

VARMENNETOIMINTA

Esipuhe

Viestintävirasto perusti 6.2.2001 työryhmän selvittämään varmennepalveluiden tietoturva vaatimuksia ja yleisiä toimintaedellytyksiä.

Työryhmän tehtävänä oli selvittää, kuinka Viestintävirasto hoitaa sähköisistä allekirjoituksista annetun lain mukaisia tehtäviään ja samalla luoda ehdotukset Viestintäviraston määräyksiksi ja suosituksiksi.

Työryhmän toimintaan osallistuivat seuraavat henkilöt:

Timo Lehtimäki	Viestintävirasto	Puheenjohtaja
Minna Aalto-Setälä	Finnet-liitto ry	
Mikko Huopio	Sampo Pankki Oyj	
Taina Kallio-Miettinen/ Sakari Myllymäki	Osuuspankkikeskus	
Hannu Konttinen	Oy Radiolinja Ab	
Kaarlo Korvola	Sisäasiainministeriö	
Juha Lampinen	Keskusrikospoliisi	
Leena Linnainmaa	Keskuskauppakamari	
Kirsi Kareinen/ Mirva Peltola	Novotrust Oy	
Rami Peltosaari/ Heikki Myllyniemi	Elisa Communications Oyj	
Urpo Pennanen	ICL Invia	
Heikki Sinervo / Seppo Perkiö	Teollisuuden ja Työnantajain Keskusliitto	
Tuire Saaripuu	Väestörekisterikeskus	
Mikko Niva/ Tapio Ranta/	Sonera Oyj	
Leena Save	Sonera Solutions Oy/ Sonera Oyj	
Jyri Terämaa/ Juha Suni	Nordea Pankki Suomi Oyj	
Sami Kilkkilä	Viestintävirasto	
Kirsi Sunila-Putilin/ Eeva Lantto	Viestintävirasto	Sihteerit

Sisällys	
Esipuhe.....	1
1. Johdanto.....	4
2. Laki sähköisistä allekirjoituksista.....	5
2.1. Lain soveltamisala.....	5
2.1.1. Soveltaminen sähköisiin allekirjoituksiin.....	5
2.1.2. Soveltaminen sähköisiin allekirjoituksiin liittyvien tuotteiden tai palveluiden tarjontaan ..	5
2.1.3. Soveltaminen sähköisiin allekirjoituksiin liittyvien tuotteiden tai palveluiden tarjontaan yleisölle	5
2.2. Laatuvarmenteiden tarjoajille laissa asetetut vaatimukset.....	6
2.3. Viestintäviraston tehtävät.....	6
2.3.1. Laatuvarmenteita yleisölle tarjoavien varmentajien valvonta	6
2.3.2. Tarkastuslaitosten toiminnan valvonta	6
2.3.3. Lain noudattamisen valvonta ja pakkokeinot	6
2.3.4. Teknisten määräysten ja suositusten antaminen	7
3. Varmentajan toiminta.....	7
3.1. Toiminnan aloittaminen.....	7
3.2. Toiminnan keskeyttäminen tai lopettaminen.....	7
3.3. Yleiset tietoturvallisuusvaatimukset	7
3.3.1. Toiminnallinen tietoturvallisuus.....	8
3.3.2. Fyysinen turvallisuus	8
3.3.3. Tietoliikenneturvallisuus.....	8
3.3.4. Laitteisto- ja ohjelmistoturvallisuus	8
3.3.5. Tietoaineistoturvallisuus.....	8
3.4. Varmennepalveluihin liittyvät yleiset tietoturvallisuusvaatimukset	8
3.4.1. Hallinnolliset vaatimukset	8
3.4.2. Järjestelmät ja toiminnot	9
3.4.3. Tunnistaminen.....	10
3.4.4. Varmentajan avainten hallinta	10
3.4.5. Kirjanpito ja auditoinnit	11
3.4.6. Arkistointi	11
3.4.7. Varmuuskopiot ja toipuminen	12
3.5. Varmennepalveluiden eri osa-alueiden tietoturvallisuusvaatimukset.....	12
3.5.1. Rekisteröinti	12
3.5.2. Laatuvarmenteiden luominen	12
3.5.3. Laatuvarmenteiden jakelu	13
3.5.4. Laatuvarmenteiden peruuttaminen eli sulkulistapyyntöjen hallinta	13
3.5.5. Laatuvarmenteiden voimassaolon tarkistaminen eli sulkulistapalvelu	14
3.5.6. Aikaleimapalvelu (lisäpalvelu).....	14
3.5.7. Turvallisen allekirjoituksen luomisvälineen jakelu.....	14
3.6. Luotettavuuteen ja tietoturvallisuusvaatimukseen liittyvä dokumentaatio	15
3.6.1. Hallinnolliset ja johtamista koskevat menettelytavat.....	15
3.6.2. Tietoturvapoliittikka ja -periaatteet sekä riskien hallinta.....	15
3.6.3. Varmennepoliittikka ja varmennuskäytäntö	15
3.6.4. PDS (PKI Disclosure Statement)	16
3.6.5. Allekirjoituspolitiikka (Signature Policy)	16
4. Viestintäviraston suorittama varmentajien valvonta	16
4.1. Viestintävirastolle toimitettavat tiedot.....	17
4.1.1. Rekisteröinti ja toiminnan aloittaminen	17
4.1.2. Vuosiraportti	18
4.1.3. Toiminnan muutokset.....	18
4.1.4. Muut säännöllisesti toimitettavat tiedot.....	19
4.1.5. Tarkastukset	19
4.1.6. Lopettamisilmoitus	19
4.2. Viestintäviraston julkaisemat tiedot.....	20
5. Yhteentoimivuus.....	20
5.1. Sisämarkkinaperiaatteet ja kansainväliset näkökohdat.....	20
5.2. Standardointi	20
5.2.1. EESSI-projekti	20

6. Turvallinen allekirjoituksen luomisväline	21
6.1. Tarkastuslaitokset	21
7. Pätevydentoteamis- ja arviointilaitokset	22
7.1. Akkreditointi	22
7.2. Sertifiointi	22
7.3. Turvallisten allekirjoituksen luomisvälineiden arviointilaitokset	22
8. Maksut	23
8.1. Maksut varmentajilta	23
8.2. Arviointilaitosten valvontamaksut	23
9. Työryhmän ehdotukset	23
9.1. Maksut varmentajilta	23
9.2. Viestintäviraston määräykset ja suositukset	24
LIITE 1: Laatuvarmenteita tarjoavan varmentajan tietoturvallisuuden tarkistuslista	1
SISÄISET TOIMINNOT (PROSESSIT JA TOIMINTATAVAT)	1
1. Hallinnolliset vaatimukset (Management)	1
2. Järjestelmät ja toiminnot	1
3. Sisäänkirjautuminen ja tunnistaminen	2
4. Avainten hallinta	2
5. Accounting and Auditing	3
6. Arkistointi	4
7. Varmuuskopiointi ja palautus	5
PERUSPALVELUT	6
1. Yleistä	6
2. Rekisteröinti	6
3. Varmenteen luominen	6
4. Laatuvarmenteiden jakelupalvelu	7
5. Laatuvarmenteiden sulkupalvelu	7
6. Laatuvarmenteen sulkulistapalvelu	7

1. Johdanto

Tässä raportissa käsitellään varmennetoimintaa sähköisistä allekirjoituksista annetun lakiehdotuksen (HE 197/2001) pohjalta. Varmennetoiminnalla tarkoitetaan tässä raportissa varmentajan tai tämän apunaan käyttämän tahon suorittamia toimenpiteitä kuten esimerkiksi varmenteiden luomista, rekisteröintiä, myöntämistä, peruuttamista ja jakelua.

Sähköisistä allekirjoituksista annetun lakiehdotuksen mukaan varmennetoiminnan yleinen ohjaus ja kehittäminen kuuluu liikenne- ja viestintäministeriölle. Viestintäviraston tehtävänä on valvoa lain ja sen nojalla annettujen säännösten noudattamista. Varmennepalveluita on monen tasoisia, joista laissa säädellään etupäässä laatuvarmenteita tarjoavia varmentajia. Tässä raportissa käsitellään lähinnä laatuvarmenteita tarjoavia varmentajia koskevia vaatimuksia, mutta raportin sisältö on monilta osin sovellettavissa myös muun tasoiseen varmennetoimintaan. Jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää lain 18 §:n mukaan ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteesen ja on luotu turvallisella allekirjoituksen luomisvälineellä. Mainitut vaatimukset täyttävä sähköinen allekirjoitus samaistetaan perinteiseen, käsintehtyyn allekirjoitukseen. Säännös ei kuitenkaan vaikuta muiden sähköisten allekirjoitusten oikeudelliseen arviointiin.

Raportissa käsitellään Viestintävirastolle laissa annettuja tehtäviä sekä varmennetoiminnan tietoturvallisuus- ja luotettavuusvaatimuksia. Raportissa ehdotetaan laadittavaksi eräitä varmennetoimintaa koskevia määräyksiä ja suosituksia, joilla lain sääntelyä pyritään täsmentämään. Raportissa ei kuvata Viestintäviraston sisäisiä järjestelyitä lain velvoitteiden täyttämiseksi.

Raportissa on kaksi pääosaa:

- 1) Ensimmäisessä osassa on käsitellään laatuvarmenteiden tarjontaan liittyviä vaatimuksia lain ja standardointityön pohjalta sekä yleisiä varmennetoiminnan alueita liittyen muun muassa standardointityöhön ja yhteentoimivuuteen.
- 2) Toisessa osassa käsitellään työryhmän näkemyksiä laatuvarmenteita tarjoavien varmentajien valvonnasta ja siihen liittyvistä Viestintäviraston määräyksistä sekä ehdotuksia jatkotoimenpiteiksi. Raportissa käsitellään myös varmennetoiminnasta perittäviä valvontamaksuja ja niiden vaikutusta varmennetoiminnan ja tietoyhteiskunnan palveluiden kehittymiseen.

Työryhmäraportin yhteenvedona voidaan todeta, että määräyksissä ei voida asettaa lisävaatimuksia laissa määriteltyjen vaatimusten lisäksi. Samalla määräyksillä on kuitenkin pyrittävä täsmentämään laissa asetettuja vaatimuksia siten, että varmentajat voivat käytännön toiminnassaan täyttää varmennetoiminnalle asetetut vaatimukset ja että näiden vaatimusten täytymistä voidaan arvioida. Varmennetoiminnan käynnistysvaiheessa on laatuvarmentajilta perittävien valvontamaksujen määrä keskeinen kannattavuuteen vaikuttava tekijä. Erityisesti työryhmän toimijat ovat painottaneet, että vasta kehittymässä olevaa liiketoimintaa ei tulisi rasittaa suurilla valvonnasta perittävillä maksuilla, ettei toiminta niiden takia tulisi kannattamattomaksi.

2. Laki sähköisistä allekirjoituksista

Liikenne- ja viestintäministeriö on valmistellut hallituksen esityksen (HE 197/2001) laiksi sähköisistä allekirjoituksista (tässä raportissa "laki" tai "SakL"). Esitys lähetettiin julkiselle lausuntokierrokselle 26.2.2001. Valtioneuvosto päätti sähköisiä allekirjoituksia koskevan lain sisällöstä 25.10.2001.

Lailla pannaan täytäntöön Euroopan parlamentin ja neuvoston direktiivi (1999/93/EY) sähköisiä allekirjoituksia koskevista yhteisön puitteista (tässä raportissa "direktiivi"). Direktiivi perustuu siihen, että varmennepalvelujen tarjoaminen on vapaa elinkeino, mutta vain korkeat laatuvaatimukset täyttävän hyväksytyin varmenteen (qualified certificate) ja turvallisen allekirjoituksen luomisvälineen avulla tehty kehittynyt sähköinen allekirjoitus on direktiivin mukaan hyväksyttävä oikeusvaikutuksiltaan perinteisen allekirjoituksen veroiseksi. Direktiivissä säännellään nimenomaan hyväksytyjä varmenteita ja niitä tarjoavia varmentajia. Laissa ja tässä raportissa hyväksytystä varmenteesta käytetään nimeä laatuvarmenne. Direktiivissä kielletään kuitenkin epäämästä oikeusvaikutusta muiltakaan sähköisiltä allekirjoituksilta esimerkiksi yksinomaan sillä perusteella, että allekirjoitus on sähköisessä muodossa.

Varmentaja voi olla luonnollinen tai oikeushenkilö. Laatuvarmenteita yleisölle tarjoavan henkilön on kuitenkin lain 9 §:n mukaan tehtävä ilmoitus toiminnastaan Viestintävirastolle, joka valvoo lain noudattamista ja erityisesti laatuvarmenteiden tarjontaa.

2.1. Lain soveltamisala

Varmenteiden tarjoamiseen liittyy useita osa-alueita ja uusia sähköisiin allekirjoituksiin liittyviä palveluita on kehitteillä. Lain tavoitteena on turvata suotuisat kehittymisedellytykset näille uusille palveluille. Lakia sovelletaan sähköisiin allekirjoituksiin sekä niihin palveluntarjoajiin, jotka tarjoavat sähköisiin allekirjoituksiin liittyviä tuotteita tai palveluita yleisölle. Laissa annetaan tarvittavia säädöksiä sähköisiin allekirjoituksen luomiseen käytettävien varmenteiden tarjonnasta ja erityisesti laatuvarmenteita yleisölle tarjoavien varmentajien velvollisuuksista. Lain 2 lukua sovelletaan vain laatuvarmenteiden tarjontaan. Henkilötietojen käsittelyä koskevien säännösten noudattamista valvoo Tietosuojavaltuutettu.

2.1.1. Soveltaminen sähköisiin allekirjoituksiin

Soveltamisalan ulkopuolelle jääviä varmenteiden käyttötarkoituksia olisivat muun muassa varmenteiden käyttö yksinomaan muuhun kuin allekirjoitustarkoitukseen kuten esimerkiksi vain tunnistamiseen tai viestinnän salaamiseen.

2.1.2. Soveltaminen sähköisiin allekirjoituksiin liittyvien tuotteiden tai palveluiden tarjontaan

Lain 2 luku koskee ainoastaan sellaisia varmentajia, jotka tarjoavat laatuvarmenteita yleisölle. Laatuvarmenteiden tarjoaminen asettaa vaatimuksia sekä varmenteen tietosisällölle (SakL 7 §) että varmentajan toiminnalle (SakL 10 -15 §§). Laatuvarmenteella tarkoitetaan varmennetta, jonka sisältö täyttää lain vaatimukset ja jonka lain vaatimukset täyttävä varmentaja on myöntänyt. Laatuvarmenteita myönnetään ainoastaan luonnollisille henkilöille. Varmenteiden tarjoamiseen voi liittyä myös muita palveluita, kuten aikaleima- tai notariaattipalveluja. Ne kuuluvat lain soveltamisalaan, mutta niistä ei ole laissa erityisiä säädöksiä.

2.1.3. Soveltaminen sähköisiin allekirjoituksiin liittyvien tuotteiden tai palveluiden tarjontaan yleisölle

Lakia sovelletaan sähköisiin allekirjoituksiin liittyvien tuotteiden tai palveluiden tarjoamiseen yleisölle ja lisäksi lain 2 lukua sovelletaan vain varmentajiin, jotka tarjoavat laatuvarmenteita yleisölle. Yleisöllä tarkoitetaan käyttäjryhmää, jota ei ole ennalta rajattu esimerkiksi työ-, virka-, tai asiakassuhteen perusteella tai muulla vastaavalla tavalla. Siten laki ja työryhmän valmistelemat määräykset eivät koske esimerkiksi yrityskonsernin sisäiseen käyttöön tarkoitettujen varmenteiden

tarjoamista. Lakia ei sovelleta myöskään vapaaehtoiisiin siviilioikeudellisiin sopimuksiin, joilla on sovittu sähköisen allekirjoituksen käytöstä tietyn, rajatun osanottajajoukon kesken. Avoimena käyttäjäryhmänä tulisi pitää ainakin tapauksia, joissa varmenteeseen luottava osapuoli ei ennakolta ole minkäänlaisessa sopimussuhteessa varmentajaan taikka allekirjoittajaan. Hallituksen esityksen mukaan yleisön käsitteen tarkempi tulkinta jää oikeuskäytännön varaan.

2.2. Laatuvarmenteiden tarjoajille laissa asetetut vaatimukset

Lain 2 luvussa säädetään laatuvarmenteita tarjoavan varmentajan velvollisuuksista, joiden tarkoitus on parantaa sähköisen allekirjoituksen luotettavuutta. Yleisölle laatuvarmenteita tarjoavalle varmentajalle säädettyt velvollisuudet koskevat muun muassa hakemistopalvelun tarjoamista, henkilön luotettavaa tunnistamista, turvallisten järjestelmien käyttöä ja käytettävän henkilöstön pätevyyttä. Laissa on lisäksi säädetty laatuvarmenteen sisältöä koskevat minimivaatimukset.

2.3. Viestintäviraston tehtävät

Lain 22 §:n mukaan varmennetoiminnan yleinen ohjaus ja kehittäminen kuuluu liikenne- ja viestintäministeriölle. Direktiivin 3 artiklan mukaisesti kunkin jäsenvaltion on varmistettava alueellensa sijoittautuneiden laatuvarmenteita tarjoavien varmentajien valvonta. Viestintäviraston tehtävänä on valvoa ehdotetun lain ja sen nojalla annettujen säännösten noudattamista. Virasto voi lain 9 ja 22 §:ien nojalla antaa tarvittaessa teknisiä määräyksiä ja suosituksia ilmoitusvelvollisten varmentajien antamien tietojen tarkemmasta sisällöstä sekä mainittujen varmentajien toiminnan luotettavuus- ja tietoturvallisuusvaatimuksista.

Lain tehtävien hoitaminen edellyttää, että Viestintävirasto valmistelee tarpeelliset tekniset määräykset ja suositukset ja huolehtii, että sillä on asianmukaiset tiedolliset, taidolliset ja taloudelliset resurssit varmentajien toiminnan tarkastamiseksi ja valvomiseksi sekä erimielisyyksien selvittämiseksi. Tehtävien suorittamiseksi Viestintävirasto tekee yhteistyötä varmennepalvelujen tarjoajien kanssa esimerkiksi erilaisissa hallinnollisissa ja standardointiin liittyvissä työryhmissä.

2.3.1. Laatuvarmenteita yleisölle tarjoavien varmentajien valvonta

Viestintäviraston tehtäviin kuuluu lain mukaan:

- ottaa vastaan varmentajien ilmoitukset ennen toiminnan aloittamista (SakL 9 § 1 mom),
- tehdä viipymättä mahdolliset kieltopäätökset, jos varmenne ja/tai varmentaja eivät täytä säädettyjä vaatimuksia (SakL 9 § 2 mom),
- pitää yllä julkista rekisteriä laatuvarmenteita myöntävistä varmentajista (SakL 9 § 4 mom).

2.3.2. Tarkastuslaitosten toiminnan valvonta

Tarkastuslaitosten tehtävänä on lain mukaan arvioida, täyttääkö allekirjoituksen luomisväline laissa säädetty vaatimukset. Viestintäviraston tehtäviin kuuluu:

- hakemuksesta nimetä mahdolliset tarkastuslaitokset, mikäli hakija täyttää säädetty edellytykset,
- valvoa tarkastuslaitosten toimintaa,
- ottaa vastaan tarkastuslaitosten toimintaa koskevat muutosilmoitukset,
- peruuttaa nimeäminen tarvittaessa.

2.3.3. Lain noudattamisen valvonta ja pakkokeinot

Viestintäviraston tehtäviin kuuluu lain mukaan:

- valvoa sähköisistä allekirjoituksista annetun lain noudattamista (SakL 22 § 2 mom),
- suorittaa varmentajia koskevia tarkastuksia (24 § 1 mom),
- velvoittaa lakia tai sen nojalla annettuja säädöksiä ja määräyksiä rikkonut valvottava taho korjaamaan virheensä tai laiminlyöntinsä,
- tiedottaa ja neuvoa (esim. Viestintäviraston www-sivuilla).

2.3.4. Teknisten määräysten ja suositusten antaminen

Viestintäviraston tehtäviin kuuluu lain 9 §:n ja 22 §:n nojalla antaa teknisiä määräyksiä ja suosituksia laatuvarmenteita yleisölle tarjoavien varmentajien Viestintävirastolle tekemässä ilmoituksessa annettavien tietojen tarkemmasta sisällöstä sekä mainittujen varmentajien toiminnan luotettavuus- ja tietoturvaluusvaatimuksista. Tehtävä edellyttää standardointityön seuraamista, tiedottamista ja varmennetyöryhmän toiminnan hyödyntämistä.

3. Varmentajan toiminta

Tässä kappaleessa on käsitelty laatuvarmenteita tarjoavien varmentajien toimintaan liittyviä peruskäytäntöjä sekä luotettavuuteen ja tietoturvaluuteen liittyviä vaatimuksia.

3.1. Toiminnan aloittaminen

Toiminnan aloittamisen yhteydessä laatuvarmenteita tarjoavan varmentajan tulee huolehtia, että sillä on riittävät taloudelliset ja henkilöstölliset resurssit toiminnan harjoittamiseksi luotettavasti ja turvallisesti. Varmentajan on myös huolehdittava, että sillä on riittävä henkilöstö ja riittävä varmennetoimintaan liittyvä asiantuntemus ja että varmentajan koko henkilöstö tiedostaa varmentajalle asetetut vaatimukset.

3.2. Toiminnan keskeyttäminen tai lopettaminen

Laatuvarmenteita tarjoavan varmentajan lopettaessa tai keskeyttäessä toimintansa varmentajan on huolehdittava riittävästä tiedottamisesta ja järjestelyistä varmenteen haltijoiden ja apunaan käyttävien henkilöiden (esimerkiksi alihankkijat) sekä yhteistyökumppaneiden suhteen. Yhteistyökumppaneilla tässä tarkoitetaan kaikkia niitä tahoja, joille on tärkeää saada tieto asiasta (esimerkiksi muut varmentajat). Varmentajan on myös minimoitava toiminnan lopettamisesta aiheutuvat haitat allekirjoittajille ja laatuvarmenteisiin luottaville tahoille. Varmentajan on lopetettava alihankkijoiden toiminta laatuvarmenteidensa myöntämisen osalta siten, ettei uusia varmenteita myönnetä tai hakemuksia oteta vastaan toiminnan päättymisen jälkeen.

Varmentajan on huolehdittava niiden arkistoitujen tietojen säilyttämisestä, joilla on merkitystä kiistojen selvittelyissä. Säilyttämisestä aiheutuvien kustannusten osalta varmentajalla tulee olla riittävät taloudelliset voimavarat tai vakuutukset, jotka kattavat myös mahdollisen konkurssin.

Toiminnan lopettamisen yhteydessä varmentajan allekirjoitusavaimet on tuhottava siten, ettei niitä voida enää käyttää.

Varmentajan tietoturvaluuskäytännöissä tai varmennuskäytännöissä tulisi selostaa varmentajan toiminta lopettamisen yhteydessä. Käytännöissä tulisi selvittää ainakin:

- kuinka toiminnan lopettamisesta tiedotetaan asianomaisille,
- kuinka varmentajan vastuut siirretään toisille tahoille,
- kuinka käsitellään voimassaolevia laatuvarmenteita ja sulkulistatietoja.

3.3. Yleiset tietoturvaluusvaatimukset

Tietoturvaluudella tarkoitetaan tietojen, järjestelmien ja palvelujen suojaamista sekä normaali- että poikkeusoloissa hallinnollisten ja teknisten toimenpiteiden avulla. Tietoturvaluus rakentuu tiedon kolmen ominaisuuden: luottamuksellisuuden, eheyden ja käytettävyyden turvaamisesta.

- Luottamuksellisuudella tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat vain niihin oikeutettujen saatavissa eikä niitä luvatta paljasteta tai muutoin saateta sivullisten käyttöön.
- Eheydellä tarkoitetaan sitä, etteivät tiedot, järjestelmät tai palvelut ole laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet.

- Käytettävyydellä tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat tarvittaessa niihin oikeutettujen esteettä hyödynnettävissä.

3.3.1. Toiminnallinen tietoturvaluisuus

Toiminnan tietoturvaluisuuden tulee kattaa seuraavat alueet:

- Hallinnollinen ja organisatorinen turvaluisuus
- Henkilöstöturvaluisuus
- Käyttöturvaluisuus

Hallinnollisella ja organisatorisella turvaluudella tarkoitetaan organisaatiossa noudatettavia tietoturvaluusperiaatteita, toimintalinjoja ja tietoturvaluisuuden organisointia. Hallinnollinen tietoturvaluisuus käsittää myös riskien arvioinnin.

Henkilöstöturvaluudella tarkoitetaan henkilöstöön liittyvien riskien hallintaa toimenkuvien, käyttöoikeuksien määrittelyn sekä turvaluuskoulutuksen ja valvonnan avulla.

Käyttöturvaluudella tarkoitetaan organisaatiossa noudatettavia turvaluisia käyttöperiaatteita ja käyttöympäristöön ja tietojenkäsittelyn turvaluuteen vaikuttavien tapahtumien valvontaa.

3.3.2. Fyysinen turvaluisuus

Fyysisellä turvaluudella tarkoitetaan tilojen ja järjestelmien suojaamista fyysisiltä uhilta ja vahingoilta.

3.3.3. Tietoliikenneturvaluisuus

Tietoliikenneturvaluudella tarkoitetaan välitettävien viestien luottamuksellisuuden, eheyden ja käytettävyyden turvaamisesta. Tietoliikenneturvaluutta voidaan parantaa usein teknisin keinoin kuten muodostamalla salattuja yhteyksiä (esimerkiksi VPN).

3.3.4. Laitteisto- ja ohjelmistoturvaluisuus

Laitteistoturvaluudella tarkoitetaan laitteistojen suunnitteluun, rakenteeseen, kokoonpanoon, valmistukseen, kunnossapitoon ja laadunvarmistukseen liittyviä tietoturvaluustoimenpiteitä. Ohjelmistoturvaluudella tarkoitetaan ohjelmistoihin sisältyviä tunnistamis-, pääsynvalvonta-, tarkkailu- ja varmistusominaisuuksia. Pääsynvalvontaa voidaan toteuttaa useilla teknisillä menetelmillä ja laitteilla esimerkiksi palomureilla, pääsyn hallinnalla ja autentikoinnilla (tunnistamisella).

3.3.5. Tietoaineistoturvaluisuus

Tietoaineistoturvaluudella tarkoitetaan eri tallennusmuodoissa olevien dokumenttien ja tietovarastojen tunnistamista, turvaluusluokitusta ja sen mukaista käsittelyä niiden kaikissa elin vaiheissa. Tietoaineistoturvaluuteen kuuluvia alueita ovat muun muassa: virustorjunta, sisällön valvonta ja salaus.

3.4. Varmennepalveluihin liittyvät yleiset tietoturvaluusvaatimukset

3.4.1. Hallinnolliset vaatimukset

Varmentajalla tulee olla tietoturvaluuspolitiikka, joka on johdon hyväksymä ja johon koko henkilöstö johto mukaan lukien on sitoutunut. Tietoturvaluuden toteuttamiseksi ja tarkistamiseksi tulee myös järjestää sisäisiä auditointeja ja johdon katselmuksia. Varmentajan on kehitettävä jatkuvasti tietoturvaluuttaan ja tietoturvaluuden hallinta (esimerkiksi organisointi ja katselmukset) tulee olla dokumentoitu.

Varmentajan tietoturvallisuuden tulee olla hallinnoitua ja järjestelmien tulee tukea erilaisia käyttöoikeuksia. Käyttöoikeudet tulisi jakaa esimerkiksi seuraaviin eri luokkiin:

1. tietoturvallisuusvastaava
 - o Tietoturvapoliittikan ja -käytäntöjen suunnittelu sekä kokonaisvastuu tietoturvallisuudesta
2. rekisteröintivastaava
 - o Laatuvarmenteiden luonnin, jakelun ja sulkulistatoimenpiteiden hyväksyntä
3. järjestelmän ylläpitäjä
 - o Laitteiden ja järjestelmien asennus, konfigurointi ja ylläpito sekä varmuuskopioiden ja toipumisten hallinta
4. järjestelmän käyttäjä
 - o Järjestelmän päivittäinen käyttö
5. järjestelmän arvioija
 - o Järjestelmien arkistojen ja tarkastuslokien arviointi

Yksittäisen työntekijän ei tulisi saada oikeuksia kaikkiin käyttöoikeusluokkiin. On suositeltavaa ettei yksittäinen työntekijä saa oikeuksia kuin yhteen käyttöoikeusluokkaan.

3.4.2. Järjestelmät ja toiminnot

Varmentajan käyttämien laitteiden tulisi täyttää CEN/ISSS:n määrittelemien CWA 14167-1 ja CWA 14167-2 mukaiset vaatimukset. Käytettävyyden osalta varmentajan on määriteltävä ne menettelytavat, joiden avulla voidaan mahdollisimman hyvin varmistaa järjestelmien keskeytymätön käyttö. Suunnitelmien tulee kattaa esimerkiksi mahdollinen toimintahäiriö, järjestelmään murtautuminen ja varmentajan toiminnan lopettaminen. Varmentajan käyttämien algoritmien ja avainpituuksien tulee vastata EESSI-projektin algoritmiyöryhmän vaatimuksia.

3.4.2.1. Toimintojen hallinta

Varmentajan luotettavien järjestelmien tulee varmistaa varmentamiseen liittyvien toimintojen riittävä turvallisuus. Erityisesti on varmistettava laitteistojen ja ohjelmien käytön ohjeistaminen siten, että niiden käyttö on oikeutettua ja turvallista, järjestelmävikojen esiintyminen on minimoitu ja järjestelmät on suojattu viruksilta sekä muilta haittaohjelmilta.

3.4.2.2. Toiminnan jatkuvuus

Toiminnan jatkuvuuden turvaamiseksi on varmistettava ettei laitteistovikojen vuoksi aiheudu turhia keskeytyksiä varmentajan palveluihin. Erityisesti on huolehdittava varmenteiden jakelun, sulkulistapyyntöjen hallinnan ja sulkulistapalvelujen toimivuudesta. Näiden palveluiden käytettävyyden tulisi olla vähintään 99,9%.

Varmentajan laitteistojen tavalla tai toisella tuhoutuessa tulisi varmentajan pystyä jatkamaan toimintaansa vaihtoehtoisilla järjestelmillä aiheuttamatta ylimääräistä riskiä tietojen luottamuksellisuudelle ja järjestelmien luotettavuudelle.

3.4.2.3. Fyysinen turvallisuus

Oikeudeton pääsy varmentajan luotettaviin järjestelmiin tulee estää. Pääsyoikeuksien tulisi perustua minimimäärään oikeuksia ja pääsynvalvonnasta tulisi kerätä lokitietoja. Lisäksi tulisi muutoinkin estää salassa pidettävän aineiston joutuminen vääriin käsiin. Ympäristöuhkista tulisi myös huolehtia esimerkiksi varavoimalaitosten, ilmastoinnin ja palontorjuntajärjestelmien avulla.

3.4.2.4. Tietoliikenneturvallisuus

Avoimiin ja epäluotettaviin verkkoihin kytkeydyttäessä tulee huolehtia riittävästä verkkotason turvallisuudesta esimerkiksi salausten menetelmin. Muut kuin sallitut palvelut tulee estää. Varmentajan luotettavat järjestelmät sisältävä verkko on erotettava riittävin pääsynvalvontajärjestelyin myös sisäisestä verkosta.

3.4.2.5. Ajan synkronointi

Varmenteiden luominen ja niiden hallinta on aikaan sidottu. Luotettavien järjestelmien tulee olla synkronoitu riittävän luotettavaan ajanlähteeseen. Ajasta riippuvien varmentajan palveluiden tulisi olla tahdistettu vähintään 1 sekunnin tarkkuudella kansainväliseen normaaliaikaan (UTC, Coordinated Universal Time). Lisäksi on suositeltavaa käyttää kahta erillistä ajanlähdetä.

3.4.3. Tunnistaminen

Luotettavien järjestelmien on tunnistettava ja todennettava jokainen käyttäjä ennen kuin toimenpiteitä voidaan suorittaa järjestelmässä. Toistuvien epäonnistuneiden todennusyritysten jälkeen järjestelmän tulee estää uudet yritykset ellei kyseessä ole järjestelmän ylläpitäjä. Järjestelmän ylläpitäjän osalta toistuvien epäonnistuneista yrityksistä tulisi jäädä merkintä järjestelmän lokiin.

3.4.4. Varmentajan avainten hallinta

Varmentajan käyttämät avaimet voidaan luokitella riskien hallinnan helpottamiseksi. Avaimet voidaan jakaa esimerkiksi seuraavasti:

1. Laatuvarmenteiden allekirjoitusavaimet
 - Avainpari jota käytetään laatuvarmenteiden luomisessa varmentajan allekirjoituksen liittämiseksi laatuvarmenteeseen.
2. Järjestelmäavaimet
 - Avaimet joita luotettavat järjestelmät käyttävät allekirjoittaessaan varmenteen statustarkistuksia, avainten sopimiseksi eri järjestelmien kesken, tietojen salaamiseksi jne.
3. Hallinta-avaimet
 - Avaimet joita luotettavien järjestelmien käyttäjät käyttävät itsensä tunnistamiseen ja todentamiseen sekä käyttääkseen järjestelmiä oikeuksiensa mukaisesti.

Järjestelmä- ja hallinta-avaimet voivat olla joko symmetrisiä tai epäsymmetrisiä.

3.4.4.1. Avainten luominen

Laatuvarmenteiden allekirjoitusavainten luomisessa on käytettävä kryptografista modulia, jonka tulee täyttää joko FIPS 140-1 tason 3 vaatimukset tai CEN/ISSS:n määrittelemässä CWA 14167-2:ssa asetetut Common Criterion mukaiset vaatimukset. Avainten luomisen tulee tapahtua kahden ihmisen valvomana.

Järjestelmäavainten luomisiessa on käytettävä kryptografista modulia, jonka tulee täyttää joko FIPS 140-1 tason 2 vaatimukset tai CEN/ISSS:n määrittelemässä CWA 14167-2:ssa asetetut Common Criterion mukaiset vaatimukset.

3.4.4.2. Avainten jakelu

Yksityisiä ja salaisia avaimia ei saa jakaa selväkielisinä. Julkiset mutta vielä varmentamattomat avaimet tulee säilyttää turvallisesti esimerkiksi manipuloinnin tai kopioinnin estämiseksi.

Laatuvarmenteiden ja sulkulistojen allekirjoitukseen käytettyjen yksityisiä avaimia vastaavat julkiset avaimet tulee toimittaa allekirjoittajille ja allekirjoituksiin luottaville tahoille luotettavalla tavalla. Laatuvarmenteiden allekirjoitusavainta vastaava julkinen avain voidaan toimittaa joko varmentajan itse allekirjoittamassa varmenteessa tai toisen varmentajan allekirjoittamana. Itse allekirjoitetun varmenteen käytön luotettavuutta voidaan lisätä esimerkiksi tarjoamalla varmenteen "sormenjäljen" tarkistusmahdollisuus jostain muusta luotettavasta lähteestä.

3.4.4.3. Avainten käyttö

Pääsynvalvontaa tulisi käyttää kaikissa varmentajan avainten käyttöön liittyvissä tilanteissa.

Useiden järjestelmäavainten käyttö on suositeltavaa yksittäisen avaimen paljastumisesta aiheutuvan riskin vähentämiseksi.

Allekirjoittajan sähköisiin allekirjoituksiin käytettävät avaimet tulisi erottaa muihin käyttötarkoituksiin (kuten salaus) käytetyistä avaimista.

Avaimia tulisi käyttää vain niiden sallitun eliniän ajan. Epäsymmetristen avainten osalta myös varmenteiden voimassaolo on tarkistettava.

3.4.4.4. Avainten vaihtaminen

Järjestelmä- ja hallinta-avaimet tule vaihtaa säännöllisin väliajoin (esim. vuosittain). Avainten vaihdon on tapahduttava luotettavasti.

3.4.4.5. Avainten tuhoaminen

Laatuvarmenteiden allekirjoitusavaimet tulee tuhota tai muutoin varmistaa, ettei avaimia voida enää ottaa uudelleen käyttöön niiden elinkaaren päätyttyä.

Yksityisten tai salaisten avainten luontiin, käyttöön tai talletukseen käytettyjen järjestelmien avaimet täytyy tuhota järjestelmien käytön loputtua. Järjestelmien on kyettävä tuhoamaan sekä HW- että SW-pohjaisesti tallennetut salaiset ja yksityiset avaimet luotettavalla tavalla (esimerkiksi riittävän usealla ylikirjoittamisella).

3.4.4.6. Avainten varastointi ja kopiointi

Kaikki yksityiset ja salaiset avaimet on tallennettava turvallisesti. Varmentajan avainten (allekirjoitus-, järjestelmä-, hallinta-avaimet) varastointi, varmuuskopiointi ja uudelleen käyttöönotto tulee tapahtua turvallisessa ympäristössä ja oikeutettujen henkilöiden toimesta

Laatuvarmenteen haltijan allekirjoitusavaimista ei saa tehdä varmuuskopioita eikä niitä saa luovuttaa kolmansien osapuolten käyttöön.

3.4.4.7. Avainten arkistointi

Allekirjoittajan allekirjoitusavainta ei saa arkistoida.

3.4.5. Kirjanpito ja auditoinnit

Seuraavat tapahtumat tulee vähintään kirjata:

- luotettavien järjestelmien merkittävät tapahtumat sekä avainten ja varmenteiden hallinnan tapahtumat,
- auditoinnin aloittaminen ja lopettaminen,
- auditointiparametrien muutokset,
- toimenpiteet auditointitietojen tallennusvirheiden johdosta.

Lisäksi on suositeltavaa kirjata kaikki kirjautumiset (mukaan lukien epäonnistuneet yritykset) järjestelmään.

Lokitiedostot tulee säilyttää, eikä järjestelmän tule niitä automaattisesti ylikirjoittaa. Järjestelmässä on oltava riittävästi tallennuskapasiteettia.

3.4.6. Arkistointi

Varmentajan luotettavien järjestelmien tulisi arkistoida ainakin:

- kaikki laatuvarmenteet,
- kaikki laatuvarmenteiden sulkulistat,
- kaikki lokitiedostot.

Myös tapahtumien ajankohdat tulee arkistoida. Turvallisuuteen liittyviä parametrejä ei saa arkistoida selväkielisessä muodossa.

3.4.7. Varmuuskopiot ja toipuminen

Varmentajan luotettavien järjestelmien tulee mahdollistaa varmuuskopioiden tekeminen. Varmuuskopioiden tarkoituksena on palauttaa järjestelmän tila halutuksi esimerkiksi syntyneen ohjelmistovian jälkeen. Varmuuskopiot tulee suojata muutoksilta ja kriittisiä turvallisuuteen vaikuttavia parametrejä ei tule kopioida selväkielisessä muodossa.

3.5. Varmennepalveluiden eri osa-alueiden tietoturvallisuusvaatimukset

3.5.1. Rekisteröinti

Laatuvarmenteen hakijan henkilöllisyys ja muut mahdolliset tiedot tarkistetaan rekisteröinnin yhteydessä.

3.5.1.1. Laatuvarmenteen hakeminen

Hakijan henkilöllisyys on tarkistettava luotettavasti. Laatuvarmenteita yleisölle tarjoavan varmentajan on tunnistettava hakija henkilökohtaisesti. Hakijalta on kerättävä riittävät tiedot laatuvarmenteen tietosisällön vaatimusten täyttämiseksi. Mikäli varmentaja ei luo avainparia, on varmentajan tarkistettava, että hakijalla on hallussaan varmennettavaa julkista avainta vastaava yksityinen avain. Laatuvarmennetta haettaessa on tallennettava tieto hakemisajankohdasta sekä tieto laatuvarmenteen julkaisemisesta julkisessa hakemistossa.

3.5.1.2. Laatuvarmenteen hakijan tietojen käsittely

Laatuvarmenteen hakemiseen liittyvät luottamukselliset tiedot on suojattava paljastumiselta. Varmentajan tulee huolehtia siitä, että laatuvarmenteen tietosisältö on laatuvarmenteeseen perustuvaan sähköiseen allekirjoitukseen luottavan tahon saatavilla esimerkiksi merkistämällä laatuvarmenne julkiseen hakemistoon tai sopimalla hakijan kanssa muista menettelytavoista.

3.5.1.3. Tietojen tallettaminen laatuvarmenteen hakemisesta

Kaikki rekisteröintiin liittyvät tapahtumat on tallennettava mukaan lukien laatuvarmenteen uusiminen tai vaihtaminen. Kaikki hyväksytyt varmentamispyynnöt on rekisteröitävä.

3.5.2. Laatuvarmenteiden luominen

Laatuvarmenne luodaan rekisteröinnin yhteydessä saatujen tietojen perusteella ja allekirjoitetaan varmentajan yksityisellä avaimella (laatuvarmenteiden allekirjoitusavain) tehdyllä kehittyneellä sähköisellä allekirjoituksella.

3.5.2.1. Laatuvarmenteiden luonti

Laatuvarmenteiden luontipalvelun tulee säilyttää tietojen alkuperäisyys, luottamuksellisuus ja eheys. Laatuvarmenne voidaan luoda ainoastaan mikäli hakemus täyttää varmennepolitiikan ehdot.

Laatuvarmenteiden allekirjoittaminen tulee tapahtua siihen tarkoitukseen tarkoitettulla avaimella. Samaa avainta voidaan käyttää myös sulkulistojen allekirjoittamiseen.

Laatuvarmenteiden on täytettävä direktiivin liitteen I vaatimukset (ETSI TS 101 862) ja erityisesti seuraavat ominaisuudet:

- laatuvarmenteen julkinen avain vastaa hakijan yksityistä avainta

- laatuvarmenteessa on varmentajan laatuvarmenteiden allekirjoitusavaimella tehty kehittynyt sähköinen allekirjoitus
- laatuvarmenteessa on luotettavilla järjestelmillä tai prosesseilla luotu ainutkertainen varmenteen yksilöivä tunniste
- laatuvarmenteesta on käytävä ilmi voimassaoloaika sekä voimassaoloajan alkamisen että loppumisen muodossa
- käytettyjen algoritmien ja avainpituuksien tulee vastata EESSI:n algoritmi työryhmän asettamia vaatimuksia
- viittaus varmentajan toteuttamaan varmennepolitiikkaan

3.5.2.2. *Laatuvarmenteiden uusiminen*

Laatuvarmenteiden uusimisen tulee tapahtua ennen voimassaolon päättymistä.

3.5.2.3. *Ristiinvarmennus*

Ristiinvarmennuksessa on varmistettava, että osapuolien tietoturva- ja varmennepolitiikat sekä tietoturva- ja varmennuskäytännöt vastaavat toisiaan.

3.5.2.4. *Tietojen tallettaminen laatuvarmenteiden luomisesta*

Seuraavat tapahtumat laatuvarmenteiden luomisesta tulisi tallentaa:

- kaikki varmentajan varmenteiden elinkaaren hallintaan liittyvät tapahtumat,
- kaikki varmentajan laatuvarmenteiden allekirjoitusavainten elinkaaren hallintaan liittyvät tapahtumat,
- kaikki asiakkaiden laatuvarmenteiden elinkaaren hallintaan liittyvät tapahtumat,
- kaikki ristiinvarmennuspyynnöt ja vastaukset.

3.5.3. Laatuvarmenteiden jakelu

Laatuvarmenne luovutetaan varmenteen hakijalle ja myös muille tahoille mikäli allekirjoittajan kanssa ei ole sovittu siitä, että allekirjoittaja itse toimittaa varmenteen siihen luotettaville tahoille. Lisäksi varmentajan tehtävänä on jakaa laatuvarmenteisiin liittyvä varmennepolitiikka ja varmennuskäytäntö.

3.5.4. Laatuvarmenteiden peruuttaminen eli sulkulistapyyntöjen hallinta

Palvelun tarkoituksena on vastaanottaa peruuttamisilmoituksia ja tehdä ilmoitusten perusteella päätöksiä varmenteiden asettamisesta sulkulistalle.

3.5.4.1. *Laatuvarmenteiden statuksen muutospyynnöt*

Laatuvarmenne voidaan asettaa sulkulistalle joko allekirjoittajan pyynnöstä tai jos siihen muutoin on erityistä syytä. Ennen lopullista peruuttamista laatuvarmenne voidaan asettaa keskeytykseen (suspension-tila), josta se on vielä palautettavissa käyttöön (esimerkiksi allekirjoittajan pyynnöstä). Peruuttamisen jälkeen laatuvarmennetta ei voi enää palauttaa käyttöön.

Varmentajan tulee käsitellä peruuttamis- tai keskeytyspyynnöt välittömästi ja siten, että kaikki pyynnöt tunnistetaan ja hyväksytään riittävällä tarkkuudella. Sulkulistojen päivityksen tulee tapahtua ilman ylimääräisiä viiveitä – kuitenkin viimeistään 24 tunnin kuluessa pyynnön saapumisesta.

3.5.4.2. *Laatuvarmenteiden peruuttaminen tai keskeytys*

Varmentajan ja sen käyttämien luotettavien järjestelmien on kyettävä peruuttamaan kaikki varmentajan myöntämät laatuvarmenteet olosuhteista riippumatta. Laatuvarmenteiden peruuttaminen voidaan päivittää joko reaaliaikaisesti tai säännöllisin väliajoin.

3.5.4.3. *Tietojen tallettaminen laatuvarmenteen sulkulistapyynnöistä*

Sulkulistapyyntöjen hallinnassa tulee tallettaa kaikki tiedot laatuvarmenteiden statuksen muuttamispyyntöistä.

3.5.5. Laatuvarmenteiden voimassaolon tarkistaminen eli sulkulistapalvelu

Laatuvarmenteisiin luottavien tahojen tulee olla mahdollista tarkistaa laatuvarmenteiden voimassaolo sulkulistapalvelun avulla. Sulkulistapalvelu voi olla joko reaaliaikainen tai sen täytyy päivittyä säännöllisin väliajoin.

3.5.5.1. *Laatuvarmenteiden sulkulistatiedot*

Sulkulistapalvelun on varmistettava, että laatuvarmenteiden statustiedot tulevat luotettavalta sulkulistapyyntöjen hallinnalta.

3.5.5.2. *Laatuvarmenteiden sulkulistakyselyt ja vastaukset*

Kaikki sulkulistavastaukset tai sulkulistat tulee allekirjoittaa. Vastauksen tulee sisältää allekirjoitusaika.

3.5.5.3. *Tietojen tallettaminen sulkulistapalvelun käytöstä*

Sulkulistapalvelujen käytöstä voidaan tallettaa lokitietoihin kaikki laatuvarmenteen tarkistuspyynnöt ja vastaukset.

3.5.6. Aikaleimapalvelu (lisäpalvelu)

Palvelun tarkoituksena on tuottaa aikaleima, jonka perusteella voidaan todistaa tietyn datan olemassaolo ennen kyseistä ajanhetkeä. Tätä tietoa voidaan käyttää kiistämättömyyden saavuttamiseksi.

3.5.6.1. *Aikaleimapyyntöjen oikeellisuus*

Aikaleimapyyntöjen oikeellisuus on tarkistettava ja pyyntöjen on oltava toteutettu EESSI-projektin algoritmiyöryhmän määrittelemillä turvallisilla algoritmeilla.

3.5.6.2. *Täsmällisen ajan määrittely*

Ajanlähteen tarkkuuden tulee olla vähintään 1 sekunti. Luotettavan ajan varmistamiseksi voi käyttää kahta erillistä ajanlähdeä.

3.5.6.3. *Aikaleimatiedon luonti*

Aikaleiman yhteydessä käytettävän sarjanumeron tulee olla ainutkertainen. Ajan lisäksi aikaleiman tulee sisältää tieto käytetyn ajanlähteen tarkkuudesta sekä tieto käytetystä politiikasta, jonka mukaisesti aikaleimapalveluiden tarjoaja toimii.

3.5.6.4. *Tietojen tallettaminen aikaleimapalvelun käytöstä*

Aikaleimapalvelun käytöstä tulisi tallentaa seuraavat tiedot:

- aikaleimapalvelun varmenteen uusimiseen tai avainten vaihtoon liittyvät tapahtumat,
- aikaleimapalvelun allekirjoitusavaimen elinkaaren hallintaan liittyvät tapahtumat,
- luotettuihin ajanlähteisiin liittyvät ongelmat.

3.5.7. Turvallisen allekirjoituksen luomisvälineen jakelu

Palvelun tarkoituksena on valmistella ja luovuttaa allekirjoittajalle allekirjoituksen luomistiedot ja/tai turvallinen allekirjoituksen luomisväline. Tämä palvelu voi esimerkiksi luoda asiakkaan avainparin ja luovuttaa yksityisen avaimen turvalliselle allekirjoituksen luomisvälineelle, esimerkiksi toimikortille tallennettuna. Turvallisen allekirjoituksen luomisvälineen luovuttamiseen voi kuulua myös esimerkiksi aktivointitietojen asettaminen.

3.5.7.1. Allekirjoituksen luomisvälineen valmistelu

Turvallisen allekirjoituksen luomisvälineen vaatimustenmukaisuudesta on varmistuttava, ja valmistelu on tehtävä turvallisessa ympäristössä. Valmistelun on tapahduttava turvallisista arvoja käyttäen ja tehtävään oikeutettujen henkilöiden toimesta. Luomisvälineeseen jäävän konfiguroinnin on oltava turvallinen eikä sitä tule voida väärinkäyttää.

Avaimet on luotava turvallisesti, ja mikäli avaimet luodaan allekirjoituksen luomisvälineen ulkopuolella, on niiden siirrossa käytettävä luotettavaa kanavaa. Kun avaimet on siirretty allekirjoituksen luomisvälineelle, tulee mahdolliset avainten luomisessa syntyneet kopiot hävittää.

3.5.7.2. Allekirjoituksen luomisvälineen jakelu/luovutus

Varmentajan on taattava allekirjoituksen luomisvälineen luovutus ainoastaan oikealle ja todennetulle laatuvarmenteen hakijalle.

3.5.7.3. Aktivointitietojen luonti ja jakelu

Allekirjoituksen luomisvälineen aktivointitiedot on luotava luotettavasti ja toimitettava laatuvarmenteen hakijalle allekirjoituksen luomisvälineestä erillään. Myöskään varmentajan käyttämällä henkilöstöllä ei saa olla mahdollisuutta käyttää allekirjoituksen luomisvälinettä väärin.

3.6. Luotettavuuteen ja tietoturvasuhteisiin liittyvä dokumentaatio

Varmentajalla on oltava kirjallisesti määriteltynä ne toimintatavat ja periaatteet sekä laitteet ja ohjelmistot, joiden avulla varmentaja kattaa lain vaatimukset mukaan lukien tietoturvasuhteiden eri osa-alueet. Lain vaatimuksien täyttymistä ja toiminnan luotettavuutta voidaan arvioida seuraavien kohtien mukaisella dokumentaation avulla:

3.6.1. Hallinnolliset ja johtamista koskevat menettelytavat

Varmentajan hallinnollisten ja johtamista koskevien menettelytapojen tulee olla kirjallisesti määritelty. Dokumentaation tulee sisältää eri toimintojen vastuiden jako.

3.6.2. Tietoturvasuhteiden ja -periaatteet sekä riskien hallinta

Varmentajalla tulee olla johdon hyväksymä tietoturvasuhteiden ja -periaatteiden politiikka, jota koko organisaatio on sitoutunut noudattamaan. Tietoturvasuhteiden ja -periaatteiden politiikassa määritellään minimivaatimukset koko toiminnan tietoturvalle. Tietoturvasuhteiden ja -periaatteiden politiikan on tarkoitus olla yleisen tason dokumentti, jossa määritellään tavoitteita. Tietoturvasuhteiden ja -periaatteiden politiikkaa tarkentavat tietoturvasuhteiden ja -periaatteiden, joiden perusteella voidaan laatia yksityiskohtaisia toimintaohjeita. Tietoturvasuhteiden ja -periaatteiden tulee ottaa kantaa yleisiin tietoturvasuhteisiin koko organisaation osalta, kun varmennepolitiikka ja varmennuskäytäntö kattavat toiminnan varmennepalvelujen osalta.

3.6.3. Varmennepolitiikka ja varmennuskäytäntö

Varmennepolitiikka (Certificate Policy CP) on dokumentti, jonka perusteella varmentaja myöntää varmenteita ja joka käyttäjän pitää hyväksyä. Varmennepolitiikan perusteella voidaan arvioida varmentajan toimia ja asetettujen vaatimuksien täyttymistä.

Varmennepolitiikassa määritellään säännöt varmentajan toiminnalle, ja sen perusteella voidaan siten arvioida varmenteiden käytettävyyttä tiettyyn sovellukseen. Varmennepolitiikka on korkean tason dokumentti, joka vastaa kysymykseen mitä varmentaja tekee ja määrittelee siten vaatimuksia varmentajan toiminnalle ja johdolle. Varmennepolitiikka voi olla yhteinen useille eri varmentajille. ETSI:ssä on määritelty mallipolitiikka laatuvarmenteita tarjoaville varmentajille (ETSI TS 101 456, Policy requirements for certification authorities issuing qualified certificates).

Varmentajalla on oltava kirjallisesti määriteltynä omaan organisaatioonsa soveltuva varmennuskäytäntö (Certification Practise Statement, CPS), joka on tarkempi kuvaus siitä, miten varmentaja omassa organisaatiossaan toteuttaa varmennepolitiikkaa. CPS:n avulla voidaan tutkia kuinka varmentaja on toteuttanut politiikan ja täyttääkö varmentaja politiikan vaatimukset. Varmennuskäytännön tulisi sisältää IETF:n RFC 2527:n (Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practises Framework) mukaiset asiat. Varmennepolitiikka ja varmennuskäytäntö on oltava julkisesti saatavilla esimerkiksi varmentajan www-sivuilla.

3.6.4. PDS (PKI Disclosure Statement)

Varmennepolitiikka ja varmennuskäytäntö ovat dokumentteja joita käytetään riskien ja varmentajan toimien tietoturvan ja luotettavuuden arvioimiseksi. Nämä dokumentit ovat kuitenkin usein turhan laajoja tiedon välittämiseksi asiakkaille ymmärrettävästi, selkeästi ja yksiselitteisesti. Tätä tarkoitusta varten varmentajalla on mahdollisuus laatia ns. PDS, joka on selkeämpi ja yksinkertaistettu kuvaus laatuvarmenteiden käytön ehdoista ja rajoituksista.

3.6.5. Allekirjoituspolitiikka (Signature Policy)

Allekirjoituspolitiikka sisältää hyväksytyjä toimintatapoja allekirjoituksen hyväksymiseksi ja sitä voidaan käyttää allekirjoittajan ja allekirjoituksen vastaanottajan välisen luottamuksen lisäämiseksi ja yhteisten pelisääntöjen muodostamiseksi. Allekirjoituspolitiikka sisältää säännöt mm.

- sulkulistojen käytöstä,
- avainten luomisesta (itse/varmentaja),
- allekirjoituksen luomisvälineiden käytöstä,
- aikaleimapalvelujen käytöstä,
- algoritmien ja avainpituuksien hyväksymisestä,
- arkistoinnista,
- yksityisten avainten suojaamisesta,
- attribuuttien käytöstä.

4. Viestintäviraston suorittama varmentajien valvonta

Viestintäviraston tehtävänä on valvoa niiden Suomeen sijoittautuneiden varmentajien toimintaa, jotka tarjoavat sähköisiin allekirjoituksiin liittyviä laatuvarmenteita yleisölle. Valvonnan kannalta tarpeellisia luotettavuus- ja tietoturva-vaatimuksia on esitetty omassa kappaleessaan.

Varmentajan toiminnassa havaitut puutteet ja huomautukset sekä Viestintäviraston toimenpiteet voidaan luokitella kolmeen ryhmään:

1. Kieltopäätökset (SakL 9 §)

Erittäin vakavan puutteen ilmetessä Viestintävirasto tekee viipymättä kieltopäätöksen, jolloin varmentaja ei saa jatkaa varmenteidensa myöntämistä laatuvarmenteina. Viestintävirasto tekee varmentajan osalta muutoksen ylläpitämäänsä listaan laatuvarmenteiden tarjoajista (esimerkiksi poistamalla varmentajan listalta tai merkitsemällä laatuvarmenteiden tarjonnan päättyneen). Jos varmentaja korjaa virheensä, se voi jatkaa uudelleen laatuvarmenteiden tarjoamista puutteet korjattuaan. Laatuvarmenteiden tarjoamisen aloittaminen uudelleen edellyttää kuitenkin ilmoitusta Viestintävirastolle, joka silloin tutkii täyttääkö varmentaja tai varmenne lain vaatimukset. Esimerkkejä tällaisesta tilanteesta ovat:

- varmentajan allekirjoitusavain paljastuu ulkopuolisille,

- varmentaja kopioi tai luovuttaa ulkopuolisille varmenteen haltijoiden yksityisiä avaimia,
- varmentajan käyttämät algoritmit ja avainpituudet ovat heikkoja,
- varmentaja on lopettanut sulkulistan ylläpidon,
- varmentaja laiminlyö laatuvarmenteen hakijan tunnistamisen,
- varmenteen sisältö ei vastaa laatuvarmenteele asetettuja vaatimuksia,
- varmentajan varmenteiden allekirjoitusavainta käytetään hallitsemattomasti.

2. Velvoitepäätökset

Niiden puutteiden osalta, jotka eivät edellytä kieltopäätöstä, varmentaja voidaan velvoittaa lain 27 §:n mukaisesti korjaamaan virheensä tai laiminlyöntinsä. Velvoitepäätöksessä varmentajalle voidaan antaa aikaa tilanteen korjaamiseksi ja päätöksen tehosteeksi voidaan asettaa uhkasakko, toiminnan keskeyttämisuhka tai teettämisuhka. Toiminnan keskeyttämisuhka voi koskea lain soveltamisalaan kuuluvan toiminnan osaa tai koko toimintaa. Tehosteeksi asetetun uhan on oltava suhteessa valvottavan tahon virheen tai laiminlyönnin vakavuuteen. Uhkasakko tai teettämisuhka ovat ensisijainen tehokeino lain velvoitteiden täyttämiseksi, jos välitöntä kieltopäätöstä ei ole tarvetta tehdä. Toiminnan keskeyttämisuhkaa käytetään pääsääntöisesti vain tilanteissa, jossa valvottava taho ei ole korjannut virhettään tai laiminlyöntiään uhkasakosta tai teettämisuhasta huolimatta. Esimerkkejä tilanteista, joissa voidaan antaa velvoitepäätös ovat:

- viiveet sulkulistojen päivityksissä suhteessa varmentajan politiikan vaatimuksiin,
- poikkeamiset varmennepolitiikan ja varmennekäytäntöjen mukaisista toimintatavoista,
- puutteet toiminnassa hävitettävien tietojen käsittelyn osalta,
- puutteet varmuuskopioiden käsittelyssä,
- puutteet henkilöstön vastuissa ja tehtäväkuivissa.

3. Muut huomautukset

Muiden huomautusten osalta Viestintävirasto voi antaa varmentajalle aikaa korjata toimintansa tiettyyn ajankohtaan, esimerkiksi seuraavaan vuosiraporttiin tai tarkastukseen mennessä. Huomautukset koskevat vähäisiä havaittuja puutteita.

4.1. Viestintävirastolle toimitettavat tiedot

Varmentajan, joka tarjoaa laatuvarmenteita yleisölle, on tehtävä Viestintävirastolle toimintansa aloittamista koskeva ilmoitus, jonka jälkeen on varmentajalla myös velvollisuus ilmoittaa muutoksista sekä raportoida Viestintävirastolle toiminnastaan vuosittain. Tiedot on toimitettava kirjallisesti. Kirjallisen muotovaatimuksen täyttää myös sähköisesti toimitettu ilmoitus siten kuin sähköisestä asioinnista hallinnossa erikseen säädetään.

4.1.1. Rekisteröinti ja toiminnan aloittaminen

Varmentajan, jonka tarkoituksena on tarjota laatuvarmenteita yleisölle, on ennen toiminnan aloittamista tehtävä kirjallinen ilmoitus (rekisteröinti) Viestintävirastolle (SakL 9 § 1 mom). Ilmoituksen tulee sisältää tiedot, joiden perusteella varmentajan toimintaa voidaan arvioida yksiselitteisesti. Ilmoituksista selvinneiden puutteiden tai virheellisen toiminnan vuoksi Viestintäviraston on viipymättä kiellettävä varmentajaa tarjoamasta varmenteitaan laatuvarmenteina, jos varmenne tai varmentaja eivät täytä laissa säädettyjä vaatimuksia. Varmentajalla on kuitenkin mahdollisuus esittää tarkennuksia tai lisätietoja Viestintäviraston pyynnön mukaisesti ennen kuin Viestintävirasto tekee kieltopäätöksen, ellei kyseessä ole sellainen varmentajan toiminnan luotettavuuteen ja tietoturvasuhteeseen kohdistuva puute, jonka vuoksi Viestintävirasto on lain mukaan velvoitettu tekemään kieltopäätöksen viipymättä.

Ilmoituksen tulee sisältää varmentajan yhteystiedot, kuten:

- yrityksen nimi
- Y-tunnus
- postiosoite

- käyntiosoite
- puhelinnumero
- fax-numero
- yhdyshenkilö
- sähköpostiosoite
- linkki www-sivuille (URL, Uniform Resource Locator)
- kaupparekisteriote

Varmentajan on toimitettava Viestintävirastolle tiedot, joiden perusteella varmentajan toimien luotettavuutta ja tietoturvallisuutta voidaan arvioida harjoitettavan varmennetoiminnan suhteen. Näitä tietoja ovat mm:

- varmentajan hallinnolliset ja johtamista koskevat menettelytavat,
- varmentajan toimien tietoturvapoliittikka ja -periaatteet sekä riskien hallinta,
- menettelytavat, joiden mukaisesti varmentaja myöntää laatuvarmenteita (varmennepoliittikka, CP certificate policy),
- yksityiskohtaiset tiedot varmennepoliittikan menettelytapojen toteuttamisesta (varmennuskäytäntö, CPS certification practise statement),
- selvitys varmentajan taloudellisista voimavaroista,
- varmentajan käyttämän henkilöstön pätevyys ja tehtäväkuvaukset / yleinen organisaatiokuvaus,
- tiedot tai kuvaus varmentajan varmennepalveluissaan käyttämistä järjestelmistä ja tuotteista,
- tiedot apuna käytetyistä henkilöistä (rekisteröinti, laatuvarmenteiden luominen, laatuvarmenteiden jakelu, sulkulistapyyntöjen hallinta, sulkulistapalvelu) esimerkiksi alihankkijoista,
- tiedot myöntämiensä laatuvarmenteiden tietosisällön rakenteesta,
- tiedot tarjoamistaan laatuvarmenteisiin liittyvistä palveluista sekä niiden sopimusehdot ja hinnastot,
- selvitys käytetyistä ohjelmistoista (ml. käytetyt avainpituudet ja algoritmit),
- tiedot noudatetuista standardeista,
- tiedot mahdollisista pätevydentoteamislaitosten tekemistä arvioinneista.

4.1.2. Vuosiraportti

Varmentajan on toimitettava Viestintävirastolle vuosittain raportti toiminnastaan. Vuosiraporttiin tulee sisältyä tiedot, joiden perusteella Viestintävirasto voi todeta varmentajan toiminnalle asetettujen toiminnan luotettavuutta ja tietoturvallisuutta koskevien vaatimusten täyttymisen. Raportin tulee kattaa varmentajan koko sähköisiin allekirjoituksiin ja laatuvarmenteisiin liittyvä varmennetoiminta.

Vuosiraportin tulee sisältää vastaavat tiedot kuin mitä ilmoituksessa toiminnan aloittamisen yhteydessä vaaditaan. Tietoja ei kuitenkaan tarvitse toimittaa, mikäli muutoksia toiminnassa ei ole tapahtunut eikä Viestintävirastolle toimitetussa dokumentaatiossa ole tapahtunut muutoksia tai tiedot näistä muutoksista on jo toimitettu Viestintävirastolle.

Vuosiraporttiin tulee lisäksi sisältyä tiedot toiminnan laajuudesta edellisellä vuonna (esimerkiksi vuosikertomus) sekä tilastointi havaituista ongelmatilanteista ja muut toiminnan kannalta merkittävät tapahtumat. Näitä ovat esimerkiksi:

- myönnettyjen laatuvarmenteiden lukumäärä,
- peruutettujen laatuvarmenteiden määrä,
- asiakasvalitusten määrä (mahdollisesti erikseen laskutusvalitukset ja palvelun vikaa tai häiriötä koskevat valitukset),
- varmennepoliittikan muutokset,
- käytettyjen laitteiden ja ohjelmistojen olennaiset muutokset,
- muut oleelliset muutokset Viestintävirastolle toimitetuissa tiedoissa.

4.1.3. Toiminnan muutokset

Varmentajan on ilmoitettava viipymättä Viestintävirastolle kaikista varmennetoimintaan liittyvistä muutoksista, jotka koskevat Viestintävirastolle toimitettuja tietoja varmentajan toiminnasta (SakL 9 § 3 mom).

Viestintävirastolle viipymättä ilmoitettavia tietoja ovat esimerkiksi muutokset Viestintäviraston ylläpitämässä julkisessa rekisterissä olevissa tiedoissa sekä merkittävästi varmentajan toiminnan tietoturvallisuuteen ja luotettavuuteen liittyvät muutokset ja tapahtumat.

Varmentajasta julkisessa rekisterissä ylläpidettäviä tietoja ovat esimerkiksi:

- laatuvarmenteiden nimi,
- laatuvarmenteiden myöntämisessä käytetty varmennepolitiikka (OID numero),
- varmentajan yhteystiedot (nimi, postiosoite, www-osoite, puhelinnumero),
- varmentajan yhteyshenkilö,
- varmentajan toiminnan lopettaminen,
- keskeytys varmentajan toiminnassa.

Merkittäviä tietoturvallisuuteen ja luotettavuuteen liittyviä muutoksia ovat esimerkiksi:

- varmentajan laatuvarmenteiden allekirjoitusavaimen paljastuminen,
- varmentajan sulkulistojen allekirjoitusavaimen paljastuminen,
- varmentajan asettaminen selvitystilaan.

Viestintävirastolle on myös viipymättä ilmoitettava tietoturvallisuutta ja luotettavuutta olennaisesti vaarantavista tapahtumista ja häiriötilanteista sekä näiden korjaamiseksi tehdyistä toimenpiteistä.

Näitä ovat esimerkiksi:

- häiriöt varmentajan ylläpitämien sulkulistojen toimivuudessa,
- tunkeutuminen varmentajan järjestelmiin,
- varmentajan järjestelmien päivittäminen merkittävän tietoturva-aukon johdosta.

4.1.4. Muut säännöllisesti toimitettavat tiedot

Taloudellisten voimavarojen riittävyyden valvonnan mahdollistamiseksi varmentajan tulisi toimittaa Viestintävirastolle osavuosikatsaus, mikäli varmentajan tulee sellainen lain mukaan laatia.

4.1.5. Tarkastukset

Viestintävirasto suorittaa varmennepalveluiden tarjoajien valvontaa yleistarkastusten muodossa. Viestintävirastolla on mahdollisuus tehdä ylimääräisiä tarkastuksia tarpeen vaatiessa esimerkiksi ongelmatilanteiden selvittämiseksi.

Viestintäviraston suorittama yleistarkastus suoritetaan kolmessa vaiheessa:

1. Varmentajan toimittaman materiaalin tutkiminen ja käsittely. Materiaalin tulee kattaa valvontatehtävään suorittamisen kannalta riittävät tiedot.
2. Tarkastuskäynti, jossa selvitetään varmentajan toimien ja vuosiraportissa annetun dokumentaation vastaavuus.
3. Puutteiden korjaaminen ja vuosiraportin täydentäminen puuttuvilla tiedoilla.

Viestintävirasto kirjaa kaikki tarkastuksissa havaitut puutteet ja annetut huomautukset ja antaa näistä tiedon varmentajalle. Näin syntyneiden historiatietojen avulla voidaan seurata varmentajan toiminnan kehittymistä ja arvioida varmentajan toimien luotettavuutta.

Varmentajan tarkastukseen voidaan sisällyttää varmentajan alihankkijoiden ja/tai eri toimipisteiden tarkastuksia.

4.1.6. Lopettamisilmoitus

Varmentajan tulee ilmoittaa Viestintävirastolle laatuvarmenteiden tarjoamisen päättymisestä. Ilmoituksessa tulee kertoa, kuinka varmentaja huolehtii tai tulee huolehtimaan toiminnan lopettamista koskevasta tiedottamisesta ja lain 15 §:n mukaisten tietojen säilyttämisestä.

4.2. Viestintäviraston julkaisemat tiedot

Viestintäviraston tehtävänä on ylläpitää julkista rekisteriä laatuvarmenteita myöntävistä varmentajista (SakL 9 § 4 mom). Rekisteristä on saatavissa tiedot niistä Suomeen sijoittautuneista varmentajista, jotka ovat ilmoittaneet Viestintävirastolla tarjoavansa laatuvarmenteita. Rekisterissä julkaistavat tiedot perustuvat osin varmentajalta saatuihin tietoihin ja varmentajan on ilmoitettava viipymättä Viestintävirastolle kaikista muutoksista, jotka koskevat julkisessa rekisterissä esitettyjä tietoja. Rekisteri sisältää ainakin seuraavat tiedot:

- laatuvarmenteiden nimi,
- laatuvarmenteiden myöntämisessä käytetty varmennepolitiikka (OID numero),
- varmentajan yhteystiedot (nimi, postiosoite, www-osoite, puhelinnumero),
- varmentajan toiminnan lopettaminen.

Edellä mainitut tiedot laatuvarmenteita tarjoavista varmentajista julkaistaan Viestintäviraston www-sivuilla. Rekisterin tiedoilla olisi kuitenkin ainoastaan informatiivinen tehtävä.

5. Yhteentoimivuus

Turvallisuuden ja luotettavuuden ohella tuotteiden, järjestelmien ja palvelujen yhteentoimivuus on keskeinen edellytys sähköisten allekirjoitusten ja sähköisen kaupankäynnin yleistymiselle.

5.1. Sisämarkkinaperiaatteet ja kansainväliset näkökohdat

Direktiivin 4 artiklassa määritellään sisämarkkinaperiaatteet. Direktiivin nojalla annettuja kansallisia säädöksiä sovelletaan kaikkiin jäsenvaltion alueelle sijoittautuneisiin varmennepalvelujen tarjoajiin sekä niiden tarjoamiin palveluihin. Myöskään toisesta jäsenvaltiosta peräisin olevan varmennepalvelun tarjontaa ei saa kansallisin säännöksin rajoittaa. Jäsenvaltioiden on lisäksi varmistettava, että sähköisiin allekirjoituksiin liittyvät tuotteet liikkuvat vapaasti sisämarkkinoilla.

Direktiivin 7 artiklassa käsitellään kansainvälisiä näkökohtia. Artiklassa on säännöksiä siitä, miten kolmanteen maahan sijoittautuneen varmentajan tunnustetaan oikeusvaikutuksiltaan Euroopan yhteisöjen alueella. Tunnustaminen voi tapahtua, jos varmentaja täyttää direktiivin vaatimukset ja on direktiivin tarkoittamassa akkreditointijärjestelmässä, tai jos yhteisöön sijoittautunut varmentaja takaa varmenteen, tai jos varmenne tai varmentaja on tunnustettu Euroopan yhteisön kolmannen maan tai kansainväliseen maan kanssa tekemän sopimuksen nojalla. Komissio voi antaa neuvostolle ehdotuksia määräenemmistöllä päätettävistä neuvotteluvalltuuksista näitä kansainvälisiä sopimuksia varten.

5.2. Standardointi

Sähköistä allekirjoitusta ja varmennepalveluja koskevia standardointihankkeita ja yhteistyöfoorumeita on useita. Direktiivin mukaisesti komissio voi vahvistaa ja julkaista sähköisiin allekirjoituksiin liittyviä tuotteita koskevien yleisesti tunnustettujen standardien viitenumeroita Euroopan yhteisöjen virallisessa lehdessä. Komissiota avustaa sähköisen allekirjoituksen komitea. Viestintävirasto on mukana komitean toiminnassa.

5.2.1. EESSI-projekti

EESSI-projekti (European Electronic Signature Standardization Initiative) on perustettu laatimaan standardeja tuotteille, järjestelmille ja palveluille sähköisen allekirjoituksen direktiivin vaatimusten täyttämiseksi.

Ensimmäisenä työnään EESSIn kokoama asiantuntijaryhmä laati raportin, jossa toisaalta analysoidaan ja kommentoidaan direktiivin (tuolloin vielä valmisteilla olleen luonnoksen) sisältöä ja toisaalta esitetään konkreettisia suosituksia jatkotyön organisoinnista. Tarkoituksena oli kartoittaa

tulevaisuuden tehtäviä ja standardointialueita sähköisiin allekirjoituksiin liittyen. Ensimmäisenä työnä (vaihe 1) oli asiantuntijaraportti, jossa nämä työalueet esiteltiin.

EESSIn toisessa vaiheessa ryhdyttiin standardoimaan tärkeimpiä alueita. Samalla aloitettiin tutkimushankkeita myös sellaisista tehtävälajeista, joita ei vielä nähty tarpeeksi kypsiksi standardoitaviksi. Standardointityö on jakaantunut lähinnä ETSIn tietoturvakomitean (TC SEC, Technical Committee Security) sähköisten allekirjoitusten ja infrastruktuurin työryhmän (ESI WG, Electronic Signatures and Infrastructure Working Group) ja CEN/ISSS:n sähköisten allekirjoitusten workshopin (WS/E-sign) kesken.

Joillekin standardeille (esim. sähköisen allekirjoituksen formaatti) yritetään kuitenkin yhteensopivuuden varmistamiseksi saada välitön maailmanlaajuinen hyväksyntä siten, että ne hyväksytetään myös IETF:n RFC-dokumenteiksi.

EESSIn ensimmäisen standardointivaiheen tulokset valmistuivat ETSIn osalta vuoden 2000 lopulla. Tuloksena oli neljä teknistä spesifikaatioita (TS = ETSI Technical Specification):

- TS 101 456, Varmennepoliittikka (Policy requirements for certification authorities issuing qualified certificates)
- TS 101 733, Sähköisen allekirjoituksen formaatti (Electronic signature formats)
- TS 101 862, Laatuvarmenteen profiili (Qualified certificate profile)
- TS 101 861, Aikaleiman profiili (Time stamping profile)

CEN/ISSS:n työalueiden suhteen ensimmäiset tulokset (työryhmien sopimukset, CWA = CEN Workshop Agreement) valmistuivat vuoden 2001 aikana:

- CWA 14167-1, Varmenemisen luotettavat järjestelmät (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures)
- CWA 14168 & 14169, Turvallinen allekirjoituksen luomisväline (Secure Signature-Creation Devices)
- CWA 14170, Turvavaatimukset allekirjoituksen luomisjärjestelmille (Security Requirements for Signature Creation Systems)
- CWA 14171, Allekirjoituksen todentamisen menettelyt (Procedures for Electronic Signature Verification)
- CWA 14172-1,2,3,4,5, Vaatimusten mukaisuus (Conformity Assessment Guidance)

6. Turvallinen allekirjoituksen luomisväline

Jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä (direktiivi 5 art, SakL 18 §). Käytännössä tällä tarkoitetaan rinnastusta käsinkirjoitettuun allekirjoitukseen. Turvallisen allekirjoituksen luomisvälineen (direktiivi liite III, SakL 5 §) katsotaan täyttävän säädetyt vaatimukset, mikäli se on Euroopan yhteisöjen virallisessa lehdessä julkaistujen standardien mukainen tai arviointitehtävää suorittava tarkastuslaitos on sen hyväksynyt. Eri tahoilla on kuitenkin päädytty tulkitsemaan direktiivin vaatimuksia siten, että vaikka standardien vaatimusten täyttäminen on riittävä ehto, ei valmistaja saa sitä itse todeta. Vaatimusten mukaisuuden osoittamiseen on siis käytettävä tarkastuslaitosta.

6.1. Tarkastuslaitokset

Euroopan yhteisöjen virallisessa lehdessä on 16.11.2000 julkaistu komission päätös 6.11.2000 vähimmäisedellytyksistä, jotka jäsenvaltioiden on huomioitava nimetessään turvallisen allekirjoituksen luomisvälineen tarkastuslaitoksia. Minimivaatimukset ovat seuraavat:

1. Tarkastuslaitoksen on oltava tunnistettavissa erillisenä yksikkönä.
2. Tarkastuslaitos ja sen henkilökunta eivät saa osallistua toimintoihin, jotka ovat ristiriidassa työssä vaadittavan itsenäisen arvostelukyvyn ja puolueettomuuden kanssa. Lisäksi edellytetään taloudellista riippumattomuutta.
3. Tarkastuslaitoksen ja sen henkilökunnan on toimittava luotettavasti ja riittävällä teknisellä pätevyydellä.
4. Tarkastuslaitoksen on toimittava syrjimättömällä tavalla.

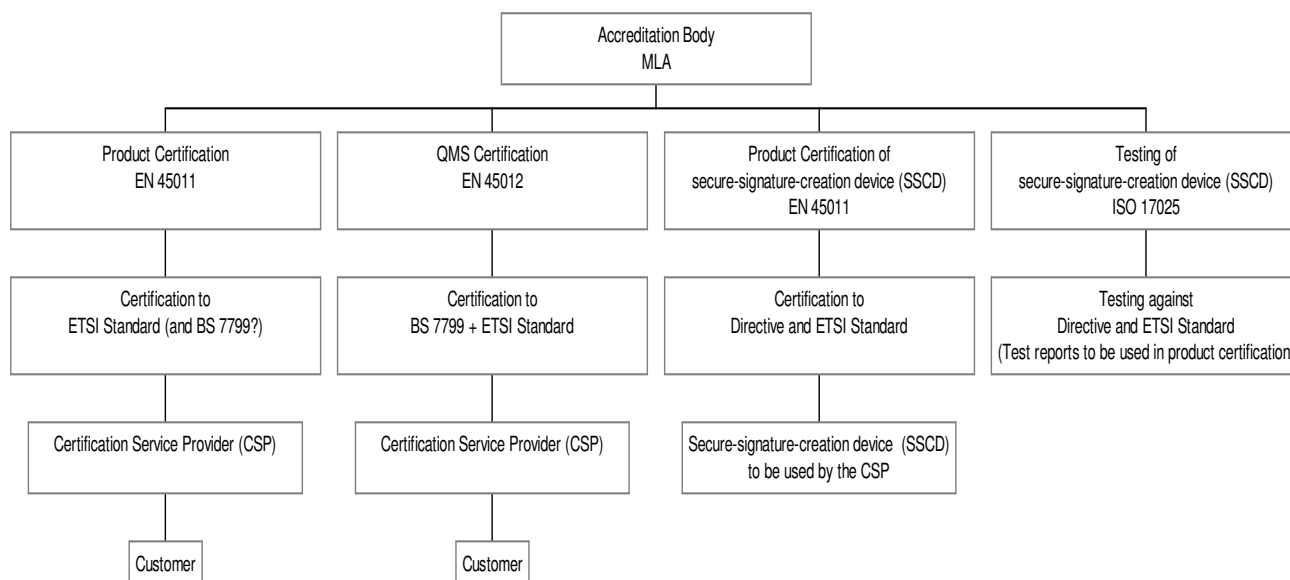
5. Tarkastuslaitoksella on oltava käytettävissään tarvittava henkilöstö ja välineistö työn suorittamiseksi ripeästi ja oikein.
6. Henkilökunnalla on oltava riittävä tekninen ja ammatillinen koulutus erityisesti sähköisen allekirjoituksen tekniikoiden ja niihin liittyvien tietoteknisten turvallisuusnäkökohtien alalta.
7. Henkilökunnan puolueettomuus on taattava.
8. Tarkastuslaitoksen on järjestettävä riittävä suoja toiminnastaan syntyvien vastuiden kattamiseksi esimerkiksi vakuutuksin.
9. Tarkastuslaitoksen on taattava toimintansa luottamuksellisuus.
10. Tarkastuslaitos kantaa täyden vastuun myös silloin kun se on ulkoistanut joitain sille kuuluvia tehtäviä.

7. Pätevydentoteamis- ja arviointilaitokset

Viestintävirasto voi hyödyntää valvontatehtävässään varmentajien suorittamien vapaaehtoisuuteen perustuvien akkreditointi- tai sertifiointilaitosten tuloksia.

7.1. Akkreditointi

Akkreditointia suorittaa Suomessa FINAS (the Finnish Accreditation Service) Mittatekniikan keskuksen (MIKES) palveluna. Akkreditointitoiminta kohdistuu usein erilaisiin testauslaboratorioihin ja sertifiointilaitoksiin. Akkreditoinnin suhde varmennepalveluihin voidaan kuvata oheisen kuvan mukaisesti. Kuten myös kuvasta käy ilmi, ei akkreditointitoiminta tyypillisesti suoraan kohdistu varmennepalveluihin. Useissa yhteyksissä direktiivin termi akkreditointi onkin tulkittu sertifiointina, koska direktiivin määritelmien mukainen toiminta ei vastaa Eurooppalaisen akkreditointielinten järjestön (EA) määritelmiä akkreditointielinten toiminnalle.



7.2. Sertifiointi

Sertifiointitoimintaa suorittavia organisaatioita on useita. Sähköisiin allekirjoituksiin liittyvien tuotteiden ja palveluiden sertifiointia ei Suomessa mikään taho kuitenkaan tällä hetkellä vielä suorita ja tilanne on pitkälti sama myös muualla Euroopassa. Syynä tämän kaltaisen toiminnan puuttumiseen on markkinoiden pienuus tällä hetkellä sekä arviointikriteerien puute. Euroopassa on perustettu joitain arviointijärjestelmiä kuten tScheme (Iso-Britannia) ja TTP.NL (Hollanti).

7.3. Turvallisten allekirjoituksen luomisvälineiden arviointilaitokset

Suomessa ei tällä hetkellä suoriteta turvallisten allekirjoitusten luomisvälineiden arviointeja. Turvallisia allekirjoituksen luomisvälineitä arvioivia laitoksia on ainakin Saksassa.

8. Maksut

8.1. Maksut varmentajilta

Viestintävirasto on nettobudjetoitu virasto ja syntyneet kustannukset katetaan erilaisilla maksuilla. Esimerkkinä voidaan mainita Viestintävirastolle telemarkkina- ja laissa yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturva-asetetut tehtävät, joita Viestintävirasto rahoittaa pääasiassa teleyrityksiltä perittävillä numerointimaksuilla. Viestintäviraston maksuista säädetään valtion maksuperustelaisissa ja lisäksi on annettu liikenne- ja viestintäministeriön asetus 842/2001 Viestintäviraston maksuista.

Laki sähköisistä allekirjoituksista lisää Viestintäviraston tehtäviä uudella varmennetoiminnan alueella. Laissa asetettu valvontavollisuus kohdistuu lähinnä laatuvarmenteita tarjoaviin varmentajiin, eikä siten esimerkiksi teleyrityksiltä perittävillä maksuilla voida kattaa varmentajien valvonnasta aiheutuvia kustannuksia. Viestintävirasto tulee perimään maksuja varmennetoiminnasta valvontatoiminnan kattamiseksi. Maksuja peritään ainoastaan valvontatoiminnan kulujen kattamiseksi, eikä näihin maksuihin sisällytetä tietoturva-alueen muita kustannuksia. Viestintäviraston maksut määritellään vuosittain.

Toiminnan aloituksen yhteydessä suoritetaan Viestintävirastolle maksu, jonka suuruus määritellään liikenne ja viestintäministeriön Viestintäviraston maksuista antamassa asetuksessa. Maksun suuruus määritellään siten, että se kattaa toiminnan aloittamisilmoituksen ja sen liitteiden tarkistamisesta aiheutuneet kulut.

Varmentajan vuosimaksu voisi perustua esimerkiksi myönnettyjen laatuvarmenteiden lukumäärään. Vuosimaksun suuruutta muutetaan toiminnan muutosten mukaisesti esimerkiksi siten, että varmennetoiminnan kehittyessä ja lisääntyessä Viestintäviraston keräämät maksut vastaavat varmentajien valvonnasta aiheutuvia kuluja.

8.2. Arviointilaitosten valvontamaksut

Viestintäviraston tehtävänä on toimia myös turvallisten allekirjoitusten luomisvälineiden tarkastuslaitosten valvojana. Euroopan yhteisöjen komissio on antanut päätöksen kyseisten laitosten vähimmäisedellytyksistä, jotka jäsenvaltioiden on otettava huomioon nimetessään kyseisiä laitoksia. Nimeämisen tekee Viestintävirasto, mutta toistaiseksi ei ole selvää, onko laitosten nimeämiselle tarvetta.

9. Työryhmän ehdotukset

9.1. Maksut varmentajilta

Varmennetoiminta ei ole vielä käynnistynyt laajamittaisesti, ja siten ei myöskään ole helppo arvioida toiminnan varsinaisia taloudellisia mahdollisuuksia tai rajoituksia. Työryhmän toimijoiden mielipide kuitenkin on, että varmennetoiminnalle ei tulisi asettaa turhia taloudellisia raskaita, sillä ne saattavat olla este toiminnan käynnistymiselle. Samalla tietoyhteiskunnan palvelujen tarjonnan kehittymiselle voi muodostua esteitä esimerkiksi henkilön luotettavaa tunnistamista vaativien palveluiden osalta.

Maksujen suhteen työryhmä esittää kantanaan kerättävien valvontamaksujen minimointia ja valvonnan pitämistä mahdollisimman kevyenä, mutta kuitenkin riittävänä toiminnan luotettavuuden ja toimijoiden yhdenvertaisen kohtelun takaamiseksi. Työryhmän ehdotuksena on maksurakenteen määräytyminen varmentajilta perittävistä maksuista käsittelykappaleen mukaisesti ja maksujen suuruuden määräytyminen kehittyneiden markkinoiden laajuuteen.

perustuen. Tällöin valvontamaksut olisivat toiminnan laajuuteen perustuvia ja toiminnan laajuus määriteltäisiin voimassaolevien laatuvarmenteiden lukumäärän mukaisesti. Maksurakenteessa määritellyt luokat tulisi myös hinnoitella epälineaaraisesti siten, että toiminnan laajeneminen olisi kannattavaa ja maksu voimassaolevaa varmennetta kohden putoaisi volyymin kasvaessa.

Vuosittaisen valvontamaksun lisäksi laatuvarmenteita tarjoavilta varmentajilta perittäisiin maksu toiminnan aloittamisesta. Tämän maksun suuruuden tulisi olla suhteessa Viestintäviraston tekemään arviointityöhön ottaen huomioon toiminnan aloittamisen yhteydessä toimitetun materiaalin tutkinnan laajuus.

9.2. Viestintäviraston määräykset ja suositukset

Työryhmä on laatinut raportin ohessa kaksi luonnosta Viestintäviraston määräyksiksi laatuvarmenteita yleisölle tarjoaville varmentajille. Nämä määräykset koskevat Viestintävirastolle valvontatehtävien hoitamiseksi toimitettavia tietoja sekä varmentajan tietoturvasuoritus- ja luotettavuusvaatimuksia.

Määräysten tarkoituksena on selkeyttää laatuvarmenteita tarjoavien varmentajien toimintaan liittyviä kysymyksiä sekä muodostaa yhtenäinen käytäntö eri toimijoiden ja Viestintäviraston toiminnalle. Määräysten ei siten ole tarkoitus mitenkään lisätä laissa määriteltyjä velvollisuuksia ja vastuita vaan ainoastaan selkeyttää niitä. Ongelmana varmennetoiminnalle on käytännön toimintalinjojen ja yhteisten pelisääntöjen puuttuminen.

Määräysten lisäksi on laadittu luonnokset määräyksiä vastaavista suosituksista, joissa edelleen tarkennetaan määräysten tekstejä ja annetaan esimerkkejä määräysten toteuttamisesta käytännössä.

Sekä määräykset että suositukset on pyritty laatimaan siten, että tekninen kehitys ei muodostaisi estettä niiden toteuttamiselle. Vaikka käsiteltävä alue on uusi ja voimakkaan kasvun ja mahdollisesti myös muutosten kohteena, on määräysten voimassaoloajaksi määritelty viisi vuotta. Tarvittaessa määräyksiä tullaan muokkaamaan toiminnan vaatimusten edellyttämällä tavalla.

LIITE 1: Laatuvarmenteita tarjoavan varmentajan tietoturvallisuuden tarkistuslista**SISÄISET TOIMINNOT (PROSESSIT JA TOIMINTATAVAT)****1. Hallinnolliset vaatimukset (Management)**Järjestelmän ja turvallisuuden hallinta

- Onko varmentajan tietoturvallisuuspolitiikka määritelty?
- Onko tietoturvallisuuspolitiikan toimeenpanosta vastuullinen henkilö nimetty?
- Onko nimetty valmiuspäällikkö vastaamaan poikkeusolojen valmiussuunnittelusta?
- Tukeeko järjestelmä rooleja eri käyttöoikeuksilla?
- Tarjoaako varmentajan järjestelmä riittävät mahdollisuudet tehtävien eriyttämiseen, esimerkiksi seuraaviin rooleihin?
 - tietoturvallisuusvastaava
 - rekisteröintivastaava
 - järjestelmän ylläpitäjä
 - järjestelmä käyttäjä
 - järjestelmän arvioija
- Mahdollistaako järjestelmä käyttäjätunnusten yhdistämisen näihin rooleihin?
- Onko järjestelmän arvioijan ja tietoturvallisuusvastaavan roolit erotettu toisistaan ja niitä hoitavat eri henkilöt?
- Onko järjestelmän ylläpitäjän rooli erotettu arvioijan ja tietoturvallisuusvastaavan rooleista ja nämä tehtävät jaettu eri henkilöille?

2. Järjestelmät ja toiminnotToimintojen hallinta

- Tarjoaako varmentajan järjestelmien valmistaja ohjeet, jotka takaavat seuraavat asiat?
 - varmentajan järjestelmää voidaan käyttää oikein ja turvallisesti
 - varmentajan järjestelmää voidaan käyttää siten, että järjestelmän tai jonkin sen osan pettämisen riski on mahdollisimman pieni
 - varmentajan järjestelmä voidaan suojata viruksilta ja vahingollisilta ohjelmilta
- Tarjoaako valmistaja seuraavat ohjekirjat?
 - asennusohje
 - ylläpito-ohje
 - käyttöohje

Toiminnan jatkuvuus

- Onko nimetty valmiuspäällikkö vastaamaan poikkeusolojen valmiussuunnittelusta?
- Kestävätkö seuraavat varmentajan järjestelmän osat yksittäiset virhetilanteet toiminnan jatkuessa keskeytyksettä?
 - laatuvarmenteiden jakelu
 - laatuvarmenteiden sulkulistapyyntöjen hallinta
 - laatuvarmenteiden sulkulistapalvelu
- Voidaanko järjestelmän pettäessä siirtyä käyttämään varajärjestelmää?
- Tapahtuuko siirtyminen varajärjestelmään vaarantamatta järjestelmän luottamuksellisuutta?

Fyysinen ja ympäristön turvallisuus

- Ovatko arkaluonteista tietoa kryptografialaitteiston ulkopuolella käsittelevät järjestelmän osat suojattu elektromagneettisen säteilyn aiheuttamalta tiedon paljastumiselta (esimerkiksi Faradayn häkillä)?

- Onko avainhenkilöriskit kartoitettu ja sijaisuusjärjestelyt olemassa?
- Onko henkilöstöllä kirjalliset ohjeet oman työpaikkansa tietoturvallisuuden huolehtimisesta?
- Onko henkilökunnan toiminta palotilanteissa harjoitettu, onko kriittisen materiaalin pelastussuunnitelma olemassa?
- Ovanko järjestelmän tilat omana palo-osastona ja varustettu automaattisin paloilmoituslaittein?
- Saadaanko järjestelmän tiloihin tunkeutumisesta ilmoitus murtohälytysjärjestelmällä?

Tietoliikenteen ja tietoverkkojen turvallisuus

- Jos varmentajan järjestelmä on kytketty verkkoon johon ei voida luottaa (esim. Internet), onko käytössä soveltuvat verkkotason turvaratkaisut (esim. palomuri)?
- Onko järjestelmä asetettu siten, että kaikkien verkon solmukoneiden kuten palomuurien tulee kieltää pääsy ellei sitä ole erikseen sallittu?

Ajan synkronointi

- Synkronisoidaanko varmentajan järjestelmän kaikki kellot vähintään sekunnin tarkkuudella UTC-aikaan?
- Onko ajan synkronointiin käytettävissä kaksi erillistä luotettavaa ajanlähdettä?

3. Sisäänkirjautuminen ja tunnistaminen

Käyttäjän sisäänkirjautuminen ja tunnistaminen

- Täytyykö jokaisen käyttäjän kirjautua sisään varmentajan järjestelmään voidakseen suorittaa toiminnon?
- Vaaditaanko uloskirjautumisen jälkeen aina uudelleenkirjautuminen järjestelmään?
- Onko tunnistamiseen käytettävä ns. haaste (Authentication challenge data) ainutlaatuinen ja kertakäyttöinen?

Käyttäjän sisäänkirjautumisen epäonnistuminen

- Onko epäonnistuneiden sisäänkirjautumisyritysten määrä rajoitettu?
- Jos sisäänkirjautuminen epäonnistuu useammin kuin on sallittua, suljetaanko käyttäjän pääsy järjestelmään?
- Jos sisään kirjautuminen epäonnistuu useammin kuin on sallittua, tehdäänkö tästä ilmoitus?

4. Avainten hallinta

Avainten luominen

- Luodaanko laatuvarmenteiden allekirjoitusavaimet hyväksytyssä ja turvallisessa kryptografiamoduulissa?
- Tapahtuuko laatuvarmenteiden luomiseen käytettävien allekirjoitusavainten generointi aina kahden ihmisen valvonnassa?
- Luodaanko järjestelmäavaimet hyväksytyssä ja turvallisessa kryptografiamoduulissa?
- Luodaanko hallinta-avaimet turvallisessa kryptografiamoduulissa?
- Täyttääkö avainten generointi EESSI:n algoritmiryhmän määrittelemät kryptografiset vaatimukset?

Avainten jakelu

- Jaetaanko yksityiset ja salaiset avaimet salatusti ja suojassa muutoksilta?
- Ovanko varmentamattomat julkiset avaimet suojattu sieppaukselta ja manipulaatiolta?
- Jakaako varmentaja kryptografiset avaimet määritellyn jakotavan mukaisesti?
- Onko laatuvarmenteiden allekirjoitusavaimiin liittyvä julkiset avaimet ja parametrit suojattu muutoksilta niiden jakelun yhteydessä?
- Onko itse allekirjoitetulla (self-signed) varmenteella aina seuraavat ominaisuudet?

- varmenne on tarkastettavissa sen sisältämällä tiedoilla
- varmenteen myöntäjä- ja haltijakentät ovat identtiset

Avainten käyttö

- Onko kaikkiin kryptografialaitteistoihin, jotka käyttävät hallinta-, järjestelmä- tai laatuvarmenteen allekirjoitusavaimia, rajoitettu pääsy sekä kulunvalvonta?
- Tarjoaako laatuvarmenteen luonti mahdollisuuden kahden ihmisen hallintaan käytettäessä hallinta-avaimia?
- Onko rekisteröinnissä, laatuvarmenteen luonnissa ja laatuvarmenteen sulkulistapyyntöjen hallinnalla erilliset järjestelmäavaimet?
- Ovatko laatuvarmenteeseen liittyvät allekirjoitusavaimet (varmenteen haltijan yksityinen avain) erillisiä muihin toimintoihin tarkoitetuista avaimista (esimerkiksi salausavaimet)?
- Tarkistetaanko hallinta- ja järjestelmäavaimiin liittyvien laatuvarmenteiden voimassaolo ennenkuin näihin avaimiin luotetaan?

Avainten vaihto

- Uusitaanko hallinta- ja järjestelmäavaimet säännöllisesti?
- Tapahtuuko avaimien uusiminen turvallisesti?

Avainten tuhoaminen

- Kun laatuvarmenteiden allekirjoitusavainten voimassaolo loppuu, tuhotaanko ne siten ettei niitä voi enää palauttaa?
- Kun salaisia avaimia käyttävä tai hallussaan pitävä järjestelmän osa otetaan pois käytöstä tai siirretään, tuhotaanko tämän avaimet?
- Tarjoaako järjestelmä mahdollisuuden nollata salaamattomat yksityiset ja salaiset avaimet jotka on talletettu ohjelmallisesti tai "rautaan"?
- Käytetäänkö ohjelmallisesti talletetun avaimien tuhoamiseen prosesseja jotka varmistavat tiedon todellisen häviämisen (kirjoitetaan yli useampaan kertaan tms.)?

Avainten säilytys, varmuuskopiointi sekä palautus

- Säilytetäänkö kaikki yksityiset ja salaiset avaimet turvallisesti?
- Säilytetäänkö yksityiset järjestelmä- ja laatuvarmenteiden allekirjoitusavaimet turvallisessa kryptografiamoduulissa?
- Säilytetäänkö salaiset hallinta-avaimet turvallisessa kryptografiamoduulissa?
- Jos jokin salainen avain otetaan ulos kryptografiamodulista, onko se suojattu ennen talletusta modulin ulkopuolelle?
- Takaako järjestelmä että vamenteiden allekirjoitusavaimien varmuuskopiointi, säilytys sekä palautus tapahtuu vain hyväksytyyn henkilön toimesta fyysisesti turvallisessa ympäristössä?
- Takaako järjestelmä että salaisten järjestelmä-, hallinta- ja varmenteiden allekirjoitusavainten varmuuskopiointi, säilytys sekä palautus tapahtuu kahden ihmisen valvonnassa?
- Taataanko ettei laatuvarmenteen haltijan yksityisiä avaimia varmuuskopioida eikä saateta kolmansien osapuolten tietoon?

Avainten arkistointi

- Onko laatuvarmenteen haltijan yksityisten avainten kopiointi ja arkistointi estetty?

5. Accounting and Auditing

Auditointitiedon kerääminen

- Tallennetaanko merkintä lokiin ainakin kaikista seuraavista tapahtumista?
 - järjestelmän ympäristöön, avainten ja varmenteiden hallintaan liittyvät tapahtumat
 - auditointitoiminnon käynnistys ja alasajo

- auditointiparametrien muutos
- auditointitiedon varaston vikatilaa aiheuttamat toimenpiteet

Takuu auditointitiedon saatavuudesta

- Ylläpitääkö järjestelmä auditointilokia?
- Onko auditointitiedoille varattu riittävästi tilaa?
- Onko auditointiloki toteutettu siten, että sitä ei automaattisesti ylikirjoiteta?

Auditointitiedon parametrit

- Sisältääkö auditointiloki seuraavat tiedot?
 - tapahtuman aika ja päivämäärä
 - tapahtuman tyyppi
 - tapahtuman käynnistäjän henkilöllisyys
 - tieto tapahtuman onnistumisesta tai epäonnistumisesta

Valinnainen auditointi

- Onko järjestelmässä mahdollisuus tapahtumien etsimiseen auditointilokista tapahtuman tyyppiin ja/tai sen käynnistäjän identiteetin perusteella?
- Onko auditointilokin tiedot esitetty käyttäjälle helposti luettavassa muodossa?

Rajattu auditointi

- Onko auditointitiedon luku kiellettyä kaikilta muilta kuin niiltä käyttäjiltä, joille lukuoikeus on erikseen myönnetty (esim. ne joilla on järjestelmän arvioijan rooli)?
- Onko auditointilokin tietojen muuttaminen jälkikäteen estetty?

Automaattinen hälytys

- Tehdäänkö kaikista potentiaalisista tietoturvan vaarantumisista hälytys (hälytys voi olla esimerkiksi sähköposti tietoturvavastaavalle)?

Takuu tiedon oikeellisuudesta

- Onko auditointitiedon eheys taattu (esim. järjestelmien luomalla digitaalisella allekirjoituksella)?

Takuu tapahtuma-ajasta

- Merkitäänkö tapahtuman ajaksi aika, joka saadaan luotettua aikalähdettä käyttäen (kts. Ajan synkronointi)?

6. Arkistointi

Arkistoinnin toteutus

- Onko järjestelmässä arkistointimahdollisuus?
- Arkistoidaanko ainakin seuraavat asiat?
 - Kaikki varmenteet
 - Kaikki sulkulistat
 - Kaikki auditointilokit
- Sisältävätkö kaikki arkistoon talletetut tietoalkiot tapahtuma-ajan?
- Onko kaikki arkistoon talletettu luottamuksellinen tieto suojattu?
- Säilytetäänkö arkiston tietoalkiot, jotka liittyvät varmenteisiin, arkistossa niin kauan kuin niitä voidaan käyttää todisteina oikeudessa?

Valinnainen haku

- Voidaanko arkistoituja tapahtumia hakea niiden tyyppin perusteella?

Arkistoidun tiedon eheys

- Ovatko kaikki arkistoon talletetut tietoalkiot suojattu muutoksilta?

7. Varmuuskopiointi ja palautus

Varmuuskopiointi

- Onko järjestelmässä varmuuskopiointimahdollisuus?
- Riittääkö varmuuskopioitu tieto järjestelmän tilan täydelliseen palauttamiseen tarvittaessa?
- Voiko käyttäjä, jonka roolin oikeudet riittävät siihen, käynnistää varmuuskopioinnin tarvittaessa?
- Säilytetäänkö varmuuskopiot vähintään kahden tunnin paloluokitellussa tietovälinekaapissa tai holvissa?

Varmuuskopioidun tiedon oikeellisuus ja luottamuksellisuus

- Ovatko varmuuskopiot suojattu muutoksilta (esim. digitaalisilla allekirjoituksilla)?
- Onko kaikki luottamuksellinen tai salassa pidettävä tieto suojattu asiattomilta?

Palautus

- Onko järjestelmässä palautusmahdollisuus, jonka avulla järjestelmän tila voidaan palauttaa varmuuskopiolta?
- Voiko käyttäjä, jonka roolin oikeudet riittävät siihen, käynnistää palautuksen tarvittaessa?

PERUSPALVELUT

1. Yleistä

- Täyttävätkö kaikki peruspalveluiden luomat viestit seuraavat ehdot?
 - Viestit ovat suojattuja käyttäen järjestelmäavaimia;
 - Viestit sisältävät ajan milloin lähettäjä loi viestin;
 - Viestit sisältävät toistohyökkäyksen (replay attack) eston.

2. Rekisteröinti

Laatuvarmenteen hakeminen

- Tarkistetaanko hakijan henkilöllisyys?
- Välitetäänkö varmennehakemus suojattuna (salattuna) rekisteröinnistä laatuvarmenteiden luontiin (jos se sisältää luottamuksellista tietoa hakijasta)?
- Kerätäänkö hakijasta laatuvarmenteen myöntämisessä tarvittavat tiedot?
- Varmistaako järjestelmä, että varmennehakemuksen lähettäjä on siihen liittyvän yksityisen avaimen haltija?
- Tarjoaako järjestelmä mahdollisuuden rekisteröijälle hyväksyä varmennehakemukset ennen kuin ne lähtevät ulos rekisteröintipalvelusta?
- Liitetäänkö varmennehakemukseen tieto hakemisajankohdasta sekä tiedot laatuvarmenteen julkaisemisesta julkisessa hakemistossa?
- Allekirjoitetaanko kaikki rekisteröintipalvelun lähettämät viestit järjestelmä- tai hallinta-avaimilla?

Laatuvarmenteen hakijan tietojen käsittely

- Käsitelläänkö laatuvarmenteen hakijan tietoja siten, että niiden luottamuksellisuus ja salassapito on turvattu?

Rekisteröintipalvelun valvonta ja tietojen tallentaminen

- Tallennetaanko merkintä lokiin kaikista seuraavista tapahtumista?
 - kaikki tapahtumat jotka liittyvät rekisteröintiin ja laatuvarmenteen uusimiseen
 - kaikki hyväksytyt varmennehakemukset

3. Varmenteen luominen

Laatuvarmenteen luominen

- Varmistetaanko laatuvarmenteen luomisessa varmennehakemuksen alkuperä, luottamuksellisuus ja eheys?
- Käsitelläänkö varmennehakemus turvallisesti ja tarkistetaanko sen sopivuus voimassa olevaan varmennepolitiikkaan?
- Onko ennen laatuvarmenteen luomista tarkastettu että laatuvarmenteen hakijalla on julkiseen avaimen liittyvä yksityinen avain hallussaan?
- Käytetäänkö laatuvarmenteiden allekirjoittamiseen käytettyä avainta ainoastaan laatuvarmenteiden (ja mahdollisesti sulkulistojen) allekirjoittamiseen?
- Luoko järjestelmä vain sellaisia laatuvarmenteita, jotka ovat tietoturvasuostavien asettamien sallittujen profiilien mukaisia?

Varmenteen uusiminen

- Onko laatuvarmenteen uusimisjärjestelmä suojattu ns. "laatuvarmenteen vaihto" -hyökkäyksiltä (certificate substitution attack)?
- Uusitaanko laatuvarmenteiden allekirjoitusavaimet ennen niiden vanhentumista?
- Tarjoaako järjestelmä turvallisen tavan uusida sekä varmentajan että varmenteiden haltijoiden varmenteet?

Ristiinvarmennus

- Vastaavatko osapuolien tietoturva- ja varmennepolitiikat sekä varmennuskäytännöt toisiaan?

Laatuvarmenteen luontipalvelun valvonta ja tietojen tallentaminen

- Tallennetaanko merkintä lokiin kaikista seuraavista tapahtumista?
 - laatuvarmenteiden allekirjoitusvarmenteiden, järjestelmävarmenteiden ja hallintavarmenteiden elinkaaren hallintaan liittyvät tapahtumat
 - laatuvarmenteiden allekirjoitusavainten elinkaaren hallintaan liittyvät tapahtumat
 - laatuvarmenteiden elinkaaren hallintaan liittyvät tapahtumat
 - ristiinvarmennuspyynnöt ja -vastaukset

4. Laatuvarmenteiden jakelupalvelu

Laatuvarmenteiden jakelun hallinta

- Onko laatuvarmenteen tietosisältö laatuvarmenteeseen perustuvaan sähköiseen allekirjoitukseen luottavien kolmansien osapuolten saatavilla?

5. Laatuvarmenteiden sulkupalvelu

Laatuvarmenteen tilan muutospyynnöt

- Tarkastetaanko peruutus-, keskeytys- ja keskeytyksen peruutuspyyntöjen alkuperä ja oikeellisuus?
- Onko peruutetun laatuvarmenteen uudelleen käyttöön ottaminen estetty?
- Onko laatuvarmenteiden allekirjoitusavainten ja järjestelmäavainten varmenteiden mitätöinti mahdollista vain kahden henkilön valvonnassa?
- Voidaanko laatuvarmenteiden tilaa muuttaa vain seuraavasti?
 - i. tietoturvallisuusvastaava voi muuttaa järjestelmä- ja hallintavarmenteiden tilaa
 - ii. rekisteröijä ja tietoturvallisuusvastaava voivat muuttaa myönnettyjen laatuvarmenteiden tilaa
 - iii. laatuvarmenteiden haltijat voivat pyytää omien varmenteidensa tilaa muutettavaksi
- Päivitetäänkö varmenteiden tila -tietokanta heti tilanmuutoshakemuksen käsittelyn jälkeen?

Laatuvarmenteen mitätöinti ja keskeytys

- Pystyvätkö varmentajan järjestelmät mitätöimään minkä tahansa varmentajan myöntämän laatuvarmenteen, huolimatta järjestelmän pettämisestä?

Peruutuspalvelun valvonta ja tietojen tallentaminen

- Tallennetaanko merkintä lokiin kaikista seuraavista tapahtumista?
 - Kaikki laatuvarmenteiden tilan muutospyynnöt ja pyyntöjen hyväksyntä;

6. Laatuvarmenteen sulkulistapalvelu

Sulkulistan tilatieto

- Saako sulkulistapalvelu tilatietoviestinsä vain luotetulta sulkulistapyyntöjen hallinnalta?
- Tarkastaako palvelu tilatietoviestien eheyden ja alkuperäisyyden?
- Varmistaako sulkulistapalvelu vastauksien kohdistuvan kysytyyn laatuvarmenteeseen?

Tilakysely ja -vastaus

- Allekirjoitetaanko kaikki on-line sulkulistapalveluiden laatuvarmenteiden tilakyselyiden vastaukset?
- Onko off-line sulkulistapalvelun tuottama sulkulista allekirjoitettu?
- Luottaako tilakyselyn tekijä vastauksen allekirjoitusavaimeen tai varmentajaan joka on myöntänyt tämän avaimen?
- Sisältääkö vastaus ajankohdan jolloin sulkulistapalvelu allekirjoitti sen?

Laatuvarmenteen sulkulistapalvelun valvonta ja tietojen tallentaminen

- Tallennetaanko on-line sulkulistapalvelun (esim. OCSP) lokiin merkintä laatuvarmenteiden tilan muutospyynnöistä ja pyyntöjen hyväksymisestä