



Määräys

TUNNISTUSPALVELUN TARJOAJIEN JA LAATUVARMENTEITA TARJOAVIEN VARMENTAJIEN TOIMINNAN LUOTETTAVUUS- JA TIETOTURVALLISUUSVAATIMUKSISTA

Annettu Helsingissä 20 päivänä lokakuuta 2010

Viestintävirasto on määrännyt 7 päivänä elokuuta 2009 vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain (617/2009) 8 §:n 3 momentin ja 42 §:n 2 momentin nojalla:

1 §

Soveltamisala

Tätä määräystä sovelletaan vahvan sähköisen tunnistuspalvelun tarjoajiin ja laatuvarmenteita tarjoaviin varmentajiin. Näistä käytetään jäljempänä yhteisnimitystä palveluntarjoaja.

2 §

Tietoturvallisuuden hallinta

Tietoturvallisuuden organisointi

Palveluntarjoajan on määriteltävä kirjallisesti tietoturvallisuuden organisointi, vastuut ja raportointisuhteet. Määrittelyt on pidettävä ajan tasalla ja niiden ajantasaisuus on tarkistettava vähintään kerran vuodessa. Tietoturvallisuuden johtotehtäviin osallistuvien henkilöiden tietoturvallisuusvastuiden on käytävä ilmi tällaisten henkilöiden toimenkuvista.

Tietoturvallisuuden ohjausasiakirjat

Palveluntarjoajalla on oltava johdon vahvistama kirjallinen näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta. Näkemys on saatettava tunnistus- tai laatuvarmennepalvelun tarjoamiseen liittyvän henkilöstön tietoon.

Lisäksi palveluntarjoajan on otettava kirjallisesti huomioon seuraavat erityisosa-alueet niiltä osin, kuin ne soveltuvat tarjottavaan palveluun:

- 1) hallinnollinen tietoturvallisuus,
- 2) henkilöstöturvallisuus,
- 3) fyysinen turvallisuus,
- 4) laitteisto- ja ohjelmistoturvallisuus,
- 5) tietoliikenneturvallisuus,
- 6) tietoaineistoturvallisuus,
- 7) käyttöturvallisuus ja
- 8) tietoturvaloukkauksiin ja väärinkäyttöihin puuttuminen.

Riskien hallinta

Palveluntarjoajan on laadittava suunnitelma palveluun liittyvien riskien arvioimiseksi. Palveluntarjoajan on tunnistettava ja arvioitava tunnistamis- ja laatuvarmennepalvelun kannalta tärkeiden toimintojen, tietojen ja järjestelmien tietoturvaloukkauksia. Palveluntarjoajalla on oltava hyväksymismenettelyt niiden merkittävien riskien osalta, joiden hallitsemiseksi ei riskien arvioinnin perusteella kohdisteta toimenpiteitä. Riskien hallinnan on oltava systemaattista, säännöllistä ja dokumentoitua.

Tietoturvatyökalut

Palveluntarjoajalla on oltava riskianalyysin tulosten pohjalta laadittu suunnitelma, jossa määritellään toimenpiteet, vastuut ja aikataulut tunnistettujen riskien hallitsemiseksi. Palveluntarjoajan on säännöllisesti seurattava toimenpiteiden soveltuvuutta niiden käyttötarkoitukseen.

Palveluntarjoajan on määriteltävä yksityiskohtaiset ja riittävät ohjeet tietoturvaloukkauksen kannalta olennaisten yksittäisten käytäntöjen osalta. Palveluntarjoajan on huolehdittava tunnistus- ja laatuvarmennepalvelun tarjoamiseen liittyvän henkilöstön koulutuksesta annettujen ohjeistuksien osalta.

Palveluntarjoajalla on oltava käytössä tarjottavan palvelun kannalta tärkeiden tietoaineistojen luokitusjärjestelmä.

Palveluntarjoajan on huolehdittava, että tietoturvaloukkauksen kannalta merkittävät tapahtumat havaitaan. Palveluntarjoajan on puututtava havaittuihin ongelmatilanteisiin.

Tietoturvallisuuden hallinnan seuranta

Määräyksen velvoitteiden toteutumista on tarkasteltava säännöllisin väliajoin ja aina tarpeen niin vaatiessa.

3 §

Hakijan ensitunnistaminen ja rekisteröinti

Tunnistuspalveluntarjoajan on tunnistettava tunnistusvälineen hakija vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 17 §:n mukaisesti. Laatuvarmenteita tarjoavan varmentajan on tunnistettava laatuvarmenteen hakija lain 35 §:n mukaisesti. Ensitunnistamisen tarkoituksena on turvata tunnistusvälineen tai laatuvarmenteen tietosisällön ja niiden avulla tapahtuvan sähköisen asiainnin oikeellisuus ja luotettavuus.

Ensitunnistaminen on tehtävä tunnistusvälineen tai laatuvarmenteen hankkimisen yhteydessä. Hakijan henkilöllisyys ja muut hakijaan liittyvät tiedot on tarkistettava huolellisesti ennen kuin tunnistusväline tai laatuvarmenne luovutetaan hakijalle ensimmäisen kerran.

Tunnistuspalvelun tarjoajan on tallennettava tiedot hakijan ensitunnistamisesta ja siinä käytetystä asiakirjasta.

Jos tunnistusmenetelmä perustuu varmenteeseen tai kyseessä on laatuvarmenne, palveluntarjoajan on kerättävä ja tallennettava varmenteen tietosisältöön kuuluvat tiedot. Mikäli varmentaja ei luo avainparia, on varmentajan tarkistettava että hakijalla on hallussaan varmennettavaa julkista avainta vastaava yksityinen avain.

Laatuvarmenteita tarjoavan varmentajan on merkittävä hakijan tiedot rekisteriin laatuvarmenteen hakemisen yhteydessä. Rekisteriin merkittäviä tietoja ovat hakijan nimi ja riittävät tiedot samanimisten henkilöiden erottamiseksi. Rekisteriin on lisäksi merkittävä tiedot ensitunnistamisesta, tarvittavat tiedot tunnistamisessa käytetyistä asiakirjoista sekä muut laatuvarmenteen myöntämisen kannalta oleelliset tiedot.

4 §

Tunnistusvälineiden ja laatuvarmenteiden luonti

Tunnistusväline tai laatuvarmenne voidaan luoda ainoastaan, mikäli tunnistusvälineen tai laatuvarmenteen hakijan hakemus täyttää laatuvarmenteiden tai tunnistusvälineiden myöntämisen ehdot. Tunnistusvälinettä tai laatuvarmennetta ei saa luoda ennen hakijan ensitunnistamista.

Palveluntarjoajan on tallennettava tieto tunnistusvälineiden ja laatuvarmenteiden luomisesta.

Palveluntarjoajan järjestelmien on tunnistusvälineitä ja laatuvarmenteita luotaessa säilytettävä tietojen luottamuksellisuus ja eheys.

Palveluntarjonnassa on riittävällä luotettavuudella varmistettava, että ainoastaan tunnistusvälineen tai laatuvarmenteen haltija voi käyttää tunnistusvälinettä tai laatuvarmennetta.

Tunnistusmenetelmässä ja laatuvarmenteessa käytettyjen algoritmien ja avainten on oltava turvallisia ja yleisesti hyväksytyjen standardien tai suositusten mukaisia.

5 §

Varmenteiden jakelu

Palveluntarjoaja ja varmenteen haltija voivat sopia varmenteen saattamisesta varmenteeseen luottavien osapuolten tietoon. Jos palveluntarjoaja julkaisee varmenteet julkisessa hakemistossa, on hakemiston oltava ympärivuorokautisesti käytettävissä.

Palveluntarjoaja ei saa kopioida varmenteeseen liittyviä salaisia tietoja, koska niiden tulisi olla ainoastaan hakijan tiedossa tai käytettävissä.

6 §

Palvelun tarjonta**Palvelun tarjontaan liittyvät asiakirjat**

Palveluntarjoajan on pidettävä varmenteiden osalta varmennepolitiikka ja varmennuskäytäntö, sekä tunnistuspalvelun osalta tunnistusperiaatteet yleisesti saatavilla ja ajantasaisina.

Ristiinvarmennuksessa osapuolien tietoturva- ja varmennepolitiikan, tunnistusperiaatteiden sekä tietoturva- ja varmennuskäytäntöjen on vastattava toisiaan.

Tunnistusvälineen ja laatuvarmenteen peruuttaminen ja voimassaolon tarkistaminen

Palveluntarjoajan on käsiteltävä tunnistus- ja allekirjoitusvälineiden peruuttamispyynnöt viipymättä ja siten, että kaikki pyynnöt tunnistetaan ja käsitellään riittävällä tarkkuudella.

Palveluntarjoajan on tallennettava tieto tunnistus- tai allekirjoitusvälineen asettamisesta keskeytystilaan, ottamisesta takaisin käyttöön keskeytystilasta sekä välineen peruuttamisesta. Tämän tiedon on oltava palveluun luottavan tahon käytettävissä viipymättä peruuttamiseen tai keskeyttämiseen johtavan perusteen tultua palveluntarjoajan tietoon.

Palveluntarjoajan on kyettävä peruuttamaan kaikki tunnistus- ja allekirjoitusvälineet. Palveluntarjoajan on ilmoitettava peruuttamisesta tunnistus- ja allekirjoitusvälineen haltijalle.

Varmenteeseen luottavalla taholla on oltava mahdollisuus tarkistaa varmenteen tila sulkulistapalvelun avulla. Sulkulistapalvelu voi olla reaaliaikainen tai säännöllisin väliajoin päivitettävä. Palveluntarjoajan on allekirjoitettava sulkulista ja sulkulistavastaukset. Allekirjoitettuun sulkulistaan tai sulkulistavastaukseen on sisällytettävä tieto listan julkaisemisen tai vastauksen ajankohdasta.

Varmentajan allekirjoitusavaimet

Palveluntarjoajan on huolehdittava siitä, ettei varmenteiden luomisessa käytettyjä yksityisiä allekirjoitusavaimia voida ottaa uudelleen käyttöön niiden elinkaaren päätyttyä.

Palveluntarjoajan on varmistuttava siitä että kaikki varmenteiden luonnissa ja allekirjoittamisessa käytetyt yksityiset ja salaiset avaimet säilytetään turvallisesti ja niiden varastointi ja varmuuskopiointi tapahtuu turvallisessa ympäristössä ja vain valtuutettujen henkilöiden toimesta.

Palveluntarjonnassa tapahtuvat merkittävät tapahtumat

Palveluntarjoajan on tallennettava tiedot kaikista palvelun tarjoamisen kannalta merkittävistä tapahtumista.

Oikeudettoman käytön estäminen

Palveluntarjoajan on suojattava tunnistusväline ja laatuvarmenne oikeudettomalta käytöltä.

Palveluntarjoajan on varmistettava, etteivät laatuvarmenteeseen tai tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.

7 §

Toiminnan lopettaminen

Tunnistuspalvelun tarjoajan on tiedotettava toimintansa lopettamisesta Viestintävirastolle, tunnistustoiminnassa apunaan käyttämilleen henkilöille, tunnistusvälineiden haltijoille, tunnistuspalvelua käyttäville palveluntarjoajille sekä muille tunnistustoimintaan liittyville yhteistyötahoille. Tunnistuspalvelun tarjoajan on myös huolehdittava siitä, että sen toiminnan lopettamisesta aiheutuvat haitat tunnistusvälineiden haltijoille ja tunnistuspalvelua käyttäville palveluntarjoajille ovat mahdollisimman vähäiset.

Laatuvarmenteita tarjoavan varmentajan on tiedotettava toimintansa lopettamisesta Viestintävirastolle, varmennetoiminnassaan apunaan käyttämilleen henkilöille, laatuvarmenteiden haltijoille sekä varmennetoimintaansa liittyville yhteistyötahoille. Varmentajan on myös huolehdittava siitä, että sen toiminnan lopettamisesta aiheutuvat haitat laatuvarmenteiden haltijoille ja laatuvarmenteisiin luottaville tahoille ovat mahdollisimman vähäiset.

8 §

Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 20 päivänä lokakuuta 2010 ja on voimassa toistaiseksi. Määräyksellä kumotaan 27 päivänä elokuuta 2009 annettu määräys 8 B/2009 M tunnistamispalvelun tarjoajien ja yleisölle laatuvarmenteita tarjoavien varmentajien luotettavuus- ja tietoturvallisuusvaatimuksista.

9 §

Tiedonsaanti ja julkaiseminen

Tämä määräys on julkaistu Viestintäviraston määräyskokoelmassa ja se on saatavissa Viestintäviraston asiakaspalvelusta:

Käyntiosoite	Itämerenkatu 3 A, HELSINKI
Postiosoite	PL 313, 00181 HELSINKI
Puhelin	09 6966 500
Telekopio	09 6966 410
WWW-sivusto	http://www.ficora.fi/
Y-tunnus	0709019-2

Helsingissä 20 päivänä lokakuuta 2010

Pääjohtajan sijainen Jorma Koivunmaa

Johtaja Timo Lehtimäki