Finanssiala ry

Lausunto

27.08.2025

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:

Finanssiala ry (FA) kannattaa lähtökohtaisesti komission pyrkimystä edistää entistä paremmin jäsenvaltioiden rajat ylittävää sähköistä asiointia ja liiketoimintaa. Pääministeri Orpon hallitusohjelmasta löytyy myös kirjaus siitä, että kansallista lisäsääntelyä tulisi välttää. HE-luonnoksessa on nähdäksemme onnistuttu tämän kansallisen tavoitteen osalta varsin hyvin.

Kansallisesti täytäntöönpantava uudistettu ja voimassa oleva eIDAS-asetus antaa vain raamit eurooppalaisen digitaalisen identiteetin lompakon (EUDI-lompakko) käyttöönotolle. Komissiolle on annettu toimivaltaa säätää lompakon yksityiskohtaisemmista vaatimuksista täytäntöönpanoasetuksien muodossa. Koska nämä eivät kuulu eduskunnan toimivaltaan, FA ei tässä yhteydessä lausu niistä.

FA haluaa tuoda esiin muutaman huomion kansallisen liikkumavaran ja avoimen lähdekoodin määrittelyn osalta. FA:n mielestä nykytilanteessa on epäselvää, onko avoin lähdekoodi määritelty jonkun tietyn lisenssin tai lisenssiperheen perusteella vai onko määritelty ne ominaisuudet, jotka lisenssin tulee täyttää. Lisäksi tulisi määrittää, mikä taho nämä lisenssit hyväksyy. Nykytilanne on epäselvä molempien em. seikkojen osalta. Avoin lähdekoodi ilman lisenssiä ei ole avointa, mutta se voi kuitenkin olla auditoitavaa. Suljettujen komponenttien käytön osalta on myös hyvä huomioida, että suljetut komponentit mobiililaitteen puolella ovat tärkeitä huijauksien estämiseksi (kloonaus, väliintulohyökkäys, varastaminen yms.).

Yhteiset komponentit eli lompakon ydintoiminnot, jotka ovat kaikkien käytettävissä, eivät saa olla siten lisensoituja, että se estää lisäämästä ohjelmistoon avoimen lähdekoodin lisenssein tai

toimittajan omin lisenssein lisensoituja ohjelmiston osia. Tämä tarkoittaa myös sitä, että kaikkien käytettävissä olevien ydintoimintojen on oltava lisensoitu tietyin avoimen lähdekoodien lisenssein, jotka sallivat mahdollisimman laajan yhteensopivuuden muiden avoimen lähdekoodin lisenssien ja toimittajalisenssien suhteen. Näin ollen yhteisesti käytettävissä olevien komponenttien tulisi olla lisensoitu mahdollisimman sallivin avoimen lähdekoodin lisenssein (esim. MIT). Tässä yhteydessä tulisi välttää lisenssien epäyhteensopivuuden ja toimijoiden lisensointiin liittyvän sekä sovellusteknisen valintamahdollisuuden turvaamiseksi vastavuoroisuutta edellyttävien lisenssien käyttämistä (esim. GPL-3.0). Jos toimija haluaa lisätä omien lisenssien alaista (suljettua) lähdekoodia, niin loppukäyttäjän etua voitaisiin valvoa järjestämällä ohjelmistolle auditointi. Näiltä osin käytetty kansallinen liikkumavara on kannatettavaa.

Huomiot koskien digitaalista henkilöllisyystodistusta:

FA on jo vuosien ajan suhtautunut myönteisesti valtion tuottamaan digitaaliseen henkilöllisyystodistukseen. Toivomme, että kansalaiset ottavat todistuksen laajasti käyttöönsä.

FA haluaa muistuttaa siitä, että digitaalisen henkilöllisyystodistuksen aitouden tarkistaminen tulee käytännössä edellyttämään QR-koodilukulaitteita asiointipisteissä (pankkikonttorit, kaupan kassat, virastojen palvelupisteet jne.). Näiden hankkiminen ja asentaminen tulee viemään kaikilta osapuolilta aikaa. Lisäksi on tärkeää huomioida, että QR-koodeja on hyödynnetty kasvavissa määrin esimerkiksi pankkitunnusten kalastelussa ja muissa väärinkäytöksissä. Näin ollen QR-koodien ja koodilukulaitteiden osalta on hyvä kiinnittää huomiota asioinnin turvallisuuteen ja selkeyteen, jotta asiakkaat ymmärtävät, miten uusia välineitä käytetään turvallisesti ja oikein.

EUDI-lompakon ja lompakossa asuvan digitaalisen henkilöllisyystodistuksen käyttöotolle on ratkaisevan tärkeää valtion kansalaisille tarjoama asiakastuki, johon tulee varata riittävät resurssit.

Huomiot kansallisen vahvan sähköisen tunnistamisen turvallisuutta parantavista muutoksista:

Turvallisuutta voi ja pitää aina parantaa. Turvallisuutta parantavissa muutoksissa on myös hyvä huomioida esimerkiksi palveluiden kitkaton käytettävyys ja muutosten kustannushyötysuhde. FA:n huomioita:

7 b §. Tieto passin tai henkilökortin voimassaolosta:

Tunnistusvälineen tarjoajan on varmistettava, että tunnistusväline ei ole käytettävissä ennen kuin asiakirjan voimassaolo on varmistettu. Tämä asettaa todella tiukan vaatimuksen käyttää poliisin tarjoamaa rajapintaa voimassaolon tarkistamiseksi. FA:n jäsenpankeilta saadun tiedon mukaan poliisin tarjoaman rajapinnan toimivuudessa esiintyy jonkin verran häiriöitä eli tulee ns. vääriä vastauksia (muuta kuin kyllä tai ei), mikä on aiheuttanut hankaluuksia asiakaspalvelutilanteissa. Näitä tilanteita varten säännöksestä olisi hyvä löytyä jonkinlainen varajärjestely esimerkiksi niin, että tunnistusvälineen myöntäjä voisi muilla keinoin varmistaa asiakirjan voimassaolon ja sen, että asiakirja on oikean henkilön hallussa.

18 a §. Tunnistusvälineen käytön kieltäminen ensitunnistamisessa:

Tunnistusvälineen tarjoajan on mahdollistettava se, että tunnistusvälineen haltija voi kieltää tunnistusvälineen käytön ensitunnistamiseen haettaessa vahvaa sähköistä tunnistusvälinettä. Tämä muutos vaatisi tunnistusvälineen tarjoajilta järjestelmämuutoksia ja muutoksia luottamusverkoston rajapintoihin. Tiedon kiellosta pitäisi siis käytännössä kulkea mukana ketjutuspyynnön tapahtumassa. Kielto voisi teoriassa parantaa turvallisuutta, mutta pelkona on se, että tätä toiminallisuutta ei käytännössä tultaisi juurikaan hyödyntämään käyttäjien keskuudessa eli vain pieni osa käyttäjiä asettaisi kiellon. Näin ollen muutoksesta saatava hyöty olisi pieni verrattuna aiheutuviin implementointi- ja operointikustannuksiin. FA katsoo, että tämä muutos vaatisi ensin laajempaa keskustelua luottamusverkoston yhteistoimintaryhmän toimijoiden keskuudessa.

Kiellon sijasta tunnistusvälineen ketjuttamisen turvallisuutta parantava keino saattaisi löytyä ottamalla mallia maksupalvelulainsäädännöstä. PSD2:seen liittyvä komission delegoitu asetus (EU) 2018/389 on käytännössä toteutettu hyödyntämällä kahta toisistaan erillään olevaa turvallista sähköistä viestintäkanavaa. Huomioitavaa on myös EU neuvoston tämänhetkinen ehdotus tulossa olevaan Payment Services Regulation (PSR)-sääntelyyn (art. 51:5): ”Where the payment service provider offers the payment service user the possibility to initiate or give consent to payment transactions by means of a mobile application, the payment service provider shall require strong customer authentication and the use of different communication channels to activate the mobile application on a new device, if done remotely.”. Tunnistusvälineiden ketjuttamisen turvallisuuden parantamiseksi voitaisiin siis asettaa vaatimus uuden tunnistusvälineen aktivoinnin lisävarmistukselle.

Muut HE-luonnoksen ehdotukset ovat sellaisenaan kannatettavia. FA haluaa vielä muistuttaa riittävien siirtymäaikojen tärkeydestä. Kokemuksesta voimme todeta, että ne useimmiten alimitoitetaan.

Huomiot koskien kansallista ekosysteemikuvausta:

FA:lla ei ole huomioitavaa. Kuvaus vastaa VM:n ja DVV:n lukuisten infotilaisuuksien ja webinaarien tilannekatsauksia. Kiitoksia niistä.

Jansson Peter
Finanssiala ry