

**MÄÄRÄYKSEN 7 PERUSTELUT JA  
SOVELTAMINEN**

**TUNNISTUSPALVELUN TARJOAJIEN JA  
YLEISÖLLE LAATUVARMENTEITA  
TARJOAVIEN VARMENTAJIEN  
ILMOITUSVELVOLLISUUDESTA  
VIESTINTÄVIRASTOLLE**

**SISÄLLYS**

<b>SISÄLLYS</b> .....	<b>1</b>
<b>1 LAINSÄÄDÄNTÖ</b> .....	<b>2</b>
1.1 MÄÄRÄYKSEN LAINSÄÄDÄNTÖPERUSTA.....	2
1.2 EY-LAINSÄÄDÄNTÖ .....	2
1.3 MUUT ASIAAN LIITTYVÄT SÄÄNNÖKSET.....	2
<b>2 MÄÄRÄYKSEN TARKOITUS JA MUUTOSHISTORIA</b> .....	<b>2</b>
2.1 MÄÄRÄYKSEN TARKOITUS .....	2
2.2 KESKEISET MUUTOKSET JA MUUTOSHISTORIA.....	3
2.3 MÄÄRITELMÄT .....	3
<b>3 PYKÄLÄKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET</b> .....	<b>3</b>
3.1 1 § SOVELTAMISALA .....	3
3.2 2 § TUNNISTUSPALVELUN TARJOAJAN TOIMINNAN ALOITTAMISILMOITUS .....	4
<b>3.2.1 Tunnistuspalvelun tarjoajan toiminnan luotettavuuden arviointi</b> .....	<b>4</b>
<b>3.2.2 Tunnistusmenetelmän tietoturvallisuuden arviointi</b> .....	<b>5</b>
3.3 3 § LAATUVARMENTEITA YLEISÖLLE TARJOAVAN VARMENTAJAN TOIMINNAN ALOITTAMISILMOITUS .....	6
<b>3.3.1 Varmentajan toiminnan luotettavuuden arviointi</b> .....	<b>6</b>
<b>3.3.2 Varmennepalvelun tietoturvallisuuden arviointi</b> .....	<b>7</b>
3.4 4 § TOIMINNAN MUUTOSILMOITUS .....	8
3.5 5 § VUOSIRAPORTTI.....	9
3.6 6 § TOIMINNAN LOPETTAMIS-/SIIRTYMISILMOITUS.....	9
3.7 7 § MUUT ILMOITUKSET .....	10
<b>4 VIITTELUETTELO</b> .....	<b>10</b>

## **1 LAINSÄÄDÄNTÖ**

Tämän luvun tarkoituksena on antaa määräyksen käyttäjälle kokonaiskuva siitä, mihin säädöksiin määräys perustuu. Lisäksi luvussa listataan aihepiiriin liittyvä muu oleellinen säädäntö.

### **1.1 Määräyksen lainsäädäntöperusta**

Määräys 7 B /2009 M perustuu vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain (617/2009), jäljempänä tunnistuslain [1], 10 §:n 4 momenttiin, 32 §:n 1 momenttiin ja 42 §:n 2 momenttiin. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista tuli voimaan 1.9.2009 ja sillä pantiin osaltaan täytäntöön Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY [2].

Tunnistuslain 10 §:n mukaan Suomeen sijoittautuneen tunnistuspalvelun tarjoajan on tehtävä ilmoitus Viestintävirastolle ennen toimintansa aloittamista. Yleisölle laatuvarmenteita tarjoavan varmentajan ilmoitusvelvollisuudesta säädetään lain 32 §:ssä. Tunnistuspalvelun tarjoajan velvollisuudesta ilmoittaa tietoturvaan kohdistuvista uhkista ja häiriöistä säädetään lain 16 §:ssä. Lain 42 §:ssä säädetään Viestintäviraston valtuudesta antaa teknisiä määräyksiä palveluntarjoajien toiminnan luotettavuus- ja tietoturva-vaatimuksista.

Tunnistuslain 43 §:n mukaan Viestintävirastolla on tiedonsaantioikeus tunnistuspalvelun ja laatuvarmenteiden tarjoajilta. Viestintäviraston tehtävänä on lain 42 §:n mukaan valvoa lain ja sen nojalla annettujen säännösten noudattamista. Teknisten määräysten antamiseen liittyvät säännökset ovat lain 8 §:n 3 mom, 10 §:n 4 mom, 32 §:n 1 mom ja 42 §:n 2 mom.

Tunnistuslain 51 §:n 1 momentin siirtymäsäännöksen mukaan tunnistuspalvelun tarjoajien on tehtävä Viestintävirastolle 10 §:ssä tarkoitettu ilmoitus kuuden kuukauden kuluessa lain voimaantulosta. Pykälän 4 momentin mukaan sellaisen laatuvarmenteita tarjoavan varmentajan, joka on tehnyt sähköisistä allekirjoituksista annetun lain 9 §:n 1 momentin mukaisen ilmoituksen ja jatkanut toimintaansa keskeytyksettä tunnistuslain voimaan tulon saakka, ei tarvitse tehdä uutta ilmoitusta 32 §:n 1 momentin mukaisesti.

### **1.2 EY-lainsäädäntö**

Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY [2].

Mainittu direktiivi saatettiin Suomessa aikanaan voimaan lailla 14/2003 laki sähköisistä allekirjoituksista. Tunnistuslailla korvattiin laki sähköisistä allekirjoituksista. Lakiin siirrettiin myös laatuvarmenteita koskeva sääntely.

EY:n tasolla ei ole määräyksen 7 B/2009 voimaan tullessa olemassa tunnistamispalveluihin liittyvää säädäntöä.

### **1.3 Muut asiaan liittyvät säännökset**

Viestintäviraston antama määräys (Viestintävirasto 8) tunnistamispalvelujen tarjoajien ja yleisölle laatuvarmenteita tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvasääntelyistä.

## **2 MÄÄRÄYKSEN TARKOITUS JA MUUTOSHISTORIA**

Tämän luvun tarkoituksena on antaa määräyksen käyttäjälle tieto määräyksen tavoitteista ja tarkoituksesta. Luvussa käsitellään myös merkittävimmät muutokset määräystä edeltäneisiin velvoitteisiin ja suosituksiin.

### **2.1 Määräyksen tarkoitus**

Viestintävirasto on tunnistuslain 10 §:n 4 momentin ja 32 §:n 1 momentin nojalla antanut määräyksen Viestintävirasto 7 B/2009 M tunnistuspalvelun tarjoajien ja yleisölle laatuvarmenteita tarjoavien varmentajien ilmoitusvelvollisuudesta Viestintävirastolle. Määräyksen 2 - 7 §:issä käsitellään

tarkemmin tunnistuspalvelun tarjoajan ja yleisölle laatuvarmenteita tarjoavien varmentajien Viestintävirastolle tekemien ilmoitusten sisältövaatimuksia.

## **2.2 Keskeiset muutokset ja muutoshistoria**

Määräykseen 7 A tehtiin seuraavat muutokset:

Määräykseen lisättiin uudet tunnistuspalvelun tarjoajan ilmoitusvelvollisuutta koskevat säännökset.

Laatuvarmentajan raportointivelvollisuutta kevennettiin hieman osavuosikatsausten ja vuosiraportin osalta sekä tehtiin joitakin vähäisempiä muutoksia tiedonantovelvollisuuksia koskeviin muihin säännöksiin.

Määräykseen lisättiin myös velvollisuus ilmoittaa Viestintävirastolle, mikäli laatuvarmentaja takaa ETA:n ulkopuolisen varmentajan varmenteet laatuvarmenteiksi.

Määräyksen voimassaoloaika muutettiin toistaiseksi voimassa olevaksi.

## **2.3 Määritelmät**

Määräyksessä ja sen soveltamisohjeessa käytetyt termit vastaavat tunnistuslain määritelmiä. Palveluntarjoajalla määräyksessä ja sen perusteluissa tarkoitetaan sekä tunnistuspalvelun tarjoajaa että yleisölle laatuvarmenteita tarjoavaa varmentajaa.

## **3 PYKÄLÄKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET**

Tässä luvussa käydään läpi pykäläkohtaisesti pykälän perustelut sekä sen soveltamissuosituksukset.

### **3.1 1 § Soveltamisala**

Viestintäviraston määräystä sovelletaan tunnistuspalvelun tarjoajiin sekä varmentajiin, jotka tarjoavat sähköisiin allekirjoituksiin liittyviä laatuvarmenteita yleisölle.

Tunnistuspalvelun tarjoajalla tarkoitetaan palveluntarjoajaa, joka tarjoaa vahvan sähköisen tunnistamisen palveluita niitä käyttäville palveluntarjoajille tai laskee liikkeelle tunnistusvälineitä yleisölle tai molempia. Tunnistuspalvelun tarjoaja voi näin ollen tarjota tunnistusvälineen liikkeelle laskua, muuta tunnistuspalvelua tai molempia.

Tunnistuslakia ja siten myöskään määräystä ei sovelleta yhteisön sisäiseen tunnistamiseen tai jos yhteisö käyttää omaa tunnistusmenetelmäänsä omien asiakkaidensa tunnistamiseen omissa palveluissaan. Näin ollen esimerkiksi tunnistamismenetelmät kuuluvat määräyksen soveltamisalaan vain siltä osin, kuin tunnistuspalvelun tarjoaja tarjoaa tunnistusmenetelmää tunnistuspalvelun kautta muille palveluntarjoajille käytettäväksi näiden muiden palveluntarjoajien asiakkaiden tunnistamiseen.

Varmentajan katsotaan tarjoavan varmenteita yleisölle, mikäli se tarjoaa varmenteita käyttäjäryhmälle, jota ei ole ennalta rajattu. Määräykset eivät koske suljetulle käyttäjäryhmälle, kuten yrityskonsernin sisäiseen käyttöön tarkoitettujen varmenteiden tarjoamista. Määräystä ei sovelleta myöskään vapaaehtoisin siviilioikeudellisiin sopimuksiin, joilla on sovittu sähköisen allekirjoituksen käytöstä tietyn, rajatun osanottajajoukon kesken. Avoimena käyttäjäryhmänä voidaan pitää ainakin tilannetta, jossa varmenteeseen luottava osapuoli ei ole sopimussuhteessa varmentajaan eikä allekirjoittajaan.

Määräystä ei sovelleta myöskään tunnistusvälineiden tai sähköisen allekirjoittamisen välineiden valmistamiseen, maahantuontiin tai myyntiin. Tunnistamisvälineiden liikkeelle lasku voidaan erottaa niiden valmistamisesta, maahantuonnista ja myynnistä siten, että liikkeelle laskijan ja välineen haltijan välillä vallitsee pääsääntöisesti sopimussuhde. Sähköisen allekirjoittamisen osalta esimerkiksi varmentajan ylläpitämä sulkulista tekee toiminnasta palvelua erotuksena puhtaasta välineen valmistamisesta, maahantuonnista tai myynnistä.

### **3.2 2 § Tunnistuspalvelun tarjoajan toiminnan aloittamisilmoitus**

Suomeen sijoittautuneen tunnistuspalvelun tarjoajan on toimitettava Viestintävirastolle ennen toiminnan aloittamista<sup>1</sup> tiedot, joiden perusteella virasto pystyy arvioimaan tunnistuspalvelun tarjoajan ja tarjottavan palvelun lainmukaisuutta. Ilmoitus on tehtävä kirjallisesti. Kirjallisen muotovaatimuksen täyttää myös sähköisesti toimitettu ilmoitus siten kuin sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003) [3] erikseen säädetään.

Ilmoitusvelvollisuus on asetettu Suomeen sijoittautuneelle tunnistuspalvelun tarjoajalle. Lain mukaan ilmoituksen voi tehdä myös sellainen palveluntarjoajien yhteenliittymä, jonka hallinnoimaa palvelua on pidettävä yhtenä tunnistuspalveluna.

Viestintävirasto selvittää tunnistuspalvelun tarjoajalle ja tämän tarjoamalle palvelulle laissa säädettyjen edellytysten täyttymisen ennen kuin se merkitään tunnustuslain 12 §:n mukaiseen Viestintäviraston ylläpitämään rekisteriin. Tunnistuspalvelun tarjoaja voi kuitenkin aloittaa toimintansa heti ilmoituksen tehtyään jo ennen rekisteriin tehtävää merkintää.

Mikäli ilmoitus on puutteellinen, Viestintäviraston on kehoitettava ilmoituksen tekijää täydentämään ilmoitustaan. Jos palvelu tai palveluntarjoaja ei täytä laissa asetettuja vaatimuksia, Viestintäviraston on ilmoituksen saatuaan kiellettävä palveluntarjoajaa tarjoamasta palveluaan vahvana sähköisenä tunnistamisena. Jos puutteellisuutta voidaan pitää ainoastaan vähäisenä, Viestintävirasto voi kehottaa palveluntarjoajaa korjaamaan puutteellisuuden määräajassa.

#### **3.2.1 Tunnistuspalvelun tarjoajan toiminnan luotettavuuden arviointi**

Tunnistuspalvelun tarjoajan toiminnan luotettavuuden arvioimiseksi tunnistuspalvelun tarjoajan on ilmoitettava Viestintävirastolle seuraavat tiedot:

##### **Tiedot tunnistuspalvelun tarjoajasta**

Tunnistuspalvelun tarjoajan on ilmoitettava Viestintävirastolle yhteystietoina soveltuvin osin seuraavat tiedot:

- yrityksen/tunnistuspalvelun tarjoajan nimi
- Y-tunnus
- kaupparekisteriote
- postiosoite
- käyntiosoite
- puhelinnumero
- fax-numero
- yhdyshenkilö
- sähköpostiosoite
- linkki www-sivuille

Lisäksi tunnistuspalvelun tarjoajan on ilmoitettava Viestintävirastolle yhteystiedot tunnustuslain 25 § 1 momentin mukaiseen palveluun, minne tunnistusvälineen haltija voi tehdä tunnistusvälineen peruuttamista tai käytön estämistä koskevan ilmoituksen.

##### **Tiedot tunnistusperiaatteista**

Tunnistusperiaatteissa määritellään, kuinka tunnistamispalvelun tarjoaja täyttää tunnustuslaissa säädetyt velvollisuudet. Tunnistusperiaatteet sisältävät:

- tiedot ensitunnistamisen toteuttamisesta
- palvelukuvaukset tarjottavista palveluista
- tiedot palveluntarjoajan tärkeimmistä yhteistyökumppaneista ja

---

<sup>1</sup> Tunnustuslain 50 §:n 1 momentin siirtymäsäännöksen mukaan tunnistuspalvelun tarjoajien on tehtävä Viestintävirastolle ilmoitus toiminnan aloittamisesta kuuden kuukauden kuluessa lain voimaantulosta.

- tiedot ulkopuolisten arviointilaitosten suorittamista tarkastuksista.

Palvelukuvauksesta on käytävä ilmi, tarjoaako tunnistuspalvelun tarjoaja yksinomaan tunnistusvälineen liikkeelle laskua, muuta tunnistuspalvelua vai molempia. Palvelukuvaukseen tulee sisältyä myös tieto siitä, voidaanko tunnistuspalvelun tarjoajan tunnistusvälineillä tehdä sähköisiä allekirjoituksia ja millaisia nämä allekirjoitukset ovat.

Tunnistusperiaatteista tulee käydä ilmi myös se, miten tunnistuspalvelun tarjoajan on järjestänyt tunnistusvälineen haltijoille tunnituslain 25 §:n mukaisen mahdollisuuden ilmoittaa tunnistusvälineen katoamisesta, oikeudettomasta käytöstä tai joutumisesta oikeudettomasti toisen haltuun.

### **Tiedot henkilöstöstä**

Tunnistuspalvelun tarjoajan on toimitettava Viestintävirastolle myös olennaiset tiedot henkilöstöstään, tunnistamispalveluiden tarjoamisessa apunaan käyttämistään henkilöistä sekä muut tiedot, joiden perusteella tunnistuspalvelun tarjoajan asiantuntemusta, kokemusta ja pätevyyttä voidaan arvioida. Tunnistamispalvelun tarjoajan on toimitettava Viestintävirastolle myös vakuutus siitä, että sen organisaation vastuulliset henkilöt ovat luotettavia ja täyttävät tunnistuspalvelun tarjoajalle tunnituslain 9 §:ssä asetetut vaatimukset.

### **Tiedot tietoturvallisuuden periaatteista**

Viestintävirastolle toimitettavia tietoja tunnistuspalvelun tietoturvallisuuden ja palveluntarjoajan toiminnan luotettavuuden arvioimiseksi ovat esimerkiksi kirjallisesti määritelty ja johdon hyväksymä näkemys tunnistuspalvelun tarjoajan tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta. Lisäksi tunnistuspalvelun tarjoajan tulee toimittaa tiedot noudattamistaan standardeista sekä mahdollisista pätevyydentoteamislaitosten tekemistä arvioinneista, mikäli nämä tiedot eivät sisälly tunnistusperiaatteisiin. Näiden tietojen perusteella voidaan arvioida, onko toiminnan tietoturvallisuuteen kiinnitetty riittävästi huomiota ja onko sitä koskevat vastuut määritelty riittävällä tasolla.

### **Tiedot tietojen tallentamisesta**

Lisäksi ilmoitukseen on liitettävä mukaan kuvaus menettelytavoista tunnistustapahtumaa ja tunnistusvälinettä koskevien tietojen tallentamisessa. Kuvauksesta on käytävä ilmi muun muassa kuinka eri tallennusmuodoissa olevien tietojen käsittely ja saatavuuden varmistaminen on huomioitu näiden tietojen kaikissa elin vaiheissa. Tietoaineistoturvallisuudesta säädetään tarkemmin määräyksessä Viestintävirasto 8.

### **Muut palveluntarjoajan toiminnan luotettavuuden kannalta olennaiset tiedot**

Tunnistuspalvelun tarjoajalla on oltava harjoitettuun toimintaan nähden riittävät taloudelliset voimavarat toiminnan järjestämiseksi ja mahdollisen vahingonkorvausvastuun kattamiseksi. Toimitettavista tiedoista tulee kokonaisuutena tarkastellen pystyä muodostamaan oikea ja riittävä kuva tunnistamispalvelun tarjoajan taloudellisista voimavaroista sekä toimintaan liittyvistä taloudellisista riskeistä ja riskienhallintaperiaatteista.

Tunnistuspalvelun tarjoajan taloudellisten voimavarojen riittävyttä voidaan arvioida esimerkiksi yritystä koskeva edellisen vuoden vuosikertomuksen ja tilinpäätöstietojen sekä budjetti- ja toimintasuunnitelmien perusteella. Aloittavan yrityksen osalta taloudellisten voimavarojen riittävyttä voidaan arvioida esimerkiksi ensimmäiselle tilikaudelle laaditun tulos- ja tasebudjetin ja toimintasuunnitelman sekä kahden seuraavan tilikauden budjettisuunnitelmien perusteella.

Yleisistä tietoturvallisuusvaatimuksista säädetään tarkemmin määräyksessä Viestintävirasto 8.

### **3.2.2 Tunnistusmenetelmän tietoturvallisuuden arviointi**

Tunnistusmenetelmän tietoturvallisuuden arvioimiseksi tunnistuspalvelun tarjoajan on ilmoitettava Viestintävirastolle seuraavat tiedot.

### **Tiedot tunnistusvälineestä**

Tunnistuspalvelun tarjoajan on toimitettava Viestintävirastolle kuvaus tunnistusvälineessä käytävistä avainpituuksista ja algoritmeista sekä muista tunnistusvälineen luotettavuuteen vaikuttavista seikoista.

### **Tiedot järjestelmistä**

Tunnistuspalvelun tarjoajan on toimitettava Viestintävirastolle tiedot/kuvaus tunnistuspalvelun kannalta olennaisista järjestelmistä ja tuotteista, mukaan lukien sulkulistapalvelu. Selvityksen tulee sisältää tiedot käytetyistä laitteista ja ohjelmistoista (ml. käytetyt avainpituudet, algoritmit ja käyttötarkoitukset) sekä tiedot noudatetuista standardeista ja mahdollisista pätevydentoteamislaitosten tekemistä arvioinneista. Näiden tietojen perusteella voidaan arvioida onko tunnistuspalvelun tarjoajan laitteiden tietoturvasta ja käytettävyydestä huolehdittu laissa määritellyllä tavalla.

### **Varmenteen tietosisällön rakenne**

Jos tunnistusmenetelmä perustuu varmenteeseen, tunnistuspalvelun tarjoajan tulee toimittaa Viestintävirastolle myös tieto varmenteen tietosisällön rakenteesta. Varmenteen tietosisällön rakenteen tulee vastata laissa asetettuja vaatimuksia.

### **3.3 3 § Laatuvarmenteita yleisölle tarjoavan varmentajan toiminnan aloittamisilmoitus**

Laatuvarmenteita yleisölle tarjoavan varmentajan on toimitettava ennen toiminnan aloittamista<sup>2</sup> Viestintävirastolle tiedot, joiden perusteella Viestintävirasto arvioi varmentajan kykyä toimia laatuvarmenteiden tarjoajana sekä tarjottavan varmennuspalvelun lainmukaisuutta. Viestintävirasto selvittää varmentajalle ja varmennuspalvelulle laissa säädettyjen edellytysten täyttymisen ennen kuin varmentaja merkitään tunnistuslain 32 §:n 4 momentin mukaiseen Viestintäviraston ylläpitämään rekisteriin. Varmentaja voi kuitenkin aloittaa toimintansa heti ilmoituksen tehtyään jo ennen rekisteriin tehtävää merkintää.

Viestintäviraston on viipymättä kiellettävä varmentajaa tarjoamasta varmenteitaan laatuvarmenteina, mikäli varmente tai varmentaja eivät täytä lain vaatimuksia. Kieltopäätös voidaan tehdä esimerkiksi silloin, kun Viestintävirasto ei toimitettujen tietojen puutteellisuuden johdosta voi arvioida varmentajan toiminnan tai sen myöntämien varmenteiden vaatimustenmukaisuutta. Varmentajalla on ennen kieltopäätöstä kuitenkin oikeus täydentää ja/tai korjata toimittamiaan tietoja Viestintäviraston pyynnön mukaisesti.

#### **3.3.1 Varmentajan toiminnan luotettavuuden arviointi**

Yleisölle laatuvarmenteita tarjoavan varmentajan toiminnan luotettavuuden arvioimiseksi varmentajan on ilmoitettava Viestintävirastolle seuraavat tiedot:

#### **Tiedot varmentajasta**

Varmentajan yhteystietoina on ilmoitettava soveltuvin osin seuraavat tiedot:

- yrityksen/varmentajan nimi
- Y-tunnus
- kaupparekisteriote
- postiosoite
- käyntiosoite
- puhelinnumero
- fax-numero
- yhdyshenkilö
- sähköpostiosoite
- linkki www-sivuille

---

<sup>2</sup> Tunnistuslain 51 §:n 4 momentin siirtymäsäännöksen mukaan sellaisen varmentajan, joka on tehnyt sähköisistä allekirjoituksista annetun lain 9 §:n 1 momentin mukaisen ilmoituksen ja jatkanut toimintaansa keskeytyksettä tunnistuslain voimaan tulon saakka, ei tarvitse tehdä uutta ilmoitusta.

Lisäksi varmentajan on ilmoitettava Viestintävirastolle yhteystiedot tunnustuslain 36 §:n mukaiseen palveluun, mistä allekirjoittaja voi pyytää laatuvarmenteen peruuttamista.

### **Tiedot tarjottavista palveluista**

Ilmoituksen tulee sisältää tiedot tarjottavista sähköisiin allekirjoituksiin ja laatuvarmenteisiin liittyvistä palveluista. Varmentajan on ilmoitettava Viestintävirastolle menettelytavoista, joiden mukaisesti se toimii sekä tiedot näiden menettelytapojen toteuttamisesta ja tiedot tarjottavista laatuvarmenteisiin liittyvistä palveluista.

Ilmoitettavia tietoja ovat ainakin laatuvarmenteen hakijalle rekisteröimisen yhteydessä annettavat tiedot, tiedot varmentajan asettamista laatuvarmenteiden käytön ehdoista ja edellytyksistä, varmennepolitiikka ja varmennekäytäntö. Varmennepolitiikan ja varmennuskäytännön avulla voidaan arvioida, toteutuvatko laissa laatuvarmenteita tarjoavalle varmentajalle asetetut menettelyvaatimukset varmentajan toiminnassa.

### **Tiedot henkilöstöstä**

Varmentajan on annettava selvitys käyttämästään henkilöstöstä sekä sen pätevyys- ja tehtäväkuvaukset. Tehtäväkuvaukset voidaan osoittaa esimerkiksi organisaatiokuvauksella ja yleisillä pätevyysvaatimuksilla eri tehtäväluokille (esimerkiksi järjestelmän ylläpitäjä, varmenteen myöntäjä). Varmentajan on myös toimitettava tiedot varmentamiseen liittyvien toimiensa jakamisesta esimerkiksi alihankkijoiden kesken sekä edellä mainitut tiedot henkilöstöstä, jota alihankkija käyttää varmentajan tehtäviä suoritettaessa. Varmentajan ulkoistamia toimintoja voivat olla esim.

- rekisteröinti
- laatuvarmenteiden luonti
- laatuvarmenteiden jakelu
- sulkulistapyyntöjen hallinta
- sulkulistapalvelu.

### **Tiedot tietoturvallisuuden periaatteista**

Tietoturvallisuuspolitiikan ja -periaatteiden avulla voidaan arvioida, onko tietoturvallisuuteen kiinnitetty riittävästi huomiota ja onko sitä koskevat vastuut määritelty riittävällä tasolla.

### **Muut olennaiset tiedot**

Varmentajalla on oltava harjoitettuun toimintaan nähden riittävät taloudelliset voimavarat toiminnan järjestämiseksi ja mahdollisen vahingonkorvausvastuun kattamiseksi. Toimitettavista tiedoista tulee kokonaisuutena tarkastellen pystyä muodostamaan oikea ja riittävä kuva varmentajan taloudellisista voimavaroista sekä toimintaan liittyvistä taloudellisista riskeistä ja riskienhallintaperiaatteista.

Varmentajan taloudellisten voimavarojen riittävyttä voidaan arvioida esimerkiksi yritystä koskevan edellisen vuoden vuosikertomuksen ja tilinpäätöstiетоjen sekä budjetti- ja toimintasuunnitelmien perusteella. Aloittavan yrityksen osalta taloudellisten voimavarojen riittävyttä voidaan arvioida esimerkiksi ensimmäiselle tilikaudelle laaditun tulos- ja tasebudjetin ja toimintasuunnitelman sekä kahden seuraavan tilikauden budjettisuunnitelmien perusteella.

### **3.3.2 Varmennepalvelun tietoturvallisuuden arviointi**

Varmennepalvelun tietoturvallisuuden arvioimiseksi laatuvarmenteita yleisölle tarjoavan varmentajan on ilmoitettava Viestintävirastolle seuraavat tiedot:

#### **Tiedot järjestelmistä**

Varmentajan on toimitettava Viestintävirastolle tiedot/kuvaus laatuvarmenteiden tarjoamisen kanalta olennaisista järjestelmistä ja tuotteista. Selvityksen tulee sisältää tiedot käytetyistä laitteista

ja ohjelmistoista (ml. käytetyt avainpituudet ja algoritmit) sekä tiedot noudatetuista standardeista ja mahdollisista pätevydentoteamislaitosten tekemistä arvioinneista. Näiden tietojen perusteella voidaan arvioida, ovatko varmentajan käyttämät järjestelmät laissa määritellyllä tavalla luotettavia.

Sähköisiin allekirjoituksiin ja laatuvarmenteisiin sekä varmentajan toimintaan liittyviä standardeja ja teknisiä spesifikaatioita on valmisteltu esimerkiksi CEN/ISSS:n, ETSI:n ja IETF:n toimesta. Nämä dokumentit kattavat esimerkiksi laatuvarmenteiden tietosisällön, varmennepolitiikan laatuvarmenteita tarjoaville varmentajille, turvallisen allekirjoituksen luomisvälineen ja varmentajan luotettavat järjestelmät.

### **3.4 4 § Toiminnan muutosilmoitus**

Tunnistuspalvelun tarjoajan ja yleisölle laatuvarmenteita tarjoavan varmentajan on oma-aloitteisesti ilmoitettava toiminnassaan ja 2-3 §:ien nojalla annetuissa tiedoissa tapahtuvista merkittävistä muutoksista Viestintävirastolle.

#### **Viestintäviraston ylläpitämä julkinen rekisteri**

Tunnistuspalvelun tarjoajan ja laatuvarmenteita yleisölle tarjoavan varmentajan on aina ilmoitettava muutoksista Viestintäviraston ylläpitämän julkisen rekisterin tietoihin. Näistä muutoksista on ilmoitettava kuukautta ennen muutoksen voimaantuloa.

Viestintävirasto ylläpitää tunnistuspalvelun tarjoajista julkisessa rekisterissä ainakin seuraavia tietoja:

- tunnistuspalvelun tarjoajan nimi
- tunnistuspalvelun tarjoajan yhteystiedot (nimi, postiosoite, www-osoite, puhelinnumero)
- tarjottavat palvelut
- tunnistuspalvelun tarjoajan toiminnan lopettaminen
- yhteystiedot palveluun, minne tunnistusvälineen haltija voi tehdä tunnistusvälineen peruuttamista tai käytön estämistä koskevan ilmoituksen

Viestintävirasto ylläpitää yleisölle laatuvarmenteita tarjoavista varmentajista julkisessa rekisterissä ainakin seuraavia tietoja:

- laatuvarmenteiden nimi
- varmentajan yhteystiedot (nimi, postiosoite, www-osoite, puhelinnumero)
- laatuvarmenteiden myöntämisessä käytetty varmennepolitiikka (OID numero)
- varmentajan toiminnan lopettaminen
- yhteystiedot palveluun, mistä allekirjoittaja voi pyytää laatuvarmenteen peruuttamista

#### **Palvelun tietoturvallisuuden liittyvät muutokset**

Tunnistuspalvelun tarjoajan ja yleisölle laatuvarmenteita tarjoavan varmentajan on ilmoitettava Viestintävirastolle tunnistus- tai varmennustoimintaa koskevista tietoturvallisuuden ja luotettavuuden liittyvistä muutoksista.

Muutoksia, joista palveluntarjoajan tulee tehdä Viestintävirastolle ilmoitus, ovat muun muassa:

- muutokset sulkulistapalveluihin ja varmenteiden luontiin käytettäviin järjestelmiin:
  - merkittävät laitteistopäivitykset,
  - ohjelmistojen versiopäivitykset ja
  - ohjelmistojen vaihtaminen toiseksi.

#### **Muutokset palveluntarjoajan luotettavuudessa**

Tunnistuspalvelun tarjoajan ja yleisölle laatuvarmenteita tarjoavan varmentajan on toimitettava Viestintävirastolle selvitykset palveluntarjoajan henkilöstöön, sen apuna käyttämiin henkilöihin ja

yleiseen luotettavuuteen kohdistuvista merkittävistä muutoksista. Tällaisina voidaan pitää esimerkiksi:

- toimintojen ulkoistamista
- ulkoistettujen toimintojen siirtämistä toiselle toimijalle
- avainhenkilöiden osalta tapahtuvia henkilöstömuutoksia
- toimintojen siirtämistä toisiin toimitiloihin

Lisäksi tunnistuspalvelun tarjoajan ja yleisölle laatuvarmenteita tarjoavan varmentajan on toimitettava Viestintävirastolle kaikki selvitykset, joista käy ilmi palveluntarjoajan taloudellisen aseman olennainen heikentyminen tai taloudellisten riskien merkittävä kasvu. Nämä selvitykset on toimitettava Viestintävirastolle välittömästi niiden valmistuttua. Taloudellisen aseman olennaista heikentymistä tai taloudellisten riskien merkittävää kasvua osoittavana seikkana voidaan pitää esimerkiksi:

- palveluntarjoajan asettamista selvitystilaan
- suuria luottotappioita
- emoyrityksen konkurssia
- palveluntarjoajan velkajärjestelyä, velkasaneerausta, selvitystilaa tai konkurssia
- vastuun kattamisjärjestelmän (esimerkiksi vakuutus) kustannusten merkittävää nousua.

### **3.5 5 § Vuosiraportti**

Tunnistuspalvelun tarjoajan ja laatuvarmenteita yleisölle tarjoavan varmentajan on toimitettava Viestintävirastolle vuosittain raportti palveluntarjoajan lain soveltamisalaan kuuluvan toiminnan laajuudesta edellisenä vuonna. Vuosiraportti on toimitettava kahden kuukauden kuluessa kalenterivuoden päättymisestä.

Tunnistuspalvelun tarjoajan on toimitettava Viestintävirastolle tieto myönnettyjen tunnistusvälineiden ja tunnistustapahtumien lukumäärästä. Yleisölle laatuvarmenteita tarjoavan varmentajan on toimitettava Viestintävirastolle tieto vuoden aikana myönnettyjen ja peruutettujen sekä vuoden lopussa voimassa olleiden laatuvarmenteiden lukumäärästä. Mikäli mahdollista, vuosiraportin tulisi sisältää myös tunnistus- tai varmennetoimintaa koskeva vuosikertomus ja vahvistettu tilinpäätös.

Lisäksi palveluntarjoajien on toimitettava Viestintävirastolle tilastointi havaituista ongelmatilanteista ja muut toiminnan kannalta merkittävät tiedot, joita ovat esimerkiksi asiakasvalitusten määrä (mahdollisesti erikseen laskutusvalitukset ja palvelun vikaa tai häiriötä koskevat valitukset).

### **3.6 6 § Toiminnan lopettamis-/siirtymisilmoitus**

Tunnistuspalvelun tarjoajan ja yleisölle laatuvarmenteita tarjoavan varmentajan valvonnan kannalta Viestintäviraston on tärkeää saada mahdollisimman varhaisessa vaiheessa tieto palveluntarjoajan toiminnan loppumisesta tai toiminnan mahdollisesta siirtymisestä toiselle palveluntarjoajalle. Lopettamisen ennakoimismahdollisuuteen tähdätään ensisijaisesti toiminnan muutoksia koskevalla ilmoittamisvelvollisuudella. Muutosilmoitusten lisäksi on palveluntarjoajan kuitenkin erikseen ilmoitettava Viestintävirastolle tunnistuspalvelujen tai laatuvarmenteiden tarjoamistoiminnan loppumisesta tai toiminnan siirtymisestä toiselle palveluntarjoajalle esimerkiksi liiketoiminnan luovutuksen yhteydessä.

Tunnistuspalvelun tarjoajan ilmoituksen tulee sisältää tieto siitä, miten palveluntarjoaja on tiedottanut tai aikoo tiedottaa lopettamisesta tai toiminnan siirtymisestä tunnistusvälineiden haltijoille, tunnistuspalvelua käyttäville palveluntarjoajille sekä muille tunnistuspalvelun tarjoajan toimintaan liittyville yhteistyötahoille.

Varmentajan lopettamisilmoituksessa on oltava tieto siitä, miten varmentaja on tiedottanut tai aikoo tiedottaa toiminnan lopettamisesta tai siirtymisestä apunaan käyttämilleen henkilöille, allekirjoittajille sekä muille varmennustoimintaan liittyville yhteistyötahoille.

### 3.7 7 § Muut ilmoitukset

Tunnistuspalvelun tarjoajan ja yleisölle laatuvarmenteita tarjoavan varmentajan on ilmoitettava Viestintävirastolle ilman aiheetonta viivytystä palvelun tietoturvaan kohdistuvista merkittävistä uhkista tai häiriöistä sekä näiden korjaamiseksi tehdyistä toimenpiteistä.

Tietoturvalla tarkoitetaan tässä määräyksessä hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Koska käytettävyys on osa palvelun tietoturvaa, myös palvelun käytettävyyteen vaikuttavista vika- ja häiriötilanteista on ilmoitettava Viestintävirastolle.

Palveluntarjoajan tulee tehdä Viestintävirastolle ilmoitus muun muassa:

- häiriöistä sulkulistojen toimivuudessa,
- tunkeutumisesta palveluntarjoajan järjestelmiin,
- varmentajan varmenteiden allekirjoitusavaimen paljastumisesta,
- tunnistus- ja allekirjoitusvälineiden käytössä havaituista vakavista väärinkäytöksistä ja
- vakavista sisäisistä väärinkäytöksistä.

Ilmoituksessa tulee kuvata mahdollisimman tarkasti muun muassa seuraavat asiat:

- tapahtuma-ajankohta,
- miten ja kenen toimesta tapahtuma havaittiin,
- tapahtumaan johtaneet syyt,
- tapahtuman laajuus ja vaikutukset
- suunnitellut/tehdyt korjaustoimenpiteet, sekä korjausaikataulu ja
- tapahtumasta vastaavan henkilön yhteystiedot

Mikäli kaikkia tarvittavia tietoja ei ole heti saatavilla, ne voidaan toimittaa Viestintävirastolle myös jälkikäteen. Tärkeintä on, että ilmoitus tapahtumasta tulee viipymättä Viestintäviraston tietoon.

Laatuvarmenteita yleisölle tarjoavan varmentajan on ilmoitettava Viestintävirastolle, mikäli se takaa ETA:n ulkopuolisen varmentajan varmenteet laatuvarmenteiksi lain 31 §:n 1 momentin 3 kohdassa tarkoitetulla tavalla. Ilmoituksessa on oltava kyseisen ETA:n ulkopuolisen varmentajan nimi ja yhteystiedot sekä tieto siitä, mitkä kyseisen, ETA:n ulkopuolisen varmentajan varmenteet Suomeen sijoittautunut varmentaja takaa laatuvarmenteiksi.

## 4 VIITELUETTELO

[1] Alkuperäinen lakiteksti (617/2009) koskien lakia vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista

<http://www.finlex.fi/fi/laki/alkup/2009/20090617>

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

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:FI:NOT>

[3] Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003), ajantasainen versio:

<http://www.finlex.fi/fi/laki/ajantasa/2003/20030013>

[4] ETSI TS 101.862 Qualified Certificate Profile

<http://pda.etsi.org/pda/queryform.asp>

[5] RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile

<http://www.ietf.org/rfc/rfc3039.txt>

[6] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

<http://www.ietf.org/rfc/rfc3280.txt>