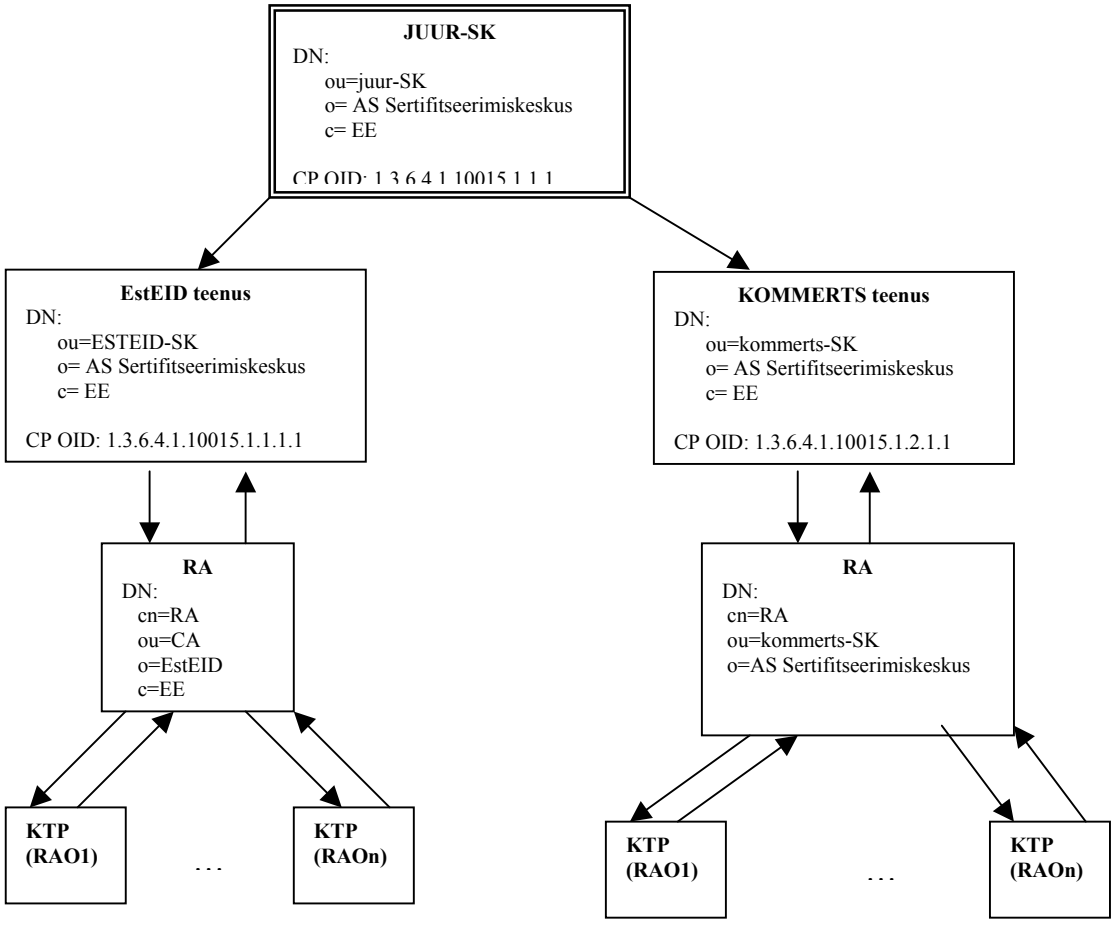
1.3 Organisatsioon ja kasutusvaldkond

1.3.1 Sertifitseerimiskeskus (SK)

SK osutab sertifitseerimisteenust vastavalt käesoleva CPSi põhjal koostatud sertifitseerimispoliitikale koos sellega seonduvate lisateenustega (kataloogiteenus).

Sertifitseerimispoliitikate tüübid ja nendele vastavad OIDid on toodud tabelis 1. Sertifitseerimispoliitika OID on toodud ära vastava sertifitseerija kinnitusvõtme sertifikaadi sertifitseerimispoliitika laienduses.

SK struktuur on toodud ära skeemil 1.



Skeem 1. SK PKI struktuur

Sertifitseerimispoliitika OID	Kirjeldus	Kasutusala piirangud
1.3.6.4.1.10015.1.1.1	SK juur sertifitseerija; alamsertifitseerijate loomine ja sertifitseerimine;	Alamsertifitseerijate sertifitseerimine
1.3.6.4.1.10015.1.1.1.1	Sertifitseerimispoliitika riigi EstEID kaartidele väljastatavate sertifikaatide teenindamiseks	Isikusertifikaadid: digitaalallkirja võimaldavad sertifikaadid; autentimissertifikaadid
1.3.6.4.1.10015.1.2.1.1	Ärilisel eesmärgil väljastatavate sertifikaatide teenindamiseks.	Isikusertifikaadid: Piiranguid ei ole (digitaalallkirja võimaldavad sertifikaadid; autentimissertifikaadid; e-maili sertifikaadid; rollisertifikaadid vms);

Tabel 2. SK sertifitseerijate sertifitseerimispoliitikad

1.3.2 Registreerimiskeskus

1.3.2.1 SK klienditeeninduspunkt (KTP)

SK klienditeeninduspunkt tegutseb SK esindajana SK ja Kliendi vahelistes suhetes. SK klienditeeninduspunkt, käesoleva CPSi mõistes, võtab vastu avaldusi sertifikaatide taotlemiseks, uuendamiseks, kehtivuse lõpetamiseks, sertifikaatide peatamiseks ja sertifikaatide peatatuse lõpetamiseks.

SK klienditeeninduspunktide töötajad on saanud vastava koolituse kvaliteetse teenuse osutamiseks SK klientidele.

SK klienditeeninduspunktid võivad erinevate sertifitseerimispoliitikate puhul olla erinevad. SK klienditeeninduspunkti ja SK vaheline suhe on ära määratud kahepoolse lepinguga.

SK klienditeeninduspunktide arv võib erinevate sertifitseerimispoliitikate puhul erineda.

Informatsiooni SK klienditeeninduspunktide ja nende kontaktandmete kohta esitatakse SK koduleheküljel.

1.3.2.2 Abiliin

Abiliin tegutseb SK esindajana klientide telefoniteenindusega ja :

- võtab ööpäevaringselt klientidelt ja teistelt osapooltelt vastu taotlusi sertifikaatide peatamiseks, eelnevalt identifitseerides isiku vastavalt kehtestatud isikusamasuse kontrolli protseduuridele;
- pakub ööpäevaringselt esmast abi sertifikaatide kasutamisel ning annab turvalisust puudutavaid nõuandeid.

Informatsiooni abiliini ja tema kontaktandmete kohta esitatakse SK koduleheküljel (http://www.sk.ee). Samas on toodud ära ka juhised abiliini poole pöördumiseks.

1.3.3 Kasutaja

1.3.3.1 Klient

Klient on käesoleva CPSi alusel koostatud sertifitseerimispoliitika alusel väljastatud sertifikaadi omanik.

Kliendi eraldusnimi sertifikaadis koostatakse vastavalt sertifitseerimispoliitikates toodud sertifikaadiprofiilile, mis on koostatud vastavalt punktis 7.1 toodud nõuetele. SK tagab kliendi eraldusnime ja sertifikaadi kinnitamisel kasutatud SK salajase võtmega seotud sertifikaadi eraldusnime kombinatsiooni unikaalsuse.

1.3.3.2 Huvitatud isik

Huvitatud isik on osapool, kes võtab sertifikaadi põhjal vastu otsuse ja kasutades sertifikaati:

- on eelnevalt tutvunud käesoleva CPSiga ja selles viidatud dokumentidega
- kontrollib sertifikaadi kehtivust SK avalikus kataloogis või värskeimas tühistusnimekirjas
- kontrollib sertifikaadi kasutusala vastavust
- digitaalset allkirjastamist võimaldavate sertifikaatide puhul kontrollib digitaalselt allkirjastatud andmekogumi terviklikkust ja identifitseerib allkirjastaja

1.3.4 Sertifikaatide kasutusvaldkond

Sertifikaatide kasutamine peab olema kooskõlas sertifikaadi sertifitseerimispoliitikas toodud nõuetele ja EV kehtestatud õigusaktidele.

Väljastatavate sertifikaatide kasutusvaldkond võib vastavalt sertifikaadi profiilile olla piiratud. Vastavad piirangumehhanismid on kirjeldatud sertifikaadi väljastamisel aluseks olevas sertifitseerimispoliitikas.

Käesolev CPS ei piira SK poolt väljastatud sertifikaatide kasutamist erinevates tarkvararakendustes.

1.4 Kontaktandmed

Kõikides sertifitseerimisteenusega seotud küsimustega (näiteks sertifitseerimiskeskuse, registreerimiskeskuse ja abiliini tegevusega seotud küsimustega) tuleb pöörduda järgnevalt toodud aadressil:

AS Sertifitseerimiskeskus
Äriregistri kood 10747013
Pärnu mnt 12, 10148 Tallinn
Tel +372 610 1880
Faks +372 610 1881
E-post: pki@sk.ee
http://www.sk.ee/

Kontaktandmete muutumisel teavitatakse sellest koheselt SK koduleheküljel.

2 Üldtingimused

2.1 Kohustused

2.1.1 SK kohustused

SK tagab, et
- sertifitseerimisteenuse osutamine on kooskõlas EV õigusaktidega;
- sertifitseerimisteenuse osutamine on kooskõlas käesoleva CPSiga.

SK on teenuste osutamise perioodil kohustatud säilitama enda registreerituse sertifitseerimise riiklikus registris.

SK kohustub:
- avalikustama oma sertifitseerimispõhimõtted ja sertifikaatide sertifitseerimispoliitikad ning tagama nende kättesaadavuse üldkasutatavas andmesidevõrgus;
- tagama sertifitseerimisteenuse osutamisel teatavaks saanud avaldamisele mittekuuluva teabe saladuses hoidmise;
- pidama arvestust enda poolt väljastatud sertifikaatide ja nende kehtivuse üle;
- digitaalallkirja võimaldavate sertifikaatide puhul võtma ööpäevaringselt vastu avaldusi sertifikaatide kehtivuse peatamiseks;
- digitaalallkirja võimaldavate sertifikaatide puhul tõendama huvitatud isiku nõudel oma esindaja digitaalallkirjaga enda poolt väljastatud sertifikaadis sisalduvale avalikule võtmele vastava isikliku võtmega antud digitaalallkirja kehtivust;
- tagama ööpäevaringselt sertifikaatide kehtivuse kontrollivõimaluse üldkasutatavas andmesidevõrgus;
- säilitama sertifitseerimisega seotud dokumentatsiooni oma tegevuse lõpuni;

- tagama igal aastal infosüsteemi auditi teostamise ning esitama auditi tulemused sertifitseerimisteenuse riikliku registri volitatud töötlejale;
- avalikustama kohustusliku kindlustuslepingu tingimused üldkasutatavas andmesidevõrgus.
- olla registreeritud sertifitseerimise riiklikus registris;

SK töötajal ei tohi olla karistatust tahtlikult toimepandud kuriteo eest.

2.1.2 Registreerimiskeskuse kohustused

2.1.2.1 Klienditeeninduspunkti kohustused

Klienditeeninduspunkt kohustub vastu võtma taotlusi sertifikaatide väljastamiseks, peatamiseks, peatatuse lõpetamiseks ja tühistamiseks ja kontrollima nende avalduste õigsust ja terviklikkust. Klienditeeninduspunkt kohustub kõikide nimetatud toimingute teostamisel kontrollima taotluse esitaja isikusamasust.

Klienditeeninduspunkt kohustub edastama õiged ja terviklikud andmed SKle.

Klienditeeninduspunkti kohustub teenuse osutamist takistava tehnilise rikke korral teatama sellest koheselt SKle ja tegema kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

Klienditeeninduspunkti töötajad kohustuvad läbima teenuse kvaliteetseks osutamiseks vajaliku koolituse. Klienditeeninduspunkti töötajal ei tohi olla karistatust tahtlikult toimepandud kuriteo eest.

2.1.2.2 Abiliini kohustused

Abiliin kohustub osutama Kliendile kõneedastusteenust ööpäevaringselt 7 päeva nädalas.

Abiliin kohustub teenuse osutamist takistava tehnilise rikke korral teatama sellest koheselt SKle ja tegema kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

2.1.3 Kliendi kohustused

Klient peab järgima SK poolt käesolevas CPSis kehtestatud protseduure.

Klient peab edastama SK-le sertifikaaditaotluse esitamisel õiget informatsiooni ning sertifikaati kantud andmete muutumise korral teatab õiged andmed vastavalt sertifikaadi sertifitseerimispoliitikas kehtestatud reeglite kohaselt. Klient on teadlik sellest, et SK võib keelduda sertifikaadi väljastamisest, kui Klient on

sertifikaaditaotluses esitanud informatsiooni, mis on teadlikult vale, ebakorrektne või mittetäielik.

Klient kohustub oma isiklikke võtmeid ja neile vastavaid sertifikaate kasutama SK poolt ettenähtud korras ja viisil.

Klient peab hoidma oma isiklikku võtit turvaliselt.
Klient on teadlik, et isiklikku võtit kaitseva salasõna avalikuks tulek on samaväärne isikliku võtme avalikuks tulekuga. Klient teatab viivitamatult isikliku võtme tema nõusolekuta kasutamise võimalusest.

Klient on teadlik sellest, et SK ei vastuta kliendi isikliku võtme hoidmise eest mitte mingil viisil ega juhul.

Klient on teadlik sellest, et aegunud, kehtetuks tunnistatud või peatatud digitaalallkirja sertifikaadi alusel antud digitaalallkirjad on kehtetud.

2.1.4 Huvitatud isiku kohustused

Huvitatud isik peab tutvuma sertifikaadi aktsepteerimisega seotud kohustuste ja riskidega, mis on toodud käesolevas CPSis ja konkreetse sertifikaadi sertifitseerimispoliitikas.

Kui sertifikaadiga või digitaalallkirjaga ei kaasne piisavalt tõendusmaterjali sertifikaadi kehtivuse kohta, peab huvitatud isik kontrollima sertifikaadi kehtivust sertifikaadi kasutamise või digitaalallkirja andmise ajal kehtinud tühistusnimekirja järgi.

Huvitatud isik peab jälgima sertifikaati kantud piiranguid ning veenduma sertifitseerimispoliitika vastavuses aktsepteeritava tehingu spetsiifikaga.

2.1.4.1 Kataloogiteenuse kohustused

Täpsed kataloogiteenuse kohustused tuuakse ära vastava sertifikaadi sertifitseerimispoliitikas.

Kataloogiteenus peab vastama järgmistele nõuetele:

- ✓ kataloog peab sisaldama kehtivaid sertifikaate ja tühistusnimekirju
- ✓ kataloogis olevad sertifikaadid sisaldavad õiget ja terviklikku informatsiooni
- ✓ kataloog ei tohi sisaldada nn tundlikke isikuandmeid, mis on toodud isikuandmete kaitse seaduses
- ✓ kataloog peab olema ööpäevaringselt kättesaadav avalikus andmesidevõrgus
- ✓ peab olema rakendatud turvameetmed kataloogiteenuse teeskluse vältimiseks

2.2 Vastutus

2.2.1 SK vastutus

SK on vastutav kõigi punktis 2.1.1 ja 2.1.4.1 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 vastutab kõigi punktis 2.1.2.2 toodud kohustuste täitmise eest.

2.2.3 Vastutuse piirid

SK ei vastuta klientide isiklike võtmete salastatuse, sertifikaatide võimaliku väärkasutuse ning huvitatud osapoole poolse sertifikaatide puuduliku kontrolli eest.

SK ei vastuta enda kohustuste mittetäitmise eest, kui selle põhjuseks on sertifitseerimise riikliku registri, andmekaitse järelevalveasutuse või mistahes muu avalik-õigusliku asutuse poolsed vead või turbeprobleemid.

Sertifitseerimispõhimõtetest tulenevate kohustuste mittetäitmist ei loeta rikkumiseks, kui selle põhjuseks olid kohustuse täitja kontrollile mittealluvad nn vääramatu jõud (*Force Majeure*).

2.3 Vaidluste lahendamine

Kõik osapoolte vahelised vaidlused lahendatakse läbirääkimiste teel. Kokkuleppe mittesaavutamise või kestvate eriarvamuste korral lahendatakse vaidlused SK asukohajärgses kohtus.

Pretensioonist tuleb teisi osapooli teavitada hiljemalt 30 kalendripäeva jooksul pretensiooni põhjuse ilmnemisest, kui õigusaktides ei ole sätestatud teisiti.

2.4 Informatsiooni avaldamine ja kataloogiteenus

2.4.1 SK informatsiooni avaldamine

SK kehtiv juursertifikaat ning varem kehtinud sertifikaatide arhiiv avaldatakse aadressil http://www.sk.ee/certs

SK poolt väljaantud ja kehtivad sertifikaadid on avaldatud avalikus kataloogis. Samas on avaldatud ka sertifikaatide tühistusnimekirjad.

Kõik SK otsese tegevusega seotud dokumendid on kättesaadavad avalikus andmesidevõrgus aadressilt http://www.sk.ee/cps/.

SK tagab kogu eelpool nimetatud informatsiooni kättesaadavuse ööpäevaringselt 7 päeva nädalas.

2.4.2 Avaldamise sagedus

Väljastatud sertifikaadid avalikustab SK koheselt avalikus kataloogis.

Sertifikaatide tühistusnimekirju avaldatakse vastavalt peatamisele ja kehtetuks tunnistamisele, kuid vähemalt iga 12 tunni järel.

SK tagab oma koduleheküljel adekvaatse ja ajakohase info sertifitseerimisteenuse kohta.

2.4.3 Juurdepääsureeglid

Üldkasutatavas andmesidevõrgus informatsiooni kättesaamine on tasuta ning juurdepääsu ei piirata. Teistel avaldamisviisidel võib SK kehtestada hinnakirjaga määratava tasu.

2.4.4 Kataloogiteenus

SK poolt väljastatud tühistusnimekirjad ja kehtivad sertifikaadid on avaldatud sertifikaatide kataloogis aadressil ldap://ldap.sk.ee. Tühistusnimekirjade koopiad asuvad aadressil http://www.sk.ee/crls/ .

Kataloogistruktuur ja kasutamiseks vajalikud juhised on toodud SK koduleheküljel.

2.5 Audit

SK tegevust ja toimimist auditeeritakse järgnevalt:

- ✓ SK tegevus auditeeritakse kord aastas vastavalt teede- ja sideministri 3. oktoobri 2000. a määrusele nr 83, “Teenuse osutajate infosüsteemide auditeerimise kord”.
- ✓ kord kvartalis viiakse läbi sisemine audit keskuse siseaudiitori poolt
- ✓ vajadusel auditeeritakse infosüsteem välisauditori poolt peale infosüsteemi muudatusi ja uute teenuste lisandumisel.

Välisaudiitoriks on KPMG Eesti CISA sertifitseeritud audiitor.

Sisemise auditi läbiviimisele esitatakse järgmised nõuded:

a) auditi viib läbi pädev ja vastavate kogemustega spetsialist
b) audit viiakse läbi sõltumata keskuse töötajatest
c) audit viiakse läbi lähtuvalt ISO vastavatest standarditest
d) auditeerimisaruandes esitatud järeldusotsuste täitmise eest vastutab otseselt SK
vastutav esindaja

Sisemise auditeerimise aluseks on järgmised valdkonnad:

a) teenuse kvaliteet
b) teenuste turvalisus
c) SK operatsioonide ja protseduuride turvalisus
d) SK kliendiandmete kaitse ja SK turvalisuspoliitika kehtivus
e) CPSi kehtivus

Auditeerimistulemused avaldatakse SK koduleheküljel.

2.6 Konfidentsiaalsus

2.6.1 Konfidentsiaalne informatsioon

Kogu sertifitseerimisteenuse osutamisel teatavaks saanud ning avaldamisele mittekuuluv informatsioon (näiteks SK toimimise tehnilisi üksikasju käsitlev info) on konfidentsiaalne.

Konfidentsiaalse informatsiooni avalikustamine või edastamine kolmandale poolele on lubatud üksnes informatsiooni õigusliku valdaja kirjalikul loal, kohtu otsuse põhjal või teistel õigusaktides sätestatud juhtudel.

Kõik SK koostööpartnerid on sõlminud vastastikuse konfidentsiaalse informatsiooni lepingu (NDA).

2.6.2 Avalik informatsioon

Avaliku informatsiooni alla kuuluvad järgmised materjalid:

- sertifitseerimispõhimõtted koos viidatavate dokumentidega;
- sertifitseerimispoliitikad koos viidatavate dokumentidega;
- kohustusliku kindlustuslepingu tingimused;
- isikuandmete kaitse põhimõtted;
- SK avalikud võtmed;
- auditeerimistulemused;

Üldkasutatavas andmesidevõrgus informatsiooni kättesaamine on tasuta ning juurdepääsu ei piirata. Teistel avaldamisviisidel võib SK kehtestada hinnakirjaga määratava tasu. Üldkasutavas andmesidevõrgus oleva informatsiooni kättesaadavus on tagatud ööpäevaringselt.

2.6.3 Isikuandmete kaitse

SK isikuandmete kaitse põhimõtted on toodud dokumendis “Isikuandmekaitse põhimõtted”. Isikuandmete kaitsepõhimõtete täitmise tagamisega garanteeritakse avaldamisele mittekuuluva informatsiooni konfidentsiaalsus, kliendiinformatsiooni kogumise põhjendatus ning isikuandmete kaitse seaduse ja andmekogude seaduse täitmine.

3 Kliendi identifitseerimine

3.1 Kliendi isikusamasuse kontroll

Kliendi isikusamasust kontrollitakse kehtiva isikut tõendava dokumendi alusel vastavalt isikut tõendavate dokumentide seadusele.

3.2 Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord

Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord on toodud sertifikaadiga seotud sertifitseerimispoliitikas.

3.3 Eraldusnimi

Kliendi eraldusnimi koostatakse vastavalt sertifitseerimispoliitikas määratud sertifikaadi- ja tühistusnimekirja profiilile.

SK tagab kliendi eraldusnime ja sertifikaadi kinnitamisel kasutatud SK isikliku võtmega seotud sertifikaadi eraldusnime kombinatsiooni unikaalsuse.

SK kannab väljastatavatesse sertifikaatidesse unikaalse sertifikaadi järjenumbri.

4 Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtajad

4.1 Sertifikaaditaotluse esitamine

Sertifikaadi taotlemine on võimalik ainult SK poolt volitatud klienditeeninduspunktis.

Sertifikaaditaotluse esitamise kord peab olema kooskõlas järgnevate punktidega:

- Enne klienditeeninduspunktis avalduse esitamist on klient eelnevalt tutvunud SK sertifitseerimispõhimõtetega, sertifikaadi sertifitseerimispoliitikaga jt seotud dokumentidega;
- Klienditeeninduspunkti töötaja annab kliendile sertifikaaditaotluse läbiviimiseks vajaliku avalduseblanketi;
- Sertifikaaditaotluse avaldus peab sisaldama järgnevaid punkte:
    - viide taotletava sertifikaadi sertifitseerimispoliitikale;
    - märge selle kohta, et klient volitab SK genereerima kliendile võtmepaari;
    - märge selle kohta, et klient volitab SK genereerima kliendi võtmepaarile vastava sertifikaadi;
    - viide teavituskanalile, mille kaudu edastatakse kliendile sertifitseerimisteenuse osutamisel tekkinud informatsiooni (näiteks informatsiooni sertifikaadi peatamise kohta);
- Klient täidab sertifikaaditaotluse avalduse ja allkirjastab selle;
- Klienditeeninduspunkti töötaja tuvastab avalduse allkirjastanud kliendi isikusamasuse kehtiva isikut tõendava dokumendi alusel;

4.2 Sertifikaaditaotluse menetlemine

Sertifikaaditaotluse avalduse täpne läbivaatamise kord ja töötlemise tähtajad määratakse ära vastavas sertifitseerimispoliitikas. Sertifikaaditaotluse avalduse menetlemisel kontrollitakse kliendi poolt esitatud andmete õigsust ja täielikkust.

4.2.1 Otsuse tegemine

Sertifikaaditaotluse avalduse rahuldamise või mitterahuldamise otsustab SK klienditeenindusbüroo vähemalt 5 tööpäeva jooksul.

SK klienditeenindusbüroo lähtub otsuse langetamisel:
- kas kliendil on vastavalt EV õigusaktidele õigus saada sertifikaati;
- kas klient on esitanud taotluses enda kohta õigeid ja täielikke andmeid
- kas klient ei oma sama kasutusvaldkonna ja eraldusnimega sertifikaati

Klienti teavitatakse otsusest sertifitseerimispoliitikas toodud või avalduses kokkulepitud teavituskanali kaudu.

4.2.2 Sertifikaadi väljastamine

SK väljastab automaatselt peale SK klienditeeninduspunkti poolt edastatud sertifikaaditaotluse autentsuse ja terviklikkuse kontrolli taotlusele vastavad sertifikaadid, mis laetakse kiipkaardile kliendi tulekul SK klienditeeninduspunkti sertifikaadi kättesaamiseks.

Enne sertifikaadi väljastamist kliendile kontrollitakse kliendi isikusamasust.

4.2.3 Sertifikaatide üle arvestuse pidamise kord

Kõik väljastatud sertifikaadid hoitakse SK suletud infosüsteemi osas olevas sertifikaatide andmebaasis.

Sertifikaadi väljastamisel salvestatakse sertifikaadi koopia sertifikaatide kataloogi, mis on avalikus andmesidevõrgus ööpäevaringselt kättesaadav kõigile teenuse kasutajatele. Kataloogi kaudu on tagatud juurdepääs kõikidele kehtivatele sertifikaatidele ja tühistusnimekirjadele. Kataloogile võib vajadusel juurdepääsu piirata, kui seda nõuavad sertifitseerimispoliitika ja nõuded süsteemi käideldavusele.

Sertifikaadi tühistamisel või peatamisel kustutatakse sertifikaadi koopia avalikust kataloogist.

4.2.4 Sertifikaadi kontroll ja tõestamine

Huvitatud isiku nõudmisel tõendab SK esindaja enda digitaalallkirjaga SK poolt väljastatud sertifikaadis sisalduvale avalikule võtmele vastava isikliku võtmega antud digitaalallkirja kehtivust.
Sertifikaatide tõendamise teenuse osutamisel kasutatavad andmeformaadid, teenuse hinna ja osutamise ajalised piirangud määrab SK. Täpsed tingimused avaldatakse SK koduleheküljel.

4.2.5 Sertifikaadi uuendamine

Sertifikaadi uuendamise tingimused ja sellega seotud protseduurid ning tähtajad tuuakse ära sertifikaadi sertifitseerimispoliitikas.
Sertifikaadi sertifitseerimispoliitika peab tooma välja järgmised uuendamisvõimalused:

a) sertifikaadi uuendamine sertifikaadi aegumise järel
b) sertifikaadi uuendamine sertifikaadi kehtetuks tunnistamise järel

Need uuendamisevõimalused peavad sisaldama informatsiooni selle kohta, kas uus sertifikaat antakse välja samale võtmepaarile või mitte.

4.3 Sertifikaadi peatamise ja kehtetuks tunnistamise taotlused

4.3.1 Sertifikaadi peatamise ja kehtetuks tunnistamise taotluste volituste kontroll

Sertifikaatide peatamis- ja kehtetuks tunnistamise volitusi kontrollitakse vastavalt järgnevale tabelile 3.

Tabel 3. Peatamis- ja kehtetuks tunnistamise volitused

Taotluse esitamisviis	Peatamistaotlus	Peatatuse lõpetamise taotlus	Tühistustaotlus

Taotluse esitamisviis	**Peatamistaotlus**	**Peatatuse lõpetamise taotlus**	**Tühistustaotlus**
Telefoni teel, helistades SK abiliinile. Sertifikaatide peatamisel küsitakse peatamise taotleja isikuga seotud andmeid ning võrreldakse neid SK infosüsteemis olevate andmetega.	Peatatakse isikuandmeid puudutavatele kontrollküsimustele usaldusväärselt vastamise korral.	Ei aktsepteerita	Peatatakse isikuandmeid puudutavatele kontrollküsimustele usaldusväärselt vastamise korral ning pakutakse kliendile sobilik kanal tühistustaotluse esitamiseks.
Faksi teel, saates SK kontaktandmetes toodud SK faksi numbrile.	Ei aktsepteerita.	Ei aktsepteerita	Ei aktsepteerita.
Kirja teel, saates kirja SK kontaktandmetes toodud aadressidel.	Peatatakse usaldusväärse kirja sisu ning sertifikaadiomaniku allkirja korral.	Ei aktsepteerita	Peatatakse usaldusväärse kirja sisu ning sertifikaadiomaniku allkirja korral ning pakutakse kliendile sobilik kanal tühistustaotluse esitamiseks.
Avalikus andmesidevõrgus SK koduleheküljel olevas rakenduses http://www.sk.ee	Peatatakse isikuandmeid puudutavatele kontrollküsimustele usaldusväärselt vastamise korral.	Ei aktsepteerita	Peatatakse isikuandmeid puudutavatele kontrollküsimustele usaldusväärselt vastamise korral ning pakutakse kliendile sobilik kanal tühistustaotluse esitamiseks.
Avalikus andmesidevõrgus autendituna SK koduleheküljel olevas rakenduses http://www.sk.ee	Peatatakse.	Ei aktsepteerita	Peatatakse.
SK klienditeeninduspunktis isikut tõendava dokumendi esitamisel.	Peatatakse.	Peatatus lõpetatakse	Tühistatakse.

4.3.2 Kehtetu, peatatud või aegunud sertifikaadi õigusliku kasutamise välistamine

Kehtetu, peatatud või aegunud sertifikaadi õigusliku kasutamise välistamine tagatakse peale sertifikaadi kehtivuse kaotamist, peatamist või aegumist selle kataloogist kustutamisega ja tühistusnimekirjas publitseerimisega.

4.3.3 Sertifikaadi õigusliku aluseta kehtetuks tunnistamise tagajärjed

Isik või asutus, kelle tahtluse või raske ettevaatamatuse tõttu on sertifikaat tunnistatud ilma õigusliku aluseta kehtetuks, on kohustatud hüvitama sertifikaadi kehtetuks tunnistamisega tekkinud otsese kahju.

4.4 Sertifikaatide peatamine

4.4.1 Sertifikaadi peatamise tingimused ja menetlus

4.4.1.1 Tingimused sertifikaadi peatamiseks

Täpsed tingimused sertifikaadi peatamise kohta tuuakse sertifikaadile vastavas sertifitseerimispoliitikas. Sertifikaadi peatamisvõimalus peab olema toodud ära digitaalallkirja võimaldavates sertifitseerimispoliitikates.

Vastavalt DASile sertifikaadi kehtivus peatatakse, kui:

- SK-l tekib põhjendatud kahtlus, et sertifikaati on kantud ebaõiged andmed või et sertifikaadis sisalduvale avalikule võtmele vastavat isiklikku võtit on võimalik kasutada sertifikaadi omaniku nõusolekuta;
- sertifikaadi kehtivuse peatamist nõuab sertifikaadi omanik või tema notariaalselt kinnitatud volitustega esindaja;
- sertifikaadi kehtivuse peatamist nõuab andmekaitse järelevalveasutus või SRR vastutav töötleja, kui tal tekib põhjendatud kahtlus, et sertifikaati on kantud ebaõiged andmed või et sertifikaadis sisalduvale avalikule võtmele vastavat isiklikku võtit on võimalik kasutada sertifikaadi omaniku nõusolekuta;
- sertifikaadi peatamist nõuab kohus, prokuratuur või kriminaalasjas kohtueelset uurimist teostav asutus kuritegude tõkestamiseks.

4.4.1.2 Sertifikaadi peatamise volitused

Sertifikaadi võivad peatada:

- klient (sertifikaadi omanik)
- SK vastutav töötaja
- SRR vastutav töötleja
- DASis nimetatud vastava volitustega ametnik kohtueelse uurimise teostamiseks ja kuritegude tõkestamiseks

4.4.1.3 Peatamistaotluse esitamine

Peatamistaotluse esitaja esitab kirjaliku avalduse sertifikaadi peatamiseks lähimas SK klienditeeninduspunktis.
Klient saab peatamistaotlusi esitada ka ööpäevaringselt telefoni teel abiliini kaudu.
Informatsiooni klienditeeninduspunktide ja nende lahtiolekuaegade kohta edastatakse SK koduleheküljel.
Avalduse registreerimisel märgitakse üles avalduse esitaja isikutuvastamisel kasutatud dokumendi identifikaator (passinumber, sertifikaadi eraldusnimi).

4.4.1.4 Peatamistaotluse menetlus

Sertifikaadi peatamise menetlus toimub järgnevalt:

- peatamise esitamisviisi volituste kontroll vastavalt tabelile 3
- kui klient esitab taotluse sertifikaadi peatamiseks SK klienditeeninduspunktis, siis eelnevalt peab ta täitma vastava avalduseblanketi ja allkirjastama selle;
- peatamistaotleja volituste kontroll;
- sertifikaadi peatamise avalduse seaduslikkuse kontroll;
- peatamisekõne registreeritakse abiliini operaatori poolt või peatamise registreerimine SK klienditeeninduspunkti telleri poolt;
- peatamistaotleja isikuga seotud andmete kontrollimine;
- sertifikaadi peatamisavalduse käesolevale sertifitseerimispoliitikale vastavuse kontroll SK infosüsteemi poolt;
- sertifikaadi peatamistaotluse registreerimine SK infosüsteemis;
- sertifikaatide andmebaasis sertifikaadi peatatuks märkimine (tühistusnimekirjas on vastavaks põhjuskoodiks 6 (*hold)*);
- sertifikaadi kustutamine avalikust kataloogist;
- peatamise vastuvõtja veendub kontrollimisel sertifikaadi otsingu sooritamisega kataloogist, et see sertifikaat on sealt kustutatud;
- uue sertifikaatide tühistusnimekirja välja andmise algatamine ja väljastamine;
- peatamistaotluse aluseks olevate materjalide arhiveerimine;
- kui peatamine esitati abiliini kaudu, siis teavitatakse sertifikaadi omanikku sertifikaadi peatamisest ID-kaardi taotluses kliendi poolt määratud teavituskanali kaudu;
- klient veendub tühistusnimekirja põhjal, et sertifikaat on peatatud

4.4.1.5 Peatamise operatiivsus

Sertifikaadi peatamine kajastub koheselt SK sertifikaatide andmebaasis.
Esimesel võimalusel peale peatamist väljastab SK uue tühistusnimekirja, mis sisaldab peatatud sertifikaadi järjekorranumbrit.

4.5 Sertifikaadi peatatuse lõpetamine

4.5.1 Tingimused sertifikaadi peatatuse lõpetamiseks

Sertifikaadi peatatus lõpetatakse sertifikaadi omaniku või sertifikaadi kehtivuse peatamist nõudnud isiku või asutuse kirjaliku avalduse alusel vastavate andmete kandmisega sertifikaatide andmebaasi.

4.5.2 Sertifikaadi peatatuse lõpetamise volitused

Sertifikaadi peatatust võivad lõpetada:
- sertifikaadi peatanud sertifikaadiomanik
- SRR vastutav töötaja
- SK ametnik
- Vastavalt DASile muu vastava volitustega ametnik, kes tegutses sertifikaadi peatamisel vastavalt punktile 4.4.1.2)

4.5.3 Sertifikaadi peatatuse lõpetamise taotluse esitamine

Sertifikaadi peatatuse lõpetamise taotlus esitatakse kirjalikult täidetud avaldusblanketil peale isikutuvastamist ja volituste kontrolli SK klienditeeninduspunktis;

Sertifikaadi peatatuse lõpetamise tunnistamise taotlemiseks esitatud avaldus peab sisaldama:
- avalduse esitaja nime;
- avalduse esitaja allkirja;
- peatatud sertifikaadi omaniku nime ja isikukoodi;
- peatatud sertifikaadi väljastanud SK eraldusnime;
- peatatuse lõpetamise aluse;

Kui avaldust ei esitanud sertifikaadiomanik vaid vastavaid volitusi omav ametnik või SK vastutav töötaja, siis peab avaldusele olema lisatud peatatuse lõpetamist lubavad dokumendid.

Avalduse registreerimisel märgitakse üles avalduse esitaja isikutuvastamisel kasutatud dokumendi identifikaator (passinumber, sertifikaadi eraldusnimi).

4.5.4 Sertifikaadi peatatuse lõpetamise menetlus

Peatatuse lõpetamise menetlus toimub järgnevalt:

- klient koostab kirjaliku avalduse sertifikaadi peatatuse lõpetamiseks SK klienditeeninduspunktis vastavale blanketile;
- klient täidab SK klienditeeninduspunktis sertifikaadi peatatuse lõpetamiseks vastava avalduseblanketi ja allkirjastab selle;
- peatatuse lõpetamise volituse kontroll;
- sertifikaadi peatatuse lõpetamise avalduse seaduslikkuse kontroll;
- peatatuse lõpetamise vastavuse kontroll SK infosüsteemi poolt;

- sertifikaadi peatatuse lõpetamise registreerimine SK infosüsteemis;
- sertifikaatide andmebaasis sertifikaadi peatatuse tühistamine;
- sertifikaadi kopeerimine avalikku kataloogi;
- uue sertifikaatide tühistusnimekirja välja andmise algatamine ja väljastamine;
- kliendile teatatakse peale peatatuse lõpetamistaotluse registreerimist hetk, mil ükski kehtiv tühistusnimekiri enam sertifikaadi kasutamist ei piira;
- klient veendub tühistusnimekirja põhjal, et sertifikaat on aktiivne;

4.5.5 Sertifikaadi peatatuse lõpetamise operatiivsus

Sertifikaadi peatamine kajastub koheselt SK sertifikaatide andmebaasis.
Esimesel võimalusel peale peatatuse lõpetamist väljastab SK uue tühistusnimekirja, mis ei sisalda peatatuse lõpetanud sertifikaadi järjekorranumbrit.

4.6 Sertifikaadi kehtetuks tunnistamine

4.6.1 Sertifikaadi kehtetuks tunnistamise volitused

Sertifikaadi kehtetuks tunnistamise avalduse võib esitada sertifikaadiomanik, tema notariaalselt kinnitatud volitusega esindaja või muu õigusaktides toodud isik.

4.6.2 Sertifikaadi kehtetuks tunnistamise avalduse esitamine

Sertifikaadi kehtetuks tunnistamine toimub kirjaliku avalduse alusel.

Sertifikaadi kehtetuks tunnistamise avaldus peab sisaldama:
- avalduse esitaja nime;
- avalduse esitaja allkirja;
- tühistatava sertifikaadi omaniku nime ja isikukoodi;
- tühistatava sertifikaadi väljastanud SK eraldusnime;
- sertifikaadi tühistamise põhjust;
- vajadusel tõendusmaterjali sertifikaadi tühistamise põhjuse asjaolude tõendamiseks.

Kehtetuks tunnistamise avalduse esitaja identifitseeritakse SK klienditeeninduspunktis kehtiva isikut tõendava dokumendi alusel. Avalduse registreerimisel märgitakse üles avalduse esitaja identifitseerimisel kasutatud dokumendi identifikaator (passinumber, sertifikaadi eraldusnimi).

4.6.3 Sertifikaadi kehtetuks tunnistamise menetlus

Sertifikaadi kehtetuks tunnistamise menetlus toimub järgnevalt:

- klient koostab kirjalikult sertifikaadi kehtetuks tunnistamise avalduse SK klienditeeninduspunktis vastavale blanketile;

- klient täidab SK klienditeeninduspunktis sertifikaadi kehtetuks tunnistamiseks vastava avalduseblanketi ja allkirjastab selle;
- sertifikaadi kehtetuks tunnistamise avalduse seaduslikkuse kontroll;
- kehtetuks tunnistamise avalduse õigsuse kontroll SK infosüsteemi poolt;
- sertifikaadi kehtetuks tunnistamise avalduse registreerimine SK infosüsteemis;
- sertifikaadi kustutamine avalikuks kataloogist;
- sertifikaatide andmebaasis sertifikaadi kehtetuks märkimine;
- uue sertifikaatide tühistusnimekirja välja andmise algatamine ja väljastamine;
- kehtetuks tunnistamise avalduse aluseks olevate materjalide arhiveerimine;
- klient veendub tühistusnimekirja põhjal, et sertifikaat on tühistatud

4.6.4 Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus

Sertifikaat tuleb tühistusnimekirja kanda esimesel võimalusel peale kehtetuks tunnistamise avalduse registreerimist ja selle kontrollimist.

4.7 Protseduurid jälgitavuse tagamiseks

4.7.1 Dokumentide säilitamine

Sertifitseerimisteenuse osutamisega seotud dokumentatsiooni säilitab SK kuni oma tegevuse lõpuni.

Sertifikaatide kehtetuks tunnistamise põhjust tõestavad dokumendid säilitatakse kuni SK tegevuse lõpuni, kui seaduses ei ole sätestatud teisiti.

Kui SK-le on esitatud sertifikaadi kohta pretensioon või kui sertifikaat on tõendusmaterjaliks kohtulikus vaidluses, siis selle sertifikaadi kohta käivat informatsiooni ja dokumentatsiooni säilitatakse lõpliku lahenduseni jõudmiseni.

SK teenuste osutamise lõpetamise järel antakse vastavalt seadusandlusele ja kehtestatud korrale kogu digitaalallkirja võimaldavate sertifikaatidega seotud dokumentatsioon üle SRR-le.

4.7.2 Kontrolljälge jätvad tegevused

SK infosüsteemid jätavad kontrolljälje:

- kõigist SK kinnitamise võtmete elutsükli etappidest ja kasutamistest;
- kõigist klientide võtmete elutsükli etappidest;
- kõigist turvasündmustest, nagu kasutajate autoriseerimised või edutud autoriseerimise katsed;
- eriõigustega süsteemikasutajate tegevustest.

SK kasutab standarditele vastavaid infoturbelahendusi isiklike võtmete, aktiveerimiskoodide, pääsukoodide (näiteks PINide) jt turvakriitilise informatsiooni kontrolljäljes mittesalvestumise.

Kõik intsidendid, eriolukorrad ja probleemid registreeritakse ning olulisusest ja iseloomust sõltuvalt edastatakse edasisele käsitlemisele vastavalt SK sisekorrale.

Tugiinfosüsteemide kontrolljälgede käsitlemise korra määrab SK.

4.7.3 Kontrolljälje säilitamise kestvus

Kõik punktis 4.7.2 nimetatud kontrolljäljed säilitatakse SK infosüsteemis vähemalt 36 kuud. Ülejäänud kontrolljälgede säilitamise ja analüüsi nõuded kehtestab SK sisekorraeeskirjadega.

4.7.4 Kontrolljälje kaitse

SK tagab infotehnoloogiliste ja organisatsiooniliste vahenditega kontrolljälje muutmatuse, säilimise ja konfidentsiaalsuse.

4.7.5 Kontrolljälje analüüs

SKs on kehtestatud kord kontrolljälgede regulaarseks analüüsiks ning võimaliku ründe kiireks avastamiseks.

4.8 Tegutsemine eriolukorras

SK on koostanud riskianalüüsi SK sertifitseerimissüsteemi kohta, et ennetada võimaliku ohtu SK tegevuse käideldavusele.

SK kasutab teenuse osutamisel tehnilisi vahendeid ja infosüsteemi turbemeetodeid, et minimiseerida sertifitseerimisteenuse oma kontrolli alt väljumise ohtu.
SK on koostanud sisemised dokumendid „ASi Sertifitseerimiskeskus infoturbepoliitika“, „ASi Sertifitseerimiskeskus käideldavuse strateegia ja poliitika“, „ASi Sertifitseerimiskeskus IT süsteemide taastamise poliitika“ ja spetsiaalsed juhendid ja taasteplaanid kriisisituatsioonis tegutsemiseks, säilitamaks teenuse osutamise turvalisus ja kvaliteet. ASi Sertifitseerimiskeskus infosüsteem ja kasutatav dokumentatsioon on auditeeritud sõltumatu IT audiitori poolt.

Käsitletavad juhendid ja taasteplaanid hõlmavad tegutsemiskavasid järgnevate kriisisituatsioonide puhul:

- SK kinnitusvõtme avalikustumine või avalikustumise kahtluse korral;
- SK tegevuse võimaliku jäljendamise korral;
- SK sertifitseerija isikliku võtme hävimise korral;
- SK sertifikaatide andmebaasi hävimise korral;
- SK teenuse jäljendamise kahtluse või jäljendamise korral;
- andmetöötluskeskust sisaldava hoone täielik või osaline hävimise korral;

- andmetöötluskeskust avaliku andmesidevõrguga ühendava sidekanali tõrke korral;
- tootekeskkonna elektri- või veevärgi tõrke korral;
- teenuse tõkestamiseks teostatud infotehnoloogilise ründe korral;
- olulise personali osa üheaegne töövõimetuse korral.

Tegutsemiskavades esitatakse teenuse osutamiseks vajalike minimaalsed kvaliteedinõuded tegutsemiseks *force majeure'*i tingimustes.

Eriolukorra ilmnemise korral teavitab SK viivitamatult, vähemalt ilmnemisele järgneva tööpäeva jooksul, teenuse kasutajaid tekkinud eriolukorrast ja planeeritud lahenduskavast avaliku teabelevituskanalite kaudu.

Kui eriolukorra tõttu sai võimalikuks sertifikaadi andmebaasi sisu muutumine, sertifikaatide väljastamine, peatamine, peatatuse lõpetamine, kehtetuks tunnistamine, siis SK taastab viivitamatult, vähemalt ilmnemisele järgneva ööpäeva jooksul, eriolukorrale eelnenud sertifikaatide andmebaasi seisu ja teavitab sellest sertifikaadi omanikke oma koduleheküljel.

4.9 Sertifitseerimisteenuse osutaja töö lõpetamine

Sertifitseerimisteenuse osutamine lõpetatakse:

1) SK otsusega;
2) teenuse osutamise üle järelevalvet teostava asutuse otsusega;
3) kohtuotsusega;
4) ASi Sertifitseerimiskeskuse likvideerimise või tegevuse lõpetamise korral.

Sertifitseerimisteenuse osutamise lõpetamisel annab SK teenuse osutamisega seotud dokumentatsiooni üle SRRile vastavalt kehtestatud korrale.

SK teenuse lõpetamisest teavitatakse SK koduleheküljel http://www.sk.ee

SK kohustub lisaks DASis esitatud nõuetele teenuse lõpetamisel tunnistama kehtetuks kõik väljaantud ja kehtivad sertifikaadid.

SK valduses olevad riistvaralised seadmed kas reinitsialiseeritakse või hävitatakse, sõltuvalt konkreetsest turvalisuse nõuetest.

SK ei vastuta teenuse lõpetamisel teenuse kasutajale tekkida võivate mistahes kahjude eest, kui SK on sellest avaliku teabekanali kaudu teatanud vähemalt 1 kuu enne teenuse osutamise lõpetamist.

5 Füüsilised ja organisatsioonilised turbemeetmed

5.1 Turbehaldus

SK juhindub turbe haldamisel tunnustatud standarditest, näiteks ISO 13335, ISO 13569.

SK juhtkond on koostanud infoturbekontseptsiooni, mis on infoturbe järjepidevuse, täielikkuse ja juhtkonna toetuse aluseks.

SK haldab infovarade registrit ning klassifitseerib kõik infovarad turbeklassidesse vastavalt turvaanalüüsi tulemustele. Kõigil olulistel infovaradel on määratud vastutaja.

SK infoturbe dokumentatsiooni täitmist jälgitakse korraliste auditite käigus sõltumatu audiitori poolt.

5.2 Füüsilised turbemeetmed

5.2.1 SK füüsiline pääsukontroll

Pääs SK ruumidesse on piiratud.
SK ruumides kasutatakse füüsilist või elektroonilist valvet.
SK andmetöötluskeskusesse tohivad SK töötajad siseneda üksnes kinnitatud nimekirja alusel. Kõigi SK andmetöötluskeskusesse sisenemiste kohta peetakse päevikut.
Teisaldatava meedia, seadmete ja tarkvara SK ruumidest väljaviimine toimub kehtestatud korra alusel. Andmekandjaid tundliku informatsiooniga tohib säilitada üksnes spetsiaalses andmekandjate hoidmiseks määratud tulekindlas seifis.

5.3 Nõuded tööprotseduuridele

SK infosüsteemi kasutatakse üksnes sihipäraselt.

Arenduseks ja testimiseks kasutatakse töösüsteemist täielikult eraldatud ning sõltumatut infosüsteemi koos täielikult sõltumatute isiklike võtmete, paroolide, koodide ja teiste pääsutunnustega.

5.3.1 Oluliste toimingute läbiviimine

5.3.1.1 Jagatud kontroll

Sertifikaatide kinnitamiseks kasutatava SK sertifikaadi ning isikliku võtme aktiveerimine toimub jagatud kontrolli alusel. Vastavad kontrolli meetmed kehtestatakse SK sisemiste protseduurireeglitega.

5.3.1.2 Toimingute dokumenteerimine

Turvalisuse aspektist oluliste toimingute sooritamise kohta koostatakse akt. Need toimingud peavad vähemalt sisaldama:

- kõik SK kinnitamisvõtme elutsükli etapid ja kasutuskordasid;
- eriolukordade lahendusi

5.4 Personali turbenõuded

Töötajal, kes on seotud käesolevas CPSis kirjeldatud teenuse osutamisega, ei tohi olla karistatust tahtlikult toime pandud kuriteo eest. Need töötajad peavad olema piisavalt koolitatud ning omama vajalikke kogemusi töölepingus ja ametijuhendis ettenähtud töö tegemiseks.

SK töötajate töölepingutes on kohustus hoida saladuses töö käigus teatavaks saanud konfidentsiaalset informatsiooni vähemalt 10 aastat peale töölepingu lõppemist.

SK töötajad ei tohi omada ärihuve konkureerivas ettevõttes, mis võivad mõjutada nende otsuseid teenuse osutamisel.

SK töötajatel peavad olema ametijuhendid, milles on ära märgitud järgnevatesse turvakriitilistesse rollidesse kuulumine:

- infoturbeülem: vastutav infoturbepoliitika koostamise ja ellu viimise eest;
- RAO: Vastutav sertifikaatide kinnitamise, väljastamise, kehtivuse peatamise, peatatuse lõpetamise ja tühistamise taotluse seaduslikkuse kontrolli eest;
- süsteemiadministraator: vastutav SK infosüsteemi paigaldamise, konfigureerimise ja haldamise eest; ei oma juurdepääsu turvakriitilisele informatsioonile;
- süsteemioperaator: vastutav SK infosüsteemi igapäevase halduse eest, sh varukoopiate tegemine ning süsteemi taastamise.
- siseaudiitor: omab õigust jälgida dokumendiarhiive ja infosüsteemide kontrolljälgi.

Vähemalt infoturbeülema, siseaudiitori ja süsteemiadministraatori rollid peavad olema täielikult eraldatud ning täidetud erinevate isikute poolt.

6 Tehnilised turbenõuded

6.1 Võtmehaldus

6.1.1 SK kinnitusvõtmed

6.1.1.1 SK kinnitusvõtmete loomine

Sertifitseerimisteenuse osutamisel kasutatakse RSA algoritmi võtmeid järgmiste miinimumpikkustega:

- SK kinnitusvõti - 2048 bitti
- sertifikaadile vastav salajane võti - 1024 bitti

Sertifitseerimisteenuse osutamiseks vajalikud SK kinnitusvõtmed luuakse vastavalt SK sisekorrale „SK juurvõtme loomise protseduur“ ja „SK alamsertifitseerijate võtmete loomise protseduur“. SK võtmete loomist jälgib komisjon, kes koostab peale võtmete loomist vastavasisulise akti, mis sisaldab võtmepaarile loodud sertifikaadi avaliku võtit ja räsi. Võtmete loomise akt avaldatakse keskuse koduleheküljel.

6.1.1.2 Võtmete kaitse

SK võtmetele juurdepääs ja kasutamine on võimalik vähemalt kahe volitatud isiku osavõtul.

Käideldavusnõuete rahuldamiseks luuakse SK kinnitusvõtmetest varukoopia. Võti jagatakse kolmeks osaks, mida säilitavad erinevad isikud. SK kinnitusvõtme säilitamisel kasutatakse turvaümbrikku, mille avamine on tuvastatav.

SK kinnitusvõtmed on kasutatavad üksnes aktiveeritud olekus. SK kinnitusvõtme aktiveerimiseks on vajalik vähemalt kahe volitatud isiku osavõtt.

SK kinnitusvõtmed deaktiveeruvad võtmete säilitamisel kasutatava turvamooduli avamise katsel, konfiguratsiooni muutmisel, vooluvõrgust eemaldamisel, teisaldamisel ja teistel turvalisust ohustada võivatel sündmustel.

Sertifitseerimisteenuse osutamisel kasutatavad turvamoodulid vastavad turvastandardis FIPS PUB 140-1 Level 3 toodud nõuetele.

6.1.1.3 SK kinnitusvõtme hävitamine

SK isiklikest võtmetest hävitatakse aegumise või tühistamise järel kõik koopiad nii, et nende edasine kasutamine või tuletamine on võimatu.

6.1.2 Kliendi võtmed

6.1.2.1 Kliendi võtmete moodustamine

Kliendi võtmete moodustamine toimub vastavalt sertifikaadi sertifitseerimispoliitikas toodud põhimõtete järgi.

Kliendi võtmed peavad olema kaitstud ainult kliendile teadaolevate PIN koodidega e aktiveerimiskoodidega.

6.1.2.2 Kliendi isikliku võtme ja aktiveerimiskoodide kaitse valmendamise käigus

Kui kliendi isiklikud võtmed genereerib SK, siis peab olema tagatud genereeritud kliendi isikliku võtme ning aktiveerimiskoodide konfidentsiaalsus ja volitusteta mittekasutamine kuni nende kliendile üleandmiseni.

Aktiveerimiskoodid trükitakse ühes eksemplaris otse turvaümbrikusse, mis edastatakse avamata kliendile.

6.1.2.3 Kliendi salajase võtme aktiveerimine

Igakordne isikliku võtme kasutamine eeldab aktiveerimiskoodi sisestamist. Kliendi erinevatele võtmetele peab olema võimalik kehtestada erinevaid aktiveerimiskoode.

Aktiveerimiskoodid vastavavad järgmistele tingimustele:

- aktiveerimiskoode ei salvestata ega puhverdata kaardis, kaardilugejas ega rakendustarkvaras;
- aktiveerimiskoodid on kliendile muudetavad;
- aktiveerimiskoodide pikkus ei tohi olla lühem kui 4 ega pikem kui 12 sümbolit;
- aktiveerimiskoode käsitlevate tarkvara- ja riistvarakomponentide terviklus peab olema tagatud;
- aktiveerimiskoodi sisestamisel peab olema võimalik seda teha kolmandate isikute eest varjatult;
- kolme vale PIN-koodi sisestamise järel kiipkaart lukustub; avamiseks on vajalik PUK-koodi sisestamine;
- isikliku võtme aktiveerimise ajal peab klient olema teadlik sooritatavast tegevusest: digitaalallkirja andmisel tuleb esitada allkirjastatava dokumendi sisu

6.1.2.4 Kliendi võtmete hävitamine

Sertifikaatide tühistamise või kehtivuse lõpu järel saab SK ainult SK-le teada oleva salakoodi abil kiipkaarti algväärtustada sellest kogu informatsiooni kustutamise teel. kiipkaardi algväärtustamise järel ei ole sellest võtmete eraldamine võimalik.

kiipkaardi algväärtustamise järel luuakse uued võtmed ning sertifitseeritakse need kooskõlas käesoleva dokumendile ja sellega seotud dokumentidega.

6.1.2.5 Kliendi võtmete varundamine ja deponeerimine

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

6.2 Süsteemiturve

6.2.1 Pääsukontroll

SK realiseerib pääsukontrollisüsteemi, mis identifitseerib, autoriseerib ja registreerib usaldusväärselt kõik SK infosüsteemi kasutajad, ka SK klienditeeninduspunkti töötajad.

6.2.2 Tarkvara turve

SK infosüsteemis, sh kõigis töökohtades on rakendatud meetmeid tarkvara ja konfiguratsiooni terviklikkuse tagamiseks ja pahatahtliku tarkvara tuvastamiseks ning levimise piiramiseks.

Infosüsteemis kasutatakse üksnes otseselt tööülesannete täitmiseks vajalikku tarkvara, mis on kooskõlastatud infoturbejuhiga ja pärineb usaldusväärsest allikast.

6.2.3 Võrguühenduste turve

Tundlike andmete edastamine üle SK välise võrgu on krüpteeritud.

SK sisevõrgu kaabeldus ja aktiivseadmed koos konfiguratsiooniga on kaitstud füüsiliste ja organisatsiooniliste meetmetega.

SK sisevõrgu ning välisühenduste turvalisust jälgitakse pidevalt.

6.2.4 Kellaaegade sünkroniseerimine

Sertifitseerimisteenuse osutamise süsteemi kõigi osade kellaaegade maksimaalne erinevus on kuni üks sekund.

Selle tagamiseks on kasutusel sisemine etalonkella teenus, mille järgi sünkroniseeritakse kõikide sertifitseerimisteenuse osutamise süsteemi osade ajaarvamist.

Etalonkella sünkroniseeritakse vähemalt kahte usaldusväärset ja sõltumatut allikat kasutades.

6.3 Sertifitseerimisteenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus

SK kasutab sertifitseerimisteenuse osutamisel firma *Baltimore Technologies* ITSEC-3 sertifitseeritud sertifitseerimistarkvara *Unicert*. Sertifikaatide väljastamine toimub kaitstud võrgusegmendis nn tootekeskkonnas paiknevas ainult selleks otstarbeks eraldatud sertifitseerimisserveri sertifitseerijamoodulis CA.

Sertifitseerimismooduli CA juhtimine toimub operaatormooduli CAO kaudu, mida saab kasutada ainult selleks volitatud operaatorid sertifitseerimisserveri juures asuva konsooli abil. Sertifitseerimismooduli isiklike võtmete turvaliseks säilitamiseks on kasutusel turvamoodul, mis vastab *FIPS Pub 140-1 Level 3* standardile.

Sertifikaaditaotluste töötlus toimub selleks eraldatud registreerimismoodulis RA, mille juhtimise tarkvarana kasutatakse laiendatud võimalustega registreerimisoperaatorit ARM.

Kataloogiteenuse osutamiseks on kasutusel firma *iPlanet* kataloogiteenuse server *iPlanet Directory Server*.

Sertifitseerimisteenuse osutamisel kasutatakse firmade SUN servereid ja IBM tüüpi töökohaarvuteid.

6.4 Sertifitseerimisteenuse osutamisel tekkinud andmete säilitamine ja kaitse

SK hoiab ja arhiveerib elektrooniliselt informatsiooni kõigi sertifikaatide ja nende staatuse muudatustega seotud toimingute kohta. Andmete varukoopiaid hoitakse turvaliselt kahes erinevas asukohas.

Andmekaitsepõhimõtted on toodud dokumendis “Isikuandmete kaitse põhimõtted”. SK säilitab sertifitseerimisteenuse osutamisel tekkinud andmeid oma tegevusaja lõpuni.

7 Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid

7.1 Sertifikaatide profiil

Sertifikaadiprofiilid on avaldatud või viidatud realiseeritavates sertifitseerimispoliitika dokumentides.

Sertifitseerijate sertifikaatide profiilid esitatakse dokumendis “AS Sertifitseerimiskeskuse CA sertifikaatide profiilid”.

Sertifikaadi profiil peab olema koostatud vastavalt RFC 2459’s esitatud nõuetele ja sisaldama vähemalt järgmisi punkte:

- ✓ Sertifikaadi vormingu versiooni number. Kõik SK poolt väljastatud sertifikaadid vastavalt standardile ITU-T X.509 v3.
- ✓ Sertifikaadi unikaalne SK sertifitseerija poolt antud järjekorranumber

- ✓ Sertifikaadi laiendused, OID ja nende kriitilisuse aste
- ✓ Kinnitamiseks kasutatavad krüptoalgoritmid ja nende OID
- ✓ Eraldusnimed, mida kasutatakse CA, RA ja sertifikaadi omaniku määratlemiseks. Sertifikaadi omaniku nimi eraldusnimes peab sisaldama omaniku ees- ja perekonnanime ning vajadusel isikukoodi. CA ja RA eraldusnimes peab olema fikseeritud SK nimi. Väljaandja (CA) andmed peavad sisaldama registrikoodi
- ✓ Sertifikaadi kehtivusaeg
- ✓ Sertifikaadi avaliku võtme esitlusinfo
- ✓ Sertifikaadi kasutusvaldkonna piirangud (digitaalseks allkirjastamiseks, autentimiseks, jne)
- ✓ Tühistusnimekirjade levituspunktid
- ✓ Sertifikaadi rakendusala kirjeldava sertifitseerimispoliitika OID(-d)
- ✓ Sertifitseerimispoliitika ulatuse piirid, URI viide konkreetsele CPSile ja kasutusala kirjeldamine sertifitseerimispoliitika laienduses. Sertifitseerimispoliitikate hierarhia kirjeldused.

7.2 Tühistusnimekirjad (CRL)

SK väljastab tühistusnimekirju vastavalt RFC 2459's esitatud nõuetele:

Tühistusnimekirjad peavad sisaldama vähemalt järgmisi punkte:

- ✓ versiooni number
- ✓ tühistusnimekiri ja tühistusnimekirja kirje laiendused ja nende kriitilisuse astmed

Kõik SK poolt väljastatavad CRL-id peavad sisaldama kohustuslikult välju:

- Authority Key Identifier
- CRL number

Väljal **authorityKeyIdentifier** esitatakse SK vastava avaliku võtme (millele vastavat privaatvõtit kasutati antud CRL-i kinnitamiseks) identifikaator, mis on oluline SK sertifikaatide ahela loomiseks.

Väli **CRLnumber** on monotoonselt kasvav arv ning määrab konkreetse, SK poolt välja antud, CRL-i järjekorranumbri.

SK võib välja anda ka *deltaCRL*-e, järgides RFC2459-s esitatud nõudeid. *DeltaCRL*-i olemus on esitatud samas RFC-s.

Samuti võib SK võimalusel kasutada ka *CRL Entry* laiendusi, järgides RFC2459-s esitatud nõudeid ja soovitusi.

8 Sertifitseerimispõhimõtete haldus

Sertifitseerimispõhimõtete 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 sertifitseerimispõhimõtete versioon olema eelnevatest selgelt eristatav. Uus versioon peab kandma ühe võrra suurendatud versiooninumbrit. Muudetud sertifitseerimispõhimõtted koos kehtima hakkamise päevaga, mis ei või olla varasem, kui 30 päeva avaldamisest, tuleb avaldada elektrooniliselt SK koduleheküljel

Kõik muudatused kooskõlastatakse SRR-ga.

9 Viidatud dokumendid

[1] Andmekogude seadus, RT 1 1997, 28, 423
[2] Eesti Vabariigi digitaalallkirja seadus, RT 1 2000, 26, 150.
[3] Isikut tõendavate dokumentide seadus, RT 1 1999,25,365
[4] Euroopa Liidu Komisjoni direktiiv "*Directive 1999/93/Ec Of The European Parliament And Of The Council"*
[5] Isikuandmete kaitse põhimõtted
[6] Isikuandmete kaitse seadus RT 1 1996, 48, 944.
[7] RFC 2459 – Request For Comments 2459, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile
[8] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

10 Kasutatud terminoloogia

Termin	Definitsioon
Autentimine	Isiku ühene identifitseerimine tema väidetavat identiteeti kontrollides
Avalik võti	Digitaalallkirja kontrollimise vahend
Digitaalallkiri	Andmekogumile lisatud andmed või rakendatud transformatsioon, mis võimaldab andmekogumi saajal teha kindlaks andmete allikat ja terviklust ning kaitsta võltsimise eest.
Direktiiv	Euroopa Liidu Komisjoni direktiiv "*Directive 1999/93/Ec Of The European Parliament And Of The Council"*
Eraldusnimi	Unikaalne, üheselt objekti identifitseeriv identifikaator
Eriõigustega süsteemikasutaja	Süsteemiadministraator; arvutisüsteemi kasutaja, kes ei allu tavapärastele õiguste piirangutele süsteemi haldamise võimaldamiseks
Huvitatud isik	(*Relying Party*) Osapool, kes võtab digitaalallkirja põhjal vastu mingi otsuse.
Isiklik võti	Isiku valduses olev krüptivõti, mille abil tõendab ta oma

Termin	Definitsioon
	isikut (digitaalallkirja andmise vahend).
Isikusertifikaat	Füüsilisele isikule väljastatud digitaalne sertifikaat
Kataloogiteenus	Sertifikaatide kehtivusinfo edastamise teenus
Kiipkaart	Tehniline seade isiklike võtmete ja sertifikaatide hoidmiseks. Isiklik võti ei välju kunagi kiipkaardist.
Klienditeeninduspunkt	Käesolevale CPSile vastava sertifitseerimispoliitika alusel toimiv SK teeninduspunkt sertifitseerimisega seotud teenuste osutamiseks.
Klient	Füüsiline isik, kes on isikusertifikaadi omanik
Krüpteerimine	Informatsiooni töötlusviis, mille puhul muudetakse informatsiooni loetematuks neile, kes ei oma selleks vajalikke teadmisi või õigusi
Objektiidentifikaator	(OID)– Ühene identifitseerimisnumber mingi objekti, näiteks sertifitseerimispoliitika ja sertifitseerimispõhimõtete identifitseerimiseks.
Räsifunktsioon	Matemaatiline teisendus, mille alusel viiakse sõnum (suvaline andmekogum) vastavaks fikseeritud pikkusega andmekogumiga -- sõnumilühendiga. Raske on leida kahte erinevat sõnumit, mille sõnumilühendid ühtivad.
Sertifikaat	DAS mõistes dokument, mis on välja antud, võimaldamaks digitaalallkirja andmist, ja milles avalik võti seotakse üheselt füüsilise isikuga.
Sertifitseerija	SK struktuuriüksus, mis väljastab ja kinnitab oma digitaalallkirjaga digitaalseid sertifikaate ja tühistussertifikaate.
Sertifitseerimispoliitika	Reeglite kogum, millega määratakse väljastatava sertifikaadi rakendusala ning rakendatavad turbenõuded.
Sertifitseerimispõhimõtted	Reeglite ja tingimuste kogum, millest SK sertifitseerimisteenuse osutamisel juhindub
Sertifitseerimisteenus	Sertifikaatide väljaandmine, sertifikaatide alusel antud digitaalallkirja kontrollimise võimaldamine ning sertifikaatide kehtivuse peatamise, peatatuse lõpetamise ja kehtetuks tunnistamise menetlemine.
Terviklus	Andmekogumi omadus: informatsiooni pole muudetud pärast andmekogumi loomist
Turvasündmus	Sündmus, mille tagajärjeks on (või võib olla) organisatsiooni varade kadu või kahjustus, või toiming, mis on vastuolus organisatsiooni turvaprotseduuridega.
Tühistusnimekiri	Kehtivuse kaotanud (tühistatud, peatatud) sertifikaatide loetelu

11 Lühendid

Lühend	Definitsioon
CA	*(Certification Authority)* Sertifitseerija
CP	*(Certificate Policy)* Sertifitseerimispoliitika
CPS	*(Certification Practise Statement)* Sertifitseerimispõhimõtted

CRL	*(Certificate Revocation List)* Tühistusnimekiri
DAS	Eesti Vabariigi digitaalallkirja seadus
DN	*(distinguished name)* eraldusnimi
KTP	SK klienditeeninduspunkt
NDA	*(non-disclosure agreement)* konfidentsiaalse informatsiooni kaitse leping
OID	*(Object Identifier)* Objektiidentifikaator, unikaalne objekti tunnuskood
PIN	*(Personal Identification Number)* 4-12-kohaline numbritest koosnev salakood, mis on vajalik isikliku võtme aktiveerimiseks enne iga kasutuskorda. PIN-koodi avalikuks tulek on samaväärne isikliku võtme avalikuks tulekuga.
PKI	*(Public Key Infrastructure)*Avaliku võtme infrastruktuur, vajalik digitaalallkirja andmise ja kasutamise süsteemi moodustamiseks
PKCS	(*Public Key Cryptography Standards*) Seeria avaliku võtme krüptograafial põhinevaid standarddokumente.
PUK	PIN-koodi lukustumise korral uue PIN-koodi määramiseks kasutatav 8-12-kohaline, numbritest koosnev salakood
RA	*(Registration Authority)* SK struktuuriüksus, mis tegeleb sertifikaaditaotluste vastuvõtmise, taotluse kontrolli ja/või taotluse sertifitseerijale edastamisega
RAO	*(Registration Authority Operator)* registreerimiskeskuse operaator
RT	Riigi Teataja
SRR	Sertifitseerimise Riiklik Register
SK	Sertifitseerimisteenuse osutaja, AS Sertifitseerimiskeskus
URI	*(Unified Resource Identifier)* Allikaviite tähistusviis