TeliaSonera Finland Oyj

2.12.2008

Sonera CA

Varmennepolitiikka

Sonera Class 2 -varmenne

Voimassa 2.12.2008 lähtien
Versio 2.5

Varmennepolitiikan OID-tunnus:
1.3.6.1.4.1.271.2.3.1.1.2

Ohjelmistovarmenteet

– yksityinen avain tallennettu työasemalle tai palvelimelle

Tämä suomenkielinen versio on epävirallinen käännös englanninkielisestä dokumentista ”Sonera CA Certificate Policy, Sonera Class2 Certificate” joka on alkuperäinen ja virallinen varmennepolitiikka.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

Varmennepolitiikan TeliaSonera Finland CP-Class2 versionhallinta

Versionumero	Dokumentin nimi	Päivämäärä	Kuvaus
V 1.0	Sonera CA, CP - Certificate Policy for Sonera Class 2 Certificates	1.3.2001	Ensimmäinen Class 2 politiikka
V 1.1	Ks. yllä	1.3.2002	Tarkennuksia
V. 2.0	Sonera CA, Varmennepolitiikka, Sonera Class 2 -varmenne	22.9.2003	Rakenteen muutos
V. 2.1	Ks. yllä	22.1.2004	Tarkennuksia
V. 2.2	Ks. yllä	30.5.2005	Tarkennuksia
V. 2.3	Ks. yllä	15.6.2007	Tarkennuksia ja pieniä muutoksia
V. 2.4	Ks. yllä	2.10.2007	Ali-CA määritykset lisätty
V. 2.5	Ks. yllä	13.11.2008	Muutoksia luvuissa 4.4.4, 5.2.2, 6.1.1 ja 6.1.4

Kaikki julkaistut versiot ovat saatavissa osoitteesta:
http://support.partnergate.sonera.com/.

Sisällysluettelo

Copyright © TeliaSonera Finland 2004. All rights reserved

Copyright © TeliaSonera Finland 2004. All rights reserved

Copyright © TeliaSonera Finland 2004. All rights reserved

Copyright © TeliaSonera Finland 2004. All rights reserved

Määritelmiä

Ali-CA: *CA, jonka varmenteiden allekirjoitusavaimen on allekirjoittanut toinen CA. Ali-CA:n toiminta määräytyy kyseisen toisen CA:n mukaan.*

Aktivointitieto*: Tunnusluku (esim. PIN-koodi), jolla Varmenteen haltija aktivoi yksityisen avaimensa. Tunnusluku on annettava erikseen joka kerta kun avainta käytetään.*

Asiakasorganisaatio*: TeliaSonera Finland Oyj:n (jäljempänä "Sonera") yritysasiakas, joka käyttää Soneran varmennepalveluita.*

Avainpari*: Varmenteen haltijan käytössä oleva yksityinen avain ja siihen liittyvä julkinen avain muodostavat avainparin.*

Issuer: *Varmenteen kenttä, jossa määritellään varmenteen allekirjoittanut Varmentaja. Tämän politiikan mukaisesti myönnetyissä varmenteissa Issuer-kentässä Varmentaja on "Sonera Class2 CA".*

Julkinen avain, Public key: *Varmenteen haltijalle kuuluvan asymmetrisen avainparin se osa, joka on Luottavien osapuolten käytössä.*

Julkisen avaimen infrastruktuuri, Public Key Infrastructure (PKI)*: Infrastruktuuri, joka koostuu ohjelmistosta, laitteistosta, henkilöistä, politiikoista ja menettelytavoista, jotka hyödyntävät julkisen avaimen salaustekniikkaa ja joiden avulla voidaan luoda, hallinnoida, säilyttää, jakaa ja peruuttaa varmenteita [PKIX Roadmap].*

Luottava osapuoli*: Osapuoli, joka luottaa varmenteessa oleviin tietoihin tehdessään päätöksiä [ISO/IEC 9594-8; ITU-T X.509].*

Rekisteröijä, Registration Authority, (RA): *Osapuoli, joka on vastuussa Varmenteen haltijan tunnistamisesta, mutta joka ei allekirjoita tai myönnä varmenteita (ts., RA hoitaa tiettyjä toimintoja Varmentajan puolesta) [RFC 2527].*

Rekisteröintivastaava: *Henkilö, joka suorittaa Rekisteröijälle kuuluvia tehtäviä vastuullaan mm. Varmenteiden luonnin ja jakelun hyväksyntä.*

Salaustekninen laite: *Varmentajan käytössä oleva ohjelmistoa ja elektroniikkaa sisältävä laite, joka toteuttaa salausteknisiä algoritmeja ja jota käytetään Varmentajan salausavainten luomisen, tallennuksen ja käytön tietoturvan takaamiseksi.*

Sonera: *Termi tarkoittaa tässä dokumentissa TeliaSonera Finland Oyj:tä.*

Sonera Class2 CA: *Tämä CA voi myöntää Ali-CA varmenteita. Ali-CA:n avain tallennetaan salaustekniseen laitteeseen.*

Sonera Class 2 -varmenne: *Varmenne, joka myönnetään luonnolliselle henkilölle tai Laitteelle. Varmenne ja siihen liittyvä yksityinen avain on tallennettu ohjelmistoon.*

Copyright © TeliaSonera Finland 2004. All rights reserved

Sonera PKI: *Infrastruktuuri, joka koostuu ohjelmistosta, laitteistosta, käytännöistä, menettelytavoista ja politiikoista, joita hallinnoi Sonera CA. Sonera PKI:n avulla pystytään tarjoamaan julkisen avaimen järjestelmää ja varmennusmenettelyjä käyttäviä turvapalveluita.*

Sulkulista, Certificate Revocation List, (CRL): *Lista, joka sisältää tietyn varmentajan myöntämien peruutettujen varmenteiden sarjanumerot sekä muuta peruuttamiseen liittyvää tietoa.*

Sulkulistapalvelu: *Palvelu, josta Luottavat osapuolet voivat tarkistaa onko varmenne peruutettu (esim. hakemisto).*

Sulkupalvelu: *Palvelu, joka hoitaa varmenteiden peruuttamispyyntöjen vastaanottamisen ja lähettää oikeutetut peruuttamispyynnöt edelleen Varmentajalle.*

Sähköinen allekirjoitus: *Sähköisessä muodossa oleva tieto, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä [SAK Laki].*

Tietovarasto: *Järjestelmä, johon Varmentaja on tallentanut varmennustoimintaansa liittyvät julkiset dokumentit ja josta ne ovat noudettavissa. Sonera Class 2 -varmenteisiin liittyvään tietovarastoon pääsee internetin kautta ja se sijaitsee osoitteessa http://support.partnergate.sonera.com/.*

Tilaaja: *Yhden tai useamman Varmenteen haltijan puolesta toimiva Varmentajan asiakas. Varmenteen haltija voi olla Tilaaja joka toimii omasta puolestaan. [ETSI TS 101 456 v1.2.1]*

Varmenne, Certificate: *Varmenteen haltijan julkinen avain sekä muuta tietoa allekirjoitettuna Varmentajan yksityisellä avaimella siten, että niitä ei voi väärentää [ISO/IEC 9594-8; ITU-T X.509.]*

Varmennepolitiikka, Certificate Policy (CP): *Säännösdokumentti, joka määrittelee varmenteen soveltuvuuden tietylle käyttäjäryhmälle ja / tai tietyntyyppisiin sovelluksiin, joilla on yhteiset tietoturvavaatimukset [ISO/IEC 9594-8; ITU-T X.509].*

Varmennepolitiikkayksikkö, Policy Authority: *Varmentajan yksikkö, joka määrittelee, hyväksyy ja ylläpitää varmennepolitiikkaa sekä valvoo sovellettuja käytäntöjä.*

Varmennuskäytäntö, Certification Practice Statement (CPS): *Dokumentti käytännöistä, joita Varmentaja noudattaa myöntäessään varmenteita [RFC 2527].*

Varmentaja, Certification Authority (CA): *Osapuoli, johon yksi tai useampi käyttäjä luottaa varmenteiden luomisessa ja myöntämisessä. Varmentaja voi myös mahdollisesti luoda käyttäjien avaimet. [ISO/IEC 9594-8; ITU-T X.509]. Tässä politiikassa Varmentaja on TeliaSonera Finland Oyj.*

Varmenteen hakija: *Henkilö, jolle haetaan varmennetta. Varmenteen myöntämisen jälkeen kutsutaan nimellä Varmenteen haltija.*

Varmenteen haltija: *Varmenteessa mainittua julkista avainta vastaavan yksityisen avaimen (varmenteessa mainittu) haltija [ETSI TS 101 456 v1.2.1]. Varmenteen haltija voi olla myös laite (tietojärjestelmän komponentti tai ohjelmisto, joista käytetään jatkossa nimitystä ”Laite”).*

Varmenteen valmistaja, Certificate Manufacturer (CM): *Osapuoli, joka on vastuussa määritellyin osin Varmentajan allekirjoittamien varmenteiden tai allekirjoituksen luomisvälineen valmistuksesta ja/tai toimituksesta. Sonera PKI:ssa Varmenteen valmistajana on esim. Korttivalmistaja.*

Yksityinen avain: *Varmenteen haltijalle kuuluvan asymmetrisen avainparin se osa, jota vain kyseinen henkilö tai Laite voi käyttää siihen liittyvän aktivointitiedon avulla.*

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

1 Johdanto

1.1 Yleistä

Tämä dokumentti on varmennepolitiikka (Certificate Policy, CP) luonnollisille henkilöille tai Laitteille (Varmenteen haltija) myönnettäville varmenteille Sonera PKI:ssä (PKI = Public Key Infrastructure, julkisen avaimen infrastruktuuri). Tätä dokumenttia hallinnoi Soneran Varmennepolitiikkayksikkö (Sonera CA Policy Authority). Dokumentti määrittelee politiikan Sonera Class 2 -varmenteille. Varmenteita voidaan käyttää tunnistamiseen ja tiedon tai tapahtuman kiistämättömyyden, luottamuksellisuuden tai eheyden varmistamiseen.

Varmentaja voi luoda Ali-CA:ita Sonera Class2 CA:n alle huolimatta siitä mitä tässä politiikassa myöhemmin määritellään. Tämän politiikan määräykset ja käytännöt eivät koske Ali-CA varmenteita vaan ainoastaan käyttäjä- ja laitevarmenteita. Ali-CA:n myöntämiä varmenteita koskevat määräykset ja käytännöt määritellään aina Ali-CA:n omassa varmennekäytännössä.

Seuraavat vaatimukset pätevät Sonera Class 2 -varmenteisiin:

- Sonera Class 2 myöntämien käyttäjä- ja laitevarmenteiden yksityinen avain on tallennettu työasemalle tai palvelimelle.
- Ali-CA varmenteiden yksityiset avaimet tallennetaan salaustekniselle laitteelle.
- Varmenteen on allekirjoittanut Sonera Class2 CA.
- Varmenteet on allekirjoitettu Varmentajan avaimella, joka on vähintään 2048 bittiä pitkä.
- Henkilö- ja laitevarmenteen voimassaoloaika on enintään viisi (5) vuotta.
- Ali-CA varmenteen voimassaoloaika on enintään kaksitoista (12) vuotta.

Tämän politiikan rakenne perustuu dokumenttiin RFC 2527 ”Certificate Policy and Certification Practices Framework”.

Varmentaja voi hankkia osan toiminnoistaan, esim. varmenteen valmistus (Varmenteen valmistaja, Certificate Manufacturer), rekisteröinti (Rekisteröijä, Registration Authority) ja Sulkupalvelu (Revocation Service), alihankintana. Varmentajalla on kuitenkin aina kokonais- ja vahingonkorvausvastuu myöntämistään varmenteista.

Tämä varmennepolitiikka on tarkoitettu Luottaville osapuolille (Relying Party), jotka tämän politiikan pohjalta voivat arvioida myönnetyn varmenteen luotettavuutta.

Tähän varmennepolitiikkaan viitataan jokaisessa Sonera Class 2 -varmenteessa käyttämällä Object Identifier (OID) –tunnistetta. Varmenteen OID –kentän sisältämän tunnisteen perusteella varmennetta hyödyntävä sovellus voi automaattisesti tarkistaa onko varmenne sopiva aiottuun käyttöön.

Tämän dokumentin käyttäjät voivat myös tarkistaa varmennuskäytännöstä (Certification Practice Statement, CPS) miten tämän politiikan vaatimukset on toteutettu.

1.2 Dokumentin tunnus

Tämän politiikan nimi on **”Sonera CA, Varmennepolitiikka, Sonera Class 2 -varmenne”** ja sen tunnus on **” TeliaSonera Finland CP-Class2 v. 2.4”**. Tämä politiikka on rekisteröity Soneran Varmennepolitiikkayksikön toimesta ja sille on annettu seuraava yksilöllinen tunniste (Object Identifier, OID): 1.3.6.1.4.1.271.2.3.1.1.2

Copyright © TeliaSonera Finland 2004. All rights reserved

{iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) telecomFinland(271) services(2) serviceProducts(3) soneraCA(1) certificatePolicies(1) soneraClass2CAPolicy(2)}

1.3 Osapuolet ja soveltamisala

Tämä varmennepolitiikka sitoo TeliaSonera Finland Oyj:tä (myöhemmin ”Varmentaja”), joka myöntää varmenteita, joissa on viittaus tähän politiikkaan. Tämä dokumentti kuvaa myös muiden Sonera PKI:hin liittyvien osapuolten oikeudet ja velvollisuudet. Näitä ovat mm. Varmenteen valmistajat, Rekisteröijät, Tilaajat, Varmenteen haltijat ja Luottavat osapuolet.

Varmentaja noudattaa politiikan toteuttamisessa Suomen lakia.

1.3.1 Varmentaja (CA)

Osapuolta, johon varmennepalveluiden käyttäjät (sekä Tilaajat, Varmenteen haltijat että Luottavat osapuolet) luottavat varmenteiden luonnissa ja myöntämisessä, kutsutaan Varmentajaksi (CA). Varmentajalla on kokonaisvastuu varmennepalveluiden toimittamisessa. Näihin palveluihin kuuluu varmenteiden myöntäminen, julkaisu, Sulkupalvelu sekä Sulkulistapalvelu. Varmentajan yksityistä avainta käytetään varmenteiden ja sulkulistojen allekirjoittamiseen, ja avaimen haltija (Varmentajan nimi) näkyy myönnetyn varmenteen tai julkaistun sulkulistan ”Issuer”-kentässä. Issuer-kentässä oleva Varmentajan nimi on “Sonera Class2 CA”. Muille varmentajille, lukuun ottamatta Sonera Class2 CA:n Ali-CA:ita, ei ole myönnetty oikeutta myöntää tämän politiikan mukaisia varmenteita. Tätä politiikkaa sovelletaan myös kaikkiin Sonera Class2 CA:n Ali-CA:hin.

Varmentaja voi käyttää muita osapuolia varmennepalveluiden tuottamisessa. Varmentajalla säilyy kuitenkin aina kokonaisvastuu politiikan vaatimusten toteuttamisesta.

1.3.2 Varmenteen valmistaja

Varmentaja on kokonaisvastuussa varmenteiden valmistuksesta ja hallinnoinnista. Varmentaja voi kuitenkin ulkoistaa osia toiminnoistaan Varmenteen valmistajille.

1.3.3 Rekisteröijä (RA)

Vain Varmentajan hyväksymät organisaatiot voivat toimia Rekisteröijinä.

Varmentaja on kuitenkin viime kädessä vastuussa myöntämistään varmenteista. Rekisteröijän tulee siis sitoutua tässä politiikassa määriteltyihin velvollisuuksiin, jotka koskevat rekisteröintiä, tunnistusta ja henkilöllisyyden tarkastamista, allekirjoittamalla niistä sopimus Varmentajan kanssa.

HUOM. Poikkeus tähän sääntöön saattaa syntyä, kun Luottava osapuoli päättää ottaa vastuulleen myös Rekisteröijän velvollisuudet. Tässä tapauksessa Luottava osapuoli voi ottaa osapuolten välisessä sopimuksessa sovitussa laajuudessa osan Varmentajan vastuusta.

1.3.4 Varmenteen haltija

Varmentaja myöntää asiakasorganisaatioiden nimeämille henkilöille tai niiden hallinnoimille Laitteille varmenteita, joissa viitataan tähän politiikkaan. Luonnollisista henkilöistä ja Laitteista, joille on myönnetty varmenne, käytetään tässä politiikassa nimitystä Varmenteen haltija.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

Asiakasorganisaation nimeämälle henkilölle voidaan myöntää varmenteita sen perusteella, että tämä on sopimussuhteessa organisaation kanssa. Varmentajalla on omalla päätöksellään oikeus olla myöntämättä varmennetta Varmenteen hakijalle.

Asiakasorganisaation nimeämälle Laitteelle voidaan myöntää varmenteita sen perusteella, että tämä on asiakasorganisaation hallinnassa. Varmentajalla on omalla päätöksellään oikeus olla myöntämättä varmennetta Laitteelle.

1.3.5 Tilaaja

Tilaaja on Varmentajan asiakas, jonka tilauksen perusteella Varmentaja myöntää varmenteita. Tilaaja sitoutuu noudattamaan tässä politiikassa mainittuja velvoitteitaan omasta puolestaan tai yhden tai useamman Varmenteen haltijan puolesta.

1.3.6 Luottava osapuoli

Tämä varmennepolitiikka on tarkoitettu henkilöille ja organisaatioille (Luottava osapuoli), jotka hyödyntävät tämän politiikan mukaisesti myönnettyjä varmenteita. Luottamalla varmenteisiin Luottava osapuoli sitoutuu velvoitteisiin, jotka tässä dokumentissa on kuvattu.

1.3.7 Sopimussuhteet

Varmentaja on sopimussuhteessa Tilaajiin, sekä kaikkiin osapuoliin, jotka suorittavat Varmentajan toimintaan kuuluvia tehtäviä. Varmentaja vastaa alihankkijoidensa varmennustoimintaan liittyvästä toiminnasta kuin omastaan. Sopimuksista tulee käydä selkeästi ilmi osapuolten oikeudet ja velvollisuudet.

1.3.8 Soveltamisala

Varmenteita voidaan käyttää digitaalisten allekirjoitusten yhteydessä.

Varmenteita voidaan käyttää vain seuraavissa sovelluksissa:

- Varmenteen haltijan tunnistaminen,
- Sähköisessä muodossa olevan tiedon alkuperän ja eheyden todentaminen,
- Sähköisessä muodossa olevan tiedon luottamuksellisuuden varmistaminen,
- Sähköisen allekirjoituksen todentaminen.

Tämän politiikan mukaisia varmenteita hyödyntävien sovellusten tulee ottaa huomioon varmenteen “Key Usage” –lisäkentässä mainittu avaimen käyttötarkoitus.

Lisäksi Tilaajan ja Varmentajan välisessä sopimuksessa mahdollisesti määritellyt avainten käyttötarkoitukset ja rajoitukset tulee ottaa huomioon varmenteita käytettäessä.

1.4 Yhteystiedot

Tämän politiikan on rekisteröinyt TeliaSonera Finland Oyj / Data Networking Solutions. Tätä politiikkaa hallinnoi Varmentajan Varmennepolitiikkayksikkö.

TELIASONERA FINLAND OYJ
00051 SONERA
Puhelin: +358 (0) 20401

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

Yhteyshenkilö varmennepolitiikkaan liittyvissä asioissa:

Sonera CA Tuotepäällikkö
Sähköposti: cainfo@sonera.com
Puhelin: +358 (0) 20401

Asiakaspalvelu: +358 (0) 800 17000 (ma-pe klo 8-21 ja la 9-16:30)
Tekninen asiakaspalvelu: +358 (0) 800 19101 (ma-pe klo 8-21 ja la 9-16:30)
Sulkupalvelu: +358 (0) 800 156677 (24h)
Internet: http://support.partnergate.sonera.com/

Copyright © TeliaSonera Finland 2004. All rights reserved

2 Yleiset säännökset

2.1 Velvollisuudet

2.1.1 Varmentajan velvollisuudet

Varmentaja vastaa siitä, että kaikki tämän dokumentin Varmentajalle asettamat vaatimukset täytetään.

Varmentaja vastaa tämän politiikan vaatimusten täyttymisestä myös silloin, kun osa Varmentajan toiminnoista on ulkoistettu alihankkijoille.

Varmentaja tarjoaa kaikki varmennepalvelunsa varmennuskäytäntö-dokumenttinsa (CPS) mukaisesti.

Varmentaja vastaa tämän politiikan sisältämistä vaatimuksista ja politiikan ylläpidosta.

2.1.1.1 Juridiset vaatimukset

Varmentajan on taattava juridisten vaatimusten toteutuminen. Näitä ovat:

- Kaikki tärkeät tiedot ja tiedostot suojataan häviämiseltä, tuhoamiselta ja väärentämiseltä. Joitain tietoja saatetaan myöhemmin joutua palauttamaan joko oikeudellisista syistä tai oleellisten liiketoimien tukemiseksi.
- Euroopan Unionin tietosuojaa käsittelevän direktiivin vaatimukset täytetään siten kuin ne on toteutettu kansallisessa lainsäädännössä.
- Varmentaja on suojannut henkilötiedot riittävillä teknisillä ja organisatorisilla toimenpiteillä laittomalta tai luvattomalta käytöltä sekä vahingossa tapahtuvalta katoamiselta, tuhoutumiselta tai vahingoittumiselta.
- Käyttäjien Varmentajalle luovuttamaa tietoa ei luovuteta muille ilman käyttäjän suostumusta, tuomioistuinpäätöstä tai muuta lakiin perustuvaa vaatimusta.

2.1.1.2 Organisaatiovaatimukset

Varmentajan organisaation tulee toimia luotettavasti. Erityisesti seuraavat vaatimukset on täytettävä:

- Varmentaja on juridinen henkilö voimassa olevan lainsäädänön mukaisesti.
- Varmentajalla on tietoturvallisuuden hallintajärjestelmä, joka on riittävä sen tarjoamille varmennepalveluille.
- Varmentaja on huolehtinut riittävistä järjestelyistä, joiden avulla se pystyy hoitamaan toiminnastaan koituvat vastuut.
- Varmentaja on taloudellisesti vakavarainen ja sillä on riittävät taloudelliset voimavarat toimia tämän politiikan mukaisesti.
- Varmentajalla on varmennepalveluiden tarjoamiseen riittävä määrä työntekijöitä, joilla on tarvittava koulutus, tekninen osaaminen ja kokemus, ottaen huomioon varmennepalveluiden luonne, kattavuus ja volyymi.
- Varmentajalla on asianmukaiset sopimukset ja sopimussuhteet niiden palveluiden tuottamisesta, joihin liittyy ulkoistusta, alihankintaa tai muuta kolmansien osapuolten käyttöä.
- Varmenteen luomiseen ja peruuttamiseen liittyviä tehtäviä hoitavien Varmentajan organisaation osien rakenteen tulee olla dokumentoitu.

Copyright © TeliaSonera Finland 2004. All rights reserved

2.1.1.3 Ilmoitukset varmenteen myöntämisestä ja peruuttamisesta

Varmentaja ei tee erikseen ilmoitusta Tilaajalle, Varmenteen haltijalle tai muille osapuolille myönnetystä varmenteesta.

Kun varmenteen peruuttamispyynnön tiedot tarkistetaan Sulkupalvelussa puhelimitse, tieto pyynnön onnistuneesta välityksestä Varmentajan järjestelmään annetaan pyynnön tekijälle puhelun aikana.

2.1.2 Rekisteröijän velvollisuudet

Rekisteröijä hoitaa Varmentajan puolesta Varmenteen hakijan tunnistamisen varmennuskäytäntöjen mukaisesti. Rekisteröijän velvollisuuksiin kuuluu:

- Varmenteen hakijan henkilöllisyyden todentaminen.
- Varmistuminen siitä, että varmenteen hakijalla on oikeus hakea varmennetta.
- Asianmukaisen ja täydellisen varmennepyynnön toimittaminen Varmentajalle ensimmäistä varmennetta haettaessa, varmennetta uusittaessa ja avainpareja uusittaessa.

Asiakasorganisaatioissa toimivien Rekisteröijien velvollisuuksiin kuuluu lisäksi omaan organisaatioonsa kuuluvien Varmenteen haltijoiden osalta:

- Varmenteiden peruuttamispyyntöjen toimittaminen Sulkupalveluun peruuttamista edellyttävissä olosuhteissa.

2.1.3 Tilaajan velvollisuudet

Varmentaja ja Tilaaja tekevät sopimuksen, joka velvoittaa Tilaajan huolehtimaan siitä, että Varmenteen haltija sitoutuu seuraaviin velvollisuuksiin:

- Varmenteen haltijan on annettava tarkat ja täydelliset tiedot Varmentajalle tämän politiikan mukaisesti, erityisesti rekisteröinnin yhteydessä.
- Varmenteen haltija saa käyttää yksityistä avaintaan vain sellaisiin tarkoituksiin, jotka vastaavat kappaleessa 1.3.8 ”Soveltamisala” määriteltyjä varmenteen käyttötarkoituksia sekä varmenteen “Key Usage” –lisäkentässä määriteltyjä avainten käyttötarkoituksia, sekä niiden rajoitusten mukaisesti, jotka Tilaajalle on ilmoitettu.
- Varmenteen haltijan tulee noudattaa riittävää huolellisuutta estääkseen yksityisen avaimensa luvattoman käytön.
- Varmenteen haltijan tulee viipymättä tehdä Varmentajalle toimitettava ilmoitus, mikäli varmenteen voimassaoloaikana:
    - Varmenteen haltijalla on syytä epäillä että hänen yksityinen avaimensa on kadonnut, varastettu tai mahdollisesti paljastunut tai otettu luvattomasti käyttöön,
    - Varmenteen haltija on menettänyt yksityisen avaimensa hallinnan, koska sen aktivointitieto (ts. tunnusluku) on kadonnut tai joutunut vääriin käsiin, tai jostain muusta syystä,
    - Varmenteen haltijalle on käynyt ilmi, että varmenteen tiedot eivät enää päde tai että niissä on epätarkkuuksia.
- Paljastumisen jälkeen Varmenteen haltijan yksityisen avaimen käyttö lopetetaan heti ja pysyvästi.

Varmentaja toimittaa Tilaajan saataville Varmenteen haltijoille edelleen annettavaksi erillistä ohjeistusta varmennepalveluiden asiakkaan vastuista edellä mainittujen velvollisuuksien noudattamiseksi.

2.1.4 Luottavan osapuolen velvollisuudet

Voidakseen luottaa varmenteeseen riittävin perustein on Luottavan osapuolen suoritettava vähintään seuraavat toimenpiteet:

- tarkistettava varmenteen aitous ja voimassaolo joko itse tai hankittava tarkistus palveluna,

Copyright © TeliaSonera Finland 2004. All rights reserved

- otettava huomioon kaikki rajoitteet, jotka koskevat varmenteen käyttöä ja jotka on ilmoitettu Luottavalle osapuolelle varmenteessa, tässä politiikassa tai sopimuksessa.

2.2 Vahingonkorvausvastuu

Varmentaja on rajoittanut vahingonkorvausvastuitaan varmennuskäytännössä. Asiakas-organisaatioiden kanssa tehtävät sopimukset voivat myös sisältää vahingonkorvausvastuiden rajoituksia. Lisäksi vahingonkorvausvastuun osalta pätee mitä on mainittu Soneran palveluiden yleisissä toimitusehdoissa yritysasiakkaille.

2.3 Taloudellinen vastuu

Varmentaja kantaa taloudellisen vastuun varmennepalveluiden tuotantoon liittyvistä seikoista varmennepolitiikan, varmennuskäytännön sekä sopimusehtojen mukaisesti mukaan lukien palveluiden tuottaminen, ylläpito ja kehittäminen, sekä omalta osaltaan että alihankkijoidensa puolesta.

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

Varmentaja ei vastaa niiden asiakasorganisaatioiden sovellusten toimivuudesta tai sisällöstä, joiden yhteydessä varmennepalveluita käytetään. Asiakasorganisaatio kantaa itse sovelluksiinsa ja niiden käyttöön liittyvät taloudelliset riskit.

2.3.1 Korvaukset asiakasorganisaatiolta

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

- asiakasorganisaatioon liittyvä Varmenteen haltija ei ole suojannut yksityistä avaintaan tai tehnyt riittäviä toimenpiteitä estääkseen sen katoamisen, paljastumisen tai joutumisen ulkopuolisten käsiin.
- Varmenteen peruuttamispyyntöä ei ole toimitettu Sulkupalveluun kappaleessa 2.1.3 ”Tilaajan velvollisuudet” mainituissa tilanteissa, jotka edellyttävät Varmentajalle ilmoittamista.
- asiakasorganisaatio ei ole Luottavana osapuolena tarkistanut varmenteen voimassaoloa kappaleen 2.1.4 ”Luottavan osapuolen velvollisuudet” mukaisesti.
- Luottavana osapuolena asiakasorganisaatio on luottanut varmenteeseen muutoin perusteettomasti olosuhteisiin nähden.

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

2.4 Asiakaspalautteet

Valitusten käsittelyssä noudatetaan Soneran palveluiden yleisiä toimitusehtoja yritysasiakkaille.

2.5 Varmennepolitiikan tulkinta ja täytäntöönpano

Tämän politiikan tulkintaan, täytäntöönpanoon ja voimassaoloon sovelletaan Suomen lakia. Menettelyt riitatilanteessa on kuvattu varmennuskäytännöissä.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

2.6 Maksut

Varmennepalveluista peritään Varmentajan ja asiakasorganisaation välisen sopimuksen mukaiset maksut. Maksujen perusteena voi olla mm.:

- Varmenteen myöntäminen,
- Varmenteen ylläpito,
- Varmenteen uusiminen,
- Varmenteen käyttö,
- Sulkulistojen ja varmenteen tilan tarkistus,
- Varmenteita hyödyntävän palvelun perustaminen.

Varmennuskäytännöissä on kuvattu maksujen palautuksissa noudatettavat ehdot.

2.7 Tietojen julkaiseminen ja tietovarastot

2.7.1 Varmentajan tiedot ja tietovarastot

2.7.1.1 Ehdot

Varmenteen käyttöön liittyvät ehdot on ilmoitettu tässä politiikassa ja varmennuskäytännöissä. Määriteltyihin ehtoihin sisältyvät mm.:

- varmenteen käytön rajoitukset,
- Tilaajan velvollisuudet, siten kuin ne on tässä politiikassa määritelty,
- tiedot siitä, miten varmenteen voimassaolo tarkistetaan sisältäen sulkulistan tarkistusvaatimukset, joiden mukaan toimimalla Luottava osapuoli voi kohtuudella luottaa varmenteeseen,
- rekisteröintitietojen säilytysaika,
- Varmentajan järjestelmien tapahtumatietojen säilytysaika,
- valitusten ja riitojen sovittelun toimintatavat,
- sovellettava laki.

Yllä mainittujen tietojen tulee olla pysyvästi saatavilla tietovarastosta. Tiedot voidaan toimittaa sähköisessä muodossa.

2.7.1.2 Varmenteiden jakelu

Varmentaja huolehtii siitä, että varmenteet ovat Luottavien osapuolten saatavilla tarvittaessa.

Varmentaja vastaa erityisesti seuraavista asioista:

- Varmenne asetetaan saataville Varmentajan varmennehakemistoon, jollei toisin Tilaajan kanssa sovita.
- Varmenteet julkaistaan viipymättä.

2.7.1.3 Sulkulistatietojen jakelu

Sulkulistatiedot ovat saatavissa Sulkulistapalvelun kautta.

2.7.2 Tietojen julkaisemisaika

Kaikki Varmentajalle saatetut julkaisua vaativat tiedot julkaistaan viipymättä. Sulkulistojen julkaisuajat on ilmoitettu varmennuskäytännöissä.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

2.7.3 Pääsynvalvonta

Tietovarastot, joihin on tallennettu tämä politiikka ja siihen liittyvä varmennuskäytäntö sekä varmennepalveluiden ehdot ja säännöt, ovat vapaasti ja julkisesti saatavilla. Varmenteen haltijan varmenne on saatavilla Luottaville osapuolille tarvittaessa. Sulkulistapalvelu on julkisesti saatavilla.

2.8 Toiminnan auditointi

2.8.1 Varmentajan itse suorittamat tarkastukset

Varmentaja valvoo toimintansa tietoturvallisuutta sisäisin tarkastuksin. Varmentajalla on oikeus tarkastaa myös asiakasorganisaatioissa toimivien Rekisteröijien toiminta. Varmentajan alihankkijat käyttävät omia tarkastusmenettelyjään oman toimintansa auditoinnissa.

2.8.2 Ulkopuolisen auditoijan suorittama auditointi

Varmentaja käyttää myös kolmatta osapuolta auditoimaan toimintaansa säännöllisesti. Ulkoinen auditointi suoritetaan vähintään kerran vuodessa. Auditointi kattaa Varmentajan ja sen alihankkijoiden toiminnan, mutta ei asiakasorganisaatioissa toimivien Rekisteröijien toimintaa.

Auditoinnin suorittaa Varmennepolitiikkayksikön hyväksymä tietoturva-auditoija. Tällaisen auditoinnin tarkoituksena on varmistaa ainakin seuraavat asiat:

- Varmentajalla ja sen alihankkijoilla on käytössä järjestelmä, joka takaa tarjottavien palveluiden laadun,
- Varmentaja ja sen alihankkijat toimivat tämän politiikan kaikkien vaatimusten mukaisesti,
- Varmentajan varmennuskäytännöt ovat yhteneväisiä tämän politiikan kanssa.

Varmentajan on ryhdyttävä asianmukaisiin toimenpiteisiin, mikäli auditoinnissa havaitaan puutteita.

2.9 Salassapitopolitiikka

Tilaajia ja Varmenteen haltijoita koskevat tiedot, jotka Varmentaja ja Rekisteröijä saavat rekisteröinnin yhteydessä, ovat luottamuksellista tietoa eikä niitä anneta kolmannelle osapuolelle ilman kyseisen henkilön lupaa, ellei laki toisin vaadi. Itse varmenne on julkinen, joten siinä olevat tiedot Varmenteen haltijasta ovat julkisia.

2.10 Immateriaalioikeudet

2.10.1 Varmentajan tietojen immateriaalioikeudet

Seuraavien tietojen immateriaalioikeudet kuuluvat Varmentajalle:

- Varmentajan varmennepalveluiden yhteydessä käyttämät tavaramerkit ja nimet
- tämä varmennepolitiikka ja politiikkaan liittyvä varmennuskäytäntö
- muu varmennepalveluihin liittyvä Varmentajan tuottama dokumentaatio
- Varmentajan luomat varmenteet ja sulkulistat
- Varmentajan luomat ja käyttämät tai Varmenteen haltijoille toimittamat avainparit

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

2.10.2 Käyttöoikeus ohjelmistoihin ja dokumentteihin

Varmennepalveluiden toteuttamiseksi tarpeelliseen kokonaisuuteen kuuluvien kaikkien ohjelmistojen, dokumenttien ja muun aineiston omistus- ja immateriaalioikeudet kuuluvat Varmentajalle tai kolmannelle osapuolelle. Tilaaja tai Luottava osapuoli saa tämän politiikan mukaisen rajoitetun käyttöoikeuden Varmentajan toimittamien ohjelmistojen konekielisiin versioihin ja asiakirjoihin sekä palvelun testaamiseksi toimitettuun aineistoon ja tietoihin. Käyttöoikeuden perusteella Tilaaja tai Luottava osapuoli saa käyttää ohjelmistoja ja asiakirjoja sekä testausaineistoa ja -tietoja ainoastaan Varmentajan ohjeiden mukaan ja vain välittömästi palvelun käyttöön tai sen testaukseen liittyen. Ohjelmistojen, asiakirjojen, testausaineiston ja -tiedon sekä niiden muutettujen versioiden omistus- sekä immateriaalioikeudet ovat Varmentajan tai kolmannen osapuolen (kuten Varmentajan päämiehen tai alihankkijan) omaisuutta eikä Tilaajalla tai Luottavalla osapuolella ole ilman Varmentajan etukäteen antamaa kirjallista suostumusta oikeutta kopioida, kääntää tai muuttaa aineistoa, asiakirjoja tai ohjelmistoja taikka luovuttaa niitä kolmannen käyttöön, ellei pakottavasta lainsäädännöstä muuta johdu.

Käyttöoikeuden päättyessä Tilaajan tai Luottavan osapuolen on omalla kustannuksellaan joko palautettava tai Varmentajan pyynnöstä tuhottava hallussaan olevat alkuperäis- ja jäljennöskopiot, tietovälineet ja dokumentaatio.

Copyright © TeliaSonera Finland 2004. All rights reserved

3 Tunnistaminen

3.1 Nimeämiskäytäntö Varmentajan varmenteissa

Varmentajalla, joka myöntää tämän politiikan mukaisia varmenteita, on yksikäsitteinen X.501:n mukainen Distinghuished Name (DN) -nimi, joka löytyy Varmentajan varmenteesta sekä ”Issuer”- että ”Subject” –kentästä sekä kaikkien Varmentajan myöntämien muiden varmenteiden ”Issuer”-kentästä. Nimi koostuu seuraavista attribuuteista:

Attribuutti	**Sisältö**
commonName (CN)	Sonera Class2 CA
Organization (O)	Sonera
Country (C)	FI

Ali-CA varmeissa Country arvo on valinnainen. Common name- ja organisaatioarvot määrittelee Varmentaja. Ali-CA varmenteiden Issuer-arvo on ”Sonera Class2 CA”.

3.2 Uuden Varmenteen haltijan rekisteröinti

3.2.1 Varmenteen haltijan nimeäminen

Varmenteen haltijan yksikäsitteisenä nimenä käytetään varmenteen ”Subject” –kentässä X.501:n mukaista Distinguished Name (DN) –nimeä, ja se sisältää aina seuraavat attribuutit:

Attribuutti	**Kuvaus sisällöstä**
commonName (CN)	Varmenteen haltijan nimi
Organization (O)	Asiakasorganisaatio, jonka yhteydessä Varmenteen haltija tunnistetaan. (Jos Varmenteen haltijana on Laite ja varmenne liittyy Soneran palveluun, jossa attribuutin arvo määräytyy kyseisen palvelun mukaisesti, attribuutin sisältö on Soneran määrittelemä merkkijono.)

”Subject”-kentässä voi olla myös seuraavia attribuutteja riippuen siitä, mihin käyttöön varmenne on luotu:

Attribuutti	**Kuvaus sisällöstä**
organizationalUnit (OU)	Laitteille myönnettävät varmenteet: Soneran määrittelemä merkkijono, joka ilmoittaa, minkä Soneran palvelun yhteydessä varmennetta käytetään. Henkilöille myönnettävät varmenteet: Määräytyy sen sovelluksen tai palvelun

Copyright © TeliaSonera Finland 2004. All rights reserved

	toteutuksen edellyttämällä tavalla, jonka yhteydessä varmennetta käytetään.
State	Laitteen sijaintia kuvaava määritys.
Location	Laitteen sijaintia kuvaava määritys.

Muitakin attribuutteja voidaan tarvittaessa käyttää.

3.2.2 Nimien merkitykset ja tulkinta

HUOM: Tilaajan organisaation sisällyttäminen varmenteeseen on vain informatiivisiin tarkoituksiin, eikä sen esiintyminen varmenteessa sinänsä anna minkäänlaisia valtuuksia tai muita oikeuksia.

3.2.2.1 Luonnollisten henkilöiden nimien tulkinta

”commonName” –attribuutti voi sisältää Varmenteen haltijan todellisen nimen tai pseudonyymin (salanimen).

Jos attribuutti sisältää Varmenteen haltijan todellisen nimen, nimi koostuu henkilön etu- ja sukunimestä ja voi sisältää myös henkilön muita etunimiä tai näiden alkukirjaimia.

Jos attribuutti sisältää pseudonyymin, se on yksi sana, joka koostuu perättäisistä merkeistä ilman välilyöntejä.

3.2.2.2 Laitenimien tulkinta

”commonName” –attribuutti esittää Varmenteen haltijan nimen jommassakummassa seuraavista muodoista:

- Kun asiakaorganisaatio määrittelee Laitteen nimen tilauksessa, se on joko Laitteen IP-osoite tai domain-nimi (verkkotunnus).
- Jos varmenne liittyy Soneran palveluun, jossa Laitteen nimi määritellään palvelun mukaisesti, se on Soneran määrittelemä merkkijono.

”organizationName” –attribuutti määrittelee sen asiakasorganisaation, jonka yhteydessä Varmenteen hakija tunnistetaan. Jos Varmenteen haltijana on Laite ja varmenne liittyy Soneran palveluun, jossa attribuutti määräytyy kyseisen palvelun mukaisesti, se on Soneran määrittelemä merkkijono.

3.2.3 Nimien yksikäsitteisyys

Varmenteessa olevan ”Subject”-kentän tulee olla yksikäsitteinen kaikille Varmentajan luomille varmenteille ja noudattaa yksikäsitteisyyden suhteen X.500-standardia. Yksikäsitteisyys tarkoittaa, että Varmentaja ei myönnä eri henkilöille tai laitteille varmenteita, joissa olisi identtiset kenttien arvot. Varmentaja voi kuitenkin myöntää samalle henkilölle tai laitteelle useita varmenteita, joissa ”Subject”-kentän arvot ovat samat.

3.2.4 Nimierimielisyyksien ratkaisumenettely

Varmentaja edellyttää, että asiakasorganisaatiot eivät varmenteita hakiessaan loukkaa muiden nimiin liittyviä omistusoikeuksia. Varmentaja ei kuitenkaan tarkista asiakasorganisaation oikeutta niiden nimien käyttöön, joita tämä antaa varmenteita hakiessaan varmenteisiin tallennettavaksi, eikä osallistu minkään kauppanimien, domain-nimien, tavaramerkkien tai palvelunimien omistusoikeuksiin liittyvien kiistojen ratkaisuun. Varmentaja pidättää itsellään oikeuden olla myöntämättä sellaista varmennetta tai peruuttaa jo myönnetty varmenne, jonka sisältöön liittyy nimen omistusoikeutta koskeva kiista.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

3.2.5 Organisaation tunnistaminen

Varmentaja tunnistaa asiakasorganisaation ja tarkistaa organisaatiossa myönnettyjä valtuuksia silloin kun asiakasorganisaatio otetaan Tilaajaksi, asiakasorganisaatiossa toimiville rekisteröintivastaaville annetaan näiden tarvitsemat oikeudet ja kun asiakasorganisaatio tilaa varmenteita Laitteille. Rekisteröintivastaava tunnistetaan aina tämän hakiessa varmennetta. Varmenteita voidaan myös myöntää automaattisesti virtuaalisen rekisteröintivastaavan toimesta sellaisissa tapauksissa, joissa varmenteen hakijan identiteetti on tarkistettu TeliaSoneran hyväksymästä hakemistosta. Tunnistamis- ja tarkastusmenettelyt on kuvattu tarkemmin varmennuskäytännöissä.

3.2.6 Varmenteen hakijan henkilöllisyyden ja nimen tarkistaminen

Varmenteen hakijan henkilöllisyyden ja nimen tarkistaminen tehdään rekisteröinnin yhteydessä asiakasorganisaatioiden Rekisteröintivastaavien toimesta varmennuskäytännöissä kuvatuilla tavoilla.

3.2.7 Yksityisen avaimen hallussapidon todentaminen

Mikäli Varmentaja ei luo Varmenteen haltijan avainparia vaan se luodaan asiakasorganisaatiossa, varmennepyyntö hyväksytään vain kun se allekirjoitetaan ko. avainparin yksityisellä avaimella.

3.3 Varmenteen uusiminen, uuden avainparin luonti ja tietojen päivitys

Varmentajan on varmistettava, että varmenteita koskevat toimenpidepyynnöt ovat asianmukaisia ja luvallisia. Tämä koskee varmenteiden uusimista, uuden avainparin luontia ennen varmenteen voimassaolon päättymistä ja Varmenteen haltijan varmenteen tietojen päivittämistä. Rekisteröijinä toimivat asiakasorganisaatiot on sopimuksin ja niihin sisältyvin ohjeistuksin velvoitettu osaltaan tekemään rekisteröintiin liittyvät varmistukset.

Erityisesti seuraavista asioista on huolehdittava:

- Varmennetta uusittaessa tai uutta avainparia luotaessa on varmistettava, että varmenteen alkuperäinen käyttötarkoitus on vielä olemassa.
- Jos varmenne uusitaan Varmenteen haltijan tietojen päivittämiseksi varmenteeseen, tietojen tarkistus tehdään kuten ensimmäistä varmennetta haettaessa.
- Jos Varmentajan asettamat ehdot ovat muuttuneet, ne on ilmoitettava Tilaajalle.
- Varmentaja myöntää uuden varmenteen Varmenteen haltijan aikaisemmin varmennetulle julkiselle avaimelle vain, jos sitä voidaan yhä pitää riittävän turvallisena uuden varmenteen elinkaaren ajaksi eikä ole mitään syytä epäillä, että Varmenteen haltijan yksityinen avain olisi paljastunut.

3.4 Avainten uusiminen varmenteen peruuttamisen jälkeen

Peruutettuja ja vanhentuneita varmenteita ei voi uusia. Jos varmenteen hakijalla ei ole voimassa olevaa Sonera Class 2 -varmennetta, rekisteröinnissä noudatetaan tällöin samaa prosessia kuin haettaessa ensimmäistä varmennetta.

3.5 Peruuttamispyyntö

Varmentajan Sulkupalveluvastaavilla on oikeus toimittaa varmenteen peruuttamispyyntö Varmentajan järjestelmään. Sulkupalveluvastaava tunnistetaan varmenteen perusteella.

Copyright © TeliaSonera Finland 2004. All rights reserved

Varmenteen peruuttamista pyytävä henkilö on tunnistettava Sulkupalvelussa. Tunnistus täytyy tehdä sellaisella tavalla, että pyytäjän oikeus pyytää peruuttamista voidaan riittävällä tasolla todentaa. Tunnistusmekanismien on otettava huomioon luvattomien peruuttamispyyntöjen tekemisen mahdollisuus sekä toisaalta tarve peruuttaa varmenne nopeasti. Tunnistustavat on kuvattu varmennuskäytännöissä.

Myös asiakasorganisaatiossa toimivalla Rekisteröintivastaavalla voi olla Sulkupalveluvastaavan oikeudet omaan organisaatioonsa liittyvien Varmenteen haltijoiden (luonnollisten henkilöiden ja Laitteiden) osalta. Varmenteen peruuttamispyynnön oikeellisuuden varmistaminen on tällöin asiakasorganisaation Sulkupalveluvastaavan vastuulla. Sulkupalveluvastaava tunnistetaan varmenteen perusteella.

3.6 Varmenteen käytön tilapäisen eston purkaminen

Jos varmenne on ollut jäädytettynä, se voidaan palauttaa käyttöön asiakasorganisaation pyynnöstä. Palautusta pyytävä henkilö on tunnistettava. Tunnistus täytyy tehdä sellaisella tavalla, että pyytäjän oikeus pyytää palautusta voidaan todentaa. Tunnistustavat on kuvattu varmennuskäytännöissä.

Varmentaja nimeää ja valtuuttaa erikseen henkilöt, jotka tarkistavat palautuspyynnöt. Vain näiden henkilöiden luvalla Varmentajan Sulkupalveluvastaavilla on oikeus purkaa varmenteen käytön tilapäinen esto. Sulkupalveluvastaavat tunnistetaan varmenteen avulla.

Copyright © TeliaSonera Finland 2004. All rights reserved

4 Toiminnalliset vaatimukset

4.1 Varmenteen hakeminen

Varmennehakemukset ja -pyynnöt tulee tehdä ja täyttää annettujen ohjeiden mukaisesti ja niiden tulee sisältää vaaditut ja oikeat tiedot. Varmenteen hakijat on tunnistettava huolellisesti.

Erityisesti seuraavista asioista on varmistuttava:

- Ennen kuin Varmentaja tekee sopimuksen Tilaajan kanssa, Varmentajan on toimitettava Tilaajalle varmenteen käytön ehdot.
- Ehtojen tulee olla pysyvästi saatavilla. Ne voidaan toimittaa sähköisessä muodossa.
- Tilaajan on annettava osoite- ja muut yhteystiedot, joista Tilaajan tavoittaa.
- Henkilö- ja laitevarmenteen hakija tulee tunnistaa varmennuskäytännössä kappaleessa 3.2 ”Uuden Varmenteen haltijan rekisteröinti” kuvatulla tavalla.
- Kansallisen tietosuojalainsäädännön vaatimuksia on noudatettava rekisteröintiprosessissa.

Varmennuskäytännöissä on tarkemmat kuvaukset varmenteiden hakumenettelyistä.

4.2 Varmenteen myöntäminen

Varmennusjärjestelmä luo vastaanotetun sähköisesti allekirjoitetun varmennepyynnön pohjalta varmenteen, joka on Varmentajan allekirjoittama. Varmentaja vastaa myönnettyjen varmenteiden oikeellisuudesta.

Varmentajan myöntämien Sonera Class 2 -varmenteiden voimassaoloaika on korkeintaan **viisi (5) vuotta**. Varmenteen sisältö on kuvattu kappaleesssa 7.1 ”Varmenteen profiili”. Yksityiskohtaisemmat kuvaukset on annettu varmennuskäytännöissä.

Erityisesti seuraavista asioista on huolehdittava:

- Varmenteiden myöntämismenettely on turvallisesti liitetty rekisteröinnissä, varmenteen uusimisessa ja uuden avainparin varmentamisessa käytettyihin prosesseihin.
- Luodessaan Varmenteen haltijan avainparin Varmentajan on varmistuttava seuraavista asioista:
  - Varmenteen myöntäminen on turvallisesti liitetty avainparin luontiin,
  - Yksityinen avain toimitetaan Tilaajalle tai rekisteröidylle Varmenteen haltijalle turvallisesti.
- Varmentajan on pidettävä huolta, että Varmenteen haltijan yksikäsitteinen nimi pysyy yksikäsitteisenä Varmentajan myöntämissä varmenteissa (ts. Varmentajan toiminnan aikana myönnettyä yksikäsitteistä nimeä ei anneta toiselle henkilölle).
- Rekisteröintitietojen luottamuksellisuus ja eheys suojataan erityisesti siirrettäessä tietoja Tilaajalta tai Varmenteen haltijalta Varmentajalle, tai Varmentajan järjestelmän osien välillä.
- Varmentajan tulee varmistua, että ulkoisia Rekisteröijiä käytettäessä tietoja vaihdetaan vain valtuutettujen ja tunnistettujen Rekisteröijien kanssa.

4.3 Varmenteen hyväksyminen

Varmenteen haltijan, tai Laitteille haettavien varmenteiden tapauksessa Tilaajan, katsotaan hyväksyneen varmenteen, kun se on asennettu työasemaan tai palvelimelle.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

4.4 Varmenteen peruuttaminen ja jäädyttäminen

4.4.1 Peruuttamisolosuhteet

Varmenteen haltijan tai Tilaajan tulee pyytää viipymättä varmenteen peruuttamista kappaleen 2.1.3 ”Tilaajan velvollisuudet” Varmenteen haltijan ilmoitusvastuuta kuvaavassa kohdassa mainituissa olosuhteissa.

Sulkupalvelu lähettää Varmentajalle peruuttamispyynnön, ja Varmentaja peruuttaa pysyvästi tai toistaiseksi varmenteen, mikäli

- Tilaaja tai Varmenteen haltija pyytää peruuttamista,
- Tilaaja tai Varmenteen haltija ei täytä tämän politiikan tai varmennuskäytäntöjen oleellisia ehtoja tai rikkoo muuta varmennepalveluun liittyvää sopimusta, säädöstä tai lakia,
- on syytä uskoa, että Varmenteen haltijan yksityinen avain on paljastunut,
- on syytä uskoa, että varmenteessa olevat tiedot ovat epätarkkoja tai muuttuneet,
- Varmentajalle selviää, että varmennetta ei ollut myönnetty tämän politiikan ja vastaavien varmennuskäytäntöjen mukaisesti,
- on olemassa jokin muu perusteltu syy varmenteen peruuttamiselle.

4.4.2 Kuka voi pyytää peruuttamista

Tämän politiikan mukaisten varmenteiden peruuttamista voivat pyytää vain Tilaaja, asiakasorganisaation Rekisteröintivastaava, Varmenteen haltija tai Varmentaja.

Sulkupalvelu lähettää peruuttamispyynnöt Varmentajalle vasta pyynnön tekijän tunnistuksen jälkeen.

4.4.3 Peruuttamispyyntöjen käsittely

Varmentajan on huolehdittava, että varmenteet peruutetaan viipymättä joko pysyvästi tai toistaiseksi (ts. jäädytetään. ks. kappale 4.4.4 ”Varmenteen jäädyttäminen”) ja perustuen luvallisiin ja tunnistettuihin peruuttamispyyntöihin. Mm. seuraavista asioista on huolehdittava:

- Sulkupalveluun liittyvät pyynnöt (liittyen esim. Varmenteen haltijan yksityisen avaimen paljastumiseen, Varmenteen haltijan kuolemaan, Varmenteen haltijan tai Tilaajan sopimuksen tai liiketoimien yllättävään päättymiseen tai sopimusehtojen rikkomiseen) käsitellään viipymättä vastaanotettaessa.
- Sulkupalveluun liittyvien pyyntöjen tekijät tunnistetaan ja varmistetaan, että peruuttamispyynnön tekee taho, jolla on siihen oikeus. Pyynnöt tarkastetaan Varmentajan käytäntöjen mukaisesti.
- Kun varmenne on peruutettu lopullisesti (ts. ei jäädytetty), sitä ei voi enää ottaa käyttöön.

4.4.4 Varmenteen jäädyttäminen

Varmenteita voidaan Varmentajan niin päättäessä pitää jäädytettynä, kunnes asianmukainen palauttamispyyntö on vastaanotettu ja varmenne palautettu käyttöön, tai peruuttamispyyntö on lopullisesti vahvistettu, tai jäädyttämisestä on kulunut tietty määräaika, jolloin varmenne peruutetaan lopullisesti.

4.4.5 Sulkulistojen julkaisu

Varmentaja tarjoaa Sulkulistapalvelua, josta tieto suljetuista varmenteista on jatkuvasti ja julkisesti saatavilla. Sulkulistat julkaistaan säännöllisesti (myös jos uusia peruuttamispyyntöjä ei ole vastaanotettu). Sulkulistojen julkaisukäytäntö, julkaisutiheydet ja voimassaoloajat määritellään varmennuskäytännöissä. Sulkulistatietojen eheys ja autenttisuus on taattava.

Copyright © TeliaSonera Finland 2004. All rights reserved

Täydellisen sulkulistan julkaisemisen sijasta on mahdollista julkaista myös sen muunnelma, ns. Delta CRL, joka sisältää vain edelliseen julkaistuun sulkulistaan nähden muuttuneet tiedot. Myös muu sulkulistamenettely on mahdollista.

4.4.6 Sulkulistan tarkistamisvelvollisuus

Luottavalla osapuolella on velvollisuus tarkistaa varmenteen voimassaolo sulkulistalta joko itse tai hankkimalla tarkistus palveluna. Tarkistus on tehtävä käyttämällä voimassaolevaa sulkulistatietoa, joka on asetettu Luottavien osapuolten saataville. Sulkulistalta on tarkistettava varmenteen voimassaolo, jäädyttäminen (tilapäinen peruuttaminen) tai peruuttaminen. Tarkistamismenettelyt on kuvattu varmennuskäytännöissä.

Varmennuskäytännöissä on annettu sulkulistojen osoiteteet. Mikäli voimassa olevaa sulkulistatietoa ei ole saatavilla, varmenteeseen ei saa luottaa.

4.5 Varmenteen käytön tilapäisen eston purkaminen

Mikäli varmenne on peruutettu tilapäisesti eli jäädytetty, se voidaan palauttaa käyttöön asiakasorganisaation pyynnöstä. Menettelyt käyttöön palauttamiseksi on kuvattu varmennuskäytännöissä.

4.6 Tietoturvallisuuden valvonta

Varmentaja tallentaa ja seuraa säännöllisesti varmennustoiminnassa syntyviä ja siihen liittyviä oleellisia tietoja. Osa näistä tiedoista tallentuu automaattisesti Varmentajan järjestelmiin ja osa tallennetaan manuaalisesti Varmentajan henkilöstön toimesta.

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

Varmennuskäytännöissä on kuvattu tarkemmin tallennettavat tiedot, niiden kerääminen, säilytys, suojaus, varmistus ja seuranta sekä Varmentajan järjestelmän haavoittuvuuden testaaminen ulkopuolisten tunkeutumisyrityksiä vastaan.

4.7 Tietojen arkistointi

Varmentaja arkistoi oleellisimmat varmennustoimintaan liittyvät tiedot. Varmentajan tulee huolehtia arkistoinnissaan mm. seuraavasta:

- Varmentaja arkistoi kaikki Varmentajan avainparin elinkaareen liittyvät tapahtumat, myöntämiensä varmenteiden elinkaareen liittyvät tapahtumat sekä varmenteen sulkemiseen liittyvät pyynnöt ja niistä seuranneet toimenpiteet.
- Varmentaja huolehtii, että kaikki rekisteröintiin liittyvät tapahtumat arkistoidaan mukaan lukien varmenteiden ja avainparien uusimispyynnöt.
- Varmentajan ympäristöön sekä avainten ja varmenteiden hallintaan liittyvien merkittävien toimien tarkat ajankohdat arkistoidaan.
- Jokaista Varmentajan myöntämää varmennetta koskevat olennaiset tiedot arkistoidaan riittävän pitkäksi ajaksi.
- Varmenteita koskevien arkistojen tietojen luottamuksellisuudesta ja eheydestä huolehditaan.
- Varmenteita koskevat arkistot voidaan pyydettäessä luovuttaa käytettäväksi varmennuksen todisteena oikeudessa.
- Tapahtumat arkistoidaan siten, että niitä ei helposti pystytä poistamaan tai tuhoamaan sinä ajanjaksona, jona niitä säilytetään.
- Varmentaja vastaa, että Varmenteen haltijan tietojen yksityisyydensuoja säilyy.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

Yllä olevien vaatimusten toteuttamista on kuvattu tarkemmin varmennuskäytännöissä, joissa on määritelty arkistoitavat tiedot, arkiston säilytysaika, suojaus ja varmistus sekä arkistotiedon saanti- ja tarkistamismenettelyt.

4.8 Varmentajan allekirjoitusavaimen vaihtaminen

Varmentajalle luodaan uusi allekirjoitusavain ennen kuin käytössä olevan (vanhan) allekirjoitusavaimen käyttöaika varmenteiden allekirjoittamiseen päättyy. Uutta allekirjoitusavainta varten Varmentajalle luodaan myös uusi nimi, joka näkyy Varmentajan myöntämien Sonera Class 2 -varmenteiden ”Issuer”-kentässä.

4.9 Toipuminen katastrofeista ja avainten paljastumisesta

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

4.9.1 Toipuminen hätätilanteista

Varmentajalla on oltava liiketoiminnan jatkuvuussuunnitelma tai muu tarkoituksenmukainen suunnitelma hätätilanteiden varalle. Varmentajan on pystyttävä tarjoamaan tämän politiikan mukaisia varmennepalveluita kohtuullisen ajan kuluessa odottamattomasta hätätilanteesta. Suunnitelmaan tulee sisällyttää säännöllinen toimintavalmiuden testaus.

4.9.2 Tietokoneresurssit, ohjelmisto ja/tai tieto ovat käyttökelvottomia

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

4.9.3 Varmentajan yksityisen avaimen paljastuminen

Varmentajan liiketoiminnan jatkuvuussuunnitelman tai muun hätätilanteiden varalle laaditun suunnitelman tulee sisältää menettelyohjeet Varmentajan yksityisen avaimen paljastumisen tai epäillyn paljastumisen varalle.

Mikäli yksityinen avain on paljastunut, ainakin seuraavat toimenpiteet on suoritettava:

- lopetettava yksityisen avaimen käyttö
- informoitava välittömästi paljastumisesta Tilaajia ja muita varmentajia, joiden kanssa Varmentajalla on sopimus,
- ilmoitettava, että paljastuneella avaimella allekirjoitetut varmenteet ja sulkulistatiedot eivät enää ole voimassa.

4.9.4 Luonnon- tai muun katastrofin jälkeinen tuotantotilojen turvaaminen

Varmentajan järjestelmät sijoitetaan riittävän turvallisiin tiloihin ottaen huomioon toiminnan keskeytymättömyyden vaatimus.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

4.10 Varmentajan toiminnan lopettaminen

Varmentaja huolehtii, että Tilaajille ja Luottaville osapuolille koituu mahdollisimman vähän häiriöitä Varmentajan toiminnan lopettamisesta. Varmentaja ei takaa arkistojen säilytystä sen jälkeen kun Varmentajan toiminta on päättynyt.

Ennen kuin Varmentaja lopettaa toimintansa, vähintään seuraavat toimenpiteet on suoritettava:

- Varmentaja informoi kaikkia Tilaajia ja muita varmentajia, joiden kanssa Varmentajalla on sopimus,
- Varmentaja lopettaa kaikki valtuutukset, jotka koskevat Varmentajan ulkoistamia toimintoja varmenteen myöntämisprosessiin liittyen,
- Varmentaja huolehtii siitä, että sen myöntämiä varmenteita ei enää voi käyttää tai niihin ei voi enää riittävin perustein luottaa.
- Varmentajan yksityiset avaimet tuhotaan tai poistetaan käytöstä.

Copyright © TeliaSonera Finland 2004. All rights reserved

5 Fyysisen turvallisuuden, käyttöturvallisuuden ja henkilöstöturvallisuuden hallinta

5.1 Fyysinen ja ympäristöön liittyvä tietoturvallisuus

Varmentajan on taattava, että fyysistä pääsyä kriittisiin palveluihin valvotaan ja että varmenteiden tuotantojärjestelmään kohdistuvat fyysiset riskit minimoidaan. Tämä edellyttää mm. seuraavien suojatoimien varmistamista:

- Fyysisen pääsyn varmenteiden luontiin, allekirjoituksen luomisvälineiden valmistukseen ja Sulkupalveluun liittyviin tiloihin tulee olla rajoitettu siten, että vain valtuutetut henkilöt pääsevät tiloihin.
- Varmentajan järjestelmiin kuuluvien laitteiden tai ohjelmistojen rikkoutumisen, tuhoutumisen, tai vaarantumisen ja niistä mahdollisesti aiheutuvan liiketoiminnan keskeytymisen estämiseksi tulee olla toteutettuna riittävät suojatoimet.
- Varmentajan palveluihin liittyvät laitteistot, tiedot, tietovälineet ja ohjelmistot tulee suojata luvattomalta Varmentajan tiloista pois siirtämiseltä.
- Tietojen paljastumisen tai varastamisen ja tietojen käsittelyssä käytettäviin tiloihin murtautumisen estämiseksi tulee olla toteutettuna riittävät suojatoimet.
- Tuotantotilan tarjoamien resurssien ja varsinaisten järjestelmäresurssien suojaamiseksi sekä tuotantoa tukevien järjestelmien ja palveluiden varmistamiseksi tulee järjestää tuotantoympäristöön liittyvä turvavalvonta. Varmentajan tulee kuvata ja toteuttaa varmenteiden tuotantoympäristöön liittyvät turvatoimet, jotka kohdistuvat mm. fyysiseen pääsynvalvontaan, paloturvallisuuteen, tukipalveluiden katkosten hallintaan (mm. sähkökatkos, tietoliikennekatkos), vesivahinkoihin, suojautumiseen murtoja ja varkauksia vastaan sekä katastrofitilanteista toipumiseen.

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

- Tilojen sijainti ja rakenteet
- Pääsy tiloihin
- Virransyöttö ja ilmastointi
- Vesivahingoille altistuminen
- Palontorjunta
- Tallenteet
- Jätemateriaalin käsittely
- Varmuuskopioiden tallennus erillään.

5.2 Käyttöturvallisuus

5.2.1 Luotetut roolit

Varmentajan toimintaan liittyvät luotetut roolit tulee määritellä selkeästi.

Luotetut roolit sisältävät seuraavanlaisia vastuita:

- **Tietoturvallisuusvastaava** (Security Manager): kokonaisvastuu turvakäytäntöjen toteutuksen hallinnasta ja järjestelmien tuottamien lokien tarkistaminen.
- **Järjestelmän pääkäyttäjä** (PKI Administrator): rekisteröintiin, varmenteiden luontiin, allekirjoituksen luomisvälineen valmistamiseen ja toimittamiseen sekä varmenteiden peruuttamiseen liittyvien Varmentajan luotettavien järjestelmien konfigurointi, ylläpito ja asennustilaukset sekä PKI-vianselvitykset ja Varmentajan yksityisten avainten hallintatoimenpiteet.

Copyright © TeliaSonera Finland 2004. All rights reserved

- **Järjestelmän ylläpitäjä** (System Administrator): Varmentajan luotettavan järjestelmän päivittäinen käytönvalvonta, varmuuskopioiden ottaminen, varajärjestelmän käyttöönotto ja toipumisen hallinta sekä tilausten mukaiset asennukset ja järjestelmätason vianselvitykset.
- **Rekisteröintivastaava** (Registration Officer): varmenteiden luontiin ja jakeluun liittyvien toimenpiteiden hyväksyntä.
- **Sulkupalveluvastaava** (Revocation Officer): varmenteiden peruuttamiseen ja sulkulistaan liittyvien toimenpiteiden hyväksyntä.

Luotetuissa rooleissa toimivat henkilöt sitoutuvat noudattamaan tätä varmennepolitiikkaa.

5.2.2 Tehtäviin tarvittavien henkilöiden lukumäärä

Seuraavien toimenpiteiden suorittamiseen vaaditaan vähintään kahden henkilön yhtäaikaista paikallaoloa:

- Muutokset Varmentajan tuotantojärjestelmäympäristöön.
- Varmentajan avainten luonti,
- Varmentajan yksityisen avaimen varmuuskopiointi ja palauttaminen.

5.2.3 Rooleihin liittyvä tunnistaminen

Tärkeimmissä luotetuissa rooleissa toimivien henkilöiden tunnistaminen edellyttää varmenteen käyttöä. Rooleihin liittyvä tunnistaminen on kuvattu varmennuskäytännöissä.

5.2.4 Sisäinen dokumentaatio

Sisäinen dokumentaatio on kuvattu varmennuskäytännöissä.

5.3 Henkilöstöturvallisuus

5.3.1 Taustatiedot, pätevyys, työkokemus ja muut vaatimukset

Varmentajan tulee varmistaa, että sen henkilöstöpolitiikka tukee Varmentajan toiminnan luotettavuutta. Mm. seuraavista asioista on huolehdittava:

- Varmentaja palkkaa henkilöstöä, jolla on asiantuntemusta, työkokemusta ja riittävä pätevyys tarjottavien palveluiden hoitamiseen ja osoitettuihin työtehtäviin.
- Esimies- ja vastuutehtäviin tulee palkata henkilöitä, joilla on asiantuntemusta sähköisten allekirjoitusten teknologiasta, kokemusta tietoturvasta ja riskienhallinnasta, sekä sellaista perehtyneisyyttä turvamenettelyihin, jota vaaditaan turvallisuudesta vastaavilta henkilöiltä.
- Varmentajan tietoturvapolitiikassa määritellään roolit ja niihin liittyvät vastuut.
- Tietoturvasta vastaava ylempi johto nimittää Varmentajan henkilöstön luotettuihin rooleihin.
- Varmentaja ei nimitä luotettuihin rooleihin tai johtotehtäviin henkilöitä, joilla tiedetään olevan tuomio vakavasta rikoksesta tai muusta rikkeestä, joka saattaisi vaikuttaa tehtävän hoitamiseen. Henkilöstöä ei päästetä luotettuihin toimintoihin, ennen kuin tarvittavat tarkistukset on tehty.
- Varmentajan työntekijöille määritellyt vastuut tähtäävät eri tehtävien erotteluun ja työntekijälle annettavat valtuudet rajataan tehtävien mukaan.
- Henkilöstön tulee suorittaa hallintaan ja ylläpitoon liittyvät toimet ja ylläpitää prosessit Varmentajan kuvaamien tietoturvan hallintamenettelyjen mukaisesti.

Copyright © TeliaSonera Finland 2004. All rights reserved

5.3.2 Taustatietojen tarkistaminen

Varmentaja suorittaa tarpeelliset tarkistukset kaikille palkkaamilleen henkilöille. Tarkistuksessa selvitetään henkilön luotettavuus ja ammattitaito Varmentajan henkilöstökäytännön mukaisesti.

Varmentajan tärkeimmissä luotetuissa rooleissa toimiville henkilöille suoritetaan kolmannen osapuolen toimesta taustatietojen tarkistaminen. Nämä roolit on määritelty varmennuskäytännöissä. Henkilöt, jotka eivät läpäise alkutarkastusta tai mahdollisesti myöhemmässä vaiheessa tehtävää tarkastusta, eivät voi toimia tai jatkaa luotetussa roolissa.

5.3.3 Koulutusvaatimukset

Kaikkien Varmentajan ja Rekisteröijän toimintaan sekä varmenteen valmistukseen liittyvien henkilöiden on saatava riittävä koulutus tehtäviinsä. Asiantuntemusta on myös pidettävä ajan tasalla täydennyskoulutuksella.

5.3.4 Seuraukset luvattomista toimenpiteistä

Varmentajan havaitessa varmennustoimintaan liittyviä väärinkäytöksiä se ryhtyy välittömästi tarpeellisiin toimenpiteisiin niistä johtuvien haittojen poistamiseksi ja väärinkäytösten uusiutumisen estämiseksi.

5.3.5 Henkilöstölle toimitettava dokumentaatio

Kaikkien Varmentajan ja Rekisteröijän toimintaan sekä varmenteen valmistukseen liittyvien henkilöiden on saatava perusteelliset käyttöoppaat liittyen ohjelmistojen toimintaan sekä käytäntöihin varmenteen rekisteröinnissä, valmistuksessa, päivityksessä, uusimisessa, jäädyttämisessä ja peruuttamisessa.

Copyright © TeliaSonera Finland 2004. All rights reserved

6 Teknisen turvallisuuden hallinta

6.1 Varmentajan avainparin luonti, käyttöönotto ja suojaaminen

6.1.1 Varmentajan avainparin luonti

Varmentajan on huolehdittava, että Varmentajan avaimet luodaan valvotuissa olosuhteissa.

Erityisesti on otettava huomioon, että Varmentajan avainten luonti tapahtuu fyysisesti turvallisessa ympäristössä luotetuissa rooleissa toimivien henkilöiden toimesta. Tehtävän suorittaminen vaatii vähintään kahden henkilön yhtäaikaista paikallaoloa. Varmentajan on rajattava käytäntöjensä mukaisesti mahdollisimman pieneksi niiden henkilöiden määrä, jotka ovat oikeutettuja suorittamaan tämän toimenpiteen.

6.1.2 Varmentajan julkisen avaimen toimittaminen käyttäjille

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

Varmentajan julkinen avain on saatavilla Internetin kautta varmennuskäytännöissä määritellyistä osoitteista.

6.1.3 Varmentajan avainten pituudet ja käytetty algoritmi

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

6.1.4 Varmentajan avainparin käyttöikä

Varmentajan yksityisen avaimen käyttöikä ja Varmentajan varmenteen voimassaoloaika on korkeintaan kaksikymmentäviisi (25) vuotta. Varmentajan yksityisellä avaimella voidaan allekirjoittaa varmenteita Varmentajan avainparin käyttöiän ajan vähennettynä Varmenteen haltijan varmenteen voimassaoloajalla. Tämän jälkeen Varmentajalle tulee luoda uusi avainpari varmenteiden allekirjoitukseen. Sulkulistoja allekirjoitetaan yksityisellä avaimella koko Varmentajan avainparin käyttöiän ajan.

6.1.5 Varmentajan avainten käyttötarkoitukset

Varmentaja huolehtii siitä, että Varmentajan allekirjoitusavaimia ei käytetä muihin tarkoituksiin kuin varmenteiden myöntämiseen ja sulkulistatietojen julkaisuun ja että Varmentajan allekirjoitusavaimia käytetään vain fyysisesti turvallisissa tiloissa.

6.1.6 Varmentajan yksityisen avaimen suojaaminen

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

Copyright © TeliaSonera Finland 2004. All rights reserved

Kun yksityinen allekirjoitusavain on turvallisen allekirjoituksen luomisvälineen ulkopuolella, sen tulee olla salattu käyttäen algoritmiä 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 luotetussa roolissa olevien henkilöiden toimesta fyysisesti suojatussa ympäristössä. Näiden toimenpiteiden suorittaminen vaatii vähintään kahden henkilön yhtäaikaista paikallaoloa. Varmentajan on rajattava käytäntöjensä mukaisesti mahdollisimman pieneksi niiden henkilöiden määrä, jotka ovat oikeutettuja suorittamaan nämä toimenpiteet.

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 tulee suojata salausteknisellä laitteella, joka noudattaa vähintään FIPS 140-2 level 3 -standardia.

6.1.7 Varmentajan yksityisen avaimen key escrow

Varmentajan yksityisestä allekirjoitusavaimesta ei anneta kopioita säilytykseen kolmansille osapuolille siten, että sellaisia olisi tietyissä olosuhteissa Varmentajan toimintaan kuulumattomien henkilöiden käytettävissä (menetelmää kutsutaan nimellä key escrow).

6.1.8 Varmentajan yksityisen avaimen varmuuskopiointi

Varmentaja ottaa yksityisestä avaimestaan varmuuskopioita siten, että palauttaminen varmuuskopiosta voidaan tehdä samaa turvallisuustasoa noudattaen kuin Varmentajan yksityisen avaimen luominen.

6.1.9 Varmentajan yksityisen avaimen arkistointi

Varmentajan yksityistä avainta ei arkistoida.

6.1.10 Varmentajan yksityisen avaimen aktivointi

Varmentajan yksityinen avain aktivoidaan samalla, kun avaimet luodaan kappaleen 6.1.1 ”Varmentajan avainparin luonti” mukaisesti. Avain säilyy aktiivisena kunnes sen käyttö keskeytetään esim. huoltotoimenpiteiden takia.

6.1.11 Varmentajan yksityisen avaimen deaktivointi

Varmentajan yksityisen avaimen deaktivointi tehdään tarvittaessa esim. huoltotoimenpiteiden takia Varmentajan luotetuissa rooleissa toimivien henkilöiden toimesta.

6.1.12 Varmentajan yksityisen avaimen tuhoaminen

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

Copyright © TeliaSonera Finland 2004. All rights reserved

6.1.13 Varmentajan julkisen avaimen arkistointi

Varmentaja arkistoi voimassa olevat ja vanhentuneet Varmentajan julkiset avaimet kappaleen 4.7 ”Tietojen arkistointi” mukaisesti.

6.2 Varmenteen haltijan avainparin luonti, käyttöönotto ja suojaus

6.2.1 Varmenteen haltijan avainparin luonti

Sonera Class 2 -varmenteisiin liittyvät avainparit luodaan pääsääntöisesti asiakasorganisaatiossa. Myös Varmentaja voi luoda avainparit. Tällöin Varmentaja huolehtii siitä, että se luo avainparit turvallisesti ja että yksityisen avaimen luottamuksellisuus säilyy.

6.2.2 Varmenteen haltijan yksityisen avaimen toimittaminen Varmenteen haltijalle

Jos avainpari luodaan Varmentajan toimesta, Varmenteen haltijan yksityinen avain toimitetaan tälle tiedostossa sähköpostin välityksellä.

6.2.3 Varmenteen haltijan julkisen avaimen toimittaminen Varmentajalle

Pääsääntöisesti asiakasorganisaatio, Varmentajan rekisteröintipiste tai Varmentajan valtuuttama henkilö, joka luo Sonera Class 2 -varmenteisiin liittyvät avaimet, toimittaa julkisen avaimen sähköisesti allekirjoitettuna varmennepyynnössä varmennusjärjestelmään.

Laitevarmennetta varten asiakasorganisaatiossa luodun avainparin julkinen avain voidaan toimittaa tiedostossa Varmentajan rekisteröintipisteeseen, joka toimittaa julkisen avaimen sähköisesti allekirjoitettuna varmennepyynnössä varmennusjärjestelmään.

6.2.4 Varmenteen haltijan avainten pituudet ja käytetty algoritmi

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

6.2.5 Varmenteen haltijan avainparin käyttöikä

Varmenteen haltijan julkisten ja yksityisten avainten käyttöikä on enintään **kymmenen (10) vuotta**. Samat avaimet voidaan varmentaa uudelleen varmenteen vanhentuessa. Julkisia ja yksityisiä avaimia ei saa enää käyttää, mikäli salausalgoritmit ja niihin liittyvät parametrit eivät enää ole riittävän vahvoja tai muuten sopivia.

6.2.6 Varmenteen haltijan avainten käyttötarkoitukset

Tämän politiikan mukaan myönnettyihin varmenteisiin liittyviä yksityisiä avaimia voidaan käyttää vain seuraavien turvapalveluiden toteuttamiseksi:

- Varmenteen haltijan tai Laitteen tunnistaminen,
- Sähköisessä muodossa olevan tiedon alkuperän ja eheyden todentaminen,
- Sähköisessä muodossa olevan tiedon luottamuksellisuuden varmistaminen,

Copyright © TeliaSonera Finland 2004. All rights reserved

- Sähköisen allekirjoituksen todentaminen.

6.2.7 Varmenteen haltijan yksityisen avaimen suojaaminen

Kun Varmentaja luo Varmenteen haltijan Sonera Class 2 -varmenteeseen liittyvän yksityisen avaimen, Varmentaja säilyttää kopiota avaimen sisältävästä tiedostosta virhetilanteiden varalta 5 arkipäivän ajan. Muutoin yksityinen avain tulee suojata seuraavalla tavalla:

- yksityinen avain on Varmenteen haltijan yksinomaisessa hallinnassa sen jälkeen kun avain on luovutettu Varmenteen haltijalle,
- yksityinen avain on riittävästi suojattu, jotta se pysyy luottamuksellisena,
- Varmenteen haltija pystyy luotettavasti suojaamaan yksityisen avaimensa muiden luvattomalta käytöltä.

Kun Varmentaja luo avaimet, Varmentaja on myös vastuussa avainten salassapidosta ennen kuin ne on toimitettu Tilaajalle tai Varmenteen haltijalle. Varmentajan on huolehdittava tarvittavasta ohjeistuksesta Tilaajalle tai Varmenteen haltijalle yksityisen avaimen suojaamiseksi.

6.2.8 Varmenteen haltijan yksityisen avaimen key escrow

Varmenteen haltijan yksityisestä allekirjoitusavaimesta ei anneta kopioita käytettäväksi eikä säilytykseen kolmansille osapuolille.

6.2.9 Varmenteen haltijan yksityisen avaimen varmuuskopiointi

Kun Varmentaja luo Varmenteen haltijan yksityisen avaimen, Varmentaja säilyttää kopiota avaimen sisältävästä tiedostosta virhetilanteiden varalta 5 arkipäivän ajan, jonka jälkeen tiedosto tuhotaan.

6.2.10 Varmenteen haltijan yksityisen avaimen arkistointi

Varmenteen haltijan yksityistä avainta ei arkistoida ellei siitä erikseen sovita asiakkaan kanssa.

6.2.11 Varmenteen haltijan yksityisen avaimen aktivointi

Varmenteen haltijan yksityisen avaimen aktivointi tulee suojata PIN-koodilla.

6.2.12 Varmenteen haltijan yksityisen avaimen lukkiutuminen

Varmenteen haltijan yksityisen avaimen lukkiutuminen riippuu käytössä olevasta ohjelmistosta.

6.2.13 Varmenteen haltijan yksityisen avaimen tuhoaminen

Varmenteen haltijan yksityisiä avaimia ei tuhota niiden käyttöajan jälkeen, vaan ne jäävät Varmenteen haltijalle niiden elinkaaren päättymisen jälkeen.

6.2.14 Varmenteen haltijan julkisen avaimen arkistointi

Varmentaja arkistoi Varmenteen haltijan julkisen avaimen kappaleen 4.7 ”Tietojen arkistointi” mukaisesti.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

6.3 Varmenteen haltijan aktivointitieto

6.3.1 Aktivointitiedon luonti ja käyttöönotto

Jos avainpari luodaan Varmentajan toimesta, Varmenteen haltijan yksityisen avain ja siihen liittyvä avainparin luonnin yhteydessä muodostettava aktivointitieto (PIN-koodi) toimitetaan Varmenteen haltijalle erillisinä toimituksina erillisiä reittejä pitkin.

Jos avainpari luodaan asiakasorganisaatiossa, Tilaaja vastaa aktivointitiedon turvallisesta luonnista ja käyttöönotosta organisaatiossa.

Kun Varmenteen haltijalla on mahdollisuus vaihtaa aktivointitieto, Tilaajan velvollisuutena on huolehtia siitä että uusi aktivointitieto koostuu riittävän monesta merkistä, eikä ole helposti arvattavissa tai pääteltävissä.

6.3.2 Aktivointitiedon suojaaminen

Tilaajan velvollisuutena on huolehtia siitä, että Varmenteen haltija sitoutuu säilyttämään aktivointitietonsa riittävän turvallisesti.

6.4 Tietojärjestelmien turvavaatimukset

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

Erityisesti seuraavat seikat on otettu huomioon:

- kaikkien käyttäjien tunnistaminen,
- roolipohjainen pääsynvalvonta,
- tiettyjen tietoturvaan liittyvien 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.

6.5 Elinkaareen liittyvät tekniset turvatoimet

6.5.1 Järjestelmäkehityksen hallinta

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

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

6.5.2 Tietoturvallisuuden hallinta

6.5.2.1 Tietoturvallisuuden ylläpito

Varmentajan on huolehdittava siitä, että hallinta- ja ylläpitokäytännöt ovat riittäviä ja vastaavat tunnettuja standardeja.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

Mm. seuraavista asioista on huolehdittava:

- Varmentaja suorittaa liiketoimintaan liittyvää riskien arviointia tarvittavien turva- ja toimintamallien luomiseksi.
- Varmentaja vastaa varmennepalveluista kaikilta osin, vaikka osa toiminnoista on ulkoistettu alihankkijoille. Kolmansien osapuolten vastuut on selkeästi määritelty Varmentajan toimesta, ja riittävät toimenpiteet on suoritettu, jotta kolmannet osapuolet ovat sitoutuneita Varmentajan käytäntöihin. Varmentaja vastaa osapuolia koskevien käytäntöjen toimittamisesta kaikille osapuolille.
- Varmentajan organisaation johto ohjaa tietoturvaan liittyvää toimintaa ja vastaa Varmentajan tietoturvapolitiikan määrittelystä ja julkaisusta sekä politiikan viestittämisestä kaikille niille työntekijöille, joiden työhön se vaikuttaa.
- Varmentajan tietoturvan hallintaan tarvittavaa tietoturvajärjestelmää ylläpidetään jatkuvasti. Kaikki tietoturvan tasoon vaikuttavat muutokset hyväksyy Varmentajan organisaation johto.
- Varmennepalveluiden tuottamisessa käytettävien Varmentajan tuki- ja tuotantojärjestelmien ja tietoaineiston tietoturvan hallinta ja käytännön menettelyt täytyy dokumentoida sekä panna täytäntöön ja ylläpitää.
- Varmentaja huolehtii siitä, että tietoturvan taso säilyy riittävänä, kun Varmentajan toimintoja on ulkoistettu toiselle organisaatiolle tai osapuolelle.

6.5.2.2 Resurssien hallinta

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

6.5.2.3 Käyttöpalvelun hallinta

Varmentaja huolehtii siitä, että sen järjestelmät ovat turvallisia sekä huolellisesti ylläpidettyjä ja että toimintahäiriön riski on minimaalinen.

Varmentaja huolehtii mm. seuraavista toimenpiteistä:

- Varmentajan järjestelmien ja tietojen eheys suojataan viruksilta sekä luvattomilta ja järjestelmää vahingoittavilta ohjelmilta.
- Hyökkäyksistä ja toimintahäiriöistä aiheutuvaa vahinkoa minimoidaan raportoinnilla ja asianmukaisilla toimenpiteillä.
- Kaikkia tallennuslaitteita, tietovälineitä ja tietovarastoja käsitellään huolellisesti, jotta estettäisiin vahingot, murrot ja luvaton käyttö.
- Kaikille kappaleessa 5.2.1 ”Luotetut roolit” määritellyille rooleille luodaan ja toteutetaan riittävät toimintamallit ja -käytännöt.

<u>Tietovälineiden (esim. cd-levyt ja magneettinauhat) käsittely ja tietoturva</u>

Kaikkia tietovälineitä käsitellään huolellisesti. Luottamuksellista tietoa sisältävät tietovälineet varastoidaan turvallisesti hävitystä varten tai tuhotaan, kun niitä ei enää tarvita.

<u>Järjestelmäsuunnittelu</u>

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

<u>Tapahtumien raportointi ja toimenpiteet</u>

Varmentaja toimii huolellisesti ja hallitusti, jotta poikkeamiin pystytään reagoimaan nopeasti ja rajaamaan tietoturvaongelmien vaikutukset. Kaikki poikkeamat raportoidaan mahdollisimman pian tapahtuman jälkeen.

<u>Käyttöpalvelun toimintatavat ja -vastuut</u>

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

Varmentajan tietoturvaan liittyvät käyttötoiminnot tulee erottaa normaaleista järjestelmien käyttötoiminnoista.

6.5.2.4 Järjestelmien pääsynvalvonta

Varmentaja huolehtii siitä, että vain tietyillä valtuutetuilla henkilöillä on pääsy Varmentajan järjestelmiin.

Varmentaja huolehtii pääsynvalvonnasta mm. seuraavin toimenpitein:

Varmentajan yleinen toiminta

- Järjestelmien turvaamiseksi ja osana pääsynhallintaa Varmentaja huolehtii järjestelmien käyttäjien hallinnasta, johon kuuluu käyttäjätunnusten luonti, käytön seuranta ja oikea-aikainen käyttöoikeuksien muuttaminen ja poisto. Käyttäjiin lasketaan mm. järjestelmän operoijat, ylläpitäjät ja kaikki käyttäjät, joille on annettu pääsy järjestelmään.
- Varmentaja huolehtii siitä, että tietoon ja järjestelmän toimintoihin pääsyä rajoitetaan pääsynvalvontapolitiikan mukaisesti ja että Varmentajan järjestelmässä on riittävät turvamenettelyt erottamaan toisistaan kappaleessa 5.2.1 ”Luotetut roolit” määritellyt roolit. Erityisesti tietoturvan ylläpitäjän rooli on pidettävä erillään käyttötoiminnoista ja järjestelmän käyttöympäristön hallintaan liittyvien ohjelmien käyttöä on rajoitettava ja valvottava.
- Varmentajan henkilöstön tunnistus on suoritettava onnistuneesti ennen kuin he voivat käyttää varmenteiden hallintaan liittyviä kriittisiä ohjelmia.
- Varmentajan eri henkilöiden toimien on oltava selvitettävissä, esim. tallennetuista tapahtumalokeista.
- Luottamuksellinen tieto tulee suojata siten että se ei paljastu luvattomille käyttäjille, kun samoja tietovälineitä käytetään uudelleen (esim. poistetut tiedostot).

Varmenteiden jakelu

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

Sulkulistapalvelu

- Sulkulistapalveluun käytettävä sovellus käyttää pääsynvalvontaa estämään luvaton sulkulistatietojen muuttaminen.

6.5.2.5 Salausteknisen laitteiston elinkaaren hallinta

Varmentaja huolehtii varmenteiden ja sulkulistojen allekirjoitukseen käytettävään salausteknisen 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, aktivointi, varmistus ja palauttaminen laitteeseen vaativat vähintään kahden luotetun työntekijän yhtäaikaista paikallaoloa.
- Laite toimii käytössä oikein.
- Laitteeseen tallennetut Varmentajan yksityiset allekirjoitusavaimet tuhotaan, kun laitteisto poistetaan käytöstä.

6.6 Verkon turvallisuuden hallinta

Varmentaja huolehtii verkon turvallisuuden hallinnasta mm. seuraavin toimenpitein:

- Varmentajan sisäinen verkko suojataan ulkoisilta kolmansien osapuolten käyttämiltä verkoilta.
- Luottamuksellinen tieto suojataan, kun sitä siirretään turvattomissa verkoissa.
- Varmentaja vastaa siitä, että sen paikallisverkon komponentit (esim. reitittimet) pidetään fyysisesti turvallisessa ympäristössä ja että niiden konfiguraatiot tarkastetaan säännöllisesti vaatimustenmukaisuuden varmistamiseksi.

Copyright © TeliaSonera Finland 2004. All rights reserved

- Varmentaja seuraa järjestelmiä niissä mahdollisesti ilmenevien yllättävien tapahtumien varalta jatkuvan monitoroinnin, valvonnan ja hälytyslaitteiston avulla. Tällaisiin tapahtumiin luetaan mm. luvattoman käytön yritys tai epänormaali resurssien käyttö.

Copyright © TeliaSonera Finland 2004. All rights reserved

7 Sonera Class 2 -varmenteiden ja sulkulistojen (CRL) profiilit

7.1 Varmenteen profiili

Kaikki tähän politiikkaan viittaavat varmenteet julkaistaan X.509–standardin version 3 mukaisessa muodossa.

Varmenteet täyttävät dokumentin RFC 3280 ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile" vaatimukset.

7.1.1 Varmenteen kentät ja niiden sisällöt

Sonera Class 2 -varmenteen kentät on määritelty varmennuskäytännössä. Alla on kuvattu oleellisimpien kenttien sisältöä.

7.1.1.1 Varmenteen peruskentät

7.1.1.1.1 Versionumero

Sonera Class 2 -varmenteen profiilin versionumero on v3.

7.1.1.1.2 Issuer -kenttä

”Issuer”-kentän sisältö on kuvattu kappaleessa 3.1. ”Nimeämiskäytäntö Varmentajan varmenteissa”.

7.1.1.1.3 Subject -kenttä

”Subject”-kentän sisältö on kuvattu kappaleessa 3.2 ”Uuden Varmenteen haltijan rekisteröinti”.

7.1.1.2 Varmenteen lisäkentät

7.1.1.2.1 Varmennepolitiikan tunniste (OID)

Sonera Class 2 -varmenteet sisältävät tämän varmennepolitiikan tunnisteen, joka on määritelty kappaleessa 1.2.

Varmenne voi myös sisältää muiden politiikkojen tunnisteita, joita Varmentaja noudattaa.

7.1.1.3 Varmenteen kenttien sisällöt

Varmenteen kenttien sisällöt on kuvattu yksityiskohtaisesti varmennuskäytännöissä.

7.2 Sulkulistan profiili

Sulkulistat julkaistaan standardin X.509 version 2 mukaisessa muodossa. Sulkulistat täyttävät dokumentin RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" vaatimukset.

Copyright © TeliaSonera Finland 2004. All rights reserved

TeliaSonera Finland Oyj

Varmennuskäytännöissä määritellään sulkulistoissa käytettävät kentät ja niiden merkitykset.

Copyright © TeliaSonera Finland 2004. All rights reserved

8 Varmennepolitiikan hallinnointi

8.1 Muutoskäytännöt

8.1.1 Muutokset, jotka eivät vaadi ilmoitusta

Tähän dokumenttiin voidaan tehdä oikeinkirjoitukseen ja ulkoasuun liittyviä korjauksia, sekä muutoksia yhteystietoihin ilman ilmoitusta käyttäjille. Dokumentista voidaan myös julkaista käännöksiä eri kielillä ilman erillistä ilmoitusta.

8.1.2 Muutokset, jotka vaativat ilmoituksen

Seuraavat muutokset vaativat ilmoituksen:

- Osapuolten välisiin sopimusehtoihin vaikuttavista muutoksista ilmoitetaan kyseisten sopimusehtojen mukaisesti.
- Mitä tahansa varmennepolitiikan kohtaa voidaan muuttaa ilmoittamalla muutoksesta 15 päivää ennen muutoksen voimaanastumista.

Kaikki ilmoitusta vaativat ehdotetut muutokset julkaistaan osoitteessa http://support.partnergate.sonera.com/

Sopimusehtoihin vaikuttavista muutoksista ilmoitetaan kirjallisesti sopimuksen allekirjoittajan yhteystiedoissa mainittuun osoitteeseen.

8.1.3 Muutokset, jotka vaativat uuden politiikan

Jos Varmennepolitiikkayksikkö toteaa muutosten vaikuttavan merkittävästi laajaan politiikan käyttäjäryhmään, se voi oman harkintansa mukaan myöntää uuden tunnisteen (OID) muutetulle politiikalle. Uusi varmennepolitiikka toimitetaan niiden osapuolten saataville, joita se koskee.

8.2 Varmennepolitiikan julkaiseminen

Kopio tästä varmennepolitiikasta on saatavilla sähköisessä muodossa internetistä osoitteesta http://support.partnergate.sonera.com/

8.3 Varmennepolitiikan hyväksymismenettely

Varmentajan Varmennepolitiikkayksikkö vastaa tämän dokumentin sisällöstä ja kaikki politiikan muutokset edellyttävät Varmennepolitiikkayksikön hyväksyntää.

Copyright © TeliaSonera Finland 2004. All rights reserved

9 Varmennuskäytännöt (CPS)

Varmentajan täytyy osoittaa, että se on riittävän luotettava varmennepalveluiden tarjoajana. Erityisesti seuraavista asioista on huolehdittava:

a) Varmentajalla on julkinen dokumentti käytännöistä ja menettelytavoista, joiden avulla toteutetaan kaikki varmennepolitiikan vaatimukset.

b) Varmennuskäytäntö sisältää vaatimukset kaikille ulkoisille organisaatioille, jotka tukevat ja suorittavat Varmentajan toimintoja. Nämä vaatimukset sisältävät sovellettavat politiikat ja käytännöt.

c) Varmentaja toimittaa Tilaajien ja Luottavien osapuolten saataville varmennuskäytännöt sekä muun olennaisen dokumentaation, joka on tarpeen sen toteamiseksi, että toiminta on varmennepolitiikan mukaista.

d) Varmentaja saattaa Tilaajien ja potentiaalisten Luottavien osapuolten tietoon varmenteen käyttöön liittyvät ehdot.

e) Varmentajalla on johtoryhmä, jolla on viime kädessä valtuudet ja vastuu hyväksyä varmennuskäytännöt.

f) Varmentajan ylempi johto vastaa siitä, että toiminta on varmennuskäytännön mukaista.

g) Varmentaja määrittelee käytäntöjen noudattamiselle seurantaprosessin. Prosessi sisältää varmennuskäytäntöjen ylläpitovastuut.

h) Varmentaja antaa asiaankuuluvan ilmoituksen varmennuskäytäntöihin aiotuista muutoksista, ja kohdassa e) mainitun hyväksymismenettelyn jälkeen muutetut varmennuskäytännöt julkaistaan välittömästi kuten kohdassa c) edellytetään.

Varmennuskäytännöt ovat dokumentteja, joissa Varmentaja kuvaa, kuinka se toteuttaa tiettyä varmennepolitiikkaa. Tätä politiikkaa vastaavat käytännöt on kuvattu varmennuskäytännöissä jotka ovat saatavilla internetistä osoitteesta http://support.partnergate.sonera.com/.

Copyright © TeliaSonera Finland 2004. All rights reserved

Viiteluettelo

[ISO/IEC 9594-8; ITU-T X.509]	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. Also published as ITU-T Rec. X.509: Public key and attribute certificates frameworks
[RFC 2527]	IETF:n dokumentti: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
[SAK Laki]	Laki sähköisistä allekirjoituksista (tullut voimaan 1.2.2003)
[PKIX Roadmap]	IETF:n dokumentti: Internet X.509 Public Key Infrastructure: Roadmap
[ETSI TS 101 456 v1.2.1]	ETSI Technical Standard: Policy Requirements for certification authorities issuing qualified certificates
[RFC 3280]	IETF:n dokumentti: Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile

Copyright © TeliaSonera Finland 2004. All rights reserved