

**MÄÄRÄYKSEN 8 PERUSTELUT JA
SOVELTAMINEN**

**TUNNISTUSPALVELUN TARJOAJIEN JA
LAATUVARMENTEITA TARJOAVIEN
VARMENTAJIEN TOIMINNAN
LUOTETTAVUUS- JA
TIETOTURVALLISUUSVAATIMUKSISTA**

SISÄLLYS

SISÄLLYS	1
1 LAINSÄÄDÄNTÖ	2
1.1 MÄÄRÄYKSEN LAINSÄÄDÄNTÖPERUSTA.....	2
1.2 MUUT ASIAAN LIITTYVÄT SÄÄNNÖKSET.....	2
2 MÄÄRÄYKSEN TARKOITUS JA MUUTOSHISTORIA	2
2.1 MÄÄRÄYKSEN TARKOITUS	2
2.2 KESKEISET MUUTOKSET JA MUUTOSHISTORIA.....	3
2.3 MÄÄRITELMÄT.....	3
3 PYKÄLÄKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET	6
3.1 1 § SOVELTAMISALA	6
3.2 2 § TIETOTURVALLISUUDEN HALLINTA	7
3.3 3 § HAKIJAN ENSITUNNISTAMINEN JA REKISTERÖINTI.....	18
3.4 4 § TUNNISTUSVÄLINEIDEN JA LAATUVARMENTEIDEN LUONTI	21
3.5 5 § VARMENTEIDEN JAKELU	22
3.6 6 § PALVELUN TARJONTA.....	23
3.7 7 § TOIMINNAN LOPETTAMINEN	25
4 VIITELUETTELO	26

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

Viestintäviraston määräysehdotus perustuu lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009, jälj. tunnistuslaki) [1] 8 § 3 momenttiin ja 42 § momenttiin.

1.2 Muut asiaan liittyvät säännökset

Tässä kappaleessa kuvataan Viestintäviraston antamat tämän määräyksen aihepiiriin liittyvät muut määräykset.

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 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

Tietoturvan hallintaa on kuvattu kattavasti muun muassa ISO 27001 (Information Security Management - Specification With Guidance for Use) standardissa [2]. Tämän standardin kattava noudattaminen voi olla liian raskasta erityisesti pienille palveluntarjoajille Suomessa.

Määräyksessä kuvataan ne vähimmäisvaatimukset tietoturvan hallinnoinnille, jotka jokaisen palveluntarjoajan tulee toteuttaa toiminnassaan. Vaatimuksilla pyritään turvaamaan palveluntarjoajan laatuvarmenne- ja/tai tunnistuspalvelun perustietoturvaso, joka toimii pohjana tarjottujen palvelujen tietoturvallisuuden varmistamiseksi. Vaatimuksissa keskitytään erityisesti ensitunnistamisen tärkeyteen, tietoturvallisuuden hallinnan jatkuvaan kehittämiseen, suunnitteluun, toteuttamiseen ja arviointiin. Määräyksellä pyritään myös pienentämään tietoturvariskien aiheuttamia vahingollisia vaikutuksia tarjottavan palvelun toiminnalle.

2.2 Keskeiset muutokset ja muutoshistoria

Määräyksen soveltamisalaa on laajennettu siten, että kaikkia määräyksen pykälää sovelletaan sekä tunnistuspalvelun että laatuvarmennepalvelun tarjoajiin. Määräyksen sisällöllisiä vaatimuksia on muutettu niin, että ne soveltuvat lähtökohtaisesti sekä tunnistuspalveluun että laatuvarmennepalveluun. Mikäli vaatimus soveltuu vain laatuvarmennepalveluun tai varmenteen avulla tarjottavaan tunnistuspalveluun, se on mainittu määräyksessä erikseen.

Tietoturvallisuuden hallintaa koskevia määräyksiä on uusittu siten, että ne on esitetty kootusti määräyksen 2 §:ssä. Lisäksi aikaisemmin vain varmenteen peruuttamista ja voimassaolon tarkistamista koskeva pykälää (aik. 7 §, nyt 6 §) on laajennettu koskemaan palvelun tarjontaa yleisemmin.

2.3 Määritelmät

Tässä kappaleessa kuvataan määräyksessä käytetyt määritelmät.

2.3.1 Palveluntarjoaja

Palveluntarjoajalla tarkoitetaan tässä määräyksessä sekä laatuvarmenteita tarjoavaa varmentajaa, että vahvan sähköisen tunnistuspalvelun tarjoajaa.

2.3.2 Tietoturva

Tietoturvalla tarkoitetaan 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.

2.3.3 Tietoturvariski

Tietoturvariskeillä tarkoitetaan tässä määräyksessä sellaista tahatonta tai tahallista tekijää, joka vaarantaa tarjotun palvelun luottamuksellisuutta, eheyttä tai käytettävyyttä. Tietoturvariskin erottaa tietoturvauhasta sillä, että sen todennäköisyyttä ja vaikutuksia on arvioitu.

Tietoturvariskit voivat aiheutua esimerkiksi:

- inhimillisistä virheistä,
- henkilöstölle annettujen ohjeiden puutteista tai noudattamatta jättämisestä,
- varkauksista,
- kapasiteettivajeista,
- laitteiden rikkoutumisista,

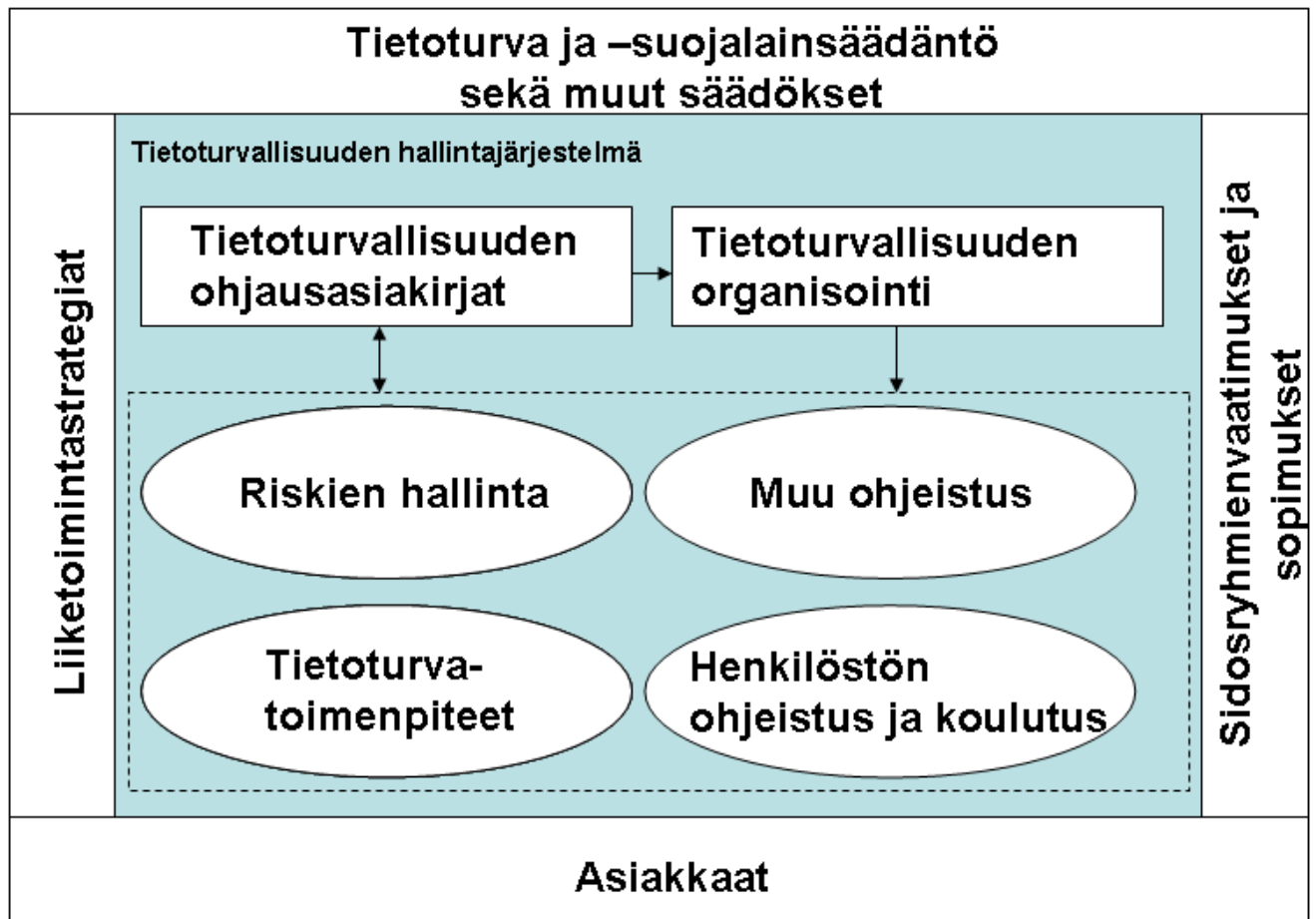
- sovellusvirheistä,
- haittaohjelmien leviämisestä,
- tietoliikennehäiriöistä,
- ilkivallasta,
- tulipalosta ja
- alihankkijan tai kumppanuusverkostoon kuuluvan toimijan virheistä ja laiminlyönneistä.

2.3.4 Varmenne

Varmenteella tarkoitetaan tässä määräyksessä sekä EU:n sähköisen allekirjoituksen direktiivin vaatimukset täyttäviä laatuvarmenteita että vahvaan sähköiseen tunnistamiseen perustuvia, tunnistusvälineessä käytettyjä varmenteita.

2.3.5 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan tässä yhteydessä palveluntarjoajan johtamisjärjestelmän osaa, joka perustuu riskien arviointiin ja hallintaan. Palveluntarjoajalta edellytetään oman toimintaympäristön tuntemusta ja sen erityispiirteiden huomioonottamista oman tietoturvallisuuden hallintajärjestelmän kehityksessä. Hallintajärjestelmän vaatimukset tulevat liiketoimintastrategian lisäksi yleensä tietoturva ja -suojalainsäädännöstä, Viestintäviraston antamista määräyksistä, muista säädöksistä sekä asiakkaiden ja sidosryhmien vaatimuksista ja sopimuksista.



Palvelun tarjoajan tietoturvasta huolehtimisen vaatimukset tulevat tietoturva ja -suojalainsäädännöstä, sekä muista säädöksistä esimerkiksi:

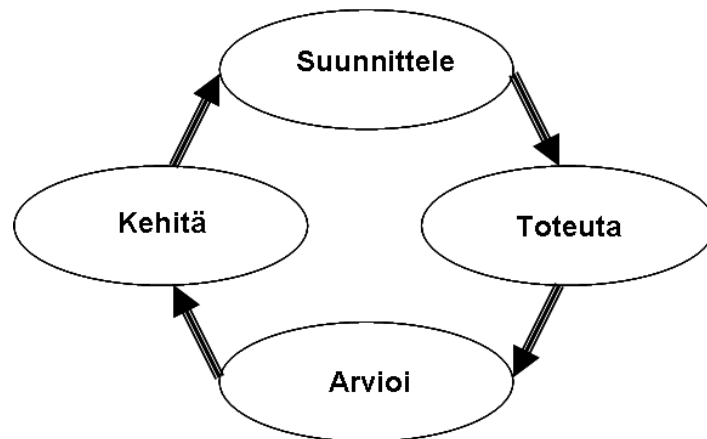
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista,
- Viestintäviraston määräys 8/2010 M
- Henkilötietolaki.

Palveluntarjoajan toimintaan saattaa kohdistua myös muita vaatimuksia tietoturvan osalta, kuten esimerkiksi:

- asiakkaiden vaatimukset,
- tunnistusvälineisiin ja laatuvarmenteisiin liittyvät muut määräykset, säädökset ja standardit
- toimialakohtaiset vaatimukset

Hallintajärjestelmän tarkoituksena on toimia tietoturvallisuuden kehittämisen, suunnittelun, toteutuksen ja arvioinnin tukena.

Tietoturvallisuuden hallintajärjestelmää kuvataan yleisesti esitettynä nelivaiheisena prosessina:

**Suunnitteluvaihe:**

Suunnitteluvaiheessa luodaan politiikat, määritellään tavoitteet ja kohteet sekä tarvittavat toiminnot tietoturvallisuuden osalta.

Toteutusvaihe:

Toteutusvaiheessa sovelletaan tietoturvapoliittikoja, -kontrolleja ja -toimintoja.

Arviointivaihe:

Arviointivaiheessa mitataan toimenpiteiden vaikutuksia suunnitteluvaiheessa määriteltyihin tavoitteisiin, politiikkoihin ja käytännön kokemuksiin.

Kehitysvaihe:

Kehitysvaiheessa kehitetään tietoturvallisuuden hallintajärjestelmää arviointivaiheen tulosten pohjalta. Kehityskohteita voivat olla esimerkiksi tietoturvapoliittikat ja tietoturvatoinnot.

3 PYKÄLÄKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET

Tässä luvussa käydään läpi pykäläkohtaisesti pykälän perustelut sekä sen soveltamissuositukset.

Tämän dokumentin tarkoituksena on kuvata hyviä käytäntöjä ja auttaa niiden toteuttamisessa. Se ei sellaisenaan sido tunnistuspalvelujen tarjoajia tai laatuvarmentajia, eikä sitä myöskään sellaisenaan käytetä tunnistuspalvelujen tarjoajien tai laatuvarmentajien tietoturvajärjestelyjen arvioinnin tai auditoinnin mittapuuna. Suositusluontoiset asiat on kirjattu suositus-muotoon.

Tässä dokumentissa on mukana myös määräyksestä tulevat velvoitteet ja ne on kirjattu tarkoituksella määräävään muotoon.

3.1 1 § Soveltamisala

Tätä määräystä sovelletaan vahvan sähköisen tunnistuspalvelun tarjoajiin ja laatuvarmenteita tarjoaviin varmentajiin. Kun määräyksessä viitataan sekä tunnistuspalvelun tarjoajiin että laatuvarmenteita tarjoaviin varmentajiin, käytetään yhteisnimitystä palveluntarjoaja.

Tunnistuspalvelun tarjoajalla ja laatuvarmenteita tarjoavalla varmentajalla tarkoitetaan samaa kuin tunnistuslaissa eikä määritelmiä ole tarpeen erikseen toistaa määräyksessä. Tunnistuslain 2 §:n 4 kohdan mukaan tunnistuspalvelun tarjoajalla tarkoitetaan palveluntarjoajaa, joka tarjoaa vahvan sähköisen tunnistamisen palveluita niitä käyttäville palveluntarjoajille tai laskee liikkeelle tunnistusvälineitä yleisölle tai molempia.

Varmentajalla tarkoitetaan lain 2 §:n 8 kohdan mukaan luonnollista henkilöä tai oikeushenkilöä, joka tarjoaa varmenteita yleisölle. Laatuvarmenteita tarjoava varmentaja on sellainen varmentaja, joka tarjoaa lain 30 §:n mukaisia laatuvarmenteita. Koska varmenteen tarjoaminen yleisölle on edellytyksenä jo tunnistuslain varmentajan määritelmässä, sitä ei ole tarpeen tässä yhteydessä erikseen toistaa.

3.2 2 § Tietoturvallisuuden hallinta

Tietojen, tietojärjestelmien ja toimintaedellytysten turvaaminen edellyttää tietoturvatointojen tehokasta organisointia yrityksessä. Perusedellytyksenä on, että tietoturvatointojen vastuut ja velvollisuudet on määritelty.

3.2.1 Tietoturvallisuuden organisointi

Tietoturvallisuuden hallintajärjestelmään tulee sisällyttää ylimmän johdon näkemys siitä, miten tietoturvallisuuden vastuut jakautuvat organisaatiossa. Tietoturvallisuuden vastuut ja velvollisuudet voivat olla sekä hallinnollisia vastuuta että operatiivisia vastuuta. Tietoturvastuuta on syytä tarkistaa erityisesti silloin kun organisaatiossa tapahtuu muutoksia. Kysymyksessä voi olla esimerkiksi henkilöstössä tapahtunut muutos tai yritysjärjestelyn toimintaympäristöön aiheuttama muutos.

Tietoturvallisuuden vastuut voivat olla jaoteltuina ryhmiin. Hallinnollisen vastuun osalta voidaan esimerkkinä mainita tietoturvallisuusryhmä. Operatiivisista ryhmistä esimerkkinä mainittakoon cert/csirt -ryhmät.

Esimerkkejä hallinnollisista tietoturvallisuusvastuista ovat tietoturvallisuuden hallintajärjestelmän ja ohjausasiakirjojen kehittäminen, yrityksen tietoturvallisuustilannetta kuvaavan seurantajärjestelmän ylläpitäminen, tietoturvallisuusasioiden huomioiminen riskienhallinnassa ja jatkuvuussuunnittelussa, asiaan kuuluvien tietojärjestelmien ylläpitäminen ja kehittämien sekä tietoturvallisuustoimintojen ja -investointien oikeasuhtainen resursointi ja tietoturvallisuusasioiden huomioiminen erityisesti avaintoimintojen henkilökunnan koulutuksessa.

Koska nämä vastuut koskettavat useita yrityksen johtamisjärjestelmän osa-alueita, on suositeltavaa ohjata ja valvoa tietoturvallisuusvastuiden toteutumista koordinoidulla tavalla. Toimivan koordinoinnin merkitys on sitä tärkeämpi, mitä laajemmin tietoturvallisuusvastuut on yrityksen organisaatiossa hajautettu. Yrityksen koosta riippuen tietoturvallisuusasioiden kehittäminen ja seuranta tulee olla vastuutettu yhdelle tai useammalle tietoturvallisuusvastaavalle. Tietoturvallisuusasioita tulee käsitellä osana normaalia johdon raportointia.

Tietoturvaloukkaustapausten koordinoidusta ensivasteen toiminnasta ja ilmoitusyhteyspisteen ylläpidosta käytetään joissakin yhteyksissä nimityksiä CERT (Computer Emergency Response Team) - tai CSIRT (Computer Security Incident Response Team)-toiminta.

Palveluntarjoajalla on aina oltava perusvalmius omaan toimintaansa kohdistuvien ja merkittävällä tavalla asiakkaisiin vaikuttavien tietoturvaloukkausten ja -riskien hallinnoimiseksi.

Hallinnollisilla vastuilla voidaan esimerkiksi tarkoittaa vastuuta:

- tietoturvapoliitikan suunnittelusta,
- henkilöstön tietoturvakoulutuksen suunnittelusta,
- palveluntarjoajan oman tietoturvatason seuraamisesta,
- riskien hallinnan suunnittelusta ja organisoinnista ja
- tietoturvaa parantavien hankkeiden käsittelystä ja suunnittelusta.

3.2.2 Tietoturvallisuuden ohjausasiakirjat

Tietoturva on osa tarjotun palvelun laatua. Tietoturvallisuuden ohjausasiakirjat ovat tietoturvallisuuden perusdokumentteja, joilla organisaation johto osoittaa tietoturvallisuuden tahtotilan ja yleiset periaatteet. Dokumentit luovat perustan järjestelmälliselle tietoturvakehitykselle ja tietoturvan hallinnalle, sekä auttavat tietoturvaluusunvestointien kohdentamisessa.

Palveluntarjoajan on suunniteltava tietoturvallisuuden ohjausasiakirjat omien riskiensä ja tarpeidensa mukaan. Esimerkiksi tietoturvaryhmä tai muu riittävän laaja edustus organisaatiosta valmistelee asiakirjat johdon hyväksymistä varten. Asiakirjat valmistellut toimija voi myös huolehtia niiden julkaisemisesta ja tarkoituksenmukaisesta tiedottamisesta kaikille organisaation työntekijöille. Ohjausasiakirjojen tulee olla helposti kaikkien työntekijöiden saatavilla, esimerkiksi organisaation intranet-sivujen kautta. Lisäksi asiakirjojen tulee olla osana uuden henkilön perehdytysohjelmaa. Palveluntarjoajan on huolehdittava, että asiakirjoissa esitettyjä tietoturvallisuuden pääperiaatteiden noudattamista valvotaan.

Tietoturvallisuuden ohjausasiakirjoista tulee ilmetä seuraavat asiat yrityksen tunnistamis- tai laatuvarmennepalveluna pidettävän toiminnan osalta:

- tietoturvatavoitteet,

- vastuut tietoturvasta huolehtimiselle,
- tietoturvallisuusorganisaatio ja
- keinot organisaation oman tietoturvallisuuden ylläpitämiseksi ja kehittämiseksi esimerkiksi sisäisten auditointien osalta.

Palveluntarjoajalla on oltava kirjallisesti dokumentoituna se, miten seuraavat erityysoa-alueet on käytännössä huomioitu ja toteutettu niiltä osin, kuin ne ovat soveltuvia tunnistamis- ja laatuvarmennepalveluun:

- Henkilöstöturvallisuus
 - Henkilöiden tietoturvallisuuteen liittyvät vastuut ja velvollisuudet.
 - Henkilöstön tietoturvaosaaminen ja sen kehittäminen.
 - Avainhenkilöriskien kartoitus mahdollisine taustatarkastuksineen.
 - Palvelun tarjonnan kannalta vaarallisten vastuu- ja tehtäväkokonaisuuksien estäminen.
 - Ohjeet työsuhteen päättyessä noudatettavasta menettelystä.
- Fyysinen turvallisuus
 - Asiattomien pääsyn estäminen toimitiloihin
 - Tiloihin pääsyn valvonta
 - Järjestelmien palo-, vesi-, sähkö- ja ilmastointivahinkojen ennalta ehkäiseminen
- Laitteisto-, ja ohjelmistoturvallisuus
 - Riittävä dokumentaatio havaitun haavoittuvuuden korjauksen kohdentamiseksi.
 - Varaosien saanti.
 - Yleinen järjestelmien muutosten hallintaprosessi.
- Tietoliikenneturvallisuus
 - Riittävästä verkkotason tietoturvallisuudesta huolehtiminen avoimiin ja epäluotettaviin verkkoihin kytkettyäessä esimerkiksi salausmenetelmin.
 - Välitettävien viestien luottamuksellisuuden ja eheyden varmistaminen
 - Verkkotason riittävästä pääsynhallinnasta huolehtiminen esimerkiksi palomuurein
- Tietoaineistoturvallisuus
 - Tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistaminen: Miten tiedot luokitellaan ja miten henkilöstö ohjeistetaan tietojen käsittelystä.
- Käyttöturvallisuus
 - Käyttöoikeusrekisterin ylläpitovastuut: käyttöoikeuksien jakaminen, muuttaminen ja poistaminen.
 - Käyttöoikeuksien kasaantumisen estäminen.
 - Asiaankuulumattomien pääsyn estäminen palveluiden toteuttamiseen liittyviin hallinta- ja konfiguraatietietoihin.
- Tietoturvaloukkauksiin ja väärinkäyttöihin puuttuminen
 - Toimintavastuut tietoturvallisuuden kannalta merkittävien tapahtumien havaitsemiseen ja niihin puuttumiseen.
 - Toimintaohjeet ja prosessit tietoturvaongelmista toipumiseksi.

- o Vakavuuden arviointi.
- o Viranomaisilmoitukset.
- o Poikkeamista tiedottaminen.
- o Poikkeaman jälkeinen toiminta.
- o Henkilöstön väärinkäytökset ja ohjeistuksen vastaiset toimet.

Palveluntarjoajan tulee lisäksi määritellä riittävän yksityiskohtaiset ohjeet tietoturvallisuuden kannalta olennaisten yksittäisten käytäntöjen osalta. Käytännössä tämä tarkoittaa tarkan ohjeistuksen määrittelemistä muun muassa henkilötietojen käsittelystä.

Alihankinta- / toimintojen ulkoistamissopimuksissa tulee huolehtia siitä että tietoturva-astuiden rajat on määritelty riittävän tarkasti palveluntarjoajan ja alihankkijan välillä. Kokonaisvastuu palveluiden tietoturvallisuudesta kuuluu kuitenkin aina palveluntarjoajalle, riippumatta siitä onko toimintoja ulkoistettu vai hoidetaanko ne itse.

Alihankintasopimukseen on syytä sisällyttää viittaukset palvelun tarjontaa koskeviin velvoittaviin säädöksiin ja sanktiot säädösten rikkomisesta.

Huoltovarmuuskeskus on julkaissut suosituksia [3], joihin voidaan viitata sopimuksissa toiminnan jatkuvuuden hallinnan osalta. Nämä suositukset käsittelevät:

- johtamista,
- toiminnan ohjausta,
- henkilöstöä ja henkilöressurssien hallintaa,
- kumppanuuksia ja
- toiminnan jatkuvuuden hallinnan arviointia.

3.2.3 Riskien hallinta

Tietoturvallisuuden hallintajärjestelmän yksi tärkeimmistä komponenteista on tehokas riskienhallinta. Sillä tarkoitetaan yleensä yrityksen liiketoimintaan liittyvien merkittävien riskien tunnistamista, tunnistamisen jälkeistä riskien arviointia ja hallitsemistoimenpiteitä sekä toimenpiteiden toteuttamisen valvontaa. Hallintajärjestelmän päätehtävänä on suojella organisaatiota ja sen kykyä suorittaa sille annettuja tehtäviä normaali-, normaaliolojen häiriö- ja poikkeusoloissa taloudelliset seikat huomioon ottaen. Riskienhallinta voi olla osa yrityksen varautumis- tai jatkuvuussuunnittelua.

Riskien hallinnan tavoitteena on muun muassa:

- nopeuttaa tietoturvaongelmista toipumista,
- vähentää tietoturvaongelmista aiheutuneita kustannuksia ja vahinkoja,
- kohdentaa tietoturvallisuutta parantavia investointeja,
- palvelun laadun ja tuottavuuden parantaminen,
- palveluun kohdistuvien riskien hallinnan taloudellinen optimointi ja

- palveluun kohdistuvien riskien toteutumisen ennaltaehkäisy.

Riskien hallinnan vaatimuksilla pyritään varmistamaan se, että palveluntarjoaja on tietoinen riskien toteutumisen aiheuttamista seurauksista ja ovatko riskiä pienentävät toimenpiteet riittäviä.

Riskien hallinnasta on laadittu mm. seuraavia standardeja ja julkaisuja:

- ISO/IEC TR 13335-3, Information technology - Guidelines for the management of IT Security - Techniques for the management of IT Security. [4],
- ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management [5],
- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology [6],
- Enisa: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools [7],
- COSO ERM (Enterprise Risk Management - Integrated Framework (2004)) [8],
- BS 31100:2008, Risk management. Code of practice [9],
- ISO 31000 Risk management -- Principles and guidelines [10],
- The Institute of Risk Management (IRM), Risk Management Standard [11] ja
- PK-RH:n Pk-yrityksien riskien hallinta [12].

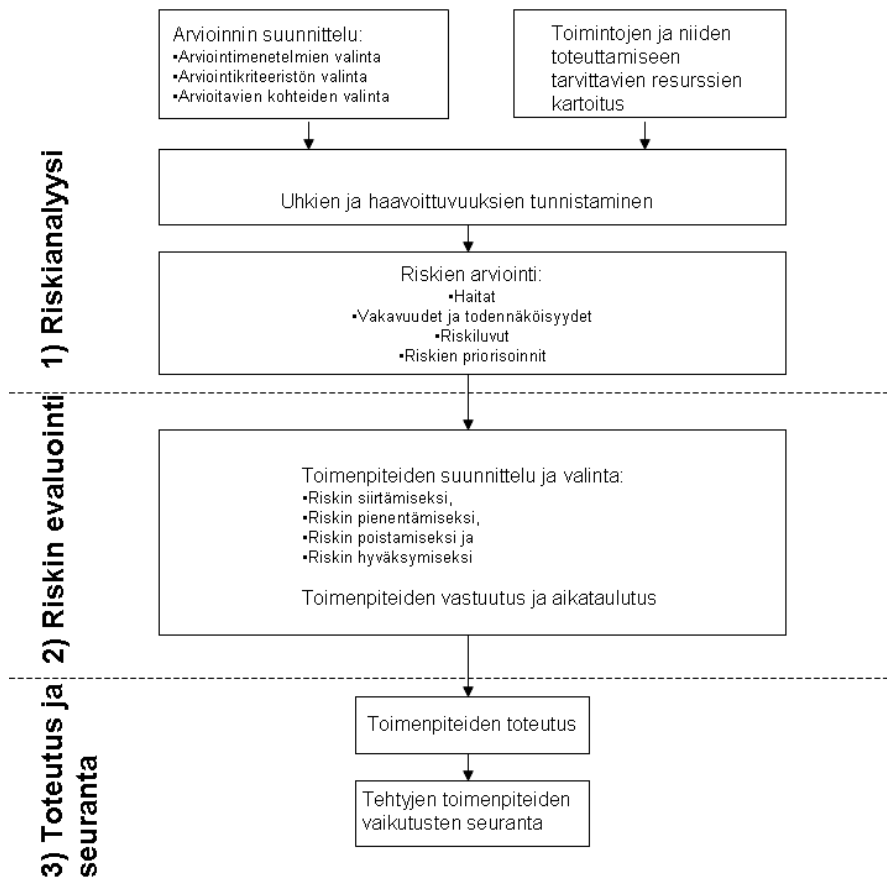
Tässä määräyksessä ei aseteta velvoitetta tietyn standardin noudattamiselle. Riskienhallintamallit vaihtelevat yhtiöittäin, eikä yhtä jokaiselle sopivaa mallia ole olemassa. Keskeistä on sitoa riskienhallintajärjestelmän tavoitteet yhtiön toiminnallisiin tavoitteisiin ja pitää huolta yhtiön johdon tuesta.

Minimivaatimuksena riskien hallinnan osalta voidaan pitää, että:

- Palveluntarjoaja on luokitellut tarjotun palvelun kannalta tärkeimmät ja kriittisimmät toiminnot, prosessit ja järjestelmät,
- Palvelun tarjoamiseen liittyvät tietoturvallisuus riskit on kartoitettu ja
- Palvelun tarjoaja seuraa säännöllisesti tarjottuun palveluun liittyvää tietoturvallisuuden tasoa. Tietoturvallisuuden tasoa voidaan seurata esimerkiksi pistokokeiden, tietoturvallisuustarkastusten ja tietoturvallisuusauditointien avulla.

Palvelun tarjoamiseen liittyvät tietoturvallisuusriskit on kartoitettava tarjotun palvelun kannalta tärkeimpien ja kriittisimpien toimintojen, prosessien ja järjestelmien osalta ja toimenpiteet havaittujen riskien pienentämiseksi, poistamiseksi ja siirtämiseksi on dokumentoitava.

Riskien hallinta voidaan karkeasti jakaa kolmeen eri vaiheeseen:



3.2.3.1 Riskianalyysi

Riskianalyysillä tarkoitetaan niitä järjestelmällisiä toimenpiteitä, joilla pyritään tunnistamaan palvelun toteuttamista vaarantavia tietoturvaluuhkia ja haavoittuvuuksia, sekä arvioimaan mahdollisesti toteutuvien uhkien seurauksia. Riskianalyysi on suunniteltava, toteutettava ja dokumentoitava laadukkaasti. Riskianalyysi tulisi tehdä kohteelle ennalta määrättyyn tavoitetasoon nähden. Tällä tarkoitetaan esimerkiksi Viestintäviraston määräyksessä tai asiakassopimuksessa asetettua vaatimusta palvelun käytettävyydelle. Riskianalyysillä haetaan erityisesti niitä uhkia jotka vaarantavat kohteelle asetetun tavoitteen täyttymisen.

Riskianalyysi koostuu viidestä osa-alueesta, jotka ovat:

- arvioinnin suunnittelu,
- palvelua vaarantavien tietoturvaluuhkien tunnistaminen,
- alttiina olevien järjestelmien ja toimintojen tunnistaminen,
- riskien vakavuuksien ja todennäköisyyksien arviointi ja
- riskien priorisointi.

Riskianalyysin keskeisimpinä tavoitteina on:

- tukea tietoturvaluuhkijohtamista ja investointien kohdentamista,

- tietoturvallisuuden parantaminen ja
- tunnistaa palvelun toimintaa vaikuttavat tietoturvallisuusriskit ja niiden vakavuudet.

Riskianalyysin tavoitteista johtuen riskianalyysin tekijöiden olisi syytä tuntea hyvin riskianalyysin kohteen toiminta, toiminnan tavoitteet ja siihen kohdistuvat vaatimukset.

Riskien arvioinnin suunnittelu

Riskiarvoinnin suunnittelun tulee sisältää käytettävät riskien arviointimenetelmät, riskien arvioinnin kriteerit ja arvioinnin tavoitteet sekä aihealueet joihin arviointi kohdistuu.

Arvioinnin suunnittelussa on syytä ottaa huomioon tarjotun palvelun laajuus ja organisaation mahdollisuudet. Minimivaatimus riskien arvioinnin suunnittelun kannalta on kuitenkin se, että pelkistetykin arviointimenetelmät on dokumentoitu.

Riskien arvioinnissa kannattaa hyödyntää esimerkiksi aiempia tietoturvaluustarkasteluja, "läheltä piti" tilanteista saatavilla olevaa tietoa ja muuta tietoturvallisuuteen liittyvää aineistoa.

Palvelun tarjoajan tulee varmistaa, että arviointiin osallistuvilla henkilöillä on riittävä tietämys käytettävästä riskien arviointimenetelmästä.

Suunnitteluvaiheessa tulee sopia myös riskien arvioinnin kirjaamisesta, tallentamisesta ja arvioinnin tulosten käsittelystä.

Toimintojen ja niiden toteuttamiseen tarvittavien resurssien kartoitus

Järjestelmien ja toimintojen tunnistamisen perusedellytys on, että tarjotun palvelun kannalta keskeisten järjestelmien ja toimintojen kartoitus on tehty ainakin seuraavilta osa-alueilta:

- Laitetilat,
- Laitteistot ja ohjelmistot,
- Tietoliikenneyhteydet,
- Tietoaineistot ja
- Järjestelmien ylläpito- ja tukihenkilöt.

Kartoitus parantaa palvelun tarjoajan mahdollisuuksia arvioida tietojärjestelmien ja käsiteltävien tietojen kriittisyyttä, arkaluontoisuutta ja tarvittavaa resursointia. Lisäksi kartoitus helpottaa tietoturvallisuutta parantavien toimenpiteiden kohdentamista.

Uhkien tunnistaminen

Uhkalla tarkoitetaan tässä yhteydessä palvelun toimintaa vaarantavaa tilannetta, jonka todennäköisyyttä tai vakavuutta ei ole arvioitu. Uhkien määrittely riippuu valittavasta riskianalyysikohteesta ja rajauksesta. Uhkien määrittelyssä tulee hyödyntää riskianalyysin kohteeseen tehtyjen tietoturvallisuusauditointien tuloksia sekä aikaisemmin realisoituneita riskejä tai tietoturvapoikkeamia. Tietoturvallisuusauditoinnit voidaan toteuttaa joko talon sisäisinä auditointeina tai ne voidaan ostaa palveluna ulkopuoliselta toimittajalta. Auditointeja olisi suositeltavaa tehdä kohteen kriittisyydestä riippuen 6kk - 2 vuoden välein ja aina silloin kun arvioitavassa kohteessa tapahtuu merkittäviä muutoksia.

Uhkan toteutumiseen liittyy aina jokin haavoittuvuus eli alttius palvelun toimintaa uhkaavalle tekijälle. Haavoittuvuudet voivat olla joko teknisiä tai ei teknisiä, ja ne voivat liittyä esimerkiksi:

- laitteistoihin ja ohjelmistoihin,
- prosesseihin ja
- henkilöstöön.

Laitteistoihin ja ohjelmistoihin liittyvällä uhalla tarkoitetaan esimerkiksi sitä, että jokin haittaohjelma estää ko. laitteen tai ohjelmiston toiminnan.

Prosesseihin liittyvillä uhalla voidaan tarkoittaa esimerkiksi edellä mainitun haittaohjelmatartunnasta selviämisen viivästyminen. Haavoittuvuutena voi olla esimerkiksi sovittujen toimintatapojen puuttuminen.

Henkilöstöön liittyvä uhka voi olla, että jokin palvelu jää ilman vastuuhenkilöä. Tähän liittyvä haavoittuvuus on esimerkiksi vastuuhenkilön sairaus tai irtisanoutuminen.

Riskien arviointi

Riskien arvioinnilla tarkoitetaan tunnistetun uhan vakavuuden ja sen toteutumisen todennäköisyyden arviointia.

Analysoidut riskit voidaan priorisoida esimerkiksi riskiluvun perusteella, joka voidaan muodostaa esimerkiksi uhan vakavuuden ja uhan todennäköisyyden kertolaskun tuloksena. Riskien priorisointi niiden liiketoiminnalle aiheuttamien vaikutusten kannalta on erityisesti suurimmissa yrityksissä yleisesti käytetty menetelmä. Pääasia on kuitenkin se, että havaitut riskit on luokiteltu jollain tavoin käytössä olevien resurssien kohdistamiseksi vakavimpiin riskeihin.

Riskien luokittelu toimii suosituksena, joka tukee päätöksen tekoa korjaavia toimenpiteitä suunniteltaessa ja kohdennettaessa

Dokumentointi:

Dokumentoinnin tulee sisältää sellaiset tiedot, joiden perusteella voidaan jälkikäteen arvioida riskien hallinnan toteutumista ja riskikartoituksen ja toimenpiteiden riittävyyttä. Dokumentoinnin tulee sisältää ainakin seuraavat asiat:

- riskianalyysi
 - riskianalyysin tavoitteet,
 - riskianalyysin rajaukset,
 - riskianalyysin tuotokset ja
 - riskianalyysin loppuraportti.

- riskien evaluointi
 - lista suurimmista riskeistä ja
 - lista kriittisimmistä puutteista.

3.2.3.2 Riskin evaluointi

Riskin evaluoinnissa nostetaan esiin keskeisimmät kehittämistarpeet riskien arvioinnin tulosten pohjalta. Tästä riskien arvioinnin yhteenvedosta käy ilmi muun muassa:

- suurimmat riskit,
- kriittisimmät puutteet ja
- lisäselvitysten kohteet.

Toimenpiteiden suunnittelu ja valinta

Riskianalyysin pohjautuvien tietoturvatöiden valinnassa on syytä ottaa huomioon ratkaisujen kustannukset, henkilöresurssit, yrityksen riskinottohalukkuus ja riskin toteutumisesta aiheutuvat tappiot.

Jos merkittävää riskiä ei voida kokonaan poistaa, tulee palvelun tarjoajan tehdä toipumissuunnitelma riskin toteutumisen varalle.

Riskin toteutumisesta aiheutuvat kustannukset voidaan myös siirtää kolmannelle osapuolelle esimerkiksi vakuutuksilla tai sopimuksilla. Riskin toteutuessa kokonaisvastuu palvelun tietoturvasta säilyy joka tapauksessa palveluntarjoajalla.

Vaikutuksiltaan vähäiset riskit voidaan usein hyväksyä, jos riskit eivät ole lainsäädännön ja määräysten vastaisia. Usean vähäisen riskin toteutuminen samanaikaisesti voi kuitenkin muuttaa tilannetta merkittävästi esimerkiksi tarjottavan palvelun laadun suhteen. Tehtäessä päätöksiä riskien hyväksymisestä on otettava tapauskohtaisesti huomioon kenen kannalta ja missä olosuhteissa riski on hyväksyttävissä, sekä riskin toteutumisesta aiheutuvat seuraamukset ja kustannukset.

Toiminnon tai palvelun omistajan tulee huolehtia siitä, että riskit tulevat hyväksytyksi. Päätös riskien hyväksymisestä tapahtuu yrityksen päätäntävaltuuksien mukaisesti.

3.2.3.3 Toteutus ja seuranta

Valituille tietoturvaa parantaville toimenpiteille tulee laatia suunnitelma, jossa on määritelty muun muassa vastuuhenkilöt päätetyille toimenpiteille ja toteutuksille sekä aikataulu niiden seurannalle.

Tietoturvaa parantavia toimenpiteitä riskin poistamisen osalta ovat esimerkiksi:

- tietyn tuotteen, protokollan tai menetelmän välttäminen,
- epämääraisten sopimuskumppaneiden välttäminen ja
- liian suuren riskin omaavasta toiminnasta luopuminen.

Tietoturvaa parantavia toimenpiteitä riskien pienentämisen osalta ovat esimerkiksi:

- henkilöstön koulutus tietoturvallisuuden osalta,
- toimintaohjeet,
- tietoturvallisuutta parantavien tuotteiden käyttöönottoaminen,
- varajärjestelmät,
- ajantasaiset varmuuskopiot,
- dokumentaation turvaluokitukset ja
- kulunvalvonta.

Riskien ennalta havainnointia voidaan parantaa esimerkiksi suorittamalla kohteille säännöllisiä auditointeja, ottamalla riskienhallinta mukaan tuotekehitykseen mahdollisimman aikaisessa vaiheessa, henkilöstön tietoturvallisuustietoisuuden lisääminen ja ongelmatilanteista raportoinnin ohjeistaminen.

Riskejä voidaan ennaltaehkäistä henkilöriskien osalta esimerkiksi varahenkilöjärjestelyin ja tietojärjestelmien osalta varajärjestelmillä.

Palveluntarjoajan tulee määritellä yksityiskohtaiset ja riittävät ohjeet tietoturvallisuuden kannalta olennaisten yksittäisten käytäntöjen osalta. Nämä ohjeet voivat koskea esimerkiksi seuraavia osia:

- vierailijakäytännöt,
- kulkuoikeuksien hallinnointi,
- palveluntarjonnassa käytettyjen järjestelmien etäkäyttö ja
- arkaluontoisten tietoaisteiden käsittely (esim. asiakastiedot).

Palveluntarjoajalla on oltava käytössä tarjotun palvelun kannalta tärkeiden tietoaisteiden käsittelyohje. Käsittelyohjeen tulee kattaa muun muassa seuraavat asiat:

- yleiset periaatteet tietoaisteiden turvaluokan ja luottamuksellisuuden arvioimiseksi ja tietoaisteiden salassa pysymiseksi,
- käsittely- ja muutosoikeudet tietoaisteiden lukuoikeuksien jakamisesta, muutosoikeuksista sekä näiden oikeuksien jakamisesta,
- luottamuksellisuusluokan määrittäminen,
- tiedon tai asiakirjan julkisuus: esimerkiksi asiasta puhumisesta julkisesti,
- asiakirjan ominaisuudet: paperi, leima ja muut merkinnät

- säilytys ja salaaminen
- tulostaminen ja kopiointi
- vastaanottaminen, jakaminen, lähettäminen ja kuljettaminen,
- tietojen ja asiakirjan käsittelyn dokumentoiminen ja
- asiakirjan arkistointi, käsittely tai käsittelyoikeuksien päättyminen, tietojen ja asiakirjan hävittäminen.

Kaikelle turvaluokitellulle tietoaineistolle on erikseen määriteltävä käyttäjä- tai käyttäjäryhmäkohtaiset käsittelyoikeudet. Samalla on huolehdittava siitä, että asiaan kuulumattomat eivät pääse käsiksi turvaluokiteltuihin tietoaineistoihin. Turvaluokiteltujen tietoaineistojen on kuitenkin oltava niiden käsittelyyn oikeutettujen käytettävissä.

Palveluntarjoajan tietoaineistojen käsittelyohje voi pohjautua soveltuvin osin esimerkiksi Valtionvarainministeriön valmistelemaan valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohjeeseen[13].

Palveluntarjoajan on huolehdittava, että tarjotun palvelun käytettävyyden kannalta olennaisista tietoaineistoista on ajan tasalla olevat varmuuskopiot, jotka säilytetään lukituissa tiloissa ja erillään kyseisistä laitteista. Varmuuskopiot on voitava ottaa käyttöön alkuperäisen tietoaineiston vaurioituessa esimerkiksi ohjelmistovian, laitevian tai laiteilassa tapahtuneen onnettomuuden jälkeen. Tällaisia tietoaineistoja ovat esimerkiksi käyttäjätiedot ja konfiguraatitiedot.

3.2.4 Väärinkäytöksiä ja tietoturvallisuusongelmien havaitseminen ja niihin puuttuminen

Palveluntarjoajalla tulee olla kyky reagoida tietoturvaloukkauksiin ja tietoturvauhkiin, jotka vaikuttavat toisaalta yrityksen kyvyn tarjota palveluita sekä toisaalta oleellisella tavalla vaarantavat palveluntarjoajan asiakkaiden tietoturva.

Tarjottujen palveluiden väärinkäytöksiin ja tietoturvallisuusongelmiin puuttuminen tulee olla organisoitua ja sisältää ainakin seuraavia toimintoja:

- Ohjeiden ja prosessien valmistelu väärinkäytösten ja tietoturvallisuusongelmiin puuttumisesta
- Asiakaspalautteen seuraaminen
- Väärinkäytöksistä ja tietoturvaongelmista raportoiminen
- Vastuut ja toiminnot väärinkäytöksiä ja tietoturvaongelmien tutkimiselle, esitutkintaan saattamiselle ja niiden vakavuuksien arvioimiselle
- Vastuut ja toiminnot vahinkojen rajoittamiselle, väärinkäytöksen tai tietoturvallisuusongelman poistamiselle, sekä ylemmän johdon tiedottamiselle
- Viranomaisilmoitukset esimerkiksi Viestintäviraston antaman määräyksen 7 B/2009 M osalta.

- Vastuut ja toiminnot väärinkäytöksestä tai tietoturvallisuusongelmasta toipumiselle
- Toiminnot tapahtuman uusiutumisen estämiselle

3.2.5 Tietoturvallisuuden hallinnan seuranta

Tietoturvallisuuden hallinta on jatkuvaa, muutoksiin reagoivaa ja osa yrityksen normaalia toimintaa palveluiden suunnittelusta ylläpitämis-vaiheeseen.

Organisaation johdon on huolehdittava riittävästä resursseista tietoturvallisuuden hallintajärjestelmän suunnitteluun, toteutukseen, arvioimiseen ja ylläpitämiseen.

Tietoturvallisuuden hallintajärjestelmää tulee ylläpitää säännöllisesti ja päivittää tarvittaessa. Muutostarpeita tulee tarkastella kerran vuodessa ja aina tarpeen vaatiessa. Tarvetta hallintajärjestelmän muutoksille voi tulla esimerkiksi organisaatiomuutosten tai yrityksen strategiamuutosten yhteydessä. Myös henkilöstövaihdokset voivat luoda tarpeen hallintajärjestelmän päivitykselle. Muutosten yhteydessä on varmistettava tietoturvakäytäntöjen ja sopimusten yhteensopivuudesta.

3.3 3 § Hakijan ensitunnistaminen ja rekisteröinti

Ensitunnistaminen

Tunnistuspalvelun tarjoajan ja laatuvarmenteita tarjoavan varmentajan on todennettava tunnistusvälineen tai laatuvarmenteen hakijan henkilöllisyys huolellisesti laissa asetettujen edellytysten mukaisesti. Tunnistusvälineen hakijan ensitunnistamisesta on säädetty tunnituslain 17 §:ssä ja laatuvarmenteen hakijan tunnistamisesta lain 35 §:ssä.

Ensitunnistaminen on tehtävä tunnistusvälineen tai laatuvarmenteen hankkimisen yhteydessä. Ensitunnistamista ei siis voida tehdä ennalta siltä varalta, että asiakas haluaisi joskus ottaa tunnistusvälineen käyttöönsä. Jos tunnistusvälineen hakijalla on jo voimassa saman palveluntarjoajan antama tunnistusväline ja väline uusitaan tai vaihdetaan toiseen, ensitunnistamista ei tarvitse tehdä uudelleen vaan asiakas voidaan tunnistaa sähköisesti olemassa olevalla tunnistusvälineellä. Välineen uusimisella ei tässä tapauksessa tarkoiteta pelkän uuden avainlukulistan lähettämistä vaan esimerkiksi tunnistusvälineen vaihtamista toiseen tai määräaikaisen sopimuksen uusimista. Väestörekisterikeskuksen myöntämää laatuvarmennetta voidaan hakea sähköisesti voimassaolevalla laatuvarmenteella lain väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 68 §:n nojalla.

Ensitunnistamisessa hakija on tunnistettava henkilökohtaisesti. Ensitunnistamisen henkilökohtaisuudesta voidaan poiketa lain 17 §:n 2 momentin mukaan, jos tunnistuspalvelun tarjoajat ovat tehneet keskenään sopimuksen mahdollisuudesta luottaa toistensa tekemään ensitunnistamiseen. Tällöin tunnistusvälinettä voidaan hakea myös sähköisesti sillä edellytyksellä,

että alkuperäisen ensitunnistuksen henkilökohtaisesti tehneen tunnistuspalvelun tarjoajan on aina oltava sopimuksen toinen osapuoli.

Tunnistuspalvelun tarjoaja voi käyttää asiamiestä ensitunnistuksen tekemiseen. Tunnistuspalvelun tarjoajan tulisi varmistaa asiamiehen luotettavuus, tietoturvan taso ja toimintatapojen turvallisuus. Tunnistuspalvelun tarjoajan vastaa kuitenkin myös tältä osin apunaan käyttämiensä tahojen toiminnasta siten kuin tunnituslain 13 § 4 momentissa säädetään.

Tunnituslaissa ei edellytetä tunnistusvälineen tai laatuvarmenteen luovuttamista hakijalle henkilökohtaisesti vaan se voidaan luovuttaa hakijan kanssa sovitulla tavalla. Hakijan henkilöllisyys ja muut hakijaan liittyvät tiedot on kuitenkin tarkistettava huolellisesti ennen kuin tunnistusväline tai laatuvarmenne luovutetaan hakijalle ensimmäisen kerran. Muilla hakijaan liittyvillä tiedoilla tarkoitetaan tässä erityisesti sellaisia tunnistusvälineelle tai laatuvarmenteelle tallennettuja tietoja, joiden luotettavuuden palveluntarjoaja takaa.

Tunnistusvälineen tai laatuvarmenteen hakija on tunnistettava myös silloin, kun hakija on alaikäinen tai muuten vajaavaltainen. Tällöin hakijan on oltava itse henkilökohtaisesti paikalla. Välineen luovuttamisen edellytyksenä voi kuitenkin olla edunvalvojan suostumus tai läsnäolo. Tässä määräyksessä ei edellytetä, että edunvalvonnan päätyttyä (esimerkiksi lapsen tullessa täysi-ikäiseksi) tunnistusvälineen tai laatuvarmenteen voimassaoloaika päättyisi, mutta tällainen käytäntö olisi suotavaa erityisesti silloin jos välineelle voidaan määrittää voimassaoloaika.

Tunnituslain 17 §:n mukaan tunnistusvälineen hakija on tunnistettava voimassa olevasta Euroopan talousalueen, Sveitsin tai San Marinon viranomaisen myöntämästä passista tai henkilökortista. Halutessaan tunnistuspalvelun tarjoaja voi käyttää ensitunnistamiseen myös Euroopan talousalueen jäsenvaltion viranomaisen 1.10.1990 jälkeen myöntämää voimassa olevaa ajokorttia tai muun valtion viranomaisen myöntämää voimassa olevaa passia. Ensitunnistamiseen hyväksyttävät asiakirjat on mainittava palveluntarjoajan tunnustusperiaatteissa.

Muiden kuin Suomen viranomaisen myöntämillä henkilökorteilla on laissa tarkoitettu vain matkustusasiakirjaksi kelpaavia henkilökortteja.

Tunnituslaissa tarkoitettuja passeja ovat kaikki tavalliset passit ja diplomaattipassit. Passien osalta ongelmia tunnistamisessa tuottanee lähinnä muukalaispassi ja pakolaisen matkustusasiakirja. Sekä muukalaispassi että pakolaisen matkustusasiakirja ovat Suomen viranomaisen myöntämiä asiakirjoja, mutta niitä ei ole tarkoitettu ensisijaisesti henkilöllisyyden toteamiseen vaan matkustusasiakirjaksi. Molemmat em. asiakirjat voidaan myöntää joko siten, että sitä hakeva henkilön henkilöllisyys pystytään toteamaan luotettavasti tai siten, että henkilöllisyyttä ei ole pystytty varmistamaan. Jos muukalaispassin tai pakolaisen matkustusasiakirjan haltijan henkilöllisyys on varmistettu, tunnistuspalvelun tarjoaja voi halutessaan käyttää asiakirjaa myös ensitunnistamiseen. Mikäli henkilöllisyyttä ei ole pystytty

luotettavasti varmistamaan, muukalaispassiin tai pakolaisen matkustusasiakirjaan tehdään tästä merkintä (henkilöllisyys varmistamaton). Mikäli muukalaispassissa tai pakolaisen matkustusasiakirjassa on merkintä siitä, ettei haltijan henkilöllisyyttä ole pystytty varmistamaan, asiakirjaa ei pitäisi käyttää myöskään tunnistuslain mukaiseen ensitunnistamiseen.

Ajokorttia käytetään tällä hetkellä varsin yleisesti henkilöllisyyden osoittamiseen, mutta sen hyväksymiseen henkilöllisyyden todentamisasiakirjana liittyy ongelmia. Ajokortin myöntöprosessi ei ole samantasoinen kuin passilla ja henkilökortilla, ja ajokorttien turvatekijät ovat vähäisiä. Erityisen ongelmallisena voidaan pitää myös ulkomailla myönnettyjen ajokorttien sekä Suomessa ulkomaalaisille vaihdettavien ajokorttien hyväksymistä henkilöllisyystodistuksena. Ulkomaalainen henkilö saa kansainvälisten tieliikennesopimusten mukaan vaihtaa ajokorttinsa suomalaiseen ajokorttiin vuoden maassa oleskelun jälkeen. Näin ollen henkilö, jonka henkilöllisyyttä ei ole voitu varmistaa ja tästä on merkintä hänen matkustusasiakirjassaan, voi vaihtaa ajokorttinsa suomalaiseen ajokorttiin ilman että tieto henkilöllisyyden epävarmuudesta tulee merkityksi ajokorttiin. Tätä vaihdettua ajokorttia voi sitten käyttää henkilöllisyyden todentamiseen. Viestintävirasto kehottaa palveluntarjoajia arvioimaan ajokorttien hyväksymisestä aiheutuvat riskit ja suhtautumaan kriittisesti sellaisiin ajokortteihin, joiden erityisehtokentässä (kenttä nro 12, koodi 70 ja maatunnus viimeisimmästä vaihtomaasta) näkyy kortin olevan vaihdettu.

Jos palveluntarjoaja ei pysty luotettavasti tunnistamaan tunnistusvälineen tai laatuvarmenteen hakijaa tai asiakirjaa, palveluntarjoaja voi ohjata hakijan poliisin tunnistettavaksi. Poliisi tunnistaa hakijan, jonka jälkeen se lähettää todistuksen hakijan henkilöllisyydestä tunnistuspalvelun tarjoajalle kirjattuna kirjeenä. Hakijalla on oltava mukanaan kaksi valokuvaa, tunnistamista mahdollisesti edesauttavat asiakirjat sekä palveluntarjoajan yhteystiedot, jonne todistus tehdystä tunnistamisesta lähetetään. Vaihtoehtoisesti tunnistusvälineen hakija voi hankkia väliaikaisen henkilökortin poliisilta.

Laatuvarmenteiden osalta lain 35 §:ssä ei ole erikseen lueteltu asiakirjoja, joista laatuvarmenteen hakijan henkilöllisyys voidaan luotettavasti tarkistaa. Luotettavina asiakirjoina voidaan pitää lain 17 §:ssä mainittuja asiakirjoja.

Tietojen tallentaminen

Tunnistuspalvelun tarjoajan on tallennettava tieto hakijan ensitunnistamisesta ja siinä käytetystä asiakirjasta sekä tunnistusvälineen käyttöön mahdollisesti liittyvistä estoista tai rajoituksista. Tietojen tallentaminen on tarpeen esimerkiksi tilanteissa joissa tunnistusväline on annettu väärälle henkilölle. Tallennettavia tietoja voivat olla esimerkiksi passin tai henkilökortin numero. Joissain tilanteissa voi olla tarpeen säilyttää valokopio käytetystä asiakirjasta. Rahanpesulain soveltamisalaan kuuluvien yritysten on otettava tietojen tallentamisessa huomioon myös rahanpesulain 10 §:ssä asetetut vaatimukset.

Mikäli tunnistusmenetelmä perustuu varmenteeseen tai kyseessä on laatuvarmenne, palveluntarjoajan on kerättävä varmenteen tietosisältöön kuuluvat tiedot. Tunnistuspalvelun tarjoajien osalta varmenteen vähimmäistietosisällöstä on säädetty tunnistuslain 19 §:ssä. Laatuvarmenteen tietosisällöstä on säädetty lain 30 §:n 2 momentissa. Tällaisia tietoja voivat olla esimerkiksi varmenteen tiettyyn käyttötarkoitukseen mahdollisesti liittyvät erityiset tiedot, kuten hakijan edustama yritys tai organisaatio sekä toimenkuva tai asema. Mikäli varmentaja ei luo avainparia, on varmentajan tarkastettava, että hakijalla on hallussaan varmennettavaa julkista avainta vastaava yksityinen avain.

Tunnistuslain 37 §:n mukaan laatuvarmenteita tarjoavan varmentajan tulee ylläpitää varmennerekisteriä myöntämistään laatuvarmenteista. Rekisteröitävät tiedot on kerättävä laatuvarmenteen hakijalta rekisteröinnin yhteydessä. Laatuvarmenteen tietosisällön lisäksi rekisteriin on merkittävä laatuvarmenteen liikkeelle laskemisen ja ylläpidon kannalta tarpeelliset hakijan henkilöön liittyvät tiedot. Tällaisia tietoja ovat

- koko nimi (sukunimi ja etunimi)
- syntymäaika ja -paikka
- henkilötunnus tai muu henkilön yksilöivä tunnus,
- muut tiedot jotka ovat tarpeen esimerkiksi henkilön erottamiseksi toisista samannimisistä henkilöistä
- osoite ja/tai muut yhteystiedot

Laatuvarmenteita tarjoavan varmentajan varmennerekisteriin on merkittävä myös tieto laatuvarmenteen hakemisajankohdasta, tehdystä ensitunnistamisesta ja siinä käytetyistä asiakirjoista sekä muut laatuvarmenteen myöntämisen kannalta olennaiset tiedot. Tällaisia tietoja voivat olla esimerkiksi laatuvarmenteen käyttöön kohdistuvat rajoitukset.

3.4 4 § Tunnistusvälineiden ja laatuvarmenteiden luonti

Asiakkaan sähköinen henkilöllisyys ja varmenteen tietosisältö perustuvat laatuvarmenteen tai tunnistusvälineen hakemuksen yhteydessä saatuihin tietoihin. Palvelun tarjoajan tulisi varmistaa hakemuksen alkuperä, luottamuksellisuus ja oikeellisuus.

Tunnistusväline ja laatuvarmenne voidaan luoda ainoastaan, jos hakemus täyttää laatuvarmenteiden tai tunnistusvälineiden myöntämisen ehdot. Tämä tarkoittaa mm. sitä, että tunnistusväline tai laatuvarmenne voidaan luoda vasta sen jälkeen, kun hakija on tunnistettu tämän määräyksen 3 §:n mukaisesti ja hakija on antanut hakemuksessa vaaditut tiedot.

Varmenteen luomisella tarkoitetaan prosessia jossa varmentaja yhdistää julkisen avaimen hakijaan ja allekirjoittaa varmenteen yksityisellä avaimellaan tehdyllä kehittyneellä sähköisellä

allekirjoituksella. Muuhun kuin varmenteeseen perustuva tunnistusvälineen luomisella tarkoitetaan tunnistusvälineen yhdistämistä hakijaan.

Palveluntarjoajan on tallennettava tiedot tunnistusvälineiden ja laatuvarmenteiden luomisesta. Jos palvelun tarjoaja luo itse avaimet on tallennettava tiedot myös avainten luomisesta. Näiden tietojen perusteella on jälkikäteen pystyttävä selvittämään tunnistusvälineen tai laatuvarmenteen luomisen ajankohta, ja miten hakija on tässä tilanteessa tunnistettu.

Palveluntarjoajan on riittävällä tavalla varmistuttava, että ainoastaan tunnistusvälineen tai laatuvarmenteen haltija voi käyttää tunnistusvälinettä tai laatuvarmennetta. Tällaisia ratkaisuja ovat esimerkiksi jokin minkä vain välineen haltija tietää (esimerkiksi PIN-koodi) tai mitä välineen haltija on (biometriset tunnisteet).

Tunnistusmenetelmässä, laatuvarmenteessa ja niiden avaimien luonnissa käytettyjen algoritmien ja avainten on oltava turvallisia ja yleisesti hyväksytyjen standardien tai suositusten mukaisia. Tällaisia standardeja on tehty muun muassa NIST:n [14], ANSI:n [15], ISO:n [16] ja VAHTI-ryhmän [17] toimesta.

3.5 5 § Varmenteiden jakelu

Määräyksen 5 §:ää sovelletaan laatuvarmenteita tarjoaviin varmentajiin sekä niihin tunnistuspalvelun tarjoajiin, joiden tunnistusmenetelmä perustuu varmenteeseen.

Palveluntarjoajan tehtävänä on luovuttaa tunnistamis- ja allekirjoituksen tekemiseen tarvittavat tiedot eli yksityinen avain ja sen suojaamiseen käytetyt tunnukset ainoastaan välineen haltijalle. Allekirjoituksen tai tunnistamisen todentamisessa käytettävän tiedon eli varmenteen ja siinä olevan julkisen avaimen jakelu on järjestettävä siten, että ne ovat kaikkien varmenteeseen ja sillä tehtyyn sähköiseen allekirjoitukseen tai tunnistamiseen luottavien osapuolten saatavilla. Palveluntarjoaja voi käyttää varmenteiden jakelukanavana esimerkiksi julkista hakemistopalvelua. Hakemistopalvelun on oltava ympärivuorokautisesti käytettävissä. Palveluntarjoaja voi myös sopia varmenteen haltijan kanssa siitä, että varmenteen haltija toimittaa varmenteen tietosisällön varmenteeseen luottavien tahojen saataville.

Palveluntarjoaja ei saa kopioida välineeseen liittyviä salaisia tietoja, koska niiden tulisi olla ainoastaan hakijan tiedossa tai käytettävissä. Tällaisia tietoja ovat esimerkiksi kortille tallennetut varmenteisiin liittyvät yksityiset avaimet.

Varmenteiden ja allekirjoituksen luomiseen tai tunnistustapahtumaan liittyvien tietojen jakelu tulisi toteuttaa siten, että:

- Yksityisiä ja salaisia avaimia ei jaeta selväkielisinä,

- Julkiset, mutta vielä varmentamattomat avaimet säilytetään turvallisesti esimerkiksi manipuloinnin estämiseksi ja
- Varmenteen haltijan kanssa sovitaan tavasta, jolla varmenteen tietosisältö toimitetaan varmenteeseen luottavien kolmansien osapuolten saataville ja tämä sopimus talletetaan.

3.6 6 § Palvelun tarjonta

Palvelun tarjontaan liittyvät asiakirjat

Palveluntarjoajan on pidettävä varmenteiden osalta varmennepolitiikka ja varmennuskäytäntö, sekä tunnistuspalvelun osalta tunnistusperiaatteet yleisesti saatavilla ja ajantasaisina. Varmennepolitiikassa kuvataan muun muassa varmentajan menettelytavat, varmenteen käyttörajoitukset sekä varmentajan ja allekirjoittajan velvollisuudet. Varmennepolitiikassa kuvataan myös tiedot, jotka varmenteeseen luottavan osapuolen on tarkistettava arvioidessaan varmenteen luotettavuutta. Varmennuskäytännössä kuvataan tarkemmin, kuinka varmennepolitiikan vaatimukset toteutetaan varmentajan toiminnassa. Tunnistusperiaatteissa kuvataan, kuinka tunnistuspalveluntarjoaja täyttää sille laissa asetetut velvollisuudet. Yleisesti saatavilla tarkoitetaan esimerkiksi niiden julkaisemista palveluntarjoajan www-sivuilla.

Ristiinvarmennuksessa osapuolien tietoturva- ja varmennepolitiikkojen, tunnistusperiaatteiden sekä tietoturva- ja varmennuskäytäntöjen on vastattava toisiaan. Tämä tarkoittaa muun muassa sitä, että vahvoja sähköisiä tunnisteita myöntävä varmennusviranomainen ei voi ristiinvarmentaa ei-vahvoja sähköisiä tunnisteita myöntävää varmennusviranomaista. Ristiinvarmennuksella tarkoitetaan sitä, että kaksi varmennusviranomaista voivat varmentaa toistensa julkiset avaimet.

Tunnistusvälineen ja laatuvarmenteen peruuttaminen ja voimassa olon tarkistaminen

Varmenteeseen ja sen avulla tehtyyn allekirjoitukseen tai tunnistamiseen luottavien tahojen on voitava tarkistaa laatuvarmenteen tai tunnistusvälineen voimassaolo sulkulistapalvelun avulla. Sulkulistapalvelu voi olla joko reaaliaikainen tai sen täytyy päivittyä säännöllisin väliajoin.

Tunnistusvälineiden ja laatuvarmenteiden peruuttaminen tulisi toteuttaa siten, että:

- Tunnistusväline suljetaan ja varmenne asetetaan sulkulistalle joko sen haltijan pyynnöstä tai, jos siihen muutoin on erityistä syytä. Perusteet tunnistusvälineen sulkemiselle muuten kuin tunnistusvälineen haltijan pyynnöstä on lueteltu vahvasta sähköisestä tunnistamisesta ja laatuvarmennetoiminnasta annetun lain 26 §:ssä.
- peruuttamis-, keskeytys- ja keskeytyksen peruutuspyyntöjen alkuperä ja oikeellisuus tarkistetaan riittävän luotettavasti ja huolellisesti. Palveluntarjoaja voi sulkea välineen myös jos sillä on epäily välineen oikeudettomasta käytöstä tai käytön turvallisuuden vaarantumisesta muutoin.
- peruutetun tunnistusvälineen ja laatuvarmenteen ottaminen uudelleen käyttöön estetään
- varmenteiden allekirjoitusavainten ja järjestelmäavainten peruuttaminen on mahdollista vain kahden henkilön valvonnassa

- tunnistusvälineiden ja laatuvarmenteiden peruuttaminen päivitetään viiveettä peruuttamishakemuksen käsittelyn jälkeen palveluntarjoajan tietokantaan.
- Jos peruutettuja varmenteita koskevat tiedot julkaistaan sulkulistan avulla, tieto varmenteen peruuttamisesta julkaistaan sulkulistalla joko välittömästi tai määritellyn säännöllisen päivityksen mukaisesti – kuitenkin viimeistään 24 tunnin kuluessa peruuttamis- tai keskeytyspyynnön saapumisesta varmentajalle
- sulkulistan päivitys julkaistaan säännöllisesti riippumatta siitä, onko siihen tullut muutoksia;
- varmentajan käyttämät luotettavat järjestelmät kykenevät peruuttamaan kaikki varmentajan myöntämät laatuvarmenteet
- palveluntarjoaja ilmoittaa tunnistusvälineen tai varmenteen peruuttamisesta tunnistusvälineen tai laatuvarmenteen haltijalle. Tunnistusvälineen peruuttamisesta tai käytön estämisestä lain 26 §:n nojalla sekä laatuvarmenteen peruuttamisesta on aina ilmoitettava tunnistusvälineen tai laatuvarmenteen haltijalle. Ilmoitus voidaan tehdä esimerkiksi SMS-viestillä, tunnistuspalveluun kirjaantumisen yhteydessä annettavalla tiedotteella ja perinteisellä kirjeellä. Ilmoittamisessa on suositeltavaa käyttää useampaa viestintäkanavaa. Jos tunnistusvälineen tai laatuvarmenteen haltija pyytää itse välineen peruuttamista, ei erillistä ilmoitusta välttämättä tarvita.
- varmentaja allekirjoittaa kaikki sulkulistat tai sulkulistavastaukset kehittyneellä sähköisellä allekirjoituksellaan ja sulkulistavastaus sisältää allekirjoitusajan (aika voi olla muodostetun sulkulistan allekirjoitusaika tai reaaliaikaisen sulkulistavastauksen aika).
- lokiin tallennetaan merkintä kaikista seuraavista tapahtumista:
 - tunnistusvälineiden ja laatuvarmenteiden tilan muutospyynnöt ja hyväksyttiinkö pyyntö vai ei
 - ylläpitoon liittymättömät sulkupalvelusta lähtevät ja sinne saapuvat viestit
 - mahdollisesti sulkulistan tarkistuspyynnöt ja vastaukset

Varmentajan allekirjoitusavaimet

Varmentajan allekirjoitusavainta käytetään ainoastaan varmenteiden ja mahdollisesti sulkulistojen ja/tai sulkulistavastausten allekirjoittamiseen.

Palveluntarjoajan on huolehdittava siitä, ettei varmentajan allekirjoitusavaimia voida ottaa uudelleen käyttöön niiden elinkaaren päätyttyä. Palveluntarjoajan avaimia käytetään vain niiden sallitun eliniän ajan ja epäsymmetristen avainten osalta varmenteiden voimassaolo tarkistetaan. Palveluntarjoajan infrastruktuuri- ja hallinta-avaimet vaihdetaan säännöllisin väliajoin (esim. vuosittain) ja avainten vaihto tapahtuu luotettavasti. Palveluntarjoajan varmenne tulisi uusia ennen sen vanhentumista.

Varmenteiden allekirjoitusavainten luomisessa ja säilyttämisessä tulisi käyttää kryptografista moduulia. Laatuvarmenteiden osalta kryptografisen moduulin on täytettävä joko FIPS 140-2 tason 3 [18] vaatimukset tai CWA 14167-3:ssa [19] asetetut Common Criterion mukaiset vaatimukset. Avainten luominen tapahtuu kahden ihmisen valvomana.

Palveluntarjonnassa tapahtuvat merkittävät tapahtumat

Palvelun tarjoajan on tallennettava tiedot kaikista palvelun tarjoamisen kannalta merkittävistä tapahtumista. Palveluntarjoajan tulisi varmistaa, että lokiin tallentuvat:

- kaikki tapahtumat, jotka liittyvät varmenteiden ja tunnistusvälineiden, myös varmentajan toiminnassaan käyttämien varmenteiden, luomiseen, keskeytystilaan asettamiseen ja peruuttamiseen
- kaikki tapahtumat, jotka liittyvät varmentajan allekirjoitusavainten hallintaan
- kaikki viestit rekisteröintipalvelusta, laatuvarmenteiden jakelupalvelusta ja lisäpalveluista vaikka ne eivät liittyisi järjestelmän hallintaan
- lokijärjestelmän käynnistys ja alasajo
- lokijärjestelmän asetusten muutos

Oikeudettoman käytön estäminen

Palveluntarjoajan on varmistettava, etteivät välineeseen liittyvät salaiset tiedot paljastu missään tilanteessa ennen kuin ne on luovutettu haltijalle. Tällaisia tietoja ovat esimerkiksi välineen käyttöä suojaava PIN-koodi. Lukkiutuneen välineen avaamisen yhteydessä palveluntarjoajan on varmistettava riittävin keinoin, että nämä tiedot eivät paljastuisi. Tällaisia keinoja voivat olla turvakuoret, raaputuspinnot tai erilliset taustajärjestelmät. Tällainen taustajärjestelmä voi olla esimerkiksi järjestelmä jossa asiakas voi palveluntarjoajan asiointipisteessä tunnistautua kertakäyttösalasanalla rajatun ajan itsepalveluportaaliin ja asettaa tunnistusvälineeseen tai laatuvarmenteeseen uudet PIN-koodit.

3.7 7 § Toiminnan lopettaminen

Tunnistuspalvelun tarjoajan on tiedotettava ilman aiheutonta viivytystä toimintansa lopettamisesta Viestintävirastolle, kaikille tunnistustoimintaan liittyville yhteistyötahoille ja apunaan käyttämille henkilöille (esimerkiksi alihankkijat) sekä tunnistusvälineen haltijoille ja tunnistuspalvelua käyttäville palveluntarjoajille. Viestintävirastolle ilmoitus on tehtävä tunnistuslain 10 §:n mukaan kirjallisesti.

Tunnistuspalvelun tarjoajan on myös minimoitava toiminnan lopettamisesta aiheutuvat haitat tunnistusvälineen haltijoille ja tunnistuspalvelua käyttäville palveluntarjoajille. Tunnistuspalvelun tarjoajan on mahdollisuuksien mukaan huolehdittava esimerkiksi tunnistustapahtumia ja tunnistusvälineitä koskevien tietojen asianmukaisesta säilyttämisestä toiminnan lopettamisen yhteydessä.

Laatuvarmenteita tarjoavan varmentajan on tiedotettava ilman aiheutonta viivytystä toimintansa lopettamisesta Viestintävirastolle, kaikille varmennetoimintaansa liittyville

yhteistyötahoille (esimerkiksi toisille varmentajille) ja apunaan käyttämille henkilöille (esimerkiksi alihankkijoille) sekä laatuvarmenteiden haltijoille. Varmentajan on myös minimoitava toiminnan lopettamisesta aiheutuvat haitat laatuvarmenteiden haltijoille ja laatuvarmenteisiin luottaville tahoille. Viestintävirastolle ilmoitus on tehtävä kirjallisesti.

Laatuvarmenteita tarjoavan varmentajan on lopetettava alihankkijoiden toiminta laatuvarmenteiden myöntämisen osalta siten, ettei uusia varmenteita myönnetä tai hakemuksia oteta vastaan toiminnan päättymisen jälkeen. Laatuvarmenteita tarjoavan varmentajan on mahdollisuuksien mukaan huolehdittava varmennerekisterin tietojen säilyttämisestä myös toiminnan lopettamisen yhteydessä. Varmentajalla tulee olla riittävät taloudelliset voimavarat tai vakuutukset tms. tietojen säilyttämisestä aiheutuvien kustannusten kattamiseksi.

Laatuvarmenteita tarjoavan varmentajan tietoturvallisuuskäytännöissä tai varmennuskäytännöissä on oltava kerrottuna varmentajan toiminta lopettamisen yhteydessä. Käytännöistä on selvittävä ainakin:

- kuinka toiminnan lopettamisesta tiedotetaan allekirjoittajille ja varmentajan yhteistyökumppaneille ja varmenteisiin luottaville tahoille
- kuinka varmentajan vastuut siirretään toisille tahoille
- kuinka käsitellään voimassaolevia laatuvarmenteita ja erityisesti niiden sulkulistatietoja.

4 VIITELUETTELO

[1] Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009), ajantasainen versio

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

[2] Information Security Management - Specification With Guidance for Use

<http://www.iso.org/iso/home.htm>

[3] Huoltovarmuuskeskus: Sopimuksiin perustuva varautuminen tietoyhteiskuntasektorilla

http://www.huoltovarmuus.fi/documents/3/SOPIVA_julkaisu.pdf

[4] ISO/IEC TR 13335-3, Information technology - Guidelines for the management of IT Security - Techniques for the management of IT Security

<http://www.iso.org/iso/home.htm>

[5] ISO/IEC 27005:2009 Information technology - Security techniques - Information security risk management

<http://www.iso.org/iso/home.htm>

[6] NIST Special Publication 800-30, Risk Management guide for Information Technology

Systems, Recommendation of the National Institute of Standards and Technology

<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

[7] Enisa: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools

http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf

[8] COSO ERM (Enterprise Risk Management - Integrated Framework (2004))

<http://www.coso.org/-ERM.htm>

[9] BS 31100:2008, Risk management. Code of practice.

<http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030191339>

[10] ISO 31000 Risk management -- Principles and guidelines

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170

[11] The Institute of Risk Management (IRM), Risk Management Standard

<http://www.theirm.org/publications/PUstandard.html>

[12] PK-RH:n pk-yrityksen riskienhallinta

www.pk-rh.fi/riskilajit/tietoriskit/tietoriskit

[13] Valtiovarainministeriö: Tietoaineistojen käsittelyn tietoturvallisuusohje

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3386/3388_fi.pdf

[14] National Institute of Standards and Technology

<http://www.nist.gov/index.html>

[15] American National Standards Institute

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

[16] International Organization for Standardization

<http://www.iso.org/iso/home.html>

[17] Valtionhallinnon tietoturvallisuuden johtoryhmä

http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/index.jsp

[18] FIPS 140 Security Requirements for Cryptographic Modules

<http://csrc.nist.gov/groups/STM/cmvp/standards.html#03>

[19] CWA 14167-3 Cryptographic module for CSP key generation services protection profile CMSKGPP
<http://www.cen.eu/esearch/>