Samlink Customer CA

Versio 1.0

18.09.2009

Voimassa 22.09.2009 alkaen

Samlink Customer CA - Varmennuskäytäntö

WS-Aineistopalvelut varmenteita varten
OID: 1.2.246.558.10.09704098.11.1.

SAMLINK

Sisällysluettelo

VERSIOLUETTELO

Dokumnetin versiotiedot

Versionro	Päiväys	Muutokset
1.0	18.09.2009	Hyväksytty PKI-ohjausryhmässä

1 KÄSITTEET JA LYHENTEET

Avainpari	Muodostuu julkisesta ja yksityisestä salausavaimesta, jotka ovat matemaattisesti toisiinsa liittyviä siten, että niiden avulla voidaan tehdä salausoperaatioita.
CA	Certificate Authority, Varmentaja - luotettu puolueeton kolmas osapuoli, joka myöntää ja ylläpitää sähköisiä varmenteita sekä niihin liittyviä muita palveluja (rekisteröinti, julkisten avainten hakemistot, sulkulistat)
CRL	Certificate Revocation List. Sulkulista, mitätöintilista, revokointi-lista. Lista käytöstä poistetuista varmenteista.
FIPS	Federal Information Protection Standard. FIPS-140-1 ja FIPS-140-2 ovat salausmoduuleita ja -algoritmeja koskevia tietoturva-vaatimuksia.
Hakemisto	Tietovarasto, johon voidaan tallettaa mm. varmenteet ja sulkulistat.
HSM-laite	Hardware Security Module. Salausavainten suojaamiseen tarkoitettu erikoislaite.
Hyväksyminen	Samlinkin PKI-ohjausryhmä hyväksyy dokumenttiin tehdyt muutokset. Dokumentin ylläpitovastuu on varmentajalla. Varmenne-tuotanto ja varmentaja huolehtivat omalta osaltaan tarvittavista päivityksistä ja toimittavat päivitetyn dokumentin varmentajan vastuuhenkilölle. Varmentajan vastuuhenkilö toimittaa hyväksymisen jälkeen dokumentin varmennetuotannon arkkitehtuurivastaavalle.
Julkinen avain	Yleiseen tietoon tarkoitettu salausavain. Julkisella avaimella salatut tiedot voidaan lukea vain käyttäen sen vastinparina toimivaa yksityistä avainta. Julkista avainta käytetään myös sähköisen allekirjoituksen tarkistukseen.
Juridinen henkilö	Oikeushenkilöitä, eli juridisia henkilöitä ovat kauppaoikeudelliset yhteisöt (kuten osakeyhtiöt ja osuuskunnat), siviilioikeudelliset yhteisöt (kuten yhdistykset ja säätiöt) sekä julkisyhteisöt (kuten valtio, kunnat tai seurakunnat).
Laite	Laitteella tarkoitetaan fyysistä laitetta, kuten esimerkiksi työasema (workstation) tai palvelin laite (server).
LDAP	Lightweight Directory Access Protocol. Hakemistokäyttöön tarkoitettu standardi rajapinta.
LDAPS	LDAP-prokollan SSL-tekniikalla suojattu (salattu) versio
Luottava osapuoli	Varmentajan toimintaan ja sen luomiin varmenteisiin luottava sekä niitä hyödyntävä taho.
OID	Object Identifier. Globaalisti yksikäsitteinen tunnistenumero.
Palvelin	Palvelimella tarkoitetaan palvelua (service) jonka ilmentymää voidaan ajaa useassa eri laitteessa
Palvelinhallinta	Samlinkin tai Samlinkin asiakasyrityksen infrasta vastuussa oleva organisaatio.

Palvelusopimus	Sopimus palvelusta, jonka käyttö edellyttää tässä dokumentissa kuvattujen varmenteiden käyttöä
PKI	Public Key Infrastructure. Varmentajan toimintaan liittyvien teknisten ja hallinnollisten ratkaisujen kokonaisuus.
Rekisteröijä	Taho, joka vastaa rekisteröinnistä.
Rekisteröinti	Prosessi, joka sisältää varmenteen haltijan tunnistamisen, tarvittavien tietojen keräämisen ja niiden toimittamisen varmennepyyntöä varten. Rekisteröintiin voi liittyä useita rekisteröintivastaavia.
Rekisteröintivastaava	Henkilö, joka vastaa tietojen keräämisestä ja rekisteröinnistä Varmennepyyntöä varten.
RFC	Request For Comments. Kokoelma standardeja, jotka mm. määrittelevät vaatimuksia varmentajan toiminnalle.
RSA	Epäsymmetrinen salausalgoritmi, joka perustuu avainparien käyttöön.
Samlinkin asia-kasyritys	Samlinkin asiakasyrityksellä tarkoitetaan yrityksiä, joille Samlink toimittaa tietojärjestelmiä tai tietojärjestelmäpalveluja.
Palvelusopimuksen haltija	Palvelusopimuksen haltijana toimii pääsääntöisesti pankki, mutta palvelusopimuksen haltijana voi toimia myös Samlink.
Pankki	Pankki toimii varmenteita käyttävän palvelun tarjoajana. Varmenteen haltija hankkii varmenteet tekemällä palvelusopimuksen palvelusta, jonka käyttöön varmenteet liittyvät
Sopimusten sulku-palvelu	Palvelusopimusten sulkupyyntöjä vastaanottava taho, jonka varmentaja on valtuuttanut erillisellä sopimuksella.
Sopimusjärjestelmä	Tietojärjestelmä, jolla rekisteröidään varmenteen haltijalle palvelusopimus palvelusta, jonka käyttämiseen tässä dokumentissa kuvattuja varmenteita käytetään
Sovellus	Sovelluksella (application) tarkoitetaan ohjelmaa, jonka eri ilmentymiä voidaan ajaa useassa eri laitteessa.
SSL	Secure Sockets Layer, internetissä yleisesti käytettävä tietoturva-protokolla
SSW	Sonera SecureWeb, varmennetuotannon tietoturvapalvelu, jonka avulla useimmat varmennetuotannon varmennehallintaohjelmistot on suojattu
Sulkulista	Kts. CRL
Sulkupalvelu	Varmenteiden sulkupyyntöjä vastaanottava taho.
Varmenne	Varmenteen haltijan nimestä ja julkisesta avaimesta muodostettu tieto, jonka varmentaja on allekirjoittanut sähköisesti. Varmenne todistaa tietyn julkisen avaimen kuuluvan tietylle haltijalle.
Varmennepalvelu	Varmenteiden tuottamiseen liittyvät järjestelmät, henkilöit ja prosessit kokonaisuutena. Varmennepalvelun osatoimintoja ovat rekisteröinti, varmennetuotanto, hakemistopalvelu, sulkupalvelu ja sulkulistapalvelu.
Varmenneperiaatteet	Kuvaa vaatimukset varmenteiden myöntämiselle, tuottamiselle ja käytölle.

Varmennepyyntö	Varmenteen hakijan tiedot ja julkisen avaimen sisältävä pyyntö varmenteen tuottamisesta.
Varmennetuotanto	Varmennetuotanto hallinnoi varmennusjärjestelmää, tuottaa varmenteet ja ylläpitää niiden tilatietoa.
Varmennuskäytäntö	Kuvaa varmentajan toiminnan varmenneperiaatteita noudattaen.

2 JOHDANTO

Tämä Samlink Customer CA Varmennuskäytäntö (jäljempänä varmennuskäytäntö) on Oy Samlink Ab:n (jäljempänä Samlink) hyväksymä kuvaus käytännöistä, joita noudatetaan Samlink Customer CA Varmenneperiaatteiden (jäljempänä varmenneperiaatteet) mukaisia varmenteita myönnettäessä ja käytettäessä.

Varmentajan (Samlink) ja sen mahdollisten alihankkijoiden sekä varmenteen haltijoiden ja varmenteeseen luottavien tahojen täytyy noudattaa tätä varmennuskäytäntöä varmentajan myöntämien varmenteiden yhteydessä.

Varmennuskäytännön rakenne noudattaa Samlinkin varmenneperiaatteissa käytettyä rakennetta, joka kattaa pääosin Internet Engineering Task Forcen standardin RFC 2527 suosittelemat varmenteen luotettavuuteen ja tuottamiseen liittyvät asiat.

Varmennepalvelussa on huomioitu laatuvarmenteen tuottamiseen vaadittavat tekniset ja hallinnolliset vaatimukset.

2.1 YLEISKUVAUS

Tätä Varmennuskäytäntöä sovelletaan Varmenteisiin, joita Samlink Varmentajana myöntää laatimiensa Varmenneperiaatteiden mukaisesti.

Varmentaja voi käyttää Varmennepalvelun toteuttamisessa alihankkijoita.

2.2 TUNNISTEET

Tämän asiakirjan tunniste on Samlink Customer CA Varmennuskäytäntö, jonka yksikäsitteinen tunnus on OID 1.2.246.558.10.09704098.11.1 v.1.0

Varmennuskäytäntö on kaikkien niiden osapuolten saatavilla, joiden edellytetään noudattavan sitä.

2.3 VARMENNUSORGANISAATIO JA VARMENTEIDEN SOVELTUVUUS

2.3.1 Varmentaja

Tämän varmennuskäytännön mukaisesti toimiva varmentaja on Samlink. Varmentajan myöntämissä varmenteissa on varmentajan nimenä ”CN = Samlink Customer CA, O = Samlink, C = FI”.

Varmenteiden myöntämisen ja julkaisemisen lisäksi varmentaja huolehtii myös siitä, että varmenteen haltijoita varten on tarjolla sulkupalvelu ja luottavia osapuolia varten sulkulistapalvelu.

2.3.2 Varmennetuotanto

Varmennetuotanto hallinnoi varmenteiden tuotantojärjestelmää, luo ja julkaisee varmenteet ja ylläpitää niiden tilatietoa koko niiden elinkaaren ajan. Varmennetuotanto sitoutuu noudattamaan tätä varmennuskäytäntöä omalta osaltaan.

2.3.3 Rekisteröijä

Rekisteröijä hoitaa varmenteen haltijan tunnistamisen, tarvittavien tietojen keräämisen ja niiden toimittamisen varmennepyyntöä varten. Rekisteröintiin voi liittyä useita rekisteröintivastaavia.

Rekisteröijinä voivat toimia Varmentajan omaan organisaatioon kuuluvat Rekisteröinti-toimintaan valtuutetut henkilöt ja muut Varmentajan mahdollisesti valtuuttamat tahot.

Kaikki Rekisteröijät velvoitetaan omalta osaltaan noudattamaan tätä Varmennuskäytäntöä.

2.3.4 Varmenteen haltija

Varmenteen haltijat on määritelty varmenneperiaatteissa. Varmenteen sisältämää julkista avainta vastaava yksityinen avain on tarkoitettu Varmenteen haltijan yksinomai-seen käyttöön.

2.3.5 Luottava osapuoli

Varmentajan myöntämiä varmenteita hyödyntävät luottavat osapuolet on määritelty varmenneperiaatteissa. Luottavan osapuolen täytyy sitoutua noudattamaan tässä dokumentissa kuvattuja velvollisuuksiaan.

2.3.6 Sulkupalvelu

Sulkupalvelussa toimivat velvoitetaan noudattamaan omalta osaltaan tätä varmennus-käytäntöä.

Sulkupalvelu on määritelty tarkemmin varmenneperiaatteissa.

2.3.7 Hakemisto

Varmentaja julkaisee hakemistossa varmenteiden sulkulistat.

2.3.8 Soveltuvuus

Varmentajan myöntämiä varmenteita voidaan käyttää vain seuraavissa toiminnoissa:

- Sähköisessä muodossa olevan tiedon alkuperän ja eheyden todentaminen
- Sähköisessä muodossa olevan tiedon tai avainten salaukseen
- Sähköisessä muodossa olevan tiedon luottamuksellisuuden varmistaminen.

Eri varmennetyyppien soveltuvuus on kuvattu asianomaisissa varmenneperiaatteissa

Varmenteita hyödynnettäessä täytyy ottaa huomioon varmenteen “Key Usage” -lisäkentässä mainittu avaimen käyttötarkoitus.

Tiedostoa tai viestiä, joka on salattu varmentajan myöntämään varmenteeseen liittyvällä avaimella, ei ole tarkoitettu arkistoitavaksi tai säilytettäväksi pitkäaikaisesti salatussa muodossa. Salausta ei voi purkaa, jos purkamiseen tarkoitettu avain ei ole enää käytettävissä.

Varmennepalvelua koskevassa sopimuksessa saattaa olla avainten käyttötarkoituksiin liittyviä rajoituksia, jotka täytyy ottaa huomioon varmenteita käytettäessä.

2.4 YHTEYSTIEDOT

Samlinkin turvallisuusosasto vastaa tämän varmennuskäytännön hallinnoimisesta, ylläpidosta ja päivityksistä. Tekijänoikeudet tämän varmennuskäytännön osalta kuuluvat Samlinkille.

Varmennuskäytännön hyväksyy Samlinkin johtoryhmän nimeämä Samlink PKI ohjausryhmä. Esittelijänä toimii Samlinkin turvallisuuspäällikkö.

Tätä varmennuskäytäntöä koskevat kysymykset voi lähettää osoitteeseen:

Oy Samlink Ab	turvallisuus@samlink.fi
PL 130, Linnoitustie 9	Puh. (09) 548 050 02601
ESPOO	Fax. (09) 5480 5853

Samlinkin muut yhteystiedot ja palveluajat löytyvät osoitteesta http://sonetti.saminet.fi/.

3 YLEISET EHDOT

3.1 VELVOLLISUUDET

3.1.1 Varmentajan velvollisuudet

Varmentajan velvollisuudet eri varmenteiden osalta on määritelty asianomaisissa varmenneperiaatteissa kappaleessa 3.1.1.

3.1.2 Varmennetuotantoon liittyvät velvollisuudet

Varmennetuotantoon liittyvät velvollisuudet on määritelty kunkin varmennetyypin osalta sen omissa varmenneperiaatteissa kappaleessa 3.1.2.

3.1.3 Rekisteröijän velvollisuudet

Rekisteröijän velvollisuudet on kuvattu varmenneperiaatteissa kappaleessa 3.1.3

3.1.4 Varmenteen haltijan velvollisuudet

Varmenteen haltijan vastuu on varmenneperiaatteissa asetettu kyseisen järjestelmäelementin ylläpitäjälle. Tämän vastuun noudattaminen edellyttää seuraavia toimenpiteitä:

- Ylläpitäjän täytyy huolehtia siitä, että yksityisestä avaimesta on saatavilla varmuuskopio.
- Ylläpitäjän täytyy tehdä välittömästi varmenteen sulkupyyntö sopimusten sulkupalveluun sen palveluaikana, kun yksityinen avain on korruptoitunut tai poistettu käytöstä, tai on syytä epäillä sen vaarantuneen.
- Ylläpitäjän täytyy ilmoittaa palvelun lopettamisesta palvelun tarjoajalle. Palvelun lopettaminen aiheuttaa automaattisesti myös varmenteen sulkupyynnön.
- Ylläpitäjän täytyy hävittää yksityinen avain ja varmenne laitteelta tai palvelinsovellukselta varmenteen voimassaolon päätyttyä tai kun varmennetta ei enää tarvita alkuperäiseen käyttötarkoitukseen.

3.1.5 Sulkupalvelun velvollisuudet

Sulkupalvelun velvollisuudet on märitelty varmenneperiaatteissa kappaleessa 3.1.6.

3.1.6 Varmenteeseen luottavan osapuolen velvollisuudet

Varmenteeseen Luottavan osapuolen velvollisuudet on määritelty varmenneperiaatteissa kappaleessa 3.1.5.

3.1.7 Tietovarastoon liittyvät velvollisuudet

Tietovarastoon liittyvät velvollisuudet on määritelty varmenneperiaatteissa kappaleessa 3.1.7.

3.2 VASTUUVELVOLLISUUS

Varmentajan ja rekisteröijän vastuuvelvollisuudet on kuvattu varmenneperiaatteissa kappaleessa 3.2.

3.3 TALOUDELLINEN VASTUU

Taloudellinen vastuu on kuvattu Varmenneperiaatteissa kappaleessa 3.3.

3.4 TULKINTA JA TÄYTÄNTÖÖNPANO

3.4.1 Sovellettava lainsäädäntö

Tähän varmennuskäytäntöön sovelletaan Suomen lakia.

3.4.2 Erimielisyyksien ratkaiseminen

Mikäli varmenteen haltijan ja varmentajan välillä syntyy varmennepalveluun liittyviä erimielisyyksiä, ne pyritään ensisijaisesti sopimaan neuvotteluin. Mikäli erimielisyyksistä ei päästä sopimukseen, niiden ratkaisussa noudatetaan varmentajan ja varmenteen haltijan välisiä sopimuksia.

3.5 MAKSUT

Varmennepalveluiden maksut peritään kulloinkin voimassa olevan palveluhinnaston mukaan. Veloitusperusteet on tarkemmin kuvattu varmenneperiaatteissa kappaleessa 3.5

3.6 TIETOJEN JULKAISEMINEN JA TIETOVARASTO

Tietojen julkaiseminen on kuvattu varmenneperiaatteissa kappaleessa 3.6.

3.7 TARKASTUKSET

Samlinkin sisäisen tarkastuksen suorittamassa varmennustoiminnan tarkastuksessa mahdollisesti esille tulleiden puutteiden korjaamisen käynnistää Samlinkin PKI ohjausryhmä.

Varmentajan omassa toiminnassa havaittujen puutteiden korjaamiseksi laaditaan suunnitelma, johon sisältyvät korjausaikataulut määräytyvät puutteen vakavuuden ja korjaustoimenpiteen vaatiman ajan perusteella.

Mikäli puutteita on havaittu varmentajan alihankkijoiden toiminnassa, näistä tiedotetaan asianomaisille ja alihankkijaa edellytetään korjaamaan puutteet kohtuullisen ajan kuluessa.

Mikäli tarkastuksista seuraa muutostarpeita varmenneperiaatteisiin tai varmennuskäytäntöön, muutokset tehdään ja niistä tiedotetaan kunkin dokumentin kappaleen 9.1 ”Muutosmenettely” mukaisesti.

Jos varmenteen haltija tai luottava osapuoli vaatii erillistä varmennepalvelun auditointia, se vastaa auditoinnista aiheutuvista kustannuksista.

3.8 LUOTTAMUKSELLISUUS

Varmenteen haltijoita koskevien henkilötietojen luottamuksellisuus sekä henkilö- ja tunnistamistietojen käsittely on kuvattu varmenneperiaatteissa kappaleessa 3.8.

3.9 OMISTUS- JA IMMATERIAALIOIKEUDET

Omistus- ja immateriaalioikeudet on kuvattu varmenneperiaatteissa kappaleessa 3.9.

3.10 SOPIMUKSET

Varmennepalvelun eri osapuolten sopimukset on kuvattu varmenneperiaatteissa kappaleessa 3.10.

4 TUNNISTUS JA TODENTAMINEN

4.1 NIMEÄMISKÄYTÄNTÖ VARMENTAJAN VARMENTEESSA

Varmentajan Varmenteen yksilöintitiedot:

Tieto (Attribute)	Selite	Esimerkki
Julkaisija (Issuer)	Varmenteen julkaisija	C=FI, O=Samlink, CN=Samlink Customer CA
Tunnistenimi (Subject)	Varmenteen yksilöllinen nimi	C=FI, O=Samlink, CN=Samlink Customer CA
Sarjanumero (SerialNumber)	Varmenteen yksilöivä tunniste	80:8e:c2:f0:14:25:e2:a3:99:01:a5:12:06:71:19:39

Sama varmentajan nimi esiintyy ”Issuer”-kentässä myös kaikissa muissa varmentajan myöntämissä varmenteissa.

4.2 ENSIREKISTERÖINTI

4.2.1 Nimeämiskäytännöt

Rekisteröitäessä uutta varmenteen haltijaa määritellään tiedot, jotka tästä tallennetaan Varmenteeseen. Näitä tunnistetietoja voi olla Varmenteen ”Subject”-kentässä ja ”Subject Alternative Name” –kentässä.

Nimeämiskäytännöt ja nimen osien käyttö on kuvattu varmenneperiaatteiden kappaleessa 4.2.1.

4.2.2 Nimivaatimukset

Nimivaatimukset on kuvattu varmenneperiaatteissa kappaleessa 4.2.2.

4.2.3 Nimien yksikäsitteisyys

Tunnistenimen täytyy olla yksikäsitteinen kaikille varmentajan myöntämille varmenteille. Yksikäsitteisyys tarkoittaa, että varmentaja ei myönnä eri laitteille, sovelluksille tai ohjelmille varmenteita, joissa olisi identtiset tunnistenimien arvot.

4.2.4 Nimiepäselvyyksien ratkaiseminen

Nimiepäselvyyksien ratkaiseminen on kuvattu varmenneperiaatteissa kappaleessa 4.2.4.

4.2.5 Yksityisen avaimen hallussapidon osoittaminen

Varmenteita haettaessa varmennepyyntö toimitetaan varmentajalle sähköisesti allekirjoitettuna tai kertakäyttöisellä tunnuksella ja salasanalla vahvistettuna tai asianmukaisella asiakirjalla, jonka perusteella voidaan todentaa hakemuksen alkuperä ja oikeudellisuus ja tarkistaa muulla tietovälineellä olevan varmennepyynnön sisällön vastaavuus.

Varmentaja todentaa pyynnön tulleen sellaisesta lähteestä, jossa varmennettavaa julkista avainta vastaava yksityinen avain on ollut käytettävissä.

4.2.6 Rekisteröijän todentaminen

Varmentaja tunnistaa ja valtuuttaa oman rekisteröintipisteensä rekisteröintivastaavat. rekisteröintitehtävissä rekisteröintivastaavat todennetaan varmenteen avulla.

Vain valtuutettu rekisteröijä voi suorittaa rekisteröintejä.

Varmenneperiaatteissa on tarkempi kuvaus rekisteröijän todentamisesta.

4.2.7 Organisaation todentaminen

Rekisteröijän on varmistettava varmenteeseen tulevan organisaationimen käyttöoikeus varmenteessa.

Varmenneperiaatteissa on tarkempi kuvaus organisaation todentamisesta.

4.2.8 Varmenteen haltijan tunnistaminen

Varmenteen haltijaa edustaa varmennetta hakeva henkilö, jonka valtuudet varmenteen hakemiseksi varmistetaan rekisteröinnin yhteydessä.

Varmenneperiaatteissa on tarkempi kuvaus varmenteen haltijan tunnistamisesta.

4.3 VARMENTEEN UUSIMINEN VOIMASSAOLON PÄÄTTYESSÄ

Käytössä olleita varmennettuja avaimia ei varmenneta uudelleen, vaan luodaan uudet avaimet.

Varmenneperiaatteissa on tarkempi kuvaus voimassaolon päättyessä.

4.4 VARMENTEEN UUSIMINEN VOIMASSAOLON PÄÄTTYMISEN TAI MITÄTÖINNIN JÄLKEEN

Jos varmenne on mitätöity tai sen voimassaolo on päättynyt, käytössä olleille avaimille ei luoda uutta Varmennetta. varmenteen uusiminen edellyttää uusien avainten luontia.

Uuden varmenteen hakumenettely on sama kuin ensirekisteröinnissä.

4.5 VARMENTEEN MITÄTÖINTI- TAI VOIMASSAOLON KESKEYTTÄMISPYYNTÖ

Varmenteen voimassaolon keskeytys ei ole mahdollinen.

Mitätöintiä pyytävä henkilö on tunnistettava sulkupalvelussa. Tunnistus täytyy tehdä sellaisella tavalla, että pyytäjän oikeus pyytää mitätöintiä voidaan todentaa. Tunnistusmekanismien on otettava huomioon luvattomien pyyntöjen tekemisen mahdollisuus.

Tunnistustapa on kuvattu varmenneperiaatteissa.

Vain sulkupalveluvastaavilla on oikeus toimittaa varmenteen mitätöintipyyntö varmentajan järjestelmään. Sulkupalveluvastaava tunnistetaan varmenteen perusteella.

4.6 VARMENTEEN PALAUTTAMISPYYNTÖ

Varmennetta ei voi enää palauttaa mitätöinnin jälkeen.

5 TOIMINNALLISET VAATIMUKSET

5.1 VARMENTEEN HAKEMINEN

Varmennetilaukset ja -pyynnöt täytyy tehdä ja täyttää annettujen ohjeiden mukaisesti ja niiden täytyy sisältää vaaditut ja oikeat tiedot.

Varmenneperiaatteissa on tarkempi kuvaus varmenteen hakumenettelystä.

5.2 VARMENTEEN MYÖNTÄMINEN

Varmennetuotanto luo vastaanotetun sähköisesti allekirjoitetun varmennepyynnön perusteella varmenteen, joka on varmentajan allekirjoittama. Varmentaja vastaa siitä, myönnettyjen varmenteiden yksilöintitiedot ovat varmennepyynnön ja rekisteröintitietojen mukaiset.

Varmenteen sisältö on kuvattu kappaleessa 8.1 ”Varmenneprofiilit”.

Erityisesti seuraavista asioista on huolehdittava:

- Varmenteiden myöntämismenettely on turvallisesti liitetty avainten luonnissa ja rekisteröinnissä käytettyihin prosesseihin.
- Varmentajan on pidettävä huolta, että varmenteen haltijan yksikäsitteinen käyttäjätunnus pysyy yksikäsitteisenä Varmentajan myöntämissä, voimassaolevissa varmenteissa.

Rekisteröintitietojen eheys suojataan erityisesti siirrettäessä tietoja tilausprosessin toimijoiden välillä.

5.3 VARMENTEEN HYVÄKSYMINEN

Varmenteen asentaminen laitteelle tai sovellukselle ilmaisee sen, että Varmenteen halti-ja hyväksyy Varmenteen ja sitoutuu noudattamaan Varmenneperiaatteita.

5.4 VARMENTEEN MITÄTÖINTI

Mitätöidystä varmenteesta julkaistaan hakemistossa olevalla sulkulistalla varmenteen sarjanumero, sulkemisaika ja syykoodi. Mitätöity varmenne on sulkulistalla vähintään varmenteeseen merkityn voimassaoloajan loppuun saakka.

5.4.1 Olosuhteet Varmenteen mitätöimiseksi

Varmentaja voi myös Samlinkin turvallisuusosaston päätöksellä ilman varmenteen haltijalta tullutta pyyntöä mitätöidä varmenteen, jos siihen on olemassa perusteltu syy. Näitä syitä ovat mm seuraavat:

- Varmentaja toteaa, että varmennetta ei ole myönnetty sitä koskevien varmenneperiaatteiden tai tämän varmennuskäytännön mukaisesti.
- Varmenteen sisältöön liittyy nimen omistusoikeutta koskeva kiista.
- Varmenteen haltija rikkoo oleellisesti varmentajan kanssa tehtyä sopimusta.

5.4.2 Oikeus pyytää Varmenteen mitätöintiä

Varmenteen mitätöinnin voi panna alulle kuitenkin myös Varmentaja Samlinkin Tur-vallisuusosaston luvalla perustuen minkä tahansa osapuolen esille tuomaan luotettavaan ja pätevään tietoon, joka viittaa tämän dokumentin kappaleen 5.4.1 ”Olosuhteet Var-menteen mitätöimiseksi” tai Varmenneperiaatteissa olevan vastaavan kappaleen mukai-siin mitätöintiolosuhteisiin.

5.4.3 Mitätöintipyyntömenettely

Varmenteen mitätöintipyyntö voidaan tehdä sulkupalveluun joko:

- puhelimitse (varmistetaan tarvittaessa takaisinsoitolla)
- sähköpostilla, joka on palvelinhallinnan henkilön sähköisesti allekirjoittama.

Kaikki mitätöintiin liittyvät tapahtumat (pyyntö, peruste ja tunnistustapa) täytyy arkistoida.

Kun Varmenne on mitätöity lopullisesti, sitä ei voi enää ottaa käyttöön.

5.4.4 Mitätöintipyynnön odotusaika

Varmenteen haltija vastaa siitä, että Sulkupalveluun toimitetaan mitätöintipyyntö vii-pymättä Sulkupalvelun palveluaikana tätä edellyttävissä olosuhteissa.

Varmentaja ei vastaa laitteelle tai palvelinsovellukselle luodun yksityisen avaimen oikeudettomasta käytöstä aiheutuneesta vahingosta.

Varmentaja vastaa mitätöintitiedon julkaisemisesta sulkulistalla varmenneperiaatteissa ja varmennuskäytännössä ilmoitettujen periaatteiden mukaisesti.

5.4.5 Sulkulistan julkaisu

Sulkulistapalvelu toteutetaan julkaisemalla varmentajan sähköisesti allekirjoittamat Sulkulistat julkisessa hakemistossa. Sulkulistan eheys taataan varmentajan sähköisellä allekirjoituksella.

Sulkulista julkaistaan kahden (2) tunnin välein ja se on voimassa viisi (5) vuorokautta. Vika-, huolto- ja muissa poikkeustilanteissa uusi sulkulista julkaistaan viimeistään ennen edellisen sulkulistan voimassaoloajan 5 vuorokautta päättymistä. Jokaisessa sulkulistassa ilmoitetaan sen voimassaolon päättymishetki.

Sulkulista on saatavilla hakemistosta 24 tuntia päivässä, 7 päivää viikossa, lukuun ottamatta ennalta ilmoitettuja huoltokatkoksia. Varmentaja ei vastaa palvelun saatavuudesta, mikäli vika tai katkos ilmenee Varmentajasta riippumattomissa järjestelmissä tai palveluissa.

Hakemistossa saattaa olla yhtä aikaa saatavana useita voimassa olevia sulkulistoja. Näistä viimeisimmäksi julkaistu sisältää ajantasaisimmat tiedot.

5.4.6 Sulkulistan tarkastusvaatimukset

Ennen varmenteeseen luottamista luottavan osapuolen on varmistettava, että varmennetta ei ole asetettu sulkulistalle. Varmenteeseen ei voida luottaa, jos ei noudateta huolellisesti seuraavia sulkulistatiedon tarkastusmenettelyjä:

- Luottavan osapuolen, joka hakee sulkulistan hakemistosta, täytyy varmistaa sulkulistan aitous tarkistamalla sen sähköinen allekirjoitus ja siihen liittyvä varmennuspolku.
- Luottavan osapuolen täytyy myös tarkistaa sulkulistan voimassaoloaika varmistuakseen siitä, että sulkulistan voimassaolosta.
- Varmenteita voidaan tallentaa paikallisesti luottavan osapuolen järjestelmään, mutta ennen käyttöä jokaisen tällaisen varmenteen senhetkinen tila täytyy tarkistaa sulkulistalta mahdollisen mitätöinnin varalta.
- Jos voimassa olevaa sulkulistatietoa ei ole saatavissa esim. järjestelmä- tai palvelu-häiriön takia, yhteenkään varmenteeseen ei pidä luottaa. Varmenteen hyväksyminen vastoin tätä ehtoa tapahtuu luottavan osapuolen omalla riskillä.

Sulkulistat löytyvät seuraavasta osoitteesta:

URL=ldap://194.252.124.241:389/cn=Samlink%20Customer%20CA,o=Samlink,c=fi?certificaterevocationlist;binary

5.5 VARMENTEEN PALAUTTAMINEN KÄYTTÖÖN

Varmenteiden voimassaolon keskeytys ei ole mahdollinen, joten ne eivät ole palautettavissa käyttöön.

5.6 TIETOTURVALLISUUDEN VALVONTA

5.6.1 Tallennettavat tiedot

Varmentaja ja varmennetuotanto tallentavat automaattisesti tai manuaalisesti seuraavat oleelliset varmennustoimintaan liittyvät tiedot:

Varmentajan avainten elinkaareen liittyvät tiedot

- avainten luonti, varmuuskopiointi, palautus ja tuhoaminen
- salausteknisen laitteen elinkaareen liittyvät ylläpitotapahtumat

Varmentajan ja varmenteen haltijoiden varmenteiden elinkaareen liittyvät ylläpitotapahtumat:

- Varmennetilaukset ja -pyynnöt, varmenteiden uusimispyynnöt uusille avaimille
- Sopimusten tilapäiset sulkemiset
- Varmenteiden mitätöinnit
- Varmenteiden luomiset ja julkaisemiset
- Sulkulistojen luomiset ja julkaisemiset. Sulkulistaa ei arkistoida, mutta varmennejärjestelmässä tarkistetaan vuorokauden vaihteen jälkeen, että sulkulistalta löytyvät kaikki mitätöidyt varmenteet.

Tietoturvallisuuden ylläpitoon liittyvät tapahtumat

- Varmenteiden hakua varten toimitettujen ohjelmistotyökalujen avulla suoritetut tapahtumat
- Varmennetuotannon henkilöstön suorittamat varmennusjärjestelmään tai turvajärjestelmiin kohdistuvat toimenpiteet, mm. ohjelmistojen, laitteiden ja päivitysten asennukset, palautukset, järjestelmien alasajot ja uudelleenkäynnistykset sekä järjestelmän asetusten muutokset
- järjestelmien kaatumiset, laitteistoviat ja muut poikkeamat järjestelmissä
- reitittimien ja palomuurien ja hyökkäyksenhavaitsemisjärjestelmien tapahtumat
- kulunvalvontatapahtumat varmennusjärjestelmän tiloihin.

Tallennettaviin tietoihin sisältyy tietojen tyyppi, päivämäärä ja kellonaika sekä automaattisesti tallentuviin lokeihin juokseva numero ja lokia tuottavan järjestelmän tunniste.

Varmentajan sulkupalvelussa tallennetaan mitätöintipyyntöihin liittyen kappaleessa 5.4.3 ”Mitätöintipyyntömenettely” mainitut tiedot.

5.6.2 Lokitietojen seuranta

Merkittäviä turvallisuuteen ja toimintaan liittyviä lokeja seurataan säännöllisesti varmennetuotannon henkilöstön toimesta.

Järjestelmien tuottamien hälytysten perusteella suoritetaan lokien läpikäyntiä epäilyttävien tai poikkeavien tapahtumien selvittämiseksi.

5.6.3 Lokitietojen säilytysaika

Varmennusjärjestelmän lokitietoja säilytetään vähintään vuoden ajan niiden syntymisestä, ja sen jälkeen tiedot arkistoidaan kappaleessa 5.7.2 ”Arkiston säilytysaika” mainituksi ajaksi.

Varmentamiseen liittyvien muiden järjestelmien tuottamia oleellisia lokitietoja säilytetään järjestelmissä itsessään vähintään 10 päivän ajan niiden syntymisestä. Lisäksi lokitietoja voidaan siirtää myös erilliselle lokipalvelimelle säilytettäväksi ja viedä tallennusmedialle arkistointia varten.

5.6.4 Lokitietojen suojaus

Manuaalisesti tallennettavat lokit sekä varmentajan ja varmennetuotannon järjestelmien automaattisesti tuottamat lokit on suojattu muuttamiselta, tuhoamiselta ja oikeudettomalta lukemiselta järjestelmien käyttövaltuushallinnalla ja kulunvalvonnalla.

Varmennusjärjestelmän lokitiedot on allekirjoitettu sähköisesti.

5.6.5 Lokitietojen varmistus

Varmennusjärjestelmän lokitiedoista otetaan säännöllisesti varmuuskopiot.

Muiden varmentajan ja varmennetuotannon järjestelmien tuottamien lokitietojen varmistuskäytäntö riippuu järjestelmästä ja lokitietojen kriittisyydestä. Oleellisimmista lokitiedoista otetaan säännöllisesti varmuuskopiot.

5.6.6 Lokitietojen keruujärjestelmä

Varmentajan ja varmennetuotannon järjestelmät tukevat lokitietojen keräystä. Tietyt tuotantojärjestelmälle tehtävät hallintatapahtumat, esim. järjestelmän muutokset ja päivitykset sekä CA-avaimiin liittyvät hallintatapahtumat kirjataan käsin fyysiseen lokiin.

Järjestelmissä automaattisesti syntyvät lokitiedot tallennetaan sovellus-, verkkolaite- ja käyttöjärjestelmätasolla. Manuaaliset lokit tuotetaan pöytäkirjoina varmennetuotannon henkilöstön toimesta.

5.6.7 Järjestelmien haavoittuvuuden testaus

Varmennetuotannossa testataan säännöllisesti kriittisten järjestelmien haavoittuvuutta ulkopuolisten suorittamien tunkeutumisyritysten varalta. Testaustulosten perusteella päivitetään tarvittaessa palomuurien ja muiden järjestelmien konfiguraatioita sekä toimintaperiaatteita ja käytäntöjä.

5.7 TIETOJEN ARKISTOINTI

5.7.1 Arkistoitavat tiedot

Varmennetuotanto arkistoi kappaleessa 5.6.1 ”Tallennettavat tiedot” kuvatuista lokitiedoista kriittisimmät, mm. kaikki varmennusjärjestelmän tuottamat lokit sekä manuaalisesti syntyvät varmennusjärjestelmään kohdistuvista toimenpiteistä tehdyt lokit.

Edellä mainittujen lokitietojen lisäksi vähintään alla olevat tiedot arkistoidaan Varmentajan tai varmennetuotannon toimesta:

- varmennepalveluihin liittyvät sopimukset
- varmennetuotantoon liittyvät sopimukset
- varmentajan vastaanottamat varmennetilaukset ja -hakemukset
- myönnetyt varmenteet
- Varmentajan sulkupalvelun vastaanottamat Varmenteiden mitätöintipyynnöt
- sopimusten sulkupalvelun vastaanottamat Palvelusopimusten voimassaolon keskeyttämispyynnöt
- julkaistut sulkulistat
- kaikki varmentajan julkaisemat varmenneperiaatteiden versiot
- kaikki varmentajan julkaisemat varmennuskäytäntöversiot
- Samlinkin sisäisen tarkastuksen laatimat tarkastuspöytäkirjat.

Tietoja voidaan arkistoida sekä sähköisessä muodossa että fyysisinä dokumentteina.

5.7.2 Arkiston säilytysaika

Kaikki kappaleessa 5.7.1 ”Arkistoitavat tiedot” mainitut tiedot arkistoidaan vähintään kolmen (3) vuoden ajaksi niiden syntymishetkestä laskettuna.

Varmennepalveluun ja varmennetuotantoon liittyvät sopimukset säilytetään vähintään kolmen (3) vuoden ajan niiden voimassaolon päättymisestä laskettuna.

Julkaistut varmenteet ja niihin liittyvät rekisteröintitiedot sekä sulkulistat arkistoidaan vähintään kolmen (3) vuoden ajaksi varmenteen voimassaoloajan päättymisestä laskettuna.

Varmentaja ei takaa arkistojen säilytystä sen jälkeen kun varmentajan toiminta on päättynyt.

5.7.3 Arkiston suojaus

Arkistot, jotka sisältävät sähköisessä muodossa tallennetut varmenteiden luomiseen ja mitätöintiin liittyvät tiedot sekä varmenteet ja sulkulistat, sijaitsevat kulunvalvonnalla suojatuissa paloturvallisissa tiloissa. Myös varmenteiden tuotantojärjestelmäympäristön muutoksia koskevat tiedot arkistoidaan kulunvalvonnalla suojatuissa paloturvallisissa tiloissa. Muut arkistoitavat tiedot sijaitsevat vähintään kulunvalvonnalla suojatuissa tiloissa.

5.7.4 Arkiston varmistus

Varmennusjärjestelmän tuottamista arkistotiedoista otetaan varmuuskopiot tiedon häviämisen tai tuhoutumisen varalta, jotta varsinaisen arkiston tuhoutuessa tiedot voidaan palauttaa varmuuskopioista.

5.7.5 Arkistotiedon saanti- ja tarkistamismenettelyt

Arkistotietoja säilytetään siten, että vain valtuutetut Varmentajan tai Varmennetuotannon henkilöt voivat päästä niihin käsiksi. Arkistotietojen katseluun oikeutettuja ovat ne henkilöt, jotka suorittavat tarkastuksia kappaleen 3.7 ”Tarkastukset” mukaisesti. Muutoin tietoja toimitetaan ainoastaan kirjalliseen pyyntöön perustuen Suomen lain sallimissa ja velvoittamissa rajoissa ja Samlinkin Turvallisuusosaston valvonnassa.

Varmenteen haltijalle luovutetaan häntä itseään koskevia arkistotietoja. Tiedot luovutetaan henkilötietolaissa määritellyn tarkastusoikeuden rajoissa veloituksetta. Muutoin tiedon hakemisesta ja toimittamisesta veloitetaan kohtuulliset työmäärään perustuvat maksut.

5.8 VARMENTAJAN AVAINTEN UUSIMINEN

Varmentajalle luodaan uusi allekirjoitusavain vähintään pisimmän varmentajan myöntämän varmenteen eliniän verran ennen kuin käytössä olevan allekirjoitusavaimen käyttöaika varmenteiden allekirjoittamiseen päättyy. Avainta käytetään varmenteiden allekirjoittamiseen korkeintaan niin kauan, että sillä myönnetyn viimeisenkin varmenteen voimassaoloaika on päättynyt, ennen kuin avaimen käyttöaika päättyy. Näin varmistetaan, että sulkulista voidaan aina allekirjoittaa samalla avaimella, jolla sille mahdollisesti päätyvät Varmenteet on allekirjoitettu.

- Seuraavat Varmenteet julkaistaan avainten vaihtamisen yhteydessä:
- Varmentajan uudella Yksityisellä avaimella allekirjoitettu Varmenne Varmentajan vanhalle Julkiselle avaimelle
- Varmentajan vanhalla Yksityisellä avaimella allekirjoitettu Varmenne Varmentajan uudelle Julkiselle avaimelle
- Varmentajan uudella Yksityisellä avaimella allekirjoitettu Varmenne saman Avain-parin Julkiselle avaimelle.

5.9 KATASTROFISTA JA VARMENTAJAN AVAIMEN PALJASTUMISESTA TOIPUMINEN

5.9.1 Tietokonelaitteet, ohjelmistot, ja/tai tiedot ovat korruptoituneet

Tuotantojärjestelmä on kahdennettu. Laitevian tapauksessa tuotanto siirtyy varalaitteelle. Ohjelmistovian tapauksessa suoritetaan ohjelmiston uudelleenasennus. Tiedon korruptoituessa tiedot palautetaan varmuuskopiolta, jollainen otetaan aina ennen ja jälkeen jokaista järjestelmän muutosta ja muutoin säännöllisesti. Kriittisimmistä tiedoista otetaan varmuuskopio vähintään 4 kertaa viikossa. Laaja-alaisempi tuotantojärjestelmän osan tuhoutuminen aiheuttaa palvelun keskeytymisen, jonka pituus riippuu ongelman laajuudesta.

5.9.2 Varmentajan yksityinen avain on paljastunut

Mikäli varmentajan yksityinen avain paljastuu, toimitaan seuraavasti. Tällä avaimella allekirjoitetut sulkulistat poistetaan sulkulistapalvelusta välittömästi, jolloin kyseisellä avaimella allekirjoitettuihin varmenteisiin ei voi riittävin perustein luottaa. Varmentaja ilmoittaa varmenteen haltijoille avaimen paljastumisesta sekä antaa tietoa sen edellyttämistä toimenpiteistä varmentajan ja pankkien käytössä olevilla intranet-sivuilla, sekä sähköpostitse. Toiminnan jatkaminen vaatii uusien varmentajan allekirjoitusavainten luonnin sekä uusien varmenteiden luonnin varmenteen haltijoille ja tietojärjestelmien elementeille.

5.10 VARMENNUSTOIMINNAN LOPETTAMINEN

Toiminnan lopettamiseen liittyvät keskeiset toimenpiteet on kuvattu varmenneperiaatteissa. Samlink PKI ohjausryhmä vastaa periaatteiden toteuttamisesta tältä osin.

Varmentaja tiedottaa toimintansa lopettamisesta seuraavasti:

- Varmennustoiminnan lopettamisesta ilmoitetaan varmentajan ja pankkien käytössä olevilla intranet-sivuilla sekä julkisessa web-sivustossa
- Mahdollisille varmennepalveluun liittyviä tehtäviä hoitaville alihankkijoille lopettamisesta ilmoitetaan kirjeellä, jolla samalla irtisanotaan sopimus Varmennepalveluiden toimintojen hoitamisesta varmentajan puolesta.

Lisäksi Varmentaja toteuttaa seuraavat toimenpiteet toimintansa lopettamisen yhteydessä:

- Varmentaja lopettaa sulkulistapalvelun, jonka jälkeen sen myöntämiin varmenteisiin ei voi enää perustellusti luottaa.
- Varmentaja tuhoaa tai poistaa käytöstä yksityiset allekirjoitusavaimensa siten, että niitä ei voida enää ottaa käyttöön.

6 TURVATOIMENPITEET

6.1 FYYSISET TURVARATKAISUT

Rekisteröijän toimitiloissa ja henkilöstön rekrytoinnissa noudatetaan toimitila- ja henkilöstöturvallisuudesta annettuja ohjeita.

Seuraavat kohdat koskevat varmentajaa ja mahdollista varmennetuotannosta vastaavaa alihankkijaa.

6.1.1 Laitetilan sijainti ja rakenne

Varmenteiden tuotantolaitteisto sijaitsee suomessa sellaisissa tiloissa, joiden fyysinen suojaus vastaa vähintään viestintäviraston määräyksen teleyritysten tilojen ja televerkkojen fyysisestä suojaamisesta (THK 48/1999 M) vaatimuksia ”erittäin tärkeille tiloille”.

6.1.2 Fyysinen pääsynvalvonta

Asiattomien pääsy tiloihin, joissa sijaitsee varmennepalvelun tuottamisessa käytettyjä laitteistoja, on estetty. Oman henkilöstön lisäksi ainoastaan eri laitteiden huoltohenkilöstö ja siivoojat pääsevät laitetiloihin ja hekin vasta, kun ovat todistaneet henkilöllisyytensä ja käyntinsä tarpeellisuuden. Mikäli henkilölle ei ole myönnetty pysyvää henvkilökohtaista kulkuoikeutta, hän voi liikkua tiloissa ainoastaan jonkun kulkuun oikeutetun henkilön seurassa.

Laitetiloissa käyvien henkilökuntaan kuuluvien henkilöiden kulku on järjestetty siten, että jokaisella on omana työaikanaan pääsy vain niihin tiloihin, joissa hänen työtehtäviensä takia tarvitsee oleskella. Henkilöstön käyntejä seurataan säännöllisesti kulunvalvontajärjestelmän lokitiedoista.

Kulunvalvonta varmistuksia sisältäviin tiloihin on järjestetty siten, ettei kukaan voi päästä sinne ilman, että käynnistä jää merkintä kulunvalvontajärjestelmään.

6.1.3 Sähkönsyöttö ja ilmastointi

Varmennusjärjestelmän keskeytymätön toiminta varmistetaan katkeamattoman virran-syöttöjärjestelmän ja varavoimalaitteiden avulla. Laitetiloissa on ilmastointijärjestelmä, jonka tuottaman ilman lämpötilaa ja kosteutta seurataan.

6.1.4 Vesivahingoilta suojautuminen

Laitetilaa valvotaan kosteusilmaisimilla. Laitetiloissa on korotettu lattia ja vedenpoistojärjestelmä vesivuotojen varalle.

6.1.5 Paloturvallisuus

Laitetilat kuuluvat automaattisen palohälytysjärjestelmän piiriin. Tilat on varustettu palonilmaisimilla. Lisäksi hätätilanteiden varalta ylläpidetään ensisammutusryhmää.

6.1.6 Tietomateriaalin säilytys

Tietovälineet, joille on tallennettu varmenteiden tuotantojärjestelmään liittyvää tai siinä syntyvää tietoa, varastoidaan samoissa turvallisissa tiloissa, joissa itse järjestelmä sijaitsee. Ks. myös kappale 6.1.8 ”Toisaalla säilytettävät turvakopiot”.

6.1.7 Jätemateriaalin hävittäminen

Varmennusjärjestelmän levyt, magneettinauhat ja asennuslevykkeet varmuuskopioineen, joita ei varastoida pysyvästi varmenteiden tuotantotiloihin, hävitetään turvallisesti niiden tultua tarpeettomiksi.

6.1.8 Toisaalla säilytettävät turvakopiot

Varmennusjärjestelmän tuottamista lokitiedoista otetaan varmuuskopiot, jotka säilytetään varmentajan tuotantotiloista erillään sijaitsevissa tiloissa. Näiden tilojen suojaus on samantasoinen kuin varmentajan tuotantotilojen suojaus.

6.2 TOIMINNALLISET TURVARATKAISUT

6.2.1 Luotetut toimenhaltijat

- luotetuilla toimenhaltijoilla on seuraavanlaisia vastuita:
- tietoturvallisuusvastaava; kokonaisvastuu turvakäytäntöjen toteutuksen hallinnasta
- järjestelmän pääkäyttäjä; varmenteiden luontiin, Varmenteiden mitätöintiin liittyvien varmentajan luotettavien järjestelmien konfigurointi, ylläpito ja asennustilaukset sekä vianselvitykset ja varmentajan yksityisten avainten hallintatoimenpiteet
- järjestelmän ylläpitäjä; varmentajan luotettavan järjestelmän päivittäinen käytönvalvonta, varmuuskopioiden ottaminen, varajärjestelmän käyttöönotto ja toipumisen hallinta sekä tilausten mukaiset asennukset ja järjestelmätason vianselvitykset
- järjestelmän arvioija; varmentajan luotettavien järjestelmien arkistojen ja tarkastuslokien ylläpito ja tarkistaminen
- rekisteröintivastaava; varmenteiden luontiin tarvittavien tietojen kerääminen ja rekisteröiminen
- varmentajan sulkupalveluvastaava; varmenteiden mitätöintiin ja Sulkulistaan liittyvien toimenpiteiden hyväksyntä.
- luotetut toimenhaltijat sijoittuvat varmennustoiminnan eri osapuolten vastuulle kuuluviin tehtäviin seuraavan taulukon mukaisesti.

Luotettu toimenhaltija	**Varmennustoiminnan osapuoli**
Tietoturvallisuusvastaava	Varmentaja, Varmennetuotanto
Järjestelmän pääkäyttäjä	Varmennetuotanto
Järjestelmän ylläpitäjä	Varmennetuotanto
Järjestelmän arvioija	Varmentaja, Varmennetuotanto
Rekisteröintivastaava	Palvelusopimuksen haltija
Varmentajan sulkupalveluvastaava	Varmentaja
Sopimusten sulkupalveluvastaava	Sulkupalvelusta vastaava ulkoinen toimija

Luotetuissa rooleissa toimivat henkilöt sitoutuvat noudattamaan tätä varmennuskäytäntöä.

6.2.2 Tehtäviin vaadittavien henkilöiden lukumäärät

Varmentaja huolehtii siitä, että jokaista tehtävää kohden on palkattu riittävästi henkilöstöä ja että yksittäiset henkilöt eivät voi toimia kaikissa rooleissa samanaikaisesti.

Tiettyihin toimenpiteisiin vaaditaan usean henkilön yhtäaikainen osallistuminen. Muu-tosten toteuttaminen sekä Varmentajan Yksityisen avaimen varmuuskopiointi ja palauttaminen Varmentajan tuotantojärjestelmäympäristöön vaatii vähintään kahden henkilön osallistumisen. Varmentajan Yksityisen avaimen luonti edellyttää vähintään neljän henkilön paikallaoloa.

6.2.3 Luotettujen toimenhaltijoiden tunnistaminen ja todentaminen

Seuraavien toimenhaltijoiden tunnistamiseen vaaditaan Varmenne:

- Järjestelmän pääkäyttäjä
- Varmentajan sulkupalveluvastaava

Alla lueteltujen toimenhaltijoiden tunnistamisessa käytetään pääsääntöisesti käyttäjä-tunnusta ja salasanaa. Silloin kun luotettuun toimeen kuuluvien velvollisuuksien hoitaminen edellyttää varmentajan kriittisimpien järjestelmien käyttöä, kirjautuminen näihin edellyttää myös alla luetelluissa rooleissa toimivilta varmenteeseen pohjautuvaa tunnistamista.

- Tietoturvallisuusvastaava
- Järjestelmän ylläpitäjä
- Järjestelmän arvioija

6.3 HENKILÖTURVALLISUUS

6.3.1 Taustatietojen tarkastusmenettely

Seuraaville toimenhaltijoille suoritetaan taustatietojen tarkistaminen:

- Tietoturvallisuusvastaava
- Järjestelmän pääkäyttäjä

Muutoin Varmentaja ja mahdollinen varmennetuotannosta vastaava alihankkija tarkistuttavat työntekijöidensä taustatiedot harkintansa mukaan riippuen työntekijän roolista varmennepalvelujen tuotannossa.

6.3.2 Koulutusvaatimukset

Varmentajan ja mahdollisen varmennetuotannosta vastaavan alihankkijan uudet työntekijät perehdytetään varmennustoimintaan yleisesti, siihen liittyviin turvallisuusvaatimuksiin sekä erityisesti omiin työtehtäviinsä. Käsiteltävään aineistoon kuuluu mm. tietoturvaperiaatteet, varmenneperiaatteet ja varmennuskäytäntö. Tarvittaessa järjestetään henkilön työtehtäviin ja rooliin sovitettu yksilöllinen perehdyttäminen ja koulutus.

Työntekijöille järjestetään tarvittaessa täydennyskoulutusta.

6.3.3 Seuraukset luvattomista toimenpiteistä

Jos Varmentaja tai mahdollinen Varmennetuotannosta vastaava alihankkija havaitsee väärinkäytöksen, siihen syyllistynyt työntekijä siirretään välittömästi toisiin tehtäviin ja kaikki hänen pääsyoikeutensa varmennustoimintaan liittyviin järjestelmiin peruutetaan. Jatkotoimenpiteiden suhteen noudatetaan Varmentajan ja kyseisen alihankkijan voimassa olevia käytäntöjä.

6.3.4 Sopimustyöntekijävaatimukset

Sopimustyöntekijöiden vaatimukset ovat samat kuin vakinaisenkin henkilöstön vaatimukset.

7 TEKNISET TURVARATKAISUT

Tämä luku sisältää julkisten ja yksityisten avainten hallintaperiaatteiden ja niihin liittyvän teknisen valvonnan vaatimukset, jotka koskevat varmentajaa, mahdollista varmennetuotannosta vastaavaa alihankkijaa, muita mahdollisia alihankkijoita ja varmenteen haltijoita.

7.1 VARMENTAJAN AVAINPARIN LUOMINEN, KÄYTTÖÖNOTTO JA SUOJAAMINEN

7.1.1 Varmentajan avainparin luominen

Varmentajan avainparin luonti tapahtuu varmentajan hyväksymän avaintenluontiproseduurin mukaisesti. Avainpari luodaan varmennetuotannon fyysisesti suojatuissa tiloissa varmennusjärjestelmää hyväksi käyttäen korkean turvatason HSM-laitteessa (ks. kappale 7.1.6 ”Varmentajan yksityisen avaimen suojaaminen”). Avaintenluontiin osallistuvat henkilöt ovat luotettuja toimenhaltijoita, jotka on valtuutettu tähän tehtävään ja joista vähintään kahden on oltava paikalla. Lisäksi vähintään kahden varmentajan valtuuttaman valvojan on oltava paikalla. Avaintenluontiproseduurin toimenpiteet kirjataan pöytäkirjaan, ja jokainen proseduuriin osallistuva henkilö vahvistaa pöytäkirjan allekirjoituksellaan. Pöytäkirja säilytetään kappaleen 5.7 ”Tietojen arkistointi” mukaisesti.

7.1.2 Varmentajan Julkisen avaimen toimittaminen Luottaville osapuolille

Varmentajan julkinen avain on saatavilla varmentajan ja pankkien käytössä olevilta intranet-sivuilta sekä julkisesta Web-sivustosta, jossa julkaistaan varmentajan itsensä allekirjoittama varmentajan julkisen avaimen varmenne sekä varmenteen tiiviste, ns. sormenjälki.

7.1.3 Varmentajan avainten pituudet ja käytetty algoritmi

Varmentaja käyttää varmenteiden ja sulkulistatietojen allekirjoittamiseen RSA-algoritmiin perustuvaa allekirjoitusavainta, jonka pituus on vähintään 4096 bittiä.

7.1.4 Varmentajan avainparin käyttöikä

Varmentajan yksityisen avaimen käyttöikä on korkeintaan 25 vuotta. Käyttöikä ei voi olla pidempi kuin avaimeen liittyvän varmentajan varmenteen voimassaoloaika. Mikäli varmenteen haltijan varmenne mitätöidään, sulkulista allekirjoitetaan samalla avaimella, jolla kyseinen varmenne on allekirjoitettu. Avainta on voitava käyttää siihen liittyvän varmenteen voimassaoloaikana viimeisenkin sillä allekirjoitetun varmenteen haltijan varmenteen mitätöintiin koko tämän varmenteen voimassaoloajan. Avainta voidaan siis käyttää varmenteen haltijoiden varmenteiden allekirjoittamiseen avaimen käyttöiän ajan vähennettynä pisimmällä varmenteen haltijan

Varmenteen voimassaoloajalla. Tämän jälkeen varmentajalle täytyy luoda uusi avainpari varmenteiden allekirjoitukseen.

7.1.5 Varmentajan avainten käyttötarkoitukset

Varmentajan allekirjoitusavaimia voidaan käyttää vain varmentajan fyysisesti suojatuissa tiloissa luotettujen toimenhaltijoiden valvonnassa käyttäen varmennusjärjestelmää ja kappaleessa 7.1.6 ”Varmentajan Yksityisen avaimen suojaaminen” määriteltyä HSM-laitetta.

Varmentajan Julkisen avaimen käyttötarkoitukset, jotka on ilmoitettu Varmentajan Varmenteen “key usage”-kentässä, ovat:

- keyCertSign (Varmentajan allekirjoituksen tarkistaminen varmenteen haltijoiden varmenteista)
- CRLSign (Varmentajan julkaisemien sulkulistatietojen allekirjoituksen tarkistaminen).

HUOM. Varmentaja voi käyttää allekirjoitusavaimiaan varmenteiden myöntämiseen myös juurivarmentajana, jolloin myönnetyn varmenteen haltija on toinen varmentaja.

7.1.6 Varmentajan yksityisen avaimen suojaaminen

Varmennetuotanto on toteuttanut varmentajan yksityisen allekirjoitusavaimen suojaamisen fyysisten suojausten, määriteltyjen proseduurien, pääsynvalvonnan ja käyttöoikeuksien yhdistelmällä.

Turvallisissa fyysisesti suojatuissa tiloissa sijaitsevaan varmennusjärjestelmään kuuluu HSM-laite (Hardware Security Module), jolla varmentajan allekirjoitusavain on suojattu. HSM-laite noudattaa vähintään FIPS 140-2 level 2 -standardia.

Varmennetuotanto huolehtii teknisen valvonnan ja määriteltyjen proseduurien avulla, että kukaan ei yksinään saa haltuunsa keinoja siihen ympäristöön pääsemiseksi, jossa yksityinen avain on tallennettuna, tai pysty käyttämään avainta millään tavalla. Kriittisiä allekirjoitusavaimeen liittyviä toimenpiteitä, kuten avaimen tallennus, varmistus ja palautus, on suorittamassa aina useampi kuin yksi henkilö.

Avaimen palautus edellyttää sellaisen aktivointitiedon käyttöä, joka on tallennettu osiin jaettuna erillisiin turvallisiin tiloihin ja jonka haltuun saanti on hajautettu varmentajan

määrittelemälle määrälle luotettuja toimenhaltijoita. Avaimen palauttaminen edellyttää, että palautusproseduuriin osallistuu vähintään kaksi luotettua toimenhaltijaa ja kaksi varmentajan valtuuttamaa valvojaa.

7.1.7 Varmentajan yksityisen avaimen tallentaminen kolmannen osapuolen toimesta

Varmentajan yksityiselle avaimelle ei suoriteta key escrow –tyyppistä kopiointia ja tallennusta missään olosuhteissa.

7.1.8 Varmentajan yksityisen avaimen varmuuskopiointi

Varmentajan yksityisen allekirjoitusavaimen tuhoutumisen varalta on olemassa järjestely sen palauttamiseksi. Varmentajan yksityisen avaimen tulee olla varmuuskopioissa salatussa tai jaetussa muodossa. Varmuuskopioiden fyysisessä käsittelyssä tulee olla läsnä varmennetuotannon kaksi luotettua toimenhaltijaa.

7.1.9 Varmentajan yksityisen avaimen arkistointi

Varmentajan yksityistä avainta ei arkistoida.

7.1.10 Varmentajan yksityisen avaimen aktivointi

Varmentajan yksityisen avaimen aktivointi sisältyy kappaleen 7.1.1 ”Varmentajan avainparin luominen” mukaiseen proseduuriin. Aktivointi tapahtuu luotetun toimenhaltijan toimesta sen jälkeen kun varmennusjärjestelmä on tunnistanut toimenhaltijan vahvalla tunnistamismekanismilla. Avain säilyy varmennusjärjestelmässä aktiivisena, kunnes sen käyttö keskeytetään esim. huoltotoimenpiteiden takia.

7.1.11 Varmentajan yksityisen avaimen deaktivointi

Varmentajan yksityinen avain voidaan deaktivoida luotetun toimenhaltijan toimesta.

7.1.12 Varmentajan yksityisen avaimen tuhoaminen

Kun varmentajan yksityisen avaimen käyttö lopetetaan, sen kaikki kopiot tuhotaan tai niitä säilytetään siten, että niiden käyttö on estetty.

7.1.13 Varmentajan julkisen avaimen arkistointi

Varmentaja arkistoi voimassa olevat ja vanhentuneet Varmentajan Julkiset avaimet kappaleen 5.7 ”Tietojen arkistointi” mukaisesti.

7.2 VARMENTEEN HALTIJAN AVAINPARIN LUOMINEN, KÄYTTÖÖNOTTO JA SUOJAAMINEN

7.2.1 Varmenteen haltijan avainparin luominen

Varmenteen haltija huolehtii tilaamiinsa Varmenteisiin liittyvien Avainparien luonnista omilla komponenteillaan ja näiden komponenttien tarjoaman turvatason mukaisesti.

7.2.2 Varmenteen haltijan julkisen avaimen toimittaminen varmentajalle

Varmenteen haltija vastaa laitteen tai palvelinsovelluksen käyttöön tulevan Julkisen avaimen turvallisesta toimittamisesta Varmentajalle.

7.2.3 Varmenteen haltijan avainten pituudet ja käytetty algoritmi

Varmenteen haltijoiden käytössä olevien RSA-algoritmin yhteydessä käytettävien avainten pituus on vähintään 2048 bittiä.

7.2.4 Varmenteen haltijan Avainparin käyttöikä

Varmenteen voimassaoloaika määrää Varmenteen haltijan Julkisten ja Yksityisten avainten käyttöiän, joka on korkeintaan kaksi (2) vuotta. Avaimia ei varmenneta uudelleen, kun niihin liittyvien Varmenteiden voimassaoloaika on päättymässä.

7.2.5 Varmenteen haltijan avainten käyttötarkoitukset

Varmenteen haltijan yksityisiä avaimia voidaan käyttää ainoastaan sellaisiin tarkoituksiin, jotka vastaavat asianomaisten varmenneperiaatteiden kappaleen 8.1. ”Varmenne-profiilit” taulukoissa mainittuja julkisten avainten käyttötarkoituksia.

7.2.6 Varmenteen haltijan yksityisen avaimen suojaaminen

Varmenteen haltijan tulee suojata varmenteeseen liittyvä yksityinen avain.

7.2.7 Varmenteen haltijan yksityisen avaimen arkistointi

Varmenteen haltijan yksityistä avainta ei arkistoida varmentajan toimesta.

7.2.8 Varmenteen haltijan yksityisen avaimen tuhoaminen

Varmenteen haltija huolehtii varmenteeseen liittyvän yksityisen avaimen tuhoamisesta varmenteen elinkaaren päättymisen jälkeen.

7.2.9 Varmenteen haltijan Julkisen avaimen arkistointi

Varmentaja arkistoi Varmenteen haltijan Julkisen avaimen kappaleen 5.7 ”Tietojen arkistointi” mukaisesti.

7.3 TIETOJÄRJESTELMIEN TURVARATKAISUT

Tietojärjestelmien tietoturvan ylläpidossa noudatetaan Varmentajan tietoturvallisuusperiaatteiden vaatimuksia.

7.3.1 Tietojärjestelmien turvaluokitus

Varmennetuotannon järjestelmien turvaluokituksessa noudatetaan Varmennetuotannos-ta vastaavan alihankkijan määrittelemää monitasoista tietojärjestelmien turvaluokituskäytäntöä.

7.3.2 Tietojärjestelmän käyttäjien tunnistaminen ja pääsynvalvonta

Pääsynvalvonnalla huolehditaan eri luotettujen toimenhaltijoiden tunnistamisesta ennen järjestelmiin pääsyä (ks. kappale 6.2.3 ”Luotettujen toimenhaltijoiden tunnistaminen ja todentaminen”). Järjestelmät tarjoavat myös eri käyttäjien tekemien toimenpiteiden jäljitettävyyden.

7.3.3 Usean henkilön osallistumista vaativat toimenpiteet

Tiettyjen varmennusjärjestelmään liittyvien toimenpiteiden suorittaminen edellyttää useamman henkilön osallistumista (ks. kappale 6.2.2 ”Tehtäviin vaadittavien henkilöiden lukumäärät”).

7.3.4 Kapasiteetin valvonta

Järjestelmän resurssien käyttö on jatkuvassa seurannassa ja automaattinen valvontajärjestelmä antaa hälytyksen asetettujen rajojen ylittyessä.

7.3.5 Tietoturvallisuuden valvontaan liittyvät vaatimukset

Varmentajan järjestelmien ja toiminnan tietoturvallisuuteen liittyvät vaatimukset on kuvattu kappaleessa 5.6 ”Tietoturvallisuuden valvonta”.

7.3.6 Poikkeustilanteiden hoito

Erilaisten poikkeustilanteiden varalta on määritelty raportointimenettelyt ja toimenpidesuunnitelmat.

7.3.7 Tietoaineistoon liittyvät turvavaatimukset

Tallenteiden varastointi, arkistointi ja tarpeettomaksi tulleen tietoaineiston käsittely on kuvattu kappaleissa 6.1.6 ”Tietomateriaalin säilytys” ja 6.1.7 ”Jätemateriaalin hävittäminen”.

7.4 ELINKAAREN HALLINNAN TURVARATKAISUT

7.4.1 Järjestelmäkehityksen hallinta

Varmennetuotannon järjestelmäkehityksessä käytetään erillistä testausympäristöä, jossa kehitystyön tuloksena syntyneet muutokset testataan ennen niiden vientiä tuotantojärjestelmään.

Kaikki tuotantoon vietävät järjestelmän muutokset dokumentoidaan huolellisesti.

7.4.2 Tietoturvallisuuden hallinta

7.4.2.1 Tietoturvallisuuden ylläpito

Varmentaja noudattaa kaikessa toiminnassaan laatimiaan tietoturvaperiaatteita, Varmenneperiaatteita ja tätä Varmennuskäytäntöä. Toiminnan tarkastuksia on kuvattu kappaleessa 3.7 ”Tarkastukset”.

Varmentaja huolehtii sopimuksin tietoturvan säilymisestä ulkoistettujen toimintojen osalta sekä määriteltyjen periaatteiden ja käytäntöjen noudattamisesta alihankkijoita käytettäessä.

7.4.2.2 Resurssien hallinta

Varmentaja ja mahdollinen Varmennetuotannosta vastaava alihankkija noudattavat käyttämiensä resurssien sekä tuottamansa ja käyttämänsä tiedon suojauksessa laatimiaan tietoturvaperiaatteita.

7.4.2.3 Käyttöpalvelun hallinta

Käyttöpalvelun hallinta perustuu Varmentajan ja mahdollisen Varmennetuotannosta vastaavan alihankkijan tietoturvaperiaatteiden toteuttamiseen, laadittujen ohjeistusten noudattamiseen ja alihankkijoiden kanssa tehdyissä sopimuksissa määriteltyjen vastuiden toteuttamiseen sekä tietoturvaperiaatteiden, ohjeistuksen ja vastuiden edellyttämän toiminnan valvontaan.

7.4.2.4 Järjestelmien pääsynvalvonta

Varmentajan ja Varmennetuotannon järjestelmien käyttöoikeuksien hallinnassa ja pääsynvalvonnassa noudatetaan tietoturvaperiaatteita ja määriteltyjä käytäntöjä. Eri järjestelmien käyttöoikeuksien hallintaa hoitavat erikseen tätä tehtävää varten valtuutetut henkilöt.

7.4.2.5 HSM-laitteen elinkaaren hallinta

Varmennetuotanto on laatinut ohjeen Varmenteiden ja Sulkulistojen allekirjoitukseen käytettävän HSM-laitteen elinkaaren hallintamenettelystä Varmenneperiaatteissa määriteltyjen vaatimusten toteuttamiseksi.

7.5 TIETOLIIKENNEVERKON TURVARATKAISUT

Varmennusjärjestelmä on erotettu julkisesta verkosta palomuurein. Kriittisimmät järjestelmän osat on täysin erotettu julkisesta verkosta. Käytössä on myös hyökkäyksen-tunnistusjärjestelmä.

Varmentajan järjestelmän osien välisessä liikenteessä käytetään vahvaa tunnistusta sekä salausta.

8 VARMENNE- JA SULKULISTAPROFIILIT

8.1 VARMENNEPROFIILIT

Kaikki näiden varmenneperiaatteiden mukaisesti myönnetyt varmenteet noudattavat X.509–standardia. Varmenteet täyttävät dokumentin RFC 5280 ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile" vaatimukset.

Varmenteet noudattavat X.509 –standardin versiota 3 ja niissä käytetään seuraavia standardissa määriteltyjä varmennelaajennuksia:

- Varmentajan Julkisen avaimen tunniste (Authority key identifier)
- Varmenteen haltijan Julkisen avaimen tunniste (Subject key identifier)
- Sulkulistan julkaisupaikka (CRL distribution points)
- Avaimen käyttötarkoituksen laajennus (Extended key usage)

X.509-standardi sallii myös itse määritellyt varmennelaajennukset. Varmenteissa ei käytetä yksityisiä varmennelaajennuksia.

Varmennelaajennus määritellään kriittiseksi, kun varmennetta hyödyntävän järjestelmän halutaan hylkäävän varmenteen, mikäli se ei tunnista kriittiseksi määriteltyä laajennusta. Mitään yllä mainituista laajennuksista ei ole määritelty kriittiseksi.

Varmenneperiaatteille on haettu virallinen tunnistenumero (OID)ja varmenteessa on viittaus varmenneperiaatteisiin.

8.1.1 CA-varmenne

Samlink Customer CA-järjestelmään liittyy yksi CA-varmenne, jossa käytetään seuraavia kenttiä:

Kentän nimi	Field name	Kentän sisältö
Versio	Version	3
Sarjanumero	Serial number	80:8e:c2:f0:14:25:e2:a3:99:01:a5:12:06:71:19:39
Allekirjoitusalgoritmi	Signature algorithm	sha256WithRSAEncryption

Varmenteen myöntäjä	Issuer	C=FI, O=Samlink, CN=Samlink Customer CA
Voimassaoloaika	Validity	Not Before: Aug 18 08:00:35 2009 GMT Not After : Aug 18 08:00:35 2034 GMT
Varmenteen haltija	Subject	C=FI, O=Samlink, CN=Samlink Customer CA
Varmenteen haltijan julkisen avaimen tiedot	Subject public key info	Public Key Algorithm: rsaEncryption RSA Public Key: (4096 bit)
Varmentajan julkisen avaimen tunniste	Authority key identifier	keyid:CA:80:38:33:93:8A:63:04:91:8D:05:69:56:68:42:35:E5:C7:FF:BC
Varmenteen haltijan julkisen avaimen tunniste	Subject key Identifier	CA:80:38:33:93:8A:63:04:91:8D:05:69:56:68:42:35:E5:C7:FF:BC
Avaimen käyttötarkoituksen laajennus	Key usage	critical Digital Signature, Certificate Sign, CRL Sign

8.2 SULKULISTAPROFIILI

CRL-listat julkaistaan CA-järjestelmästä varmennetuotannon ylläpitämään julkiseen hakemistoon, johon on viite varmenteiden CDP-kentässä (ks. arvot varmennemäärittelystä).

Julkaisut tehdään salatulla LDAPS-protokollalla. Lähdeosoite on jokin arvoista 62.71.12.240-242.

CRL-listat muodostetaan aina täydellisinä normaalilla PKIX-standardin versio2-formaatilla siten että tiivistealgoritmina on SHA256. Käytetyt kentät ovat:

Kentän nimi	**Field name**	**Kentän sisältö**
Versio	Version	V2
Allekirjoitus-algoritmi	Signature algorithm	SHA256
Sulkulistan julkaisija	Issuer	• CN = Samlink Customer CA • O = Samlink • C = FI
Sulkulistan julkaisuaika	Effective date	CRL:n luomishetki
Seuraavan sulkulistan julkaisuaika	Next update	CRL:n voimassaolon päättymishetki (5 vrk luomishetkestä)
Mitätöidyt varmenteet	Revoked certificates	
Sulkulistan allekirjoitus-avaimen tunniste	Authority key identifier	ca 80 38 33 93 8a 63 04 91 8d 05 69 56 68 42 35 e5 c7 ff bc
Sulkulistan järjestysnumero	CRL number	Juokseva CRL:n järjestysnumero

CRL-listoista automaattisesti poistetaan PKIX-suosituksen mukaisesti vanhentuneiden varmenteiden sarjanumerot.

9 VARMENNUSKÄYTÄNNÖN HALLINNOINTI

9.1 MUUTOSMENETTELY

Aina kun varmenneperiaatteisiin tehdään muutoksia tai kirjoitetaan uudet varmenne-periaatteet, uusien vaatimusten vaikutukset varmennuskäytäntöön arvioidaan. Samlinkin turvallisuusosasto vastaa arvioinnin käynnistämisestä. Dokumentin muuttamiseen voi olla myös muita varmenneperiaatteisiin liittyvistä muutoksista riippumattomia syitä. Mikäli dokumenttiin tehdään hyväksyjien mielestä vähämerkityksinen muutos, dokumentin revisionumeroa (desimaaliosa) kasvatetaan. Mikäli muutos on suurempi, dokumentin versionumeroa (kokonaisosa) kasvatetaan.

Vähämerkityksinen muutos voi astua voimaan välittömästi, kun se on hyväksytty ja muutos on viety varmennuskäytäntöön. Suuremmasta muutoksesta ilmoitetaan vähintään 15 päivää ennen sen voimaantuloa niille, joiden toimintaan se vaikuttaa.

9.2 HYVÄKSYMISMENETTELY

Kaikki muutokset tähän varmennuskäytäntöön, lukuun ottamatta ulkoasuun, oikeinkirjoitukseen tai yhteystietoihin liittyviä muutoksia, täytyy hyväksyä Samlink PKI-ohjausryhmässä.

9.3 JULKAISEMINEN

Varmennuskäytäntö asetetaan niiden osapuolten saataville, joiden edellytetään noudattavan sitä.

Varmennuskäytäntö julkaistaan osapuolille, joiden edellytetään noudattavan sitä, Samlinkin ja pankkien käytössä olevissa intranet-sivustoissa , julkisessa Web-sivustossa tai muulla erikseen sovitulla tavalla.

Myös aikaisemmat voimassa olleet Varmennuskäytännön versiot ovat saatavissa edellä mainituista osoitteista vähintään kunkin Varmenneperiaatteiden mukaan myönnettyjen Varmenteiden elinkaaren päättymiseen asti.

Samlinkin ja pankkien käytössä olevissa intranet-sivustoissa voidaan julkaista myös muita mahdollisia Varmennepalveluun liittyviä kuvauksia ja ohjeita.