

**SAMLINK CUSTOMER CA**

**Varmenneperiaatteet**

**WS-AINEISTOPALVELUT  
VARMENTEITA VARTEN**

OID: 1.2.246.558.10.09704098.11.4

VOIMASSA 30.11.2022 ALKAEN

## Contents

<b>LUETTELO VERSIOISTA .....</b>	<b>6</b>
<b>1 KÄSITTEET JA LYHENTEET .....</b>	<b>7</b>
<b>2 JOHDANTO.....</b>	<b>11</b>
<b>2.1 YLEISKUVAUS .....</b>	<b>11</b>
<b>2.2 TUNNISTEET .....</b>	<b>11</b>
2.2.1 Varmenteen ja sitä vastaavien Varmenneperiaatteiden yhteys .....	11
<b>2.3 VARMENNUSORGANISAATIO JA VARMENTEIDEN SOVELTUVUUS .....</b>	<b>11</b>
2.3.1 Varmentaja .....	11
2.3.2 Varmennetuotanto .....	12
2.3.3 Rekisteröijä.....	12
2.3.4 Varmenteen haltija.....	12
2.3.5 Luottava osapuoli .....	12
2.3.6 Sulkupalvelu .....	12
2.3.7 Hakemisto .....	13
2.3.8 Soveltuvuus.....	13
<b>2.4 YHTEYSTIEDOT .....</b>	<b>13</b>
<b>3 YLEISET EHDOT .....</b>	<b>14</b>
<b>3.1 VELVOLLISUUDET.....</b>	<b>14</b>
3.1.1 Varmentajan velvollisuudet .....	14
3.1.2 Varmennetuotantoon liittyvät velvollisuudet .....	14
3.1.3 Rekisteröijän velvollisuudet.....	15
3.1.4 Varmenteen haltijan velvollisuudet.....	15
3.1.5 Varmenteeseen Luottavan osapuolen velvollisuudet .....	16
3.1.6 Sulkupalvelun velvollisuudet .....	16
3.1.7 Tietovarastoon liittyvät velvollisuudet.....	16
<b>3.2 VASTUUVELVOLLISUUS.....</b>	<b>16</b>
3.2.1 Varmentajan vastuuvollisuus.....	16
3.2.2 Rekisteröijän vastuuvollisuus .....	17
<b>3.3 TALOUDELLINEN VASTUU .....</b>	<b>17</b>
3.3.1 Vahingonkorvaukset .....	17
3.3.2 Korvaukset Varmenteen haltijalta .....	17
3.3.3 Osapuolten väliset suhteet.....	18
3.3.4 Hallinnolliset prosessit .....	18
<b>3.4 TULKINTA JA TÄYTÄNTÖÖNPANO.....</b>	<b>18</b>
3.4.1 Sovellettava lainsäädäntö .....	18
3.4.2 Erimielisyyksien ratkaiseminen .....	18
<b>3.5 MAKSUT .....</b>	<b>18</b>
<b>3.6 TIETOJEN JULKAISEMINEN JA TIETOVARASTO .....</b>	<b>18</b>
3.6.1 Varmentajan tietojen julkaisu .....	18
3.6.2 Julkaisutaajuus .....	18
3.6.3 Pääsynvalvonta .....	19

<b>3.7 TARKASTUKSET</b> .....	<b>19</b>
<b>3.8 LUOTTAMUKSELLISUUS</b> .....	<b>19</b>
<b>3.9 OMISTUS- JA IMMATERIAALIOIKEUDET</b> .....	<b>19</b>
<b>3.10 SOPIMUKSET</b> .....	<b>19</b>
<b>4 TUNNISTUS JA TODENTAMINEN</b> .....	<b>20</b>
<b>4.1 NIMEÄMISKÄYTÄNTÖ VARMENTAJAN VARMENTEESTA</b> .....	<b>20</b>
4.1.1 Varmentajan Varmenteen yksilöintitiedot .....	20
<b>4.2 ENSIREKISTERÖINTI</b> .....	<b>20</b>
4.2.1 Nimeämiskäytännöt .....	20
4.2.2 Nimivaatimukset .....	21
4.2.3 Nimien yksikäsitteisyys .....	21
4.2.4 Nimiepäselyyksien ratkaiseminen .....	21
4.2.5 Yksityisen avaimen hallussapidon osoittaminen .....	21
4.2.6 Rekisteröintivastaavan todentaminen .....	21
4.2.7 Organisaation todentaminen.....	21
4.2.8 Varmenteen haltijan tunnistaminen.....	22
<b>4.3 VARMENTEEN UUSIMINEN VOIMASSAOLON PÄÄTTYESSÄ</b> .....	<b>22</b>
<b>4.4 VARMENTEEN UUSIMINEN SEN VOIMASSAOLON PÄÄTTYMISEN TAI MITÄTÖINNIN JÄLKEEN</b> .....	<b>22</b>
<b>4.5 WEB-SERVICES-YHTEYS SOPIMUKSEN VOIMASSAOLON KESKEYTTÄMISPYYNTÖ</b> .....	<b>22</b>
<b>4.6 VARMENTEEN PALAUTTAMISPYYNTÖ</b> .....	<b>23</b>
<b>5 TOIMINNALLISET VAATIMUKSET</b> .....	<b>24</b>
<b>5.1 VARMENTEEN HAKEMINEN</b> .....	<b>24</b>
<b>5.2 VARMENTEEN MYÖNTÄMINEN</b> .....	<b>24</b>
<b>5.3 VARMENTEEN HYVÄKSYMINEEN</b> .....	<b>24</b>
<b>5.4 VARMENTEEN MITÄTÖINTI JA VARMENTEEN VOIMASSAOLON KESKEYTTÄMINEN</b> .....	<b>24</b>
5.4.1 Olosuhteet Varmenteen mitätöimiseksi.....	24
5.4.2 Oikeus pyytää Varmenteen mitätöintiä.....	25
5.4.3 Mitätöintipyyntömenettely .....	25
5.4.4 Mitätöintipyyntö odotusaika.....	25
5.4.5 Olosuhteet Varmenteen voimassaolon keskeyttämiseksi.....	26
5.4.6 Oikeus Varmenteen voimassaolon keskeyttämiseen .....	26
5.4.7 Menettelytapa Varmenteen voimassaolon keskeyttämiseksi .....	26
5.4.8 Sulkulistan julkaisu .....	26
5.4.9 Sulkulistan tarkastusvaatimukset.....	26
<b>5.5 VARMENTEEN PALAUTTAMINEN KÄYTTÖÖN</b> .....	<b>27</b>
<b>5.6 TIETOTURVALLISUUDEN VALVONTA</b> .....	<b>27</b>
<b>5.7 TIETOJEN ARKISTOINTI</b> .....	<b>27</b>
<b>5.8 VARMENTAJAN AVAINTEN UUSIMINEN</b> .....	<b>27</b>
<b>5.9 KATASTROFISTA JA VARMENTAJAN AVAIMEN PALJASTUMISESTA TOIPUMINEN</b> .....	<b>27</b>
5.9.1 Tietokone-laitteet, ohjelmistot, ja/tai tiedot ovat korruptoituneet .....	28
5.9.2 Varmentajan Yksityinen avain on paljastunut.....	28

<b>5.10 VARMENNUSTOIMINNAN LOPETTAMINEN .....</b>	<b>28</b>
<b>6 TURVATOIMENPITEET .....</b>	<b>29</b>
<b>6.1 FYYSISET TURVARATKAISUT .....</b>	<b>29</b>
<b>6.2 TOIMINNALLISET TURVARATKAISUT .....</b>	<b>29</b>
6.2.1 Luotetut toimenhaltijat.....	29
6.2.2 Tehtäviin vaadittavien henkilöiden lukumäärät.....	30
6.2.3 Luotettujen toimenhaltijoiden tunnistaminen ja todentaminen .....	30
<b>6.3 HENKILÖTURVALLISUUS .....</b>	<b>30</b>
6.3.1 Taustatietojen tarkastusmenettely .....	30
6.3.2 Koulutusvaatimukset.....	30
6.3.3 Seuraukset luvattomista toimenpiteistä.....	30
6.3.4 Sopimustyöntekijävaatimukset.....	31
<b>7 TEKNISET TURVARATKAISUT .....</b>	<b>32</b>
<b>7.1 VARMENTAJAN AVAINPARIN LUOMINEN, KÄYTTÖÖNOTTO JA SUOJAAMINEN.....</b>	<b>32</b>
7.1.1 Varmentajan Avainparin luominen .....	32
7.1.2 Varmentajan Julkisen avaimen toimittaminen Luottaville osapuolille.....	32
7.1.3 Varmentajan avainten pituudet ja käytetty algoritmi .....	32
7.1.4 Varmentajan Avainparin käyttöikä.....	32
7.1.5 Varmentajan avainten käyttötarkoitukset .....	32
7.1.6 Varmentajan Yksityisen avaimen suojaaminen .....	32
7.1.7 Varmentajan Yksityisen avaimen tallentaminen kolmannen osapuolen toimesta .....	33
7.1.8 Varmentajan Yksityisen avaimen varmuuskopiointi .....	33
7.1.9 Varmentajan Yksityisen avaimen siirto.....	33
7.1.10 Varmentajan Yksityisen avaimen arkistointi .....	33
7.1.11 Varmentajan Yksityisen avaimen aktivointi .....	34
7.1.12 Varmentajan Yksityisen avaimen deaktivointi .....	34
7.1.13 Varmentajan Yksityisen avaimen tuhoaminen.....	34
7.1.14 Varmentajan Julkisen avaimen arkistointi .....	34
<b>7.2 VARMENTEEN HALTIJAN AVAINPARIN LUOMINEN, KÄYTTÖÖNOTTO JA SUOJAAMINEN .....</b>	<b>34</b>
7.2.1 Varmenteen haltijan Avainparin luominen.....	34
7.2.2 Varmenteen haltijan Julkisen avaimen toimittaminen Varmentajalle .....	34
7.2.3 Varmenteen haltijan avainten pituudet ja käytetty algoritmi.....	34
7.2.4 Varmenteen haltijan Avainparin käyttöikä .....	34
7.2.5 Varmenteen haltijan avainten käyttötarkoitukset.....	35
7.2.6 Varmenteen haltijan Yksityisen avaimen suojaaminen.....	35
7.2.7 Varmenteen haltijan Yksityisen avaimen varmuuskopiointi .....	35
7.2.8 Varmenteen haltijan Yksityisen avaimen arkistointi.....	35
7.2.9 Varmenteen haltijan Yksityisen avaimen tuhoaminen .....	35
7.2.10 Varmenteen haltijan Julkisen avaimen arkistointi.....	35
<b>7.3 TIETOJÄRJESTELMIEN TURVARATKAISUT .....</b>	<b>35</b>
<b>7.4 ELINKAAREN HALLINNAN TURVARATKAISUT .....</b>	<b>35</b>
7.4.1 Järjestelmäkehityksen hallinta .....	35
7.4.2 Tietoturvallisuuden hallinta .....	36
<b>7.5 TIETOLIIKENNEVERKON TURVARATKAISUT .....</b>	<b>37</b>
<b>8 VARMENNE- JA SULKULISTAPROFIILIT.....</b>	<b>38</b>
8.1.1 CA-varmenne .....	38

8.1.2 Käyttäjävarmenne..... 39  
8.1.3 Sulkulistaprofiili..... 39

**9 VARMENNEPERIAATTEIDEN HALLINNOINTI .....41**

**9.1 MUUTOSMENETTELY .....41**

9.1.1 Kohdat, joita voi muuttaa ilman hyväksymismenettelyä ..... 41

9.1.2 Muutokset, joiden johdosta täytyy laatia uusi Varmenneperiaatteet-dokumentti..... 41

**9.2 HYVÄKSYMISMENETTELY .....41**

**9.3 JULKAISEMINEN.....41**

## LUETTELO VERSIOISTA

### Varmennuskäytännön versiotiedot

Versio numero	Päiväys	Muutokset
1.0	18.09.2009	Hyväksytty PKI-ohjausryhmässä
1.1	18.10.2022	1. HTTP lisätty, FIPS-140-1 -> 3 päivitetty, lisätty TLS, varmenne lisätty yksityinen avain 2 Päivitetty RFC 2527 -> 3647 2.2 OID päivitetty 2.4 Päivitetty Riski- ja turvallisuusosasto, turvallisuusjohtaja. PKI-ohjausryhmän kokoonpano. 3.1.7 ldap -> http muutos 5.4.9 url-päivitys 7.1.6 FIPS 140-2 level 2 - standardi muutettu FIPS 140-3:ksi. 8.1.2 Revokointilistan julkaisuosoite ldap → http 8.1.3 muutos LDAPS -> HTTP
1.1	7.11.2022	Versio 1.1 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-140-2 ja FIPS-140-3 ovat salausmoduuleita ja -algoritmeja koskevia tietoturva vaatimuksia.
Hakemisto	Tietovarasto, johon julkaistaan Sulkulistat. Hakemisto on käytettävissä julkisessa tietoverkossa.
HSM-laite	Hardware Security Module. Salausavainten suojaamiseen tarkoitettu erikoislaite.
HTTP	Hypertext Transfer Protocol. Hypertekstin siirtoprotokolla on protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
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 infrastruktuurissa 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-yhteyssoimimusten haltijana. Rekisteröijä voi olla myös Samlink.
Rekisteröinti	Prosessi, joka sisältää Varmenteen haltijan tunnistamisen, tarvittavien tietojen keräämisen ja niiden toimittamisen Varmentenepyyntöä varten. Rekisteröintiin voi liittyä useita Rekisteröintivastaavia.
Rekisteröintivastaava	Henkilö, joka vastaa Rekisteröintitehtävistä, esim. Varmentenepyyntöjen oikeellisuuden tarkastamisesta ja Varmenteiden luovuttamisesta Varmenteiden haltijalle. Rekisteröintivastaavana toimiminen edellyttää pankin ja Varmentajan välistä sopimusta tehtävän hoitamisesta pankissa sekä toimihenkilöltä erillistä Palvelusopimus-käyttövaltuutta. 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 Pankkiyhteyssoimimuksen sekä Web-Services-yhteyssoimimuksen
Sulkulista	Kts. CRL
Sulkupalvelu	Web-Services-yhteys soimimusten ja Varmenteiden sulkupyntöjä 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	<p>Varmenteen haltijan nimestä ja Julkisesta avaimesta muodostettu tieto, jonka Varmentaja on allekirjoittanut sähköisesti. Varmenne todistaa tietyn Julkisen avaimen kuuluvan tietylle haltijalle.</p> <p>Yksityinen avain, joka tunnetaan myös nimellä salainen avain, on kryptografiassa muuttuja, jota käytetään algoritmin kanssa tietojen salaamiseen ja purkamiseen.</p>
Varmennuskäytäntö	Kuvaa Varmentajan toiminnan Varmenneperiaatteita noudattaen.
Varmennepalvelu	<p>Varmenteiden tuottamiseen liittyvät järjestelmät, henkilöt ja prosessit kokonaisuutena.</p> <p>Varmennepalvelun osatoimintoja ovat Rekisteröinti, Varmennetuotanto, Korttituotanto, Hakemistopalvelu, Sulkupalvelu ja Sulkulistapalvelu.</p>
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 asiointissaan 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 tarkoitettua, vastaavalla Julkisella avaimella

	salatut tiedot. Yksityisellä avaimella voidaan myös luoda haltijan sähköinen allekirjoitus.
X.509	Standardi, joka kuvaa Varmennepalvelun vaatimuksia ja komponentteja.
TLS	Transport Layer Security (TLS) on salausprotokolla, joka on suunniteltu tarjoamaan tietoturvaa tietoliikenteessä tietoverkossa.

Tässä dokumentissa em. käsitteet on kirjoitettu isolla alkukirjaimella.

## 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 1.2.246.558.10.09704098.11.4, v.1.1)*

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-yhteyssojimuksella kerrotulla jakelulla.

#### 2.2.1 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.

### 2.3 VARMENNUSORGANISAATIO JA VARMENTEIDEN SOVELTUVUUS

#### 2.3.1 Varmentaja

Samlink toimii Varmentajana, jolla on kokonaisvastuu Varmennepalvelun toimittamisesta.

Varmentaja voi myöntää myös muita kuin tämän Varmenneperiaatteiden mukaisia Varmenteita. Näistä Varmenteista laaditaan erilliset Varmenneperiaatteet.

### 2.3.2 Varmennetuotanto

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

### 2.3.3 Rekisteröijä

Rekisteröijinä voivat toimia Varmentajan omaan organisaatioon kuuluvat Rekisteröintitoimintaan 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.

### 2.3.4 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.

### 2.3.5 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.

### 2.3.6 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.

### 2.3.7 Hakemisto

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

### 2.3.8 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-yhteyssojimuksessa saattaa olla avainten käyttötarkoituksiin liittyviä rajoituksia, jotka täytyy ottaa huomioon Varmenteita käytettäessä.

## 2.4 YHTEYSTIEDOT

Samlinkin Riski- ja Turvallisuusosasto vastaa Varmenneperiaatteiden hallinnoimisesta, ylläpidosta ja päivityksistä. Varmenneperiaatteiden tekijänoikeudet kuuluvat Samlinkille.

Varmenneperiaatteet hyväksyy Samlinkin johtoryhmän nimittämä Samlink PKI-ohjausryhmä. PKI:n ohjausryhmään kuuluvat Samlinkin turvallisuusjohtaja ja infrahallinnon johtaja. Esittelijänä toimii Samlinkin turvallisuusjohtaja.

Varmenneperiaatteita koskevat kysymykset voi lähettää osoitteeseen:

Oy Samlink Ab                    [turvallisuus@samlink.fi](mailto: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 pyydetty 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 suoritettut toimeksiannot

### 3.1.7 Tietovarastoon liittyvät velvollisuudet

Varmentaja julkaisee Hakemistossa Sulkulistat kappaleen 2.3.7 ”[Hakemisto](#)” mukaisesti.

Hakemistoon on kaikkialta pääsy HTTP-protokollalla. Varmentaja julkaisee Varmennepalvelua koskevaa dokumentaatiota kappaleessa 3.6 ”[Tietojen julkaiseminen ja tietovarasto](#)” mainituilla jakelukanavilla.

## 3.2 VASTUUVELVOLLISUUS

### 3.2.1 Varmentajan vastuuvollisuus

#### 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 vastuuvollisuus

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 voimassaoloa 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-yhteys sopimuksessa 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, määrittäisiin 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 käyttöehtosopimuksen, 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 osapuolten 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 myönnettyissä 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 aakostusnimi	CN=Oy Firma AB
Organisaatio (Organization)	Organisaation tai organisaatioryhmän selväkielinen nimi	O=Saastopankki

Maa (Country)	Maa, jossa ym. organisaatio toimii	C=FI
---------------	------------------------------------	------

Edellä mainitut osat ovat pakollisia kaikissa Varmenneperiaatteiden mukaisesti myönnettyissä 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 myöntämässä Varmenteissa Sukunimi-kentässä olevan käyttäjätunnuksen täytyy olla yksikäsitteisesti sopimukseen yhdistettävissä ja Palvelusopimusjärjestelmä huolehtii kentän yksikäsitteisyydestä. Poikkeuksena Samlinkin allekirjoitusvarmenne, jolle ei ole olemassa sopimusta ja sen Sukunimi-kentän arvoksi annetaan sellainen arvo, jota ei tule esiintymään Palvelusopimusjärjestelmässä.

#### 4.2.4 Nimiepäselvyyksien ratkaiseminen

Varmenteen yksilöintitietoa (käyttäjätunnus) hallitaan Palvelusopimusjärjestelmässä, joka huolehtii yksikäsitteisyydestä. 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 Varmennepyyntö, joiden alkuperä voidaan tunnistaa sähköisestä allekirjoituksesta tai Web-Services-yhteys sopimuksen haltijan toimittamalla tunnuksesta ja siihen liitettyllä kertakäyttöisellä salasanalla. Varmennepyyntö 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 varmennepyyntö 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 ja
- Varmentajan tietojärjestelmän on käsitellyt Varmenteen Varmenteen haltijalta saamansa Varmennepyyntö sekä palauttanut onnistuneesti Varmenteen Varmenteen haltijalle ja
- kun Varmenne on asennettu käyttöön, ja
- 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 Pankkiyhteys sopimuksen 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 Mitätöintipyynnön menettely

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

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. Mitätöintipyynnö 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.

#### 5.4.4 Mitätöintipyynnön odotusaika

Sopimusten sulkupalvelu ottaa mitätöintipyynnöjä 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 mitätöintipyynnö.

Sulkulistapalvelu huolehtii Varmenteen viennistä Sulkulistalle ja Sulkulistan julkaisusta määrävälein kappaleen 5.4.8 ”[Sulkulistan julkaisu](#)” mukaisesti.

#### 5.4.5 Olosuhteet Varmenteen voimassaolon keskeyttämiseksi

Varmenteen voimassaolon keskeytys ei ole mahdollinen.

#### 5.4.6 Oikeus Varmenteen voimassaolon keskeyttämiseen

Varmenteen voimassaolon keskeytys ei ole mahdollinen.

#### 5.4.7 Menettelytapa Varmenteen voimassaolon keskeyttämiselle

Varmenteen voimassaolon keskeytys ei ole mahdollinen.

#### 5.4.8 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.

#### 5.4.9 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 senhetkinen 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= <http://httpcrl.trust.telia.com/samlinkcustomerca.crl>

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 pyydettyäessä luovuttaa käytettäväksi varmennuksen todisteena oikeudessa.

Arkistoitavat tiedot säilytetään lainsäädännön tai viranomaisten vaatimusten mukaisen ajan suojattuina muuttamiselta ja häviämislä, 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 väriin käsiin ja tietokoneressien,

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 turvalvonta.

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
- Jättemateriaalin 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 käyttöä. 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 uusiutumisen 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 liittyvien 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 kestämaan 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 tarkoitettulle 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 3-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 Varmennepyyntön, jonka alkuperä tarkistetaan sähköisestä allekirjoituksesta tai kertakäyttöisellä tunnuksella ja salasanalla. Varmentajan tietojärjestelmä lähettää Varmenteen haltijan Julkisen avaimen sisältämän Varmennepyyntön 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 muutoksenhaallintakäytännöt.

#### 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 tuhoetaan, 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 käyttämillä 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
Allekirjoitus-algoritmi	Signature algorithm	sha256WithRSAEncryption
Varmenteen myöntäjä	Issuer	C=FI, O=Samlink, CN=Samlink Customer CA
Voimassaolo-aika	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

## 8.1.2 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	URL= <a href="http://httpcrl.trust.telia.com/samlinkcustomerca.crl">http://httpcrl.trust.telia.com/samlinkcustomerca.crl</a>
Avaimen käyttötarkoitus	Key usage	Critical; Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment
CP - varmennepoliittian tunnus		Arvona:  Samlink Customer CA Varmenneperiaatteet 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 HTTP-protokollalla. Lähdeosoite on <http://httpcrl.trust.telia.com/samlinkcustomerca.crl> .

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 VARMENNEPERIAATTEIDEN HALLINNOINTI

### 9.1 MUUTOSMENETTELY

Varmentaja voi muuttaa määrittämiä lainsäädännöllisten tai toiminnallisten vaatimusten vuoksi. Määrittysten muutokset on kirjattava Varmenneperiaatteet- ja Varmennuskäytäntö-dokumentteihin seuraavassa kuvatulla tavalla.

Mikäli dokumenttiin tehdään hyväksyjien mielestä vähämerkityksinen muutos, dokumentin revisionumeroa (desimaaliosa) kasvatetaan. Mikäli muutos on suurempi, dokumentin versionumeroa (kokonaisuosa) 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 myönnettyt varmenteet eivät enää mahdu uusien Varmenneperiaatteiden piiriin.

Varmennuskäytännön uudistuminen ei edellytä uuden Varmenneperiaatteet-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.