Gurulogic Microsystems Oy

Lausunto

22.07.2025

Asia: VN/10855/2024

Luonnos hallituksen esityksestä eduskunnalle sähköisestä tunnistamisesta, luottamuspalveluista ja eurooppalaisesta digitaalisesta identiteetistä annettua EU:n asetusta täydentäväksi lainsäädännöksi

Lausunnonantajan lausunto

Huomiot rajat ylittävän sähköisen tunnistamisen, sähköisten luottamuspalvelujen ja eurooppalaisen digitaalisen identiteetin kansallisesta sääntelystä:

Kansallisen liikkumavaran hyödyntäminen muutosasetuksessa:

Kannatamme lainsäädännön mahdollistaman kansallisen liikkumavaran käyttöä erityisesti lompakon avoimen lähdekoodin vaatimuksen rajoittamiseksi, muutosasetuksen artiklan 5a, kohdan 3 mukaisesti. Kansallisen turvallisuuden ja kriittisen infrastruktuurin suojaamiseksi on tärkeää rajata avoimen lähdekoodin vaatimuksen ulkopuolelle taustajärjestelmien ydinturvallisuuskomponentit, joiden lähdekoodin luovuttaminen avoimesti voisi muodostaa riskin kansalliselle turvallisuudelle ja avata hyökkäysvektoreita kriittisiin tunnistusjärjestelmiin. Tarvittaessa lähdekoodin tarkastaminen tulee voida mahdollistaa viranomaisten toimesta suljetussa ympäristössä ilman vaatimusta lähdekoodin yleisestä julkaisemisesta.

Kansalliset kyberturvallisuuden sertifiointijärjestelmät:

Koska muutosasetuksen 5 c artiklan mukaisia eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä ei vielä ole olemassa, pidämme perusteltuna esityksen linjausta kansallisten sertifiointijärjestelmien luomisesta ja soveltamisesta kunnes eurooppalaisia kyberturvallisuussertifiointijärjestelmiä on käytössä. Järjestelmän tulisi mahdollistaa erilaisten teknisten arviointi- ja validointimenetelmien hyödyntäminen tilanteen ja kohteen mukaan – mukaan lukien formaali verifiointi, manuaalinen auditointi, penetraatiotestaus sekä standardiperusteinen vaatimustenmukaisuustarkastus (esimerkiksi ISO/IEC 15408 / Common Criteria).

Erityisesti suosittelemme, että kansallinen sertifiointimalli tunnustaisi formaalin verifioinnin, kuten ProverIf:n, roolin korkeatasoisen kyberturvallisuuden arvioinnissa. Vaikka formaalit verifiointimenetelmät eivät yksin kata koko arviointikenttää, ne muodostavat perustan protokollatason tietoturvaominaisuuksien todentamiselle ja protokollien validoinnille jo suunnitteluvaiheessa, millä voidaan ehkäistä kalliita virheitä tuotannossa ja auditoinneissa. Näillä työkaluilla voidaan matemaattisesti todistaa keskeisiä ominaisuuksia, kuten viestien ja avainten luottamuksellisuus ja eteenpäin-luottamuksellisuus (”forward-secrecy”). Formaali malli on täsmällinen – ei tulkinnanvarainen – tapa arvioida turvallisuutta, jolloin vertailtavuus paranee. Ilman formaalia analyysiä ja sen tarjoamia standardoituja malleja arviointiprosessit voivat jäädä liiaksi yksittäisten arvioijien näkemyksiin perustuviksi, mikä vaikeuttaa sertifiointien toistettavuutta ja heikentää uskottavuutta.

Useat eurooppalaiset kyberturvaviranomaiset kuten ANSSI (Ranska) ja BSI (Saksa) ovat edistäneet formaalien menetelmien käyttöä Common Criteria -arvioinneissa ja julkaisseet ohjeistuksia kehittäjille ja arvioijille. Siten formaalin verifioinnin huomioiminen myös Suomen kansallisessa sertifiointimallissa tukisi eurooppalaista linjaa sekä kansallisten ratkaisujen teknologista kilpailukykyä osana eurooppalaista luottamusverkostoa.

Toivomme, että kansallinen malli toimii linjassa eurooppalaisen kehityksen kanssa ja mahdollistaa formaalisti validoitujen teknologioiden hyödyntämisen korkean varmuustason kyberturvallisuusratkaisujen arvioinnissa.

Rajat ylittävä henkilöllisyyden linkittäminen:

Esitämme muutosasetuksen 11 a artiklassa säädettyyn rajat ylittävään henkilöllisyyden linkittämiseen ratkaisuksi holvimallia, jossa jäsenvaltioiden kansalaistensa attribuuttitodistukset sisältämät holvit on linkitetty EU-tason kattoholviin. Ko. mallissa EU-holvissa ei ole tarvetta säilöä jäsenvaltioiden kansallisia attribuuttitodistuksia – ainoastaan linkitystodistuksia, jotka on allekirjoitettu kansallisen holvin toimesta ja tallennettu EU-holviin, ja joita käyttäen EU-holvi pystyy luotettavasti todentamaan henkilöllisyyden. Malli on hajautettu ja helposti skaalautuva – uusia jäsenvaltioita voidaan lisätä ilman että tietueita tarvitsee muuttaa.

Sähköisen attribuuttitodistuksen tarkistaminen:

Esitämme muutosasetuksen 45 e artiklan mukaiseen sähköisten attribuuttitodistusten tarkastamiseen ratkaisuksi kyseisen attribuuttitodistuksen ensisijaisesti säilöneen holvipalvelun/luottamuspalveluntarjoajan sähköistä allekirjoitusta kullekin attribuuttitodistukselle. Käytännössä attribuuttitodistuksen eheyden ja muuttumattomuuden tarkastaminen toteutetaan lähteen digitaalisen allekirjoituksen tarkistamisella.

Kansallisen sääntelyn lainsäädännöllisestä toteutuksesta:

Lainsäätäjä on tehnyt oikean päätöksen sääntelyn selkeyttämiseksi, sijoittamalla kansalliset vahvan sähköisen tunnistamisen vaatimukset ja eIDAS-asetukseen liittyvän täydentyvän sääntelyn omiksi laeikseen.

Lainsäätäjä on myös huomioinut hyvin muun asiaan liittyvän lainsäädännön vaatimukset, ehdottamalla kansallista lisäsääntelyä lompakon käyttöönoton vähimmäisiästä vastaamaan tietosuojalaissa säädettyä tietoyhteiskunnan palvelujen tarjoamiseen sovellettavaa 13 vuoden ikärajaa. Koska tällaisissa palveluissa voidaan edellyttää vahvaa tunnistautumista, on asianmukaista mahdollistaa se myös digitaalisen identiteettilompakon avulla.

Huomiot koskien digitaalista henkilöllisyystodistusta:

Digitaalinen henkilötodistus tuo tietoturvallisesti toteutettuna parannuksen osalta nykytilanteeseen, jossa vain yhden attribuutin/tiedon, esim. iän, todistamisessa palveluntarjoajalle pitää näyttää kaikki todistukseen sisältyvät henkilötiedot. Digitaalinen ratkaisu toteuttaa GDPR:n mukaisen tiedon minimoinnin periaatteen nykyjärjestelmää paremmin. Lisäksi suostumus henkilötietojen käsittelyyn on selkeämmin todennettavissa, kun henkilö itse luovuttaa lompakkosovelluksestaan vain ne tiedot mitä kulloinenkin asiointitilanne vaatii.

Kadonnut henkilökortti mahdollistaa väärissä käsissä identiteettivarkauden ja väärinkäyttötilanteita mutta digitaalinen todistus, kun se aukeaa vain henkilön omalla esim. biometrisellä tunnisteella, pitää henkilötiedot turvassa. Digitaalinen henkilötodistus on myös nykypäivää sillä erityisesti nuoret käyttävät asioinnissa, esim. maksamisessa, yhä enemmän vain ja ainoastaan matkapuhelinta.

Olemme esityksen kanssa samaa mieltä siitä, että digitaalinen henkilötodistus tulee ehdottomasti toteuttaa osana eurooppalaista digitaalista identiteettilompakkoa. Kuten muistiossakin todettiin, ei ole järkevää kehittää kahta erillistä sovellusta, kun henkilötodistus voidaan toteuttaa sähköisenä attribuuttitodistuksena. Kuten muistiossakin todetaan, digitaalisen henkilöllisyystodistuksen eli perustavaa laatua olevan sähköisen attribuuttitodistuksen integrointi lompakkoon todennäköisesti edistää lompakon laajempaa käyttöä.

Huomiot kansallisen vahvan sähköisen tunnistamisen turvallisuutta parantavista muutoksista:

Kannatamme muutoksia, jotka nostavat myös kansallisesti käytettävien tunnistusvälineiden turvallisuusvaatimukset samalle tasolle kuin rajat ylittävässä tunnistusvälineen käytössä.

Huomiot koskien kansallista ekosysteemikuvausta:

Kuvaus kansallisesta ekosysteemistä antaa hyvän ja käytännönläheisen kuvan lompakoista, niiden käyttötarkoituksista ja niiden ympärille syntyvistä rooleista ja vastuista. On selvää, että ydinhenkilöllisyys ja henkilön tunnistetietojen liikeellelasku nähdään ekosysteemirooliksi, joka kuuluu valtionhallinnon vastuulle. Sertifioituja lompakkoratkaisuja puolestaan voisivat tarjota sekä yksityisen että julkisen sektorin toimijat. Kuvaus ekosysteemistä jää kuitenkin torsoksi, sillä se ei sisällä mitään lompakkoasioinnin yhteensopivuuden varmistavasta infrastruktuuriroolista, joka on ekosysteemin keskiössä mahdollistamassa digitaalisen identiteetin käytön esimerkiksi kuntatason, yksityissektorin ja ulkomaisten tunnistuspalvelujen välillä ilman tarvetta keskitettyyn identiteettirekisteriin, kuten esitimme henkilöllisyyden linkittämisen ratkaisussamme.

Lummevuo Anne-Mari
Gurulogic Microsystems Oy