28.11.2018

Dnro:
1003/620/2018

Jakelun mukaan

Viite: Viestintäviraston vahvan sähköisen tunnistamisen vaatimustenmukaisuuden arvioinnin ohjeiden päivitys (mallikriteeristö 211/2016 O ja tarkastuskertomusohje 215/2016 O)

Viestintäviraston kutsu ohjeiden päivitystyöryhmään ja päivityssuunnitelma

Päivitettävät ohjeet

Viestintävirasto päivittää seuraavat ohjeet

- 211/2016 O Ohje tunnistuspalveluntarjoajan auditoinnin mallikriteeristö
- 215/2016 Ohje tunnistus- ja luottamuspalveluiden arviointikertomukset

Ohjeet koskevat vahvan sähköisen tunnistamisen välineiden tarjoajia ja välityspalveluita.

Ohjeessa 211 on standardien pohjalta laadittu esimerkkikriteeristö vahvan sähköisen tunnistamisen palvelun vaatimustenmukaisuuden arvioinnille. Malli perustuu ISO/IEC 27001 -standardiin ja muun kuin tietoturvallisuuden hallinnan osalta ja ETSI EN 319 411-1 -standardiin. Ohjeen tarkoitus on selkeyttää toimijoille, mitä palveluun liittyvien vaatimustenmukaisuuden arviointien tulisi kattaa.

Ohjeen esimerkkikriteeristön noudattaminen ei ole pakollista, mutta se on yksi tapa osoittaa Viestintäviraston määräyksen 72A/2018 M[1] 15 §:ssä täsmennettyjen vaatimusten täyttäminen.

Ohje 215 on tarkoitettu tunnistuspalveluiden vaatimuksenmukaisuuden arviointia tekeville arviointielimille ja vaatimustenmukaisuuden arviointilaitoksille, jotka tarkastavat hyväksytyn

[1] Viestintäviraston määräys sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 72A/2018 M.

luottamuspalvelun tarjoajan ja hyväksytyn luottamuspalvelun vaatimustenmukaisuuden. Ohjeen tarkoituksena on kuvata arvioinnin lopputuloksena annettavien kertomusten vähimmäissisältöä ja esittämistapaa.

Tavoitteet

Päivityksen tavoitteena on tarkentaa ja korjata ohjeita niiden havaintojen perusteella, joita tunnistuspalvelun tarjoajat, auditointeja tekevät tahot ja Viestintävirasto ovat havainneet, kun tunnistuslaissa edellytettyjä arviointeja ja tarkastuskertomuksia on ensimmäisen kerran tehty.

Mallikriteeristön kattavuudessa ja säädettyjen vaatimusten esille tuomisessa mallikriteeristössä on havaittu puutteita. Lisäksi on todettu, että kriteeristö ei riittävästi kata mobiilisovellusten arviointiin liittyviä erityiskysymyksiä.

Tarkastuskertomusohjetta voidaan tarkentaa kokemusten perusteella.

Tavoitteena on päivittää ja ajantasaistaa ohjeet niin, että ne tukevat paremmin arviointien hankkimista ja että myös uusia tunnistusmenetelmiä markkinoille tuovat tahot voivat käyttää niitä.

Mallikriteeristössä pyritään huomioimaan yhteensopivuus maksupalvelusääntelyn (PSD2) vahvaa tunnistamista koskevien vaatimusten kanssa. Direktiivin vaatimuksia asiakkaan vahvasta tunnistamisesta täydennetään komission delegoidulla asetuksella (EU) 2018/389 (nk. tekninen sääntelystandardi RTS SCA & CSC). Finanssivalvonta on luvannut seurata työtä ja osallistua siihen mahdollisuuksiensa mukaan.

Viestintävirasto on selvittänyt EU:n eIDAS-yhteistyöryhmissä, onko muualla käytössä mobiilisovelluksiin soveltuvia kriteeristöjä. Tällaisia ei ole löytynyt, ja Viestintävirasto vie kansallisen työn tuloksia tiedoksi muille jäsenvaltioille.

Päivitystyön organisointi

Viestintävirasto kutsuu päivitystyöhön työryhmän, joka on avoin kaikille. Muutoksia ohjeisiin valmistellaan virkatyönä ja työryhmän jäsenet voivat tehdä muutosehdotuksia. Ehdotuksia ja kommentteja käsitellään ja niitä voi esittää sekä kirjallisesti että työryhmän kokouksissa.

Ensimmäinen kokous järjestetään 14.12.2018 klo 12-16 Viestintävirastossa.

Ensimmäisessä kokouksessa käsitellään päivitystarpeita yleisesti, työn tarkempaa organisointia sekä Viestintäviraston ensimmäistä luonnosta mobiilisovellusten arviointikriteereistä (LIITE).

Mobiilisovellusten arviointi tunnistusvälineenä

Erilaisia menetelmiä ja teknologioita, joilla voidaan toteuttaa käyttäjän tunnistaminen, syntyy jatkuvasti uusia. Pankkien myöntämät paperiset tai muoviset tunnuslukulistat, varmenteen sisältävä henkilökortti ja mobiilivarmenne ovat saaneet rinnalleen nykyaikaisia mobiilisovelluksia, jotka käyttävät hyödykseen itse mobiilialustan tarjoamia teknologioita toteuttaessaan käyttäjän sähköiseen tunnistukseen vaadittavia toimenpiteitä. Arvioinnin kohde (ToE, Target of Evaluation) olisi erityisesti tunnistusvälineeksi laskettava mobiilisovellus tai sovelluksen osa, joka toteuttaa käyttäjän sähköistä tunnistusta.

Tunnuslukulistojen turvallisuustaso on ollut varsin helppoa todentaa. Kortti/sirupohjaisille ratkaisuille, johon myös mobiilivarmenne kuuluu, on ollut jo pidemmän aikaa Euroopan laajuiset selkeät käytännöt miten kyseisten ratkaisujen turvataso on voitu todentaa ja sertifioida käyttämällä Protection Profile -dokumentteja. Mobiilisovelluksille vastaavanlaisia keinoja todeta tunnistusmenetelmän tai -välineen turvatasoa ei ole tällä hetkellä.

Useimmat kotimaiset sähköiset tunnistusmenetelmät ja tunnistusvälityspalvelut ovat varmuustasolla *korotettu*. Tunnistuslaissa (617/2009), sitä tarkentavassa Viestintäviraston määräyksessä 72 ja EU:n komission täytäntöönpanoasetuksessa 2015/1502 säädetään vaatimukset mm. tunnistusmenetelmälle, prosesseille ja todentamismekanismille.

Uusien tunnistusmenetelmien tulee täyttää säädetyt vaatimukset, mutta vaatimusten soveltamisessa ja arvioinnissa on ongelmana sellaisen yhtenäisen auditointikriteeristön puuttuminen, jonka avulla voitaisiin varmistua markkinoille tuotavien uusien mobiililaitteisiin ja -käyttöjärjestelmiin perustuvien sovellusten vaatimustenmukaisuudesta.

Pyyntö ilmoittaa osallistumisesta työryhmään ja 14.12. tilaisuuteen sekä pyyntö toimittaa kommentteja

Viestintävirasto pyytää kaikkia ohjeiden päivitykseen osallistumisesta kiinnostuneita organisaatioita ilmoittamaan osallistujansa työryhmään. Työryhmään voi osallistua myös pelkästään seuraamalla työryhmälle perustettavaa sähköpostilistaa. Kokouksiin voi osallistua tarpeen mukaan, ja organisaatio voi lähettää kokoukseen myös muita asiantuntijoita.

Osallistujat (henkilön nimi, yritys/yhteisö, sähköposti) pyydetään ilmoittamaan osoitteeseen eidas@ficora.fi viimeistään 4.12.2018. Samalla pyydetään ilmoittamaan 14.12.2018 tilaisuuteen osallistujat.

Myös kommentteja muutostarpeista voi mielellään toimittaa etukäteen.

Lisätietoja antaa erityisasiantuntija Petteri Ihalainen puh. 0295 390 302, eidas@viestintavirasto.fi.

Jarkko Saarimäki
johtaja

Petteri Ihalainen
erityisasiantuntija

Liitteet Valmisteluluonnos v28.11.2018 suositus 211/2019 S

Jakelu Luottamusverkoston yhteistoimintaryhmä
eIDAS-työryhmä
Viestintäviraston tiedossa olevat vaatimustenmukaisuuden arvioijat
Poliisihallitus
Viestintäviraston tiedossa olevat mobiilitunnistussovellusten kehittäjät
muut kiinnostuneet toimijat (kutsu julkaistaan verkkosivuilla)