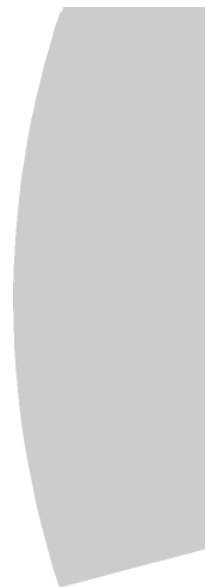


ETSI TS 101 456 v1.4.3 c2007-05_a

Tekninen spesifikaatio

Sähköiset allekirjoitukset ja järjestelmät – laatuvarmenteita myöntäviä varmentajia koskevat menettelytapavaatimukset



Viite

RTS/ESI-000058

Asiasanat

sähköinen kaupankäynti, sähköinen allekirjoitus, turvallisuus

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Puh.: +33 4 92 94 42 00 Faksi: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association 6 but non lucratif enregistree 6 la
Sous-Prefecture de Grasse (06) N° 7803/88

Tärkeä huomautus

Yksittäisiä tämän asiakirjan kopioita voi ladata osoitteesta

<http://www.etsi.org>

Tästä asiakirjasta voi olla saatavilla useampia sähköisiä tai painettuja versioita. Jos tällaisten versioiden välillä havaitaan sisällöllisiä eroavaisuuksia, lähdeversiona pidetään pdf-asiakirjaa (Portable Document Format). Riita-asioissa lähdeversiona pidetään ETSIn tulostimilla tehtävää tulostetta pdf-versiosta, jota säilytetään ETSI-sihteeristössä tietyllä verkkoasemalla.

Tämän asiakirjan käyttäjien on hyvä tietää, että asiakirjaan voidaan tehdä muutoksia tai sen tilaa voidaan muuttaa. Tiedot tämän ja muiden ETSI-asiakirjojen tilasta ovat saatavilla osoitteessa

<http://portal.etsi.org/tb/status/status.asp>

Jos havaitset virheitä tässä asiakirjassa, lähetä huomiosi johonkin palveluistamme, jonka yhteystiedot annetaan osoitteessa

http://portal.etsi.org/chaicor/ETSI_support.asp

Tekijänoikeudet

Mitään osaa ei saa jäljentää muutoin kuin kirjallisella luvalla.
Tekijänoikeudet ja edellä mainittu rajoitus koskevat jäljentämistä millä tahansa välineellä.

© European Telecommunications Standards Institute 2007.

Kaikki oikeudet pidätetään.

DECT™, PLUGTESTS™ ja UMTS™ ovat ETSIn tavaramerkkejä, jotka se on rekisteröinyt jäseniensä hyödyttämiseksi. TIPHON™ ja TIPHON logo ovat tavaramerkkejä, joita ETSI on parhaillaan rekisteröimässä jäsentensä hyödyttämiseksi. 3GPP™ on ETSIn tavaramerkki, jonka se on rekisteröinyt jäseniensä sekä 3GPP-organisaation yhteistyökumppanien hyödyttämiseksi.

Sisältö

IMMATERIAALIOIKEUDET	6
ESIPUHE.....	6
JOHDANTO	6
1 SOVELTAMISALA.....	7
2 VIITELUETTELO	7
3 MÄÄRITELMÄT JA LYHENTEET	8
3.1 Määritelmät.....	8
3.2 Lyhenteet	10
4 YLEISKÄSITTEET	10
4.1 Varmentaja	10
4.2 Varmennepalvelut.....	11
4.3 Varmennepolitiikka ja varmennuskäytäntö	12
4.3.1 Tarkoitus	12
4.3.2 Yksityiskohtaisuus	13
4.3.3 Lähestymistapa.....	13
4.3.4 Muut varmentajan julkiset asiakirjat	13
4.4 Tilaaja ja allekirjoittaja.....	13
5 JOHDANTO LAATUVARMENNEPOLITIIKKOIHIN	14
5.1 Yleistä.....	14
5.2 Yksilöintitunnukset.....	14
5.3 Käyttäjyhteisö ja sovellettavuus	15
5.3.1 QCP public + SSCD -laatuvarmennepolitiikka	15
5.3.2 QCP public -laatuvarmennepolitiikka	15
5.4 Vaatimustenmukaisuus	15
5.4.1 Yleistä	15
5.4.2 QCP public + SSCD -laatuvarmennepolitiikka	16
5.4.3 QCP public -laatuvarmennepolitiikka	16
6 VELVOLLISUUDET JA VASTUUT JA VASTUUNRAJOITUKSET.....	16
6.1 Varmentajan velvollisuudet	16
6.2 Tilaajan velvollisuudet	16
6.3 Tiedottaminen varmenteeseen luottaville osapuolille.....	17
6.4 Vastuu.....	17
7 VARMENTAJAN TOIMINTAA KOSKEVAT VAATIMUKSET	18
7.1 Varmennuskäytäntö	18
7.2 Julkisen avaimen järjestelmässä käytettävien avainten elinkaaren hallinta	19
7.2.1 Varmentajan avaimen luominen.....	19
7.2.2 Varmentajan avaimen tallennus, varmuuskopiointi ja palauttaminen	19
7.2.3 Varmentajan julkisen avaimen jakelu	20
7.2.4 Vara-avainjärjestelmä.....	20

7.2.5	Varmentajan avaimen käyttö.....	20
7.2.6	Varmentajan avaimen elinkaaren päätyminen.....	20
7.2.7	Varmenteiden allekirjoittamisessa käytettävän salauslaitteiston elinkaaren hallinta	21
7.2.8	Varmentajan tarjoamat allekirjoittajan avaimen hallintapalvelut	21
7.2.9	Turvallisen allekirjoituksen luomisvälineen valmistaminen	21
7.3	Julkisen avaimen järjestelmässä käytettävien varmenteiden elinkaaren hallinta	22
7.3.1	Allekirjoittajan rekisteröinti	22
7.3.2	Varmenteen uusiminen, sen avainparin vaihtaminen ja varmenteen päivittäminen	24
7.3.3	Varmenteiden luominen	24
7.3.4	Varmentajan toimintaan liittyvien asiakirjojen jakelu.....	25
7.3.5	Varmenteiden jakelu	26
7.3.6	Varmenteen sulkeminen ja voimassaolon keskeyttäminen tilapäisesti	26
7.4	Varmentajan johtamis- ja toimintakäytännöt.....	28
7.4.1	Turvallisuuden hallinta.....	28
7.4.2	Varantojen luokittelu ja hallinta	28
7.4.3	Henkilöstö ja tietoturva	28
7.4.4	Fyysinen ja ympäristön turvallisuus.....	30
7.4.5	Toiminnan hallinta	30
7.4.6	Järjestelmiin pääsyn hallinta.....	32
7.4.7	Luotettavien järjestelmien käyttöönotto ja ylläpito	33
7.4.8	Liiketoiminnan jatkuvuuden hallinta ja häiriötilanteiden käsittely.....	33
7.4.9	Varmentajan toiminnan päätyminen.....	34
7.4.10	Lainsäädäntöön perustuvien vaatimusten noudattaminen	35
7.4.11	Laatuvarmenteita koskevan tiedon säilyttäminen	35
7.5	Organisaatioon liittyvät vaatimukset.....	37
8	MÄÄRITTELYPUITTEET MUITA LAATUVARMENNEPOLITIIKKOJA VARTEN	37
8.1	Laatuvarmennepolitiikan hallinta	38
8.2	Poikkeukset laatuvarmennepolitiikkoihin, jotka koskevat muille kuin yleisölle myönnettäviä laatuvarmenteita 38	
8.3	Lisävaatimukset.....	38
8.4	Vaatimustenmukaisuus.....	39
	LIITE A (TIEDOKSI): SÄHKÖISTEN ALLEKIRJOITUSTEN KÄYTTÖÖN LIITTYVÄ MAHDOLLINEN VASTUU	40
	LIITE B (TIEDOKSI): VARMENNEKUVAUKSEN MALLI	44
	B.1 JOHDANTO.....	44
	B.2 VARMENNEKUVAUKSEN RAKENNE	44
	LIITE C (TIEDOKSI): SÄHKÖISIÄ ALLEKIRJOITUKSIA KOSKEVAN DIREKTIIVIN JA LAATUVARMENNEPOLITIIKAN VÄLISET RISTIVIITTAUKSET	46
	LIITE D (TIEDOKSI): IETF RFC 3647/RFC 2527 -JULKAISUJEN JA LAATUVARMENTEITA KOSKEVIEN MENETTELYTAPAVAATIMUSTEN VÄLISET RISTIVIITTAUKSET	47
	LIITE E (TIEDOKSI): VERSION 1.2.1 JÄLKEEN TEHDYT MUUTOKSET	52
	E.1 LISÄTYT VAATIMUKSET.....	52
	E.2 PÄIVITETYT VAATIMUKSET.....	52

E.3	SELVENNYKSET	52
E.4	TOIMITUKSELLISET MUUTOKSET	52
E.5	VERSION 1.3.1 JÄLKEEN TEHDYT MUUTOKSET	52
	LIITE F (TIEDOKSI): LÄHDEKIRJALLISUUS.....	53
	VERSIONHISTORIA	54

Immateriaalioikeudet

ETSille on mahdollisesti ilmoitettu tähän asiakirjaan liittyvistä olennaisista tai mahdollisesti olennaisista immateriaalioikeuksista. Tällaisiin mahdollisiin olennaisiin immateriaalioikeuksiin liittyvät tiedot ovat julkisesti **ETSI:n jäsenten sekä muiden tahojen** saatavilla ja löytyvät ETSIn julkaisusta ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", joka on saatavana ETSI-sihteeristöstä. Viimeisimmät päivitykset ovat saatavilla ETSIn verkkopalvelimelta (<http://webapp.etsi.org/IPR/home.asp>).

Immateriaalioikeuksia koskevan käytäntönsä mukaisesti ETSI ei ole selvittänyt asiaa esimerkiksi immateriaalioikeuksien hauruilla. Muiden kuin ETSI SR 000 314 -julkaisussa (tai ETSIn verkkopalvelimella olevissa päivityksissä) mainittujen immateriaalioikeuksien olemassaolosta tai niiden mahdollisesta nykyisestä tai tulevasta olennaisuudesta tähän asiakirjaan nähden ei anneta takeita.

Esipuhe

Tämän teknisen spesifikaation on laatinut sähköisiä allekirjoituksia ja järjestelmiä käsittelevä ETSIn tekninen komitea (ETSI Technical Committee Electronic Signatures and Infrastructures (ESI)).

Johdanto

Sähköinen kaupankäynti on muuttumassa merkittäväksi liiketoiminta- ja viestintätavaksi, jota käytetään julkisissa ja yksityisissä verkoissa. Sähköisen kaupankäynnin tärkeä edellytys on kyky tunnistaa sähköisen tiedon lähde vastaavalla tavalla kuin asiakirjoihin käsin tehtyjen allekirjoitusten perusteella. Tämä voidaan yleensä toteuttaa käyttämällä sähköisiä allekirjoituksia. Sähköisiä allekirjoituksia tukevat varmenteita myöntävät varmennepalvelujen tarjoajat, joita yleisesti kutsutaan varmentajiksi.

Jotta sähköisten allekirjoitusten käyttäjät voisivat luottaa sähköisten allekirjoitusten aitouteen, heidän on luotettava siihen, että varmentajalla on käytössään asianmukaiset menettelyt ja suojaamiskeinot, joilla minimoidaan julkisiin salausavainten järjestelmiin liittyvät toiminnalliset ja taloudelliset riskit.

Sähköisiä allekirjoituksia koskevista yhteisön puitteista annetussa Euroopan parlamentin ja neuvoston direktiivissä 1999/93/EY [1] (jäljempänä "direktiivi") yksilöidään laatuvarmenteeseen perustuva sähköisen allekirjoituksen erityismuoto. Direktiivin liitteessä I määritetään laatuvarmenteita koskevat vaatimukset. Direktiivin liitteessä II määritetään laatuvarmenteita myöntävien varmennepalvelujen tarjoajia koskevat vaatimukset (eli laatuvarmenteita myöntäviä varmentajia koskevat vaatimukset). Tässä asiakirjassa määritetään menettelytapavaatimukset, jotka koskevat direktiivin mukaisesti laatuvarmenteita myöntävien varmentajien toimintaa ja hallintakäytäntöjä. Tässä asiakirjassa esitetyissä menettelytapavaatimuksissa turvallisen allekirjoituksen luomisvälineen käyttö, josta esitetään vaatimuksia direktiivin liitteessä III, on valinnainen osio.

Tätä asiakirjaa sovelletaan myös varmentajiin, jotka sisällyttävät laatuvarmenteisiin attribuutteja. Attribuuttivarmenteita myöntäviä varmentajia koskevat menettelytapavaatimukset määritetään spesifikaatiossa TS 102 158 [14].

1 Soveltamisala

Tässä asiakirjassa määritetään menettelytapavaatimukset, jotka koskevat laatuvarmenteita myöntäviä varmentajia (direktiivissä [1] käytetään ilmaisua "hyväksytyjä varmenteita myöntävät varmennepalvelujen tarjoajat"). Menettelytapavaatimuksia asetetaan laatuvarmenteita myöntävien varmentajien toiminnalle ja hallintakäytännöille, jotta tilaajat, varmentajan varmentamat allekirjoittajat sekä varmenteeseen luottavat osapuolet voisivat luottaa siihen, että varmenteella voidaan vahvistaa sähköisiä allekirjoituksia.

Menettelytapavaatimukset annetaan seuraavasti:

- a) määrittellään kaksi yleisölle myönnettäviä laatuvarmenteita koskevaa, läheisesti toisiinsa liittyvää laatuvarmennepolitiikkaa, joista toinen edellyttää turvallisen allekirjoituksen luomisvälineen käyttöä
- b) esitetään määrittelypuitteet sellaisia laatuvarmennepolitiikkoja varten, joilla parannetaan edellä mainittuja varmenneimenettelytapoja tai jotka koskevat muille kuin yleisöksi katsottaville käyttäjäryhmille myönnettäviä laatuvarmenteita.

Varmentajaa koskevat menettelytapavaatimukset sisältävät vaatimuksia rekisteröintipalvelujen tarjoamisesta, varmenteiden luomisesta, varmenteiden jakelusta, varmenteiden peruuttamisen hallinnasta, sulkuilasta ja tarvittaessa allekirjoituksen luomisvälineen tarjoamisesta. Muut varmennepalvelujen tarjoajan toiminnot, kuten aikaleimat, attribuuttivarmenteet ja luottamuksellisuutta tukevat palvelut, eivät kuulu tämän asiakirjan soveltamisalaan. Tässä asiakirjassa ei esitetä vaatimuksia varmentajan varmenteille, ei myöskään varmennehierarkioiden tai ristiinvarmentamisen suhteen. Nämä menettelytapavaatimukset on rajattu koskemaan sähköisten allekirjoitusten yhteydessä käytettävien avainten varmentamista.

Nämä menettelytapavaatimukset on erityisesti kohdistettu yleisölle myönnettäviin laatuvarmenteisiin, joita käytetään tukemaan sähköisiä laatu-allekirjoituksia (eli sellaisia sähköisiä allekirjoituksia, jotka oikeusvaikutuksiltaan vastaavat käsittehtyjä allekirjoituksia sähköisiä allekirjoituksia koskevasta yhteisön puitteista annetun EU-direktiivin 5 artiklan 1 kohdan [1] mukaisesti). Erityisesti käsitellään vaatimuksia, jotka koskevat direktiivin [1] liitteiden I ja II mukaisesti laatuvarmenteita myöntäviä varmentajia. Liitteen III mukaisen turvallisen allekirjoituksen luomisvälineen käyttö, joka on 5 artiklan 1 kohdan mukaisesti sähköisiä allekirjoituksia koskeva vaatimus, on tässä asiakirjassa esitetyissä menettelytapavaatimuksissa valinnainen osio.

Näiden menettelytapavaatimusten mukaisesti myönnettyjä varmenteita voidaan käyttää henkilön todentamisessa, kun henkilö toimii omasta puolestaan tai edustamansa luonnollisen henkilön, oikeushenkilön tai yhteisön puolesta.

Nämä menettelytapavaatimukset koskevat julkisen avaimen salauksen käyttöä sähköisten allekirjoitusten vahvistamisessa.

Asiantuntevat riippumattomat elimet voivat käyttää tätä asiakirjaa perustana arvioidessaan, täyttääkö varmentaja laatuvarmenteiden myöntämistä koskevat vaatimukset.

Tilaajia ja varmenteeseen luottavia osapuolia suositellaan lukemaan varmentajan varmennuskäytännöstä tarkempia lisätietoja siitä, kuinka kyseinen varmentaja toteuttaa tiettyä varmennepolitiikkaansa.

Tässä asiakirjassa ei kuitenkaan tarkenneta, kuinka riippumattomat osapuolet voivat arvioida tässä yksilöityjä vaatimuksia, esimerkiksi ei määritetä vaatimuksia riippumattomien arvioijien saataville annettavan tiedon tai riippumattomien arvioijien suhteen.

HUOMAUTUS: Katso vaatimustenmukaisuuden arviointia koskeva CEN-työryhmän sopimus CWA 14172 "EESSI Conformity Assessment Guidance".

2 Viiteluettelo

Tässä asiakirjassa viitataan seuraavissa asiakirjoissa esitettyihin säännöksiin, jotka muodostavat näin ollen myös tämän asiakirjan säännöksiä.

- Käytetyt viittaukset ovat täsmällisiä (yksilöidään julkaisupäivä ja/tai laitoksen tai version numero) tai yleisluontoisia.

- Täsmällisten viittausten osalta lähteen myöhempiä tarkistuksia ei sovelleta.
- Yleisluontoisten viittausten osalta sovelletaan lähteen viimeisintä versiota.

Jos lähdeasiakirjaa ei ole julkisesti saatavilla odotetussa sijainnissa, se saattaa löytyä osoitteesta <http://docbox.etsi.org/Reference>.

HUOMAUTUS: Tässä kohdassa käytetyt linkit olivat toimivia julkaisuhetkellä, mutta ETSI ei voi taata niiden toimivuutta pitkällä aikavälillä.

- [1] Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY, annettu 13 päivänä joulukuuta 1999, sähköisiä allekirjoituksia koskevista yhteisön puiteista.

HUOMAUTUS: Tässä asiakirjassa tästä käytetään ilmaisua "direktiivi".

- [2] IETF RFC 3647 (2003): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

HUOMAUTUS: Kumoo julkaisun IETF RFC 2527.

- [3] ITU-T Recommendation X.509 (2000)4SO/IEC 9594-8 (2001): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
- [4] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
- [5] FIPS PUB 140-2 (2001): "Security Requirements For Cryptographic Modules".
- [6] ETSI TS 101 862: "Qualified certificate profile".
- [7] ISO/IEC 15408 (2005) (osat 1–3): "Information technology - Security techniques - Evaluation criteria for IT security".
- [8] CEN Workshop Agreement 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".
- [9] CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)".
- [10] CEN Workshop Agreement 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)".
- [11] CEN Workshop Agreement 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP".
- [12] Neuvoston direktiivi 93/13/ETY, annettu 5 päivänä huhtikuuta 1993, kuluttajasopimusten kohtuuttomista ehdoista.
- [13] ISO/IEC 17799 (2005): "Information technology - Security techniques - Code of practice for information security management".
- [14] ETSI TS 102 158: "Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates".

3 Määritelmät ja lyhenteet

3.1 Määritelmät

Tässä asiakirjassa käytetään seuraavia käsitteitä ja määritelmiä:

kehittynyt sähköinen allekirjoitus: sähköinen allekirjoitus, joka täyttää seuraavat vaatimukset: se liittyy yksiselitteisesti

- a) sen allekirjoittajaan;
- b) sillä voidaan yksilöidä allekirjoittaja;
- c) se on luotu keinoilla, jotka allekirjoittaja voi pitää yksinomaisessa valvonnassaan, ja
- d) se on liitetty sen kohteena olevaan tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita (katso direktiivi 1999/93/EY [1]).

attribuutti: tahoon liitetty tieto, joka määrittelee tahon ominaisuuden, kuten ryhmän jäsenyyden tai roolin, tai muu kyseiseen tahoon liittyvä tieto

varmenne: sisältää käyttäjän julkisen avaimen sekä muita tietoja, joiden väärentäminen on estetty salakirjoittamalla ne varmenteen myöntäneen varmentajan yksityisellä avaimella

HUOMAUTUS: Katso ITU-T:n suositus X.509 [3].

varmentaja: varmenteita luova ja myöntävä taho, jonka toimintaan yksi tai useampi käyttäjä luottaa

HUOMAUTUS 1: Katso ITU-T:n suositus X.509 [3].

HUOMAUTUS 2: Varmentaja on varmenteita myöntävä varmennepalvelujen tarjoaja. Varmentajan käsitettä selvennetään lisää kohdassa 4.2.

varmennepolitiikka: periaatteet, joilla osoitetaan tietyn varmenteen soveltuvuus tietylle yhteisölle ja/tai sovellusluokka, jota koskee yhteiset turvallisuusvaatimukset

HUOMAUTUS 1: Katso ITU-T:n suositus X.509 [3].

HUOMAUTUS 2: Lisätietoja varmennepolitiikkojen ja varmennuskäytännön keskinäisestä suhteesta annetaan kohdassa 4.3.

varmennuskäytäntö: kuvaus toimintatavoista, joita varmentaja noudattaa varmenteiden myöntämisessä, hallinnoimisessa, peruuttamisessa ja uusimisessa sekä varmenteiden avainparin vaihtamisessa

HUOMAUTUS: Katso RFC 3647 [2].

varmenteiden sulkulista: allekirjoitettu varmenneluettelo, jonka sisältämiä varmenteita niiden myöntäjät eivät enää katso voimassa oleviksi

HUOMAUTUS: Katso ITU-T:n suositus X.509 [3].

varmennepalvelujen tarjoaja: yhteisö, oikeushenkilö tai luonnollinen henkilö, joka myöntää varmenteita tai tarjoaa muita sähköisiin allekirjoituksiin liittyviä palveluja

HUOMAUTUS 1: Katso direktiivi 1999/93/EY [1].

HUOMAUTUS 2: Tässä asiakirjassa käsitellään varmennepalvelujen tarjoajia, jotka myöntävät laatuvarmenteita (tai tarjoavat laatuvarmenteiden myöntämisen osapalveluja – katso kohta 4.1). Tässä asiakirjassa ei käsitellä varmennepalvelujen tarjoajan muuntotyypisiä toimintoja, kuten aikaleimausta ja vara-avainjärjestelmiä.

sähköinen allekirjoitus: sähköisessä muodossa oleva tieto, joka on liitetty tai loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään kyseisen muun tiedon todentamisen menetelmänä

HUOMAUTUS: Katso direktiivi 1999/93/EY [1].

laatuvarmenne: varmenne, joka täyttää direktiivin 1999/93/EY [1] liitteessä I säädetyt vaatimukset ja jonka on myöntänyt direktiivin 1999/93/EY [1] liitteessä II säädetyt vaatimukset täyttävä varmentaja

laatuvarmennepolitiikka: varmennepolitiikka, johon sisältyy direktiivin 1999/93/EY [1] liitteissä I ja II säädetyt vaatimukset

sähköinen laatuallekirjoitus: kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja joka on tehty turvallisella allekirjoituksen luomisvälineellä direktiivissä 1999/93/EY [1] olevan 5 artiklan 1 kohdan mukaisesti

varmenteeseen luottava osapuoli: varmenteen vastaanottaja, joka toimii luottaen kyseiseen varmenteeseen ja/tai digitaalisiin allekirjoituksiin, jotka on todennettu kyseisellä varmenteella

HUOMAUTUS: Katso RFC 3647 [2].

allekirjoituksen luomiseen käytettävät tiedot: ainutlaatuinen tietokokonaisuus, esimerkiksi koodit tai yksityiset salausavaimet, joita allekirjoittaja käyttää luodakseen sähköisen allekirjoituksen

HUOMAUTUS 1: Katso direktiivi 1999/93/EY [1].

HUOMAUTUS 2: Kun kyseessä ovat julkisen avaimen salaukseen perustuvat laatuvarmenteet, kuten tämän asiakirjan soveltamisalassa, allekirjoituksen luomiseen käytettävät tiedot sisältävät yksityiset avaimet. Tässä asiakirjassa allekirjoituksen luomiseen käytettävistä tiedoista käytetäänkin käsitettä yksityinen avain.

allekirjoituksen luomisväline: tarkoituksenmukaisesti määritetty ohjelmisto tai laitteisto, jolla allekirjoituksen

luomiseen käytettävät tiedot käsitellään HUOMAUTUS: Katso direktiivi 1999/93/EY [1].

turvallinen allekirjoituksen luomisväline: allekirjoituksen luomisväline, joka täyttää direktiivin 1999/93/EY [1] liitteessä III säädetyt vaatimukset

allekirjoituksen todentamiseen käytettävät tiedot: tietokokonaisuus, esimerkiksi koodit tai julkiset salausavaimet, joita käytetään sähköisen allekirjoituksen todentamiseen

HUOMAUTUS 1: Katso direktiivi 1999/93/EY [1].

HUOMAUTUS 2: Kun kyseessä ovat julkisen avaimen salaukseen perustuvat laatuvarmenteet, kuten tämän asiakirjan soveltamisalassa, allekirjoituksen todentamiseen käytettävät tiedot sisältävät julkiset avaimet. Tässä asiakirjassa allekirjoituksen todentamiseen käytettävistä tiedoista käytetäänkin käsitettä julkinen avain.

allekirjoittaja: taho, joka on varmenteessa merkitty varmenteessa annettuun julkiseen avaimen liittyvän yksityisen avaimen haltijaksi

tilaaja: taho, joka tilaa varmentajalta palvelun yhden tai useamman allekirjoittajan puolesta

HUOMAUTUS: Allekirjoittaja voi olla tilaaja, joka toimii omasta puolestaan.

3.2 Lyhenteet

Tämän asiakirjan aihealueeseen liittyviä seuraavia englanninkielisiä lyhenteitä ja käsitteitä:

CA	Certification Authority: varmentaja
CPS	Certification Practice Statement: varmennuskäytäntö
CRL	Certificate Revocation List: varmenteiden sulkulista
CSP	Certification Service Provider: varmennepalvelujen tarjoaja
PDS	PKI Disclosure Statement: varmennekuvaus
PKI	Public Key Infrastructure: julkisen avaimen järjestelmä
QCP	Qualified Certificate Policy: laatuvarmennepolitiikka
RSA	Rivest Shamir Adleman: RSA-algoritmi
SSCD	Secure Signature Creation Device: turvallinen allekirjoituksen luomisväline

4 Yleiskäsitteet

4.1 Varmentaja

Varmentajaksi kutsutaan varmenteita luovaa ja myöntävää tahoja, jonka toimintaan varmennepalvelujen käyttäjät (eli tilaajat ja varmenteeseen luottavat osapuolet) luottavat. Varmentaja on kokonaisvastuussa kohdassa 4.2 määriteltyjen varmennepalvelujen tarjoamisesta. Varmentaja on yksilöity varmenteessa varmenteen myöntäjäksi, ja laatuvarmenteet allekirjoitetaan sen yksityisellä avaimella.

Varmentaja voi käyttää varmennepalvelussaan muita osapuolia, jotka tarjoavat palvelun osia. Varmentaja säilyy kuitenkin aina kokonaisvastuussa ja varmistaa, että tässä asiakirjassa määritellyt menettelytapa-vaatimukset täyttyvät. Varmentaja voi esimerkiksi hankkia alihankintana kaikki osapalvelut, myös varmenteiden luomispalvelun. Varmenteiden allekirjoittamiseen käytettävä avain kuitenkin määritellään kuitenkin varmentajalle kuuluvaksi, ja varmentajalla säilyy kokonaisvastuu tässä asiakirjassa määriteltyjen vaatimusten täyttämistä sekä vastuu yleisölle myönnettävien

varmenteiden myöntämisestä direktiivin [1] mukaisesti.

Varmentaja on direktiivissä [1] määritellyn mukainen varmennepalvelujen tarjoaja, joka myöntää varmenteita.

4.2 Varmennepalvelut

Laatuvarmenteiden myöntäminen on tässä asiakirjassa jaoteltu vaatimusten luokittelusyistä seuraaviin osapalveluihin:

- **Rekisteröintipalvelu:** Todennetaan allekirjoittajan henkilöllisyys ja mahdolliset häneen liittyvät erityiset attribuutit. Tämän palvelun tulokset välitetään varmenteiden luomispalveluun.

HUOMAUTUS 1: Palvelu sisältää myös hallussapidon selvittämiskäytännön, avaimille jotka eivät ole CA:n luomia..

- **Varmenteiden luomispalvelu:** Luodaan ja allekirjoitetaan varmenteita, jotka perustuvat rekisteröintipalvelussa todennettuun henkilöllisyyteen ja muihin attribuutteihin.
- **Jakelupalvelu:** Jaetaan varmenteita allekirjoittajille, ja jos allekirjoittajalta saadaan lupa, varmenteet asetetaan varmenteeseen luottavien osapuolten saataville. Lisäksi palvelussa asetetaan varmentajan käyttöehdot sekä kaikki julkaistut varmennepolitiikkoja ja varmennuskäytäntöä koskevat tiedot tilaajien ja varmenteeseen luottavien osapuolten saataville.
- **Sulkupalvelu:** Käsitellään sulkupyynnöt ja -ilmoitukset, ja määritetään tarvittavat toimet käsittelyn perusteella. Palvelun tulokset jaetaan sulkutilasta tiedottavan palvelun kautta.
- **Varmenteen tilatietopalvelu:** Annetaan varmenteiden tilatietoja varmenteeseen luottaville osapuolille. Palvelussa voidaan käyttää varmenteiden sulkulistoja tai reaaliaikaista yksittäisten tilatietojen välittämistä. Tilatietoja saatetaan päivittää tietyin väliajoin, joten on mahdollista, etteivät tiedot aina vastaa varmenteen nykytilaa.

sekä valinnaisesti:

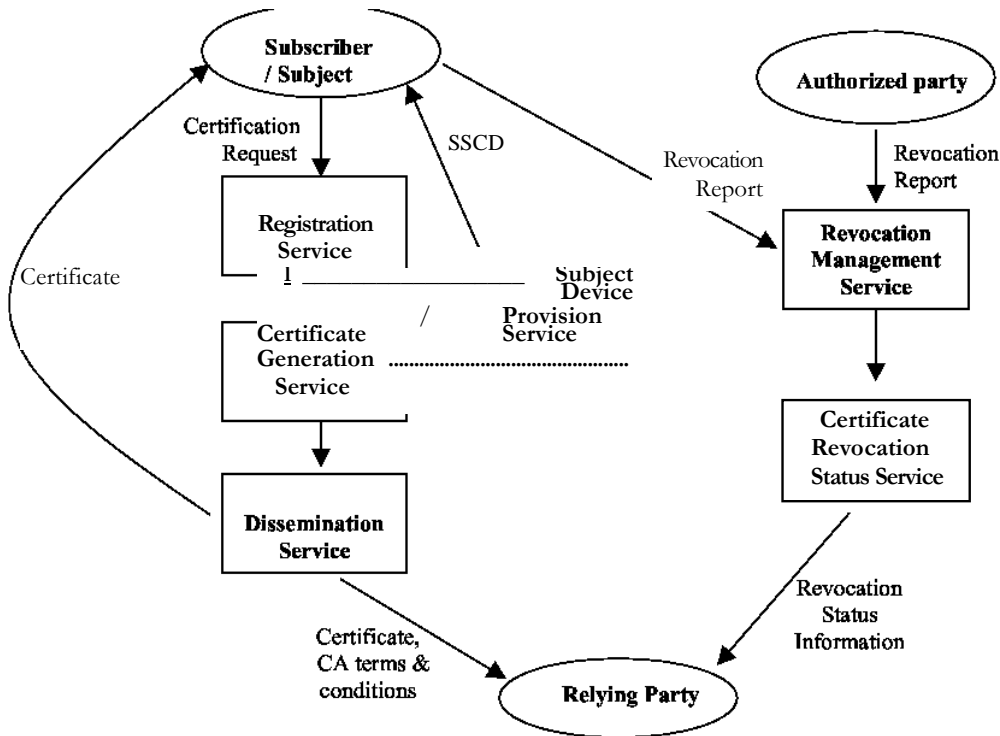
- **Välineen tarjoaminen allekirjoittajalle:** Valmistetaan ja toimitetaan allekirjoittajille

allekirjoituksen luomisväline. HUOMAUTUS 2: Esimerkkejä palvelusta:

- Palvelussa luodaan allekirjoittajan avainpari ja toimitetaan allekirjoittajalle yksityinen avain
- Palvelussa valmistetaan allekirjoittajan turvallisen allekirjoituksen luomisväline (SSCD) sekä välineen käyttöön oikeuttavat koodit, ja toimitetaan kyseinen väline rekisteröidylle allekirjoittajalle.

Käytetyn palvelujaottelun ainoa tarkoitus on selvittää menettelytapavaatimuksia, eikä tässä aseteta mitään rajoituksia varmentajan palvelutoteutuksen jaotteluun.

Kuvassa 1 esitetään palvelujen väliset suhteet.



Kuva 1: Tässä asiakirjassa käytettävä varmennepalvelujen jaottelu

Kuvatekstit:

Certificate, CA terms and conditions: Varmenne ja varmentajan käyttöehdot

Subscriber / Subject: Tilaaaja / Allekirjoittaja

Certification Request: Varmennepyyntö

Registration Service: Rekisteröintipalvelu

Certificate Generation Service: Varmenteiden luomispalvelu

Dissemination Service: Jakelupalvelu

Certificate, CA terms & conditions: Varmenne ja varmentajan asettamat ehdot ja vaatimukset

SSCD: Turvallinen allekirjoituksen luomisväline

Subject Device Provision Service: Välineen tarjoaminen allekirjoittajalle

Relying Party: Varmenteeseen luottava osapuoli

Revocation Report: Sulkupyntö

Authorized party: Valtuutettu osapuoli

Revocation Report: Sulkupyntö

Revocation Management Service: Sulkupalvelu

Certificate Revocation Status Service: Varmenteen tilatietopalvelu

Revocation Status Information: Sulkutilatieto

4.3 Varmennepolitiikka ja varmennuskäytäntö

Tässä kohdassa selostetaan varmennepolitiikan ja varmennuskäytännön välistä suhdetta. Mitään varmennepolitiikan muotoa tai varmennuskäytännön erittelyjä koskevia rajoituksia ei kuitenkaan tässä aseteta.

4.3.1 Tarkoitus

Varmennepolitiikka, jonka tunnus ilmoitetaan varmenteessa, kertoo yleisesti ottaen, "mitä on noudatettava". Varmennuskäytännössä puolestaan kerrotaan, "miten noudattaminen toteutetaan", eli mitä prosesseja varmenteen luomisessa ja ylläpitämisessä käytetään. Varmennepolitiikan ja varmennuskäytännön määrittelevien asiakirjojen välinen suhde on vastaava kuin muualla liike-elämässä: liiketoimintakohtaisissa toimintapolitiikoissa määritellään kyseiselle liiketoiminnalle asetetut vaatimukset, kun taas operatiivisissa yksiköissä määritellään käytännöt ja yksityiskohtaiset menettelyt, joilla toimintapolitiikkoja on tarkoitus toteuttaa.

Tässä asiakirjassa määritetään varmennepolitiikat, joilla täytetään laatuvarmenteita koskevat, direktiivin [1] liitteissä I ja II säädetyn mukaiset vaatimukset. Varmentajat puolestaan määrittävät varmennuskäytännöissään, kuinka nämä vaatimukset täytetään.

Mikäli varmennepolitiikkaan tehdään sen sovellettavuuteen vaikuttavia muutoksia, kyseisen varmennepolitiikan yksilöivä tunnus on syytä vaihtaa.

4.3.2 Yksityiskohtaisuus

Varmennepolitiikka ei sisällä yhtä paljon yksityiskohtia kuin varmennuskäytännön määrittelevä asiakirja. Varmennuskäytännössä kuvataan tarkemmin käytäntöjä, joita varmentaja toteuttaa varmenteiden myöntämisessä ja muussa hallinnoinnissa. Siinä määritellään, kuinka tietty varmentaja täyttää varmennepolitiikassa määritetyt tekniset sekä organisaatioon ja menettelyihin liittyvät vaatimukset.

HUOMAUTUS: Varmentajan saattaa olla tarkoituksenmukaista laatia vieläkin yksityiskohtaisempia asiakirjoja joissa selostetaan yksityiskohtaiset menettelyt, joilla varmennuskäytännössä mainitut käytännöt toteutetaan. Tällainen yksityiskohtainen ohjeisto katsotaan yleensä sisäiseksi menettelyohjeeksi, jossa voidaan määritellä organisaation sisällä tietyjä tehtäviä ja vastuualueita. Ohjeisto voi olla käytössä varmentajan päivittäistoiminnassa ja sitä saatetaan tarkentaa prosessiarvioinnin yhteydessä. Sisäisiä yksityiskohtaisia asiakirjoja pidetään kuitenkin yksityisinä ja omistusoikeuden alaisina, eivätkä ne näin ollen kuulu tämän asiakirjan soveltamisalaan. Esimerkki: Varmennepolitiikassa edellytetään yksityisten avainten turvallista hallintaa. Varmennuskäytännössä kuvataan vähintään kahdelle henkilölle hajautettua valvontaa ja turvallisia tallennuskäytäntöjä. Menettelyohjeissa tarkennetaan yksityiskohtaiset menettelyt sekä sijainnit, pääsyylistat ja pääsymenettelyt.

4.3.3 Lähestymistapa

Varmennepolitiikka ja varmennuskäytäntö ovat lähestymistavoiltaan hyvin erilaisia. Varmennepolitiikka on määritelty tietyn varmentajan toimintaympäristön yksityiskohdista riippumatta. Varmennuskäytäntö sen sijaan laaditaan nimenomaan varmentajan organisaatorakenteen, toimintatapojen, toimitilojen ja tietoteknisen ympäristön mukaisesti. Varmennepolitiikan määrittelijänä voi olla varmennepalvelujen käyttäjä, mutta varmennuskäytännön määrittelee aina varmentaja.

4.3.4 Muut varmentajan julkiset asiakirjat

Varmennepolitiikan ja varmennuskäytännön lisäksi varmentaja voi julkaista muita varmennetoimintaa ohjaavia asiakirjoja. Tällaiset asiakirjat voivat sisältää monenlaisia kaupallisia ehtoja tai liittyä muun muassa tiettyyn julkisen avaimen järjestelmään. Vaikka tällaisista ehdoista ei välttämättä ilmoiteta asiakkaalle, niitä saatetaan silti soveltaa asiassa.

Varmennekuvaus on varmentajan käyttöehtojen osa, joka liittyy julkisen avaimen järjestelmän toimintaan. Varmentajan olisi syytä asettaa varmennekuvaus sekä tilaajien että varmenteeseen luottavien osapuolien saataville.

4.4 Tilaaja ja allekirjoittaja

Joissakin tapauksissa varmenne myönnetään suoraan yksilöille heidän omaan käyttöönsä. Varmennetta pyytävä osapuoli on kuitenkin usein eri taho kuin allekirjoittaja, jota varmenne koskee. Esimerkiksi yritys saattaa tarvita varmenteita työntekijöitään varten, jotta he voisivat toteuttaa sähköistä kaupankäyntiä yrityksen puolesta. Tällaisissa tilanteissa varmentajalta varmenteita tilaava taho on eri kuin varmenteen allekirjoittaja.

Jotta näitä kahta mahdollista roolia koskevat vaatimukset tulisivat selkeästi esille, tässä asiakirjassa "**tilaajalla**" tarkoitetaan varmentajalta varmenteita sopimuksella tilaavaa tahoja ja "**allekirjoittajalla**" tahoja, jota varmenne koskee. Tilaaja on vastuussa julkiseen avaimen perustuvaan varmenteeseen liittyvän yksityisen avaimen käytöstä. Allekirjoittaja taas on henkilö, joka voidaan todentaa yksityisellä avaimella ja joka hallitsee yksityisen avaimen käyttöä.

Kun varmenteita myönnetään yksilöille heidän omaan käyttöönsä, sama taho voi olla sekä tilaaja että allekirjoittaja. Muissa tapauksissa, kuten silloin kun varmenteita myönnetään työntekijöitä varten, tilaaja ja allekirjoittaja ovat eri tahoja.

Esimerkiksi työnantaja voi olla tilaaja ja työntekijä allekirjoittaja.

Tässä asiakirjassa käytetään näitä kahta käsitettä tämän eron ilmentämiseksi, silloin kun se on tarpeen. Kaikissa tapauksissa kyseinen ero ei kuitenkaan ole aivan selvä.

5 Johdanto laatuvarmennepolitiikkoihin

5.1 Yleistä

Varmennepolitiikalla tarkoitetaan periaatteita, jotka osoittavat tietyn varmenteen soveltuvuuden tietyille yhteisölle ja/tai sovellusluokkaa, jota koskee yhteiset turvallisuusvaatimukset" [3].

Tässä asiakirjassa menettelytapavaatimukset määritellään varmennepolitiikkojen mukaan. Nämä varmennepolitiikat koskevat direktiivin [1] määrittelyjen mukaisia laatuvarmenteita, joten niitä kutsutaan laatuvarmennepolitiikoiksi. Tämän asiakirjan mukaisesti myönnetty varmenteet sisältävät varmennepolitiikan OID-yksilöintitunnuksen, jonka avulla varmenteeseen luottavat osapuolet voivat määrittää varmenteen käyttökelpoisuuden ja luotettavuuden tiettyyn käyttötarkoitukseen. Tässä asiakirjassa määritetään kaksi laatuvarmennepolitiikkaa:

- 1) yleisölle myönnettäviä laatuvarmenteita koskeva laatuvarmennepolitiikka, jossa edellytetään turvallisten allekirjoituksen luomisvälineiden käyttöä

HUOMAUTUS 1: Yleisö-käsitteen tarkka tulkinta määräytyy tilanteeseen sovellettavan kansallisen lainsäädännön mukaan. Varmentaja voidaan katsoa yleisölle varmenteita myöntäväksi, jos kyseisten varmenteiden käyttöä ei ole rajoitettu osanottajien välisin vapaaehtoisin yksityisoikeudellisin sopimuksin.

- 2) yleisölle myönnettäviä laatuvarmenteita koskeva laatuvarmennepolitiikka.

Kohdassa 8 esitetään määrittelypuitteet muille laatuvarmennepolitiikoille,

- a) joilla tehostetaan tai rajoitetaan edellä mainittuja politiikkoja, ja/tai
- b) jotka koskevat "suljetuille ryhmille" eli muille kuin yleisölle myönnettäviä laatuvarmenteita.

HUOMAUTUS 2: Tässä asiakirjassa käytettävät periaatteet on määritelty julkaisussa RFC 3647 [2] ja puitteet on määritelty julkaisussa ANSI X9.79 (katso Lähdekirjallisuus). Tässä asiakirjassa pyritään mahdollisimman suureen yhdenmukaisuuteen edellä mainittujen asiakirjojen periaatteiden ja vaatimusten kanssa.

5.2 Yksilöintitunnukset

Tässä asiakirjassa määriteltyjen laatuvarmennepolitiikkojen OID-yksilöintitunnukset ovat seuraavat:

- a) **QCP public + SSCD.** Yleisölle myönnettäviä laatuvarmenteita koskeva laatuvarmennepolitiikka, joka edellyttää turvallisen allekirjoituksen luomisvälineen käyttöä.

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456)
policy-identifiers(1) qcp-public-with-sscd (1)

- b) **QCP public.** Yleisölle myönnettäviä laatuvarmenteita koskeva laatuvarmennepolitiikka.

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456)
policy-identifiers(1) qcp-public (2)

Sisällyttämällä varmenteeseen jommankumman näistä OID-yksilöintitunnuksista varmentaja ilmaisee noudattavansa kyseistä laatuvarmennepolitiikkaa.

HUOMAUTUS: Julkaisun TS 101 862 [6] kohdassa 5.3 edellytetään, että julkaisun TS 101 862 [6] kohdan 5.2.1 mukainen lause esi4-qStatement-1

- OLISI SISÄLLYTETTÄVÄ laatuvarmennelauseen laajennukseen silloin, kun laatuvarmenne on julkaisun TS 101 862 [6] mukainen ja myönnetty viimeistään 30.6.2005
- ON SISÄLLYTETTÄVÄ laatuvarmennelauseen laajennukseen silloin, kun laatuvarmenne on julkaisun TS 101 862 [6] mukainen ja myönnetty 30.6.2005 jälkeen.

Varmentajan on sisällytettävä noudattamiensa laatuvarmennepolitiikkojen OID-yksilöintitunnukset myös tilaajien ja varmenteeseen luottavien osapuolten saataville asetettaviin käyttöehtoihin ja tällä tavoin ilmaista noudattavansa kyseisiä laatuvarmennepolitiikkoja.

5.3 Käyttäjyhteisö ja sovellettavuus

5.3.1 QCP public + SSCD -laatuvarmennepolitiikka

QCP public + SSCD -laatuvarmennepolitiikka koskee varmenteita,

- a) jotka täyttävät direktiivin [1] liitteessä I säädetyt vaatimukset
- b) jotka myöntävä varmentaja täyttää direktiivin [1] liitteessä II säädetyt vaatimukset
- c) joita saa käyttää vain direktiivin [1] liitteen III vaatimukset täyttävillä turvallisilla allekirjoituksen luomisvälineillä
- d) joita myönnetään yleisölle.

Tämän laatuvarmennepolitiikan mukaisesti myönnettäviä laatuvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka "täyttävät sähköisessä muodossa olevan tiedon osalta allekirjoitukselle asetettavat edellytykset samalla tavoin kuin käsin kirjoitettu allekirjoitus täyttää kyseiset vaatimukset paperilla olevan tiedon osalta", kuten direktiivin 5.1 artiklassa [1] säädetään.

5.3.2 QCP public -laatuvarmennepolitiikka

QCP public -laatuvarmennepolitiikka koskee varmenteita,

- a) jotka täyttävät direktiivin [1] liitteessä I säädetyt vaatimukset
- b) jotka myöntävä varmentaja täyttää direktiivin [1] liitteessä II säädetyt vaatimukset
- c) joita myönnetään yleisölle.

Tämän laatuvarmennepolitiikan mukaisesti myönnettäviä laatuvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, joilta "ei evätä oikeudellista vaikutusta ja hyväksyttävyyttä todisteena oikeudellisissa menettelyissä", kuten direktiivin 5.2 artiklassa säädetään.

5.4 Vaatimustenmukaisuus

5.4.1 Yleistä

Varmentaja saa käyttää jompaakumpaa edellä kohdassa 5.2 mainittua laatuvarmennepolitiikan yksilöintitunnusta vain,

- a) jos varmentaja ilmaisee noudattavansa yksilöityä laatuvarmennepolitiikkaa ja asettaa pyynnöstä tilaajan ja varmenteeseen luottavien osapuolten saataville todisteita vaatimustenmukaisuudesta tai

HUOMAUTUS 1: Todisteena voi olla esimerkiksi auditoijan kertomus, jossa vahvistetaan varmentajan noudattavan yksilöidyn laatuvarmennepolitiikan vaatimuksia. Kyseessä voi olla varmentajan organisaation sisäinen auditoija, mutta auditoija ei saa olla hierarkkisessa suhteessa varmentajan toimintaa toteuttavaan osastoon.

- b) jos pätevä ja riippumaton osapuoli on hiljattain arvioinut yksilöidyn laatuvarmennepolitiikan vaatimusten noudattamisen nykytilaa varmentajalla. Arviointitulokset on asetettava pyynnöstä tilaajien ja varmenteeseen luottavien osapuolten saataville

HUOMAUTUS 2: Arviointi voidaan toteuttaa direktiivin 2 artiklan 13 kohdassa [1] määritellyn "vapaaehtoisuuteen perustuvan akkreditointijärjestelmän" mukaisesti tai se voi olla pätevän ja riippumattoman auditoijan suorittama muunlainen arviointi. Katso vaatimustenmukaisuuden arviointia koskeva CEN-työryhmän sopimus CWA 14172 "EESSI Conformity Assessment Guidance" (katso Lähdekirjallisuus).

- c) jos myöhemmin osoitetaan, että varmentaja on laiminlyönyt varmennepolitiikan noudattamisen ja että tämä vaikuttaa merkittävästi sen kykyyn täyttää direktiivissä [1] määritellyt laatuvarmenteita koskevat vaatimukset, varmentajan on lopetettava kohdan 5.2 mukaisten yksilöintitunnusten sisältävien varmenteiden myöntäminen,

kunnes se on osoittanut vaatimustenmukaisuutensa tai kunnes sen on arvioitu noudattavan kyseisen laatuvarmennepolitiikan vaatimuksia; muussa tapauksessa varmentajan on ryhdyttävä kohtuullisen ajan kuluessa toimenpiteisiin vaatimustenmukaisuutta koskevan laiminlyönnin korjaamiseksi

HUOMAUTUS 3: Vaikka varmentajan tiedettäisiin laiminlyövä ratkaisevalla tavalla varmennepolitiikan noudattamista, varmentaja saa kuitenkin myöntää varmenteita sisäisiin ja testaustarkoituksiin, kunhan kyseisiä varmenteita ei aseteta saataville mitään muuta käyttöä varten.

HUOMAUTUS 4: Vaatimustenmukaisuuden osoittamiseen vaadittavat keinot voivat vaihdella varmentajan sijoittautumisvaltion lainsäädännön mukaan.

- d) varmentajan vaatimustenmukaisuus tarkistetaan säännöllisesti sekä aina, kun varmentajan toimintaa muutetaan merkittävästi.

5.4.2 QCP public + SSCD -laatuvarmennepolitiikka

Vaatimusten mukaisen varmentajan on osoitettava, että

- a) se täyttää sille kohdassa 6.1 määritellyt vaatimukset
- b) se on ottanut käyttöön hallintakeinot, jotka täyttävät kaikki kohdassa 7 esitetyt vaatimukset.

5.4.3 QCP public -laatuvarmennepolitiikka

Vaatimusten mukaisen varmentajan on osoitettava, että

- a) se täyttää sille kohdassa 6.1 määritellyt vaatimukset
- b) se on ottanut käyttöön hallintakeinot, jotka täyttävät kohdassa 7 esitetyt vaatimukset, lukuun ottamatta kohdassa 7.2.9 esitettyjä vaatimuksia sekä kohdan 6.2 alakohdissa e) ja f) määriteltyä tilaajan velvollisuutta.

6 Velvollisuudet ja vastuut ja vastuunrajoitukset

HUOMAUTUS: Tätä kohtaa sovelletaan kumpaankin kohdassa 5 yksilöityyn laatuvarmennepolitiikkaan eli QCP public- ja QCP public + SSCD -laatuvarmennepolitiikkaan, ellei muuta mainita.

6.1 Varmentajan velvollisuudet

Varmentaja varmistaa, että kaikki varmentajalle kohdassa 7 asetetut, valittua laatuvarmennepolitiikkaa koskevat vaatimukset toteutetaan (katso kohdat 5.4.2, 5.4.3 ja 8.4).

Varmentaja on vastuussa kyseisessä laatuvarmennepolitiikassa määrättyjen menettelyjen noudattamisesta, vaikka varmentajan toimintaa toteutettaisiin alihankkijavoimin.

Varmentajan on tarjottava kaikki varmennepalvelut varmennuskäytännössään mainitun mukaisesti.

6.2 Tilaajan velvollisuudet

Varmentaja velvoittaa sopimuksella (katso kohdan 7.3.1 alakohta i) tilaajan noudattamaan kaikkia seuraavassa mainittavia velvollisuuksia. Jos allekirjoittaja ja tilaaja ovat eri tahoja, tilaajan on saatettava allekirjoittajan tietoon kaikki allekirjoittajaan sovellettavat velvollisuudet (seuraavan luettelon mukaisesti):

- a) Varmentajalle on annettava oikeat ja täydelliset tiedot kyseisen laatuvarmennepolitiikan vaatimusten mukaisesti, etenkin rekisteröinnin yhteydessä.
- b) Avainparia saa käyttää vain sähköisiin allekirjoituksiin ja mahdollisten muiden tilaajalle ilmoitettujen rajoitusten mukaisesti (katso kohta 7.3.4).
- c) Tilaajan/allekirjoittajan on toiminnassaan noudatettava erityistä huolellisuutta jotta allekirjoittajan yksityistä avainta ei käytetä luvattomasti.

- d) Jos tilaaja tai allekirjoittaja luo allekirjoittajan avaimet:
- i) allekirjoittajan avaimet on luotava käyttämällä algoritmia, jonka on todettu soveltuvan sähköisiin laatuallkirjoituksiin
 - ii) avainpituutena ja algoritmina on käytettävä yhdistelmää, jonka on todettu soveltuvan sähköisiin laatuallkirjoituksiin varmenteen voimassaolon ajan

HUOMAUTUS 1: Katso algoritmeja ja niiden parametreja koskevia ohjeita julkaisusta TS 102 176-1.

- iii) allekirjoittajan yksityinen avain voidaan pitää yksinomaan allekirjoittajan valvonnassa.
- e) Mikäli varmennepolitiikassa edellytetään turvallisen allekirjoituksen luomisvälineen käyttöä (eli käytössä on QCP public + SSCD -laatuvarmennepolitiikka), varmennetta saa käyttää vain tällaisella välineellä luotujen sähköisten allekirjoitusten yhteydessä.

HUOMAUTUS 2: Edellä oleva kohta EI koske QCP public -laatuvarmennepolitiikkaa.

- f) Jos varmentaja on myöntänyt varmenteen QCP public + SSCD -laatuvarmennepolitiikan mukaisesti ja allekirjoittajan avaimet luodaan tilaajan tai allekirjoittajan valvonnassa, allekirjoittajan avaimet on luotava allekirjoittamiseen käytettävällä turvallisella allekirjoituksen luomisvälineellä.

HUOMAUTUS 3: Edellä oleva kohta EI koske QCP public -laatuvarmennepolitiikkaa.

Varmentajalle on ilmoitettava ilman aiheutonta viivytystä, mikäli ennen varmenteessa ilmoitetun voimassaolon päättymistä tapahtuu jokin seuraavista:

allekirjoittajan yksityinen avain on kadonnut tai sen käyttö on mahdotonta (esimerkiksi siksi, että avaimen käyttöön tarvittava PIN-koodi on unohtunut), yksityinen avain on varastettu, se on mahdollisesti joutunut väärin käsiin tai

allekirjoittajan yksityisen avaimen käyttö ei ole enää hallittavissa, koska aktivointitiedot (esimerkiksi PIN-koodi) ovat joutuneet väärin käsiin tai muista syistä, ja/tai

- iii) varmenteen sisältö on tilaajalle tai allekirjoittajalle ilmoitettuun nähden virheellinen tai sitä on muutettu.
- h) Jos allekirjoittajan yksityinen avain on joutunut väärin käsiin, se peruutetaan välittömästi ja lopullisesti.

Jos tietoon tulee, että allekirjoittajan varmenteen myöntäneen varmentajan toiminta on vaarantunut, on varmistettava, että allekirjoittaja ei käytä varmennetta.

6.3 Tiedottaminen varmenteeseen luottaville osapuolille

Varmenteeseen luottavien osapuolten saataville asetetuissa ehdoissa ja vaatimuksissa (katso kohta 7.3.4) on ilmoitettava, että varmenteeseen luottaminen perustellulla tavalla edellyttää, että osapuoli

- a) todentaa varmenteeseen luottavalle osapuolelle osoitetun ajantasaisen sulkutilatiedon (katso kohta 7.3.4) avulla, onko varmenne voimassa tai onko se asetettu keskeytystilaan tai peruutettu

HUOMAUTUS 1: Varmentajan käytännöistä ja varmenteiden tilatietojen jakelutavasta riippuen varmenteiden tilatietojen jakelussa voi esiintyä viivettä, joka on enintään 1 päivä.

- b) ottaa huomioon mahdolliset varmenteen käytön rajoitukset, jotka tiedotetaan varmenteeseen luottavalle osapuolelle varmenteessa tai kohdan 7.3.4 mukaisesti toimitetuissa ehdoissa
- c) noudattaa sopimuksissa tai muualla määrättyjä ehtoja

HUOMAUTUS 2: Direktiivin 6 artiklassa säädettyä, yleisölle laatuvarmenteita myöntävän varmentajan vastuuta sovelletaan osapuoliin, jotka "luottavat varmenteeseen.

6.4 Vastuu

Yleisölle laatuvarmenteita myöntäviä varmentajia koskee direktiivin 6 artiklassa [1] säädetyn mukainen vastuu (katso vastuuta koskevia lisätietoja liitteestä A).

7 Varmentajan toimintaa koskevat vaatimukset

HUOMAUTUS 1: Tätä kohtaa sovelletaan kumpaankin kohdassa 5 yksilöityyn laatuvarmennepolitiikkaan eli QCP public- ja QCP public + SSCD -laatuvarmennepolitiikkaan, ellei muuta mainita.

Varmentajan on toteutettava seuraavat vaatimukset täyttävät hallintakeinot.

HUOMAUTUS 2: Kunkin kohdan jälkeen annetaan viite siihen direktiivin artiklaan, johon vaatimus perustuu.

Tämä asiakirja koskee laatuvarmenteita tarjoavia varmentajia. Tähän sisältyy rekisteröintipalvelujen tarjoaminen, varmenteiden luominen, varmenteiden jakelu, sulkupalvelu ja varmenteen tilatietopalvelu (katso kohta 4.2). Jos vaatimus liittyy varmentajan tiettyyn palvelualueeseen, se esitetään vastaavien alaotsikoiden alla. Mikäli seuraavassa ei yksilöidä yhtään palvelualueetta tai jos mainitaan "varmentaja yleisesti", vaatimus koskee varmentajan yleistä toimintaa.

Näiden menettelytapavaatimusten tarkoituksena ei ole rajoittaa varmentajan palveluista veloittamista.

Esitettävät vaatimukset koskevat turvallisuustavoitteita sekä niiden saavuttamiseen käytettäviä hallintakeinoja, joiden osalta esitetään yksityiskohtaisia vaatimuksia, mikäli se on katsottu tavoitteiden täyttymisen kannalta tarpeelliseksi. Kunkin hallintatavoitteen jälkeen annetaan viite direktiivissä [1] asiasta esitettyyn vaatimukseen.

HUOMAUTUS 3: Kun tavoitteen saavuttamista varten edellytetään yksityiskohtia noudattavia hallintakeinoja, on kyseessä kompromissi, jolla halutaan toisaalta saavuttaa vaadittava luottamustaso mutta toisaalta halutaan rajoittaa laatuvarmenteiden myöntämistekniikkaa mahdollisimman vähän. Kohdassa 7.4 (Varmentajan johtamis- ja toimintakäytännöt) viitataan muihin yleisluontoisiin standardeihin, joita voidaan käyttää yksityiskohtaisten hallintavaatimusten lähteenä. Näiden seikkojen vuoksi tiettyyn aihealueeseen liittyvien vaatimusten tarkkuusaste voi vaihdella.

7.1 Varmennuskäytäntö

Varmentajan on varmistettava, että se osoittaa varmennepalvelujen tarjoamisen edellyttämän luotettavuuden (katso direktiivin [1] liitteen II kohta (a)).

Erityisesti:

- a) Varmentajan on laadittava julkilausuma käytännöistä ja menettelyistä, joita käytetään laatuvarmennepolitiikassa yksilöityjen vaatimusten täyttämiseksi.

HUOMAUTUS 1: Tässä varmennepolitiikassa ei aseteta varmennuskäytännön rakenteelle mitään vaatimuksia.

- b) Varmentajan varmennuskäytännössä on yksilöitävä varmentajan palvelujen tukena käytettävien kaikkien ulkoisten organisaatioiden velvollisuudet, myös sovellettavat toimintapolitiikat ja -käytännöt.
- c) Varmentajan on asetettava tilaajien ja varmenteeseen luottavien osapuolten saataville varmennuskäytäntö sekä muu asiaan liittyvä dokumentaatio, jota laatuvarmennepolitiikan vaatimustenmukaisuuden arviointi edellyttää.

HUOMAUTUS 2: Varmentajaa ei yleisesti ottaen vaadita julkaisemaan toimintansa kaikkia yksityiskohtia.

- d) Varmentajan on annettava tiedoksi kaikille tilaajille ja mahdollisille varmenteeseen luottaville osapuolille varmenteen käyttöä koskevat ehdot kohdan 7.3.4 mukaisesti.
- e) Varmentajalla on oltava päättävä taho jolla on varmennuskäytännön hyväksymisessä lopullinen toimivalta ja vastuu.
- f) Varmentajan ylemmän johdon vastuulla on varmistaa, että tässä asiakirjassa määriteltyjen sovellettavien vaatimusten saavuttamiseksi laadittuja varmennuskäytäntöjä toteutetaan asianmukaisesti.
- g) Varmentajan on määriteltävä varmennuskäytäntöjen tarkistusprosessi, joka sisältää varmennuskäytännön ylläpitovastuut.
- h) Varmentajan on annettava asianmukaisesti ilmoitus muutoksista, joita se aikoo tehdä varmennuskäytäntönsä, ja sen on edellä olevan kohdan e mukaisen hyväksynnän mukaisesti asetettava tarkistettu varmennuskäytäntö saataville edellä olevan kohdan c mukaisesti.

- i) Varmentajan on dokumentoitava allekirjoittamisessa käytettävät algoritmit ja parametrit.

7.2 Julkisen avaimen järjestelmässä käytettävien avainten elinkaaren hallinta

7.2.1 Varmentajan avaimen luominen

Varmenteiden luominen

Varmentajan on varmistettava, että varmentajan avaimet luodaan hallituissa olosuhteissa (katso direktiivin [1] liitteen II kohta g ja liitteen II kohta f.

Erityisesti:

- a) Varmentajan avaimet on luotava fyysisesti turvallisessa ympäristössä (katso kohta 7.4.4) ja luomisen toteuttaa luotetuissa rooleissa toimiva henkilöstö (katso kohta 7.4.3) vähintään kahdelle eri henkilölle hajautetussa valvonnassa. Tähän tehtävään valtuutetun henkilöstön määrä on pidettävä mahdollisimman pienenä ja varmentajan käytäntöjen mukaisena.
- b) Varmentajan avaimet on luotava välineellä, joka
- täyttää julkaisussa FIPS 140-2 [5] yksilöidyt vaatimukset vähintään tasolla 3 tai
 - täyttää jossakin seuraavista CEN-työryhmän sopimuksista (CWA) yksilöidyt vaatimukset: CEN Workshop Agreement 14167-2 [9], CWA 14167-3 [10] tai CWA 14167-4 [11], tai
 - on luotettava järjestelmä, jonka arvioinnin vakuuttavuustasoksi on luokiteltu ISO/IEC 15408 -standardin [7] mukaisesti vähintään EAL 4 tai joka täyttää vastaavat turvallisuusehdot. Järjestelmän oman turvatavoitteen tai suojaprofiilin on oltava tämän asiakirjan vaatimusten mukainen, perustuttava riskianalysiin ja sisällettävä sekä fyysiset että muut kuin tekniset turvatoimet.

HUOMAUTUS 1: Kohdan 7.2.2 alakohtien b–e sääntöjä sovelletaan avainten luomiseen myös silloin, kun se toteutetaan erillisessä järjestelmässä.

- c) Varmentajan avainten luomisessa on käytettävä algoritmia, jonka on todettu soveltuvan laatuvarmenteisiin.
- d) Varmentajan allekirjoitusavaimen avainpituuden ja algoritmin yhdistelmäksi on valittava yhdistelmä, jonka on todettu soveltuvan sellaisiin laatuvarmenteisiin, joita varmentaja myöntää.

HUOMAUTUS 2: Katso algoritmeja ja niiden parametreja koskevia ohjeita julkaisusta TS 102 176-1.

- e) Varmentajan on tarkoituksenmukaisen ajan ennen varmentajan allekirjoitusavaimen voimassaolon päättymistä (esimerkiksi varmentajan varmenteessa ilmoitettuna ajankohtana) luotava uusi avainpari varmenteen allekirjoittamiseen ja tehtävä kaikki tarpeelliset toimet, ettei kyseiseen varmentajan avaimen mahdollisesti luottavien yhteisöjen toimintaan aiheutuisi häiriöitä. Uusi varmentajan avain on luotava ja sen jakelu on toteutettava näiden menettelytapojen mukaisesti.

HUOMAUTUS 3: Nämä toimet olisi tehtävä riittävän ajoissa, jotta kaikki varmentajaan jossakin suhteessa toimivat osapuolet (allekirjoittajat, tilaajat, varmenteeseen luottavat osapuolet, ylemmällä tasolla toimivat varmentajat) saavat ajoissa tiedon varmentajan avainparin vaihtamisesta ja jotta ne voivat toteuttaa hankaluuksien ja toimintahäiriöiden välttämiseksi tarvittavat toimet. Tämä ei koske varmentajaa, joka lopettaa toimintansa ennen sen oman varmentajan varmenteen viimeistä voimassaolopäivää.

7.2.2 Varmentajan avaimen tallennus, varmuuskopiointi ja palauttaminen

Varmenteiden luominen

Varmentajan on varmistettava, että varmentajan yksityisten avainten luottamuksellisuus ja eheys säilyvät (katso direktiivin [1] liitteen II kohta g ja liitteen II kohta f.

Erityisesti:

- a) varmentajan yksityistä allekirjoitusavainta on säilytettävä ja käytettävä turvallisella salausvälineellä, joka

- täyttää julkaisussa FIPS 140-2 [5] yksilöidyt vaatimukset vähintään tasolla 3 tai
 - täyttää jossakin seuraavista CEN-työryhmän sopimuksista (CWA) yksilöidyt vaatimukset: CEN Workshop Agreement 14167-2 [9], CWA 14167-3 [10] tai CWA 14167-4 [11], tai
 - on luotettava järjestelmä, jonka arvioinnin vakuuttavuustasoksi on luokiteltu ISO/IEC 15408 -standardin [7] mukaisesti vähintään EAL 4 tai joka täyttää vastaavat turvallisuusehdot. Järjestelmän oman turvatavoitteen tai suojaprofiilin on oltava tämän asiakirjan vaatimusten mukainen, perustuttava riskianalyysiin ja sisällettävä sekä fyysiset että muut kuin tekniset turvatoimet.
- b) Turvallisen salausvälineen ulkopuolella (katso edellä oleva kohta a) varmentajan yksityinen allekirjoitusavain on suojattava turvallisen salausvälineen suojaustasoa vastaavasti.
- c) Varmentajan yksityisen allekirjoitusavaimen varmuuskopioinnin, tallentamisen ja palauttamisen saa tehdä ainoastaan luotetuissa rooleissa toimiva henkilöstö, joka käyttää vähintään kahdelle eri henkilölle hajautettua valvontaa. Nämä toimet on tehtävä fyysisesti turvallisessa ympäristössä. (Katso kohta 7.4.4). Tähän tehtävään valtuutetun henkilöstön määrä on pidettävä mahdollisimman pienenä ja varmentajan käytäntöjen mukaisena.
- d) Varmentajan yksityisten allekirjoitusavainten varmuuskopioiden osalta on käytettävä samoja tai tiukempia turvallisuuden hallintakeinoja kuin nykykäytössä olevien avainten osalta.
- e) Kun avaimet tallennetaan avainten käsittelyyn varattuun laitteistoyksikköön, on varmistettava pääsynvalvontakeinoilla, ettei avaimiin ole pääsyä laitteistoyksikön ulkopuolelta.

7.2.3 Varmentajan julkisen avaimen jakelu

Varmenteiden luominen ja jakelu

Varmentajan on varmistettava, että allekirjoituksen todentamiseen käytettävän varmentajan (julkisen) avaimen sekä siihen liittyvien parametrien eheys ja aitous säilyvät varmenteeseen luottaville osapuolille jakelun aikana (katso direktiivin [1] liitteen II kohdat g ja f).

Erityisesti:

- a) Allekirjoitusten todentamiseen käytettävät varmentajan (julkiset) avaimet on asetettava varmenteeseen luottavien osapuolten saataville siten, että varmistetaan varmentajan julkisen avaimen eheys ja todennetaan avaimen aitous.

HUOMAUTUS: Esimerkki: Varmentajan julkisia avaimia voidaan jakaa varmentajan itse allekirjoittamissa varmenteissa, kun mukana on vakuutus siitä, että avain todentaa varmentajan, tai niitä voidaan jakaa toisen varmentajan myöntämissä varmenteissa. Itse allekirjoitetusta varmenteesta ei voida tietää, tuleeko se varmentajalta. Tällöin kyseisen varmenteen oikeellisuuden varmistamiseen tarvitaan lisätoimia, kuten varmenteen sormenjäljen vertaamista luotettavasta lähteestä toimitettuun tietoon.

7.2.4 Vara-avainjärjestelmä

Allekirjoittajan yksityisiä allekirjoitusavaimia ei saa säilyttää salauksen purun ja varmuuskopioinnin mahdollistavalla tavalla, jolloin valtuutetut tahot voisivat tietyissä tilanteissa purkaa salauksen hyödyntämällä yhden tai useamman osapuolen antamia tietoja (yleisesti tätä kutsutaan vara-avainjärjestelmäksi) (katso direktiivin [1] liitteen II kohta j).

7.2.5 Varmentajan avaimen käyttö

Varmentajan on varmistettava, ettei varmentajan yksityisiä allekirjoitusavaimia käytetä epäasiallisesti. Erityisesti:

Varmenteiden luominen

- a) Varmenteiden luomiseen käytettäviä, kohdassa 7.3.3 mainitun mukaisia varmentajan allekirjoitusavaimia voi käyttää myös muuntotyyppisten varmenteiden ja sulkutilatietojen allekirjoittamiseen, kunhan noudatetaan kohtien 7.2.1–7.2.3, 7.2.5–7.2.7 ja 7.4 mukaisia varmentajan toimintaympäristöä koskevia toimintavaatimuksia.
- b) Varmenteen allekirjoitusavaimia saa käyttää vain fyysisesti turvallisissa tiloissa.

7.2.6 Varmentajan avaimen elinkaaren päätyminen

Varmentajan on varmistettava, ettei varmentajan yksityisiä allekirjoitusavaimia käytetä niiden elinkaaren päättymisen jälkeen (katso direktiivin [1] liitteen II kohdat g ja f).

Erityisesti:

Varmenteiden luominen

- a) Kaikki varmentajan yksityisten allekirjoitusavainten kopiot on tuhottava tai tehtävä käyttökelvottomiksi.

7.2.7 Varmenteiden allekirjoittamisessa käytettävän salauslaitteiston elinkaaren hallinta

Varmentajan on varmistettava salauslaitteiston turvallisuus koko sen elinkaaren ajan (katso direktiivin [1] liitteen II kohta f).

Varmenteiden luominen

Erityisesti varmentajan on varmistettava, että

- a) varmenteita ja sulkuilatietoja allekirjoittavaan salauslaitteistoon ei päästä kajoamaan kuljetuksen aikana
- b) varmenteita ja sulkuilatietoja allekirjoittavaan salauslaitteistoon ei päästä kajoamaan säilytyksen aikana
- c) varmentajan allekirjoitusavainten asennus, aktivointi, varmuuskopiointi ja palauttaminen salauslaitteistossa edellyttävät aina vähintään kahden luotetun työntekijän yhtäaikaista valvontaa
- d) varmenteita ja sulkuilatietoja allekirjoittava salauslaitteisto toimii asianmukaisesti
- e) varmentajan salauslaitteistoon tallennetut varmentajan yksityiset allekirjoitusavaimet tuhoetaan, kun väline poistetaan käytöstä.

7.2.8 Varmentajan tarjoamat allekirjoittajan avaimen hallintapalvelut

Varmentajan on varmistettava, että kaikki sen luomat allekirjoittajan avaimet luodaan turvallisesti ja että allekirjoittajan yksityisen avaimen luottamuksellisuus on turvattu (katso direktiivin [1] liitteen II kohdat f ja j).

Varmenteiden luominen

Jos varmentaja luo allekirjoittajan avaimet,

varmentajan luomat allekirjoittajan avaimet on luotava käyttämällä sellaista algoritmia, jonka on todettu soveltuvan sähköisiin laatuallekirjoituksiin varmenteen voimassaolon ajan
varmentajan luomien allekirjoittajan avainten avainpituuden sekä avainten yhteydessä käytettävän julkisen avaimen algoritmin on oltava todetusti sähköisiin laatuallekirjoituksiin soveltuvia varmenteen voimassaolon ajan

HUOMAUTUS 1: Katso algoritmeja ja niiden parametreja koskevia ohjeita julkaisusta TS 102 176-1.

HUOMAUTUS 2: Yhdysvaltalaisen varmentajan Federal Bridgen kanssa toimimisen osalta tämän asiakirjan julkaisuhetkellä sovellettavassa Yhdysvaltain hallituksen politiikassa edellytetään, että RSA-avainten pituuksien on allekirjoitusavaimissa oltava vähintään 1 024 bittiä. Lisäksi Yhdysvaltain hallitus edellyttää hash-algoritmien yhteydessä käytettyjen RSA-avaimien pituudeksi vähintään 2 048 bittiä (lähde NIST SP 800-78).

- c) varmentajan luomat allekirjoittajan avaimet on luotava ja tallennettava turvallisesti ennen kuin ne toimitetaan allekirjoittajalle
- d) allekirjoittajan yksityinen avain on toimitettava allekirjoittajalle tarvittaessa tilaajan kautta siten, että avaimen luottamuksellisuus ja eheys eivät vaarannu ja jotta allekirjoittajalle toimittamisen jälkeen yksityinen avain voi säilyä allekirjoittajan yksinomaisessa hallinnassa
- e) allekirjoittajalle toimittamisen jälkeen kaikki varmentajan hallussa mahdollisesti olevat allekirjoittajan yksityisen avaimen kopiot on tuhottava.

7.2.9 Turvallisen allekirjoituksen luomisvälineen valmistaminen

HUOMAUTUS 1: Tätä kohtaa ei sovelleta QCP public -laatuvarmennepolitiikkaan.

Jos varmentaja myöntää turvallisia allekirjoituksen luomisvälineitä (SSCD), varmentajan on varmistettava sen turvallinen toteuttaminen (katso direktiivin [1] liite III).

Välineen tarjoaminen allekirjoittajalle

Erityisesti jos varmentaja myöntää turvallisen allekirjoituksen luomisvälineen,

- palveluntarjoajan on valvottava turvallisesti kyseisen turvallisen allekirjoituksen luomisvälineen valmistamista
- turvallinen allekirjoituksen luomisväline on tallennettava ja jaeltava turvallisesti
- turvallisen allekirjoituksen luomisvälineen käytöstä poistamista ja uudelleen käyttöön ottamista on valvottava turvallisesti
- jos turvalliseen allekirjoitusvälineeseen liittyy käyttäjän aktivointitietoja (esimerkiksi PIN-koodi), aktivointitiedot on laadittava turvallisesti ja jaeltava turvallisesta allekirjoituksen luomisvälineestä erillisenä.

HUOMAUTUS 2: Erillisyyks voidaan saada aikaan varmistamalla, että aktivointitietojen jakelu ja turvallisen allekirjoituksen luomisvälineen toimittaminen tapahtuvat eri aikoina tai eri reittejä.

HUOMAUTUS 3: Turvallisen allekirjoituksen luomisvälineen valmistamista koskevat edellä luetellut vaatimukset voidaan täyttää esimerkiksi käyttämällä soveltuvaa suojausprofiilia, joka on määritelty ISO/IEC 15408 -standardin [7] mukaisesti tai vastaavasti.

7.3 Julkisen avaimen järjestelmässä käytettävien varmenteiden elinkaaren hallinta

7.3.1 Allekirjoittajan rekisteröinti

Varmentajan on varmistettava, että allekirjoittajat tunnistetaan ja todennetaan asianmukaisesti ja että allekirjoittajan varmennepyynnöt ovat virheettömiä, paikkansapitäviä ja asianmukaisesti valtuutettuja (katso direktiivin [1] liitteen II kohta d).

Erityisesti:

Rekisteröinti

HUOMAUTUS 1: Rekisteröinnissä allekirjoittaja tunnistetaan henkilöksi, johon liittyy tiettyjä attribuutteja. Attribuutit ovat erityismääreitä, jotka voivat ilmaista esimerkiksi henkilöön liittyvän organisaation tai roolin.

- Ennen kuin varmentaja muodostaa sopimussuhteeseen tilaajan kanssa, varmentajan on ilmoitettava tilaajalle varmenteen käytön ehtoista kohdan 7.3.4 mukaisesti (katso direktiivin [1] liitteen II kohta k).
- Varmentajan on ilmoitettava nämä tiedot siten, että niiden eheys säilyy ja selvästi ymmärrettävällä kielellä. Tiedot voidaan välittää sähköisesti.

HUOMAUTUS 2: Tässä viestinnässä voidaan käyttää pohjana liitteessä B annettavaa varmennekuvausten mallia.

- Palveluntarjoajan on rekisteröinnin yhteydessä todennettava tarkoituksenmukaisin keinoin kansallisen lainsäädännön mukaisesti sen henkilön henkilöllisyys, ja tarvittaessa tietyt attribuutit, jolle laatuvarmenne myönnetään. Henkilöllisyys on tarkistettava vertaamalla suoraan fyysiseen henkilöön tai on turvauduttava välillisesti tehtyyn tarkistukseen, jonka tarkistuskeinoilla henkilöllisyys on voitu varmistaa vastaavasti kuin fyysisen läsnäolon perusteella (katso huomautus 3). Henkilöllisyyttä osoittavat asiakirjat voidaan toimittaa paperisina tai sähköisinä asiakirjoina.

HUOMAUTUS 3: Fyysiseen henkilöön välillisesti vertaamalla saatuja henkilöllisyyttä osoittavia asiakirjoja voivat olla esimerkiksi rekisteröinnissä esitettävät asiakirjat, jotka on saatu jonkin fyysisestä läsnäolosta edellyttävän hakemuksen tuloksena.

HUOMAUTUS 4: Attribuuttivarmenteet eivät kuulu tämän asiakirjan soveltamisalan piiriin, koska ne eivät sisällä julkisia allekirjoitusavaimia.

- d) Jos allekirjoittaja on henkilö, henkilötietoina on esitettävä
- koko nimi (sukunimi ja etunimet sovellettavan lainsäädännön ja kansallisten tunnustuskäytäntöjen mukaisesti)
 - syntymäaika ja -paikka, kansallinen henkilötunnus, tai muita attribuutteja, joilla voidaan mahdollisimman pitkälle erottaa henkilö muista samannimisistä henkilöistä.

HUOMAUTUS 5: Syntymäpaikka on suositeltavaa antaa kansallisesti käytettävien syntymäpaikkojen rekisteröintikäytäntöjen mukaisesti.

HUOMAUTUS 6: Varmentaja on vastuussa siitä, että "kaikki varmenteen sisältämät tiedot" ovat paikkansapitäviä (katso liite A).

- e) Jos allekirjoittaja on henkilö, joka tunnustetaan oikeushenkilön tai muun organisaatioyksikön yhteydessä, selvitys esitettävä seuraavista:

- allekirjoittajan koko nimi (sukunimi ja etunimet)
- allekirjoittajan syntymäaika ja -paikka, kansallisesti tunnustettu henkilötunnus, tai muita attribuutteja, joilla voidaan mahdollisimman pitkälle erottaa henkilö muista samannimisistä henkilöistä
- asiaan liittyvän oikeushenkilön tai muun organisaatioyksikön koko nimi ja oikeusasema
- asiaan liittyvää oikeushenkilöä tai muuta organisaatioyksikköä koskevat olennaiset nykyiset rekisteröintitiedot (esimerkiksi yrityksen rekisteröinti)
- selvitys siitä, että allekirjoittaja liittyy oikeushenkilöön tai muuhun organisaatioyksikköön.

- f) Varmentajan on säilytettävä kaikki allekirjoittajan henkilöllisyyden todentamisessa käytetyt tiedot ja mahdollisesti asiaa koskevat tietyt attribuutit, kuten todentamisessa käytettyjen asiakirjojen viitenumerot, sekä niiden mahdolliset voimassaolorajoitukset.

Jos muu taho kuin allekirjoittaja tilaa varmentajan palvelut (eli tilaaja ja allekirjoittaja ovat eri osapuolia – katso kohta 4.4), on esitettävä todisteet siitä, että tilaaja on valtuutettu toimimaan allekirjoittajan puolesta määritellyn mukaisesti (esimerkiksi valtuutettu toimimaan kaikkien yksilöidyn organisaation jäsenten puolesta).

- h) Tilaajan on esitettävä käyntiosoite tai muita attribuutteja, joilla kuvataan, miten tilaajaan saa yhteyden.
- i) Varmentajan on säilytettävä tilaajan kanssa allekirjoitettu sopimus, joka sisältää
- tilaajan velvollisuuksien hyväksymisen (katso kohta 6.2)
 - varmentajan niin edellyttäessä suostumuksen turvallisen allekirjoituksen luomisvälineen käyttämiseen

HUOMAUTUS 7: Edellä olevaa kohtaa ei sovelleta QCP Public -laatuvarmennepolitiikkaan.

- suostumuksen siihen, että varmentaja säilyttää tiedot, joita on käytetty rekisteröinnissä (katso kohdan 7.4.11 alakohdat h, i ja j), välineen toimittamisessa allekirjoittajalle (katso kohdan 7.4.11 alakohdat m ja n), varmenteen mahdollisessa myöhemmässä peruuttamisessa (katso kohdan 7.4.11 alakohta o) sekä varmenteeseen sisältyvät tiedot henkilön henkilöllisyydestä ja häneen liittyvistä tietyistä attribuuteista, ja että kyseiset tiedot saa välittää kolmansille osapuolille kyseessä olevan varmennepolitiikan mukaisin ehdoin, mikäli varmentaja lopettaa palvelunsa
- tiedon siitä, edellyttääkö tilaaja varmenteen julkaisemista ja millaisin ehdoin, sekä suostuuko allekirjoittaja siihen
- vakuutuksen siitä, että varmenteen sisältämät tiedot ovat virheettömät.

HUOMAUTUS 8: Tilaaja ja allekirjoittaja voivat hyväksyä tämän sopimuksen eri kohtia rekisteröinnin eri vaiheiden aikana. Esimerkiksi sen hyväksyntä, ovatko varmenteen sisältämät tiedot virheettömät, voidaan antaa muiden hyväksyntää edellyttävien kohtien jälkeen.

HUOMAUTUS 9: Tämän sopimuksen muodostamiseen voi osallistua muita osapuolia (esimerkiksi asiaan

liittyvä oikeushenkilö). HUOMAUTUS 10: Tämä sopimus voi olla sähköisessä muodossa.

Edellä yksilöidyt tiedot on säilytettävä tilaajalle ilmoitettua vastaavan ajan (katso edellä olevat kohdat a ja b) sekä varmennuksesta oikeudellisissa menettelyissä edellytettävien todisteiden esittämistä varten sovellettavan lainsäädännön mukaisesti.

HUOMAUTUS 11: Kun määritellään "sovellettavaa lainsäädäntöä", on otettava huomioon seuraavat seikat:

- i) Varmentajan sijoittautumisvaltion lainsäädäntö on aina otettava huomioon.
 - ii) Jos allekirjoittajat ovat rekisteröityneet muussa kuin varmentajan sijoittautumisvaltiossa sijaitsevan rekisteröijän kautta, kyseisen rekisteröijän on noudatettava myös oman valtionsa säädöksiä ja määräyksiä.
 - iii) Jos lisäksi jotkin tilaajat sijaitsevat toisessa valtiossa, on otettava huomioon myös tällaisia tilaajia koskevat sopimuksiin ja lainsäädäntöön perustuvat vaatimukset.
- k) Jos varmentaja ei luo allekirjoittajan avainparia, varmennepyyntöprosessissa on varmistettava, että allekirjoittajan hallussa on varmentamisen yhteydessä esitettävään julkiseen avaimen liittyvä yksityinen avain.
- l) Jos varmentaja ei luo allekirjoittajan avainparia ja varmennepolitiikka edellyttää turvallisen allekirjoituksen luomisvälineen käyttöä,
(QCP public + SSCD -laatuvarmennepolitiikka), varmennepyyntöprosessissa on varmistettava, että varmennettava julkinen avain on peräisin avainparista, joka on tosiasiallisesti luotu turvallisella allekirjoituksen luomisvälineellä.

7.3.2 Varmenteen uusiminen, sen avainparin vaihtaminen ja varmenteen päivittäminen

Varmentajan on varmistettava, että jo aikaisemmin rekisteröityneelle allekirjoittajalle myönnettäviä varmenteita koskevat pyynnöt ovat täydelliset, paikkansapitävät ja asianmukaisesti valtuutetut. Näihin sisältyvät varmenteen uusiminen, peruuttamisen jälkeen tai ennen voimassaolon päättymistä tehtävä avainparin vaihtaminen, sekä allekirjoittajan attribuuttien muuttumisesta johtuva päivittäminen (katso direktiivin [1] liitteen II kohta g).

HUOMAUTUS: Mikäli varmentaja tarjoaa varmenteen uusimispalvelua, tilaaja voi pyytää uusimista esimerkiksi silloin, jos varmenne varten varmentajalle esitetyt oleelliset attribuutit ovat muuttuneet tai jos varmenteen käyttöaika on päättymässä.

Erityisesti:

Rekisteröinti

- a) Varmentajan on tarkistettava uusittavan varmenteen olemassaolo ja voimassaolo ja että allekirjoittajan henkilöllisyyden ja häneen liittyvien attribuuttien todentamisessa käytetty tieto on edelleen voimassa.
- b) Mikäli varmentajan käyttöehtoihin on tehty muutoksia, niistä on ilmoitettava tilaajalle ja sovittava kohdan 7.3.1 alakohtien a, b ja i mukaisesti.
- c) Mikäli varmennettuja nimiä tai attribuutteja on muutettu tai mikäli aiempi varmenne on peruutettu, rekisteröintitiedot on todennettava ja tallennettava ja tilaajan on hyväksyttävä ne kohdan 7.3.1 alakohtien c–g mukaisesti.
- d) Varmentaja myöntää uuden varmenteen käyttämällä allekirjoittajan aiempaa varmennettua julkista avainta vain, jos sen salausturvallisuus on uuden varmenteen voimassaolon ajan edelleen riittävä ja jos merkkejä ei ole allekirjoittajan yksityisen avaimen joutumisesta väärin käsiin.

7.3.3 Varmenteiden luominen

Varmentaja varmistaa, että se myöntää varmenteita turvallisesti niiden aitouden säilyttämiseksi (katso direktiivin [1] liitteen II kohta g). Erityisesti:

Varmenteiden luominen

- a) Varmenteet on luotava ja myönnettävä direktiivin [1] liitteen I mukaisesti. Laatuvarmenteessa on oltava
 - osoitus siitä, että varmenne on myönnetty laatuvarmenteena
 - tiedot varmentajasta [varmennepalvelujen tarjoajasta] ja valtiosta, johon se on sijoittautunut
 - allekirjoittajan nimi tai salanimi, jonka osalta on mainittava kyseessä olevan salanimi

- mahdollisuus lisätä allekirjoittajaan liittyvä asiaankuuluva attribuutti, riippuen varmenteen aiotusta käyttötarkoituksesta
- allekirjoituksen todentamiseen käytettävät tiedot, jotka vastaavat allekirjoittajan valvonnassa olevia allekirjoituksen luomiseen käytettäviä tietoja;
- tieto varmenteen voimassaoloajan alkamis- ja päättymisajankohdasta
- varmenteen tunnusnumero
- varmenteen myöntävän varmennepalvelujen tarjoajan kehittynyt sähköinen allekirjoitus
- mahdolliset varmenteen käyttörajoitukset, ja
- mahdolliset arvomääräiset rajoitukset toimille, joihin varmennetta voidaan käyttää.

HUOMAUTUS 1: Julkaisussa TS 101 862 [6] määritellään vakiomuotoinen laatuvarmenteiden malli, joka täyttää direktiivin [1] liitteen I vaatimukset.

- b) Varmentajan on toteutettava toimenpiteet varmenteiden väärentämisen ehkäisemiseksi ja, silloin kun varmentaja luo allekirjoituksen luomiseen käytettävät tiedot, taattava luottamuksellisuus kyseisiä tietoja luotaessa (katso direktiivin [1] liitteen II kohta g)
- c) Varmenteen myöntämismenettely on liityttävä turvallisesti siihen liittyvään rekisteröintiin, varmenteen uusimiseen tai varmenteen avainparin vaihtamiseen, mukaan luettuna mahdollinen allekirjoittajan luoman julkisen avaimen tarjoaminen.
- d) Jos varmentaja luo allekirjoittajan avaimen,
 - varmenteen myöntämismenettely on liityttävä turvallisesti varmentajan suorittamaan avainparin luomiseen
 - yksityinen avain (tai turvallinen allekirjoituksen luomisväline, katso kohta 7.2.9) on välitettävä rekisteröidylle allekirjoittajalle turvallisesti.
- e) Varmentajan on varmistettava, että allekirjoittajalle osoitettu yksilöivä nimi säilyy ajan kuluessa ainutlaatuisena varmentajan toimialueella. (Toisin sanoen myönnettyssä varmenteessa käytettyä yksilöityä nimeä ei saa koskaan varmentajan elinkaaren aikana antaa toiselle yhteisölle.)
- f) Rekisteröintitietojen luottamuksellisuus ja eheys on suojattava erityisesti, kun tietoja vaihdetaan tilaajan, allekirjoittajan tai varmentajan järjestelmän hajautettujen osien välillä.

HUOMAUTUS 2: Katso myös tietosuojavaatimuksia koskeva kohta 7.4.10.

- g) Varmentajan on todennettava, että rekisteröintitietoja vaihdetaan sellaisten tunnustettujen rekisteröintipalvelujen tarjoajien kanssa, joiden henkilöllisyys on todennettu, mikäli käytetään ulkoisia rekisteröintipalvelujen tarjoajia.

7.3.4 Varmentajan toimintaan liittyvien asiakirjojen jakelu

Varmentajan on varmistettava, että ehdot ja ohjeet asetetaan tilaajien ja varmenteeseen luottavien osapuolten saataville (katso direktiivin [1] liitteen II kohta k).

Erityisesti:

- a) Varmentajan on asetettava tilaajien ja varmenteeseen luottavien osapuolten saataville varmenteen käyttöä koskevat ehdot, myös direktiivin [1] liitteen II kohta k:
 - laatuvarmennepolitiikkaa sovellettaessa on ilmoitettava selkeästi, koskeeko politiikka yleisölle myönnettäviä varmenteita ja edellytetäänkö siinä turvallisen allekirjoituksen luomisvälineen käyttöä
 - mahdolliset varmenteen käyttöä koskevat rajoitukset
 - kohdassa 6.2. määritellyn mukaiset tilaajan velvollisuudet, myös edellytetäänkö varmennepolitiikassa **turvallisen allekirjoituksen luomisvälineen käyttöä**
 - tiedot siitä, kuinka varmenne todennetaan sisältäen vaatimukset tarkistaa varmenteen sulkutila, jotta varmenteeseen luottavan osapuolen voidaan perustellusti katsoa voivan luottaa varmenteeseen (katso

kohta 6.3)

- vastuunrajoitukset, mukaan luettuina käyttötarkoitukset, joiden osalta varmentaja hyväksyy (tai ei hyväksy) olevansa vastuussa
- rekisteröintitietojen säilytysaika (katso kohta 7.3.1)
- varmentajan tapahtumalokien säilytysaika (katso kohta 7.4.11)
- valitus- ja riitojenratkaisumenettelyt
- sovellettava oikeusjärjestelmä ja
- onko varmentaja todistettu yksilöidyn laatuvarmennepolitiikan vaatimusten mukaiseksi ja millä arviointijärjestelmällä tämä on todettu.

b) Edellä kohdassa a yksilöityjen tietojen on oltava saatavilla siten, että niiden eheys säilyy ja selvästi ymmärrettävällä kielellä. Tiedot voidaan välittää sähköisesti.

HUOMAUTUS 1: Tässä viestinnässä voidaan käyttää pohjana liitteessä B annettavaa varmennekuvauksen mallia. Vaihtoehtoisesti tiedot voidaan toimittaa tilaajan tai varmenteeseen luottavan osapuolen sopimuksen osana. Käyttöehdot voidaan sisällyttää varmennuskäytäntöön edellyttäen, että ne erottuvat lukijalle selvästi.

HUOMAUTUS 2: Yleisölle myönnettäviä varmenteita koskevien sopimusehtojen osalta on otettava huomioon kuluttajalainsäädännön vaatimukset, myös kuluttajasopimusten kohtuuttomista ehdoista annettu direktiivi 93/13/ETY [12].

7.3.5 Varmenteiden jakelu

Varmentajan on varmistettava, että varmenteet asetetaan tarvittavalla tavalla tilaajien, allekirjoittajien ja varmenteeseen luottavien osapuolten saataville (katso direktiivin [1] liitteen II kohta 1).

Erityisesti:

Jakelu

- a) Luomisen jälkeen valmiin ja paikkansapitävän varmenteen on oltava sen tilaajan tai allekirjoittajan saatavilla, jolle varmenne myönnetään.
- b) Varmenteita koskevia hakuja on mahdollista tehdä vain silloin, kun varmenteen allekirjoittajalta on saatu lupa.
- c) Varmentajan on asetettava varmenteeseen luottavien osapuolten saataville varmenteen käyttöä koskevat ehdot (katso kohta 7.3.4).
- d) On ilmaistava selvästi, mitä käyttöehtoja tiettyyn varmenteeseen sovelletaan.
- e) Edellä kohdissa b ja c yksilöityjen tietojen on oltava saatavilla vuorokauden ympäri viikon jokaisena päivänä. Järjestelmän toimintahäiriön, palvelun tai muiden tekijöiden osalta, jotka eivät ole varmentajan hallinnassa, varmentajan on pyrittävä parhaansa mukaan varmistamaan, ettei kyseinen tiedotuspalvelu ole poissa käytöstä varmennuskäytännössä ilmoitettua enimmäisaikaa kauemmin.
- f) Edellä kohdissa b ja c yksilöityjen tietojen on oltava julkisesti ja kansainvälisesti saatavilla.

7.3.6 Varmenteen sulkeminen ja voimassaolon keskeyttäminen tilapäisesti

Varmentajan on varmistettava, että varmenteet suljetaan oikea-aikaisesti valtuutettujen ja vahvistettujen varmenteiden sulkupyyntöjen perusteella (katso direktiivin [1] liitteen II kohta b).

Erityisesti:

Sulkupyyntöjen hallinta

- a) Varmentajan on varmennuskäytännön (katso kohta 7.1) osana dokumentoitava varmenteiden sulkupyyntöjen menettelyt, mukaan luettuina tiedot seuraavista:
 - kuka saa lähettää sulkupyyntöjä ja -ilmoituksia

- kuinka ne on toimitettava
- sulkuilmoitusten ja -pyyntöjen myöhempää vahvistusta koskevat mahdolliset vaatimukset

HUOMAUTUS 1: Vahvistusta voidaan esimerkiksi vaatia tilaajalta, jos kolmas osapuoli ilmoittaa tietosuojan vaarantumisesta:

- voidaanko varmenteita asettaa keskeytystilaan ja mistä syystä
 - käytettävä sulkutilatietojen jakelumenetelmä
 - enimmäisviive, joka kuluu sulkupyynnön tai -ilmoituksen vastaanottamisesta siihen, kunnes kaikkien varmenteeseen luottavien osapuolten saatavilla olevat sulkutilatiedot on muutettu; suurin sallittu viive on 1 vuorokausi.
- b) sulkupyynnöt ja -ilmoitukset (jotka koskevat esimerkiksi allekirjoittajan yksityisen avaimen joutumista väärin käsiin, allekirjoittajan kuolemaa, odottamatonta tilaajan tai allekirjoittajan sopimuksen tai yritystoiminnan päättymistä, sopimusvelvoitteiden rikkomista) on käsiteltävä vastaanotettaessa.
- Sulkemiseen liittyvät pyynnöt ja ilmoitukset on todennettava ja tarkistettava, että ne ovat peräisin valtuutetusta lähteestä. Nämä ilmoitukset ja pyynnöt vahvistetaan varmentajan käytännössä edellytettävällä tavalla.
 - Sulkemisen vahvistamisen ollessa kesken varmenne voidaan asettaa keskeytystilaan. Varmentajan on varmistettava, ettei varmenne jää keskeytystilaan kauemmaksi kuin sulkutilan vahvistaminen edellyttää.

HUOMAUTUS 2: Varmenteen keskeytystilan tukeminen on valinnaista.

- c) Suljetun tai keskeytystilaan asetetun varmenteen allekirjoittajalle ja tapauksen mukaan tilaajalle on tiedotettava varmenteen tilan muutoksesta.
- d) Kun varmenne on lopullisesti suljettu (eli ei keskeytetty), sitä ei saa enää ottaa uudelleen käyttöön.
- Varmenteiden sulkulistoja (CRL-listoja) ja niiden muunnelmia (esimerkiksi delta-CRL-listoja, jotka sisältävät vain edelliseen listaan nähden muuttuneet tiedot) käytettäessä ne on julkaistava vähintään päivittäin ja
- jokaisessa sulkulistassa on ilmoitettava seuraavan sulkulistan julkaisuajankohta
 - uusi sulkulista voidaan julkaista ennen seuraavan sulkulistan ilmoitettua julkaisuajankohtaa
 - varmentajan tai varmentajan määrittämän yhteisön on allekirjoitettava sulkulista.

HUOMAUTUS 3: Mahdollisimman suuren yhteensopivuuden kannalta on suositeltavaa, että varmenteiden sulkulistat julkaistaan ISO/IEC 9594-8 -standardin mukaisesti [3].

- e) Sulkupalvelun on oltava saatavilla vuorokauden ympäri viikon jokaisena päivänä. Järjestelmän toimintahäiriön, palvelun tai muiden tekijöiden osalta, jotka eivät ole varmentajan hallinnassa, varmentajan on pyrittävä parhaansa mukaan varmistamaan, ettei kyseinen palvelu ole poissa käytöstä varmennuskäytännössä ilmoitettua enimmäisaikaa kauemmin.

Tilatiedot

- f) Varmenteiden tilatietojen on oltava saatavilla vuorokauden ympäri viikon jokaisena päivänä. Järjestelmän toimintahäiriön, palvelun tai muiden tekijöiden osalta, jotka eivät ole varmentajan hallinnassa, varmentajan on pyrittävä parhaansa mukaan varmistamaan, ettei kyseinen tiedotuspalvelu ole poissa käytöstä varmennuskäytännössä ilmoitettua enimmäisaikaa kauemmin.

HUOMAUTUS 4: Varmenteen tilatietoja voidaan antaa esimerkiksi käyttämällä reaaliaikaista varmenteen tilapalvelua tai sulkulistan jakelua tiettyssä tallennuspaikassa.

- g) Tilatietojen eheys ja aitous on turvattava.
- h) Sulkutilatietojen on oltava julkisesti ja kansainvälisesti saatavilla.

- i) Sulkutilatietojen on sisällettävä varmenteiden tilatiedot vähintään varmenteen voimassaolon päättymiseen asti.

7.4 Varmentajan johtamis- ja toimintakäytännöt

7.4.1 Turvallisuuden hallinta

Varmentajan on varmistettava, että noudatetaan asianmukaisia ja tunnustettujen standardien mukaisia hallinnollisia ja johtamiseen liittyviä menettelytapoja (katso direktiivin [1] liitteen II kohdan e toinen asiakohta).

Erityisesti:

Varmentaja yleisesti

- a) Varmentajan on toteutettava riskinarviointi, jossa arvioidaan liiketoimintarisikit ja määritetään tarvittavat turvallisuusvaatimukset ja toimintatavat. Riskianalyysi on katselmoitava säännöllisesti ja sitä on tarkistettava tarvittaessa.
- b) Varmentaja on vastuussa kaikista varmennepalvelujen tarjoamisen näkökohdista, vaikka osa toiminnoista olisikin ulkoistettu alihankkijoille. Varmentajan on selkeästi määriteltävä kolmansien osapuolien vastuut ja sen on tarkoituksenmukaisin järjestelyin varmistettava, että kolmannet osapuolet sitoutuvat toteuttamaan varmentajan edellyttämiä hallintakeinoja. Varmentaja on vastuussa kaikkia osapuolia koskevien käytäntöjen julkistamisesta.
- c) Varmentajan johdon on annettava tietoturvaa koskevat linjaukset tarkoituksenmukaisen korkean tason ohjausryhmän kautta. Ohjausryhmä vastaa varmentajan tietoturvapoliitikasta sekä sen tiedottamisesta kaikille työntekijöille, joita tietoturvapoliittikka koskee.
- d) Varmentajalla on oltava laadun ja tietoturvallisuuden hallintajärjestelmä tai -järjestelmiä, jotka ovat tarjottavien varmennepalvelujen kannalta tarkoituksenmukaisia.
- e) Varmentajan sisäisen turvallisuuden hallinnan kannalta välttämätöntä tietoturvajärjestelmää on ylläpidettävä jatkuvasti. Varmentajan ohjausryhmän on hyväksyttävä kaikki turvallisuustasoon vaikuttavat muutokset.

HUOMAUTUS 1: Tietoturvallisuuden hallintaa koskevia lisäohjeita esimerkiksi tietoturvallisuuden hallintajärjestelmästä, tietoturvaryhmästä ja tietoturvapoliitikoista annetaan ISO/IEC 17799 -standardissa [13]. Lähdekirjallisuudessa mainitaan myös muita ohjeistavia asiakirjoja.

- f) Turvallisuuden hallintakeinot ja menettelytavat, jotka koskevat varmennepalvelujen tarjoamiseen käytettäviä varmentajan toimitiloja, järjestelmiä ja tietovarantoja, on dokumentoitava ja niitä on noudatettava ja ylläpidettävä.

HUOMAUTUS 2: Kyseisissä asiakirjoissa (järjestelmän tietoturvakuvauksissa) on suositeltavaa yksilöidä kaikki tarjottaviin palveluihin liittyvät asiaankuuluvat kohteet ja mahdolliset uhat sekä suojauskeinot, joilla pyritään välttämään kyseisten uhkien toteutuminen tai rajoittamaan toteutumisen vaikutuksia. Asiakirjoissa on suositeltavaa kuvata ne säännöt, ohjeet ja menettelyt, joilla yksilöidyt palvelut ja niiden turvataso toteutetaan, sekä määritellä menettelytavat tietoturvaloukkausten ja hätätilanteiden yhteydessä.

Varmistajan on varmistettava tietoturvallisuuden säilyminen, mikäli varmentajan toimintoja ulkoistetaan toiselle organisaatiolle tai yhteisölle.

7.4.2 Varantojen luokittelu ja hallinta

Varmentajan on varmistettava, että sen varantojen ja tietojen suojaustaso on tarkoituksenmukainen (katso direktiivin [1] liitteen II kohta e).

Erityisesti:

Varmentaja yleisesti

- a) Varmentajan on pidettävä kirjaa kaikista sen tietovarannoista ja määriteltävä niille suojausluokka riskianalyysin mukaisesti.

7.4.3 Henkilöstö ja tietoturva

Varmentajan on varmistettava, että henkilöstö ja rekrytointikäytännöt edistävät ja tukevat varmentajan toiminnan luotettavuutta (katso direktiivin [1] liitteen II kohdan e ensimmäinen osio).

Erityisesti:

Varmentaja yleisesti

- a) Varmentajan on pidettävä palveluksessaan riittävä määrä henkilökuntaa, jolla on tarjottujen palvelujen ja työtehtävän edellyttämä asiantuntemus, kokemus ja pätevyys.

HUOMAUTUS 1: On suositeltavaa, että varmentajan henkilökunnalta edellytettävät "asiantuntemus, kokemus ja pätevyys" perustuvat tutkintoon henkilön saamiin suosituksiin tai käytännön kokemukseen tai näiden yhdistelmään.

- b) Varmentajan varmennepolitiikkojen tai menettelyjen vastaisesti toimivalle työntekijälle seuraa asianmukaisia sanktioita.
- c) Varmentajan tietoturvapolitiikassa yksilöidyt turvallisuuteen liittyvät roolit ja vastuut on kirjattava tehtäväkuvauksiin. Luotetut roolit, joista varmentajan toiminnan turvallisuus riippuu, on määriteltävä selkeästi.
- d) Varmentajan (määräaikaisen ja vakinaisen henkilöstön tehtäväkuvaukset on määriteltävä tehtävien eriyttämisen ja ainoastaan tehtävässä tarpeellisten käyttöoikeuksien näkökulmasta. Kuvauksissa on määriteltävä toimen arkaluonteisuuden aste siihen liittyvien tehtävien, käyttöoikeuksien, taustatietojen selvittämisen sekä työntekijän kouluttamisen ja tietojen näkökulmasta. Tarvittaessa kuvauksissa on eroteltava yleiset toiminnot ja varmentajakohtaiset toiminnot.

HUOMAUTUS 2: Työkuvausten on suositeltavaa sisältää taitoja ja kokemusta koskevat vaatimukset.

- e) Henkilöstön on toteutettava varmentajan tietoturvallisuuden hallintamenettelyjen mukaisia hallinnollisia ja liikkeenjohdollisia menettelytapoja (katso kohta 7.4.1).

HUOMAUTUS 3: Katso lisäohjeita ISO/IEC 17799 -standardista [13].

Rekisteröinti, varmenteiden luominen, välineen tarjoaminen allekirjoittajalle, varmenteiden sulkeminen

- f) Johtotehtävissä on pidettävä henkilöitä, joilla on johtotehtävissä toimimiseen riittävä sähköisten allekirjoitusten tekniikoihin liittyvä kokemus tai koulutus, jotka ovat perillä turvallisuudesta vastuussa olevaa henkilöstöä koskevista turvatoimista ja joilla on kokemusta tietoturvasta ja riskinarvioinnista.
- g) Niillä varmentajan henkilökunnan jäsenillä, jotka toimivat luotetuissa rooleissa, ei saa olla eturistiriitoja, jotka saattavat vaarantaa varmentajan toiminnan puolueettomuuden.
- h) Luotettuja rooleja ovat seuraavia vastuualueita sisältävät roolit:
- Turvallisuuspäällikkö: Kokonaisvastuu turvallisuuskäytäntöjen toteuttamisen hallinnasta. Lisäksi hän hyväksyy varmenteiden luomisen, peruuttamisen ja niiden asettamisen keskeytystilaan.
 - Järjestelmänvalvoja: Lupa asentaa varmentajan luotettavia järjestelmiä, joita käytetään rekisteröinnissä, varmenteiden luomisessa, välineen tarjoamisessa allekirjoittajalle ja varmenteiden peruuttamisen hallinnassa, ja määrittää niihin asetuksia ja ylläpitää niitä.
 - Järjestelmäoperaattori: Vastuussa varmentajan luotettavien järjestelmien päivittäisestä toiminnasta. Valtuutus suorittaa järjestelmän varmuuskopiointi ja palautus.
 - Järjestelmän auditoija: Valtuutus tarkastella varmentajan luotettavien järjestelmien arkistoja ja auditointilokeja.
- i) Turvallisuudesta vastaava ylempi johto nimittää henkilöt virallisesti luotettuihin rooleihin.

Varmentaja ei saa nimittää luotettuihin rooleihin tai johtoon sellaista henkilöä, jonka tiedetään tehneen vakavan rikoksen tai muunlaisen työtehtävään soveltumiseen vaikuttavan rikkomuksen. Henkilöstöllä ei saa olla pääsyä luotettuihin toimintoihin ennen kuin kaikki tarvittavat tarkistukset on tehty.

HUOMAUTUS 4: Joissakin maissa varmentaja ei ehkä pysty saamaan tietoa aiemmista tuomioista. Tällöin on

suositeltavaa, mikäli kyseisessä maassa tämä on sallittua, että työnantaja **pyytää** asiasta tietoa työnhakijalta ja tämän kieltäytyessä hylkää hakemuksen.

7.4.4 Fyysinen ja ympäristön turvallisuus

Varmentajan on varmistettava, että fyysistä pääsyä kriittisiin palveluihin valvotaan ja että varantoja koskevat fyysiset riskit minimoidaan (katso direktiivin 1999/93/EY [1] liitteen II kohta f).

Erityisesti:

Varmentaja yleisesti

- a) Vain asianmukaisesti valtuutetuille henkilöille on sallittava fyysinen pääsy toimitiloihin, jotka liittyvät varmenteiden luomiseen, välineen laatimiseen allekirjoittajalle ja varmenteiden peruuttamisen hallintapalveluihin.
- b) Käytössä on oltava hallintakeinot, joilla pyritään välttämään varantojen menetykset, vahingot ja vaarantuminen sekä liiketoiminnan keskeytyminen.
- c) Käytössä on oltava hallintakeinot, joilla pyritään välttämään tiedon ja tiedonkäsittelytilojen vaarantuminen ja niitä koskevat varkauudet.

Varmenteiden luominen, välineen tarjoaminen allekirjoittajalle (etenkin valmistaminen) ja varmenteiden peruuttamisen hallinta

- d) Varmenteiden luomisessa, välineen valmistamisessa allekirjoittajalle (katso kohta 7.2.9) ja varmenteiden peruuttamisen hallinnassa käytettävien toimitilojen ympäristön on suojattava fyysisesti palveluja, jotta estetään luvaton pääsy järjestelmiin tai tietoon ja palvelujen vaarantuminen.
- e) Tälle fyysisesti turvalliselle alueelle saapuvia henkilöitä ei saa jättää merkittäväksi ajaksi ilman valtuutetun henkilön valvontaa.
- f) Fyysinen suojaus saadaan aikaan muodostamalla selkeästi määritellyt turvallisuusrajat (fyysiset esteet) varmenteiden luomisen, allekirjoittajalle toimitettavan välineen valmistamisen (katso kohta 7.2.9) ja varmenteiden peruuttamisen hallintapalvelujen ympärille. Muiden organisaatioiden kanssa mahdollisesti yhteiskäytössä olevien tilojen on sijaittava näiden rajojen ulkopuolella.
- g) Käytössä on oltava fyysisen ja ympäristön turvallisuuden hallintakeinoja, joilla suojataan järjestelmäresurssien sijaintitiloja, järjestelmäresursseja ja niiden käyttöä tukevia toimitiloja. Varmentajan fyysistä ja ympäristön turvallisuutta koskevissa menettelytapaohjeissa on käsiteltävä varmenteiden luomiseen, allekirjoittajalle toimitettavan välineen valmistamiseen (katso kohta 7.2.9) ja varmenteiden peruutusten hallintapalveluihin liittyvien järjestelmien osalta esimerkiksi fyysisen pääsyn valvontaa, luonnonmullistuksilta suojaamista, paloturvallisuustekijöitä, kunnallisteknisten verkostojen häiriöitä (esimerkiksi sähkö, teleliikenne), rakenteiden pettämistä, putkistovuotoja, varkaus- ja murtovarkaussuojausta sekä hätätilanteesta toipumista.
- h) Käytössä on oltava hallintakeinoja, joilla suojataan varmentajan palveluihin liittyvien laitteiden, tietojen, tietovälineiden ja ohjelmistojen luvaton vienti pois paikalta.

HUOMAUTUS 1: Lisätietoja fyysisestä ja ympäristön turvallisuudesta annetaan ISO/IEC 17799 -standardissa [13].

HUOMAUTUS 2: Samalla turvallisella alueella voidaan tukea muitakin toimintoja, kunhan vain valtuutella henkilöllä on pääsy sinne.

7.4.5 Toiminnan hallinta

Varmentajan on varmistettava, että varmentajan järjestelmät ovat turvalliset ja että niitä käytetään asianmukaisesti toimintahäiriöriskit minimoiden (katso direktiivin [1] liitteen II kohta e).

Erityisesti:

Varmentaja yleisesti

- a) Varmentajan järjestelmien ja tietojen eheyttä on suojattava viruksilta sekä haitallisilta ja luvattomilta

ohjelmistoilta.

- b) Tietoturvaloukkausten ja toimintahäiriöiden vahingot on minimoitava käyttämällä tapahtumailmoituksia ja niihin reagoimista koskevia menettelyjä.
- c) Varmentajalla käytettäviä tietovälineitä on käsiteltävä turvallisesti, jotta voidaan välttää tietovälineiden vahingot, varkaudet ja luvaton käyttö.

HUOMAUTUS 1: Jokaisen johtotehtävissä toimivan henkilökunnan jäsenen vastuulla on suunnitella ja toteuttaa tehokkaasti varmennepolitiikkaa sekä siihen liittyviä käytäntöjä varmennuskäytännössä kirjatun mukaisesti.

- d) Tietovälineiden hallintamenettelyillä on turvattava, etteivät tietovälineet vanhene tai heikkene tietojen vaadittuna säilytysaikana.
- e) Kaikkia varmennepalvelujen tarjoamiseen vaikuttavia luotettuja ja hallinnollisia rooleja varten on luotava menettelyt ja niitä on toteutettava.

Tietovälineiden käsittely ja turvallisuus

- f) Kaikkia tietovälineitä on käsiteltävä turvallisesti tietojen luokittelujärjestelmän vaatimusten mukaisesti (katso kohta 7.4.2). Luottamuksellista tietoa sisältävät tietovälineet on hävitettävä turvallisesti, kun niitä ei enää tarvita.

Järjestelmäsuunnittelu

- g) Suorituskyvyvaatimuksia on seurattava ja tulevista suorituskyvyvaatimuksista on tehtävä arvioita, jotta voidaan varmistaa riittävän suoritustehon ja tallennustilan saatavuus.

Tapahtumailmoitukset ja niihin reagointi

- h) Varmentajan on toimittava oikea-aikaisesti ja koordinoitusti, jotta tietoturvaloukkauksiin voidaan reagoida ripeästi ja jotta niiden vaikutuksia voidaan rajoittaa. Kaikista tietoturvaloukkauksista on ilmoitettava niin pian kuin mahdollista tapahtuman jälkeen.
- i) Kohdan 7.4.11 vaatimukset täyttävät auditointiprosessit on aloitettava järjestelmän käyttöönoton yhteydessä ja niitä on jatkettava järjestelmän käytöstä poistamiseen asti.
- j) Auditointilokeja on seurattava ja tarkistettava säännöllisesti, jotta haitallisista toimista voidaan havaita näyttöä.

Varmenteiden luominen, peruutusten hallinta

Toiminnassa noudatettavat menettelytavat ja vastualueet

- k) Varmentajan turvatoiminta on erotettava tavanomaisesta toiminnasta.

HUOMAUTUS 2: Varmentajan turvatoiminnan vastualueita ovat

- toimintatavat ja vastualueet
- turvallisten järjestelmien suunnittelu ja hyväksyminen
- haittaohjelmilta suojautuminen
- aputoimet
- verkohallinta
- aktiivinen auditointipäiväkirjojen seuranta, tapahtumien analysointi ja seuranta
- tietovälineiden käsittely ja turvallisuus
- tietojen ja ohjelmistojen vaihto.

Varmentajan turvallisuusosasto johtaa näitä vastualueita, mutta käytännössä kuitenkin käyttökäyttöhenkilökunta saattaa toteuttaa niitä (valvonnan alaisena) turvallisuutta koskevan asianmukaisen menettelytapaohjeen mukaisesti sekä roolit ja vastualueet määrittävien asiakirjojen mukaisesti.

7.4.6 Järjestelmiin pääsyn hallinta

Varmentajan on varmistettava, että vain asianmukaisesti valtuutetuilla henkilöillä on pääsy varmentajan järjestelmään (katso direktiivin [1] liitteen II kohta f). Erityisesti:

Varmentaja yleisesti

- a) Hallintakeinoja (esimerkiksi palomureja) on toteutettava, jotta varmentajan sisäisiä verkkotoimialueita voidaan suojata kolmansien osapuolten käytettävissä olevilta ulkoisilta verkkotoimialueilta.

HUOMAUTUS 1: Palomuurien määräyksissä on suositeltavaa estää protokollat ja käyttöoikeudet, joita varmentajan toiminta ei edellytä.

- b) Luottamuksellinen tieto on suojattava luvattomalta käytöltä tai muokkaamiselta. Luottamuksellinen tieto on suojattava (esimerkiksi salauksella ja eheyden turvaavalla menetelmällä), kun sitä vaihdetaan verkoissa, jotka eivät ole turvallisia.

HUOMAUTUS 2: Rekisteröintitiedot ovat luottamuksellisia tietoja.

- c) Varmentajan on järjestelmän turvallisuuden ylläpitämiseksi varmistettava tehokas käyttäjien (näitä ovat järjestelmän operaattorit ja valvojat sekä kaikki käyttäjät, joille on annettu suorat käyttöoikeudet järjestelmään) käyttöoikeuksien hallinta, joka sisältää käyttäjätilin hallinnan, auditoinnin sekä oikea-aikaisen käyttöoikeuksien muokkaamisen tai poistamisen.
- d) Varmentajan on varmistettava, että pääsy tietoon ja sovellusten järjestelmätoimintoihin rajoitetaan pääsynvalvontaa koskevien menettelytapaohjeiden mukaisesti. Sen on myös varmistettava, että varmentajan järjestelmässä on riittävästi tietokoneiden turvallisuuden hallintakeinoja, joilla varmentajan käytännössä määritellyt luotetut roolit voidaan eriyttää ja voidaan eriyttää turvallisuutta valvova rooli operatiivisista toiminnoista. Etenkin järjestelmäpuhujelmien käyttöä on rajoitettava ja valvottava tiukasti. Käyttöoikeuksia on rajoitettava siten, että käyttäjälle annetaan oikeudet vain sellaisten resurssien käyttöön, joita tarvitaan hänelle osoitetussa roolissa tai rooleissa.
- e) Varmentajan henkilöstön jäsenet on tunnistettava ja todennettava, ennen kuin he käyttävät varmenteiden hallintaan liittyviä kriittisiä sovelluksia.
- f) Varmentajan henkilöstön jäsenet on asetettava vastuuseen omista toimistaan, esimerkiksi tapahtumalokien säilyttämisen avulla (katso kohta 7.4.11).
- g) Luottamuksellinen tieto on suojattava siten, ettei se paljastu sen vuoksi, että luvattomat käyttäjät pääsevät käyttämään uudelleen tallennuskohteita (esimerkiksi poistettuja tiedostoja).

HUOMAUTUS 3: Rekisteröintitiedot ovat luottamuksellisia

tietoja. **Varmenteiden luominen**

- h) Varmentajan on varmistettava, että paikallisverkon osat (esimerkiksi reitittimet) pidetään fyysisesti turvallisessa ympäristössä ja että säännöllisissä auditoinneissa varmistetaan, että osien kokoonpanot ovat varmentajan määrittämien vaatimusten mukaisia.
- i) Varmentajalla on oltava jatkuvakäyttöinen valvonta- ja hälytysvälineistö, jolla varmentaja voi oikea-aikaisesti havaita luvattomat ja/tai sääntöjenvastaiset yritykset käyttäen sen resursseja sekä kirjata tällaiset yritykset ja reagoida niihin.

HUOMAUTUS 4: Kyseessä voi olla esimerkiksi tunkeutumisen havaitsemisjärjestelmä, käyttöoikeuksien valvonta ja

hälytysvälineistö. **Jakelu**

- j) Jakelusovelluksessa on oltava pakotettu käytönvalvonta silloin, kun yritetään lisätä tai poistaa varmenteita tai muokata muita asiaan liittyviä tietoja.

Peruutusten hallinta

- k) Varmentajalla on oltava jatkuvakäyttöinen valvonta- ja hälytysvälineistö, jolla varmentaja voi oikea-aikaisesti

havaita luvattomat ja/tai sääntöjenvastaiset yritykset käyttää sen resursseja sekä kirjata tällaiset yritykset ja reagoida niihin.

HUOMAUTUS 5: Kyseessä voi olla esimerkiksi tunkeutumisen havaitsemisjärjestelmä, käyttöoikeuksien valvonta ja hälytysvälineistö.

Sulkuutila

- 1) Sulkuutilasovelluksessa on oltava pakotettu käytönvalvonta silloin, kun sulkuutilatietoja yritetään muokata.

7.4.7 Luotettavien järjestelmien käyttöönotto ja ylläpito

Varmentajan on käytettävä luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutostöiltä (katso direktiivin [1] liitteen II kohta f).

HUOMAUTUS 1: Luotettavia järjestelmiä koskevien vaatimusten täyttäminen voidaan varmistaa esimerkiksi käyttämällä julkaisun CWA 14167-1 [8] mukaisia järjestelmiä tai soveltuvaa suojausprofiilia (tai -profileja), joka on määritelty ISO/IEC 15408 -standardin [7] mukaisesti.

HUOMAUTUS 2: Varmentajan palveluja koskevassa riskianalysissä (katso kohta 7.4.1) on suositeltavaa yksilöidä varmentajan kriittiset palvelut, joissa edellytetään luotettavia järjestelmiä, sekä vaadittava varmuustaso

Erityisesti: Varmentaja yleisesti

- a) Kaikissa varmentajan toteuttamissa tai teettämässä järjestelmien kehityshankkeissa on tehtävä suunnittelu- ja vaatimusmäärittelyvaiheessa turvallisuusvaatimusten analysointi, jotta voidaan varmistaa, että tietotekniset järjestelmät rakennetaan turvallisiksi.
- b) Kaikkien käytettävien ohjelmistojen versioita, muutoksia ja korjauspäivityksiä varten on oltava valvontamenettelyt.

7.4.8 Liiketoiminnan jatkuvuuden hallinta ja häiriötilanteiden käsittely

Varmentajan on varmistettava hätätilanteen sattuessa, esimerkiksi varmentajan yksityisen allekirjoitusavaimen vaarantumistilanteessa, että toiminta palautetaan mahdollisimman pian (katso direktiivin [1] liitteen II kohta a).

Erityisesti:

Varmentaja yleisesti

- a) Varmentajan on määriteltävä hätätilanteen sattuessa toteutettava

jatkuvuussuunnitelma ja ylläpidettävä sitä. **Varmentajan järjestelmien**

varmuuskopiointi ja palautus

- b) Varmentajan toimintojen palauttamisessa tarvittavat varmentajan järjestelmätiedot on varmuuskopioitava ja niitä on säilytettävä turvallisessa ja asianmukaisessa paikassa, jotta varmentaja voi nopeasti palauttaa toimintansa häiriö- tai hätätilanteessa.

HUOMAUTUS 1: ISO/IEC 17799 -standardin [13] kohdan 8.4.1 mukaisesti: Liiketoiminnan olennaiset tiedot ja ohjelmistot on varmuuskopioitava säännöllisesti. Käytössä on oltava tarkoituksenmukainen varmuuskopiointivälineistö, jolla varmistetaan, että kaikki liiketoiminnan kannalta olennaiset tiedot ja ohjelmistot voidaan palauttaa hätätilanteen tai tietovälineen toimintahäiriön jälkeen. Yksittäisten järjestelmien varmuuskopiointijärjestelyt on testattava säännöllisesti, jotta voidaan varmistaa niiden täyttävän liiketoiminnan jatkuvuussuunnitelman vaatimukset.

- c) Varmuuskopiointi- ja palautustoiminnot suorittavat asiaankuuluvissa, kohdassa 7.4.3 määritellyissä luotetuissa rooleissa toimivat henkilöt.

HUOMAUTUS 2: Jos riskianalysissä on määritelty, että esimerkiksi avainten hallinta edellyttää kahden henkilön valvontaa, kahden henkilön valvontaa tarvitaan myös palauttamisessa.

Varmentajan avaimen tietosuojaan vaarantuminen

- d) Varmentajan liiketoiminnan jatkuvuussuunnitelmassa (tai hätätilanteesta palautumissuunnitelmassa) on pidettävä hätätilanteena varmentajan yksityisen allekirjoitusavaimen tietosuojan vaarantumista tai epäiltyä vaarantumista.

Varmenteen sulkutilatiedot

- e) Tiedon luotettavuuden vaarantumistilanteessa varmentajan on ryhdyttävä vähintään seuraaviin toimiin:
- Ilmoitettava vaarantumisesta seuraaville: kaikille sellaisille tilaajille ja muille tahoille, esimerkiksi varmenteeseen luottaville osapuolille ja varmentajille, joiden kanssa varmentaja on sopimussuhteessa tai muunlaisessa vakiintuneessa suhteessa. Lisäksi tämä tieto on saatettava muiden varmenteeseen luottavien osapuolten saataville.
 - Ilmoitettava, että varmenteet ja sulkulistat, joiden myöntämisessä tai julkaisussa on käytetty kyseistä varmentajan avainta, eivät ehkä ole enää voimassa.

HUOMAUTUS 3: Jos varmentaja saa tietoonsa, että jonkin toisen varmentajan tietosuojaa on vaarantunut, on suositeltavaa peruuttaa kyseisen toisen varmentajan mahdollisesti myöntämät varmentajan varmenteet.

Algoritmin vaarantuminen

- f) Jos jokin varmentajan tai sen tilaajien käyttämistä algoritmeista tai niihin liittyvistä parametreista osoittautuu riittämättömäksi sen jäljellä olevaa suunniteltua käyttöä varten, varmentajan on toimittava seuraavasti:
- Asiasta on tiedotettava kaikille sellaisille tilaajille ja varmenteeseen luottaville osapuolille, joiden kanssa varmentaja on sopimussuhteessa tai muunlaisessa vakiintuneessa suhteessa. Lisäksi tieto on saatettava muiden varmenteeseen luottavien osapuolten saataville.
 - Sen on peruutettava kaikki varmenteet, joita asia koskee.

7.4.9 Varmentajan toiminnan päättymisen

Varmentajan on varmistettava, että sen varmennepolitiikan alaisten palvelujen päättymisestä tilaajille ja varmenteeseen luottaville osapuolille aiheutuvat mahdolliset häiriöt minimoidaan ja että sellaisia tietoja ylläpidetään jatkuvasti, joilla varmentamista koskevia todisteita voidaan esittää oikeudellisissa menettelyissä (katso direktiivin [1] liitteen II kohta i).

Erityisesti:

Varmentaja yleisesti

- a) Ennen kuin varmentaja lopettaa palvelunsa, on tehtävä vähintään seuraavat toimet:

- Varmentajan on ilmoitettava lopettamisesta seuraaville: kaikille sellaisille tilaajille ja muille tahoille, esimerkiksi varmenteeseen luottaville osapuolille ja varmentajille, joiden kanssa varmentaja on sopimussuhteessa tai muunlaisessa vakiintuneessa suhteessa. Lisäksi tämä tieto on saatettava muiden varmenteeseen luottavien osapuolten saataville.

HUOMAUTUS: Varmenteeseen luottavan osapuolen osalta ei edellytetä aikaisempaa suhdetta varmentajaan.

- Varmentajan on peruutettava alihankkijoiltaan kaikki antamansa valtuutukset suorittaa varmentajan puolesta varmenteiden myöntämisprosessiin liittyviä toimintoja.
 - Varmentajan on toteutettava tarpeelliset toimet siirtääkseen velvollisuutensa säilyttää rekisteröintitiedot (katso kohta 7.3.1) ja tapahtumalokien arkistot, myös varmenteen tilatiedot, (katso kohta 7.4.11) vaaditun ajan tilaajalle ja varmenteeseen luottaville osapuolille ilmoitetun mukaisesti (katso kohta 7.3.4).
 - Varmentajan on kohdan 7.2.6 mukaisesti tuhottava yksityiset avaimensa tai pidättäydyttävä niiden käyttämisestä.
- b) Varmentajalla on oltava vähimmäisvaatimusten täyttämistä aiheutuvat kustannukset kattava järjestely, mikäli se joutuu konkurssiin tai ei muista syistä pysty itse kattamaan kustannuksia, siinä määrin kuin se on sovellettavan konkurssilainsäädännön rajoitusten mukaisesti mahdollista.
- c) Varmentajan on käytännössään ilmoitettava palvelun päättymiseen liittyvät varautumistoimet. Näihin kuuluvat
- ilmoittaminen tahoille, jota asia koskee

- varmentajan velvollisuuksien siirtäminen muille osapuolille
- edelleen voimassa olevien myönnettyjen varmenteiden tilatietojen käsittely.

7.4.10 Lainsäädäntöön perustuvien vaatimusten noudattaminen

Varmentajan on varmistettava, että lainsäädäntöön perustuvia vaatimuksia noudatetaan (katso direktiivin 8 artikla [1]).

Erityisesti:

Varmentaja yleisesti

- a) Varmentajan on varmistettava, että se täyttää kaikki sovellettavat lakisääteiset vaatimukset (myös tietosuojadirektiivin [4] vaatimukset, katso seuraava luettelukohta), jotka liittyvät tietojen suojaamiseen menetyksiltä, tuhoamiselta ja väärentämiseltä. Lakisääteisten vaatimusten noudattaminen ja olennaisten liiketoimintojen tukeminen saattaa joidenkin tietojen osalta edellyttää turvallista säilyttämistä (katso kohta 7.4.11).
- b) Varmentajan on varmistettava, että kansallisessa lainsäädännössä täytäntöönpannun EU:n tietosuojadirektiivin [4] vaatimuksia noudatetaan.

HUOMAUTUS: Näitä menettelytapoja koskevia tietosuojakysymyksiä käsitellään seuraavissa kohdissa:

- Rekisteröinti (myös salanimien käyttö) (katso kohta 7.3.1)
 - Tallennettujen tietojen luottamuksellisuus (katso kohdan 7.4.11 alakohta a sekä kohdan 7.3.3 alakohta f)
 - Henkilötietoihin pääsyn suojaus (katso kohta 7.4.6)
 - Käyttäjän lupa (katso kohdan 7.3.1 alakohta i).
- c) Asianmukaisilla teknisillä ja organisaatioon liittyvillä toimilla on estettävä luvaton tai laitton henkilötietojen käsittely, niiden häviäminen vahingossa tai niiden hävittäminen sekä henkilötietoja koskevat vahingot.
 - d) Käyttäjien varmentajalle luovuttamat tiedot on suojattava täydellisesti, jotta ne eivät joudu kenenkään tietoon ilman käyttäjän lupaa, oikeuden määräystä tai muuta lainvoimaista valtuutusta.

7.4.11 Laatuvarmenteita koskevan tiedon säilyttäminen

Varmentajan on varmistettava, että kaikki laatuvarmennetta koskevat tiedot tallennetaan tarkoituksenmukaiseksi ajaksi, erityisesti jotta se voi esittää varmentamista koskevia todisteita oikeudellisissa menettelyissä (katso direktiivin [1] liitteen II kohta i).

HUOMAUTUS 1: Laatuvarmenteita koskevia tallenteita ovat rekisteröintitiedot (katso kohta 7.3.1) ja tiedot varmentajalla sattuneista ympäristöön, avainten hallintaan tai varmenteiden hallintaan liittyvistä merkittävistä tapahtumista.

Erityisesti:

Yleisesti

- a) Laatuvarmenteita koskevien nykyisten ja arkistoitujen tallenteiden luottamuksellisuus ja eheys on säilytettävä.
- b) Laatuvarmenteita koskevat tallenteet on arkistoitava julkistettujen liiketoimintatapojen mukaisesti täydellisinä ja luottamuksellisina.
- c) Laatuvarmenteita koskevat tallenteet on tarvittaessa asetettava saataville, jotta voidaan esittää varmentamista koskevia todisteita oikeudellisissa menettelyissä. Allekirjoittajalla, ja tietosuojavaatimusten rajoissa myös tilaajalla (katso kohta 7.4.10), on oltava pääsy allekirjoittajan rekisteröintitietoihin ja muihin allekirjoittajaa koskeviin tietoihin.

HUOMAUTUS 2: Tätä voidaan käyttää esimerkiksi varmenteen ja allekirjoittajan välisen yhteyden varmistamiseen.

- d) Varmentajalla sattuneiden ympäristöön, avainten hallintaan tai varmenteiden hallintaan liittyvien merkittävien tapahtumien tarkka ajankohta on kirjattava.

HUOMAUTUS 3: Varmentajan on suositeltavaa ilmoittaa käytännössään tapahtumien ajoittamisessa käytettävän kellon tarkkuus sekä miten kyseinen tarkkuus varmistetaan.

- e) Laatuvarmenteita koskevia tallenteita on säilytettävä tarkoituksenmukaisen ajan, jota edellytetään sähköisten allekirjoitusten tueksi vaadittavien oikeudellisten todisteiden esittämiseen sovellettavan lainsäädännön mukaisesti.

HUOMAUTUS 4: Vaadittavaa tietojen säilytysajan kestoa on hankala määrittellä, sillä määrittely on kompromissi tallenteiden käytön tarpeen sekä niiden säilyttämistäkaan välillä. Tallenteita voidaan tarvita vähintään niin kauan kuin voimassa olevaan varmenteeseen liittyvä liiketapahtuma voidaan ottaa tutkintaan. Useimpia liiketapahtumia koskevat vanhentumissäännöt, jotka lopulta tekevät liiketoiminnan riittämättömäksi. Joidenkin liiketapahtumien, kuten kiinteistökauppojen, osalta juridinen vanhentuminen tapahtuu kuitenkin vasta pitkän ajan kuluttua tai ei lainkaan.

HUOMAUTUS 5: Jos käyttötarkoitukseltaan erilaisia varmenteita koskevat eri säilytysajat, varmenteissa on käytettävä eri laatuvarmennepolitiikkojen tunnuksia. Jos rekisteröintitietojen ja tapahtumalokitietojen eri osia koskevat eri säilytysajat, tästä on mainittava tilaajalle ja varmenteeseen luottavalle osapuolelle kohtien 7.3.1 ja 7.3.4 mukaisesti.

- f) Tapahtumat on kirjattava lokiin siten, ettei niitä voi helposti poistaa tai tuhota (ei koske pitkäaikaiseen tietovälineeseen siirtämistä) kyseisiltä tiedoilta vaadittavan säilytysajan kuluessa.

HUOMAUTUS 6: Tämä voidaan toteuttaa esimerkiksi käyttämällä vain kirjoittamisen sallivaa (write-only) tietovälinettä, tallennetta kaikista käytetyistä siirrettävistä tietovälineistä sekä muualla kuin kyseisellä paikalla sijaitsevia varmuuskopioita.

- g) Varmentajan on dokumentoitava ne tietyt tapahtumat ja tiedot, jotka on tallennettava lokiin.

Rekisteröinti

- h) Varmentajan on varmistettava, että lokiin kirjataan kaikki rekisteröintiin liittyvät tapahtumat, myös varmenteen uusimista tai sen avainparin vaihtamista koskevat pyynnöt.
- i) Varmentajan on varmistettava, että kaikki rekisteröintitiedot tallennetaan, vähintään seuraavat:
- rekisteröintiä varten hakijan esittämän asiakirjan tai -kirjojen tyyppi
 - tallenne yksilöivistä tunnistamistiedoista, -numeroista tai niiden yhdistelmästä (esimerkiksi hakijan ajokortin numero) tai tarvittaessa tunnistamisasiakirjoista
 - paikka, jossa säilytetään kopioita hakemuksista ja tunnistamisasiakirjoista, myös allekirjoitetusta tilaajan sopimuksesta (katso kohdan 7.3.1 alakohta i);
 - mahdolliset tarkentavat valinnat tilaajan sopimuksessa (esimerkiksi lupa varmenteen julkaisuun) katso kohdan 7.3.1 alakohta i
 - hakemuksen hyväksyvä taho
 - tunnistamisasiakirjojen aitouden todentamisessa mahdollisesti käytetty menetelmä
 - vastaanottavan varmentajan nimi ja/tai tarvittaessa toimittavan rekisteröijän

nimi.

- j) Varmentajan on varmistettava, että allekirjoittajan tiedot säilyvät luottamuksellisina.

Varmenteiden luominen

- k) Varmentajan on kirjattava lokiin kaikki varmentajan avainten elinkaareen liittyvät tapahtumat.
- l) Varmentajan on kirjattava lokiin kaikki varmenteiden elinkaareen liittyvät tapahtumat.

Välineen tarjoaminen allekirjoittajalle

- m) Varmentajan on kirjattava lokiin kaikki tapahtumat, jotka liittyvät varmentajan hallinnoimien avainten, myös varmentajan mahdollisesti luomien allekirjoittajan avainten, elinkaareen.
- n) Varmentajan on kirjattava kaikki turvallisen allekirjoituksen luomisvälineen

valmistamiseen liittyvät mahdolliset tapahtumat.

Sulkupalvelu

- o) Varmentajan on varmistettava, että kaikki varmenteen sulkemiseen liittyvät pyynnöt ja ilmoitukset sekä niitä seuranneet toimenpiteet kirjataan lokiin.

7.5 Organisaatioon liittyvät vaatimukset

Varmentajan on varmistettava, että sen organisaatio on luotettava (katso direktiivin [1] liitteen II kohta a).

Erityisesti:

Varmentaja yleisesti

- a) Varmentajan toiminnassa noudatettavien politiikkojen ja menettelyjen on oltava syrjimättömiä.
- b) Varmentajan on asetettava palvelunsa kaikkien sellaisten hakijoiden saataville, joiden toiminta kuuluu varmentajan ilmoitetun toiminta-alueen piiriin.
- c) Varmentajan on oltava kansallisen lainsäädännön mukainen oikeushenkilö.
- d) Varmentaja on tehnyt tarkoituksenmukaiset järjestelyt, joilla katetaan sen toiminnan vastuut.
- e) Varmentaja on taloudellisesti riittävän vakaa ja sillä on riittävät resurssit, jotta se voi toimia näiden menettelytapojen mukaisesti.
 - f) Varmentajalla on käytössään menettelytavat ja käytännöt, joilla ratkaistaan asiakkaiden tai muiden osapuolten tekemät, sähköisten luottamuspalvelujen tarjoamista tai muita asiaankuuluvia asioita koskevat valitukset tai riidat.
- g) Varmentajalla on asianmukaisesti dokumentoitu sopimus ja sopimussuhde, mikäli palvelujen tarjoamiseen sisältyy alihankintaa, ulkoistamista tai kolmannen osapuolen kanssa tehtyjä järjestelyjä.

Varmenteiden luominen, sulkupalvelu

- h) Varmenteiden luomiseen ja sulkupalveluun liittyvien varmentajan osien on oltava palvelujen perustamista, tarjoamista, ylläpitämistä ja keskeyttämistä koskevien päätösten osalta riippumattomia muista organisaatioista; etenkin johtajaan, johtotehtävissä toimivaan henkilöstöön ja luotetuissa rooleissa toimivaan henkilöstöön ei saa kohdistua kaupallisia, taloudellisia tai muita paineita, jotka saattaisivat heikentää luottamusta tarjottaviin palveluihin.
- i) Varmenteiden luomiseen ja peruutusten hallintaan liittyvillä varmentajan osilla on oltava toiminnan puolueettomuuden turvaava dokumentoitu rakenne.

8 Määrittelypuitteet muita laatuvarmennepolitiikkoja varten

Tässä kohdassa määritellään laatuvarmenteita myöntävien varmentajien muita varmennepolitiikkoja koskevat yleiset puitteet. Varmentaja voi ilmaista noudattavansa näiden yleisten määrittelypuitteiden vaatimuksia kohdan 8.4 mukaisesti. Yleisesti ottaen vaatimustenmukaisuus edellyttää kohtien 6 ja 7 vaatimusten noudattamista lukuun ottamatta niitä vaatimuksia, joita sovelletaan vain yleisölle varmenteita myöntäviin varmentajiin.

HUOMAUTUS: Tätä kohtaa EI sovelleta kumpaankaan kohdassa 5 yksilöityyn laatuvarmennepolitiikkaan, QCP public- ja QCP public + SSCD -laatuvarmennepolitiikkaan.

8.1 Laatuvarmennepolitiikan hallinta

Varmentajan on varmistettava, että sen varmennepolitiikka on ajantasainen. Erityisesti:

- a) Varmennepolitiikassa on yksilöitävä, kumpaan tässä asiakirjassa määriteltyyn laatuvarmennepolitiikkaan se pohjautuu ja mitä mahdollisia muunnelmia siinä sovelletaan.
- b) Varmentajalla tulee olla varmennepolitiikasta vastaava taho, joka vastaa viime kädessä laatuvarmennepolitiikan määrittämisestä ja hyväksymisestä.
- c) Liiketoimintavaatimusten arvioimiseksi ja laatuvarmennepolitiikkaan sisällytettävien turvallisuusvaatimusten määrittämiseksi kaikista edellä mainituista osa-alueista on laadittava riskinarviointi.
- d) Varmennepolitiikan tai -politiikkojen hyväksymisessä ja muokkaamisessa on noudatettava määriteltyä tarkistusprosessia, joka sisältää laatuvarmennepolitiikan ylläpitovastuut.
- e) Tarkistusprosessin tehtävänä on varmistaa, että varmentajan varmennuskäytäntö tukee laatuvarmennepolitiikkoja.
- f) Varmentajan on asetettava varmentajan tukemat laatuvarmennepolitiikat kaikkien asianomaisten tilaajien ja varmenteeseen luottavien osapuolten saataville.
- g) Varmentajan tukemien laatuvarmennepolitiikkojen tarkistukset on asetettava tilaajien ja varmenteeseen luottavien osapuolten saataville.
- h) Laatuvarmennepolitiikan on sisällettävä kaikki kohtien 6 ja 7 tai niitä tiukemmat vaatimukset, lukuun ottamatta jäljempänä ilmoitettuja poikkeuksia. Mahdollisissa ristiriitatapauksissa sovelletaan tämän asiakirjan vaatimuksia.
- i) Varmennepolitiikalle on hankittava OID-yksilöintitunnus, joka on muodoltaan ITU-T:n suosituksen X.509 [3] mukainen.

8.2 Poikkeukset laatuvarmennepolitiikkoihin, jotka koskevat muille kuin yleisölle myönnettäviä laatuvarmenteita

Mikäli varmenteita myönnetään muille kuin yleisölle, kyseistä toimintaa koskevan laatuvarmennepolitiikan ei tarvitse noudattaa seuraavia laatuvarmenteita koskevia menettelytapavaatimuksia:

HUOMAUTUS: Varmentajan ei katsota myöntävän laatuvarmenteita yleisölle, jos kyseisten varmenteiden käyttöä on rajoitettu osanottajien välisin vapaaehtoisin yksityisoikeudellisin sopimuksin.

- a) vastuu kohdan 6.3 mukaisesti
- b) varmenteiden luomispalvelun ja peruuttamisen hallintapalvelun tarjoajien riippumattomuus kohdan 7.5 alakohtien h ja i mukaisesti
- c) varmenteiden jakelu julkisesti kohdan 7.3.5 alakohdan f mukaisesti
- d) sulkutilatietojen julkinen saatavuus kohdan 7.3.6 alakohdan k mukaisesti.

8.3 Lisävaatimukset

Tilaaajille ja varmenteeseen luottaville osapuolille on ilmoitettava osana kohdan 7.3.4 vaatimusten täyttämistä,

- a) mikäli varmennepolitiikka ei koske yleistä käyttöä ja sovelletaanko kohdassa 8.2 mainittuja poikkeuksia

- b) mikäli varmennepolitiikka sisältää vaatimuksia turvallisen allekirjoituksen luomisvälineen käytöstä
- c) millä tavoin kyseinen politiikka lisää tai tiukentaa tässä asiakirjassa määritellyn laatuvarmennepolitiikan vaatimuksia.

8.4 Vaatimustenmukaisuus

Varmentaja saa ilmaista toimivansa tämän asiakirjan ja sovellettavan laatuvarmennepolitiikan mukaisesti vain,

- a) jos varmentaja ilmaisee noudattavansa yksilöityä laatuvarmennepolitiikkaa ja asettaa pyynnöstä tilaajan ja varmenteeseen luottavien osapuolten saataville todisteita vaatimustenmukaisuudesta tai

HUOMAUTUS 1: Selvityksenä voi olla esimerkiksi auditoijan kertomus, jossa vahvistetaan varmentajan noudattavan yksilöidyn laatuvarmennepolitiikan vaatimuksia. Kyseessä voi olla varmentajan organisaation sisäinen auditoija, mutta auditoija ei saa olla hierarkkisessa suhteessa varmentajan toimintaa toteuttavaan osastoon.

- b) jos pätevä ja riippumaton osapuoli on hiljattain arvioinut yksilöidyn laatuvarmennepolitiikan vaatimusten noudattamisen nykytilaa varmentajalla. Arviointitulokset on asetettava pyynnöstä tilaajien ja varmenteeseen luottavien osapuolten saataville

HUOMAUTUS 2: Arviointi voidaan toteuttaa direktiivin 3 artiklan 2 kohdassa [1] määritellyn "vapaaehtoisuuteen perustuvan akkreditointijärjestelmän" mukaisesti tai se voi olla pätevän ja riippumattoman auditoijan suorittama muunlainen arviointi. Katso vaatimustenmukaisuuden arviointia koskeva CEN-työryhmän sopimus 14172 "EESSI Conformity Assessment Guidance".

- c) jos myöhemmin osoitetaan, että varmentaja on laiminlyönyt varmennepolitiikan noudattamisen ja että tämä vaikuttaa merkittävästi varmentajan kykyyn täyttää direktiivissä [1] määritellyt laatuvarmenteita koskevat vaatimukset, varmentajan on lopetettava kyseiseen laatuvarmennepolitiikkaan viittaavien varmenteiden myöntäminen, kunnes se on osoittanut vaatimustenmukaisuutensa tai kunnes sen on arvioitu noudattavan kyseisen laatuvarmennepolitiikan vaatimuksia; muussa tapauksessa varmentajan on ryhdyttävä kohtuullisen ajan kuluessa toimenpiteisiin vaatimustenmukaisuutta koskevan laiminlyönnin korjaamiseksi

HUOMAUTUS 3: Vaikka varmentajan tiedettäisiin laiminlyövä ratkaisevalla tavalla varmennepolitiikan noudattamista, varmentaja saa kuitenkin myöntää varmenteita sisäisiin ja testaustarkoituksiin, kunhan kyseisiä varmenteita ei aseteta saataville mitään muuta käyttöä varten.

- d) varmentajan vaatimustenmukaisuus on tarkistettava säännöllisesti sekä aina, kun varmentajan toimintaa muutetaan merkittävästi.

HUOMAUTUS 4: Vaatimustenmukaisuuden osoittamiseen vaadittavat keinot voivat vaihdella varmentajan sijoittautumisvaltion lainsäädännön mukaan.

Vaatimusten mukaisen varmentajan on osoitettava, että

- a) se täyttää sille kohdassa 6.1 määritellyt vaatimukset
- b) se on ottanut käyttöön hallintakeinot, jotka täyttävät kaikki kohdassa 7 esitetyt vaatimukset, lukuun ottamatta seuraavia:
 - c) kohta 7.2.9, mikäli varmentaja ei edellytä turvallisen allekirjoituksen luomisvälineen käyttöä
 - d) kohdan 8.2 vaatimukset, mikäli varmentaja ei tarjoa palvelua yleisölle
 - e) noudattaa kohdan 8.1 vaatimukset täyttävää laatuvarmennepolitiikkaa
 - f) on ottanut käyttöön hallintakeinot, jotka täyttävät kaikki käytettäviä laatuvarmennepolitiikkoja koskevat lisävaatimukset
 - g) täyttää kohdassa 8.3 määritellyt lisävaatimukset.

Liite A (tiedoksi):**Sähköisten allekirjoitusten käyttöön liittyvä mahdollinen vastuu**

Tässä liitteessä käsitellään sähköisiä allekirjoituksia koskevan direktiivin [1] mukaisia laatuvarmenteita myöntäville ja käyttäville eri toimijoille mahdollisesti lankeavaa vastuuta.

Yleisölle laatuvarmenteita myöntäviä varmentajia (tai direktiivin [1] sanatarkan ilmaisun mukaisesti "yleisölle hyväksytyjä varmenteita myöntäviä varmennepalvelujen tarjoajia") koskevat vastuuvaatimukset esitetään direktiivissä [1] seuraavasti:

Direktiivin 6 artikla **Vastuu**

1. Jäsenvaltioiden on varmistettava ainakin se, että myöntämällä yleisölle varmenteita laatuvarmenteina tai takaamalla yleisölle varmenteen varmennepalvelun tarjoaja on vastuussa varmenteeseen perustellulla tavalla tukeutuvalla yhteisölle taikka oikeushenkilölle tai luonnolliselle henkilölle aiheutuvasta vahingosta seuraavien seikkojen osalta:
 - a) laatuvarmenteessa olevien tietojen paikkansapitävyys sen myöntämisaikana ja kaikkien laatuvarmenteessa ilmoitettavien tietojen sisältyminen varmenteeseen;
 - b) varmuus siitä, että laatuvarmenteessa yksilöidyllä henkilöllä oli varmenteen myöntämisaikana hallussaan allekirjoituksen luomiseen käytettävät tiedot, jotka vastaavat varmenteessa mainittuja tai määriteltäviä allekirjoituksen todentamiseen käytettäviä tietoja; ja
 - c) varmuus siitä, että allekirjoituksen luomiseen käytettäviä tietoja ja allekirjoituksen todentamiseen käytettäviä tietoja voidaan käyttää toisiaan täydentävästi, silloin kun varmennepalvelujen tarjoaja on luonut ne molemmat,

jollei varmennepalvelujen tarjoaja pysty todistamaan, ettei hän ole toiminut huolimattomasti.
2. Jäsenvaltioiden on varmistettava ainakin se, että varmennepalvelujen tarjoaja, joka on myöntänyt yleisölle varmenteita laatuvarmenteina, on varmenteen peruuttamista koskevan merkinnän tekemättä jättämisen johdosta vastuussa varmenteeseen perustellulla tavalla tukeutuvalla yhteisölle taikka oikeushenkilölle tai luonnolliselle henkilölle aiheutuvasta vahingosta, jollei varmennepalvelujen tarjoaja pysty todistamaan, ettei hän ole toiminut huolimattomasti.
3. Jäsenvaltioiden on varmistettava, että varmennepalvelujen tarjoajilla on mahdollisuus ilmoittaa laatuvarmenteessa kyseisen varmenteen käyttöä koskevista rajoituksista edellyttäen, että tällaiset rajoitukset ovat kolmansien osapuolten tunnistettavissa. Varmennepalvelujen tarjoaja ei ole vastuussa vahingosta, joka on aiheutunut laatuvarmenteen käytöstä siinä annettujen käyttörajoitusten vastaisesti.
4. Jäsenvaltioiden on varmistettava, että varmennepalvelujen tarjoajilla on laatuvarmenteessa mahdollisuus ilmoittaa niiden toimien arvoa koskeva rajoitus, joihin varmennetta voidaan käyttää, edellyttäen, että tällaiset rajoitukset ovat kolmansien osapuolten tunnistettavissa. Varmennepalvelujen tarjoaja ei ole vastuussa vahingosta, joka aiheutuu siitä, että tämä enimmäisrajoitus ylitetään.

Varmentaja voidaan katsoa yleisölle varmenteita myöntäväksi, jos kyseisten varmenteiden käyttöä ei ole rajoitettu osanottajien välisin vapaaehtoisin yksityisoikeudellisin sopimuksin.

Useimmissa tapauksissa vastuu määräytyy kansallisessa lainsäädännössä, joka vaihtelee EU:n eri jäsenvaltioissa. Vaikka vastuusta säädetään sähköisiä allekirjoituksia koskevassa direktiivissä (jäljempänä "direktiivi" [1]), on viitattava jäsenvaltion vastuusäännösten täytäntöönpanoon kyseisessä jäsenvaltiossa. Varmennepalvelujen tarjoamista harkitsevien yhteisöjen kannattaakin käyttää paikallista neuvonta-apua mahdollisten vastuukohtien selvittämiseen kaavailemissaan toimintamaisissa. On syytä huomata, että joissain tapauksissa, etenkin suljettujen järjestelmien yhteydessä, vastuusta määrätään sopimuksessa, joka laaditaan varmentajan sekä varmennetta käyttävien ja siihen luottavien osapuolten välille.

I) Varmentajan vastuu**A) Direktiivin [1] alainen varmentajien vastuu varmenteeseen luottaviin osapuoliin nähden**

Direktiivissä vastuun käsitteleminen alkaa johdanto-osan kappaleesta 22, jonka mukaisesti "yleisölle suunnattuja varmennepalveluja tarjoavat varmennepalvelujen tarjoajat kuuluvat kansallisten vastuusääntöjen piiriin". Näin ollen varmentajan vastuuseen sovelletaan jäsenvaltion lainsäädäntöä.

Direktiivin 6 artiklassa [1] edellytetään, että jäsenvaltiot sisällyttävät kansalliseen lainsäädäntöön ainakin tietyt vastuusäännökset. Näitä säännöksiä sovelletaan yleisölle laatuvarmenteita myöntäviin varmentajiin. Niitä ei sovelleta varmentajiin, jotka toimivat suljetuissa järjestelmissä tai myöntävät muita kuin laatuvarmenteita. Erityisesti 6 artiklassa edellytetään, että yleisölle laatuvarmenteita myöntävä varmentaja varmistaa seuraavat seikat:

- varmenteessa olevien tietojen paikkansapitävyys sen myöntämisajankohtana
- kaikkien laatuvarmenteessa ilmoitettavien tietojen sisältyminen varmenteeseen sen myöntämisajankohtana
- että varmenteessa yksilöidyllä henkilöllä on hallussaan allekirjoituksen luomiseen käytettävät tiedot, jotka vastaavat varmenteessa määriteltäviä allekirjoituksen todentamiseen käytettäviä tietoja
- että allekirjoituksen luomiseen käytettävät tiedot ja allekirjoituksen todentamiseen käytettävät tiedot toimivat yhdessä, silloin kun varmennepalvelujen tarjoaja on luonut ne molemmat
- että se kirjaa varmenteen mahdollisen peruuttamisen.

Varmentaja on vastuussa vahingoista, jotka aiheutuvat näiden velvollisuuksien laiminlyömisestä, paitsi jos varmentaja ei ole toiminut huolimattomasti (tämä riippuu sen kyvystä rajoittaa vastuutaan, kuten jäljempänä esitetään). Toisin sanoen vastuuvelite perustuu siihen, että varmentaja tekee virheen ja että kyseinen virhe johtuu varmentajan huolimattomuudesta. (Direktiivissä käytetyllä rakenteella ilmaistaan, että vastuusäännökset ulottuvat myös varmentajan piittaamattomuuteen ja tarkoituksellisiin väärinkäytöksiin.) Vastuun välttämiseksi varmentajan onkin todistettava vain, että sen oma toiminta ei ollut huolimaton. Varmenteeseen luottavan osapuolen laiminlyönneistä – kuten sulkulistan tarkistamatta jättämisestä – ei pitäisi seurata vastuuvelitettä varmentajalle. Tällöin onkin mahdollista, että varmenteeseen luottavan osapuolen luottamus varmenteeseen voidaan sen omien laiminlyöntien vuoksi katsoa perusteettomaksi, jolloin varmentaja direktiivin mukaisesti vapautuu vastuusta.

Jäsenvaltioiden tuomioistuimet tukeutuvat usein alan standardeihin määritellään, onko tietty toiminta huolimaton. Alan standardin noudattaminen, esimerkiksi tässä asiakirjassa määritettyjen menettelytapavaatimusten noudattaminen, ei kuitenkaan todista sitovasti, että varmentaja olisi täyttänyt huolellisuusvelvollisuutensa. Useimmissa jäsenvaltioissa standardien noudattamista kuitenkin pidetään alustavana näyttönä siitä, ettei varmentaja ole huolimaton. Vastaavasti alan standardin, esimerkiksi tämän asiakirjan, noudattamatta jättäminen voidaan useimmissa jäsenvaltioissa katsoa alustavaksi näytöksi huolimattomuudesta.

Direktiivin [1] mukaan varmentajat saavat rajoittaa vastuutaan rajoittamalla varmenteen käyttöä sekä niiden toimien arvoa, joihin varmennetta voidaan käyttää. Tällaiset rajoitukset on tärkeää esittää huomion kiinnittävällä tavalla, tai muutoin ne voidaan katsoa pätemättömiksi kuluttajansuojalainsäädännön tai yleisen sopimuslainsäädännön nojalla. Tällaiset rajoitukset on asetettava myös suljetuissa järjestelmissä käytettäviin varmenteisiin, jotteivät ne pääsisi "vuotamaan" muihin käyttöympäristöihin.

On huomattava, että koska vastuuta rajoitetaan toimien perusteella ja koska varmentaja ei ehkä kykene hallitsemaan niiden toimien määrää, joista se joutuu vastuuseen, varmentajan kokonaisvastuu ei mahdollisesti ole sen hallittavissa.

Vahingoista säädetään jäsenvaltion lainsäädännössä. Huolimattomuudesta voi seurata vahinkovastuu, mutta tällöin menetyksen syynä on yleensä oltava huolimattomuus. Esimerkiksi jos varmentaja huolimattomuuttaan ei julkaise sulkulistaa oikea-aikaisesti, mutta varmenteeseen luottava osapuolikaan ei tarkista sulkulistan olemassaoloa, ei varmenteeseen luottavan osapuolen kärsimän menetyksen lainmukaisena syynä todennäköisesti pidetä varmentajan huolimattomuutta vaan varmenteeseen luottavan osapuolen tarkistamatta jättämistä. Jos varmenteeseen luottava osapuoli olisi tehnyt tarkistuksen, se olisi huomannut sulkulistan olevan vanhentunut ja toiminut sen mukaisesti. Tulkinta ei kuitenkaan ole yhtä selvää silloin, jos varmentaja huolimattomuuttaan julkaisee paikkansapitämättömän sulkulistan, jota varmenteeseen luottava osapuoli ei tarkista. Tällaisessa tapauksessa varmentaja voi vedota siihen, että menetyksen syynä oli varmenteeseen luottavan osapuolen tarkistuksen laiminlyönti, sillä kyseisen osapuolen ei ollut perusteltua luottaa varmenteeseen, jota se ei ollut tarkistanut. Varmenteeseen luottava osapuoli sen sijaan voi esittää, ettei tarkistamatta jättäminen vaikuttanut menetyksen syntymiseen, sillä osapuoli ei olisi tarkistamallakaan voinut saada varmenteen peruuttamista tietoonsa.

B) Direktiivin [1] ulkopuolinen varmentajien vastuu varmenteeseen luottaviin osapuoliin nähden

Jos varmentaja ei kuulu direktiivissä [1] määritellyn vastuujärjestelmän piiriin, koska se ei myönnä laatuvarmenteita tai ei myönnä niitä yleisölle, vastuu määräytyy yleensä yhden tai kahden lähteen mukaan: sopimusoikeuden tai säädännäisoikeuden mukaan. Suljettujen järjestelmien osalta varmentaja on todennäköisesti sopimussuhteessa

varmenteeseen luottavaan osapuoleen. Tällöin vastuukysymyksistä määrätään ensisijaisesti asiaa koskevassa sopimuksessa. Jos asiaan liittyy kuluttajia, saatetaan soveltaa myös lakisäateistä kuluttajansuojaa. Avoimissa järjestelmissä on mahdollista, että varmenteeseen luottava osapuoli määritetään tilaajan ja varmentajan väliseen sopimukseen kolmantena osapuolena olevaksi edunsaajaksi. Tällöin varmentajan vastuusta varmenteeseen luottavaan osapuoleen nähden määrätään varmentajan ja tilaajan sopimuksessa. Se, syntyykö sopimuksesta vastuuvaikeuksia kolmansille osapuolille, saattaa määräytyä sopimuksen tulkinnasta sovellettavan oikeuskäytännön ja oikeudellisten säännösten mukaan. Jos varmentajan ja tilaajan välisessä sopimuksessa varmenteeseen luottavaa osapuolta ei määritetä kolmantena osapuolena olevaksi edunsaajaksi, varmentajan vastuu kolmansiin osapuoliin nähden määräytyy tällöin ainoastaan kansallisen oikeuden mukaisesti.

C) Varmentajien vastuu tilaajiin nähden

Varmentajan vastuusta tilaajaan nähden palvelun tarjoamisen laiminlyönnin yhteydessä (esimerkiksi jos sulku listoja ei julkaista oikea-aikaisesti) tai epäasianmukaisen varmenteen peruuttamisen tai keskeytystilaan asettamisen yhteydessä määrätään varmentajan ja tilaajan välisessä sopimuksessa. Jos tilaaja on kuluttaja, sovelletaan kuluttajasopimusten kohtuuttomia ehtoja koskevaa direktiiviä 93/13/ETY [12] sekä kuluttajansuojasta etäsopimuksissa annettua direktiiviä 97/7/EY (katso Lähdekirjallisuus), jotka rajoittavat varmentajan mahdollisuuksia rajoittaa vastuutaan. Kuluttajasopimusten kohtuuttomia ehtoja koskeva direktiivi kieltää ehdot, joista ei ole erikseen neuvoteltu ja jotka aiheuttavat kuluttajan vahingoksi huomattavan epätasapainon osapuolten oikeuksien ja velvollisuuksien välille. Kuluttajansuojaa etäsopimuksissa koskevaa direktiiviä sovelletaan, kun elinkeinonharjoittaja ja kuluttaja eivät tapaa henkilökohtaisesti sopimuksen syntyessä.

Jos varmentaja sai tilaajan tilaamaan katteettomin lupauksin, se saattaa joutua vastuuseen tilaajaan nähden petoslainsäädännön nojalla. Todennäköisesti petosväite kuitenkin vaatii tuekseen todisteita varmentajan syyllistymisestä tahalliseen rikkomukseen. Koska ala on osittain säännelty, joissakin jäsenvaltioissa varmentajille saatetaan asettaa suurempi huolellisuus- tai luottamusvelvollisuus vastaavasti kuin lääkäreille tai asianajajille. Tapaoikeudessa tai säädöksissä voi tällöin esiintyä muutoksenhakukeino, vastaavasti kuin hoitovirheen yhteydessä, mikäli varmentaja toimii huolimattomasti täyttäessään tilaajaan kohdistuvia velvollisuuksiaan.

Varmentajat asetetaan vastuuseen tilaajiin nähden myös, jos varmentajat eivät noudata tietosuojalakeja, jotka on säädetty tietosuojadirektiivin (95/46/EY [4]) ja sähköisiä allekirjoituksia koskevan direktiivin 8 artiklan [1] täytäntöönpanemiseksi. Tällöin varmentajia saatetaan vaatia luovuttamaan henkilötietoja viranomaisille, etenkin mikäli tilaaja käyttää salanimeä.

D) Varmentajien vastuu riippumattomiin kolmansiin osapuoliin nähden

Varmentaja voi joutua vastuuseen riippumattomaan kolmanteen osapuoleen nähden, mikäli varmentaja myöntää tilaajalle varmenteen kyseisen kolmannen osapuolen nimissä. Tällöin vastuu ei määräydy direktiivin mukaan, koska kyseinen riippumaton kolmas osapuoli ei ole tukeutunut varmenteeseen perustellulla tavalla. Vastuu ei myöskään määräydy sopimusoikeuden mukaan, koska varmentajan ja kyseisen kolmannen osapuolen välillä ei ole sopimusta. Jäsenvaltiot ovat kuitenkin saattaneet säätää säädännäisoikeudessa tai vahingonkorvauslaissa tällaisia vahinkoja koskevista muutoksenhakukeinoista, esimerkiksi kanteista henkilötietovarokautta avustanutta henkilöä vastaan. Tällaisissa tilanteissa vastuu todennäköisesti perustuu varmentajan huolimattomuuteen tai tahalliseen rikkomukseen. Joissakin oikeusjärjestelmissä saatetaan kuitenkin asettaa ankara vastuu, mikäli varmenteita myönnetään tilaajalle riippumattoman kolmannen osapuolen nimissä.

II) Tilaajien vastuu

A) Tilaajan vastuu varmentajaan nähden

Tilaajan mahdollisesta vastuusta varmentajaan nähden silloin, jos tilaaja antaa vääriä, harhaanjohtavia tai paikkansapitämättömiä tietoja, määrätään tilaajan ja varmentajan välisessä sopimuksessa. Jos tilaaja on tarkoituksellisesti antanut vääriä tai harhaanjohtavia tietoja, se saattaa joutua petoslainsäädännön nojalla vastuuseen varmentajaan nähden.

B) Tilaajan vastuu varmenteeseen luottavaan osapuoleen nähden

Tilaajan mahdollisesta vastuusta varmenteeseen luottavaan osapuoleen nähden silloin, jos tilaaja antaa vääriä, harhaanjohtavia tai paikkansapitämättömiä tietoja varmentajalle ja tämän seurauksena myönnetään varmenteen, johon varmenteeseen luottava osapuoli luottaa, määrätään tilaajan ja varmenteeseen luottavan osapuolen välisessä sopimuksessa. Jos tilaaja on tarkoituksellisesti antanut vääriä tai harhaanjohtavia tietoja, se saattaa joutua petoslainsäädännön nojalla vastuuseen varmenteeseen luottavaan osapuoleen nähden. Tilaaja on myös vastuussa nimenomaisen tai hiljaisen valtuutuksen nojalla toimivan edustajansa toimista. Joissakin olosuhteissa tilaaja voi joutua vastaamaan edustajan toimista myös silloin, jos edustajalla on asemavaltuus perustuen siihen, millaisena tilaaja näyttäytyy varmenteeseen luottavalle osapuolelle.

C) Tilaajan vastuu riippumattomaan kolmanteen osapuoleen nähden

Tilaaajan vastuusta riippumattomaan kolmanteen osapuoleen nähden silloin, jos tilaaajan varmentajalle antamien tietojen johdosta tilaajalle myönnetään varmenne kolmannen nimissä, säädetään jäsenvaltion säädännäisoikeudessa tai vahingonkorvaus- tai petoslainsäädännössä. Useimmissa tapauksissa yritys tekeytyä kolmanneksi osapuoleksi on tarkoituksellista ja näin ollen siitä voidaan nostaa petosta koskeva kanne. Jäsenvaltioissa on mahdollisesti myös säädetty henkilötietovarkauksia koskevia säädännäis- tai tapaoikeuteen perustuvia muutoksenhakukeinoja.

Liite B (tiedoksi): Varmennekuvauksen malli

B.1 Johdanto

Oheinen varmennekuvauksen malli on suunniteltu tiedottamisen lisätyökaluksi varmenteita myöntävälle varmentajalle. Varmennekuvaus helpottaa varmentajaa täyttämään säädösten vaatimukset, vastaamaan etenkin käyttöönottoon liittyviin kuluttajan huoliin sekä täyttämään erityisesti direktiivin [1] liitteen II vaatimukset. Lisäksi varmennekuvauksen mallin tarkoituksena on edistää alan sisäistä sääntelyä ja saada aikaan yhteisymmärrystä siitä, mitä varmennepolitiikan ja/tai varmennuskäytännön osa-alueita on syytä painottaa ja mistä on syytä tiedottaa.

Kirjalliset varmennepolitiikat ja varmennuskäytäntö ovat tärkeitä asiakirjoja varmennepolitiikojen ja käytäntöjen kuvaamisen ja hallinnan kannalta, mutta ne ovat julkisen avaimen järjestelmän käyttäjien, etenkin kuluttajien, mielestä usein vaikeaselkoisia. Näin ollen tarvitaan yksinkertaisempi lisäapuväline, jonka avulla julkisen avaimen järjestelmän käyttäjät voivat tehdä valistuneita luottamuspäätöksiä. Varmennekuvauksen tarkoituksena ei siis ole korvata varmennepolitiikkaa eikä varmennuskäytäntöä.

Tässä liitteessä annetaan esimerkki varmennekuvauksen rakenteesta. Käyttöön otettavan varmennekuvauksen ehdotetaan sisältävän yhdenmukaiset aihealueet (luokat).

B.2 Varmennekuvauksen rakenne

Varmennekuvauksessa käsitellään kutakin määriteltyä aihealuetta omassa kohdassaan. Kussakin varmennekuvauksen kohdassa annetaan kuvaus, joka voi sisältää hyperlinkin asiaa koskevaan varmennepolitiikan tai varmennuskäytännön osioon.

Taulukko B.1

Aihealue	Aihealueen kuvaus	Laatuvarmennepolitiikassa määritellyt erityisvaatimukset (katso kohta 7.3.4)
Varmentajan yhteystiedot:	Varmentajan tai julkisen avaimen järjestelmän nimi, sijainti ja riittävät yhteystiedot.	
Varmenteen tyyppi, tarkistamismenettelyt ja käyttötarkoitukset:	Kuvataan kaikkien varmentajan myöntämien varmenteiden tyyppi/luokka, varmenteisiin liittyvät tarkistamismenettelyt sekä mahdolliset käyttötarkoitusten rajoitukset.	Mahdolliset varmenteen käyttötarkoituksen rajoitukset Koskeeko politiikka yleisölle myönnettäviä laatuvarmenteita.
Varmenteeseen luottamisen rajoitukset:	Kuvataan mahdolliset luottamista koskevat rajoitukset.	Ilmoitetaan, että varmennetta saa käyttää sähköisten allekirjoitusten yhteydessä vain rekisteröintitietojen ja varmentajan tapahtumalokien (katso kohta 7.4.11) säilytysajan (ja kyseiset tiedot ja lokit ovat näin ollen saatavilla asiaa koskevien todisteiden esittämiseksi).
Tilaaajien velvollisuudet:	Tilaaajan kriittisten velvollisuuksien kuvaus tai viittaus niihin.	Tilaaajan kohdassa 6.2. määritellyn mukaiset velvollisuudet, myös edellytetäänkö varmennepolitiikassa turvallisen allekirjoituksen luomisvälineen käyttöä.
Varmenteeseen luottavan osapuolen varmenteen tilan tarkistamiseen liittyvät velvollisuudet:	Kuvataan, missä määrin varmenteeseen luottavat osapuolet ovat velvollisia tarkistamaan varmenteen tilan, ja viitataan lisätietoihin.	Tieto siitä, miten varmenne tarkistetaan. Tähän sisältyy vaatimukset varmenteen sulkutilan tarkistamisesta, jotta varmenteeseen luottavan osapuolen voidaan katsoa "luottavan perustellulla tavalla" varmenteeseen (katso kohta 6.3).
Rajoitettu takuu ja vastuuvapauslauseke tai vastuunrajoitus:	Tiivistelmä takuusta, vastuuvapauslausekkeista, vastuunrajoituksista ja kaikista mahdollisesti sovellettavista takuista ja vakuutusjärjestelyistä.	Vastuunrajoitukset (katso kohta 6.4).

Aihealue	Aihealueen kuvaus	Laatuvarmennepolitiikassa määritellyt erityisvaatimukset (katso kohta 7.3.4)
Varmenteeseen sovellettavat sopimukset ja varmennuskäytäntö:	Yksilöidään sovellettavat sopimukset, varmennuskäytäntö, varmennepolitiikka ja muut asiaan liittyvät asiakirjat ja annetaan viitteet niihin.	Sovellettava laatuvarmennepolitiikka.
Yksityisyyden suoja:	Kuvataan yksityisyyden suojaan sovellettavaa käytäntöä ja annetaan viite siihen.	Katso huomautus.
Korvauskäytäntö:	Kuvataan korvauksiin sovellettavaa käytäntöä ja annetaan viite siihen.	
Sovellettava lainsäädäntö, valitusten ja riitojen ratkaiseminen:	Annetaan lakiviittaus ja kerrotaan valitusmenettelystä ja riitojenratkaisumenettelyistä (tässä viitattaneen usein Kansainvälisen kauppakamarin ICC:n sovittelupalveluihin).	Valitusten ja riitojen ratkaisemiseen käytettävät menettelyt. Sovellettava oikeusjärjestelmä.
Varmentajan ja tallennuspaikkojen käyttöoikeudet, luotettavuusmerkinnät ja auditointi:	Tiivistelmä mahdollisista julkishallinnon käyttöoikeuksista ja sinettiohjelmista, kuvaus auditointimenettelyistä ja tarvittaessa auditoinnin tekevästä yhtiöstä.	Ilmaistava, onko varmentaja todistettu yksilöidyn laatuvarmennepolitiikan vaatimusten mukaiseksi ja millä arviointijärjestelmällä tämä on todettu.
HUOMAUTUS:	Näitä menettelytapoja noudattavien varmentajien on noudatettava tietoturvalainsäädännön vaatimuksia.	

**Liite C (tiedoksi):
Sähköisiä allekirjoituksia koskevan direktiivin ja laatuvarmennepolitiikan väliset ristiviittaukset**

Taulukossa C.1 esitetään, miten tässä asiakirjassa määritellyt turvallisuuden hallintakeinoja koskevat tavoitteet ja muut laatuvarmennepolitiikkojen osat vastaavat direktiivin [1] liitteessä II laatuvarmenteita myöntäville varmentajille säädettyjä vaatimuksia.

Taulukko C.1

Direktiivin liitteen II vaatimus	Viittaus laatuvarmennepolitiikkaan
a) osoitettava varmennepalvelujen tarjoamisen edellyttämä luotettavuus	Kohdat 7.1, 7.4.8, 7.4.9 ja 7.5
b) varmistettava nopea ja varma hakemistopalvelu sekä luotettava ja viivytyksetön peruuttamismahdollisuus	Kohdat 7.3.5, 7.3.6 ja 7.4.6 (k)
c) varmistettava, että varmenteen myöntämisen tai peruuttamisen päivämäärä ja aika voidaan määrittää tarkasti	Kohta 7.4.11 (d)
d) todennettava tarkoituksenmukaisin keinoin kansallisen lainsäädännön mukaisesti sen henkilön henkilöllisyys ja tarvittaessa tietyt erityismäärät, jolle laatuvarmenne on myönnetty	Kohdat 7.3.1 ja 7.3.2
e) pidettävä palveluksessaan henkilökuntaa, jolla on tarjottujen palvelujen edellyttämä asiantuntemus, kokemus ja pätevyys varsinkin johtotehtävissä toimivien osalta, sähköisten allekirjoitusten tekniikoihin liittyvä asiantuntemus ja tarkoituksenmukaisten turvatoimien tuntemus; palvelujen tarjoajien on lisäksi noudatettava asianmukaisia ja tunnustettujen standardien mukaisia hallinnollisia ja liikkeenjohdollisia menettelytapoja	Kohdat 7.4.1, 7.4.3 ja 7.4.5
f) käytettävä luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutoksilta ja joilla varmistetaan tuotteiden tukemien prosessien turvallisuus niin tekniikan kuin salaamisen osalta	Kohdat 7.4.6, 7.4.7, 7.2.1, 7.2.2 ja 7.2.8
g) toteutettava toimenpiteet varmenteiden väärentämisen ehkäisemiseksi ja, silloin kun varmennepalvelun tarjoaja luo allekirjoituksen luomiseen käytettävät tiedot, taattava luottamuksellisuus kyseisiä tietoja luotaessa	Kohdat 7.2.2, 7.2.3, 7.2.8, 7.3.1, 7.3.2 ja 7.3.3
h) hallittava tämän direktiivin vaatimusten mukaisen toiminnan edellyttämiä varoja varsinkin vahinkovastuiden kattamiseksi, esimerkiksi asianmukaisella vakuutuksella	Kohta 7.5 (d, e)
i) arkistoitava kaikki asiaankuuluvat laatuvarmennetta koskevat tiedot tarkoituksenmukaiseksi ajaksi erityisesti voidakseen esittää varmentamista koskevia todisteita oikeudellisissa menettelyissä. Tällaisia arkistoja voidaan ylläpitää sähköisessä muodossa	Kohdat 7.4.11 ja 7.4.9
j) oltava tallentamatta tai jäljentämättä varmennepalvelujen tarjoajalta salausavaimen hallintapalveluja saaneen henkilön allekirjoituksen luomiseen käytettäviä tietoja	Kohta 7.2.8
k) ennen ryhtymistä sopimussuhteeseen sähköiselle allekirjoitukselleen varmennusta hakevan henkilön kanssa ilmoitettava kyseiselle henkilölle tiedon säilyttävää viestintämuotoa käyttäen varmenteen käytön tarkoista ehdoista ja edellytyksistä, mukaan lukien sen käyttörajoitukset, vapaaehtoisuuteen perustuvan akkreditointijärjestelmän olemassaolosta sekä valitus- ja riitojenratkaisumenettelyistä. Nämä tiedot, jotka voidaan toimittaa sähköisesti, on annettava kirjallisesti ja selvästi ymmärrettävällä kielellä. Näiden tietojen olennaisten kohtien on lisäksi pyynnöstä oltava varmenteeseen tukeutuvien kolmansien osapuolien saatavilla	Kohdat 7.3.1 ja 7.3.4
l) käytettävä luotettavia järjestelmiä varmenteiden tallentamiseen todennettavassa muodossa siten, että - ainoastaan valtuutetut henkilöt voivat syöttää tietoja ja tehdä niihin muutoksia, - tietojen aitous voidaan tarkistaa, - yleisöllä on oikeus tehdä varmenteita koskevia hakuja vain silloin, kun varmenteen haltijalta on saatu lupa, ja - että näitä turvallisuusvaatimuksia vaarantavat tekniset muutokset ovat operaattorin nähtävissä.	Kohdat 7.2.3, 7.3.5, 7.3.6, 7.4.6 ja 7.4.7

**Liite D (tiedoksi):
IETF RFC 3647/RFC 2527 -julkaisujen ja laatuvarmenteita koskevien menettelytapavaatimusten väliset ristiviittaukset**

HUOMAUTUS: Tämä asiakirja ja RFC 3647 -julkaisu [2] ovat rakenteeltaan erilaiset, ja joissakin kohdin RFC 3647 [2] sisältää enemmän yksityiskohtia. Yksi tämän asiakirjan kohta voi liittyä useisiin RFC 3647 - julkaisun [2] osioihin.

Taulukko D.1: RFC 3647 -julkaisun [2] osioiden ja menettelytapavaatimusten väliset ristiviittaukset

	RFC 3647 -julkaisun [2] osio	Tämän asiakirjan kohta
1	INTRODUCTION (Johdanto)	
1.1	Overview (Yleistä)	Kohta 5.1
1.2	Document name and identification (Asiakirjan nimi ja yksilöinti)	Kohta 5.2
1.3	PKI participants (Julkisen avaimen järjestelmän osapuolet)	Kohta 5.3, kohdan 7 johdantoteksti
1.4	Certificate usage (Varmenteen käyttötarkoitus)	Kohta 5.3
1.5	Policy administration (Varmennepoliitikan hallinta)	ETSI, katso alkusivut
1.5.1	Organization administering the document (Asiakirjaa hallinnoiva organisaatio)	ETSI
1.5.2	Contact person (Yhteyshenkilö)	Katso alkusivut
1.5.3	Person determining CPS suitability for the policy (Henkilö, joka määrittää varmennuskäytännön soveltuvuuden varmennepoliitikkaan)	Kohta 7.1
1.5.4	CPS approval procedures (Varmennuskäytännön hyväksymismenettelyt)	Kohta 7.1
1.6	Definitions and acronyms (Määritelmät ja lyhenteet)	Kohta 3
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES (Julkaisemista ja tallennuspaikkoja koskevat vastuut)	
2.1	Repositories (Tallennuspaikat)	Kohta 7.3.5
2.2	Publication of certification information (Varmennustietojen julkaisu)	Kohdat 7.3.5, 7.3.6 ja 7.3.4
2.3	Time or frequency of publication (Julkaisu aika tai -tiheys)	Kohdat 7.3.5 ja 7.3.6
2.4	Access controls on repositories (Tallennuspaikkoihin pääsyn valvontakeinot)	Kohta 7.4.6
3	IDENTIFICATION AND AUTHENTICATION (Tunnistaminen ja todentaminen)	
3.1	Naming (Nimeäminen)	Kohta 7.3.3
3.2	Initial identity validation (Henkilöllisyyden tarkistaminen aluksi)	Kohta 7.3.1
3.3	Identification and authentication for re-key requests (Tunnistaminen ja todentaminen varmenteen julkisen avaimen vaihtamista koskevien pyyntöjen yhteydessä)	Kohta 7.3.2
3.4	Identification and authentication for revocation request (Tunnistaminen ja todentaminen peruuttamispyynnön yhteydessä)	Kohta 7.3.6
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (Varmenteen elinkaarta koskevat toimintavaatimukset)	
4.1	Certificate Application (Varmennehakemus)	Kohta 7.3.1
4.2	Certificate application processing (Varmennehakemuksen käsittely)	Kohta 7.3.3
4.3	Certificate issuance (Varmenteen myöntäminen)	Kohta 7.3.3
4.4	Certificate acceptance (Varmenteen hyväksyminen)	Kohta 7.3.1
4.5	Key pair and certificate usage (Avainparin ja varmenteen käyttötarkoitus)	Kohdat 6.2 ja 6.3
4.6	Certificate renewal (Varmenteen uusiminen)	Kohta 7.3.2
4.7	Certificate re-key (Varmenteen avainparin vaihtaminen)	Kohta 7.3.2
4.8	Certificate modification (Varmenteen muokkaaminen)	Kohta 7.3.2
4.9	Certificate revocation and suspension (Varmenteen peruuttaminen ja asettaminen keskeytystilaan)	Kohta 7.3.6
4.10	Certificate status services (Varmenteen tilapalvelut)	Kohta 7.3.6
4.11	End of subscription (Tilauksen päättäminen)	
4.12	Key escrow and recovery (Vara-avainjärjestelmä ja avainten palauttaminen)	Kohta 7.2.4
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS (Tiloja, johtamista ja toimintaa koskevat hallintakeinot)	
5.1	Physical controls (Fyysiset hallintakeinot)	Kohdat 7.4.1, 7.4.4 ja 7.4.5
5.2	Procedural controls (Menettelyiden hallintakeinot)	Kohdat 7.4.5, 7.4.3 ja 7.4.6
5.3	Personnel controls (Henkilöstön hallintakeinot)	Kohta 7.4.3
5.4	Audit logging procedures (Auditointilokeja koskevat menettelyt)	Kohta 7.4.11
5.5	Records archival (Tietojen arkistointi)	Kohta 7.4.11
5.6	Key changeover (Varmentajan avainparin vaihtaminen)	Kohta 7.2
5.7	Compromise and disaster recovery (Toipuminen vaarantumis- ja hätätilanteista)	Kohta 7.4.8

5.8	CA or RA termination (Varmentajan tai rekisteröijän toiminnan päätyminen)	Kohta 7.4.9
6	TECHNICAL SECURITY CONTROLS (Turvallisuuden tekniset hallintakeinot)	
6.1	Key pair generation and installation (Avainparin luominen ja asentaminen)	Kohdat 7.2.1, 7.2.3, 7.2.8 ja 7.2.9
6.2	Private Key Protection and Cryptographic Module Engineering Controls (Yksityisen avaimen suojauksen ja salausmoduulin tekniset hallintakeinot)	Kohdat 7.2.1, 7.2.2, 7.2.6 ja 7.2.7
6.3	Other aspects of key pair management (Muita avainparin hallintaan liittyviä)	Kohta 7.2
6.4	Activation data (Aktivointitiedot)	Kohdat 7.2.7 ja 7.2.9

RFC 3647 -julkaisun [2] osio		Tämän asiakirjan kohta
6.5	Computer security controls (Tietokoneen turvallisuuden hallintakeinot)	Kohdat 7.4.5, 7.4.6 ja 7.4.7
6.6	Life cycle technical controls (Elinkaaren tekniset hallintakeinot)	Kohdat 7.4.5, 7.4.6 ja 7.4.7
6.7	Network security controls (Verkon turvallisuuden hallintakeinot)	Kohta 7.4.6
6.8	Time-stamping (Aikaleimaus)	Ei kuulu soveltamisalaan
7	CERTIFICATE, CRL, AND OCSP PROFILES (Varmenteen, sulkulistan ja OCSP-protokollan profiilit)	
7.1	Certificate profile (Varmenteen profiili)	Kohta 7.3.3 (a)
7.2	CRL profile (Sulkulistan profiili)	Kohta 7.3.6
7.3	OCSP profile (OCSP-protokollan profiili)	
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS (Vaatumustenmukaisuuden auditointi ja muut arvioinnit)	
8.1	Frequency or circumstances of assessment (Arviointitiheys ja -olosuhteet)	5.4.1
8.2	Identity/qualifications of assessor (Arvioijan henkilöllisyys/pätevyys)	CWA 14172
8.3	Assessor's relationship to assessed entity (Arvioijan suhde arvioitavaan yhteisöön)	CWA 14172
8.4	Topics covered by assessment (Arvioinnin kattamat aihealueet)	Kohdat 5.4.2, 5.4.3 ja 8.4
8.5	Actions taken as a result of deficiency (Toimet, joihin ryhdytään havaitun puutteen johdosta)	Kohdat 5.4.1 ja 8.4
8.6	Communication of results (Tuloksista tiedottaminen)	Kohta 5.4.1
9	OTHER BUSINESS AND LEGAL MATTERS (Muut liiketoimintaa koskevat ja oikeudelliset seikat)	
9.1	Fees (Palkkiot)	Kohdan 7 johdanto
9.2	Financial responsibility (Taloudellinen vastuu)	Kohta 7.5
9.3	Confidentiality of business information (Liiketoimintatiedon luottamuksellisuus)	
9.4	Privacy of personal information (Henkilötietojen yksityisyyden suoja)	Kohdat 7.3.1 (k), 7.3.3 (e), 7.4.10 ja 7.4.11 (j)
9.5	Intellectual property rights (Immateriaalioikeudet)	Alkuvivut
9.6	Representations and warranties (Edustaminen ja takuut)	
9.7	Disclaimers of warranties (Takuuiden antamisesta pidättäytyminen)	
9.8	Limitations of liability (Vastuunrajoitukset)	Kohta 6.4
9.9	Indemnities (Korvaukset)	
9.10	Term and termination (Voimassaoloaika ja päätyminen)	
9.11	Individual notices and communications with participants (Yksittäiset ilmoitukset ja viestintä osapuolten kanssa)	Kohta 7.3.4
9.12	Amendments (Muutokset)	ETSIn menettelyt
9.13	Dispute resolution provisions (Riitojenratkaisua koskevat säännökset)	Kohta 7.5
9.14	Governing law (Sovellettava lainsäädäntö)	
9.15	Compliance with applicable law (Sovellettavan lainsäädännön noudattaminen)	Kohta 7.4.10
9.16	Miscellaneous provisions (Sekalaiset säännökset)	
9.17	Other provisions (Muut säännökset)	Kohta 7.5

Taulukko D.2: RFC 2527 -julkaisun osioiden ja menettelytapavaatimusten väliset ristiviittaukset

RFC 2527 -julkaisun osio		Tämän asiakirjan kohta
1	INTRODUCTION (Johdanto)	
1.1	Overview (Yleistä)	Kohta 5.1
1.2	Identification (Tunnistaminen)	Kohta 5.2
1.3	Community and Applicability (Yhteisö ja sovellettavuus)	Kohta 5.3
1.4	Contact Details (Yhteystiedot)	kansilehden jälkeinen sivu
2	GENERAL PROVISIONS (Yleiset säännökset)	
2.1	Obligations (Velvollisuudet)	Kohdat 6.1, 6.2 ja 6.3
2.2	Liability (Vastuu)	Kohta 6.4
2.3	Financial Responsibility (Taloudellinen vastuu)	Kohta 7.5
2.4	Interpretation and Enforcement (Tulkinnat ja täytäntöönpano)	Kohta 5.4

2.5	Fees (Palkkiot)	Ei kuulu soveltamisalaan
2.6	Publication and Repositories (Julkaisu ja tallennuspaikat)	Kohdat 7.3.5, 7.3.6 ja 7.3.4
2.7	Compliance Audit (Vaatimustenmukaisuuden auditointi)	Kohta 5.4
2.8	Confidentiality Policy (Luottamuksellisuutta koskevat menettelytavat)	Kohta 7.4.10 (b)
2.9	Intellectual Property Rights (Immateriaalioikeudet)	alkusivut
3	IDENTIFICATION AND AUTHENTICATION (Tunnistaminen ja todentaminen)	
3.1	Initial Registration (Aluksi tehtävä rekisteröityminen)	Kohta 7.3.1
3.2	Routine Rekey (Rutiininomainen avainparin vaihtaminen)	Kohta 7.3.2
3.3	Rekey After Revocation -- No Key Compromise (Avainparin vaihtaminen peruuttamisen jälkeen, kun avain ei ole vaarantunut)	Kohta 7.3.2
3.4	Revocation Request (Peruuttamispyyntö)	Kohta 7.3.6
4	OPERATIONAL REQUIREMENTS (Toimintaa koskevat vaatimukset)	
4.1	Certificate Application (Varmennehakemus)	Kohdat 7.3.1 ja 7.3.3
4.2	Certificate issuance (Varmenteen myöntäminen)	Kohta 7.3.3
4.3	Certificate Acceptance (Varmenteen hyväksyminen)	Kohta 7.3.1
4.4	Certificate Suspension and Revocation (Varmenteen asettaminen)	Kohta 7.3.6

RFC 2527 -julkaisun osio		Tämän asiakirjan kohta
4.5	Security Audit Procedures (Turvallisuusauditoinnin menettelyt)	Kohta 7.4.1
4.6	Records Archival (Tietojen arkistointi)	Kohta 7.4.11
4.7	Key Changeover (Varmentajan avainparin vaihtaminen)	Kohta 7.3.2
4.8	Compromise and Disaster Recovery (Toipuminen vaarantumis- ja hätätilanteista)	Kohta 7.4.8
4.9	CA Termination (Varmentajan toiminnan päättyminen)	Kohta 7.4.9
5	PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	
5.1	Physical Security Controls (Fyysiseen turvallisuuteen liittyvät hallintakeinot)	Kohta 7.4.4
5.2	Procedural Controls (Menettelyiden hallintakeinot)	Kohdat 7.4.5 ja 7.4.3
5.3	Personnel Security Controls (Henkilöstöön liittyvät turvallisuuden hallintakeinot)	Kohta 7.4.3
6	TECHNICAL SECURITY CONTROLS (Turvallisuuden tekniset hallintakeinot)	
6.1	Key Pair Generation and Installation (Avainparin luominen ja asentaminen)	Kohdat 7.2.8 ja 7.2.9
6.2	Private Key Protection (Yksityisen avaimen suojaus)	Kohta 7.2.8
6.3	Other Aspects of Key Pair Management (Muita avainparin hallintaan liittyviä seikkoja)	Kohdat 6.2 ja 7.2
6.4	Activation Data (Aktivoititiedot)	Kohdat 7.2.7 ja 7.2.9
6.5	Computer Security Controls (Tietokoneen turvallisuuden hallintakeinot)	Kohdat 7.4.5, 7.4.6 ja 7.4.7
6.6	Life Cycle Security Controls (Elinkaaren turvallisuuden hallintakeinot)	Kohdat 7.4.7 ja 7.4.1
6.7	Network Security Controls (Verkon turvallisuuden hallintakeinot)	Kohta 7.4.6
6.8	Cryptographic Module Engineering Controls (Salausmoduulin tekniset hallintakeinot)	Kohta 7.2
7	CERTIFICATE AND CRL PROFILES (Varmenteen ja sulkulistan profiilit)	
7.1	Certificate Profile (Varmenteen profiili)	Kohta 7.3.3 (a)
7.2	CRL Profile (Sulkulistan profiili)	Ei kuulu soveltamisalaan
8	SPECIFICATION ADMINISTRATION (Spesifikaation hallinta)	
8.1	Specification Change Procedures (Spesifikaation muuttamismenettelyt)	ETSI:n menettelyt
8.2	Publication and Notification Procedures (Julkaisu- ja ilmoittamismenettelyt)	ETSI:n menettelyt
8.3	Certification practice statement Approval Procedures (Varmennuskäytännön hyväksymismenettelyt)	Kohta 7.1
HUOM	RFC 2527 -julkaisu on kumottu julkaisulla RFC 3647 [2].	

**Liite E (tiedoksi):
Version 1.2.1 jälkeen tehdyt muutokset****E.1 Lisätyt vaatimukset**

Seuraavat lisätyt kohdat muuttavat vaatimuksia merkittävästi.

Kohdan 5.2 huomautus (ei valtuutusta), kohdan 5.4.1 alakohta c, kohdan 5.4.1 alakohta d, kohdan 6.2 alakohta i, kohdan 7.1 alakohta i, kohdan 7.2.1 alakohta e, kohdan 7.3.1 alakohta g, kohdan 7.3.1 alakohta 1, kohdan 7.3.2 alakohta a (tarkistettava uusittavan varmenteen olemassaolo ja voimassaolo), kohdan 7.3.3 alakohta b, kohdan 7.3.6 alakohta 1, kohdan 7.4.1 viimeinen lause, kohdan 7.4.1 alakohta d, kohdan 7.4.3 alakohta b, kohdan 7.4.4 alakohta e, kohdan 7.4.5 alakohta d, kohdan 7.4.5 alakohta i, kohdan 7.4.5 alakohta j, kohdan 7.4.6 alakohta b, kohdan 7.4.8 alakohtat a, b ja c, kohdan 7.4.8 alakohta f, kohdan 7.4.9 alakohtan a toinen asiakohta (sulkuilätietojen kirjaaminen), kohdan 8.1 alakohta a, kohdan 8.4 alakohta c, kohdan 8.4 alakohta d.

E.2 Päivitetyt vaatimukset

Seuraavia kohtia on päivitetty. Päivityksillä on laajennettu valinnanmahdollisuutta tai muutoin muutettu vaatimuksia.

Kohta 5.2, kohdan 5.4.1 alakohta b, kohdan 6.2 johdantokappale, kohdan 7.2.1 alakohta b, kohta 7.2.4, kohdan 7.2.2 alakohta a, kohdan 7.2.8 alakohta d,

kohdan 7.2.8 alakohta e, kohdan 7.3.1 alakohta i, kohdan 7.3.2 alakohta a, kohdan 7.3.2 alakohta c, kohdan 7.4.3 alakohtan g neljäs asiakohta, kohdan 7.4.6 alakohta b, kohdan 7.4.6 alakohta d, kohdan 7.4.8 alakohta e, kohdan 7.4.9 alakohta b, kohdan 8.4 alakohta b.

E.3 Selvennykset

Aiemmin määritettyjen vaatimusten selventämiseksi seuraavia kohtia on päivitetty.

Kohdan 5.4.1 huomautukset, kohdan 6.2 osakappale, kohdan 6.2 alakohtan d alakohta iii, kohdan 6.2 alakohta f, kohdan 6.2 alakohtan g alakohta iii, kohdan 6.2 alakohta i, kohdan 6.3 huomautus 1, kohdan 7.1 alakohta f, kohdan 7.2.2 alakohta b, kohdan 7.2.6 alakohta a, kohdan 7.2.7 alakohta a, kohdan 7.2.8 alakohtat a ja b, kohdan 7.2.9 huomautus 2, kohdan 7.3.1 alakohta c, kohdan 7.3.1 alakohta f, kohdan 7.3.1 alakohta h (siirretty), kohdan 7.3.1 huomautus 11, kohdan 7.3.1 alakohtan i kolmas asiakohta,

kohdasta 7.3.1 on poistettu toisteista tekstiä tietosuojasta, kohdan 7.3.2 alakohta c, kohdan 7.3.3 alakohta a, kohdan 7.3.3 alakohtan d toinen asiakohta, kohdan 7.3.4 huomautus 2, kohdan 7.3.6 alakohtan g kolmas asiakohta ja huomautus 3, kohdan 7.4.1 alakohta d (siirretty kohdasta 7.5), kohdan 7.4.3 alakohta a (yhdistetty kohdan 7.5 vastaavaan asiakohtaan), kohdan 7.4.3 huomautus 2, kohdan 7.4.3 alakohta f, kohdan 7.4.3 huomautus 4, kohdan 7.4.4 alakohtat d, f ja g, kohdan 7.4.7 huomautus 1, kohdan 7.4.8 huomautus 2, kohdan 7.4.9 ensimmäinen asiakohta, kohdan 7.4.10 alakohtat a ja b sekä huomautus, kohdan 7.4.11 alakohta e, kohta 7.5 (kaksi asiakohtaa siirretty kohdan 7.4.1 alakohtaan d ja kohdan 7.4.3 alakohtaan a), kohdan 8.4 huomautukset 1 ja 2.

E.4 Toimitukselliset muutokset

Tekstiin on tehty lukuisia toimituksellisia muutoksia, jotka eivät vaikuta tämän asiakirjan tekniseen sisältöön.

E.5 Version 1.3.1 jälkeen tehdyt muutokset

Seuraavien kohtien vaatimuksia on selvennetty:

Kohdan 7.2.5 alakohta a, kohdan 7.3.1 alakohta g ja kohta 7.2.8.

**Liite F (tiedoksi):
Lähdekirjallisuus**

TTP.NL Part 1: "Requirements and Guidance for the Certification of the Public Key Infrastructure of Certification Service Providers".

TTP.NL Part 2: "Requirements and Guidance for the Certification of Information Security Management of Certification Service Providers".

TTP.NL Part 3: "General Requirements and Guidance for the Accreditation of Certification Service Providers issuing Qualified Certificates".

"Scheme approval profiles for Trust Service Providers". HUOMAUTUS: Katso

<http://www.tscheme.org/>.

ITU-T Recommendation X.843 | ISO/IEC 15945: "Information technology – Security techniques – Specification of TTP services to support the Application of Digital Signatures".

ITU-T Recommendation X.842 | ISO/IEC 14516: "Information technology – Security techniques – Guidelines on the use and management of Trusted Third Party services".

ISO/IEC TR 13335-1 (1996): "Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security".

ISO/IEC TR 13335-2 (1997): "Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security".

ISO/IEC TR 13335-3 (1998): "Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security".

ISO/IEC TR 13335-4 (2000): "Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards".

ANSI X9.79: "Public Key Infrastructure (PKI) - Practices and Policy Framework".

Euroopan parlamentin ja neuvoston direktiivi 97/7/EY, annettu 20 päivänä toukokuuta 1997, kuluttajansuojasta etäsopimuksissa – Neuvoston ja Euroopan parlamentin lausuma 6 artiklan 1 kohdan osalta – Komission lausuma 3 artiklan 1 kohdan ensimmäisen luetelmakohdan osalta.

CEN Workshop Agreement 14172: "EESSI Conformity Assessment Guidance".

ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

NIST SP 800-78: "Cryptographic Algorithms and Key Sizes for Personal Identity Verification", Tim Polk, Donna Dodson ja William B.

Versiohistoria

Asiakirjan versiot		
V1.1.1	joulukuu 2000	julkaisu
V1.2.1	huhtikuu 2002	julkaisu
V1.3.1	toukokuu 2005	julkaisu
V1.4.1	tammikuu 2006	julkaisu
V1.4.2	joulukuu 2006	julkaisu
V1.4.3	toukokuu 2007	julkaisu