AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted

Ametlik tõlge AS Sertifitseerimiskeskuse originaaldokumendile "AS Sertifitseerimiskeskus Trust Services Practice Statement"[1]
Versioon 2.0
Kehtiv alates 01.07.2016

Versioon ja muudatused		
Kuupäev	**Versioon**	**Muudatused**
01.07.2016	2.0	Tehti järgmised muudatused ja täiendused: - Punkt 6.1.1 juhatuse liige kinnitab võtmete loomise komisjoni oma käskkirjaga. Komisjoni peab kuuluma väline ja SK-st sõltumatu audiitor; - Punkt 6.2.1 HSM on FIPS režiimil; Punkt 6.2.1 SK kontrollib ja veendub, et HSM-i ei ole rikutud peale selle saamist ning paigaldamist. See dokumenteeritakse HSM elutsükli protokollis.
01.04.2016	1.9	Mustand SK PS-i versioonist 2.0, mis hakkab kehtima 01.07.2016. Ümber kujundatud vastavalt standardile RFC 3647. Mõned muudatused on tehtud selleks, et saavutada vastavust eIDAS määrusega.
01.10.2014	1.0	Esimene avalik versioon.

[1] Inglisekeelne originaaldokument on kättesaadav https://www.sk.ee/en/repository/sk-ps/. Vastuolude korral eestikeelse tõlke ja inglisekeelse originaaldokumentide vahel tuleb juhinduda inglise keelsest originaaldokumendist.

1. SISSEJUHATUS

AS Sertifitseerimiskeskus (edaspidi SK) asutati 26. märtsil 2001. Ettevõtte omanikud on AS Swedbank, AS SEB Pank ja Telia Eesti AS. SK peamisteks tegevusaladeks on usaldusteenuste ja nendega seotud tehniliste lahenduste osutamine Baltimaades. Need teenused tagavad nii riigiasutustes kui ka ettevõtetes igapäevase turvalise ja tõendatud elektroonilise kommunikatsiooni.

Lähtudes ETSI EN 319 400 seeria standarditest, on SK jaganud oma dokumentatsiooni kolmeks osaks:

- SK usaldusteenuste põhimõtted (SK PS) kirjeldavad kõikidele usaldusteenustele kehtivaid üldisi praktikaid;
- sertifitseerimise põhimõtted ja ajatempli teenuse osutaja põhimõtted kirjeldavad neid osi, mis kehtivad konkreetsele alam CA-le või ajatembeldusüksusele;
- tehnilised profiilid asuvad eraldi dokumentides.

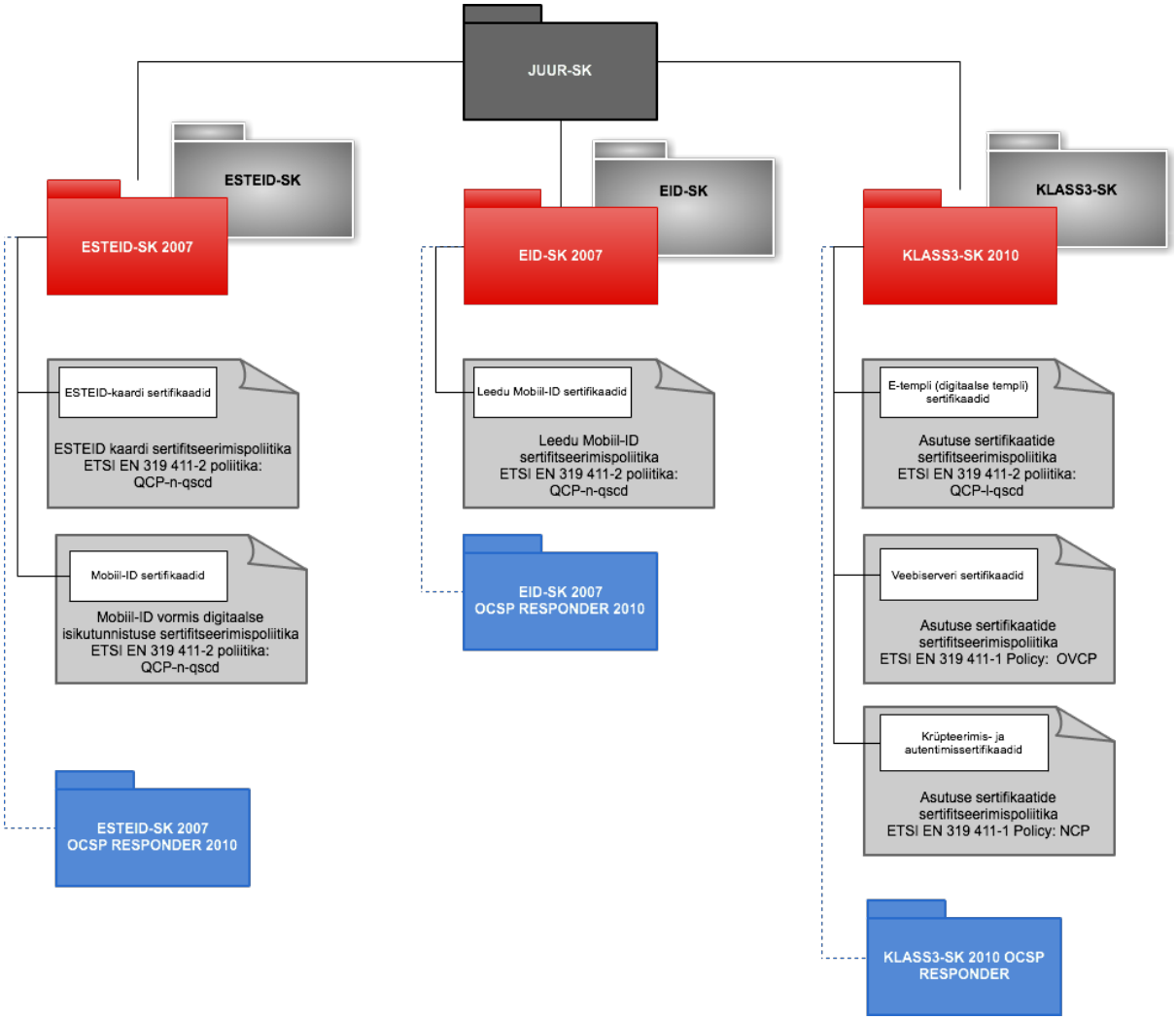
IETF RFC 3647 [4] kohaselt jaguneb käesolev dokument üheksaks osaks. RFC 3647 [4] poolt määratletud vormi säilitamiseks on nende lõikude pealkirjade juures, mis ei kehti, märge „ei kohaldata“. Lõigud, mis kirjeldavad ainult ühele teenusele spetsiifilisi tegevusi, sisaldavad viiteid ainult konkreetse teenuse põhimõtetele. Kui alalõigud jäetakse välja, kohaldub neile kõigile üks viide. Igas esmatasandi peatükis on viide ETSI EN 319 401 [2] vastavale peatükile.

1.1 Ülevaade

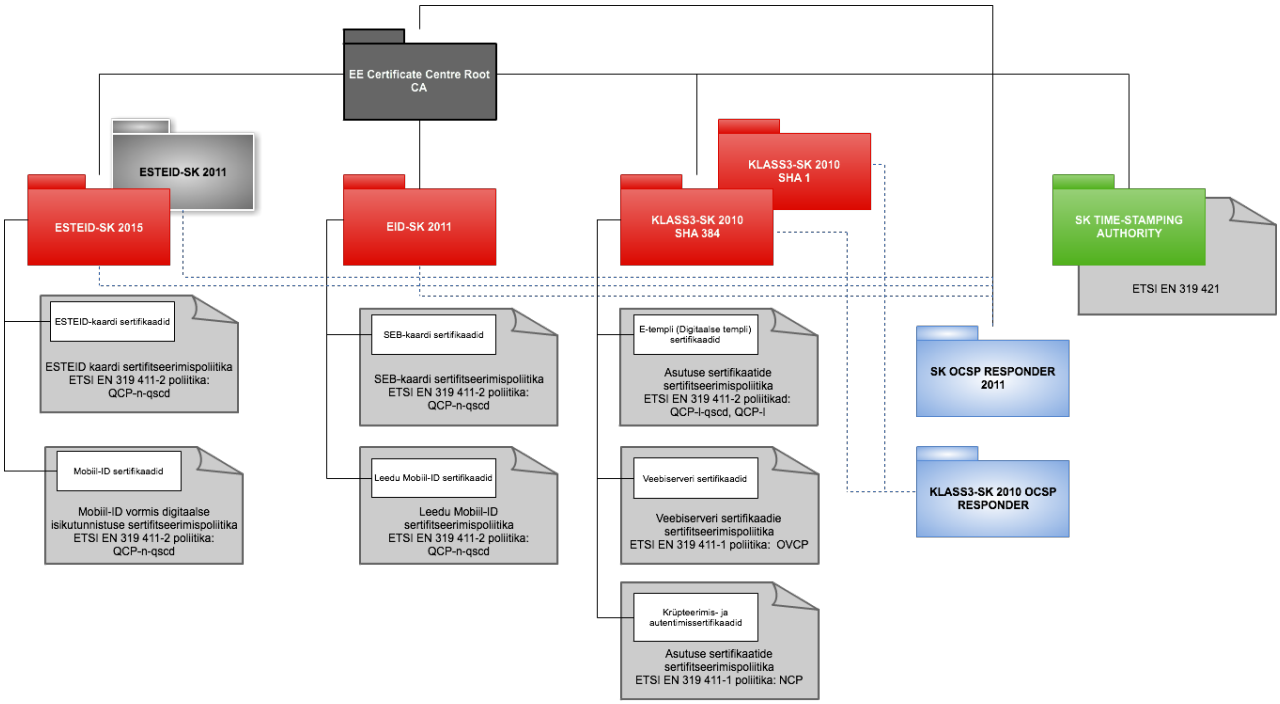
SK kasutab usaldusteenuste osutamiseks avaliku võtme infrastruktuuri. SK kasutab käesoleval ajal kahte sertifitseerimisahelat; juursertifitseerimisasutusteks on Juur-SK ja EE Certification Centre Root CA.

Nende seos alam CA-de ja sertifitseerimispoliitikatega on näidatud järgmistel joonistel:

1) Juur-SK, kehtiv 2001-2016



2) EE Certification Centre Root CA ahel, kehtiv 2010-2030



AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted (SK PS) esitavad SK kehtestatud elektrooniliste usaldusteenuste osutamise kriteeriumid, mis suurendavad elektrooniliste tehingute usaldusväärsust ja kindlust. SK PS kirjeldab AS Sertifitseerimiskeskuse (SK) tegevusi kvalifitseeritud usaldusteenuste osutamisel, mis on kooskõlas eIDAS määruse [1], Eestis kehtivate õigusaktide, ETSI EN 319 401 usaldusteenuste osutajatele kohaldatavate üldiste poliitikanõuete [2] ja teiste teenusel põhinevate standardnõuetega. Lisaks järgib SK CA/Browser Forumi sertifitseerimispoliitika põhinõudeid avalikult usaldatud sertifikaatide väljastamiseks ja haldamiseks [3].

SK PS kirjeldab tegevusi, mis on vajalikud SK juhtkonna poolt heaks kiidetud turbetaseme saavutamiseks. SK on omandanud ISO/IEC 27001:2013 sertifikaadi. Kohaldusmäärang sisaldab turbemeetmete täpsemat kirjeldust.

Juhul, kui SK PS-i ja teatud konkreetsete teenuste põhimõtete vahel ilmneb vastuolu, kehtivad nende konkreetsete teenuste põhimõtete sätted. Kui vasturääkivused ilmnevad ingliskeelse algdokumendi ja eesti keelde tõlgitud dokumendi vahel, võetakse aluseks ingliskeelne dokument.

1.2 Dokumendi nimi ja identifitseerimine

Käesoleva dokumendi nimi on „AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted“.

1.3 Avaliku infrastruktuuri pooled

1.3.1 Usaldusteenuse osutaja

SK on usaldusteenuse osutaja (TSP). SK ja TSP rollid on määratletud vastava teenuse poliitikas ja/või põhimõtetes.

SK kohustusi ja tagatisi on kirjeldatud käesoleva SK PS-i punktis 9.6.1.

1.3.2 Registreerimisasutused

Registreerimisasutus (RA) ja selle roll on määratletud vastava teenuse poliitikas ja/või põhimõtetes.

RA kohustusi ja tagatisi on kirjeldatud käesoleva SK PS-i punktis 9.6.2.

1.3.3 Kliendid

Klient on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

Kliendi kohustusi ja tagatisi on kirjeldatud käesoleva SK PS-i punktis 9.6.3.

1.3.4 Huvitatud isikud

Huvitatud isik on määratletud käesoleva SK PS-i punktis 1.6.1.

Huvitatud isikute kohustusi ja tagatisi on kirjeldatud käesoleva SK PS-i punktis 9.6.4.

1.3.5 Teised pooled

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

1.4 Sertifikaadi kasutamine

1.4.1. Sertifikaadi sobivad kasutusviisid

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

1.4.2 Sertifikaadi keelatud kasutusviisid

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

1.5 Poliitika haldamine

1.5.1 Dokumenti haldav organisatsioon

Käesolevat SK PS-i haldab SK.

AS Sertifitseerimiskeskus
Registrikood 10747013
Pärnu mnt 141, 11314 Tallinn
Tel +372 610 1880
Faks +372 610 1881
E-post: info@sk.ee
http://www.sk.ee

1.5.2 Kontaktisik

Kvaliteedijuht
E-post: info@sk.ee

1.5.3 SK PS-i sobivust poliitikaga määrav isik

Ei kohaldata.

1.5.4 SK PS-i heakskiitmise kord

Sertifitseerimispõhimõtete tähendust mittemuutvad muudatused, nt õigekirjavigade parandamine, tõlkimine ja kontaktandmete uuendamine, peavad olema dokumenteeritud käesoleva dokumendi osas „Versioonid ja muudatused", dokumendi versiooni numbri fraktsiooni osa tuleb täiendada.

Oluliste muudatuste korral on usaldusteenuse põhimõtete uus versioon eelmistest versioonidest selgelt eristatav. Uue versiooni puhul täiendatakse seerianumbrit ühe numbri võrra. Muudetud SK PS koos jõustumise kuupäevaga, mis ei saa olla varasem kui 30 päeva pärast dokumendi avaldamist, avaldatakse elektroonilisel kujul SK veebilehel.

SK-l on õigus enne SK PS-i avaldamist avaldada selle dokumendi mustand. Kliendil on võimalus seda kommenteerida 30 päeva jooksul alates mustandi avaldamisest. Muudetud SK PS avaldatakse elektroonilisel kujul SK veebilehel 30 päeva enne selle jõustumist.

SK PS-i kiidavad heaks SK tegevjuht ja teenusejuhid. SK tagab põhimõtete korrektse rakendamise, viies regulaarselt läbi sisekontrolli ja vastavushindamist.

Kõik muudatused tuleb esitada järelevalveasutusele.

1.6 Mõisted ja lühendid

1.6.1 Mõisted

Tühistusnimekiri	kehtetute (tühistatud, peatatud) sertifikaatide nimekiri.
Kvalifitseeritud e-allkiri (ehk kvalifitseeritud elektrooniline allkiri)	täiustatud elektrooniline allkiri, mis luuakse kvalifitseeritud elektroonilise allkirja andmise vahendiga ja mis põhineb elektrooniliste allkirjade kvalifitseeritud sertifikaadil; enne 01.07.2016 kasutati Eestis ja SK dokumentides kvalifitseeritud e-allkirja asemel mõistet „digitaalne allkiri“.
Kataloogiteenus	sertifikaadi avaldamise teenus
eIDAS määrus	Euroopa Parlamendi ja nõukogu 23. juuli 2014. a määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ.
e-allkiri (ehk elektrooniline allkiri)	elektroonilisel kujul esitatavad andmed, mis on lisatud või loogiliselt seostatud teiste elektrooniliste andmetega ja mida allkirja andja kasutab allkirjastamiseks.
Poliitika	eeskirjad, mis näitavad usaldusteenuse märgi rakendatavust mingis kindlas kogukonnas ja/või liiki rakendustes koos üldiste turbenõuetega.
Põhimõtted	põhimõtted, mida TSP rakendab usaldusteenuse osutamisel.
Registreerimisasutus	üksus, mis vastutab sertifikaadi kasutaja identifitseerimise ja autentimise eest. Lisaks sellele võtab RA vastu sertifikaatide taotlusi, kontrollib neid ja/või edastab need CA-le.
Huvitatud isik	usaldusteenuse märgi vastuvõtja, kes tegutseb sellele usaldusteenuse märgile toetudes. MÄRKUS: huvitatud isikute alla kuuluvad ka pooled, kes tõendavad digitaalset allkirja avaliku võtme sertifikaatide abil.
Isiklik võti	võti võtmepaarist, mida võtmepaari omanik hoiab salajas ja mida kasutatakse digitaalsete allkirjade loomiseks ja/või selliste elektrooniliste dokumentide või failide dekrüpteerimiseks, mida krüpteeriti vastava avaliku võtmega.
Avalik võti	võtmepaar, mida vastava isikliku võtme omanik võib avalikustada ja mida huvitatud isik kasutab selleks, et tõendada omaniku vastava isikliku võtmega digitaalseid allkirju ja/või krüpteerida teateid selliselt, et neid saaks dekrüpteerida vaid omaniku vastava isikliku võtmega.
Juur CA	kõrgema taseme sertifitseerimisasutus, kelle sertifikaati jaotavad rakendustarkvara tarnijad ja mis väljastab SK CA alamsertifikaate.

Tundlik teave	teave, mida on võimalik kasutada teenuste simulatsiooniks või replikatsiooniks või ka teenuste isikliku võtme hävitamiseks või avaldamiseks. Siia alla kuuluvad ka isikuandmed.
SK CA	SK sertifitseerimisasutus, mille sertifikaadi on allkirjastanud juur CA või teine alam CA.
Klient:	usaldusteenuste osutajaga lepingu allkirjastanud üksus, kes on seadusest tulenevalt kohustatud täitma kliendi kohustusi.
Kliendi sertifikaat	kasutaja avalik võti koos muu teabega, mis on tänu sertifitseerimisasutuse poolt väljastatud isikliku võtmega šifreerimisele võltsimiskindel.
Järelevalveasutus	asutus, mille on määranud liikmesriik selleks, et teostada liikmesriigi territooriumil eIDAS määruse [1] alusel järelevalvet usaldusteenuste ja usaldusteenuse osutajate üle.
Ajatembeldusüksus	riist- ja tarkvara komplekt, mida hallatakse tervikuna ja millel on korraga aktiivne ainult üks ajatempli signeerimisvõti.
Usaldusteenus	kirjeldatud eIDAS määruses [1] elektroonilise teenusena, mida osutatakse tasu eest ja mis hõlmab: - elektrooniliste allkirjade, elektrooniliste templite või elektrooniliste ajatemplite loomist, tõendamist ja kehtivuskontrolli, elektrooniliselt registreeritud vastuvõtuteenuseid ja nende teenustega seotud sertifikaate; - sertifikaatide loomist, tõendamist ja kehtivuskontrolli veebilehtede autentimiseks; - elektrooniliste allkirjade, templite või nende teenustega seotud sertifikaatide säilitamist.
Usaldusteenuse osutaja:	üksus, mis osutab vähemalt ühte elektroonilist usaldusteenust.
Usaldusteenuse tunnistus:	füüsiline või binaarne (loogiline) objekt, mis on loodud või väljastatud usaldusteenuse kasutamisel (nt sertifikaat).
Kvalifitseeritud usaldusteenus	usaldusteenuste osutaja, kes osutab vähemalt ühte kvalifitseeritud usaldusteenust ja kellele järelevalveasutus on andnud kvalifitseeritud staatuse.

1.6.2 Lühendid

CA	Sertifitseerimisasutus
CRL	Sertifikaatide tühistusnimekiri
DMZ	Demilitariseeritud tsoon
ETSI	Euroopa Telekommunikatsiooni Standardite Instituut
HSM	Riistvara turvamoodulid
RA	Registreerimisasutus

SK	AS Sertifitseerimiskeskus
SK PS	AS Sertifitseerimiskeskuse usaldusteenuste põhimõtted
TSA	Ajatempli asutus
TSP	Usaldusteenuse osutaja
TSU	Ajatembeldusüksus
UTC	Koordineeritud universaalaeg

2. AVALDAMINE JA REPOSITOORIUMI VASTUTUS

2.1 Repositooriumid

SK tagab oma repositooriumi kättesaadavuse 24 tundi päevas ja 7 päeva nädalas; teenuse kättesaadavus on aastas minimaalselt 99,44% ja kavandatud seisakuaeg ei ületa iga-aastaselt 0,28%.

2.2 Teabe avaldamine

SK avaldab oma avaliku teabe repositooriumis järgmist teavet:

- sertifitseerimishierarhia ülevaade (https://sk.ee/repositoorium/);
- usaldusteenuste põhimõtted (https://sk.ee/repositoorium/sk-ps/)
- sertifitseerimispõhimõtted (https://sk.ee/repositoorium/CPS/);
- ajatempliteenuse osutaja põhimõtted ja ajatembelduspõhimõtted (https://sk.ee/repositoorium/ajatembelduse-pohimotted/);
- auditi tulemused (https://sk.ee/repositoorium/audit/);
- kindlustus (https://sk.ee/repositoorium/kindlustus/);
- sertifitseerimispoliitikad (https://sk.ee/repositoorium/CP/);
- sertifikaadid, sh juursertifikaadid ja CA sertifikaadid, mille alusel sertifikaadid klientidele väljastatakse (https://sk.ee/repositoorium/sk-sertifikaadid/);
- sertifikaatide profiilid (https://sk.ee/repositoorium/profiil/);
- sertifikaatide kasutustingimused (https://sk.ee/repositoorium/kasutustingimused/);
- tühistusnimekiri (https://sk.ee/repositoorium/CRL/);
- LDAP kataloogiteenus (https://sk.ee/repositoorium/ldap/);
- kliendiandmete kaitse põhimõtted (https://sk.ee/repositoorium/andmekaitse/).

2.2.1 Avaldamine ja teavitamispoliitika

Käesolev SK PS avaldatakse SK avaliku teabe repositooriumis.

SK PS koos jõustumiskuupäevadega avaldatakse hiljemalt 30 päeva enne kehtima hakkamist.

2.2.2 Põhimõtetes avaldamata jäänud kirjed

Vaadake käesoleva SK PS-i punkti 9.3.1.

2.3 Avaldamise aeg ja sagedus

Vaadake SK PS-i punkti 2.2.1.

Teave sertifikaatide staatuse kohta on avaldatud vastavalt käesoleva SK PS-i punktidele 4.9.7 ja 4.9.9.

2.3.1 Kataloogiteenus

SK avaldab teavet sertifikaatide ja nende kehtivuse kohta LDAP kataloogiteenuse kaudu.

LDAP kataloogiteenuse eesmärgiks on pakkuda klientidele, huvitatud isikutele ja teistele isikutele juurdepääsu sertifikaatide registrile, et nad saaksid teha sertifikaatide ja nende kehtivuse kohta päringuid.

Kataloogiteenus vastab järgmistele nõuetele:

- LDAP sisaldab kehtivaid (st tühistamata ja aegumata) sertifikaate;
- LDAP kataloogis ei või olla tundlikku ja isiklikku teavet isikuandmete kaitse seaduse tähenduses;
- LDAP kataloogile pääseb ligi andmete avaliku sidevõrgu (ldap.sk.ee) kaudu 24 tundi ööpäevas.

2.4 Repositooriumide juurdepääsu kontrollimine

SK repositooriumis avaldatud teave on avalik ja seda ei loeta konfidentsiaalseks teabeks.

SK on võtnud kasutusele turbemeetmed, et tõkestada repositooriumis loata juurdepääs kannete lisamiseks, kustutamiseks või muutmiseks. SK repositooriumis avaldamine on piiratud SK volitatud töötajatega.

3. IDENTIFITSEERIMINE JA AUTENTIMINE

3.1 Nimetamine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

3.2 Identiteedi esialgne kinnitamine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

3.3 Identifitseerimine ja autentimine uue võtme taotlemiseks

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

3.4 Identifitseerimine ja autentimine tühistamise taotlemiseks

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4. SERTIFIKAADI ELUTSÜKLI TEGEVUSNÕUDED

4.1 Sertifikaadi taotlemine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.2 Sertifikaadi taotluse töötlemine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.3 Sertifikaadi väljastamine

4.3.1 CA tegevused sertifikaadi väljastamise ajal

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.3.2 Kliendi teavitamine sertifikaadi väljastamisest CA poolt

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.4 Sertifikaadi vastuvõtmine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.5 Võtmepaar ja sertifikaadi kasutamine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.6 Sertifikaadi uuendamine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.7. Sertifikaadi uus võti

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.8 Sertifikaadi muutmine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.9 Sertifikaadi tühistamine ja peatamine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.10 Sertifikaadi staatuse kontrollimise teenused

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.11 Tellimuse lõppemine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

4.12 Deponeerimine ja taastamine

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

5. VAHENDID, HALDAMINE JA TEGEVUSKONTROLL

SK juhindub turbe haldamisel üldtunnustatud standarditest, nt ISO/IEC 27001 [5], ning teistest õigusaktide ja seadustega nõutud standarditest.

SK turbehalduspoliitika dokumendid sisaldavad teenuse osutamiseks kasutatavate SK vahendite, süsteemide ja infovarade turbekontrolle ning tööprotseduure. SK teostab riskide hindamist ja ülevaatust regulaarselt selleks, et hinnata ettevõtte riske ning määrata kindlaks vajalikud turbenõuded ja tööprotseduurid.
SK juhtkond kehtestab turbepoliitika, mis on järjepideva ja tervikliku infoturbe ning juhtkonna kohustumuse aluseks.

Kõikide SK teenuste infoturbega seotud poliitikad ja põhimõtted kiidab heaks SK tegevjuht. SK juhtkond teavitab infoturbe poliitikatest ja protseduuridest töötajaid ja vastavaid ettevõtteväliseid pooli, keda need mõjutavad. Samuti määrab SK juhtkond SK lähenemise usaldusteenuste infoturbe eesmärkide saavutamiseks, sh sisekontrolli kontrollprotseduurid.

SK on omandanud ISO/IEC 27001: 2013 sertifikaadi.

5.1 Füüsiline kontroll

SK kasutab renditud serveriruumides füüsiliselt eraldatud ruumi, mis on kavandatud spetsiaalselt andmekeskuse tööks. Ruumide omaniku kohustuseks on pakkuda seadmete jaoks vajalikku keskkonda. SK ja ruumide omaniku vahel on sõlmitud teenustaseme leping, millega tagatakse häireteta turvaline töö.

5.1.1 Asukoht ja konstruktsioon

SK teenuseid viiakse läbi füüsiliselt turvalises keskkonnas, mis hoiab ära ning avastab kas varjatud või varjamata tundliku teabe ja süsteemi volitamata kasutamise, sellele juurdepääsu või selle avaldamise.

Kaitse on vastavuses tuvastatud riskidega. SK tagab, et kontrollitakse füüsilist juurdepääsu kriitilistele teenustele ja et füüsilised riskid tema varadele on minimaalsed.

5.1.2 Füüsiline juurdepääs

SK andmekeskused on kaitstud vähemalt kolmeosalise füüsilise turbega, kusjuures enne kõrgemale tasemele jõudmist nõutakse juurdepääsu madalamale tasemele. Juurdepääs kõrgeimale tasemele nõuab kahe usaldusülesandeid täitva isiku osavõttu.

SK töötajad võivad saada juurdepääsu SK usaldusteenustega seotud vahenditele ainult kinnitatud nimekirja alusel. Kõigi SK andmetöötluskeskusse sisenemiste kohta peetakse logi.

Ruumide omanikul ei ole SK serveritele iseseisvat juurdepääsu.

Sellesse füüsiliselt turvatud alasse sisenevad isikud ei jää sinna volitatud isiku järelevalveta.

5.1.3 Elekter ja kliimaseade

SK turbeseadmed on varustatud:

- elektrisüsteemidega, et tagada pidev ja katkematu juurdepääs elektrienergiale;
- soojus-, ventilatsiooni- ja õhukonditsioneerisüsteemidega temperatuuri ning suhtelise õhuniiskuse kontrollimiseks.

5.1.4 Kokkupuude veega

SK on võtnud kasutusele mõistlikud ettevaatusabinõud, et infosüsteemide veega kokkupuutumise võimalus oleks minimaalne.

5.1.5 Tulekahju ärahoidmine

SK on võtnud kasutusele mõistlikud ettevaatusabinõud, et vältida ja kustutada tulekahjusid või vältida muid kahjulikke kokkupuuteid leekide või suitsuga. SK tulekahju ennetus- ja kaitsemeetmed on vastavuses kohalike tuleohutusnõuetega.

5.1.6 Andmekandja

Teisaldatavaid andmekandjaid, seadmeid ja tarkvara tohib SK ruumidest välja viia kehtestatud korra alusel. Tundliku teabega andmekandjaid võib hoida ainult spetsiaalses tulekindlas andmekandjate hoidmiseks määratud seifis.

5.1.7 Jäätmekäitlus

Kui tundlikku teavet sisaldavaid andmekandjaid enam ei kasutata, kõrvaldatakse need ohutult. Tundlikku teavet sisaldavad paberdokumendid ja materjalid purustatakse enne hävitamist. Tundliku teabe kogumiseks või edastamiseks kasutatud andmekandjad muudetakse enne hävitamist loetamatuks. Tundlikku teavet sisaldav kasutusest eemaldatud andmekandja (eemaldatav andmekandja, kõvakettad jne) puhastatakse andmelekke vältimiseks andmetest, kui see kõrvaldatakse kasutusest või kui seda taaskasutatakse muul otstarbel.

5.1.8 Asukohavälised varukoopiad

SK teeb kriitilistest süsteemiandmetest, kontrolljälgede andmetest ja muust tundlikust teabest järjepidevalt varukoopiaid. SK-l on kättesaadavuse nõuete tagamiseks kaksikandmekeskused, mille andmebaasid on reaalajas sünkroniseeritud. Lisaks tehakse järjepidevalt varukoopiaid. Kriitilise teabe varukoopiaid (nt võtmetest ja konfiguratsioonidest) hoitakse väljaspool SK-d turvalises kohas.

5.2 Menetluslikud kontrollimeetmed

5.2.1 Usaldusülesanded

SK töötajatel on ametijuhendid, milles on määratletud järgmiste turbekriitiliste usaldusülesannete täitmine:

- turvajuht: vastutab turbetegevuste haldamise ja elluviimise eest;
- süsteemiadministraatorid: vastutavad SK infosüsteemide paigaldamise, konfigureerimise ja haldamise, sh varukoopiate tegemise ja taastamise eest;
- süsteemiaudiitor või -hindaja: vastutab perioodiliste ülevaatuste eest; selleks on tal olemas juurdepääs dokumendiarhiivi ja infosüsteemi kontrolljälgede jälgimiseks.

SK on jaganud süsteemiadministraatorid sise-eeskirjade alusel kaheks, st A- ja B-tüüpi süsteemiadministraatoriks. Jaotamine toimub inimeste kaupa tegevjuhi otsuse alusel. Vaadake üksikasju punktis 5.2.2.

SK tagab, et töötajad on saavutanud usaldatavuse ja ametlik heakskiit antakse enne, kui vastavale töötajale:

- on väljastatud juurdepääsuks vajalikud vahendid ja võimaldatud juurdepääs vajalikele vahenditele või
- on väljastatud elektroonilised tunnused juurdepääsuks ja kindlate funktsioonide täitmiseks SK-s või muus IT-süsteemis.

Turbetegevusi teostavad SK usaldusülesandeid täitvad töötajad, kuid neid võib sooritada ka dokumentides kindlaks määratud ülesannetes ja vastutusega mittespetsialistist töötaja (järelevalve all).

RA töötaja rolli loetakse samuti turbekriitiliseks, sest ta vastutab sertifikaadi kasutaja identifitseerimise ja autentimise eest ning ta võib vastutada ka registreerimise, sertifikaadi peatamise, peatatuse lõpetamise ja tühistamise protseduuride eest.

5.2.2 Tööülesannete täitmiseks vajalik töötajate arv

SK on kehtestanud ranged kontrolliprotseduurid, haldab ja viib neid täide selleks, et tagada ülesannete lahusus tulenevalt vastutusest ja et tundlike ülesannete täitmist nõutaks mitmetelt usaldusisikutelt.

Järgmised tegevused nõuavad vähemalt kahte usaldusisikust süsteemiadministraatorit, kellest üks on A-tüübi ja teine B-tüübi esindaja:

- sertifitseerimisvõtmete genereerimine;
- sertifitseerimisvõtmetest varukoopiate tegemine;
- sertifitseerimisvõtmete taastamine;
- turvatsoonis olevate HSM-i ja CA tuumsüsteemide haldamine;
- andmekeskuste füüsiline külastamine.

5.2.3 Rollide identifitseerimine ja autentimine

Kõiki usaldusülesandeid täidavad isikud, kelle on SK juhtkond nende täitmiseks määranud ja kes on nende ülesannete täitmisega nõustunud.

SK on võtnud kasutusele juurdepääsukontrolli süsteemi, mis tuvastab asutused ja registreerib kõik SK infosüsteemi kasutajad usaldusväärsel viisil.

Kõnealusele süsteemile juurdepääsu vajavatele kindla ülesandega töötajatele luuakse kasutajakontod. Kõik kasutajad peavad sisse logima oma isikliku kontoga ning administratiivsed käsud on kasutatavad ainult selgesõnalise loa ja täitmise kontrolliga. Muu kasutuse vältimiseks kasutatakse failisüsteemi õigusi ja teisi operatsioonisüsteemi turbemudelis kättesaadavaid funktsioone.

Ülesannete muutumisel lukustatakse kasutajakontod võimalikult kiiresti. Juurdepääsueeskirju auditeeritakse igal aastal.

5.2.4 Ülesannete eraldatust nõudvad rollid

Turvajuhi, süsteemiaudiitori ja süsteemiadministraatorite usaldusülesanded on üksteisest täielikult eraldatud ja nendel kohtadel töötavad erinevad isikud. Üks isik ei saa olla korraga nii A- kui ka B-tüüpi süsteemiadministraator.

5.3 Personali juhtimine

5.3.1 Kvalifikatsioon, kogemus ja turbenõuded

SK töötajad on saanud piisava väljaõppe ning neil on enne tegeliku töö alustamist töölepingus ja ametijuhendis kindlaks määratud tööülesannete täitmiseks vajalik kogemus.

SK töötajate allkirjastatud töölepingutes on määratletud järgmised kohustused:

- hoida saladuses töö käigus teatavaks saanud konfidentsiaalset teavet;
- vältida ärihuvide omamist sellises ettevõttes, mis võiks mõjutada töötajate otsuseid teenuse osutamisel;
- ei tohi olla eelnevalt karistatud tahtlikult toime pandud kuriteo eest.

Ühelgi usaldusülesandeid täitval töötajal ja RA töötajal ei tohi olla huvisid, mis võiksid mõjutada nende erapooletust seoses SK tegevusega.

5.3.2 Taustakontrolli protseduurid

Enne kui usaldusülesandeid täitvad töötajad saavad tegelikku tööd alustada, tuvastatakse kõigi usaldusülesandeid täita soovivate töötajate isikud nende isikliku (füüsilise) kohaloleku kaudu. Samuti

kontrollitakse ametlikult tunnustatud isikut tõendavaid dokumente, nt isikutunnistust või passi. Edasine sobivus selgub taustakontrolli käigus.

Taustakontroll viiakse läbi vastavalt asjakohastele seadustele, määrustele ja eetikanormidele. Kontroll on vastavuses ettevõtte nõuete, ligipääsetava teabe klassifikaatori ja tajutava riskiga. Kontrollitakse kõiki potentsiaalseid töötajaid ja lepingupartnereid, kes osutavad otseselt usaldusteenuseid ning kellel on ligipääs tooteandmetele.

Karistusregistri taustakontrolli teostatakse vähemalt iga 3 aasta tagant.

5.3.3 Koolitusnõuded

SK töötajad on saanud piisava väljaõppe ning neil on enne tegeliku töö alustamist töölepingus ja ametijuhendis kindlaks määratud tööülesannete täitmiseks vajalik kogemus.

SK tagab, et kõik seoses SK tegevusega juhtimisülesandeid täitvad töötajad saavad põhjaliku väljaõppe järgnevas:

- SK-s kehtivad turbepõhimõtted ja eeskirjad;
- SK sise-eeskirjad ja protsessid;
- ülesanded, mille täitmist neilt oodatakse.

5.3.4 Perioodiline ümberõpe ja nõuded

Käesoleva SK PS-i punkti 5.3.3 nõudeid hoitakse ajakohasena, et kohaneda muutustega SK süsteemis. Täiendkoolitusi viiakse läbi vastavalt vajadusele ja SK kontrollib kõikide töötajate turvateadlikkust vähemalt kord aastas.

5.3.5 Töökohtade rotatsiooni sagedus ja järjestus

Rotatsiooni ei kasutata.

5.3.6 Sanktsioonid volitamata tegevuste puhul

SK kehtestab, tagab ja viib täide tööhõivepoliitikat (osana SK turbepoliitikast) personali distsiplineerimiseks lubamatu teguviisi korral. Distsiplinaarkaristused hõlmavad meetmeid, mis võivad viia lepingu lõpetamiseni ning vastavad lubamatu käitumise sagedusele ja tõsidusele.

5.3.7 Nõuded sõltumatule töövõtjale

SK ei kasuta usaldusülesannete täitmiseks sõltumatuid töövõtjaid.

5.3.8 Töötajatele antud dokumentatsioon

SK annab oma töötajatele (sh usaldusülesandeid täitvatele isikutele ja RA töötajatele) vajaliku väljaõppe ning muu dokumentatsiooni, mis on vajalik nende tööülesannete asjatundlikuks ja rahuldavaks täitmiseks.

5.4 Kontrolljälgedega seotud protseduurid

5.4.1 Salvestatud sündmuste liigid

SK tagab teenuste osutamisega seotud asjakohase teabe salvestamise tõendite olemasoluks kohtumenetluse korral. Teabe hulka kuuluvad arhiiviandmed, mis on vajalikud usaldusteenuste tunnistuste kehtivuse tõendamiseks, ja usaldusteenuste osutamise kontrolljälg.

SK infosüsteemid jätava kontrolljälje:

- kõikide sündmuste kohta, mis on seotud SK hallatavate võtmete ja sertifikaatide elutsükliga, sh CA ja TSU võtmed ja sertifikaadid ning kliendi võtmepaarid;
- kõikide oluliste turbeprobleemide kohta, sh turbepoliitika sätete muutused, süsteemi käivitamine ja sulgemine, süsteemi kokkuvarisemised ja riistvaratõrked, muutused tulemüüri konfiguratsioonis ja eeskirjades ning ligipääsukatsed avaliku võtme infrastruktuuri süsteemile, eeliskasutaja õigustega süsteemikasutajate tegevused;
- kõikide sündmuste kohta, mis on seotud kella sünkroniseerimisega koordineeritud universaalajale (UTC), sünkroniseerimisest tulenevate kahjude avastamiseks;
- kõikide registreerimisega seotud sündmuste kohta, sh sertifikaadi võtme taastamise ja uuendamise taotlused;
- kogu registreerimisteabe kohta, sh isiku tõendamine:
    - dokument/dokumendid, mille taotleja esitas registreerimiseks;
    - unikaalsed isiku tuvastamise andmed ja -numbrid või isikut tõendavate dokumentide kombinatsioon;
    - taotluste ja isikut tõendavate dokumentide koopiate hoiukoht;
    - taotlust vastu võtva üksuse identiteet;
    - isikut tõendavate dokumentide kontrollimiseks kasutatav meetod;
    - vastuvõtva TSP-i/esitava registreerimisasutuse nimi;
- kõikide sertifikaadi peatamise ja peatatuse lõpetamisega seotud taotluste ja aruannete kohta;
- kõikide sertifikaadi tühistamisega seotud taotluste ja aruannete kohta, aga ka neist tulenevatele tegevuste kohta.

5.4.2 Logi ja kontrolljälgede töötlemise sagedus

Süsteemiadministraatorid vastutavad süsteemilogide regulaarse ülevaatuse ja võimalike juhtumitest teavitamise eest.

Tootejuhid vastutavad kesksest logisüsteemist oma rakenduste logide ülevaatamise ning toote rikete avastamise ja sündmuste korrelatsiooni jaoks automatiseeritud otsingu loomise eest.

Oluliste sündmuse liikide identifitseerimine ja valdkondade väljavõtmine kuulub sõltuvalt tööülesannetest süsteemiadministraatorite, tootejuhtide ja koostajate vastutusalasse.

Teenuste ärijuhid vastutavad nende aruannete vähemalt iganädalase ülevaatamise eest, mille on logisüsteem loonud nende teenuste kohta.

5.4.3 Kontrolljälgede säilitamine

Kontrolljälgi säilitati kuni 31.12.2015 kohapeal vähemalt 7 aastat. Alates 01.01.2016 säilitatakse kontrolljälgi kohapeal vähemalt 10 aastat.

Füüsilisi või digitaalseid arhiivimaterjale sertifitkaadi taotluste, registreerimisteabe ja peatamistaotluste, peatatuse lõpetamise ja tühistamise taotluste kohta säilitatakse vähemalt 10 aastat pärast vastava sertifikaadi kehtivust.

SK lõpetamise korral kontrolljäljed ja arhiivimaterjalid säilitatakse ning neile pääseb ligi ülalnimetatud säilitamistähtajani vastavalt käesoleva SK PS-i punktile 5.8.

5.4.4 Kontrolljälgede kaitse

SK kasutab standarditele vastavaid teabekaitselahendusi, mis tagavad isiklike võtmete, aktiveerimiskoodide, juurdepääsukoodide (nt PIN-koodi) või muu kontrolljäljes sisalduva turbekriitilise teabe mittesalvestamise.

Kõiki logisid hoitakse kohapeal ja need saadetakse kesksesse logiserverisse. Kesksed logiserverid rakendavad logipoliitikat – säilitamist ja arhiveerimist.

Rakenduse logidel on krüptograafiline kaitse.

Asutuse sisene arendusprotsess määratleb logiprotsessi ja logide jaoks turbenõuded, sh logide kaitse. Mitte-elektroonilist audititeavet kaitstakse volitamata vaatamise, muutmise ja hävitamise eest korralduslike vahendite abil.

Ligipääs kontrolljälgedele on piiratud rolli/privileegi põhiselt.

5.4.5 Kontrolljälgede varundamise protseduurid

SK teostab regulaarselt kriitiliste süsteemiandmete, kontrolljälgede ja muu tundliku teabe varundamist. Kontrolljälgede varundamine on osa üldisest varundamise süsteemist. SK on määratlenud varundamise strateegia ja poliitikad oma sisestes kordades.

5.4.6 Kontrolljälgede kogumissüsteem (sisemine *versus* väline)

Automatiseeritud kontrolljälgede andmeid genereeritakse ja salvestatakse rakenduse, võrgu ja operatsioonisüsteemi tasandil. Mitte-elektrooniliselt genereeritud kontrolljälgede andmeid salvestavad

SK usaldusülesandeid täitvad isikud.

5.4.7 Sündmuse põhjustanud subjekti teavitamine

Kui teenuste osutamisega seotud andmeid vajatakse teenuste nõuetekohase toimimise tõendusmaterjalina ja kohtumenetluses, tehakse need kättesaadavaks õigusorganitele ja/või isikutele, kelle juurdepääsuõigus tuleneb seadusest.

5.4.8 Haavatavuse hindamine

Sündmusi logitakse osaliselt selleks, et jälgida süsteemi haavatavusi. Teostatakse turbe haavatavuste hindamist, nende ülevaatamist ja muutmist. Need hinnangud põhinevad reaalajas automatiseeritud logiandmetel ja hinnanguid antakse igapäevaselt, igakuiselt ja igal aastal.

5.5 Andmete arhiveerimine

5.5.1 Arhiveeritud andmete liigid

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

5.5.2 Arhiivis säilitamise aeg

Arhiivis säilitamise aega on kirjeldatud käesoleva SK PS-i punktis 5.4.3.

5.5.3 Arhiivi kaitse

Arhiiv asub eraldi ruumis ja on kaitstud juurdepääsukontrolli süsteemidega.

Andmekandjal sisalduvaid arhiiviandmeid ja vajalikke rakendusi arhiiviandmete töötlemiseks säilitatakse, et tagada nõutavaks ajavahemikuks juurdepääs arhiiviandmetele.

5.5.4 Arhiivi varundamine

Arhiivi ei varundata.

5.5.5 Dokumentide ajatembelduse nõuded

Andmebaasi kanded sisaldavad täpset teavet aja ja kuupäeva kohta. Ajatemplid ei põhine krüptograafial.

5.5.6 Arhiivi kogumissüsteem (sisemine või väline)

SK kasutab arhiivi sisemist kogumissüsteemi.

RA-d võivad kasutada arhiivi välist kogumissüsteemi füüsiliste arhiividokumentide jaoks.

5.5.7 Arhiiviandmete saamine ja kontrollimine

Juurdepääsuluba arhiividele on ainult usaldusülesandeid täitvatel volitatud töötajatel.

Kui teenuste osutamisega seotud andmeid vajatakse teenuste nõuetekohase toimimise tõendusmaterjalina ja kohtumenetluses, tehakse need kättesaadavaks õigusorganitele ja/või isikutele, kelle juurdepääsuõigus tuleneb seadusest.

Teabe terviklikkust kinnitatakse taastetestide käigus. Selleks kasutatakse sisseehitatud terviklikkuse kontrolliga arhiivisüsteeme.

5.6 Võtme üleminek

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

5.7 Kompromiteerumise ja avariijärgne taaste

5.7.1 Intsidentide ja kompromiteerumise käsitlemise protseduurid

SK rakendab talitluspidevuse juhtimise raamistikku, mis hõlmab riskihindamise, intsidentide käsitlemise (sh intsidentidele ja avariidele reageerimise), taastamise ja taastamisharjutuste protseduure.

SK viib läbi iga-aastast usaldusteenuste riskihindamist, et vältida võimalikku ohtu SK tegevuse kättesaadavusele ja muuta usaldusteenuste üle kontrolli kaotamise risk minimaalseks. Kriisisituatsiooniks peetavate olukordade nimekiri määratakse kindlaks riskihindamisega. Riskihindamise tulemus hõlmab taasteplaani nõudeid ja taaste teststsenaariume. Taasteplaanid ja teststsenaariumid hõlmavad vähemalt järgmisi ohte:

- SK CA ja SK TSA jaoks – teenuste osutamisel kasutatud isiklik võti on kompromiteerunud või on tõsine kahtlus selle kohta;
- SK TSA jaoks – ajatempliteenuse kellaaja sünkroniseerimise ebaõnnestumine.

Infoturbe intsidentide, kriisi ja kriitiliste haavatavuste käsitlemise protseduurid on dokumenteeritud SK siseses kriisi lahendamise korras. Selle korra eesmärkideks on viivitamatu reageering ja kättesaadavuse taastamine ning SK teenuste pidev kaitse.

Taasteplaane kontrollitakse igal aastal.

Kriisisituatsiooni tekkimisel teavitab SK kõiki kliente ja huvitatud isikuid viivitamatult (või vähemalt 24 tunni jooksul pärast kriisikomitee otsust) kriisist ja pakutavast lahendusest avalike infokanalite kaudu.

SK teavitab järelevalveasutust ja vajaduse korral ka teisi vastavaid asutusi, nagu näiteks riiklik CERT või andmekaitse inspektsioon, ilma põhjendamatu viivituseta, kuid igal juhul 24 tunni jooksul pärast seda, kui ta sai teada turbenõuete rikkumisest või terviklikkuse kaost ning kui neil on oluline mõju osutatavatele usaldusteenustele või hallatavatele isikuandmetele.

5.7.2 Arvutisüsteemide, tarkvara ja/või andmete rikkumine

Arvutisüsteemide, tarkvara ja andmete rikkumise korral rakendadakse SK sisest kriisi lahendamise korda.

5.7.3 Üksuse protseduurid isikliku võtme ohtu sattumisel

SK isikliku võtme ohtu sattumise korral rakendatakse SK sisest kriisi lahendamise korda.

5.7.4 Talitluspidevus pärast õnnetusjuhtumit

Selleks, et ettevõte jätkaks oma tegevust ka pärast õnnetusjuhtumit, organiseerib SK perioodiliselt kriisiohjamise koolitusi. SK sisene kriisi lahendamise kord määratleb selle, kuidas toimub kriisiohjamine ja kommunikatsioon kriisisituatsioonis.

Kriisisituatsiooni ja/või teenuste katkestuse järgsete süsteemide ja teenuste taastamise prioriteetide kohta on olemas sisemised kokkuleped. SK säilitab vajalikke varukoopiaid ja arhiiviandmeid, et andmeid oleks võimalik pärast hädaolukorda taastada. Kõige kriitilisema teabe (nt võtmete ja konfiguratsioonide) varukoopiaid hoitakse turvalises kohas asukohast eemal.

SK-l on teenuste tagamiseks kaksikandmekeskused. SK kontor ja andmekeskused on teineteisest sõltumatud. Kui kriisisituatsioon puudutab andmekeskuste tööd, pääseb juhenditele, lähtekoodidele ja muudele vajalikele materjalidele ligi SK kontorist. Kui kriisisituatsioon tekib SK kontoris, jätkavad andmekeskused ikkagi tööd.

5.8 CA lõpetamine

Usaldusteenuse osutamine lõpetatakse:

- SK juhtkonna otsusega;
- teenuse osutamise üle järelevalvet teostava asutuse otsusega;
- kohtuotsusega;
- SK likvideerimise või tegevuse lõpetamise korral.

SK tagab klientidele ja huvitatud isikutele SK teenuste lõpetamisest tulenevate võimalike häirete minimeerimise ning eelkõige teabe jätkuva säilitamise, mis on vajalik usaldusteenuse tunnistuste õigsuse kontrollimiseks.

Enne kui SK usaldusteenuse osutamise lõpetab, viiakse läbi järgmised protseduurid:

- SK teavitab oma tegevuse lõpetamisest kõiki kliente ja muid üksusi, kellega SK-l on lepingud või muus vormis kehtestatud suhted. Samuti teavitatakse teisi huvitatud isikuid;
- SK teeb kõik endast oleneva, et leppida kokku teise usaldusteenuse osutajaga oma olemasolevatele klientidele teenuste osutamise üleandmises;
- SK hävitab CA ja TSU isiklikud võtmed, sh varukoopiad või kasutusest eemaldatud võtmed, sellisel viisil, et neid ei oleks võimalik taastada;
- SK taaslähtestab või hävitab kõik nimetatud teenusega seotud riistvaraseadmed sõltuvalt konkreetsetest turvanõuetest;
- SK lõpetab lepingud kõigi SK heaks tegutsenud alltöövõtjatega, kes täitsid usaldusteenuse tunnistuste väljastamisega seotud ülesandeid;
- SK säilitab usaldusteenuse osutamisega seotud dokumendid ja vajaliku teabe usaldusteenuse tunnistuste kontrollimiseks, juhul kui SK ei lõpeta teenuse osutamist vastavalt punktidele 5.4 ja 5.5. Juhul kui SK lõpetab usaldusteenuse osutamise, annab SK teenuse osutamisega seotud eelnimetatud dokumendid ja vajaliku teabe usaldusteenuse tunnistuste kontrollimiseks vastavalt kehtestatud korrale üle järelevalveasutusele.

Kompromiteerumisel peab SK lisaks:

- näitama, et CA või TSU võtit kasutades väljastatud usaldusteenuse tunnistus ja kehtivusalane teave ei pruugi enam kehtida;
- tühistama sellise CA ja TSU sertifikaadi, mida ei väljastatud SK-le, kui SK-d teavitatakse teise CA või TSA ohtu sattumisest.

Algoritmi kompromiteerumisel peab SK:

- määrama mõjutatud usaldusteenuse tunnistustele tühistamisaja.

Teade SK teenuse lõpetamisest avaldatakse massiteabevahendites.

SK ei võta vastutust sellise lõpetamise tõttu teenuse kasutaja kantud kahjude eest eeldusel, et SK on teavitanud lõpetamisest avalike infokanalite kaudu vähemalt üks kuu ette.

SK on sõlminud kulude katmiseks ja miinimumnõuete täitmiseks lepingu kindlustusasutusega juhuks, kui TSP läheb pankrotti või kui ilmnevad mingid muud põhjused, miks SK ei ole võimeline ise kulusid kandma.

Nõudeid kohaldatakse ka RA lõpetamise korral. SK võtab üle usaldusteenuse osutamisega seonduva dokumentatsiooni ja teabe ning esitab tegevusega seotud tõendid vastava teenuse poliitikas ja/või põhimõtetes määratud ajaperioodi kohta.

6. TEHNILINE TURBEKONTROLL

6.1 Võtmepaari loomine ja installeerimine

SK kasutab usaldusteenuste osutamisel krüptograafilisi võtmeid ning järgib tegevusala parimaid võtmehalduse, võtme pikkuse ja algoritmide tavasid.

6.1.1 Võtmepaari loomine

SK usaldusteenuste signeerimisvõtmed luuakse vastavalt SK sisemistele kordadele: SK juurvõtme loomise protseduurile ja alam sertifitseerimisasutustele võtmete loomise protseduurile. SK CA võtmete loomiseks kõikide CA-de puhul, kas juur või alam CA puhul, kinnitab SK tegevjuht komisjoni koosseisu sisese korraga. Komisjoni peab kuuluma väline audiitor, kes on SK-st sõltumatu. SK usaldusteenuse võtmete loomist jälgib komisjon, kes koostab pärast võtmete loomist vastava akti, kus on kirjas loodud võtmepaari avalik võti ja selle räsi. Usaldusteenuse võtmepaari loomine ja avaliku võtme hoidmine toimub HSM-is, mida kasutatakse selliste võtmete puhul, mis vastavad minimaalselt turvastandardi FIPS PUB 140-2 3. tasandi nõuetele. HSM kaitseb võtit väliste ohtude eest ja toimib füüsiliselt turvalises keskkonnas.

SK-l on dokumenteeritud protseduur SK CA võtmepaari genereerimise läbiviimiseks kõikide CA-de jaoks olenemata sellest, kas tegemist on juur või alam CA-ga, sh CA-d, mis väljastavad lõppkasutaja sertifikaate. SK esitab aruande, mis tõestab, et tegevus viidi läbi vastavalt kehtestatud protseduurile ja selle ajal tagati võtmepaari terviklikkus ja konfidentsiaalsus. Aruande allkirjastavad komisjoni liikmed, sh välisaudiitor. Võtmetalituse protseduurid dokumenteeritakse SK võtmeprotseduuride sise-eeskirjades.

Kliendi isikliku võtme loomine on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.1.2 Isikliku võtme üleandmine kliendile

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.1.3 Avaliku võtme üleandmine sertifikaadi väljastajale

Täpsustatud vastava teenuse poliitikas või põhimõtetes.

6.1.4 CA avaliku võtme üleandmine huvitatud isikutele

Kõik SK usaldusteenuste avalikud võtmed väljastatakse SK CA välja antud X.509 sertifikaatide kujul. Esmane väljastamismehhanism SK usaldusteenuste sertifikaatidele toimub SK repositooriumi kaudu veebilehel https://www.sk.ee/repositoorium/. SK võtab endale kohustuse SK usaldusteenuste sertifikaatide esitamiseks Eesti usaldusnimekirja. SK teeb endast kõik oleneva, et osaleda veebisirvijate juursertifikaatide levitamise programmides.

6.1.5 Võtmete suurused

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.1.6 Avaliku võtme parameetrite genereerimine ja kvaliteedikontroll

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.1.7 Võtme kasutuseesmärgid (X.509 v3 võtme kasutusala kohta)

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.2 Isikliku võtme kaitse ja krüptograafilise mooduli tehniline kontroll

6.2.1 Krüptograafilise mooduli standardid ja kontroll

SK poolt kasutatav HSM on sertifitseeritud vastavalt FIPS 140-2 3. tasandi standardile ja töötab FIPS režiimil.

SK kontrollib ja veendub, et HSM-i ei ole rikutud peale selle saamist ja paigaldamist. See on dokumenteeritud HSM elutsükli protokollis.

Krüptograafilised mooduli standardid ja kontroll, mida on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes, on mõeldud krüptograafilistele seadmetele, mis kannavad kliendi isiklikku võtit.

6.2.2 Isikliku võtme (n m-ist) kontrollimine mitme inimese poolt

Juurdepääs SK CA võtmetele jaguneb kaheks osaks, mida tagavad erinevad usaldusülesandeid täitvad isikud. SK signeerimisvõtme aktiveerimine nõuab vastavalt käesoleva PS-i punktile 5.2.2 vähemalt kahe volitatud isiku kohalolekut.

6.2.3 Isikliku võtme deponeerimine

SK CA isiklikke võtmeid hoitakse turvalistes krüptograafilistes seadmetes, mis on tõendatud FIPS 140-2 3. tasandi standardiga. Isikliku võtme aktiveerimine ja kasutamine nõuab mitme inimese kontrolli, nagu selgitatud käesoleva SK PS-i punktis 6.2.2.

Kliendi isiklike võtmete deponeerimist on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.2.4 Isikliku võtme varundamine

Kättesaadavuse nõuetele vastamiseks tehakse SK CA isiklikest võtmetest varukoopiad, kopeerides need turvaliselt täiendavasse HSM-i. Ligipääs võtmele jaotatakse kaheks osaks, mille tagavad erinevad isikud. SK sertifitseerimisvõtme hoidmiseks kasutatakse turvaümbrikku ja selle ümbriku avamist saab kehtestada. SK sertifitseerimisvõtmeid saab kasutada ainult siis, kui need on aktiveeritud. SK sertifitseerimisvõtme aktiveerimine nõuab vähemalt kahe volitatud isiku kohalolekut, nagu on selgitatud käesoleva SK PS-i punktis 6.2.2.

Kliendi isikliku võtme varundamine on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.2.5 Isikliku võtme arhiveerimine

SK ei arhiveeri SK CA isiklikke võtmeid, kui need on aegunud. Kõik SK CA isiklike võtmete koopiad hävitatakse, kui need on aegunud või tühistatud; seega on nende edasine kasutamine või tuletamine võimatu.

Kliendi isikliku võtme arhiveerimine on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.2.6 Isikliku võtme edastamine krüptograafilisse moodulisse ja sealt välja

Kõik SK CA võtmed tuleb genereerida krüptograafilises moodulis ja selle abil. SK genereerib CA võtmepaare HSM-is, kus neid võtmeid hiljem ka kasutatakse.

6.2.7 Isikliku võtme hoidmine krüptograafilises moodulis

SK CA isiklikke võtmeid, mida hoitakse HSM-is, säilitatakse krüpteeritud kujul.

Kliendi isikliku võtme hoidmine on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.2.8 Isikliku võtme aktiveerimine

SK CA isiklikke võtmeid aktiveeritakse vastavalt krüptograafilise mooduli tootja tehnilistele nõuetele. SK sertifitseerimisvõtme aktiveerimine nõuab vähemalt kahe volitatud isiku kohalolekut, nagu on selgitatud käesoleva SK PS-i punktis 6.2.2.

Kliendi isikliku võtme aktiveerimise viis on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.2.9 Isikliku võtme deaktiveerimine

SK CA isiklikud võtmed deaktiveeritakse, kui püütakse avada võtmete hoidmiseks kasutatud turvamoodulit, kui muudetakse konfiguratsiooni, kui toiteallikas ühendatakse lahti või kantakse üle või muude turvalisust ohtu seadvate asjaolude korral.

Kliendi isikliku võtme deaktiveerimise viis on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.2.10 Isikliku võtme hävitamine

SK CA isiklike võtmete ja sisekontrolli mehhanismide hävitamine sõltub konkreetsele turvalisele krüptograafilisele moodulile kättesaadavatest võimalustest.

6.2.11 Krüptograafilise mooduli hindamine

Vaadake käesoleva SK PS-i punkti 6.2.1.

6.3 Võtmepaari haldamise muud aspektid

6.3.1 Avaliku võtme arhiveerimine

Kõiki väljastatud sertifikaate (sh kõiki aegunud ja tühistatud sertifikaate) säilitatakse ja arhiveeritakse osana SK rutiinsest varundamisprotseduurist. Säilitamisperiood on tähtajatu.

6.3.2 Sertifikaadi ja võtmepaari kasutusaeg

Sertifikaadi kasutusaeg lõpeb pärast tühistamist. Võtmepaaride kasutusaeg on sertifikaatide kasutusajaga sama, välja arvatud see, et neid võib kasutada allkirja ehtsuse tõendamiseks ka edaspidi.

Lisaks peatab SK uute sertifikaatide väljastamise sobival ajal enne CA sertifikaadi aegumist nii, et ükski kliendi sertifikaat ei aegu pärast CA sertifikaadi aegumist.

Kui algoritm või vastav võtmepikkus ei paku sertifikaadi kehtivusajal piisavat turvalisust, tühistatakse asjasse puutuv sertifikaat ja alustatakse uue sertifikaadi taotlemist. Krüptograafiliste algoritmide ja parameetrite kohaldamist kontrollib järjepidevalt SK juhtkond.

Kliendi sertifikaatide puhul määratakse kehtivusaeg vastava teenuse poliitikas ja/või põhimõtetes.

6.4 Aktiveerimisandmed

6.4.1 Aktiveerimisandmete genereerimine ja installeerimine

SK CA isikliku võtme aktiveerimisandmed genereeritakse ja installeeritakse vastavalt HSM-i kasutusjuhendile.

Kliendi isikliku võtme PIN-koodide genereerimine ja installeerimine on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.4.2 Aktiveerimisandmete kaitse

HSM-i hoitakse turvalises kohas ja sellele pääsevad ligi ainult usaldusülesandeid täitvad volitatud isikud.

Kliendi isikliku võtme PIN-koodide kaitse on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.4.3 Aktiveerimisandmete muud aspektid

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

6.5 Arvuti turbekontroll

6.5.1 Arvuti tehnilised turbenõuded

SK tagab usaldusteenuse süsteemi komponentide turvalise ja korrektse töötamise aktsepteeritava tõrkeriskiga.

SK sertifitseerimisteenuse süsteemi komponente hallatakse vastavalt muudatuste haldamise korrale. See kord hõlmab süsteemi testimist isoleeritud testkeskkonnas ja nõuet, et muutuse peab heaks kiitma turvajuht. Kinnitus dokumenteeritakse edasiseks kasutamiseks.

Kõiki SK kriitilisi tarkvarakomponente paigaldatakse ja uuendatakse ainult usaldusväärsetest allikatest. Sertifitseerimisteenuse komponentide terviklikkuse kaitsmiseks viiruste, pahavara või volitamata tarkvara eest on olemas siseprotseduurid.

Kõik andmekandjad, mis sisaldavad tootekeskkonna tarkvara ja andmeid, kontrolljälgi, arhiivi või varukoopia teavet, säilitatakse SK ruumides asjakohase füüsilise ja loogilise juurdepääsukontrolliga, mis on piiratud volitatud töötajatele juurdepääsuks ja kaitseks juhuslike kahjude (nt vee, tule ja elektromagnetvälja) eest. Kui tundlikku teavet sisaldavaid andmekandjaid enam ei kasutata, kõrvaldatakse need turvaliselt. Kõiki eemaldatavaid andmekandjaid kasutatakse ainult kasutaja jaoks ette nähtud perioodil (kas aja või kasutuskordade järgi).

SK-l ei ole määratletud suutvushalduse protsessi. SK teenuste ja IT-süsteemide tööd kontrollivad teenuse ärijuhid ja vajalikud muudatused tehakse vastavalt sisemisele muudatuste halduse korrale.

Intsidendile reageerimise ja haavatavuse halduse protseduurid on dokumenteeritud sisemises korras. Jälgimissüsteem avastab ja hoiatab ebanormaalsetest süsteemi tegevustest, mis viitavad võimalikule turvarikkumisele, sh sissetungile võrku.

Tundlikku teavet sisaldavad paberdokumendid ja materjalid purustatakse enne hävitamist. Tundliku teabe kogumiseks või edastamiseks kasutatud andmekandjad muudetakse enne hävitamist loetamatuks.

SK turbetegevused hõlmavad töökorda ja -kohustusi, turbesüsteemide planeerimist ja kasutuselevõtmist, kaitset pahavara eest, varukoopiaid, võrguhaldust, kontrolljälgede aktiivset jälgimist,

sündmuste analüüsi ja järelkontrolli, andmekandjate käitlemist ja turvalisust, andme- ja tarkvaravahetust.

SK personal tuvastatakse enne teenustega seotud kriitiliste rakenduste kasutamist.

Kõnealusele süsteemile juurdepääsu vajavatele kindla ülesandega töötajatele luuakse kasutajakontod. Kõik kasutajad peavad sisse logima oma isikliku kontoga ning administratiivsed käsud on kasutatavad ainult selgesõnalise loa ja täitmise kontrolliga. Muu kasutuse vältimiseks kasutatakse failisüsteemi õigusi ja teisi operatsioonisüsteemi turbemudelis kättesaadavaid funktsioone. Ülesannete muutumisel lukustatakse kasutajakontod võimalikult kiiresti. Juurdepääsureeglite täitmist auditeeritakse igal aastal.

6.5.2 Arvuti turvalisuse hindamine

SK kasutab standardseid arvutisüsteeme.

6.6 Elutsükli tehniline kontroll

6.6.1 Süsteemiarenduse kontroll

SK viib süsteemi arendamise projekti kavandamisel ja nõuete kirjeldamise etapis läbi turbenõuete analüüsi; või analüüs viiakse SK nimel läbi tagamaks infotehnoloogia süsteemide turvalisus.

Tarkvara kiidab heaks turvajuht ja see peab pärinema usaldusväärsest allikast. Tarkvara uusi versioone katsetatakse vastava teenuse testkeskkonnas ja nende kasutuselevõtt teostatakse kooskõlas dokumenteeritud muudatuste haldamise korraga.

6.6.2 Turbe juhtimise kontroll

SK infosüsteemis, sh kõikides tööjaamades, rakendatakse meetmeid nii tarkvara ja konfiguratsioonide terviklikkuse tagamiseks kui ka tarkvarapettuse tuvastamiseks ning selle leviku piiramiseks. Infosüsteemis kasutatakse ainult sellist tarkvara, mida kasutatakse otseselt ülesannete täitmiseks.

6.6.3 Elutsükli turbekontroll

SK infoturbepoliitikad ja varad vaadatakse üle planeeritud ajavahemike järel või siis, kui ilmnevad märkimisväärsed muudatused; ülevaatamise põhjus on tagada nende jätkuv sobivus, vastavus ja tõhusus.

SK süsteemide konfiguratsioone kontrollitakse regulaarselt, et tuvastada SK turbepoliitikatega vastuolus olevaid muutusi. Sertifikaate väljastavad süsteemid, turbe tugisüsteemid ning abi- ja sisetugisüsteemide konfiguratsioonid vaadatakse üle vähemalt kord nädalas. Kehtestatud turbetaset mõjutavad muudatused kiidab heaks turvajuht.

SK-l on kehtestanud protseduurid, et tagada turvapaikade paigaldamine sertifitseerimissüsteemile mõistliku aja jooksul nende kättesaadavaks muutumisest, kuid mitte hiljem kui kuus kuud pärast turvapaiga kättesaadavaks tegemisest. Põhjus turvapaikade mittekasutamise kohta dokumenteeritakse.

SK registereerib infovarad ja liigitab kõik infovarad turbeklassidesse vastavalt regulaarsete turbeanalüüside tulemustele, mis on kooskõlas riskihindamisega. Kõigi oluliste infoturbevaradele on määratud vastutav isik. Kõik infoturbega seotud SK poliitikad ja varad vaadatakse ettevõttesiseselt üle planeeritud ajavahemike järel või siis, kui ilmnevad märkimisväärsed muudatused; ülevaatamise põhjus on tagada nende jätkuv sobivus, vastavus ja tõhusus.

6.7 Võrgu turvalisuse kontroll

SK võrk on jaotatud turbenõuete kohaselt tsoonidesse. Tsoonidevaheline kommunikatsioon on piiratud. Tulemüürist lubatakse läbi ainult SK teenuste jaoks vajalikud protokollid.

Abisüsteemid asuvad DMZ-is, mida kaitsevad tulemüür ja teisaldatavad veebiserverid. Tegelikud turbekriitilised teenused ja vastavad HSM-id töötavad turvatsoonis, mis on eraldatud teise tulemüüriga ja millel ei ole otsest internetiühendust.

Juursertifikaate väljastav sertifitseerimiskeskus asub kõrges turvatsoonis ja on kõikidest teistest võrkudest eraldatud. SK süsteeme konfigureeritakse ainult nende kontode, rakenduste, teenuste, protokollide ja portidega, mida kasutatakse usaldusteenuse osutamisel.

SK tagab juurdepääsu turvatsooni ja kõrgesse turvatsooni ainult usaldusülesandeid täitvatele töötajatele.

SK sisevõrgu kaableid ja aktiivseadmeid koos nende konfiguratsiooniga kaitstakse füüsiliste ja korralduslike meetmetega.

SK haldab andmekeskusi eraldi asukohtades, et vältida ülekoormust. Nende vaheline kommunikatsioon on tagatud krüptograafiliselt.

Kõiki andmekeskusi peetakse DMZ-i ja turvatsooni kaudu ühises siseturbevõrgus. SK sisevõrgust väljapoole edastatav tundlik teave krüpteeritakse.

SK sisevõrgu ja välisühenduste turvalisust jälgitakse pidevalt, vältimaks juurdepääsu protokollidele ja teenustele, mida ei ole vaja usaldusteenuste toimimiseks.

SK viib läbi enda tuvastatud avalike ja isiklike IP-aadresside osas nõrkusetesti üks kord kvartalis.

SK teeb igal aastal läbistustesti sertifitseerimissüsteemidele nende juurutamisel ja pärast selliseid infrastruktuuri või rakenduste uuendusi või muudatusi, mida SK peab oluliseks.

SK andmed tõendavad, et nõrkusotsingu ja läbistustesti viis läbi isik või üksus, kellel olid usaldusväärse aruande esitamiseks vajalikud oskused, vahendid, eetikakoodeks ja sõltumatus.

6.8 Ajatemplid

SK osutab kvalifitseeritud usaldusteenusena ajatembeldusteenuseid, mis on täpsustatud AS Sertifitseerimiskeskuse ajatempliteenuse osutaja põhimõtetes [6].

SK ei kasuta ajatempleid seoses sertifitseerimisteenusega. Andmebaasi sissekanded sisaldavad täpset aega ja teavet kuupäeva kohta. Teave aja kohta ei põhine krüptograafial. Maksimaalselt lubatud aja varieeruvus kõikides sertifitseerimissüsteemi osades on 1 sekund. Selle tagab kella sisemine viiteteenus ja selle kohaselt on kõikide sertifitseerimissüsteemi osade kellaajad sünkroniseeritud. Kell kasutab peamise ajaallikana GPS-i (globaalset positsioneerimissüsteemi), mis määrab SK süsteemis täpse aja.

7. SERTIFIKAADI, CRL-i JA OCSP PROFIILID

7.1 Sertifikaadi profiil

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

7.2 CRL-i profiil

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

7.3 OCSP profiil

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

8. VASTAVUSAUDIT JA MUUD HINDAMISED

8.1 Hindamise sagedus ja asjaolud

Infosüsteemi, poliitikate ja põhimõtete, seadmete, töötajate ja varade vastavust hindab vastavushindamisasutus vastavalt eIDAS määruses [1], asjakohastele õigusaktidele ja standarditele või siis, kui usaldusteenuse tegevustes tehakse oluline muudatus.

SK siseaudiitor viib siseauditi läbi kaks korda aastas.

8.2 Hindaja isik/kvalifikatsioon

Vastavushindamisasutus on akrediteeritud kooskõlas määrusega EÜ nr 765/2008 kui kvalifitseeritud usaldusteenuste osutaja ja tema osutatavate kvalifitseeritud usaldusteenuste vastavushindamise pädev läbiviija.

8.3 Hindaja seos hinnatava üksusega

Vastavushindamisasutuse audiitor on SK-st ja SK hinnatavatest süsteemidest sõltumatu.

Siseaudiitor ei või auditeerida seda valdkonda, mille eest ta ise vastutab.

8.4 Hinnatavad valdkonnad

Vastavushindamine hõlmab infosüsteemi, poliitikate ja põhimõtete, seadmete, töötajate ja varade vastavust eIDAS määruse [1], asjakohaste õigusaktide ja standarditega. Vastavushindamisasutus auditeerib neid SK infosüsteemi osi, mida kasutatakse usaldusteenuste osutamiseks.

Siseauditi raames auditeeritakse järgmiseid valdkondi:

- teenuse kvaliteet;
- teenuse turvalisus;
- tegevuse ja protseduuride turvalisus;
- kliendiandmete kaitse ja turbepoliitika, tööprotseduuride, lepinguliste kohustuste ning SK PS-i, vastavate teenuspõhiste poliitikate ja põhimõtete täitmine.

Vastavushindamisasutus ja siseaudiitor auditeerivad ka osa alltöövõtjate turbesüsteemist, poliitikatest ja põhimõtetest, vahenditest, töötajatest ja varadest, mis on seotud SK usaldusteenuste osutamisega (nt kaasa arvatud RA-d).

8.5 Puuduste tagajärjel kohaldatavad tegevused

Juhul, kui hindamise tulemus näitab puudusi, nõuab järelevalveasutus SK-lt nõuete täitmist takistavate puuduste kõrvaldamist järelevalveasutuse määratud aja jooksul (vajaduse korral). SK võtab kasutusele meetmed, et säilitada vastavus nõuetele ja täita kõiki puudustega seotud nõudeid õigeaegselt. Puudusi kõrvaldava tegevusplaani rakendamise eest vastutab SK juhtkond. SK hindab puuduste olulisust ja seab asjakohased tegevused tähtsuse järjekorda nii, et need täidetaks järelevalveasutuse määratud aja või mõistliku aja jooksul.

Kui ilmneb, et isikuandmete kaitse eeskirju on rikutud, teavitab järelevalveasutus vastavusauditi tulemustest andmekaitse inspektsiooni.

8.6 Tulemustest teavitamine

Auditi järeldused või usaldusteenuse sertifikaat, mis põhinevad eIDAS määruse, asjakohaste õigusaktide ja standardite alusel läbi viidud vastavushindamise auditi tulemustel, on avaldatud SK veebilehel https://www.sk.ee/repositoorium/.

Lisaks esitab SK saadud vastavushindamise aruande järelevalveasutusele kolme tööpäeva jooksul alates selle saamisest. SK esitab auditi järeldused või usaldusteenuse sertifikaadi SK-ga seotud brauseri juurprogrammide haldajatele ja teistele huvitatud isikutele.

9. MUUD TEGEVUS- JA ÕIGUSALASED KÜSIMUSED

9.1 Tasud

9.1.1 Sertifikaadi väljastamise ja uuendamise tasud

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

9.1.2 Sertifikaadi juurdepääsu tasud

SK avalik kataloogiteenus koos kehtivate ja aktiveeritud sertifikaatidega on kättesaadav LDAP kaudu veebilehel ldap.sk.ee.

9.1.3 Tühistamise ja staatuse kontrolli info juurdepääsu tasud

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

9.1.4 Muude teenuste tasud

Teenuste tasud on täpsustatud SK hinnakirjas või kliendi või huvitatud isiku lepingus.

9.1.5 Tagastamispoliitika

SK tegeleb tagastussoovidega ükshaaval.

9.2 Rahaline vastutus

9.2.1 Kindlustuskaitse

Vastavalt asjakohastele õigusaktidele avaldab SK kohustusliku kindluspoliitika tingimused oma veebilehel https://www.sk.ee/repositoorium/kindlustus/.

9.2.2 Muud varad

SK võib asjakohastest lepingutest sõltuvalt anda lisagarantiisid.

9.2.3 Kindlustus- ja tagatiskaitse lõppüksustele

Vaadake käesoleva SK PS-i punkti 9.2.1.

9.3 Tegevusalase teabe konfidentsiaalsus

9.3.1 Konfidentsiaalse teabe ulatus

Kogu teenuste osutamisel teatavaks saanud ja avaldamisele mittekuuluv teave (nt SK tegevuse ja usaldusteenuste osutamisega seotud teave) on konfidentsiaalne. Kliendil on õigus saada SK-lt teavet enda kohta vastavalt kehtivatele õigusaktidele.

9.3.2 Konfidentsiaalse teabe alla mittekuuluv teave

Igasugune teave, mida ei loeta konfidentsiaalseks teabeks või mis ei ole mõeldud asutusesiseseks kasutamiseks, on avalik teave.
SK-s avalikuks teabeks peetav teave on loetletud käesoleva SK PS-i punktis 2.2.

Lisaks loetakse avalikuks teabeks ka SK teenuste kohta käivaid mitteisikustatud statistilisi andmeid. SK võib oma teenuste kohta käivaid statistilisi andmeid avaldada.

9.3.3 Konfidentsiaalse teabe kaitsmiskohustus

SK hoiab konfidentsiaalset ja asutusesiseseks kasutamiseks mõeldud teavet ohtu sattumisest ja hoidub selle avalikustamisest kolmandatele pooltele, rakendades selleks erinevaid turvameetmeid.

Konfidentsiaalse teabe avalikustamine või edastamine kolmandatele isikutele on lubatud ainult teabe õigusliku valdaja kirjalikul loal, kohtuotsuse alusel või muudel seadusest tulenevatel juhtudel.

9.4 Isikuandmete privaatsus

9.4.1 Isikuandmete kaitse põhimõtted

SK isikuandmete kaitse põhimõtteid on kirjeldatud kliendiandmete kaitse põhimõtetes. Need põhimõtted on avaldatud SK veebilehel https://www.sk.ee/ettevottest/andmekaitse.

Järgides eelnimetatud põhimõtteid, tagab SK vastavuse nii isikuandmete kaitse seaduse [7] kui ka sellega, et konfidentsiaalset teavet ei avalikustata ja kliendi teavet hoitakse asjakohasel turvatasemel.

9.4.2 SK poolt töödeldud isikuandmed

SK poolt töödeldud isikuandmete ulatust kirjeldatakse kliendiandmete kaitse põhimõtetes [8].

9.4.3 Isikliku teabe kaitsmiskohustus

SK tagab isikuandmete kaitse, rakendades selleks käesoleva SK PS-i peatükis 5 kirjeldatud turvameetmeid.

9.4.4 Teavitus ja nõusolek erateabe kasutamiseks

Täpseid tingimusi, mille alusel annab klient SK-le oma nõusoleku kasutada isikuandmeid, on kirjeldatud kliendiandmete kaitse põhimõtetes [8].

9.4.5 Kohtu- või haldusmenetlusest tulenev avalikustamine

Asjaolusid, mille alusel võib SK kliendi isikuandmeid kolmandatele pooltele avalikustada, on kirjeldatud kliendiandmete kaitse põhimõtetes [8].

9.4.6 Teised teabe avalikustamise asjaolud

Asjaolusid, mille alusel võib SK kliendi isikuandmeid kolmandatele pooltele avalikustada, on kirjeldatud kliendiandmete kaitse põhimõtetes [8].

9.5 Intellektuaalomandi õigused

Käesoleva SK PS-i intellektuaalomandi õigused kuuluvad SK-le.

9.6 Esindamine ja tagatised

9.6.1 Usaldusteenuste osutaja esindamised ja tagatised

SK on TSP, klientide ja huvitatud isikute vaheliste vastastikuste lepingute ja kohustuste üheks pooleks. Käesolev SK PS ja teenuse põhimõtted on nende lepingute lahutamatuteks osadeks.

SK kohustub:

- osutama oma teenuseid vastavalt käesolevas SK PS-is määratud nõuetele ja protseduuridele ning teenuse poliitikatele ja põhimõtetele;
- olema vastavuses eIDAS määruse [1] ja käesolevas SK PS-is määratud õigusaktidega ning teenuse poliitikate ja põhimõtetega;
- avaldama SK PS-i, teenuse poliitikad ja põhimõtted ning tegema need kättesaadavaks üldkasutatavas andmesidevõrgus;
- avaldama ja täitma klientidele lubatud tingimusi ning tegema need kättesaadavaks ja ligipääsetavaks üldkasutatavas andmesidevõrgus;
- hoidma konfidentsiaalsena teavet, mis saab talle teatavaks teenuse osutamise käigus ja mis ei kuulu avalikustamisele;
- pidama arvestust väljastatud usaldusteenuse tunnistuste üle ja jälgima nende kehtivust ning tagama võimaluse kontrollida sertifikaatide kehtivust;
- teavitama järelevalveasutust usaldusteenuste osutamiseks kasutatava avaliku võtme muudatustest;
- teavitama järelevalveasutust ja vajadusel teisi vastavaid asutusi, nagu näiteks CERT või andmekaitse inspektsioon, osutatavale usaldusteenusele või säilitatud isikuandmetele olulist mõju avaldavast turbe rikkumisest või terviklikkuse kadudest ja seda ilma põhjendamatu viivituseta, kuid siiski 24 tunni jooksul alates selle teatavaks saamisest;
- juhul kui turbe rikkumine või terviklikkuse kadu mõjutab usaldusteenust kasutavat füüsilist või juriidilist isikut ebasoodsalt, teavitama füüsilist või juriidilist isikut turbe rikkumisest või terviklikkuse kadudest ilma liigse viivituseta;
- säilitama vastavalt punktidele 5.4 ja 5.5 usaldusteenustega seotud dokumentatsiooni, andmeid ja logisid;
- tagama nõuetekohase vastavushindamise ja esitama vastavushindamisasutuse järelduse järelevalveasutusele, et usaldusteenused oleksid jätkuvalt usaldusnimekirjas;
- omama käesoleva SK PS-iga vastavuses olemiseks vajalikku finantsilist stabiilsust ja vahendeid;
- avaldama kohustusliku kindlustuspoliisi tingimused ja vastavushindamisasutuse järeldused või sertifikaadi avalike andmesidevõrkude kaudu.

SK töötaja ei tohi olla karistatud tahtliku kuriteo toimepanemise eest.

9.6.2 RA esindamised ja tagatised

RA kohustub:

- osutama oma teenuseid vastavalt SK ja RA vahel sõlmitud lepingus, käesolevas SK PS-is, teenuse poliitikates ja põhimõtetes määratud nõuetele ja protseduuridele;
- tagama oma töötajatele kvaliteetse teenuse pakkumiseks vajaliku väljaõppe;
- teavitama SK-d ilma põhjendamatu viivituseta osutatavale usaldusteenusele või säilitatud isikuandmetele olulist mõju avaldavast turbe rikkumisest või terviklikkuse kadudest nende teatavaks saamisel.

RA töötaja ei tohi olla karistatud tahtliku kuriteo toimepanemise eest.

9.6.3 Kliendi esindamised ja tagatised

Klient kohustub:

- järgima käesolevas SK PS-is SK esitatud nõudeid, vastavaid teenuse poliitikaid ja/või põhimõtteid;
- andma teenuste taotlemisel õiget ja adekvaatset teavet ning esitatud andmete muutumisel teavitama kehtivatest andmetest vastavalt teenuse poliitikates ja põhimõtetes kehtestatud reeglitele;
- olema teadlik sellest, et SK võib keelduda teenuse osutamisest, kui klient esitab teenuse taotlemisel tahtlikult valeteavet või teavet, mis on ebakorrektne või mittetäielik;
- vastutama ainuisikuliselt oma isikliku võtme ja usaldusteenuse märgi hoidmise eest. Klient kohustub kasutama isiklikku võtit ja usaldusteenuse tunnistust vastavalt käesolevale SK PS-ile, teenuse põhimõtetele ja teenusetingimustele.

9.6.4 Huvitatud isiku esindamised ja tagatised

Huvitatud isik kohustub:

- tutvuma usaldusteenuse tunnistuste aktsepteerimisega seotud riskide ja kohustustega. Riskid ja kohustused on toodud käesolevas SK PS-is, vastavates teenuse poliitikates ja põhimõtetes ning teenusetingimustes;
- kontrollima SK osutatud kehtivusteenuste põhjal usaldusteenuste tunnistuste kehtivust, kasutades:
    - SK kodulehel https://www.sk.ee/repositoorium/ avaldatud teavet või
    - kohaldatavat kehtivusteenust või
    - asjakohast krüptograafilist teavet.

9.6.5 Teiste poolte esindamised ja tagatised

Täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

9.7 Tagatistest lahtiütlemine

SK:

- vastutab kõigi punktis 9.6.1 täpsustatud kohustuste eest Eesti Vabariigi õigusaktides määratud ulatuses;
- omab kõiki SK usaldusteenuseid katvaid kohustuslikke kindlustuslepinguid, et tagada hüvitis SK kohustuste rikkumisest tekkinud kahju eest.

SK ei vastuta:

- klientide isiklike võtmete salajas hoidmise, sertifikaatide võimaliku väärkasutuse või ebapiisava kontrolli või huvitatud isiku valede otsuste või mis tahes tagajärgede eest seoses vigade või tegevusetusega usaldusteenuse tunnistuste kehtivuskontrollis;
- kohustuste mittetäitmise eest, kui selle põhjuseks on järelevalveasutuse, andmekaitse inspektsiooni, usaldusnimekirja või muude ametiasutuste vead või turbeprobleemid;
- SK PS-ist tulenevate kohustuste mittetäitmise eest, kui mittetäitmise põhjuseks on vääramatu jõud (*Force Majeure*).

9.8 Vastutuse piirangud

Vastutuse ülempiir on kehtestatud eelnimetatud poliitikas, mis on kättesaadav veebilehel https://www.sk.ee/repositoorium/kindlustus/.

9.9 Hüvitised

Kliendi ja SK vahelisi hüvitisi reguleeritakse teenusetingimustes.

9.10 Tähtaeg ja lõpetamine

9.10.1 Tähtaeg

Vaadake käesoleva SK PS-i punkti 2.2.1.

9.10.2 Lõpetamine

Käesoleva SK PS-i ja/või teenuse põhimõtted kehtivad seni, kuni need asendatakse uue versiooniga või lõpetatakse usaldusteenuse osutamise või SK tegevuse lõpetamise tõttu.

SK kohustub pärast tegevuse lõpetamist tagama isikuandmete ja konfidentsiaalse teabe kaitse.

9.10.3 Lõpetamise tagajärjed ja kehtima jäävad sätted

SK teavitab käesoleva SK PS-i ja/või teenuse põhimõtete lõpetamise tingimustest ja tagajärgedest avaliku repositooriumi kaudu. Teavituses on täpsustatud, millised sätted jäävad pärast lõpetamist kehtima.

Pärast lõpetamist jäävad kehtima vähemalt kõik isikuandmete ja konfidentsiaalse teabe kaitsega seotud kohustused, samuti repositooriumi avaliku teabe haldamine, kindlaksmääratud ajaks SK arhiivid ja logid. Kõik kliendi kokkulepped jäävad jõusse seni, kuni sertifikaat tühistatakse või kuni see aegub, isegi juhul, kui käesolev SK PS ja/või teenuse põhimõtted lõpevad.

Käesolevat SK PS-i ja/või teenuse põhimõtteid ei saa lõpetada enne käesoleva SK PS-i punktis 5.8 kirjeldatud lõpetamistegevusi.

9.11 Individuaalsed teated ja suhtlemine pooltega

Üldiselt kasutatakse igasuguseks teavitamiseks ja suhtlemiseks SK veebilehte www.sk.ee.

Muud individuaalsete teadete viisid ja suhtlusvahendid on täpsustatud vastava teenuse poliitikas ja/või põhimõtetes.

9.12 Muudatused

9.12.1 Muudatuste läbiviimise protseduur

Vaadake käesoleva SK PS-i punkti 1.5.4.

9.12.2 Teavitusmehhanism ja -aeg

Vaadake käesoleva SK PS-i punkti 2.2.1.

9.12.3 Asjaolud, mis nõuavad OID-i muutmist

Ei kohaldata.

9.13 Vaidluste lahendamine

Kõik pooltevahelised vaidlused lahendatakse läbirääkimiste teel. Kui pooltel ei õnnestu sõbralikult kokkuleppele jõuda, lahendatakse vaidlus SK asukohakohtus.

Teist poolt teavitatakse mistahes nõudest või kaebusest hiljemalt 30 kalendripäeva jooksul pärast nõude tekkimist, välja arvatud siis, kui seaduses on sätestatud teisiti.

Klient või muu pool saab esitada oma nõude või kaebuse järgmisel e-posti aadressil: info@sk.ee.

9.14 Kohaldatav õigus

Käesolevat SK PS-i reguleerib Euroopa Liidu ja Eesti Vabariigi seadusandlus.

9.15 Vastavus kohaldatava õigusega

SK tagab vastavuse õiguslike nõuetega, et vastata kõikidele kohaldatavatele seadusest tulenevatele nõuetele andmete kaitsmisel kadumise, hävitamise ja võltsimise eest, ning järgmiste nõuetega:

- eIDAS määrus - Euroopa Parlamendi ja nõukogu 23. juuli 2014. a määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ [1];
- isikuandmete kaitse seadus [7];
- seotud Euroopa standardid:
  - ETSI EN 319 401 Elektroonilised allkirjad ja infrastruktuurid (ESI); Üldised poliitikanõuded usaldusteenuse osutajatele [2];
  - ETSI EN 319 411-1 Elektroonilised allkirjad ja infrastruktuurid (ESI); Poliitika- ja turbenõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 1. osa: Üldised nõuded [9];
  - ETSI EN 319 411-2 Elektroonilised allkirjad ja infrastruktuurid (ESI) Poliitika- ja turbenõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 2. osa: Poliitikanõuded kvalifitseeritud sertifikaate väljastavatele sertifitseerimisasutustele [9];
- CA/Browser Forum, sertifitseerimispoliitika põhinõuded avalikult usaldatud sertifikaatide väljastamiseks ja haldamiseks [3].

9.16 Muud sätted

9.16.1 Kogu lepingu ulatus

SK kohustab lepinguliselt iga RA-d ja teisi pooli vastama käesolevale SK PS-ile ja valdkonna kohaldatavatele juhistele. SK nõuab ka igalt tema tooteid ja teenuseid kasutavalt poolelt lepingu sõlmimist, mis sätestab toote või teenusega seotud tingimused. Kui lepingus on sätteid, mis erinevad käesolevast SK PS-ist, siis kohaldatakse konkreetse lepingu poolega sõlmitud kokkulepet. Kolmandad pooled ei või sellele lepingule tugineda ega kasutada meetmeid sellise lepingu jõustamiseks.

9.16.2 Loovutamine

Ükski käesoleva SK PS-i alusel tegutsev üksus ei või loovutada oma õigusi või kohustusi ilma SK eelneva kirjaliku nõusolekuta. Kui poolega sõlmitud lepingus ei ole määratud teisiti, ei esita SK loovutamise kohta teavitust.

9.16.3 Sätete kehtivus

Kui pädev kohtuasutus on tunnistanud käesoleva SK PS-i mistahes sätte kehtetuks või tühistamist, jääb ülejäänud SK PS kehtivaks ja kuulub täitmisele. Iga käesoleva SK PS-i säte, mis näeb ette vastutuse piirangud, tagatistest lahtiütlemise või kahjude välistamise, on kõikidest teistest sätetest lahutatav ja iseseisev.

9.16.4 Jõustamine (õigusabikulud ja õigustest loobumine)

SK võib nõuda poolelt tema käitumisega seotud kahjude, kaotuste ja kulude eest hüvitist ja õigusabikulusid.
Kui SK-l ei õnnestu seda käesoleva SK PS-i sätet jõustada, ei tähenda see seda, et SK loobub õigusest jõustada sama sätet hiljem või jõustada mingit muud käesoleva SK PS-i sätet. Selleks, et loobumised kehtiksid, peavad need olema esitatud kirjalikult ja SK poolt allkirjastatuna.

9.16.5 Vääramatu jõud

Vääramatu jõu subjekt ja teised pooled vastutavad mistahes nende mõistliku kontrolli alt väljas olevate asjaolude tagajärgede eest, sealhulgas (välja kuulutatud või kuulutamata) sõda, valitsuse või Euroopa Liidu tegevus, ekspordi- või impordikeelud, häired transpordis või selle üldine kättesaamatus, üldised elektrikatkestused, tulekahju, plahvatused, õnnetusjuhtumid, streigid või muu töötajate kooskõlastatud tegevus, töösulg, sabotaaž ja rahvarahutused.

Pooltevahelist suhtlust ja kohustuste täitmist vääramatu jõu korral reguleerivad lepingud.

SK PS-ist ja/või teenuse poliitikatest ja/või põhimõtetest tulenevate kohustuste täitmata jätmist ei loeta rikkumiseks, kui seda põhjustab vääramatu jõud. Mitte ükski pooltest ei saa nõuda teiselt poolelt kahjude hüvitamist või muud hüvitist viivituste või käesoleva SK PS-i ja/või teenuse poliitikate ja/või põhimõtete kohustuste täitmata jätmise eest, kui neid põhjustas vääramatu jõud.

9.17 Muud sätted

Ei kohaldata.

VIITED

[1] eIDAS määrus - Euroopa Parlamendi ja nõukogu 23. juuli 2014. a määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ;
[2] ETSI EN 319 401 Elektroonilised allkirjad ja infrastruktuurid (ESI); Üldised poliitikanõuded usaldusteenuse osutajatele;
[3] CA/Browser Forum, sertifitseerimispoliitika põhinõuded avalikult usaldatud sertifikaatide väljastamiseks ja haldamiseks https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.3.3.pdf

[4] RFC 3647 – palve kommenteerimiseks 3647, internet X.509 avaliku võtme infrastruktuur, sertifitseerimispoliitika ja -tavade raamistik: https://www.ietf.org/rfc/rfc3647.txt;
[5] ISO/IEC 27001: 2013 Infotehnoloogia – turbetehnika – infoturbe haldussüsteemid – nõuded;
[6] AS Sertifitseerimiskeskuse ajatempliteenuse osutaja põhimõtted, avaldatud: https://www.sk.ee/repositoorium/ajatembelduse-pohimotted/;
[7] Isikuandmete kaitse seadus, RT I 06.01.2016, 10;
[8] Kliendiandmete kaitse põhimõtted, avaldatud: https://sk.ee/repositoorium/andmekaitse/;
[9] ETSI EN 319 411-1 Elektroonilised allkirjad ja infrastruktuurid (ESI); Poliitika- ja turbenõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 1. osa: Üldised nõuded;
[10] ETSI EN 319 411-2 Elektroonilised allkirjad ja infrastruktuurid (ESI); Poliitika- ja turbenõuded sertifikaate väljastavatele usaldusteenuse osutajatele; 2. osa: Poliitikanõuded kvalifitseeritud sertifikaate väljastavatele sertifitseerimisasutustele.