

AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtted CPS

Version 2.1

07.10.2002

Versioonid ja muudatused:

Versioon	Kuupäev	Kommentaarid
1.1	31.08.2001	Esimene versioon
2.0	01.02.2002	Muudetud eesmärgiga olla universaalseks alusdokumendiks erinevate sertifitseerimispoliitikate jaoks: <ul style="list-style-type: none">• välja jäetud SK CA-de struktuur• CPS ei oma enam OID-i• ette nähtud võimalus osade protseduuride (nt isikutuvastus) lepingujärgseks delegeerimiseks• üldistatud on sertifikaatide ja CRL-ide profiilide punkte• ära jäetud palju ebaolulist ja/või ID-kaardi spetsiifilist Parandatud keelt ja vormindust, välja jäetud ebaolulist.
2.1	07.10.2002	Lisatud turvaline logi (vt p. 4.7.3).

Sisukord

SISUKORD.....	3
SISSEJUHATUS	6
1.1 ÜLEVAADE.....	6
1.2 ORGANISATSIOON JA KASUTUSVALDKOND	6
1.2.1 Sertifitseerimiskeskus (SK).....	6
1.2.2 Registreerimiskeskus.....	7
1.2.3 Kasutaja.....	7
1.2.4 Sertifikaatide kasutusvaldkond.....	8
1.3 KONTAKTANDMED	8
2 ÜLDTINGIMUSED	9
2.1 KOHUSTUSED	9
2.1.1 Nõuded SK-le	9
2.1.2 Nõuded registreerimiskeskusele.....	9
2.1.3 Nõuded kliendile	10
2.1.4 Nõuded huvitatud isikule.....	10
2.1.5 Nõuded kataloogiteenusele	11
2.2 VASTUTUS	11
2.2.1 SK vastutus.....	11
2.2.2 Registreerimiskeskuse vastutus.....	11
2.2.3 Vastutuse piirid	11
2.3 VAIDLUSTE LAHENDAMINE.....	11
2.4 INFORMATSIOONI AVALDAMINE JA KATALOOGITEENUS	12
2.4.1 SK informatsiooni avaldamine.....	12
2.4.2 Avaldamise sagedus.....	12
2.4.3 Juurdepääsureglid.....	12
2.4.4 Kataloogiteenus	12
2.5 AUDIT	13
2.6 KONFIDENTSIAALSUS.....	13
2.6.1 Konfidentsiaalne informatsioon.....	13
2.6.2 Avalik informatsioon.....	13
2.6.3 Isikuandmete kaitse.....	13
3 KLIENDI IDENTIFITSEERIMINE	15
3.1 KLIENDI ISIKUSAMASUSE KONTROLL	15
3.2 SERTIFIKAADI TAOTLEJA AVALIKULE VÕTMELE VASTAVA ISIKLIKU VÕTME TÕENDAMISE KORD	15
3.3 ERALDUSNIMI	15
4 SERTIFITSEERIMISTEENUSE OSUTAMINE. SERTIFITSEERIMISMENETLUSE KORD JA TÄHTAJAD	16
4.1 SERTIFIKAADITAOTLUSE ESITAMINE.....	16
4.2 SERTIFIKAADITAOTLUSE MENETLEMINE	16
4.2.1 Otsuse tegemine	16
4.2.2 Sertifikaadi väljastamine	17

4.2.3	<i>Sertifikaatide üle arvestuse pidamise kord</i>	17
4.2.4	<i>Sertifikaadi kehtivuse kontroll ja tõendamine</i>	17
4.2.5	<i>Sertifikaadi uuendamine</i>	17
4.3	SERTIFIKAADI PEATAMISE JA KEHTETUKS TUNNISTAMISE TAOTLUSED	17
4.3.1	<i>Sertifikaadi peatamise ja kehtetuks tunnistamise taotluste volituste kontroll</i> 17	
4.3.2	<i>Kehtetuks tunnistatud, peatatud või aegunud sertifikaadi õigusliku kasutamise välistamine</i>	18
4.3.3	<i>Sertifikaadi õigusliku aluseta kehtetuks tunnistamise tagajärjed</i>	18
4.4	SERTIFIKAATIDE PEATAMINE	19
4.4.1	<i>Sertifikaadi peatamise tingimused ja menetlus</i>	19
4.5	SERTIFIKAADI PEATATUSE LÕPETAMINE	20
4.5.1	<i>Tingimused sertifikaadi peatamise lõpetamiseks</i>	20
4.5.2	<i>Sertifikaadi peatamise lõpetamise volitused</i>	20
4.5.3	<i>Sertifikaadi peatamise lõpetamise taotluse esitamine</i>	21
4.5.4	<i>Sertifikaadi peatamise lõpetamise menetlus</i>	21
4.5.5	<i>Sertifikaadi peatamise lõpetamise operatiivsus</i>	21
4.6	SERTIFIKAADI KEHTETUKS TUNNISTAMINE.....	22
4.6.1	<i>Sertifikaadi kehtetuks tunnistamise volitused</i>	22
4.6.2	<i>Sertifikaadi kehtetuks tunnistamise avalduse esitamine</i>	22
4.6.3	<i>Sertifikaadi kehtetuks tunnistamise menetlus</i>	22
4.6.4	<i>Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus</i>	22
4.7	PROTSEDUURID JÄLGITAVUSE TAGAMISEKS	23
4.7.1	<i>Dokumentide säilitamine</i>	23
4.7.2	<i>Logi</i>	23
4.7.3	<i>Turvaline logi</i>	23
4.8	TEGUTSEMINE ERIOLUKORRAS.....	24
4.9	SERTIFITSEERIMISTEENUSE OSUTAJA TÖÖ LÕPETAMINE.....	25
5	FÜÜSILISED JA ORGANISATSIOONILISED TURBEMEETMED	26
5.1	TURBEHALDUS	26
5.2	FÜÜSILISED TURBEMEETMED	26
5.2.1	<i>SK füüsiline pääsukontroll</i>	26
5.3	NÕUDED TÖÖPROTSEDUURIDELE	26
5.3.1	<i>Oluliste toimingute läbiviimine</i>	26
5.4	PERSONALI TURBENÕUDED	27
6	TEHNILISED TURBENÕUDED.....	28
6.1	VÕTMEHALDUS	28
6.1.1	<i>SK kinnitusvõtmed</i>	28
6.1.2	<i>Kliendi võtmed</i>	28
6.2	SÜSTEEMITURVE	30
6.2.1	<i>Pääsukontroll</i>	30
6.2.2	<i>Tarkvara turve</i>	30
6.2.3	<i>Võrguühenduste turve</i>	30
6.2.4	<i>Kellaaegade sünkroniseerimine</i>	30
6.3	SERTIFITSEERIMISTEENUSE OSUTAMISEKS KASUTATAVATE TEHNILISTE VAHENDITE KIRJELDUS.....	30
6.4	SERTIFITSEERIMISTEENUSE OSUTAMISEL TEKKINUD ANDMETE SÄILITAMINE JA KAITSE	31

7	SERTIFIKAATIDE JA TÜHISTUSNIMEKIRJADE (CRL-IDE)	
	TEHNILISED PROFILID	32
7.1	SERTIFIKAATIDE PROFIL.....	32
7.2	TÜHISTUSNIMEKIRJAD (CRL)	32
8	SERTIFITSEERIMISPÕHIMÕTETE HALDUS	33
9	VIIDATUD DOKUMENDID	34
10	KASUTATUD TERMINOLOOGIA	35
11	LÜHENDID	37

Sissejuhatus

AS 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-i Sertifitseerimiskeskus missiooniks on kindlustada kliente usaldusväärse sertifitseerimisteenusega vastavalt EV õigusaktidele ja rahvusvahelistele standarditele, olla andmekaitse alal üks turvalisemaid asutusi Eestis ning kasutada tipp tehnoloogiaid lähtudes konkreetsest vajadusest ja majanduslikust aspektist.

1.1 Ülevaade

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

Käesolevad sertifitseerimispõhimõtted laienevad ainult AS-i Sertifitseerimiskeskus poolt väljastatud digitaalsetele sertifikaatidele.

Käesolev CPS on aluseks erinevate sertifitseerimispoliitikate koostamisel ja nendele vastavate sertifitseerimisteenuste pakkumisel AS-is Sertifitseerimiskeskus.

Käesolev CPS on registreeritud sertifitseerimise riiklikus registris (SRR). Kõik käesoleva CPS-i alusel välja antud sertifitseerimispoliitikad, mis võimaldavad välja anda sertifikaate digitaalseks allkirjastamiseks DAS-i mõistes, on samuti registreeritud SRR-is.

Käesoleva CPS-i koostamisel on kasutatud IETF-i (*Internet Engineering Task Force*) soovituslikku dokumenti RFC 2527 [7].

Käesolevale CPS-ile viidatakse AS-i Sertifitseerimiskeskus tipmise sertifikaadi sertifitseerimispõhimõtete erilaienduses (*CPS pointer qualifier*).

Käesolev CPS aitab saavutada AS-i Sertifitseerimiskeskus juhatuse poolt kinnitatud turvapoliitikas dokumenteeritud turvataset. Lähtuvalt AS-i Sertifitseerimiskeskus turvapoliitikast on andmeturve ning selle kõrgele tasemele toetuv usaldus turvalise ja kvaliteetse teenuse vastu AS Sertifitseerimiskeskuse ülim prioriteet.

1.2 Organisatsioon ja kasutusvaldkond

1.2.1 Sertifitseerimiskeskus (SK)

SK osutab sertifitseerimisteenust vastavalt käesoleva CPS-i põhjal koostatud sertifitseerimispoliitikale koos sellega seonduvate lisateenustega.

SK sertifitseerimisteenus hõlmab vaikumisi kogu võtmepaaride ja sertifikaatide elutsükliga seotud protseduure, mida on kirjeldatud käesolevas dokumendis. SK-l on õigus sõlmida lepinguid, millega delegeeritakse ülesandeid kolmandatele osapooltele. Delegeeritud ülesanded ja vastutuse jagunemine on kirjeldatud vastavas sertifitseerimispoliitikas.

Käesolev CPS on kõikide SK poolt hallatavate CA-de sertifitseerimispoliitikate baasdokumendiks. Vastava CA sertifitseerimispoliitika täpsustab siintoodud aluspõhimõtteid. Käesoleva CPS-i ja konkreetse sertifitseerimispoliitika vastuolu korral on sertifitseerimispoliitikas toodu ülimuslik.

Sertifitseerimispoliitika OID on toodud ära vastava sertifitseerija kinnitusvõtme sertifikaadi sertifitseerimispoliitika laienduses.

1.2.2 Registreerimiskeskus

1.2.2.1 SK klienditeeninduspunkt

SK klienditeeninduspunkt tegutseb SK esindajana SK ja Kliendi vahelistes suhetes. SK klienditeeninduspunkt, käesoleva CPS-i mõistes, võtab vastu avaldusi sertifikaatide taotlemiseks, uuendamiseks, kehtivuse lõpetamiseks, sertifikaatide peatamiseks ja sertifikaatide peatamise lõpetamiseks.

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

SK klienditeeninduspunktid ja nende arv võivad erinevate sertifitseerimispoliitikate puhul olla erinevad. SK klienditeeninduspunkti ja SK vaheline suhe on ära määratud kahepoolse(te) lepingu(te)ga.

Informatsiooni SK klienditeeninduspunktide ja nende kontaktandmete kohta esitatakse SK koduleheküljel vastava avaliku teenuse dokumentatsiooni juures.

1.2.2.2 Abiliin

Abiliin tegeleb SK esindajana klientide telefoniteenindusega ja võtab ööpäevaringselt klientidelt ja teistelt osapooltelt vastu taotlusi sertifikaatide peatamiseks, eelnevalt identifitseerides isiku vastavalt sertifitseerimispoliitikas määratud isikusamasuse kontrolli protseduuridele.

Informatsiooni abiliini ja tema kontaktandmete kohta esitatakse SK koduleheküljel. Samas on toodud ära ka juhised abiliini poole pöördumiseks.

1.2.3 Kasutaja

1.2.3.1 Klient

Klient on käesoleva CPS-i 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 (*distinguished name*) ja sertifikaadi kinnitamissertifikaadi eraldusnime (*issuer name*) kombinatsiooni unikaalsuse.

1.2.3.2 Huvitatud isik

Huvitatud isik on osapool, kes võtab vastu otsuse kasutades selleks ka SK poolt väljastatud sertifikaati.

Huvitatud isik:

- arvestab põhimõtetega, mis on toodud konkreetse sertifikaadi sertifitseerimispoliitikas, käesolevas CPS-is ja nendes viidatud dokumentides;
- kontrollib sertifikaadi kehtivust SK avalikus kataloogis või värskeimas tühistusnimekirjas;
- kontrollib sertifikaadi kasutusala vastavust;
- kontrollib digitaalset allkirjastamist võimaldavate sertifikaatide puhul digitaalselt allkirjastatud andmekogumi terviklikkust ja identifitseerib allkirjastaja;
- lähtub varem antud digitaalallkirja kontrollimisel sertifikaadi kehtivusest digitaalallkirja andmise hetkel.

1.2.4 Sertifikaatide kasutusvaldkond

Sertifikaatide kasutamine peab olema kooskõlas sertifikaadi sertifitseerimispoliitikas toodud nõuete ja EV kehtestatud õigusaktidega.

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

Sertifitseerimispoliitikas ja sellega kaasnevas sertifikaatide profiilis määratakse ära, kas vastavaid sertifikaate saab kasutada digitaalallkirja seaduse mõttes. Käesolev CPS ei sea mingeid piiranguid selliste sertifitseerimispoliitikate koostamisele ning toetub oma põhimõtetes täie vastavusega digitaalallkirja seadusele.

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

1.3 Kontaktandmed

Kõikides sertifitseerimisteenusena, sh sertifitseerimiskeskuse, registreerimiskeskuse ja abiliini tegevusega seotud küsimustes 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 kohe SK koduleheküljel.

2 Üldtingimused

2.1 Kohustused

2.1.1 Nõuded SK-le

SK tagab, et

- sertifitseerimisteenuse osutamine on kooskõlas digitaalallkirja seaduse ja sellega seonduvate normatiivaktidega;
- sertifitseerimisteenuse osutamine on kooskõlas käesoleva CPS-iga.

SK kohustub:

- avalikustama oma sertifitseerimis põhimõtted ja sertifikaatide sertifitseerimis poliitika 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;
- võtma digitaalallkirja võimaldavate sertifikaatide puhul vastu ööpäevaringselt avaldusi sertifikaatide kehtivuse peatamiseks;
- tõendama digitaalallkirja võimaldavate sertifikaatide puhul huvitatud isiku nõudel oma esindaja digitaalallkirjaga enda poolt väljastatud sertifikaadis sisalduva avaliku võtme 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 osutajate riikliku registri volitatud töötlejale, et tagada enda püsiv registreeritus Sertifitseerimise Riiklikus Registris;
- avalikustama kohustusliku kindlustuslepingu tingimused üldkasutatavas andmesidevõrgus.

SK töötajal ei tohi olla karistatust tahtlikult toimepandud kuriteo eest.

2.1.2 Nõuded registreerimiskeskusele

2.1.2.1 Nõuded klienditeeninduspunktile

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

Klienditeeninduspunkt peab edastama õiged ja terviklikud andmed SK-le.

Klienditeeninduspunkti peab teenuse osutamist takistava tehnilise rikke korral teatama sellest kohe SK-le ja tegema kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

Klienditeeninduspunkt garanteerib oma töötajatele teenuse kvaliteetseks osutamiseks vajaliku koolituse.

Klienditeeninduspunkti töötajal ei tohi olla karistatust tahtlikult toimepandud kuriteo eest.

2.1.2.2 Nõuded abiliinile

Abiliin peab vastama Kliendi kõnele ööpäevaringselt 7 päeva nädalas.

Abiliin peab teenuse osutamist takistava tehnilise rikke korral teatama sellest koheselt SK-le ja tegema kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

Abiliini töötajal ei tohi olla karistatust tahtlikult toimepandud kuriteo eest.

2.1.3 Nõuded kliendile

Klient peab järgima SK poolt käesolevas CPS-is kehtestatud protseduure.

Klient peab sertifikaaditaotluses esitama õiget ja piisavat informatsiooni ning sertifikaati kantud andmete muutumise korral teatama õiged andmed vastavalt sertifikaadi sertifitseerimispoliitikas kehtestatud reeglitele. Klient peab olema teadlik sellest, et SK võib keelduda sertifikaadi väljastamisest, kui Klient on sertifikaaditaotluses teadlikult esitanud valeinformatsiooni või informatsiooni, mis on ebakorrekne või mittetäielik.

Klient peab oma isiklike võtmeid ja neile vastavaid sertifikaate kasutama SK poolt ettenähtud korras ja viisil.

Klient peab teatama isikliku võtme tema nõusolekuta kasutamise võimalusest viivitamatult SK-le ning peatama või tühistama oma sertifikaadi.

Klient vastutab ainuisikuliselt oma isikliku võtme hoidmise eest. Klient peab isikliku võtme kasutamisel lähtuma käesoleva CPS-i punktis 6.1.2.3 toodust.

Klient peab olema teadlik, et DAS-i mõttes on aegunud, kehtetuks tunnistatud või peatatud digitaalallkirja sertifikaadi alusel antud digitaalallkirjad kehtetud.

2.1.4 Nõuded huvitatud isikule

Huvitatud isik peab tutvuma sertifikaadi aktsepteerimisega seotud kohustuste ja riskidega, mis on toodud käesolevas CPS-is 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 aktsepteeritava tehingu spetsiifika vastavuses sertifitseerimispoliitikaga.

2.1.5 Nõuded kataloogiteenusele

Kataloogiteenuse eesmärgiks on võimaldada klientidele, huvitatud isikutele jt osapooltele juurdepääs sertifikaadiregistrile, et pärida informatsiooni sertifikaatide ning nende kehtivuse kohta.

Täpsed nõuded kataloogiteenusele tuuakse ära sertifitseerimispoliitikas.

Kataloogiteenus peab vastama järgmistele nõuetele:

- ✓ kataloog peab sisaldama väljastatud aegumata sertifikaate ning nende staatust;
- ✓ kataloog ei tohi sisaldada delikaatseid isikuandmeid isikuandmete kaitse seaduse [5] mõistes;
- ✓ kataloog peab olema ööpäevaringselt kättesaadav avalikus andmesidevõrgus
- ✓ rakendatud peavad olema turvameetmed kataloogiteenuse teeskluse vältimiseks ja andmetervikluse tagamiseks.

2.2 Vastutus

2.2.1 SK vastutus

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

2.2.2 Registreerimiskeskuse vastutus

2.2.2.1 Klienditeeninduspunkti vastutus

Klienditeeninduspunkt vastutab kõigi punktis 2.1.2.1 toodud kohustuste täitmise eest.

2.2.2.2 Abiliini vastutus

Abiliin 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 osapoolte 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.

Sertifitseerimispoliitikat tulenevate kohustuste mittetäitmist ei loeta rikkumiseks, kui selle põhjuseks on kohustuse täitja kontrollile mittealluv nn vääramatud jõud (*Force Majeure*).

2.3 Vaidluste lahendamine

Kõik osapooltevahelised 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 juursertifikaatide 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 tervikluse ja kättesaadavuse ööpäevaringselt 7 päeva nädalas.

2.4.2 Avaldamise sagedus

Väljastatud sertifikaadid avalikustab SK koheselt avalikus kataloogis.

Sertifikaatide tühistusnimekirju avaldatakse sertifitseerimispoliitikas toodud korra kohaselt. Sertifikaadi peatamise või kehtetuks tunnistamise järel avaldatakse seotud tühistusnimekiri avalikus kataloogis.

Maksimaalne lubatud viivitus sertifikaadi staatuse muutumise registreerimisest uue tühistusnimekirja väljastamiseni ning tühistusnimekirja kehtivusaeg sätestatakse vastavas sertifitseerimispoliitikas.

SK tagab oma koduleheküljel adekvaatse ja ajakohase info sertifikaadiinfo avaldamise kohta.

2.4.3 Juurdepääsureeglid

Juurdepääs punktis 2.4.1 kirjeldatud informatsioonile üldkasutatavat andmesidevõrku kasutades on tasuta ning juurdepääsu ei piirata. Teistel avaldamisviisidel võib SK kehtestada hinnakirjaga määratava tasu ja/või nõuda teeninduslepingu olemasolu.

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 tööd 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;
- ✓ oluliste teenuste ja infosüsteemi muudatuste korral auditeeritakse infosüsteem välisaudiitori poolt.

Auditeerimise alla kuuluvad järgmised valdkonnad:

- a) teenuse kvaliteet;
- b) teenuste turvalisus;
- c) SK operatsioonide ja protseduuride turvalisus;
- d) SK kliendiandmete kaitse ja SK turvapoliitika, tööprotseduuride ja lepinguliste kohustuste ning CPS-i nõuete korrektne täitmine;

2.6 Konfidentsiaalsus

2.6.1 Konfidentsiaalne informatsioon

Kogu sertifitseerimise teenuse 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.

2.6.2 Avalik informatsioon

Avaliku informatsiooni alla kuuluvad järgmised materjalid:

- sertifitseerimis põhimõtted koos viidatavate dokumentidega;
- sertifitseerimis poliitika koos viidatavate dokumentidega;
- kohustusliku kindlustuslepingu tingimused;
- isikuandmete kaitse põhimõtted;
- SK avalikud võtmed;
- auditeerimistulemused;
- väljastatud sertifikaatide kehtivusinfo.

Avalikule informatsioonile tagatakse juurdepääs punkti 2.4.3 kohaselt.

2.6.3 Isikuandmete kaitse

SK isikuandmete kaitse põhimõtted on toodud dokumendis "Isikuandmekaitse põhimõtted" [4]. Isikuandmete kaitse põhimõtete täitmise tagamisega garanteeritakse

3 Kliendi identifitseerimine

3.1 Kliendi isikusamasuse kontroll

Kliendi isikusamasust kontrollitakse vastavalt sertifitseerimispoliitikas sätestatule lähtudes isikut tõendavate dokumentide [3] seadusest.

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 võtme seotud sertifikaadi eraldusnime kombinatsiooni unikaalsuse.

SK kannab väljastatavatesse sertifikaatidesse unikaalse sertifikaadi järjenumbri.

4 Sertifitseerimise osutamine. Sertifitseerimismenetluse kord ja tähtajad

4.1 Sertifikaaditaotluse esitamine

Sertifikaadi taotlemine on võimalik ainult SK klienditeeninduspunktis.

Täpsema sertifikaadi taotlemise korra määrab ära sertifitseerimispoliitika.

Sertifikaaditaotluse esitamise kord peab minimaalselt olema kooskõlas järgnevate punktidega:

- Klienditeeninduspunkti töötaja annab kliendile sertifikaaditaotluse blanketi;
- Sertifikaaditaotlus peab sisaldama vähemalt järgnevat punkte:
 - viide taotletava sertifikaadi sertifitseerimispoliitikale;
 - märge selle kohta, kuidas toimub võtmepaari genereerimine;
 - märge selle kohta, et klient volitab SK genereerima kliendi avalikule võtmele vastava sertifikaadi;
 - viide teavituskana lile, mille kaudu edastatakse kliendile sertifitseerimise osutamisel tekkinud informatsiooni (nt informatsiooni sertifikaadi peatamise kohta);
 - kinnitus selle kohta, et klient aktsepteerib sertifitseerimispoliitika, sertifitseerimispoliitikat ning muid sertifikaatide kasutusala ning sellest tulenevat vastutust kirjeldavaid dokumente.
- Klient täidab sertifikaaditaotluse ja allkirjastab selle;
- Klienditeeninduspunkti töötaja tuvastab avalduse allkirjastanud kliendi isikusamasuse vastavalt punktis 3.1 sätestatule.

4.2 Sertifikaaditaotluse menetlemine

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

4.2.1 Otsuse tegemine

Sertifikaaditaotluse rahuldamise või mitterahuldamise otsustab SK või sertifitseerimispoliitikas sätestatud SK lepingujärgne partner vähemalt 5 tööpäeva jooksul.

SK või sertifitseerimispoliitikas sätestatud SK lepingujärgne partner 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 sertifikaaditaotluses märgitud teavituskanali kaudu.

4.2.2 Sertifikaadi väljastamine

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

Kliendile edastatakse väljastatud sertifikaat vastavalt sertifitseerimispoliitikale.

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.

4.2.4 Sertifikaadi kehtivuse kontroll ja tõendamine

Huvitatud isiku nõudmisel tõendab SK esindaja enda digitaalallkirjaga SK poolt väljastatud sertifikaadis sisalduvale avalikule võtmele vastava isikliku võtmega antud digitaalallkirja kehtivust.

Sertifikaatide kehtivuskinnituste väljastamisel 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 uuendamisvõimalused 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 peatamise ja kehtetuks tunnistamise volitusi kontrollitakse vastavalt järgnevale tabelile 1.

Tabel 1. Peatamise ja kehtetuks tunnistamise volitused

Taotluse esitamise viis	Peatamisaotlus	Peatamise lõpetamise taotlus	Kehtetuks tunnistamise taotlus
Telefoni teel, helistades SK abiliinile. Sertifikaatide peatamisel küsitakse peatamise taotleja isikuga seotud andmeid ning võrreldakse neid SK infosüsteemis olevate andmetega.	Peatatakse isikuandmeid puudutavatele kontrollküsimustele usaldusväärset vastamise korral.	Ei aktsepteerita	Peatatakse isikuandmeid puudutavatele kontrollküsimustele usaldusväärset vastamise korral ning pakutakse kliendile sobiv kanal kehtetuks tunnistamise taotluse esitamiseks.
Avalikus andmesidevõrgus SK koduleheküljel olevas rakenduses http://www.sk.ee .	Peatatakse isikuandmeid puudutavatele kontrollküsimustele usaldusväärset vastamise korral.	Ei aktsepteerita	Peatatakse isikuandmeid puudutavatele kontrollküsimustele usaldusväärset vastamise korral ning pakutakse kliendile sobiv kanal kehtetuks tunnistamise taotluse esitamiseks.
Avalikus andmesidevõrgus autendituna SK koduleheküljel olevas rakenduses http://www.sk.ee	Peatatakse.	Ei aktsepteerita	Peatatakse.
SK klienditeeninduspunktis isikut tõendava dokumendi esitamisel.	Peatatakse.	Peatus lõpetatakse	Tunnistatakse kehtetuks.

4.3.2 Kehtetuks tunnistatud, peatatud või aegunud sertifikaadi õigusliku kasutamise välistamine

Kehtetuks tunnistatud, peatatud või aegunud sertifikaadi õigusliku kasutamise välistamine tagatakse peale sertifikaadi kehtetuks tunnistamist või aegumist selle kataloogist kustutamise ja arhiveerimisega SK infosüsteemis.

Kehtetuks tunnistatud või peatatud sertifikaat publitseeritakse tühistusnimekirjas peale selle sertifikaadi kehtetuks tunnistamist või peatamist.

4.3.3 Sertifikaadi õigusliku aluseta kehtetuks tunnistamise tagajärjed

Isik või asutus, kelle taotluse 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 DAS-ile [2] sertifikaadi kehtivus peatatakse, kui:

- SK-l või sertifitseerimispoliitikas sätestatud SK lepingujärgsel partneril 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 töötaja, 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 või sertifitseerimispoliitikas sätestatud SK lepingujärgse partneri vastutav töötaja;
- SRR vastutav töötaja;
- DAS-is 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.

Peatamistaotlusi saab 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 andmed.

4.4.1.4 Peatamistaotluse menetlus

Sertifikaadi peatamise volituste kontroll toimub vastavalt esitusviisile tabelis 1 toodud korras. Kui klient esitab taotluse sertifikaadi peatamiseks SK klienditeeninduspunktis,

peab ta eelnevalt täitma vastava avaldusblanketi ja allkirjastama selle. Seejärel toimub menetlus alljärgnevalt:

- kontrollitakse peatamistaotleja volitusi;
- kontrollitakse sertifikaadi peatamise avalduse seaduslikkust;
- registreeritakse peatamise kõne abiliini operaatori poolt või registreeritakse peatamine SK klienditeeninduspunkti töötaja poolt;
- kontrollitakse peatamistaotleja isikuga seotud andmeid;
- viiakse läbi sertifikaadi peatamisavalduse käesolevale sertifitseerimispoliitikale vastavuse kontroll SK infosüsteemi poolt;
- sertifikaadi peatamistaotlus registreeritakse SK infosüsteemis;
- sertifikaat märgitakse peatatuks sertifikaatide andmebaasis (tühistusnimekirjas on vastavaks põhjuskoodiks 6 (*hold*));
- sertifikaat kustutatakse avalikust kataloogist;
- antakse välja uus sertifikaatide tühistusnimekiri vastavalt punktis 2.4.2 sätestatule;
- arhiveeritakse peatamistaotluse aluseks olevad materjalid.

Kui peatamine esitati abiliini kaudu, teavitatakse sertifikaadi omanikku sertifikaadi peatamisest sertifikaaditaotluses kliendi poolt määratud teavituskanali kaudu. Kliendil on võimalus veenduda kataloogi või tühistusnimekirja põhjal, et sertifikaat on peatatud.

4.4.1.5 Peatamise operatiivsus

Sertifikaadi peatamine kajastub kohe SK sertifikaatide andmebaasis ja avalikus kataloogis. Peatamise järel väljastab SK vastavalt punktis 2.4.2 toodud korrale uue tühistusnimekirja, mis sisaldab peatatud sertifikaadi järjekorranumbrit.

4.5 Sertifikaadi peatuse lõpetamine

4.5.1 Tingimused sertifikaadi peatuse lõpetamiseks

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

Sertifikaadi peatuse avaldusega kinnitab sertifikaadi omanik, et sertifikaadi peatuse ajal antud digitaalallkirjad on kehtetud.

4.5.2 Sertifikaadi peatuse lõpetamise volitused

Sertifikaadi peatust võivad lõpetada:

- sertifikaadi peatanud sertifikaadiomanik;
- SRR vastutav töötaja;
- SK või sertifitseerimispoliitikas sätestatud SK lepingujärgse partneri vastutav töötaja;
- vastavalt DAS-ile muu vastava volitustega ametnik, kes tegutses sertifikaadi peatamisel vastavalt punktile 4.4.1.2.

4.5.3 Sertifikaadi peatamise lõpetamise taotluse esitamine

Sertifikaadi peatamise lõpetamise taotlus esitatakse kirjalikult täidetud avaldusblanketil peale isikutuvastamist ja volituste kontrolli SK klienditeeninduspunktis.

Sertifikaadi peatamise lõpetamise tunnustamise taotlemiseks esitatud avaldus peab sisaldama:

- avalduse esitaja nime;
- avalduse esitaja allkirja;
- peatatud sertifikaadi omaniku nime ja isikukoodi;
- peatatud sertifikaadi väljastanud SK eraldusnime;
- peatamise lõpetamise alust.

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

Avalduse registreerimisel märgitakse üles avalduse esitaja isikutuvastamisel kasutatud dokumendi andmed.

4.5.4 Sertifikaadi peatamise lõpetamise menetlus

Peatamise lõpetamise menetlus toimub järgnevalt:

- peatamise lõpetamise algataja koostab kirjaliku avalduse sertifikaadi peatamise lõpetamiseks SK klienditeeninduspunktis vastavale blankatile ja allkirjastab selle;
- kontrollitakse peatamise lõpetamise volitust;
- kontrollitakse sertifikaadi peatamise lõpetamise avalduse seaduslikkust;
- viiakse läbi peatamise lõpetamise vastavuse kontroll SK infosüsteemi poolt;
- registreeritakse sertifikaadi peatamise lõpetamise fakt SK infosüsteemis;
- avaldatakse sertifikaat uuesti avalikus kataloogis;
- antakse välja uus sertifikaatide tühistusnimekiri vastavalt punktis 2.4.2 sätestatule.

Kliendile teatatakse peale peatamise lõpetamistaotluse registreerimist hetk, mil ükski kehtiv tühistusnimekiri enam sertifikaadi kasutamist ei piira. Kliendil on võimalus veenduda kataloogi või tühistusnimekirja põhjal, et sertifikaat on aktiivne.

4.5.5 Sertifikaadi peatamise lõpetamise operatiivsus

Sertifikaadi peatamine kajastub koheselt SK sertifikaatide andmebaasis ja avalikus kataloogis. Peatamise lõpetamise järel väljastab SK vastavalt punktis 2.4.2 toodud korrale uue tühistusnimekirja, mis ei sisalda peatamise lõpetanud sertifikaadi järjekorranumbrit.

4.6 Sertifikaadi kehtetuks tunnistamine

4.6.1 Sertifikaadi kehtetuks tunnistamise volitused

Sertifikaadi kehtetuks tunnistamise avalduse võib esitada sertifikaadi omanik, 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;
- kehtetuks tunnistatava sertifikaadi omaniku nime ja isikukoodi;
- kehtetuks tunnistatava sertifikaadi väljastanud SK eraldusnime;
- sertifikaadi kehtetuks tunnistamise põhjust;
- vajadusel tõendusmaterjali sertifikaadi kehtetuks tunnistamise põhjuse asjaolude tõendamiseks.

Kehtetuks tunnistamise avalduse esitaja identifitseeritakse SK klienditeeninduspunktis kehtiva isikut tõendava dokumendi alusel. Avalduse registreerimisel märgitakse üles avalduse esitaja identifitseerimisel kasutatud dokumendi andmed.

4.6.3 Sertifikaadi kehtetuks tunnistamise menetlus

Sertifikaadi kehtetuks tunnistamise menetlus toimub järgnevalt:

- sertifikaadi kehtetuks tunnistamise taotleja koostab kirjalikult sertifikaadi kehtetuks tunnistamise avalduse SK klienditeeninduspunktis vastavale blanketile ja allkirjastab selle;
- kontrollitakse sertifikaadi kehtetuks tunnistamise avalduse seaduslikkust;
- viiakse läbi kehtetuks tunnistamise avalduse õigsuse kontroll SK infosüsteemi poolt;
- sertifikaadi kehtetuks tunnistamise avaldus registreeritakse SK infosüsteemis;
- sertifikaat märgitakse kehtetuks avalikus kataloogis;
- antakse välja uus sertifikaatide tühistusnimekiri vastavalt punktis 2.4.2 sätestatule;
- arhiveeritakse kehtetuks tunnistamise avalduse aluseks olevad materjalid.

Kliendil on võimalus veenduda avaliku kataloogi või tühistusnimekirja põhjal, et sertifikaat on tunnistatud kehtetuks.

4.6.4 Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus

Sertifikaadi kehtetuks tunnistamine kajastub kohele SK sertifikaatide andmebaasis ning avalikus kataloogis. Peale sertifikaadi kehtetuks tunnistamist väljastab SK vastavalt punktis 2.4.2 toodud korrale uue tühistusnimekirja, mis sisaldab kehtetuks tunnistatud sertifikaadi järjekorranumbrit.

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 digitaalalkirja võimaldavate sertifikaatidega seotud dokumentatsioon üle SRR-ile.

4.7.2 Logi

SK infosüsteemid logivad:

- kõiki SK kinnitusvõtmete elutsükli etappe ja kasutamist;
- kõiki klientide võtmete elutsükli etappide;
- kõiki turvasündmusi, nagu näiteks kasutajate autoriseerimised või edutud autoriseerimise katsed;
- eriõigustega süsteemikasutajate tegevusi.

SK kasutab standarditele vastavaid infoturvelahendusi, mis tagavad isiklike võtmete, aktiveerimiskoodide, pääsukoodide (näiteks PIN-ide) ja muu turvakriitilise informatsiooni logis mittesalvestumise.

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

Logid säilitatakse SK infosüsteemis vähemalt 36 kuud.

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

SK-s on kehtestatud kord logide regulaarseks analüüsiks ning võimaliku ründe kiireks avastamiseks.

4.7.3 Turvaline logi

SK infosüsteemis on rakendatud spetsiaalne turvalise logi süsteem, mis tagab krüptograafiliste meetoditega logikirjete ajalise järjestuse tervikluse. Turvalisse logisse kantakse:

- kõik sertifikaatide olekumuutused (aktiveerimine, peatamine, peatamise lõpetamine, tühistamine)

- kõik SK poolt välja antavad digitaalselt allkirjastatud sertifikaatide kehtivuskinnitused

Salgamise vääramise tagamiseks publitseeritakse turvalise logi ühte kirjet vähemalt üks kord aastas SK kodulehel ning Ametlikes Teadaannetes.

Turvaline logi tagab sertifikaatide olekuinformatsiooni auditeeritavuse. SK kodulehel paikneva rakenduse abil on võimalik kontrollida väljastatud kehtivuskinnituste olemasolu SK turvalises logis.

4.8 Tegutsemine eriolukorras

SK on koostanud riskianalüüsi SK sertifitseerimissüsteemi kohta, et ennetada võimalikku 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 „AS-i Sertifitseerimiskeskus infoturbepoliitika“, „AS-i Sertifitseerimiskeskus käideldavuse strateegia ja poliitika“, „AS-i Sertifitseerimiskeskus IT süsteemide taastamise poliitika“ ja spetsiaalsed juhendid ning taasteplaani kriisisituatsioonis tegutsemiseks, tagamaks teenuse osutamise turvalisus ja kvaliteet. AS-i Sertifitseerimiskeskus infosüsteem ja kasutatav dokumentatsioon on auditeeritud sõltumatu IT audiitori poolt.

Käsitletavad juhendid ja taasteplaani hõlmavad tegutsemiskavasid järgnevate kriisisituatsioonide puhul:

- SK kinnitusvõtme avalikustumise või avalikustumise kahtluse korral;
- SK tegevuse võimaliku jälgendamise korral;
- SK sertifitseerija isikliku võtme hävimise korral;
- SK sertifikaatide andmebaasi hävimise korral;
- SK teenuse jälgendamise kahtluse või jälgendamise korral;
- andmetöötluskeskust sisaldava hoone täieliku või osalise hävimise korral;
- andmetöötluskeskust avaliku andmesidevõrguga ühendava sidekanali tõrke korral;
- tootekeskonna elektri- või veevärgi tõrke korral;
- teenuse tõkestamiseks teostatud infotehnoloogilise ründe korral;
- olulise personaliosa üheaegse töövõimetuse korral.

Tegutsemiskavas 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 avalike teabelevituskanalite kaudu.

Kui eriolukorra tõttu sai võimalikuks sertifikaadi andmebaasi sisu muutumine, sertifikaatide väljastamine, peatamine, peatamise 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 nõukogu otsusega;
- 2) teenuse osutamise üle järelevalvet teostava asutuse otsusega;
- 3) kohtuotsusega;
- 4) AS-i Sertifitseerimiskeskus likvideerimise või tegevuse lõpetamise korral.

Sertifitseerimisteenuse osutamise lõpetamisel annab SK teenuse osutamisega seotud dokumentatsiooni üle SRR-ile vastavalt kehtestatud korrale.

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

SK kohustub lisaks DAS-is esitatud nõuetele teenuse lõpetamisel tunnistama kehtetuks kõik väljaantud ja kehtivad sertifikaadid.

SK valduses olevad riistvaralised seadmed kas reinitialiseeritakse 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, nt ISO 13335, ISO 13569.

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

SK haldab infovarade registrit ning klassifitseerib kõik infovarad turbeklassidesse vastavalt turbeanalüüsi 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 protseduuriereglitega.

5.3.1.2 Toimingute dokumenteerimine

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

- kõiki SK kinnitamisvõtme elutsükli etappe ja kasutuskordasid;
- eriolukordade lahendusi.

5.4 Personali turbenõuded

Töötajal, kes on seotud käesolevas CPS-is kirjeldatud teenuse osutamisega, ei tohi olla karistatust tahtlikult toime pandud kuriteo eest. 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 elluviimise 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 taastamine.
- siseaudiitor: omab õigust jälgida dokumendiarhiive ja infosüsteemide logisid.

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

Sertifitseerimisteenu osutamisel kasutatakse RSA algoritmi võtmeid järgmiste miinimumpikkustega:

- SK kinnitusvõti – 2048 bitti;
- sertifikaadile vastav salajane võti – 1024 bitti.

Sertifitseerimisteenu osutamiseks vajalikud SK kinnitusvõtmed luuakse vastavalt SK sisekorra dokumentidele „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

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.

Sertifitseerimisteenu 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 kehtetuks tunnistamise 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.

SK-l ei ole käesoleva CPS-i mõttes mingit vastutust kliendi võtme ja selle aktiveerimiskoodi konfidentsiaalsuse eest juhul, kui kliendi võtmed genereerib klient ise või teeb seda selle vastutuse võtnud kolmas osapool.

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 peavad vastama järgmistele tingimustele:

- 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;
- isikliku võtme aktiveerimise ajal peab klient olema teadlik sooritatavast tegevusest: digitaalallkirja andmisel tuleb esitada allkirjastatava dokumendi sisu.

SK-l ei ole käesoleva CPS-i mõttes mingit vastutust kliendi salajase võtme aktiveerimise turvalisuse eest.

6.1.2.4 Kliendi võtmete hävitamine

Kliendi võtmete hävitamine on määratud vastava sertifitseerimispoliitikaga. Juhul, kui SK on kliendi võtmeid varundanud, hävitab SK sertifikaadi kehtivuse lõpu või kehtetuks tunnistamise järel vastava kliendi võtme.

6.1.2.5 Kliendi võtmete varundamine ja deponeerimine

Klientide isiklikest võtmetest ei salvestata varukoopiaid ja neid ei deponeerita mingil moel juhul, kui vastavat isiklikku võtit kasutatakse digitaalallkirja andmiseks. Muudel juhtudel võidakse kliendi võtmeid deponeerida ja teha neist varukoopiaid juhul, kui klient esitab sellise soovi ning selline teenus on ette nähtud sertifitseerimispoliitikaga.

6.2 Süsteemiturve

6.2.1 Pääsukontroll

SK realiseerib pääsukontrollisüsteemi, mis identifitseerib, autoriseerib ja registreerib usaldusväärset 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 Kellaegade sünkroniseerimine

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

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

Etalonkella sünkroniseeritakse GPS (*Global Positioning System*) abil, mis määrab ära ka etalonkella täpsuse.

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 tootekeskonnas paiknevas ainult selleks otstarbeks eraldatud sertifitseerimisserveri sertifitseerijamoodulis CA.

Sertifitseerimismooduli CA juhtimine toimub operaatormooduli CAO kaudu, mida saavad 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*.

Sertifitseerimisteenus osutamisel kasutatakse firmade SUN servereid ja IBM tüüpi töökohaarvuteid.

6.4 Sertifitseerimisteenus osutamisel tekkinud andmete säilitamine ja kaitse

SK hoiab ja archiveerib 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 sertifitseerimisteenus osutamisel tekkinud andmeid oma tegevusaja lõpuni.

7 Sertifikaatide ja tühistusnimekirjade (CRL-ide) tehnilised profiilid

7.1 Sertifikaatide profiil

Sertifikaadiprofiilid on avaldatud või viidatud vastavates sertifitseerimispoliitika dokumentides.

Sertifitseerijate sertifikaatide profiilid on esitatud dokumendis “AS-i Sertifitseerimiskeskus CA sertifikaatide profiilid”.

Sertifikaadi profiil peab olema koostatud vastavalt RFC 2459-s [6] esitatud nõuetele.

7.2 Tühistusnimekirjad (CRL)

SK väljastab tühistusnimekirju vastavalt RFC2459-s [6] esitatud nõuetele. Sertifitseerimispoliitika võib tühistusnimekirjade nõudeid vajadusel täpsustada.

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 murrarvulist 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 koostatakse SRR-iga.

9 Viidatud dokumendid

- [1] Andmekogude seadus, RT I 1997, 28, 423
- [2] Eesti Vabariigi digitaalalkirja seadus, RT I 2000, 26, 150
- [3] Isikut tõendavate dokumentide seadus, RT I 1999, 25, 365
- [4] Isikuandmete kaitse pehimõtted, AS Sertifitseerimiskeskus
- [5] Isikuandmete kaitse seadus RT I 1996, 48, 944
- [6] RFC 2459 – Request For Comments 2459, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile
- [7] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

10 Kasutatud terminoloogia

Käesolevas CPS-is kasutatakse termineid alljärgnevas mõistes. Mõistete definitsioonid ei pruugi kokku langeda DAS-is defineeritud mõistetega.

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
Eraldusnimi	Unikaalne, üheselt objekti identifitseeriv identifikaator
Eriõigustega süsteemikasutaja	Süsteemiadministraator; arvutisüsteemi kasutaja, kes ei allu tavapärastele õiguste piirangutele süsteemi haldamise võimaldamiseks
Huvitatud isik	(<i>Relying Party</i>) Osapool, kes võtab digitaalallkirja põhjal vastu mingi otsuse, vt punkt 2.1.4
Isik	DAS-i mõistes füüsiline isik. DAS-i väliselt võib käesoleva CPS-i mõistes käsitleda isikuna ka juriidilist isikut juhul, kui ei väljastata sertifikaate digitaalseks allkirjastamiseks
Isiklik võti	Isiku valduses olev võti, mille abil tõendab ta oma isikut (digitaalallkirja andmise vahend)
Kataloogiteenus	Sertifikaatide kehtivusinfo edastamise teenus
Kinnitusvõti	Sertifitseerimisteenuse osutaja isiklik võti, mida kasutatakse sertifikaatide signeerimiseks
Klienditeeninduspunkt	Käesolevale CPS-ile vastava sertifitseerimispoliitika alusel toimiv SK teeninduspunkt sertifitseerimisega seotud teenuste osutamiseks, vt punkt 1.2.2.1
Klient	Sertifikaadi omanik, vt punkt 1.2.3.1
Krüpteerimine	Informatsiooni töötlusviis, mille puhul muudetakse informatsiooni loetamatuks neile, kes ei oma selleks vajalikke teadmisi või õigusi
Objektiidentifikaator	(OID) Ühene identifitseerimisnumber mingi objekti, näiteks sertifitseerimispoliitika ja sertifitseerimis põhimõtete identifitseerimiseks
Räsifunktsioon	Matemaatiline teisendus, mille alusel viiakse sõnum (suvaline andmekogum) vastavaks fikseeritud pikkusega andmekogumiga – sõnumilühendiga. Raske on leida kahte erinevat sõnumit, mille sõnumilühendid ühtivad
Sertifikaaditaotlus	Kliendi poolt täidetav ning käsitsi allkirjastatav kirjalik avaldus sertifikaadi saamiseks
Sertifikaat	DAS-i mõistes dokument, mis on välja antud, võimaldamaks digitaalallkirja andmist, ja milles avalik võti seotakse üheselt füüsilise isikuga. DAS-i väliselt võib sertifikaadiomanik olla ka juriidiline isik ning

Termin	Definitsioon
	sertifikaati võib kasutada ka muuks kui digitaalallkirja andmiseks.
Sertifitseerija	SK struktuuriüksus, mis väljastab ja kinnitab oma digitaalallkirjaga digitaalseid sertifikaate ja tühistus nimekirju.
Sertifitseerimispoliitika	Reeglite kogum, millega määratakse väljastatava sertifikaadi rakendusala ning rakendatavad turbenõuded.
Sertifitseerimisteenus	Sertifikaatide väljaandmise ja halduse teenus koos asjakohaste lisateenustega.
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	(<i>Certification Authority</i>) Sertifitseerija
CP	(<i>Certificate Policy</i>) Sertifitseerimispoliitika
CPS	(<i>Certification Practice Statement</i>) Sertifitseerimispõhimõtted
CRL	(<i>Certificate Revocation List</i>) Tühistusnimekiri
DAS	Eesti Vabariigi digitaalallkirja seadus
OID	(<i>Object Identifier</i>) Objektiidentifikaator, unikaalne objekti tunnuscode
PIN	(<i>Personal Identification Number</i>) Aktiveerimiskood, 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
RA	(<i>Registration Authority</i>) SK struktuuriüksus, mis tegeleb sertifikaaditaotluste vastuvõtmise, taotluse kontrolli ja/või taotluse sertifitseerijale edastamisega
RT	Riigi Teataja
SRR	Sertifitseerimise Riiklik Register
SK	Sertifitseerimisteenuse osutaja, AS Sertifitseerimiskeskus