Samlink Customer CA

Versio 1.0

18.09.2009

**Voimassa 22.09.2009 alkaen**

# Samlink Customer CA - Varmenneperiaatteet

WS-Aineistopalvelut varmenteita varten
OID: 1.2.246.558.10.09704098.11.2.

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. |
| CRL | Certificate Revocation List. Sulkulista, mitätöintilista, revokointilista. Lista käytöstä poistetuista varmenteista. |
| FIPS | Federal Information Protection Standard. FIPS-140-1 ja FIPS-140-2 ovat salausmoduuleita ja -algoritmeja koskevia tietoturvavaatimuksia. |
| Hakemisto | Tietovarasto, johon julkaistaan sulkulistat. Hakemisto on käytettävissä julkisessa tietoverkossa. |
| HSM-laite | Hardware Security Module. Salausavainten suojaamiseen tarkoitettu erikoislaite. |
| 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). |
| LDAP | Lightweight Directory Access Protocol. Hakemistokäyttöön tarkoitettu standardi rajapinta. |
| Luottava osapuoli | Varmentajan toimintaan ja sen luomiin varmenteisiin luottava sekä niitä hyödyntävä taho. |
| OID | Object Identifier. Globaalisti yksikäsitteinen tunnistenumero. |
| Palvelinhallinta | Samlinkin tai Samlinkin asiakasyrityksen infrasta vastuussa oleva organisaatio. |
| Palvelinsovellus | Sovellus, jolla voidaan allekirjoittaa, salata ja käsitellä maksuaineistoja varmenteita käyttäen. |
| PKI | Public Key Infrastructure. Varmentajan toimintaan liittyvien teknisten ja hallinnollisten ratkaisujen kokonaisuus. |
| PUK | PIN Unblocking Key. Lukkiutuneen toimikortin avaamiseen käytettävä koodi. |
| Rekisteröijä | Taho, joka vastaa rekisteröinnistä. Tyypillisesti rekisteröijä on pankki toimiessaan Web Services-yhteyssopimusten haltijana. Rekisteröijä voi olla myös Samlink. |
| Rekisteröinti | Prosessi, joka sisältää varmenteen haltijan tunnistamisen, tarvittavien tietojen keräämisen ja niiden toimittamisen varmennepyyntöä varten. Rekisteröintiin voi liittyä useita rekisteröintivastaavia. |

| | |
|---|---|
| Rekisteröintivastaava | Henkilö, joka vastaa rekisteröintitehtävistä, esim. varmennepyyntöjen oikeellisuuden tarkastamisesta ja varmenteiden luovuttamisesta varmenteiden haltijalle. Rekisteröintivastaavana toimiminen edellyttää pankin ja varmentajan välistä sopimusta tehtävän hoitamisesta pankissa sekä toimihenkilöltä erillistä palvelusopimuskäyttövaltuutta. Rekisteröintivastaavana voi olla myös varmentajan luotetuksi toimenhaltijaksi nimeämä henkilö. |
| RFC | Request For Comments. Kokoelma standardeja, jotka mm. määrittelevät vaatimuksia varmentajan toiminnalle. |
| RSA | Epäsymmetrinen salausalgoritmi, joka perustuu avainparien käyttöön. |
| Sopimusten haltija | Pankki, jonka kanssa asiakas tekee pankkiyhteyssopimuksen sekä Web Services-yhteyssopimuksen |
| Sulkulista | Kts. CRL |
| Sulkupalvelu | Web Services-yhteys sopimusten ja varmenteiden sulkupyyntöjä vastaanottava taho. |
| Toimikortti | Turvallinen väline yksityisten avainten tallettamiseen. Yksityisiä avaimia käytetään ainoastaan toimikortilla. Käyttö edellyttää avaimen aktivointia PIN-luvulla. Toimikortilla säilytetään myös myönnettyjä varmenteita. |
| Varmenne | Varmenteen haltijan nimestä ja julkisesta avaimesta muodostettu tieto, jonka varmentaja on allekirjoittanut sähköisesti. Varmenne todistaa tietyn julkisen avaimen kuuluvan tietylle haltijalle. |
| Varmennuskäytäntö | Kuvaa varmentajan toiminnan varmenneperiaatteita noudattaen. |
| Varmennepalvelu | Varmenteiden tuottamiseen liittyvät järjestelmät, henkilöit ja prosessit kokonaisuutena. Varmennepalvelun osatoimintoja ovat rekisteröinti, varmennetuotanto, korttituotanto, hakemistopalvelu, sulkupalvelu ja sulkulistapalvelu. |
| Varmenneperiaatteet | Kuvaa vaatimukset varmenteiden myöntämiselle, tuottamiselle ja käytölle. |
| Varmennepyyntö | Korttituotannon tai rekisteröijän varmennetuotantoon lähettämä, varmenteen hakijan tiedot ja julkisen avaimen sisältävä pyyntö varmenteen tuottamisesta. |
| Varmennetuotanto | Varmennetuotanto hallinnoi varmennusjärjestelmää, tuottaa varmenteet ja ylläpitää niiden tilatietoa. |
| Varmentaja | Varmennepalvelusta vastuussa oleva organisaatio. |
| Varmenteen hakija | Henkilö, jolle haetaan varmennetta, tai henkilö, joka on valtuutettu hakemaan varmennetta tietoverkon elementille. |
| Varmenteen haltija | Varmenteessa annettua julkista avainta vastaavan yksityisen avaimen haltija, joka on nimetty varmenteessa. |
| Varmenteeseen luottava osapuoli | Varmenteeseen luottavalla osapuolella tarkoitetaan tahoa, joka asioinnissaan luottaa varmenneperiaatteiden mukaisiin varmenteisiin |
| Web Services-yhteyssopimus | Varmenteen haltijan (asiakas) ja sopimusten haltijan (pankki) välinen sopimus, joka on edellytyksenä WS-Aineistopalvelut -varmenteen tilaukselle. |

| | |
|---|---|
| Yksityinen avain | Ainoastaan haltijansa haltuun ja käyttöön tarkoitettu avain. Yksityistä avainta käyttäen voidaan lukea haltijalle tarkoitetut, vastaavalla julkisella avaimella salatut tiedot. Yksityisellä avaimella voidaan myös luoda haltijan sähköinen allekirjoitus. |
| X.509 | Standardi, joka kuvaa varmennepalvelun vaatimuksia ja komponentteja. |

# 2 JOHDANTO

Nämä Samlink Customer CA Varmenneperiaatteet (jäljempänä varmenneperiaatteet) ovat Oy Samlink Ab:n (jäljempänä. Samlink) laatima säännöstö WS-Aineistopalvelut -varmenteiden myöntämiseen sekä näiden varmenteiden käyttämiseen.

Varmenneperiaatteet kattavat pääosin Internet Engineering Task Forcen standardin RFC 3647 suosittelemat varmenteen luotettavuuteen ja tuottamiseen liittyvät sisällölliset asiat.

### 2.1 YLEISKUVAUS

Varmenneperiaatteita sovelletaan WS-Aineistopalvelut varmenteisiin.

Samlink toimii varmenneperiaatteiden mukaisten varmenteiden varmentajana. Varmentaja voi käyttää toiminnassaan alihankkijoita.

Varmentajan on laadittava kuvaus varmenneperiaatteita noudattavista varmennuskäytännöistään.

## 2.2 TUNNISTEET

Tämän dokumentin tunniste on Samlink Customer CA Varmenneperiaatteet WS-Aineistopalvelut varmenteita varten, (OID 1.2.246.558.10.09704098.11.2, v.1.0)

Varmenneperiaatteista voidaan julkaista uusia versioita. Varmenneperiaatteiden kansilehdellä on ilmoitettu kyseisen version voimaantuloaika. Dokumentin tämä ja kaikki edeltävät julkaistut versiot ovat luettavissa Samlinkin ja pankkien käytössä olevilta intranet-sivuilta sekä Web Services-yhteyssopimuksella kerrotulla jakelulla.

### 2.3 VARMENTEEN JA SITÄ VASTAAVIEN VARMENNEPERIAATTEIDEN YHTEYS

Varmenteen haltija voi varmistua varmenteen olevan näiden varmenneperiaatteiden mukainen tarkistamalla että varmenteen sisältö on tässä dokumentissa kappaleessa 8. ”Varmenne- ja sulkulistaprofiilit” määritellyn varmenneprofiilin mukainen ja että varmenne on luotu näiden varmenneperiaatteiden voimassaoloaikana..

Varmenneperiaatteiden uuden version astuessa voimaan kaikki varmenteet myönnetään siitä lähtien uuden version mukaisesti. Varmenteen myöntämishetki näkyy varmenteen voimassaoloajasta, ja myöntämishetkellä voimassa ollut versio varmenneperiaatteista pätee kyseiseen varmenteeseen.

## 2.4 VARMENNUSORGANISAATIO JA VARMENTEIDEN SOVELTUVUUS

### 2.4.1 Varmentaja

Samlink toimii varmentajana, jolla on kokonaisvastuu varmennepalvelun toimittamisesta.

Varmentaja voi myöntää myös muita kuin tämän varmenneperiaatteiden mukaisia varmenteita. Näistä varmenteista laaditaan erilliset varmenneperiaatteet.

### 2.4.2 Varmennetuotanto

Varmennetuotanto on toiminto, joka hallinnoi teknistä järjestelmää, tuottaa varmenteet ja ylläpitää niiden tilatietoa.

### 2.4.3 Rekisteröijä

Rekisteröijinä voivat toimia varmentajan omaan organisaatioon kuuluvat rekisteröinti-toimintaan luotetut toimenhaltijat ja muut varmentajan mahdollisesti valtuuttamat tahot. Varmentajan valtuuttaessa muun tahon toimimaan rekisteröijänä, tehdään tästä erillinen sopimus.

Rekisteröijät sitoutuvat noudattamaan näissä varmenneperiaatteissa mainittuja rekisteröijän velvollisuuksia.

### 2.4.4 Varmenteen haltija

Varmenneperiaatteiden mukaisten varmenteiden haltijana voi toimia maksuaineistoja tai varmennejärjestelmän hallintatapahtumia tuottava, välittävä tai käsittelevä juridinen henkilö.

Varmenteen haltijan tulee noudattaa näitä varmentajan varmenneperiaatteita sekä varmentajan varmennuskäytäntöä.

### 2.4.5 Luottava osapuoli

Luottavana osapuolena, joka hyödyntää varmenneperiaatteiden mukaisesti myönnettyjä varmenteita, voi toimia maksuaineistoja tai varmennejärjestelmän hallintatapahtumia tuottava, välittävä tai käsittelevä juridinen henkilö.

Luottavan osapuolen täytyy sitoutua noudattamaan tässä dokumentissa kuvattuja velvollisuuksiaan.

### 2.4.6 Sulkupalvelu

Varmentajan sulkupalvelu on toiminto, joka suorittaa varmenteen mitätöinnin joko käyttäen automatisoitua prosessia tai suorittamalla mitätöinnin manuaalisesti käyttäen erillistä tähän tarkoitukseen tehtyä käyttöliittymää. Sulkupalvelun tulee noudattaa varmentajan varmenneperiaatteita ja varmennuskäytäntöä.

Sopimuksen sulkupalvelu on toiminto, joka suorittaa Web Services-yhteys sopimuksen sulkemisen käyttäen tähän tarkoitukseen tehtyä sovellusta. Sopimuksen sulkeminen ei sulje varmennetta, mutta sopimuksen sulkeminen estää kaikkien kyseiseen sopimukseen liittyvillä varmenteilla allekirjoitettujen tietojen käsittelyn pankin tietojärjestelmissä. Sopimuksen sulkupalvelun hoitajana toimii varmentajan valtuuttama taho, jonka tulee noudattaa varmentajan varmenneperiaatteita ja varmennuskäytäntöä.

### 2.4.7 Hakemisto

Varmennepalveluun kuuluu hakemisto, jossa julkaistaan varmenteiden sulkulista ja siihen on pääsy julkisesta verkosta.

### 2.4.8 Soveltuvuus

Varmenneperiaatteiden mukaisia varmenteita voidaan käyttää vain Samlinkin hallinnoimassa maksuaineistojen Web Services -käsittelyprosessissa, jossa varmenteita käytetään:

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

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

Tietoa, 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.

Web Services-yhteyssopimuksessa saattaa olla avainten käyttötarkoituksiin liittyviä rajoituksia, jotka täytyy ottaa huomioon varmenteita käytettäessä.

## 2.5 YHTEYSTIEDOT

Samlinkin turvallisuusosasto vastaa varmenneperiaatteiden hallinnoimisesta, ylläpidosta ja päivityksistä. Varmenneperiaatteiden tekijänoikeudet kuuluvat Samlinkille.

Varmenneperiaatteet hyväksyy Samlinkin johtoryhmän nimittämä Samlink PKI-ohjausryhmä. Esittelijänä toimii Samlinkin turvallisuusjohtaja.

Varmenneperiaatteita 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://www.samlink.fi

# 3 YLEISET EHDOT

## 3.1 VELVOLLISUUDET

### 3.1.1 Varmentajan velvollisuudet

Varmenneperiaatteiden mukaisia varmenteita myöntävän varmentajan tehtävänä on:

- Varmenneperiaatteiden mukaisten varmenne- ja hakemistopalveluiden tarjoaminen.
- Varmenneperiaatteiden mukaisten varmenteiden myöntäminen ja hallinnointi.
- Varmenteiden mitätöinti ja varmenteiden sulkulistojen julkaiseminen näiden varmenneperiaatteiden mukaisesti.
- Varmistaa, että varmentajan yksityisiä avaimia käytetään ainoastaan varmentajan varmenneperiaatteiden mukaisten varmenteiden ja sulkulistojen allekirjoittamiseen.
- Päättää ja toteuttaa mahdollinen ristiin varmentaminen muiden varmentajien kanssa.

Varmentaja vastaa siitä, että myönnetyt varmenteet on luotu varmenneperiaatteissa esitettyjen vaatimusten ja Web Services-yhteys sopimuksen tietojen mukaisesti. Varmentaja vastaa ainoastaan niistä tiedoista, jotka on tallennettu varmenteeseen.

Varmentaja vastaa siitä, että käytettäessä varmenteisiin liittyviä avainpareja asianmukaisesti varmenteet toimivat luovutushetkestä varmenteen voimassaoloajan, ellei varmennetta aseteta sulkulistalle.

Varmentaja vastaa siitä, että mitätöitäväksi pyydetyt varmenteet viedään sulkulistalle, joka julkaistaan varmenneperiaatteissa mainitussa ajassa.

Varmentaja ei vastaa yksityisen avaimen paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu varmentajan toiminnasta.

Varmentaja ei vastaa varmenteen haltijalle aiheutuneista välillisistä tai seurannaisvahingoista. Varmentaja ei myöskään vastaa varmenteeseen luottavan osapuolen kärsimistä välillisistä tai seurannaisvahingoista eikä varmenteen haltijan muun sopimuskumppanin mahdollisesti kärsimistä vahingoista.

Varmentaja ei vastaa siitä, että varmennetta käytetään vastoin sen käyttötarkoitusta.

### 3.1.2 Varmennetuotantoon liittyvät velvollisuudet

Varmentajan varmennetuotantoon liittyvät velvollisuudet ovat:

- Varmenneperiaatteita vastaavan varmennusjärjestelmän luominen, hallinta ja toimintojen lopettaminen Varmenneperiaatteiden mukaisesti.
- Varmenneperiaatteiden mukaisten varmenteiden tekninen hallinnointi niiden koko elinkaaren ajan (luonti, tallennus, varmuuskopiointi, julkaisu ja käytöstä poistaminen).
- Varmenneperiaatteiden mukaisen sulkulistan tekninen tuottaminen, ylläpito ja tallentaminen hakemistoon.

- Lokikirjan ylläpitäminen kaikista hallintatoimista.

### 3.1.3 Rekisteröijän velvollisuudet

Varmenneperiaatteiden mukaisten varmenteiden myöntämiseen osallistuvan rekisteröijän vastuulla on:

- Vastata varmenneperiaatteiden mukaisista omaa tehtäväaluettaan koskevista toimista.
- Huolehtia varmenteisiin tulevien tietojen oikeellisuudesta.

Rekisteröijien velvollisuudet koottuna ovat:

- Varmenteen haltijan henkilöllisyyden tarkistaminen ja henkilön oikeuden toimia yrityksen edustajana tässä toimenpiteessä noudattaen voimassa olevaa lainsäädäntöä sekä viranomaisten määräyksiä ja oman organisaationsa laatimia ohjeita.
- Rekisteröinnin edellytyksenä olevan sopimuksen tekeminen / tarkistaminen.
- Rekisteröintitietojen toimittaminen turvallisesti varmenteen haltijalle
- Rekisteröintiin liittyvien sopimustietojen arkistointi.

### 3.1.4 Varmenteen haltijan velvollisuudet

Varmenteen haltijan velvollisuuksista vastaa kyseessä olevan organisaation valtuuttama henkilö, jonka täytyy sitoutua alla oleviin velvollisuuksiin.

- Varmistaa, että varmenteen yksilöinnin kannalta olennaiset tiedot, jotka varmenteen haltija antaa rekisteröijälle, ovat oikeita.
- Yksityisen ja julkisen avaimen luonti.
- Yksityisen avaimen turvallinen säilytys.
- Yksityisen avaimen sisältävien varmuuskopioiden turvallisesta säilytyksestä huolehtiminen.
- Sulkupalveluun täytyy sen palveluaikana tehdä varmentajalle toimitettava ilmoitus, mikäli varmenteen voimassaoloaikana:
    - On syytä epäillä, että yksityinen avain on mahdollisesti paljastunut tai otettu luvattomasti käyttöön.
    - Yksityinen avain on korruptoitunut tai ei muutoin ole käytettävissä.
    - Varmennettu laite tai palvelinsovellus poistetaan käytöstä.
    - Yksityisen avaimen mahdollisen paljastumisen jälkeen sen käyttö lopetetaan heti ja pysyvästi.

### 3.1.5 Varmenteeseen luottavan osapuolen velvollisuudet

Varmenteeseen luottavan osapuolen päätettäväksi jää luottamus varmenneperiaatteiden mukaisiin varmenteisiin. Sen lisäksi mitä muualla varmenneperiaatteissa on sanottu, voidaan todeta seuraavaa:

- Varmentaja noudattaa varmennustoiminnassa voimassa olevaa lainsäädäntöä
- Varmentaja noudattaa varmenneperiaatteita

- Varmentajan yleinen turvataso on merkittävän korkea.

Varmenteeseen luottava on velvollinen tarkistamaan varmentajan oikeellisuuden sekä tarkistamaan, että varmenne on voimassa, ettei varmenne ole sulkulistalla eikä sulkulistan voimassaoloaika ole umpeutunut ja avaimen käyttötarkoituksen mukainen käyttö.

Käytettäessä varmenteita Samlinkin tietoverkon ja palvelujen yhteydessä Samlink voi hoitaa edellä mainitut tarkistukset Luottavan osapuolen puolesta.

#### 3.1.6 Sulkupalvelun velvollisuudet

Varmenneperiaatteiden mukaisten Web Services-yhteyssopimusten sulkemiseen osallistuvan sulkupalvelun vastuulla on:

- Suorittaa varmenteen haltijan, varmentajan tai rekisteröijän toimeksiannon perusteella sopimuksen sulkeminen
- Varmistaa toimeksiannon alkuperä ja oikeudellisuus
- Kirjata suoritetut toimeksiannot

#### 3.1.7 Tietovarastoon liittyvät velvollisuudet

Varmentaja julkaisee hakemistossa sulkulistat kappaleen 2.3.7 ”Hakemisto” mukaisesti.

Hakemistoon on kaikkialta pääsy LDAP-protokollalla. varmentaja julkaisee varmennepalvelua koskevaa dokumentaatiota kappaleessa 3.6 ”Tietojen julkaiseminen ja tietovarasto” mainituilla jakelukanavilla.

### 3.2 VASTUUVELVOLLISUUS

#### 3.2.1 Varmentajan vastuuvelvollisuus

##### 3.2.1.1 Varmenteen sisältämän informaation tarkistaminen

Allekirjoittaessaan varmenteen yksityisellä avaimellaan, varmentaja osoittaa ottavansa vastuun varmenteen tietojen oikeellisuudesta varmenneperiaatteiden mukaisesti.

##### 3.2.1.2 Vastuurajoitukset

Varmentaja ei vastaa vahingoista, jotka johtuvat varmenneperiaatteiden, käyttöehtosopimusten tai ohjeiden vastaisesta toiminnasta.

Varmentaja ei vastaa välillisistä vahingoista eikä vahingoista, jotka ovat seurausta ylivoimaisen esteen aiheuttamista häiriöistä tai virheistä varmennustoiminnassa.

Muita vastuurajoituksia voidaan määritellä erillisessä sopimuksessa, kuten esimerkiksi sopimusten sulkupalvelun ja sopimusten rekisteröintipalvelun sopimuksissa.

### 3.2.2 Rekisteröijän vastuuvelvollisuus

Varmentaja vastaa omaan organisaatioonsa kuuluvien rekisteröintipisteiden toiminnasta.

Varmentajan valtuuttamien (pankkien) hoitamien rekisteröintipisteiden toiminnasta vastaa kunkin rekisteröintipisteen organisaatio.

## 3.3 TALOUDELLINEN VASTUU

Varmentaja ei vastaa niistä taloudellisista sitoumuksista, joita syntyy varmennetta käytettäessä.

### 3.3.1 Vahingonkorvaukset

Varmentaja ei maksa vahingonkorvauksia.

### 3.3.2 Korvaukset Varmenteen haltijalta

Jos varmentajaa vastaan kohdistetaan vaatimuksia alla mainittujen seikkojen perusteella, varmenteen haltija sitoutuu korvaamaan varmentajalle kaikki tällaisista vaatimuksista ja/tai niihin vastaamisesta aiheutuvat vahingot ja kustannukset, mukaan lukien oikeudenkäynti- ja asianajokulut.

- Varmenteen haltija ei ole luottavana osapuolena tarkistanut varmenteen voimassa-oloa kappaleen 3.1.5 ”Varmenteeseen luottavan osapuolen velvollisuudet” vaatimusten mukaisesti.
- Varmennetta on käytetty vastoin sille määriteltyä soveltuvuutta tai sen sisältämän julkisen avaimen käyttötarkoitusta.
- Luottavana osapuolena varmenteen haltija on luottanut varmenteeseen muutoin perusteettomasti olosuhteisiin nähden.

Varmentaja ilmoittaa asiakkaalle tämän kappaleen mukaisista vaatimuksista kirjallisesti kohtuullisessa ajassa niistä tiedon saatuaan.

### 3.3.3 Osapuolten väliset suhteet

Varmentajan, rekisteröijän, sulkupalvelun ja varmenteen haltijan sekä varmentajan ja mahdollisten alihankkijoiden väliset toiminnalliset, juridiset ja taloudelliset suhteet on määritelty näiden keskinäisissä sopimuksissa.

### 3.3.4 Hallinnolliset prosessit

Varmentaja on määritellyt ja kuvannut varmennustoiminnassa käytettävät prosessit ja tuottanut niitä vastaavan ohjeistuksen.

### 3.4 TULKINTA JA TÄYTÄNTÖÖNPANO

#### 3.4.1 Sovellettava lainsäädäntö

Näihin varmenneperiaatteisiin sovelletaan suomen lakia.

#### 3.4.2 Erimielisyyksien ratkaiseminen

Näitä varmenneperiaatteita koskevien riitojen ratkaisemisesta sovitaan varmentajan ja varmenteen haltijan välisissä sopimuksissa.

### 3.5 MAKSUT

Varmentaja ei veloita varmennepalvelun käyttöä suoraan varmenteen haltijalta vaan varmennepalvelun veloitukset kohdistetaan Web Services-yhteys sopimuksen haltijalle kulloisenkin voimassa olevan hinnaston mukaisesti.

### 3.6 TIETOJEN JULKAISEMINEN JA TIETOVARASTO

#### 3.6.1 Varmentajan tietojen julkaisu

Varmentaja julkaisee Samlinkin ja pankkien käytössä olevissa intranet-sivustoissa sekä Web Sevices-yhteyssopimuksessa kerrotulla tavalla voimassa olevat varmenneperiaatteet. Myös aikaisemmat voimassa olleet varmenneperiaatteet ovat saatavissa tästä näistä 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.

Varmentaja julkaisee sulkulistan Samlink Customer CA Varmennuskäytäntö -dokumentin kappaleessa 5.4.6 ” Sulkulistan tarkastusvaatimukset” ilmoitetuissa osoitteissa.

#### 3.6.2 Julkaisutaajuus

Hakemistossa julkaistavat varmenteet julkaistaan viipymättä myöntämisen jälkeen. sulkulista julkaistaan kappaleen 5.4.8 ”Sulkulistan julkaisu” mukaisesti.

#### 3.6.3 Pääsynvalvonta

Varmennepalvelun dokumenttien pääsynvalvonta on toteutettu niin, että dokumentit ovat vain niiden saatavilla, joilla on niihin tarve päästä.

### 3.7 TARKASTUKSET

Varmentajan toiminnan tarkastamisesta huolehtii Samlinkin sisäinen tarkastus. Tarkastuksen avulla selvitetään, toimiiko varmennusorganisaatio varmenneperiaatteiden mukaisesti.

Varmentaja voi tarkastaa varmenteen haltijoidensa ja alihankkijoidensa toimintaa varmentajaan liittyvien toimintojen osalta.

Tarkastuksessa mahdollisesti havaittujen puutteiden korjaamisesta vastaa toiminnosta vastuussa oleva taho.

### 3.8 LUOTTAMUKSELLISUUS

Varmenteiden myöntämisen tai käytön yhteydessä mahdollisesti käsiteltävien henkilö- tai tunnistamistietojen käsittelyssä noudatetaan voimassa olevaa lainsäädäntöä.

Viranomaisille luovutetaan tietoja vain lakien, asetusten ja viranomaismääräysten perusteella.

### 3.9 OMISTUS- JA IMMATERIAALIOIKEUDET

Varmennepalveluihin liittyviin ohjelmistoihin, määrityksiin ja dokumentteihin kohdistuvat omistus- ja immateriaalioikeudet kuuluvat varmentajalle tai sen toimittajille tai alihankkijoille näiden kanssa laadittujen sopimusten mukaisesti.

### 3.10 SOPIMUKSET

Web Services-yhteys sopimuksen haltija tekee varmenteen haltijan kanssa käyttöehto-sopimuksen, jossa osapuolten vastuut ja velvollisuudet kuvataan. Allekirjoittaessaan käyttöehtosopimuksen varmenteen haltija hyväksyy sopimuksessa olevat ehdot ja sitoutuu toimimaan niiden ja näiden varmenneperiaatteiden mukaisesti.

Varmentaja laatii mahdollisten alihankkijoiden kanssa sopimuksen, jossa kuvataan osa-puolten vastuut ja velvollisuudet.

## 4 TUNNISTUS JA TODENTAMINEN

### 4.1 NIMEÄMISKÄYTÄNTÖ VARMENTAJAN VARMENTEESSA

Varmenneperiaatteiden mukaisia varmenteita myöntävän varmentajan nimi löytyy varmentajan varmenteesta sekä ”Issuer”- että ”Subject” -kentästä sekä kaikkien varmentajan myöntämien muiden Varmenteiden ”Issuer”-kentästä. Nimi koostuu ainakin seuraavista osista:

- varmentajan tunnistenimi (Common Name, CN)
- varmentajan organisaatio (Organization Name, O)
- maa (Country Name, C).

Osien tarkka sisältö on kuvattu alla.

#### 4.1.1 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 |

### 4.2 ENSIREKISTERÖINTI

#### 4.2.1 Nimeämiskäytännöt

Varmenneperiaatteiden mukaan myönnetyissä varmenteissa ”Subject”-kentässä oleva yksikäsitteinen nimi sisältää seuraavat tiedot:

| Tieto (Attribute) | Selite | Esimerkki |
|---|---|---|
| Sukunimi (SurName) | Pankin Palvelusopimusjärjestelmän tuntema käyttäjätunnus | SN=12345678 |
| Tunnistenimi (Common Name) | Pankin Palvelusopimusjärjestelmän tuntema aakkostus-nimi | CN=Oy Firma AB |
| Organisaatio (Organization) | Organisaation tai organisaatioryhmän selväkielinen nimi | O=Aineistopalvelut-Saastopankki |
| Maa (Country) | Maa, jossa ym. organisaatio toimii | C=FI |

Edellä mainitut osat ovat pakollisia kaikissa varmenneperiaatteiden mukaisesti myönnetyissä varmenteissa.

#### 4.2.2 Nimivaatimukset

Tunnistenimenä käytetään palvelusopimusjärjestelmään rekisteröityä nimeä, jonka oikeellisuus tulee rekisteröijän tarkistaa sopimuksen tekemisen yhteydessä.

#### 4.2.3 Nimien yksikäsitteisyys

Kaikissa varmentajan myöntämissä varmenteissa sukunimikentässä olevan käyttäjätunnuksen täytyy olla yksikäsitteisesti sopimukseen yhdistettävissä ja Palvelusopimusjärjestelmä huolehtii kentän yksikäsitteisyydestä. Poikkeuksena Samlinkin allekirjoitusvarmenne, jolle ei ole olemassa sopimusta ja sen sukunimikentän arvoksi annetaan sellainen arvo, jota ei tule esiintymään palvelusopimusjärjestelmässä.

#### 4.2.4 Nimiepäselvyyksien ratkaiseminen

Varmenteen yksilöintitietoa (käyttäjätunnus) hallittaan palvelusopimusjärjestelmässä, joka huolehtii yksikäsiteisyydestä. Jos varmennepyynnön nimi eroaa palvelusopimusjärjestelmän nimestä, käytetään varmenteella palvelusopimusjärjestelmän tuntemaa nimeä, mikäli muilla tiedoilla voidaan todentaa varmennepyynnön kohdistuvan kyseiseen sopimukseen.

#### 4.2.5 Yksityisen avaimen hallussapidon osoittaminen

Varmennepyyntö toimitetaan varmentajalle allekirjoitettuna sillä yksityisellä avaimella, jota vastaavalle julkiselle avaimelle varmennetta haetaan.

#### 4.2.6 Rekisteröintivastaavan todentaminen

Rekisteröintivastaavien identiteetti on rekisteröity Samlinkin järjestelmiin ja rekisteröintivastaavan verkkoon kirjautumisessa vaaditaan tunnistautuminen omalla identiteetillä..

Rekisteröintivastaavalla on oltava erillinen käyttövaltuus, jolla voi suorittaa rekisteröinnin palvelusopimusjärjestelmään. rekisteröintipisteestä vastuussa oleva organisaatio vastaa rekisteröijän käyttövaltuuksien hallinnasta.

#### 4.2.7 Organisaation todentaminen

Varmenteen haltijan nimen muuttuessa varmenteen haltijoille voidaan hakea uudet varmenteet uusimalla varmenteisiin liittyvä Web Services-yhteys sopimus. Kun vanha sopimus lakkautetaan ja avataan uusi Web Services-yhteys sopimus, uudet varmenteet myönnetään ja vanhan tunnistenimen sisältävät Varmenteet mitätöidään.

#### 4.2.8 Varmenteen haltijan tunnistaminen

Rekisteröijä tunnistaa varmenteen haltijan Web Services-yhteys sopimuksen allekirjoituksen yhteydessä noudattaen asiaan liittyvää voimassa olevaa lainsäädäntöä, viranomaisten määräyksiä sekä oman organisaationsa antamia sisäisiä ohjeita.

### 4.3 VARMENTEEN UUSIMINEN VOIMASSAOLON PÄÄTTYESSÄ

Kun varmenteen voimassaoloaika on päättymässä, varmenne uusitaan siten, että myös avainpari uusitaan. vanhenevan varmenteen uusinta ei edellytä palvelusopimuksen uudistamista. Uusintapyyntö allekirjoitetaan voimassa olevalla yksityisellä avaimella,

### 4.4 VARMENTEEN UUSIMINEN SEN VOIMASSAOLON PÄÄTTYMISEN TAI MITÄTÖINNIN JÄLKEEN

Varmenteen uusiminen edellisen varmenteen voimassaolon päättymisen tai varmenteen mitätöinnin jälkeen tapahtuu samalla menettelyllä kuin ensirekisteröinnissä.

### 4.5 WEB SERVICES-YHTEYS SOPIMUKSEN VOIMASSAOLON KESKEYTTÄMISPYYNTÖ

Sopimusten sulkupalvelu tarkistaa vastaanottamansa Web Services-yhteys sopimuksen voimassaolon keskeyttämispyynnön alkuperän sekä oikeudellisuuden.

Web Services-yhteys sopimuksen voimassaolon keskeyttämispyyntö rekisteröidään Sopimusjärjestelmään. Tämä rekisteröinti estää välittömästi Web Services-yhteys sopimuksen mukaisen palvelun käyttämisen kyseiseen sopimukseen liittyvällä varmenteella rekisteröinnin jälkeen.

Varmenteen haltijan tulee ilmoittaa Web Services-yhteys sopimuksen haltijalle Web Services-yhteys sopimuksen keskeyttämisestä.

Mikäli Web Services-yhteys sopimuksen keskeyttämispyyntö on aiheellinen, palvelusopimuksen haltija lakkauttaa Web Services-yhteys sopimuksen, josta seuraa automaattisesti varmenteen mitätöintipyyntö.

Jos Web Services-yhteys sopimuksen keskeyttämispyyntö osoittautuu aiheettomaksi, Web Services-yhteys sopimuksen haltija asettaa Web Services-yhteys sopimuksen voimassa olevaksi, jonka seurauksena sopimukseen liitettyjen varmenteiden käyttö palautuu normaaliksi.

Lakkautettua Web Services-yhteys sopimusta ei voi enää palauttaa, vaan on tehtävä uusi sopimus, josta käynnistyy varmenteen hakuprosessi.

Web Services-yhteys sopimuksen keskeyttäminen ei aiheuta mitään muutoksia varmenteen tietoihin tai sulkulistalle.

### 4.6 VARMENTEEN PALAUTTAMISPYYNTÖ

Varmenteen voimassaolon keskeytys ei ole mahdollinen, joten varmenne ei ole palautettavissa käyttöön.

## 5 TOIMINNALLISET VAATIMUKSET

### 5.1 VARMENTEEN HAKEMINEN

Varmenteen hakeminen edellyttää, että varmenteen tilaajana toimii varmenteen haltija, jolla on voimassa oleva Web Services-yhteyssopimus.

### 5.2 VARMENTEEN MYÖNTÄMINEN

Varmennusjärjestelmä hyväksyy vain sellaiset varmennepyynnöt, joiden alkuperä voidaan tunnistaa sähköisestä allekirjoituksesta tai Web Services-yhteys sopimuksen haltijan toimittamalla tunnuksella ja siihen liitetyllä kertakäyttöisellä salasanalla. Varmennepyynnön alkuperä voidaan tunnistaa myös asiakirjojen ja henkilötunnistuksen avulla.

Varmenteen myöntäminen voi tapahtua kahdella eri tavalla:

- Käyttäen Web Services-kanavaa, jossa varmennepyyntö ja varmenne välitetään XML-sanomilla.
- Varmenteen haltija toimittaa varmennepyynnön varmentajalle sähköpostin liitetiedostoja tai erillisellä tietovälineellä ja varmentaja toimittaa varmenteen haltijalle sähköpostin liitteenä tai erillisellä tietovälineellä.

### 5.3 VARMENTEEN HYVÄKSYMINEN

Varmenteen haltijan katsotaan hyväksyneen hänelle myönnetyn varmenteen, kun:

- Varmenteen haltija on pankkiyhteyssopimuksen kuittauksellaan sitoutunut noudattamaan varmenteen käyttöön liittyviä ohjeita
- Varmentajan tietojärjestelmän on käsitellyt varmenteen haltijalta saamansa Varmennepyynnön sekä palauttanut onnistuneesti varmenteen sen haltijalle
- kun varmenne on asennettu käyttöön
- varmennetta vastaava yksityinen avain on otettu käyttöön.

### 5.4 VARMENTEEN MITÄTÖINTI JA VARMENTEEN VOIMASSAOLON KESKEYTTÄMINEN

Varmenne voidaan ainoastaan mitätöidä lopullisesti. Sen voimassaoloa ei voida keskeyttää. Varmenteet, jotka on mitätöity, julkaistaan sulkulistalla hakemistossa.

Varmenne mitätöidään aina, mikäli varmenteen käyttöön liittyvä Web Services-yhteys sopimus lakkautetaan.

#### 5.4.1 Olosuhteet Varmenteen mitätöimiseksi

Varmenteen haltijan täytyy pyytää viipymättä varmenteen mitätöintiä kappaleen 3.1.4 ”Varmenteen haltijan velvollisuudet” sulkupalveluun liittyvää ilmoitusvastuuta kuvaavassa kohdassa mainituissa olosuhteissa.

#### 5.4.2 Oikeus pyytää Varmenteen mitätöintiä

Web Services-yhteys sopimuksen keskeyttämistä tai lakkauttamista voi pyytää pääsääntöisesti ainoastaan henkilö, jolla on oikeus toimia varmenteen haltijan edustajana.

Varmenteen mitätöintipyynnön ja varmenteeseen liittyvän Web Services-yhteys sopimuksen sulkupyynnön voi tehdä:

- rekisteröijä pankkiyhteyssopimuksen mukaisin ehdoin
- varmenteen haltija
- varmennepalvelun omistaja

- Samlinkin turvallisuusosasto.

Mikäli mitätöintipyynnön ja varmenteeseen liittyvän Web Services-yhteys sopimuksen sulkupyynnön on tehnyt joku muu kuin varmenteen haltija, siitä ilmoitetaan varmenteen haltijalle.

5.4.3

Mitätöintipyyntömenettely

Varmentajan on huolehdittava, että Web Services-yhteys sopimukset suljetaan sulkupalvelun palveluaikana viipymättä perustuen vastaanotettuihin mitätöintipyyntöihin.

Varmenteen mitätöinti tapahtuu pääsääntöisesti Web Services-yhteys sopimuksen lakkautuksen seurauksena ohjelmallisella prosessilla, jossa varmenteen mitätöintipyynnön lähettäjänä toimii Varmentajan tietojärjestelmä.

Poikkeustilanteita varten on varmentajan sulkupalvelun käytössä online-työkalu, jolla yksittäisen varmenteen tietoja voidaan kysellä sekä varmenne voidaan mitätöidä. Mitätöintipyyntö on tehtävä sulkupalvelulle kirjallisella ilmoituksella, jossa on seuraavat tiedot:

- pyynnön kohde (Web Services-yhteys sopimuksen käyttäjätunnus ja varmenteen haltija)
- pyynnön ajanhetki
- pyynnön vastaanottaja
- pyynnön tekijä ja tämän tunnistustapa
- pyynnön syy.

5.4.3 Mitätöintipyynnön odotusaika

Sopimusten sulkupalvelu ottaa mitätöintipyyntöjä vastaan palveluaikana. Sopimusten sulkupalvelu sulkee Web Services-yhteys sopimuksen, joka estää varmenteita käyttävien prosessien suorituksen, mutta ei vielä sulje varmennetta. Web Services-yhteys sopimuksen sulkemisen jälkeen on Web Services-yhteys sopimuksen lakkauttamisesta ilmoitettava Web Services-yhteys sopimuksen haltijalle, joka lakkauttaa Web Services-yhteys sopimuksen. Web Services-yhteys sopimuksen lakkauttamisesta syntyy automaattisesti varmenteen mitätöintipyyntö.

Sulkulistapalvelu huolehtii varmenteen viennistä sulkulistalle ja sulkulistan julkaisusta määrävälein kappaleen 5.4.8 ”Sulkulistan julkaisu” mukaisesti.

5.4.4 Olosuhteet Varmenteen voimassaolon keskeyttämiseksi

Varmenteen voimassaolon keskeytys ei ole mahdollinen.

5.4.5 Oikeus Varmenteen voimassaolon keskeyttämiseen

Varmenteen voimassaolon keskeytys ei ole mahdollinen.

5.4.6 Menettelytapa Varmenteen voimassaolon keskeyttämiselle

Varmenteen voimassaolon keskeytys ei ole mahdollinen.

5.4.7 Sulkulistan julkaisu

Varmentaja tarjoaa sulkulistapalvelua, josta tieto suljetuista varmenteista on jatkuvasti saatavilla. Sulkulistat julkaistaan säännöllisesti. Sulkulistojen julkaisukäytäntö, julkaisutiheydet ja voimassaoloajat määritellään varmennuskäytännön kappaleessa 5.4.8. Sulkulistatietojen eheys ja oikeellisuus on taattava.

5.4.8 Sulkulistan tarkastusvaatimukset

Varmenteeseen luottava osapuoli ei voi luottaa varmenteeseen, jonka voimassaoloa ei ole tarkastettu sillä hetkellä voimassa olevalta sulkulistalta.

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 sen hetkinen tila täytyy tarkistaa sulkulistalta mahdollisen mitätöinnin varalta.
- Jos voimassa olevaa sulkulistatietoa ei ole saatavissa esim. järjestelmä- tai palveluhäiriön 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

Varmenteen hyväksyminen tarkastamatta vapauttaa varmentajan vastuusta.

Jos voimassa olevaa sulkulistaa ei ole saatavilla, ei varmenteeseen saa luottaa.

**5.5 VARMENTEEN PALAUTTAMINEN KÄYTTÖÖN**

Varmenteen voimassaolon keskeytys ei ole mahdollinen, joten varmenne ei ole palautettavissa käyttöön.

**5.6 TIETOTURVALLISUUDEN VALVONTA**

Varmennetuotanto tallentaa ja seuraa säännöllisesti varmennustoiminnassa syntyviä ja siihen liittyviä oleellisia tietoja. Osa näistä tiedoista tallentuu automaattisesti tuotantojärjestelmiin ja osa tallennetaan manuaalisesti Varmennetuotannon henkilöstön toimesta.

Tallennettaviin tietoihin kuuluvat mm. varmentajan allekirjoitusavaimen elinkaareen liittyvät tiedot, kaikkien varmenteiden elinkaareen liittyvät tapahtumat sekä tietoturvallisuuden ylläpitoon liittyvät tapahtumat.

Lisäksi Sulkupalvelulla on velvollisuus tallentaa omien sulkupalveluvastaavien suorittamat Web Services-yhteys sopimusten sulkupyynnöt.

### 5.7 TIETOJEN ARKISTOINTI

Varmentaja (tai varmennetuotanto varmentajan puolesta) arkistoi oleellisimmat varmennustoimintaan liittyvät tiedot.

Varmenteita koskevien arkistojen tietojen eheydestä huolehditaan.

Tapahtumat arkistoidaan siten, että niitä ei pystytä poistamaan tai tuhoamaan sinä ajanjaksona, jona niitä säilytetään. Varmenteita koskevat arkistot voidaan pyydettäessä luovuttaa käytettäväksi varmennuksen todisteena oikeudessa.

Arkistoitavat tiedot säilytetään lainsäädännön tai viranomaisten vaatimusten mukaisen ajan suojattuina muuttamiselta ja häviämiseltä, kuitenkin vähintään kolmen (3) vuoden ajan.

### 5.8 VARMENTAJAN AVAINTEN UUSIMINEN

Varmentajan varmenteen voimassaoloaika ja varmentajan avainten käyttöaika on korkeintaan 25 vuotta. Uusi varmentajan avainpari ja varmentajan itsensä allekirjoittama varmentajan varmenne luodaan ja julkaistaan vähintään pisimmän varmentajan myöntämän varmenteen eliniän verran ennen edellisten avainten vanhenemista.

Vaihdettaessa varmentajan yksityistä avainta huolehditaan siitä, että varmennusketju säilyy vanhan ja uuden avaimen välillä.

### 5.9 KATASTROFISTA JA VARMENTAJAN AVAIMEN PALJASTUMISESTA TOIPUMINEN

Varmentaja vastaa siitä, että hätätilanteissa, joihin lasketaan mm. varmentajan yksityisen avaimen paljastuminen tai joutuminen vääriin käsiin ja tietokoneresurssien, ohjelmistojen ja/tai tietojen tuhoutuminen, varmennepalvelun toiminta palautetaan normaaliksi niin nopeasti kuin mahdollista.

#### 5.9.1 Tietokonelaitteet, ohjelmistot, ja/tai tiedot ovat korruptoituneet

Varmentajan täytyy huolehtia toiminnan jatkuvuuden kannalta kriittisimpien järjestelmiensä varmistamisesta, ohjelmistojen varmuuskopioinnista ja tietojen tallennuksesta niin, että niiden palautus varmuuskopiolta on mahdollista.

#### 5.9.2

Varmentajan yksityinen avain on paljastunut

Varmentajan tulee luoda varmentajan yksityisen avaimen paljastumisen varalle toimintaohjeet, jotka sisältävät ainakin seuraavat tehtävät:

- informoitava välittömästi paljastumisesta Varmenteen haltijoita ja muita Varmentajia, joiden kanssa Varmentajalla mahdollisesti on sopimus,

- sulkulistan poistaminen käytöstä
- Varmentajalle luotava uudet avaimet ja Varmenne.sekä
- Varmennejärjestelmästä julkaistut kyseisenä ajankohtana voimassa olevat Varmenteet on uusittava.

5.10

Varmennustoiminnan lopettaminen

Varmennustoiminnan lopettamisena pidetään tilannetta, jossa kaikki varmentajan varmenteiden myöntämiseen liittyvät palvelut lakkautetaan pysyvästi. Varmennustoiminnan lopettamisella ei tarkoiteta tilannetta, jossa varmennepalvelu siirretään organisaatioilta toiselle.

Varmentaja ilmoittaa kirjallisesti varmennustoiminnan lopettamisesta varmenteen haltijoille ja kaikille niille osapuolille, joiden kanssa varmentajalla on varmennepalveluihin liittyviä sopimuksia tai muita vakiintuneita suhteita. Ilmoitus varmennustoiminnan lopettamisesta täytyy tehdä em. tahoille mahdollisimman pian, kuitenkin vähintään kuusi (6) kuukautta ennen lopettamisen ajankohtaa.

Varmentaja lopettaa kaikki valtuutukset, jotka koskevat varmentajan ulkoistamia toimintoja Varmenteiden myöntämisprosessiin liittyen.

Varmentaja huolehtii siitä, että sen myöntämiä varmenteita ei enää voi luotettavasti käyttää.

Varmennepalvelun lopettamisen yhteydessä varmennetuotanto tuhoaa tai poistaa käytöstä varmentajan yksityisen avaimen.

Varmentaja purkaa varmenteen haltijoiden kanssa tehdyt Web Services-yhteys sopimukset noudattaen sopimuksissa mainittua irtisanomisaikaa.

# 6 TURVATOIMENPITEET

Seuraavat kohdat koskevat Varmentajaa ja mahdollista Varmennetuotannosta vastaavaa alihankkijaa.

### 6.1 FYYSISET TURVARATKAISUT

Fyysistä pääsyä kriittisiin palveluihin valvotaan ja varmenteiden tuotantojärjestelmään kohdistuvat fyysiset riskit minimoidaan. Tämä edellyttää mm. seuraavien suojatoimien varmistamista:

- Fyysisen pääsyn varmenteiden luontiin liittyviin tiloihin täytyy olla rajoitettu siten, että vain valtuutetut henkilöt pääsevät tiloihin.
- Varmentajan ja varmennetuotannon järjestelmiin kuuluvien laitteiden tai ohjelmistojen rikkoutumisen, tuhoutumisen, tai vaarantumisen ja niistä mahdollisesti aiheutuvan liiketoiminnan keskeytymisen estämiseksi täytyy olla toteutettuna riittävät suojatoimet.
- Varmennepalveluihin liittyvät laitteistot, tiedot, tietovälineet ja ohjelmistot täytyy suojata luvattomalta tiloista pois siirtämiseltä.

- Tietojen paljastumisen tai varastamisen ja tietojen käsittelyssä käytettäviin tiloihin murtautumisen estämiseksi täytyy olla toteutettuna riittävät suojatoimet.
- Tuotantotilan tarjoamien resurssien ja varsinaisten järjestelmäresurssien suojaamiseksi täytyy järjestää tuotantoympäristöön liittyvä turvavalvonta.

Edellä kuvattujen vaatimusten täyttäminen edellyttää toimenpiteitä mm. seuraavilla osa-alueilla, joiden toteutusta on kuvattu tarkemmin varmennuskäytännössä:

- Laitetilan sijainti ja rakenne
- Fyysinen pääsynvalvonta
- Sähkönsyöttö ja ilmastointi
- Vesivahingoilta suojautuminen
- Paloturvallisuus
- Tietomateriaalin säilytys
- Jätemateriaalin hävittäminen
- Toisaalla säilytettävät varmuuskopiot.

## 6.2 TOIMINNALLISET TURVARATKAISUT

### 6.2.1 Luotetut toimenhaltijat

Luetettuja toimenhaltijoita ovat kaikki ne, jotka vastaavat Varmennepalvelun toiminnan varmistamisesta, ylläpidosta ja valvonnasta.

Varmennustoimintaan osallistuvat seuraavat luotetut toimenhaltijat, joiden vastuut on kuvattu Varmennuskäytännössä:

- Tietoturvallisuusvastaava
- Järjestelmän pääkäyttäjä
- Järjestelmän ylläpitäjä
- Järjestelmän arvioija
- Rekisteröintivastaava
- Sulkupalveluvastaava.

Luotetut toimenhaltijat sitoutuvat noudattamaan Varmenneperiaatteita.

### 6.2.2 Tehtäviin vaadittavien henkilöiden lukumäärät

Seuraavien toimenpiteiden suorittamiseen vaaditaan vähintään kahden henkilön yhtäaikaista paikallaoloa:

- Muutokset varmentajan tuotantojärjestelmäympäristöön
- Varmentajan yksityisen avaimen varmuuskopiointi ja palauttaminen.

Seuraavien toimenpiteiden suorittamiseen vaaditaan vähintään neljän henkilön yhtäaikaista paikallaoloa:

- Varmentajan avainten luonti

6.2.3 Luotettujen toimenhaltijoiden tunnistaminen ja todentaminen

Tärkeimpien luotettujen toimien haltijoiden tunnistaminen edellyttää Varmenteen käyt-töä. Eri toimiin liittyvä tunnistaminen on kuvattu Varmennuskäytännössä.

### 6.3 HENKILÖTURVALLISUUS

6.3.1 Taustatietojen tarkastusmenettely

Varmentaja ja mahdolliset alihankkijat suorittavat tarpeelliset tarkistukset kaikille palkkaamilleen henkilöille henkilöstökäytäntöjensä mukaisesti. Tarkistuksessa selvitetään henkilön luotettavuus ja ammattitaito.

Tärkeimmissä luotetuissa rooleissa toimiville henkilöille suoritetaan taustatietojen tarkistaminen. Nämä roolit on määritelty varmennuskäytännössä. Henkilöt, jotka eivät läpäise alkutarkastusta tai mahdollisesti myöhemmässä vaiheessa tehtävää tarkastusta, eivät voi toimia tai jatkaa luotettuina toimenhaltijoina.

6.3.2 Koulutusvaatimukset

Henkilöstön täytyy olla varmennepalveluun liittyvään laitteisto- ja ohjelmistoympäristöön asianmukaisesti koulutettu.

6.3.3 Seuraukset luvattomista toimenpiteistä

Varmentajan tai mahdollisen Varmennetuotannosta vastaavan alihankkijan havaitessa varmennustoimintaan liittyviä väärinkäytöksiä ne ryhtyvät välittömästi tarpeellisiin toimenpiteisiin väärinkäytöksistä johtuvien haittojen poistamiseksi ja niiden uusiutumi-sen estämiseksi.

6.3.4 Sopimustyöntekijävaatimukset

Sopimustyöntekijöiden vaatimukset ovat samat kuin vakinaisenkin henkilöstön vaatimukset.

## 7 TEKNISET TURVARATKAISUT

### 7.1 VARMENTAJAN AVAINPARIN LUOMINEN, KÄYTTÖÖNOTTO JA SUOJAAMINEN

7.1.1 Varmentajan avainparin luominen

Varmentajan on huolehdittava, että varmentajan avaimet luodaan valvotuissa olosuhteissa.

Erityisesti on otettava huomioon, että varmentajan avainten luonti tapahtuu fyysisesti turvallisessa ympäristössä luotettujen toimenhaltijoiden toimesta. Tehtävän suorittaminen vaatii vähintään neljän henkilön yhtäaikaista paikallaoloa. Niiden luotettujen toimenhaltijoiden määrä, jotka ovat oikeutettuja suorittamaan tämän toimenpiteen, on rajattava mahdollisimman pieneksi.

### 7.1.2 Varmentajan julkisen avaimen toimittaminen luottaville osapuolille

Varmentaja huolehtii siitä, että varmentajan julkisen avaimen ja kaikkien siihen liittyvin parametrien eheys ja autenttisuus säilytetään, kun avain asetetaan luottavien osapuolten saataville.

Varmentajan varmenne, joka sisältää varmentajan julkisen avaimen, on luottavien osapuolien saatavilla.

### 7.1.3 Varmentajan avainten pituudet ja käytetty algoritmi

Varmentajan allekirjoitusavaimen pituus ja algoritmi, jota käytetään avaimen kanssa, täytyy valita siten, että niitä pidetään yleisesti soveltuvina varmenteisiin.

### 7.1.4 Varmentajan Avainparin käyttöikä

Varmentajan yksityisellä avaimella voidaan allekirjoittaa varmenteita varmentajan avainparin käyttöiän ajan vähennettynä pisimmällä varmenteen haltijan varmenteen voimassaoloajalla. Tämän jälkeen varmentajalle täytyy luoda uusi avainpari varmenteiden allekirjoitukseen. Sulkulistoja allekirjoitetaan yksityisellä avaimella koko varmentajan avainparin käyttöiän ajan. Varmentajan yksityisen avaimen käyttöikä ja varmentajan varmenteen voimassaoloaika on määritelty varmennuskäytäntö dokumentissa.

### 7.1.5 Varmentajan avainten käyttötarkoitukset

Varmentaja huolehtii siitä, että varmentajan allekirjoitusavaimia ei käytetä muihin tarkoituksiin kuin Varmenteiden myöntämiseen ja sulkulistan tietojen julkaisuun ja että varmentajan allekirjoitusavaimia käytetään vain fyysisesti turvallisissa tiloissa.

### 7.1.6 Varmentajan Yksityisen avaimen suojaaminen

Varmennetuotannon on huolehdittava siitä, että varmentajan yksityiset avaimet pysyvät luottamuksellisina ja eheinä.

Kun yksityinen allekirjoitusavain on turvallisen allekirjoituksen luomisvälineen ulkopuolella, sen täytyy olla salattu käyttäen algoritmia ja avainpituutta, jotka nykytiedon mukaan pystyvät kestämään salaukseen kohdistuvia hyökkäyksiä avaimen tai avaimen osan elinkaaren ajan.

Varmentajan yksityinen allekirjoitusavain voidaan varmistaa, tallentaa ja palauttaa vain luotettujen toimenhaltijoiden toimesta fyysisesti suojatussa ympäristössä. Näiden toimenpiteiden suorittaminen vaatii vähintään neljän henkilön yhtäaikaista paikallaoloa. Niiden luotettujen toimenhaltijoiden määrä, jotka ovat oikeutettuja suorittamaan näitä toimenpiteitä, on rajattava mahdollisimman pieneksi.

Varmentajan yksityisen allekirjoitusavaimen varmuuskopioihin sovelletaan vähintään samantasoisia turvamekanismeja kuin käytössä oleviin allekirjoitusavaimiin.

Kun avaimet on tallennettu avainten prosessointiin tarkoitetulle laitteistolle, pääsynvalvonnalla varmistetaan, että laitteiston ulkopuolelta ei pääse avaimiin käsiksi.

Varmentajan yksityinen allekirjoitusavain täytyy suojata HSM-laitteella (Hardware Security Module), joka noudattaa vähintään FIPS 140-2 level 2 -standardia.

7.1.7 Varmentajan yksityisen avaimen tallentaminen kolmannen osapuolen toimesta

Varmentajan yksityistä allekirjoitusavainta ei anneta säilytykseen kolmansille osapuolille siten, että se olisi tietyissä olosuhteissa varmentajan toimintaan kuulumattomien henkilöiden käytettävissä (menetelmää kutsutaan nimellä key escrow).

7.1.8 Varmentajan yksityisen avaimen varmuuskopiointi

Varmentajan yksityisestä avaimesta otetaan varmuuskopioita siten, että palauttaminen varmuuskopiosta voidaan tehdä samaa turvallisuustasoa noudattaen kuin varmentajan yksityisen avaimen siirto.

7.1.9 Varmentajan yksityisen avaimen siirto

Varmentajan on huolehdittava, että varmentajan avaimet siirretään valvotuissa olosuhteissa ja avaimet eivät ole missään vaiheessa yhdessä paikassa selväkielisenä. Avaimet on oltava joko salattuna tai jaettuna useampaan erilliseen osaan, jotka siirretään erillisinä.

Erityisesti on otettava huomioon, että varmentajan avainten siirto tapahtuu fyysisesti turvallisessa ympäristössä luotettujen toimenhaltijoiden toimesta. Tehtävän suorittaminen vaatii vähintään kahden henkilön yhtäaikaista paikallaoloa. Niiden luotettujen toimenhaltijoiden määrä, jotka ovat oikeutettuja suorittamaan tämän toimenpiteen, on rajattava mahdollisimman pieneksi

7.1.10 Varmentajan Yksityisen avaimen arkistointi

Varmentajan Yksityistä avainta ei arkistoida.

7.1.11 Varmentajan Yksityisen avaimen aktivointi

Varmentajan yksityinen avain aktivoidaan samalla, kun avaimet luodaan kappaleen 7.1.1 ”Varmentajan avainparin luominen” mukaisesti. Avain säilyy aktiivisena kunnes sen käyttö keskeytetään esim. huoltotoimenpiteiden takia.

7.1.12 Varmentajan yksityisen avaimen deaktivointi

Varmentajan yksityisen avaimen deaktivointi tehdään tarvittaessa esim. huoltotoimenpiteiden takia.

7.1.13 Varmentajan yksityisen avaimen tuhoaminen

Varmennetuotanto huolehtii siitä, että varmentajan yksityiset allekirjoitusavaimet tuhotaan tai että niitä ei käytetä niiden elinkaaren päättymisen jälkeen.

7.1.14 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 on vastuussa avainparin turvallisesta luomisesta ja yksityisen avaimen luottamuksellisuuden säilymisestä.

Varmenteen haltijan yksityistä avainta ei koskaan toimiteta varmentajalle.

7.2.2 Varmenteen haltijan julkisen avaimen toimittaminen varmentajalle

Varmenteen haltija, joka luo avainparin, toimittaa varmentajan tietojärjestelmään WS-kanavan kautta XML-sanomalla julkisen avaimen sisältämän varmennepyynnön, jonka alkuperä tarkistetaan sähköisestä allekirjoituksesta tai kertakäyttöisellä tunnuksella ja salasanalla. Varmentajan tietojärjestelmä lähettää varmenteen haltijan julkisen avaimen sisältämän Varmennepyynnön XML-sanomalla salattua yhteyttä pitkin varmennusjärjestelmään.

7.2.3 Varmenteen haltijan avainten pituudet ja käytetty algoritmi

Varmenteen haltijan yksityisen avaimen pituus ja algoritmi, jota käytetään avaimen kanssa, täytyy valita siten, että niitä pidetään yleisesti riittävän turvallisina.

7.2.4 Varmenteen haltijan avainparin käyttöikä

Varmenteen haltijan julkisen ja yksityisen avaimen käyttöikä on sama kuin niihin liittyvän varmenteen voimassaoloaika. Julkisia ja yksityisiä avaimia ei saa enää käyttää, mikäli salausalgoritmit ja niihin liittyvät parametrit eivät enää ole riittävän vahvoja tai muuten sopivia.

7.2.5 Varmenteen haltijan avainten käyttötarkoitukset

Näiden Varmenneperiaatteiden mukaan myönnettyihin varmenteisiin liittyviä yksityisiä avaimia voidaan käyttää vain seuraavien turvapalveluiden toteuttamiseksi:

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

7.2.6 Varmenteen haltijan Yksityisen avaimen suojaaminen

Varmenteen haltijan tulee suojata varmenteeseen liittyvä yksityinen avain.

7.2.7 Varmenteen haltijan Yksityisen avaimen varmuuskopiointi

Varmenteen haltija vastaa yksityisen avaimensa säilytyksestä.

7.2.8 Varmenteen haltijan Yksityisen avaimen arkistointi

Varmenteen haltijan Yksityistä avainta ei arkistoida varmentajan toimesta.

7.2.9 Varmenteen haltijan Yksityisen avaimen tuhoaminen

Varmenteen haltija vastaa yksityisen avaimensa tuhoamisesta.

7.2.10 Varmenteen haltijan Julkisen avaimen arkistointi

Varmentaja arkistoi varmenteen haltijan julkisen avaimen kappaleen 5.7 ”Tietojen arkistointi” mukaisesti.

**7.3 TIETOJÄRJESTELMIEN TURVARATKAISUT**

Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutoksilta. Erityisesti seuraavat seikat on otettu huomioon:

- kaikkien käyttäjien tunnistaminen
- roolipohjainen pääsynvalvonta
- kriittisten toimintojen vaatima useamman henkilön valvonta
- auditointilokien luonti, auditointitietojen katselu ja tietoturvaan liittyvien tapahtumien arkistointi
- varmuuskopiot, varajärjestelmät ja palauttaminen
- tietojen turvallinen tuhoaminen, kun niitä ei enää tarvita.

**7.4 ELINKAAREN HALLINNAN TURVARATKAISUT**

7.4.1 Järjestelmäkehityksen hallinta

Varmennetuotanto käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutoksilta.

Kaikkien operointiin liittyvien ohjelmistojen uusille päivityksille, versioille ja asennettaville korjauksille on olemassa muutoksenhallintakäytännöt.

### 7.4.2 Tietoturvallisuuden hallinta

#### 7.4.2.1 Tietoturvallisuuden ylläpito

Varmentajan ja mahdollisen Varmennetuotannosta vastaavan alihankkijan on huolehdittava siitä, että hallinta- ja ylläpitokäytännöt ovat riittäviä ja turvallisia.

#### 7.4.2.2 Resurssien hallinta

Varmentaja vastaa siitä, että resurssien ja tiedon suojaustaso on riittävä.

#### 7.4.2.3 Käyttöpalvelun hallinta

Varmennetuotanto vastaa siitä, että sen järjestelmät ovat turvallisia sekä huolellisesti ylläpidettyjä ja että toimintahäiriön riski on minimaalinen. Luotetuille toimenhaltijoille luodaan ja toteutetaan riittävät toimintamallit ja -käytännöt. Varmennusjärjestelmän tietojen eheys suojataan viruksilta sekä luvattomilta ja järjestelmää vahingoittavilta ohjelmilta. Kaikkia tallennuslaitteita, tietovälineitä ja tietovarastoja käsitellään huolellisesti, jotta estettäisiin vahingot, murrot ja luvaton käyttö.

Kapasiteetin käyttöä seurataan ja tulevia kapasiteettitarpeita arvioidaan sen varmistamiseksi, että riittävä prosessointiteho ja tallennuskapasiteetti ovat saatavilla.

Varmennetuotannossa tietoturvaan liittyvät käyttötoiminnot täytyy erottaa normaaleista järjestelmien käyttötoiminnoista.

#### 7.4.2.4 Järjestelmien pääsynvalvonta

Varmentaja ja mahdollinen varmennetuotannosta vastaava alihankkija huolehtivat siitä, että vain tietyillä valtuutetuilla henkilöillä on pääsy järjestelmiin. Järjestelmien käyttäjien hallintaan kuuluu käyttäjätunnusten luonti, käytön seuranta ja oikea-aikainen käyttöoikeuksien muuttaminen ja poisto.

Järjestelmissä täytyy olla riittävät turvamenettelyt erottamaan toisistaan kappaleessa 6.2.1 ”Luotetut toimenhaltijat” määriteltyjen toimenhaltijoiden roolit. Erityisesti varmennetuotannossa tietoturvan ylläpitäjän rooli on pidettävä erillään käyttötoiminnoista. Henkilöstön tunnistus on suoritettava onnistuneesti ennen kuin he voivat käyttää varmenteiden hallintaan liittyviä kriittisiä ohjelmia.

Varmenteiden julkaisuun käytetty sovellus käyttää pääsynvalvontaa estämään luvattomat yritykset poistaa, lisätä tai muuttaa varmenteita tai niihin liittyviä tietoja.

Sulkulistapalveluun käytettävä sovellus käyttää pääsynvalvontaa estämään luvaton sulkulistan tietojen muuttaminen.

#### 7.4.2.5 HSM-laitteen elinkaaren hallinta

Varmennetuotanto huolehtii Varmenteiden ja Sulkulistojen allekirjoitukseen käytettävän HSM-laitteen tietoturvasta koko sen elinkaaren ajan siten, että:

- Laitteeseen ei pääse käsiksi sen toimituksen tai varastoinnin aikana siten, että se ei olisi havaittavissa.

- Varmentajan allekirjoitusavainten asentaminen, varmistus ja palauttaminen laitteeseen vaativat vähintään neljän henkilön yhtäaikaista paikallaoloa.
- Laite toimii käytössä oikein.
- Laitteeseen tallennetut varmentajan yksityiset allekirjoitusavaimet tuhotaan, kun laitteisto poistetaan käytöstä.

### 7.5 TIETOLIIKENNEVERKON TURVARATKAISUT

Varmentaja ja mahdollinen varmennetuotannosta vastaava alihankkija huolehtivat verkon turvallisuuden hallinnasta mm. seuraavin toimenpitein:

- Varmennetuotannon sisäinen verkko suojataan ulkoisilta kolmansien osapuolten käyttämiltä verkoilta.
- Luottamuksellinen tieto suojataan, kun sitä siirretään turvattomissa verkoissa.
- Varmennetuotanto vastaa siitä, että sen paikallisverkon komponentit (esim. reitittimet) pidetään fyysisesti turvallisessa ympäristössä.
- Varmennetuotannossa seurataan järjestelmiä niissä mahdollisesti ilmenevien yllättävien tapahtumien varalta jatkuvan monitoroinnin, valvonnan ja hälytyslaitteiston avulla. Tällaisiin tapahtumiin luetaan mm. luvattoman käytön yritys tai epänormaali resurssien käyttö.

## 8 VARMENNE- JA SULKULISTAPROFIILIT

Kaikki Samlink Customer CA:n myöntämät varmenteet noudattavat X.509–standardia. Varmenteet täyttävät dokumentin RFC 5280 ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile" vaatimukset.

Samlink Customer CA:n julkaisemat sulkulistat muodostetaan aina täydellisinä normaalilla PKIX-standardin versio2-formaatilla siten että tiivistealgoritmina on SHA256.

Sulkulistan yksityiskohtainen profiili on kuvattu kappaleessa 8.1.3.

### 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<br>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<br>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 |

### 8.1.2 Käyttäjävarmenne

WS-Aineistopalvelut varmenteessa käytetyt kentät:

| **Kentän nimi** | **Field name** | **Kentän sisältö** |
|---|---|---|
| Myöntäjä | Issuer | CN=Samlink Customer CA, O=Samlink, C=FI |
| Avaimen pituus | Key | 2048 bits/RSA |
| Tiivisteet | Signature algorithm | SHA256 |
| Yksikäsitteinen nimi | DN | SN,CN,O,C (Pankin sopimusjärjestelmästä tulleet arvot); muut pyynnön mukaan |
| Laajennukset | | |
| Varmenteen haltijan julkisen avaimen tunniste | Subject Key Identifier | Avaimen tiiviste 20-tavuisena |
| Varmentajan julkisen avaimen tunniste | Authority Key Identifier | KeyID=02 aa 0c 9e bd e9 48 81 27 08 28 e6 e8 de 14 f7 15 8c b9 b6 |
| Revokointilistan julkaisuosoite | CDP CRL distribution points | [1] URL=ldap://194.252.124.241:389/cn=Samlink%20Customer%20CA,o=Samlink,c=fi?certificaterevocationlist;binary |
| Avaimen käyttötarkoitus | Key usage | Critical; Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment |
| CP – varmennpolitiikan tunnus | | Arvona: Samlink Customer CA Varmenneperiaat-teet WS-Aineistopalvelut varmenteita varten OID: 1.2.246.558.10.09704098.11.2 V.1.0 |

8.1.3 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 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<br>• O = Samlink<br>• 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 VARMENNEPERIAATTEIDEN HALLINNOINTI

### 9.1 MUUTOSMENETTELY

Varmentaja voi muuttaa määrityksiä lainsäädännöllisten tai toiminnallisten vaatimusten vuoksi. Määritysten muutokset on kirjattava varmenneperiaatteet- ja varmennuskäytäntödokumentteihin seuraavassa kuvatulla tavalla.

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 muutettu sekä uudet Varmenneperiaatteet on julkaistu. Suuremmasta muutoksesta ilmoitetaan vähintään 15 päivää ennen sen voimaantuloa.

9.1.1 Kohdat, joita voi muuttaa ilman hyväksymismenettelyä

Tähän dokumenttiin voidaan tehdä oikeinkirjoitukseen ja ulkoasuun liittyviä korjauksia sekä muutoksia yhteystietoihin ilman hyväksymismenettelyä.

Dokumentista voidaan julkaista käännöksiä eri kielillä ilman erillistä hyväksymismenettelyä. Käännöksen ja suomenkielisen tekstin ollessa ristiriidassa keskenään suomenkielinen teksti on voimassa.

Varmennuskäytännön uudistuminen ei vaadi tiedonantoa.

9.1.2 Muutokset, joiden johdosta täytyy laatia uusi varmenneperiaatteet-dokumentti

Uusi varmenneperiaatteet-dokumentti saa uuden OID:n. Varmenneperiaatteet ovat uudet, jos aiemmin myönnetyt varmenteet eivät enää mahdu uusien Varmenneperiaatteiden piiriin.

Varmennuskäytännön uudistuminen ei edellytä uuden Varmenneperiatteet-dokumentin laatimista.

**9.2 HYVÄKSYMISMENETTELY**

Kaikki muutokset näihin varmenneperiaatteisiin, lukuun ottamatta ulkoasuun, oikeinkirjoitukseen tai yhteystietoihin liittyviä muutoksia, täytyy hyväksyä Samlink PKI ohjausryhmässä. Esittelijänä toimii Samlinkin turvallisuusjohtaja.

**9.3 JULKAISEMINEN**

Varmenneperiaatteet 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 varmenneperiaatteet 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.

Varmenneperiaatteet voidaan toimittaa erikseen sovittaessa myös muulla tietovälineellä suoraan niille osapuolille, joiden edellytetään noudattavan sitä.