Neuvontamuistio 2021 määräaikaisarviointeja varten

1 Yleistä

Vuoden 2021 määräaikaisarvioinnin tilaamisessa/tekemisessä Liikenne- ja viestintävirasto nostaa tämän muiston avulla eri teemoja esille. Teemat ovat edellisissä määräaikaisarvioissa toistuvia puutteita, tai arviointiprosessin parannusehdotuksia. Neuvonnan tarkoituksena on vähentää tarvetta tarkentaville täydennyspyynnöille ja nopeuttaa arvioinnin käsittelyä sekä tunnistuspalvelun tarjoajalla että virastossa.

Neuvontamuistio voidaan jakaa kahteen osaan

- Erityishuomiota vaativat kokonaisuudet, joiden raportoinnissa on ollut puutteita edellisten määräaikaisarviointien kohdalla
- Raportointiin liittyvä vapaaehtoinen vakiomuotoinen excel-taulukko, jonka tavoitteena on varmistaa arvioinnin ja itse raportin kattavuus ja toisaalta nopeuttaa käsittelyä

2 Säädökset

Tunnistus- ja luottamuspalvelulain (617/2009) 29 §:ssä säädetään vahvan sähköisen tunnistuspalvelun tarjoajan velvollisuudesta teettää määräajoin palvelulleen 28 §:ssä mainitun arviointielimen arviointi siitä, täyttääkö tunnistus-palvelu tunnistus- ja luottamuspalvelulaissa säädetyt yhteentoimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset. Auditoinnin tarkoituksena on arvioida sitä, miten tunnistamispalvelu ja yrityksen toiminta vastaa sille asetettuja vaatimuksia.

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

Liikenne- ja viestintäviraston oikeudesta antaa tarkempia määräyksiä tunnistuspalvelun vaatimustenmukaisuuden arvioinnissa käytettävistä arviointiperusteista säädetään 42 §:ssä.

Tunnistus- ja luottamuspalvelulaissa sekä siinä viitatuilla osin Euroopan unionin komission täytäntöönpanoasetuksessa (EU) 2015/1502 (varmuustasoasetus) ja sen liitteessä säädetään tunnistuspalvelulle asetetuista edellytyksistä.

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.

Liikenne- ja viestintäviraston Ohje 211/2019 O 'Sähköisen tunnistuspalvelun arviointiohje' sisältää tunnistuspalvelujen auditoinnin tueksi laaditun yleisen arviointikriteeristön sekä mobiilitunnistusratkaisun erityiskriteeristön. Tunnistuspalveluntarjoajat voivat käyttää mainittuja kriteeristöjä taikka jotakin toista määräyksen M72 15 §:n vaatimukset täyttävää kriteeristöä tai kriteeristöjen yhdistelmää.

3 Aikataulu

Määräaika toimittaa tarkastuskertomukset liitteineen Liikenne- ja viestintävirastolle on 31.12.2021. Kaikille ennen vuotta 2021 tunnistuspalvelutoimintansa aloittaneille toimijoille on vuonna 2021 sama määräaika.

Määräaikaisarvioinnin saa toimittaa virastolle myös aikaisemmin, eikä se vaikuta seuraavan arviointikierroksen aikatauluun.

Virasto arvioi ja tiedottaa tarvittaessa erikseen määräaikaisarvioinnin aikatauluvaatimukset mahdollisille uusille rekisteröitäville tunnistuspalveluille.

4 Viraston valvontalinjaus ChaCha20+Poly1305 -salausratkaisusta

Viraston määräykseen 72A/2018 M valmistellaan muutosta, jonka on tarkoitus tulla voimaan alkuvuonna 2022. Voimassa olevan määräyksen 7 §:n mukaan symmetrisessä salauksessa käytettävän salausalgoritmin on oltava AES tai Serpent. Tiivistefunktion on oltava SHA-2, SHA-3 tai Whirlpool.

Tunnistuspalveluiden vaatimuksenmukaisuuden määräaikaisarvioinneissa ja määräysvalmistelussa on tullut ilmi, että voimassa olevassa määräyksessä lueteltujen algoritmien ja tiivistefunktioiden lisäksi yleisessä käytössä on myös uudempia riittävän turvallisia vaihtoehtoja. Määräykseen valmistellaan muutosta, jolla tullaan sallimaan myös ChaCha20-salausalgoritmi sekä Poly1305-autentikaatiokoodi.

Liikenne- ja viestintävirasto ei puutu tunnistuspalveluiden salausvaatimusten vaatimustenmukaisuuden valvonnassa ChaCha20-algoritmin ja Poly1305-autentikaatiokoodin käyttöön eikä vaadi niiden käyttöä lopetettavaksi.

5 Määräaikaisarvioinnin erityishuomiota vaativat kohteet

5.1 Tunnistusmenetelmän kuvaus

Tarkastuskertomuksen on liitettävä kuvaus ja/tai dokumentaatio tunnistusmenetelmästä ja todentamismekanismista. Kuvausten täytyy olla teknisesti niin tarkkoja, että niiden perusteella pystyy päättelemään, että kaikki vaatimusten kannalta relevantit asiat on huomioitu arvioinnissa. Kuvausten täytyy kattaa alihankkijat.

- Mitkä ovat menetelmässä käytetyt todentamistekijät (vähintään kaksi eri luokista)

- Miten niiden riippumattomuus toisistaan on varmistettu

- Miten todentamistekijät on kytketty tunnistusvälineen haltijaan

- Todentamismekanismi eli tekninen kuvaus tunnistustapahtumien toteuttamisesta

Lisäksi tarkastuskertomuksesta täytyy ilmetä tuote- tai palvelunimet, joilla käyttäjät ja asiointipalvelut tunnistavat, mistä palvelusta on kysymys. Myös tunnistuspalvelun sisäisesti käyttämät nimitykset on hyvä kertoa, jos ne esiintyvät tarkastuskertomuksessa tai tunnistuspalvelun dokumentaatiossa.

5.2 Alihankinta

Viraston määräyksen M72 15 §:ssä määrätään tunnistuspalvelun arviointikriteerit. Arvioinnin tulee kattaa tunnistuspalvelu kokonaisuudessaan.

Tunnistuspalvelun tarjoajan on siten arvioitava myös koko alihankintaketju ja sen vaatimustenmukaisuus. Kaikki alihankkijat on tunnistettava ja arvioitava alihankkijan rooli tunnistusjärjestelmän toteutuksessa.

Alihankintaorganisaation oma, esim. ISO 27001, sertifiointi voidaan ottaa huomioon, mutta arvioitaessa on kiinnitettävä huomiota sertifiointien kattavuudesta ja

soveltuvuudesta niihin toimintoihin, jotka osallistuvat tunnistusjärjestelmän toteuttamiseen. Pelkkä sertifiointien hyväksi lukeminen ei yleensä kata kaikkia osioita, joten tunnistuspalvelun tarjoajalla on velvollisuus huolehtia alihankintaverkoston vaatimustenmukaisuuden arvioinnista osana määräaikaisarviointeja.

Toiminnan olennaisissa muutostilanteissa täytyy tehdä arviointi ja toimittaa muutosta koskeva muutosilmoitus sekä tarkastuskertomus ennen muutoksen tuotantoon viemistä. Olennaisia muutoksia ovat myös ylläpitoa, laitteita, järjestelmiä tai ohjelmistoja toimittavien alihankkijoiden muutokset tai vaihtuminen.

5.3 Arkkitehtuurikuvaukset

Virastolle on pääsääntöisesti toimitettu vuoden 2019 määräaikaisarviointien yhteydessä kattavat arkkitehtuurikuvaukset.

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. Kuvausten täytyy kattaa alihankkijat.

- 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.

5.4 Tekninen havainnointi

Arviointiohjeen kohdassa 2.5.2 käsitellään arviointimenetelmiä, joita voi arvioinnissa käyttää. Dokumentoinnin tarkastuksen, haastattelujen ja paikalla tehtyjen havaintojen lisäksi tulee määräaikaisarvioinnissa toimittaa myös teknisen havainnoinnin raportit liitteenä.

5.5 Mobiilitunnistussovellusten SDK:t

Useat mobiilitunnistussovellukset on toteutettu ostamalla markkinoilta tunnistuksen toteuttava SDK, joka on liitetty isompaan kokonaisuuteen (esim. pankkisovellus), tai integroitu tunnistusvälineen tarjoajan omaan tunnistussovellukseen. SDK

on olennainen osa tunnistusmenetelmää, ja myös itse SDK tulee arvioida. Arvioinnin voi toteuttaa käyttäen viraston julkaisemaa mobiilitunnistussovelluksen arviointikriteeristöä, mutta myös valmistajan itse toimittama, kolmannen osapuolen arviointiraportti voi toimia vaatimustenmukaisuuden osoituksena. Tällöin tulee kuitenkin liittää mukaan tieto käytetystä arviointitavasta ja arvioinnin tehneestä organisaatiosta ja arvioidusta versiosta (ja onko arvioitu versio sama mikä on käytössä tunnistussovelluksessa).

6 Virastolle raportointi ja excel-pohja

Virasto on luonut arviointia varten valinnaisen mallin raportointitaulukosta. Määräaikaisarviointien sujuvuuden kannalta olisi suotavaa, että kyseistä taulukkoa käytettäisiin vuoden 2021 määräaikaisarvointien yhteydessä. Valinnaista taulukkoa käyttämällä tunnistuspalvelun tarjoaja voi myös helpommin kilpailuttaa arviointeja ja toisaalta varmistua, että kaikki tarvittavat osat tulee arvioitua. Taulukko perustuu viraston arviointikriteeristöihin viraston ohjeessa 211/2019 O.

Virasto muistuttaa vielä, että mitä kattavammat arviointiraportit ja liitteet virastolle toimitetaan, sitä paremmin saadaan määräaikaisarvioinnin tarkastus tehtyä. Mikäli arviointiraportissa on havaittu puutteita, tulisi tunnistuspalvelun tarjoajan toimittaa näihin puutteisiin kattavat selvitykset suunnitelluista korjaustoimenpiteistä ja niiden aikataulusta.