12.12.2018

Dnro:
1003/620/2018

Viestintäviraston neuvontaa tunnistuspalveluiden vaatimustenmukaisuuden arvioinnista v. 2019

1 Tausta

1.1 Tämän tulkintamuistion luonne

Viestintävirasto on koonnut tähän muistioon neuvontaa tunnistuspalveluiden arviointivaatimusten soveltamiseen liittyvistä kysymyksistä. Neuvonta on laadittu yleisellä tasolla. Viestintävirasto valvoo oma-aloitteisesti kaikkien tunnistuspalvelun arviointia koskevien vaatimusten täyttämistä kohtien 2.1. ja 2.2. linjausten mukaisesti.

Viestintävirasto voi täydentää tätä muistiota tarvittaessa.

Tunnistuspalvelun tarjoajan vastuulla on huolehtia tunnistuspalvelun tietoturvallisuuden hallinnasta ja huomioida asianmukaisesti omaan palveluunsa liittyvät riskit ja uhkat. Jos Viestintävirasto joutuu tekemään palveluntarjoajakohtaisia valvontapäätöksiä, niissä huomioidaan tapauskohtaiset tosiseikat ja säädetyt vaatimukset.

1.2 Säännökset

Tunnistus- ja luottamuspalvelulain 29 §:ssä säädetään vahvan sähköisen tunnistuspalvelun tarjoajan velvollisuudesta teettää määräajoin palvelulleen 28 §:ssä mainitun arviointielimen arviointi siitä, täyttääkö tunnistuspalvelu tässä laissa säädetyt yhteentoimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset. Auditoinnin tarkoituksena on arvioida sitä, miten tunnistamispalvelu ja yrityksen toiminta vastaa sille asetettuja vaatimuksia.

Viestintäviraston oikeudesta antaa tarkempia määräyksiä tunnistuspalvelun vaatimustenmukaisuuden arvioinnissa käytettävistä arviointiperusteista säädetään 42 §:ssä.

Viestintäviraston määräyksen 72A/2018 M 15 §:ssä tarkennetaan vaatimusalueet, joiden täytyy sisältyä riippumattomaan arviointiin. Määräyksen 16 §:ssä tarkennetaan vaatimusalueet, joista tunnistuspalveluntarjoaja voi esittää oman selvityksen.

Tunnistuspalvelun tarkastuskertomus on voimassa tunnistuslain 31 §:n mukaan voimassa arvioinnissa käytetyn standardin määrittelemän ajan, kuitenkin enintään 2 vuotta.

Tunnistuslain mainitut säännökset tulivat voimaan 1.7.2016 ja lain siirtymäsäännöksen mukaan tarkastuskertomus tuli toimittaa Viestintävirastolle viimeistään 31 päivänä tammikuuta 2017.

Tunnistuslain 10 §:n mukaan tunnistuspalvelun aloitusilmoituksessa on oltava vaatimustenmukaisuuden arviointilaitoksen, muun ulkoisen arviointi-

laitoksen taikka sisäisen tarkastuslaitoksen laatima tarkastuskertomus riippumattomasta arvioinnista 29 §:n mukaisesti ja ilmoitetuissa tiedoissa tapahtuneista muutoksista on ilmoitettava viipymättä kirjallisesti Viestintävirastolle.

Viestintävirasto on laatinut ohjeet 211/2016 arvioinnin mallikriteeristöstä ja 215/2016 tarkastuskertomuksesta. Ohjeiden päivitys- ja täydennystyö on käynnistetty 28.11.2018.

1.3 Tammikuussa 2017 toimitettujen tarkastuskertomusten käsittely

Viestintävirasto sai määräaikaan mennessä tammikuussa 2017 tarkastuskertomukset kaikilta vahvan sähköisen tunnistuspalvelun tarjoajilta, jotka olivat tunnistuslain 12 §:n mukaisessa jo rekisterissä ennen lain muutosten voimaan tuloa.

Kaikkiin tarkastuskertomuksiin on pyydetty täydennyksiä, osaan kaksi kertaa.

Lisäksi osa tunnistuspalvelun tarjoajista on toimittanut ilmoituksia muutoksista ja toimittanut niihin liittyviä tarkastuskertomuksia.

Viestintävirasto teki heinäkuussa 2017 ensimmäisen väliarvion kaikista tarkastuskertomuksista siltä osin, että huolimatta joistain puutteista tiedoissa tai toteutuksissa, lähes kaikkien vahvan sähköisen tunnistuksen palveluiden varmuustaso merkittiin lain 12 §:n mukaiseen rekisteriin. Väestörekisterikeskuksen tunnistusvarmenteista rekisteriin merkittiin kansalais- ja organisaatiovarmenne ja muiden osalta käsittely on kesken.

1.4 Muina ajankohtina tehdyt ilmoitukset ja toimitetut tarkastuskertomukset

Edellisessä kohdassa mainittujen lisäksi Viestintävirastoon on tullut ilmoituksia ja tarkastuskertomuksia uusilta tunnistuspalvelun tarjoajilta. Nämä tarkastuskertomukset on kaikilta olennaisilta osin vaadittu täydennettäväksi ennen kuin tunnistuspalvelu on merkitty rekisteriin.

2 Kysymykset ja Viestintävirasto neuvot ja linjaukset

2.1 Milloin tammikuussa 2017 tarkastuskertomuksen toimittaneiden tunnistuspalveluntarjoajien täytyy toimittaa uusi tarkastuskertomus

Lain mukaan tarkastuskertomus on voimassa enintään kaksi vuotta. Ohjeessa 215/2016 Viestintävirasto on ohjeistanut, että tarkastuskertomus on toimitettava viimeistään kahden vuoden kuluttua edellisen tarkastuskertomuksen hyväksymisestä.

Koska tarkastuskertomuksiin on jouduttu pyytämään täydennyksiä ja niiden arviointi on Viestintävirastolla edelleen kesken, ajankohta, josta kaksi vuotta lasketaan, on tulkinnanvarainen.

Viestintävirasto on todennut tunnistuspalvelun tarjoajille ennakkotietona selvittävänsä kahta tulkintavaihtoehtoa siitä, milloin tarkastuskertomus voidaan katsoa hyväksytyksi:

- Ennestään rekisterissä olleen tunnistuspalvelun varmuustason rekisteröinti (joka tehtiin siis vanhoilla palveluilla pääsääntöisesti heinäkuussa 2017) tai
- ajankohta, jolloin yksittäiseltä tunnistuspalvelun tarjoajalta on saatu tarkastuskertomukseen kaikki tarvittavat täydennykset.

Aikaisin mahdollinen ajankohta olisi siis heinäkuu 2019 ja myöhäisemmät palveluntarjoajakohtaisesti pääsääntöisesti vuoden 2020 puolella, koska vireillä on edelleen paljon täydennyspyyntöjä. Viestintävirasto **ei** siis katso, että uudet tarkastuskertomukset olisi toimitettava tammikuussa 2019 eli kahden vuoden kuluessa laissa säädetystä ensimmäisen tarkastuskertomuksen toimittamisen määräajasta.

Viestintävirasto ottaa tulkinnassa huomioon lain ja sen perustelujen lisäksi sen, että arviointien käsittely Viestintävirastossa on viivästynyt ja että arvioinnin ohjeistusta ollaan päivittämässä 2018–2019. Uusien arviointien tekemistä tukeva ohjeistus ei siten ole kaikilta osin käytettävissä vielä alkuvuonna 2019. Edelleen Viestintävirasto huomioi sen, että käsittelyruuhkan vuoksi tunnistuspalvelun tarjoajat eivät ole pystyneet itse täysin vaikuttamaan siihen, milloin Viestintävirasto saa valmiiksi arvionsa vaatimustenmukaisuuden tarkastuskertomuksen riittävyydestä.

Viestintävirasto kiinnittää huomiota siihen, että kun tammikuussa 2017 toimitetut arvioinnit on monelta osin tehty loppuvuonna 2016, tietoturvallisuuden uhkat ja riskit ovat muuttuneet eikä uutta arviointia ole syytä viivyttää tarpeettomasti.

Viestintävirasto toteaa neuvontana seuraavaa:

- Kaikille määritellään tasapuolisesti sama aikataulu, jossa Viestintävirasto valvoo tarkastuskertomusten toimittamista.
- Ellei arviointien tekemistä tai hankintaa ole vielä käynnistetty, se tulisi käynnistää vuoden 2019 alkupuolella heti, kun tunnistuspalvelulla on riittävät tiedot arvioinnin vaatimuksista. (Ks. tarkemmin seuraava kohta).
- Tarkastuskertomukset täytyy toimittaa viipymättä, kun ne valmistuvat.
- Tarkastuskertomukset täytyy viimeistään toimittaa vuoden 2019 loppuun mennessä.

2.2 Milloin vuonna 2017 tai myöhemmin rekisteriin merkittyjen tunnistuspalveluntarjoajien täytyy toimittaa uusi tarkastuskertomus

Uusi tarkastuskertomus täytyy toimittaa kahden vuoden kuluessa siitä, kun uusi tunnistuspalveluntarjoaja on merkitty tunnistuslain 12 §:n mukaiseen Viestintäviraston rekisteriin.

2.3 Miten kattava kahden vuoden välien tehtävän uusinta-arvioinnin on oltava

Viestintävirasto toteaa neuvontana seuraavaa:

1. Ennestään rekisterissä olevan tunnistuspalvelun toimintaa ei tarvitse arvioida kokonaisuudessaan uudelleen

2. Arvioinnissa on huomioitava ne seikat, joiden osalta Viestintävirasto on pyytänyt yritys/yhteisökohtaisesti täydennyksiä tai todennut täydennyspyynnöissä, että jatkossa arvioinnin tai tarkastuskertomuksen täytyy olla tarkempi tai kattavampi.

3. Arvioinnissa on huomioitava muutokset, mikäli niistä ei ole jo toimitettu Viestintävirastolle muutosilmoitusta ja tarkastuskertomusta

4. Tietoturvallisuuden hallinnan osalta riittää, että arvioidaan se, että tunnistuspalvelun vaatimukset (TunnL, eIDAS LOA-asetus ja Viestintäviraston määräys) on huomioitu hallintajärjestelmässä.

5. Häiriönhallinnan arvioinnissa on huomioitava tunnistuspalvelun kyky ja valmius havainnoida häiriöitä ja raportoida ne tarvittaessa. Viestintävirasto saa verraten vähän häiriöilmoituksia ja pitää tarpeellisena kiinnittää huomiota tunnistuspalveluiden häiriönhallintaan.

6. Tarkastuskertomukseen täytyy liittää tunnistusjärjestelmän kokonaisarkkitehtuurista kuva, kaavio tai muu selkeä esitys. Arkkitehtuuriselvityksen ja tarkastuskertomuksen perusteella on voitava varmistua siitä, että kaikki relevantit järjestelmän turvallisuuteen vaikuttavat tekijät on huomioitu arvioinnissa ja että järjestelmän arkkitehtuuri on turvallinen.

    - Järjestelmän arkkitehtuurikuvauksessa tulee olla nähtävillä tunnistamiseen liittyvät järjestelmäkomponentit.

    - Selvityksen perusteella täytyy pystyä hahmottamaan tunnistusjärjestelmän osat ja niiden toimittajat, osien väliset yhteydet/yhdyskäytävät, yhteyksien suojauskäytännöt, järjestelmän osien väliset rajapinnat ja muut seikat.

    - Arkkitehtuurikuvauksesta täytyy käydä ilmi koko tunnistusjärjestelmän komponenttien toiminnalliset suhteet kokonaisuudessaan, mm. tietovarantojen eriyttäminen, esityskerroksen ja liiketoimintalogiikan eriyttäminen, yhdyskäytävät/ympäristöjen väliset kytkennät ja näiden suojaus sekä ulkoisten toimijoiden väliset turvallisuuskontrollit.

    - Kuvauksesta pitäisi selvitä verkkotopologia, L3-tason komponentit kuten palomuurit, palvelimet ja yhteenkytkennät muihin ympäristöihin sekä hallintayhteydet, mikäli ne on eriytetty.

    - Lisäksi tulisi kuvata tunnistusprosessiin liittyvät tietovuot.

    - Jos järjestelmä käyttää hyväkseen pilvipalveluiden tuotteistettuja komponentteja tai tuotteita (Amazon Web Services, Google, Microsoft Azure jne.), tulee tuotekomponentit nimetä ja sisällyttää nämä ulkoiset komponentit alihankkijoihin kohdistuvan arvioinnin piiriin.

7. Jos käytössä on mobiilitunnistussovellus, täytyy se arvioida kaikilta niiltä osin, joilla on vaikutusta tunnistamisen vaatimustenmukaisuuteen. Jos sovellukseen on yhdistetty myös muita toimintoja, näitä muita toimintoja ei tarvitse sisällyttää arviointiin siltä osin, kun ne eivät voi vaikuttaa tunnistamisen luotettavuuteen.

8. M72A 7 §:n arvioinnista tulee toimittaa tarkastuskertomuksen lisäksi skannausraportti, josta näkyvät tunnistusjärjestelmän ulospäin tarjotun rajapinnan TLS- ja salausprofiilit.

9. Alihankkijoiden vaatimustenmukaisuus täytyy arvioida kaikilta edellä mainituilta osin.

10. Tunnistusvälineen myöntämismenettelyiden (ensitunnistaminen, luominen, toimittaminen) vaatimustenmukaisuutta ei tarvitse auditoida uudelleen muutoin kuin muutosten osalta.

    - Jos sähköinen ensitunnistaminen on otettu käyttöön, sen käytöstä on syytä arvioida se, että ensitunnistamistapahtumat tallennetaan tunnistuslain 24 §:n mukaisesti ja että tiedot ovat käytettävissä tunnistuslain 16 §:n mukaisesti.

    - Mobiilisovellusten osalta ks. kohta 7.

2.4 Muutosten ilmoittaminen ja arviointi

Toiminnan olennaisissa muutostilanteissa arviointi täytyy tehdä ja muutosta koskeva muutosilmoitus sekä tarkastuskertomus toimittaa ennen muutoksen tuotantoon viemistä.

Olennaisia muutoksia ovat aina esimerkiksi

- tunnistusmenetelmän eli todentamistekijöiden ja todentamismekanismin muutokset,

- tunnistusjärjestelmän tekniset muutokset eli ylläpito- ja tuotantojärjestelmän rakenteen, ohjelmistojen tai

- ylläpitoa, laitteita, järjestelmiä tai ohjelmistoja toimittavien alihankkijoiden muutokset tai vaihtuminen

Viestintävirastolta on kysytty, onko Tupas-rajapinnan korvaaminen SAML- tai OIDC-rajapinnalla arvioitava.

- Vuoden 2019 aikana pois jäävää rajapintatoteutusta ei tarvitse arvioida (Tupas tai muu).

- Uusi toteutus on arvioitava salausvaatimusten ja salausavainten hallinnoinnin osalta. Asiointipalvelut eivät kuulu arvioinnin piiriin, mutta niiltä edellytetyt tai niille tarjotut salausavainten hallinnointikäytännöt kuuluvat.

- Jos protokollan vaihtoon liittyy rajapinnan konfiguroinnin lisäksi muita olennaisia muutoksia tunnistusjärjestelmässä tai sen arkkitehtuurin, muutokset täytyy arvioida.