

Asutuse digitaalse kinnituse sertifikaatide sertifitseerimispoliitika

AS Sertifitseerimiskeskus

OID: 1.3.6.1.4.1.10015.7.1.1.1

Versioonid ja muudatused:

Versioon	Kuupäev	Kommentaarid
0.1	18.03.2003	Esimene versioon. Projekt
0.2	03.04.2003	Käesolev dokument. Arvestatud laekunud kommentaaridega. Projekt
0.3	12.05.2003	Terminoloogia muutmine: asutuse sertifikaat -> asutuse digitaalse kinnituse sertifikaat

Sisukord

ASUTUSE DIGITAALSE KINNITUSE SERTIFIKAATIDE SERTIFITSEERIMISPOLIITIKA.....	1
SISUKORD.....	2
1 SISSEJUHATUS	4
1.1 ÜLEVAADE.....	4
1.2 SERTIFITSEERIMISPOLIITIKA IDENTIFITSEERIMINE	4
1.3 ORGANISATSIOON JA KASUTUSVALDKOND	5
1.3.1 <i>Sertifitseerimiskeskus (SK)</i>	5
1.3.2 <i>SK registreerimiskeskus</i>	5
1.3.3 <i>Kasutaja</i>	5
1.3.4 <i>Sertifikaatide kasutusvaldkond</i>	5
1.4 KONTAKTANDMED.....	6
2 ÜLDTINGIMUSED	6
2.1 KOHUSTUSED JA NÕUDED	6
2.1.1 <i>SK kohustused</i>	6
2.1.2 <i>Registreerimiskeskuse kohustused</i>	6
2.1.3 <i>Nõuded kliendile</i>	7
2.1.4 <i>Nõuded huvitatud isikule</i>	7
2.1.5 <i>Nõuded kataloogiteenusele</i>	7
2.2 VASTUTUS	7
2.2.1 <i>SK vastutus</i>	7
2.2.2 <i>Registreerimiskeskuse vastutus</i>	7
2.2.3 <i>Vastutuse piirid</i>	7
2.3 VAIDLUSTE LAHENDAMINE	7
2.4 INFORMATSIOONI AVALDAMINE JA KATALOOGITEENUS	7
2.4.1 <i>SK informatsiooni avaldamine</i>	7
2.4.2 <i>Avaldamise sagedus</i>	8
2.4.3 <i>Juurdepääsureeglid</i>	8
2.4.4 <i>Kataloogiteenus</i>	8
2.5 AUDIT	8
2.6 KONFIDENTSIAALSUS.....	8
2.7 OMANDIÕIGUSED	8
3 KLIENDI IDENTIFITSEERIMINE	8
3.1 KLIENDI ISIKUSAMASUSE KONTROLL	8
3.2 SERTIFIKAADI TAOTLEJA AVALIKULE VÕTMELE VASTAVA ISIKLIKU VÕTME TÕENDAMISE KORD	8
3.3 ERALDUSNIMI	9
4 SERTIFITSEERIMISTEENUSE OSUTAMINE. SERTIFITSEERIMISMENETLUSE KORD JA TÄHTAJAD	9
4.1 SERTIFIKAADITAOTLUSE ESITAMINE	9
4.2 SERTIFIKAADITAOTLUSE MENETLEMINE	9

4.2.1	<i>Otsuse tegemine</i>	9
4.2.2	<i>Sertifikaadi väljastamine</i>	9
4.2.3	<i>Sertifikaatide üle arvestuse pidamise kord</i>	9
4.2.4	<i>Sertifikaadi kontroll ja tõestamine</i>	10
4.2.5	<i>Sertifikaadi uuendamine</i>	10
4.3	SERTIFIKAADI KEHTETUKS TUNNISTAMISE JA PEATAMISE TAOTLUSED	10
4.4	SERTIFIKAATIDE PEATAMINE	10
4.5	SERTIFIKAADI PEATATUSE LÕPETAMINE	10
4.6	SERTIFIKAADI KEHTETUKS TUNNISTAMINE	10
4.6.1	<i>Sertifikaadi kehtetuks tunnistamise volitused</i>	10
4.6.2	<i>Sertifikaadi kehtetuks tunnistamise avalduse esitamine</i>	11
4.6.3	<i>Sertifikaadi kehtetuks tunnistamise menethus</i>	11
4.6.4	<i>Sertifikaadi kehtetuks tunnistamise menethuse operatiivsus</i>	11
4.7	PROTSEDUURID JÄLGITAVUSE TAGAMISEKS.....	11
4.8	TEGUTSEMINE ERIOLUKORRAS.....	11
4.9	SERTIFITSEERIMISTEENUSE OSUTAJA TÖÖ LÕPETAMINE	11
5	FÜÜSILISED JA ORGANISATSIOONILISED TURBEMEETMED	11
5.1	TURBEHALDUS	11
5.2	FÜÜSILISED TURBEMEETMED	11
5.2.1	<i>SK füüsiline pääsukontroll</i>	11
5.3	NÕUDED TÖÖPROTSEDUURIDELE	11
5.4	PERSONALI TURBENÕUDED	12
6	TEHNILISED TURBENÕUDED.....	12
6.1	VÕTMEHALDUS	12
6.1.1	<i>SK kinnitusvõtmed</i>	12
6.1.2	<i>Kliendi võtmed</i>	12
6.2	SÜSTEEMITURVE	12
6.3	SERTIFITSEERIMISTEENUSE OSUTAMISEKS KASUTATAVATE TEHNILISTE VAHENDITE KIRJELDUS.....	12
6.4	SERTIFITSEERIMISTEENUSE OSUTAMISEL TEKKINUD ANDMETE SÄILITAMINE JA KAITSE	12
7	SERTIFIKAATIDE JA TÜHISTUSNIMEKIRJADE (CRLIDE) TEHNILISED PROFIILID.....	12
7.1	SERTIFIKAATIDE PROFIIL.....	12
7.2	TÜHISTUSNIMEKIRJAD (CRL)	12
8	SERTIFITSEERIMISPOLIITIKA HALDUS	13
9	KASUTATUD TERMINOLOOGIA	13
10	KASUTATUD LÜHENDID	13
11	VIIDATUD JA SEONDUVAD DOKUMENDID	13

1 Sissejuhatus

1.1 Ülevaade

Käesolev dokument (edaspidi sertifitseerimispoliitika, CP) on reeglite kogum, mis määrab ära peamised tööpõhimõtted ja -kontseptsioonid asutuse digitaalse kinnituse sertifikaadi väljastamiseks vajaliku sertifitseerimisteenuse osutamiseks.

Käesolev CP rajaneb dokumendile „AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted versioon 1.2“ [1], mis on registreeritud sertifitseerimisteenuse osutajate riiklikus registris. Need sertifitseerimispõhimõtted (edaspidi: CPS) on aluseks sertifitseerimisteenuse osutamisel, käesolev CP täpsustab täiendavalt CPS-is toodud põhimõtteid.

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

Käesolev CP laieneb ainult AS-i Sertifitseerimiskeskus poolt väljastatud ja käesolevas CP-s viidatud sertifikaadiprofiilile vastavatele digitaalsetele sertifikaatidele.

Käesolev CP koostamisel on kasutatud IETFi (*Internet Engineering Task Force*) soovitusliku dokumenti RFC 2527 [5].

1.2 Sertifitseerimispoliitika identifitseerimine

Käesoleva CP tunnuscode on **OID: 1.3.6.1.4.1.10015.7.1.1.1**

CP tunnuscode on koostatud vastavalt järgnevale tabelile 1.

Parameeter	Viide OIDis
Interneti tunnus	1.3.6.1
Eraettevõtte tunnus	4
Eraettevõtteid haldava IANA poolt registreeritud ettevõtte tunnus	1
IANA registris ASile Sertifitseerimiskeskus antud tunnus	10015
Sertifitseerimisteenuse tunnus	7.1
CP versiooni tunnus	1.1

Tabel 1. CP tunnuscode koostamine

1.3 Organisatsioon ja kasutusvaldkond

1.3.1 Sertifitseerimiskeskus (SK)

Vt CPS p.1.2.1.

1.3.2 SK registreerimiskeskus

1.3.2.1 SK klienditeeninduspunkt

SK klienditeeninduspunktiks on Sertifitseerimiskeskus AS ise.

1.3.2.2 Abiliin

Kuna käesoleva CP raames sertifikaatide peatamisteenus puudub, siis ei eksisteeri abiliini. Kõikide asutuse digitaalse kinnituse sertifikaati puudutavate küsimuste puhul tuleb pöörduda SK poole SK tööajal.

1.3.3 Kasutaja

1.3.3.1 Klient

Vt CPS p.1.2.3.1.

Käesoleva CP alusel väljastatakse sertifikaate Eesti Vabariigis registreeritud asutusele ja organisatsioonile, kes on käesoleva CP mõistes Klient.

Klient on käesoleva CP alusel väljastatud sertifikaadi omanik.

Kliendi eraldusnimi sertifikaadis koostatakse vastavalt sertifikaadiprofiilile, mis on toodud käesoleva dokumendi lisas.

1.3.3.2 Huvitatud isik

Vt CPS p.1.2.3.2.

Huvitatud isik peab lisaks olema eelnevalt tutvunud käesoleva CP-ga.

1.3.4 Sertifikaatide kasutusvaldkond

Vt CPS p.1.2.4.

Käesoleva CP alusel väljastatakse sertifikaate, mida kasutatakse Kliendi digitaalsete kinnituste andmiseks ja e-kirjade signeerimiseks.

Sertifikaatide täpne kasutusvaldkond peab olema kirjeldatud sertifikaadiga seotud Kliendi signeerimispoliitikas. Nõuded signeerimispoliitika struktuurile ja sisule on toodud dokumendis "Nõuded asutuse signeerimispoliitikale" [8].

Asutuse digitaalse kinnituse sertifikaate ei saa kasutada digitaalseks allkirjastamiseks DAS [3] mõttes.

1.4 Kontaktandmed

Vt CPS p.1.3.

2 Üldtingimused

2.1 Kohustused ja nõuded

2.1.1 SK kohustused

Vt CPS p.2.1.1.

SK tagab täiendavalt, et:

- sertifitseerimisteenus osutamine on kooskõlas AS Sertifitseerimiskeskuse sertifitseerimis põhimõtetega;
- sertifitseerimisteenus osutamine on kooskõlas käesoleva CPga.

SK kohustub täiendavalt:

- võtma vastu ja rahuldama Kliendi sertifikaaditaotlused üle elektroonse turvalise andmesidekanali;
- osutama ööpäevaringset kataloogiteenust;
- tagama, et sertifitseerimisteenus osutamisel kasutatavad kinnitusvõtmed oleksid riistvaraliste turvamoodulite abil kaitstud ning ei väljuks SK kontrolli alt;
- kinnitusvõtmete kontrolli alt väljumise korral kehtetuks tunnistama kõik väljastatud sertifikaadid;
- tagama, et kõik aktiveeritud režiimis olevad kinnitusvõtmed asuvad Eesti Vabariigi territooriumil;
- tagama, et sertifitseerimisteenus osutamisel kasutatavate kinnitusvõtmete aktiveerimine toimub jagatud kontrolli alusel;

2.1.2 Registreerimiskeskuse kohustused

2.1.2.1 SK klienditeeninduspunkti kohustused

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

2.1.2.2 Abiliini kohustused

Abiliin puudub.

2.1.3 Nõuded kliendile

Vt CPS p.2.1.3.

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

2.1.4 Nõuded huvitatud isikule

Vt CPS p.2.1.4.

Huvitatud isik peab arvestama sertifikaadi aktsepteerimisega seotud kohustuste ja riskidega, mis on toodud käesolevas CP-s.

2.1.5 Nõuded kataloogiteenusele

Vt CPS p.2.1.5.

2.2 Vastutus

2.2.1 SK vastutus

Vt CPS p.2.2.1.

SK on vastutav kõigi punktis 2.1.1 ja 2.1.2 toodud kohustuste täitmise eest Eesti Vabariigis kehtivates õigusaktides nõutud piirides.

2.2.2 Registreerimiskeskuse vastutus

2.2.2.1 Klienditeeninduspunkti vastutus

Vt CPS p.2.2.2.1.

Klienditeeninduspunkt vastutab kõigi punktis 2.1.2.1 toodud kohustuste täitmise eest.

2.2.2.2 Abiliini vastutus

Abiliin puudub.

2.2.3 Vastutuse piirid

Vt CPS p.2.2.3.

2.3 Vaidluste lahendamine

Vt CPS p.2.3.

2.4 Informatsiooni avaldamine ja kataloogiteenus

2.4.1 SK informatsiooni avaldamine

Vt CPS p.2.4.1.

Kehtiv tühistusnimekiri on kättesaadav kataloogiteenuse kaudu ja aadressil <http://www.sk.ee/crls/klass3/klass3.crl>.

2.4.2 Avaldamise sagedus

Vt CPS p.2.4.2.

Tühistusnimekirja uuendatakse regulaarselt 1 kord nädalas.

2.4.3 Juurdepääsureeglid

Vt CPS p.2.4.3.

2.4.4 Kataloogiteenus

Vt CPS p.2.4.4.

2.5 Audit

Vt CPS p.2.5.

Välisauditi tulemused avaldatakse SK koduleheküljel.

2.6 Konfidentsiaalsus

Vt CPS p.2.6.

2.7 Omandiõigused

AS Sertifitseerimiskeskus omab sertifitseerimisteenus osutamisel kasutatavale tehnilisele terviklahendusele ja dokumentatsioonile kõiki õigusi, sealhulgas omandi- ja varalisi autoriõigusi.

3 Kliendi identifitseerimine

3.1 Kliendi isikusamasuse kontroll

Kliendi ja tema poolt esitatud andmete kontrolli sätestab dokument „Asutuse digitaalse kinnituse sertifikaatide kasutamise tingimused“ [6].

Asutuse digitaalse kinnituse sertifikaadi taotluse menetlemise käigus kontrollitakse:

- Kliendi poolt esitatud andmeid;
- Kliendi isikusamasust ning tema volitusi sertifikaadi taotlemiseks ja/või tühistamiseks;

3.2 Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord

Klient esitab SK-le elektrooniliselt sertifikaadi taotluse, mis sisaldab taotleja avalikku võtit ning mis on signeeritud vastava salajase võtmega. Sertifitseerimisjärgu

signatuuri eduka kontrollimise korral saab SK eeldada, et vastav isiklik võti on taotleja valduses.

3.3 Eraldusnimi

Vt CPS p.3.3.

Kliendi eraldusnimi koostatakse vastavalt dokumendile "Asutuse digitaalse kinnituse sertifikaadi profiil" [2].

4 Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtajad

4.1 Sertifikaaditaotluse esitamine

Vt CPS p.4.1.

Sertifikaaditaotluse esitamine käib SK kodulehekülje kaudu. Klient täidab veebivormi oma kontaktandmetega ning lisab taotlusele PKCS#10 [7] vormingus signeeritud sertifikaaditaotluse. Andmete sisestamise järel väljastab veebisüsteem kliendikohase avaldusblanketi, mille Klient allkirjastab digitaalselt ja saadab koos taotluses viidatud signeerimispoliitikaga SK-sse kontaktandmetes toodud aadressile.

4.2 Sertifikaaditaotluse menetlemine

Sertifikaaditaotlus vaadatakse läbi peale kliendi poolt allkirjastatud avaldusblanketi laekumist SK-sse 5 tööpäeva jooksul.

4.2.1 Otsuse tegemine

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

- Kliendi organisatsioonilisest staatusest
- Kliendi poolt esitatud andmete õigsust ja täielikkust
- Asutuse signeerimispoliitika vastavust esitatud nõuetele.
Signeerimispoliitikale esitatud nõuded on toodud dokumendis "Nõuded asutuse sertifikaatide signeerimispoliitikale". [8]

4.2.2 Sertifikaadi väljastamine

Vt CPS p.4.2.2.

Väljastatud sertifikaat saadetakse Kliendile taotluses kontaktandmetes märgitud elektronposti aadressile.

Sertifikaadi väljastamise hetkel avaldatakse sertifikaat SK avalikus kataloogis.

4.2.3 Sertifikaatide üle arvestuse pidamise kord

Vt CPS p.4.2.3.

Kataloogile juurdepääsu ei piirata.

4.2.4 Sertifikaadi kontroll ja tõestamine

Sertifikaadi kehtivust saab huvitatud isik kontrollida SK avaliku kataloogi ja seal leiduva tühistusnimekirja abil. SK väljastab asutuse digitaalse kinnituse sertifikaadile kehtivuskinnitusteenuse poolt digitaalselt allkirjastatud kehtivustõendi.

4.2.5 Sertifikaadi uuendamine

STO saadab 4 nädalat enne sertifikaadi kehtivuse lõppu sertifikaadi taotluses toodud asutuse esindajale või taotluses märgitud administratiivsele ja tehnilisele kontaktisikule elektronposti teel vastavasisulise hoiatuse ning viite SK koduleheküljele, mis võimaldab taotleda uut sertifikaati. Kui 1 nädal enne sertifikaadi kehtivuse lõppu pole uut sertifikaati taotletud, siis saadab STO eeltoodud isikutele uue vastavasisulise hoiatuse.

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

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

4.3 Sertifikaadi kehtetuks tunnistamise ja peatamise taotlused

Asutuse digitaalse kinnituse sertifikaati peatada ei saa.

Asutuse digitaalse kinnituse sertifikaatide kehtetuks tunnistamiseks peab asutuse seaduslik esindaja või sertifikaaditaotluses näidatud volitatud isik esitama kirjaliku vastavasisulise avalduse SK-le.

4.4 Sertifikaatide peatamine

Asutuse digitaalse kinnituse sertifikaate peatada ei saa.

4.5 Sertifikaadi peatamise lõpetamine

Asutuse digitaalse kinnituse sertifikaate peatada ei saa.

4.6 Sertifikaadi kehtetuks tunnistamine

4.6.1 Sertifikaadi kehtetuks tunnistamise volitused

Vt CPS p.4.6.1.

Vastavalt ASKT-le [6] võib sertifikaadi kehtetuks tunnistada ka SK.

4.6.2 Sertifikaadi kehtetuks tunnistamise avalduse esitamine

Sertifikaadi kehtetuks tunnistamiseks esitab klient allkirjastatud avalduse, mis sisaldab:

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

Kehtetuks tunnistamise avalduse esitaja identifitseeritakse SK poolt.

4.6.3 Sertifikaadi kehtetuks tunnistamise menetlus

Vt CPS p.4.6.3.

4.6.4 Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus

Vt CPS p.4.6.4.

4.7 Protseduurid jälgitavuse tagamiseks

Vt CPS p.4.7.

4.8 Tegutsemine eriolukorras

Vt CPS p.4.8.

4.9 Sertifitseerimisteenuse osutaja töö lõpetamine

Vt CPS p.4.9.

5 Füüsilised ja organisatsioonilised turbemeetmed

5.1 Turbehaldus

Vt CPS p.5.1.

5.2 Füüsilised turbemeetmed

5.2.1 SK füüsiline pääsukontroll

Vt CPS p.5.2.1.

5.3 Nõuded tööprotseduuridele

Vt CPS p.5.3.

5.4 Personali turbenõuded

Vt CPS p.5.4.

6 Tehnilised turbenõuded

6.1 Võtmehaldus

6.1.1 SK kinnitusvõtmed

Vt CPS p.6.1.1.

6.1.2 Kliendi võtmed

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

6.2 Süsteemiturve

Vt CPS p.6.2.

6.3 Sertifitseerimisteenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus

Vt CPS p.6.3.

6.4 Sertifitseerimisteenuse osutamisel tekkinud andmete säilitamine ja kaitse

Vt CPS p.6.4.

7 Sertifikaatide ja tühistusnimekirjade (CRLide) tehnilised profiilid

7.1 Sertifikaatide profiil

Asutuse digitaalse kinnituse sertifikaat kehtib kuni **380 päeva** (1 aasta ja 15 päeva).

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

7.2 Tühistusnimekirjad (CRL)

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

Tühistusnimekirja täpne profiil on toodud dokumendis “Asutuse digitaalse kinnituse sertifikaadi profiil” [2].

8 Sertifitseerimispoliitika haldus

Sertifitseerimispoliitika sisulist tähendust mitte muutvate paranduste puhul nagu õigekirjavigade parandamine, tõlkimine ja kontaktandmete ajakohastamine, tuleb muudatused dokumenteerida käesoleva dokumendi Muudatused - sektsioonis ning suurendada dokumendi versiooninumbri murdarvulist osa.

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

9 Kasutatud terminoloogia

Vt CPS p.9.

10 Kasutatud lühendid

Vt CPS p.10.

Lühend	Definitsioon
ASKT	Asutuse digitaalse kinnituse sertifikaadi kasutamise tingimused
SK	AS Sertifitseerimiskeskus

11 Viidatud ja seonduvad dokumendid

Viidatud dokumendid:

- [1] AS-i Sertifitseerimiskeskus sertifitseerimis põhimõtted (CPS)
- [2] Asutuse digitaalse kinnituse sertifikaadi profiil
- [3] Eesti Vabariigi digitaalallkirja seadus, RT 1 2000, 26, 150.
- [4] RFC 2459 – Request For Comments 2459, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile; <http://www.ietf.org/rfc>
- [5] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
- [6] Asutuse digitaalse kinnituse sertifikaadi kasutamise tingimused. AS Sertifitseerimiskeskus.
- [7] PKCS#10 – Certification Request Syntax Standard.
<http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/>
- [8] Nõuded asutuse signeerimispoliitikale. AS Sertifitseerimiskeskus.

Seonduvad dokumendid:

- AS-i Sertifitseerimiskeskus infoturbepoliitika
- AS-i Sertifitseerimiskeskus käideldavuse strateegia ja poliitika
- AS-i Sertifitseerimiskeskus IT süsteemide taastamise poliitika

- Andmekogude seadus, RT 1 1997, 28, 423
- Isikut tõendavate dokumentide seadus, RT 1 1999,25,365
- Isikuandmekaitse põhimõtted
- Isikuandmete kaitse seadus RT 1 1996, 48, 944