TietoEVRY

Lausunto

29.08.2025

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:

eIDAS-luottamusarkkitehtuurin lisäksi tarvitaan ekosysteemikohtaisia luottamusrekistereitä

Uudistetun eIDAS-asetuksen kansallinen toimeenpano ei vielä muodosta sellaista luottamuskehystä, joka varmistaisi, että esimerkiksi ylemmän korkeakoulututkintotodisteen myöntäjä on taho, jolla on oikeus myöntää kyseisiä todisteita tai että terveystietojen esittämistä pyytävä luottava osapuoli on varmasti terveydenhuollon toimija.

Asetuksen mukaisen eIDAS-luottamuskehyksen lisäksi tarvitaan täydentäviä kovia ja pehmeitä luottamusinfrastruktuureja, jotka vastaavat eri toimialojen ja liiketoimintaverkostojen yksilöllisiin tarpeisiin ja ne voivat toimia kansallisen ja EU-tasoisen kehyksen rinnalla eIDAS-yhteentoimivuutta täydentäen. Tällaisia täydentäviä luottamusinfrastruktuureja ei ole tarpeen säädellä osana lausuttavana olevaa lakipakettia. Täydentävät luottamusinfrastruktuurit voivat nojata merkittävältä osin sopimusoikeuteen ja toimijoiden keskenään sopimiin sääntöihin, kunhan lainsäädäntö jättää selkeän mahdollisuuden tämänkaltaisten ratkaisujen hyödyntämiselle.

Digitaalinen identiteetti tulee tarjota kaikille organisaatioille

Hallituksen esityksessä todetaan olevan “ilmeistä, ettei [oikeushenkilön] tunnistetietoja voitaisi aluksi tarjota kuin keskeisille oikeushenkilömuodoille, kuten osakeyhtiölle.” Esityksestä ei käy ilmi, miksi oikeushenkilömuotoja koskeva rajoite on ilmeinen.

Uudistetun eIDAS-asetuksen tarkoituksena on tarjota digitaalinen identiteetti (luotettavalla tavalla esitettävät yksilöivät tunnistetiedot) ihmisille ja organisaatioille. Organisaatioiden pakolliset yksilöivät tunnistetiedot ovat nimi ja yksilöivä tunniste. Suomessa rekisteröidyillä organisaatioilla on yksilöivä tunniste Patentti- ja rekisterihallituksen ja Verohallinnon yhteisessä Yritys- ja yhteisötietojärjestelmässä (YTJ).

Huomautamme, että oikeushenkilön tunnistetietojen ensisijaiseksi tietolähteeksi on valittu Kaupparekisteri YTJ:n sijaan, jolloin esimerkiksi toiminimellä toimiva yrittäjä ei voi saada yritykselleen organisaation tunnistetietoja. Käsityksemme mukaan asetuksen tavoitteen “to enable and facilitate the exercise by natural and legal persons of the right to participate in digital society safely” kirjaimellinen tulkinta sulkee pois yksityiset elinkeinonharjoittajat, jotka eivät ole oikeushenkilöitä.

Näkemyksemme mukaan olisi asetuksen hengen mukaista myöntää yrityksen tunnistetiedot kaikille yrityksille, joilla on Y-tunnus.

Hallituksen esityksessä tulisi arvioida, minkälaiset vaikutukset esitetyllä lailla on yhdistysten, kuntien, asunto-osakeyhtiöiden, oppilaitosten, toiminimien ja muiden vastaavien organisaatioiden. mahdollisuuksiin osallistua digitaaliseen yhteiskuntaan. Mikäli oikeushenkilön yksilöivät tunnistetiedot voidaan myöntää vain keskeisille oikeushenkilömuodoille, tulisi kuvata, miten muut organisaatiot voivat hyödyntää digitaalisia palveluja.

Henkilöllisyyden linkityspalvelun jatkokehittämistä ei tule rajoittaa

Esityksessä ehdotetaan, että henkilöllisyyden linkittämisen toteuttaisi Suomessa Digi- ja väestötietovirasto.

Esityksen mukaan linkittämisessä ei olisi kyse uusien henkilöiden rekisteröimisestä, vaan “henkilöllisyyden linkittäminen edellyttäisi olemassa olevaa rekisteri-identiteettiä Suomessa”. Täytäntöönpanoasetuksen 2025/846 4 artiklan 4. momentti sanoo: “Jos luottava osapuoli tai keskitetty järjestelmä määrittää – –, että käyttäjää ei ole aiemmin rekisteröity, luottava osapuoli tai keskitetty järjestelmä voi pitää kyseistä käyttäjää uutena käyttäjänä ja tarvittaessa rekisteröidä käyttäjän kansallisten lakien tai hallinnollisten käytäntöjen mukaisesti.”

Esityksessä todetaan, että “velvollisuutta henkilöllisyyden linkittämisen varmistamiseen ei ole niissä tilanteissa, joissa asioidaan yksityisen sektorin palveluissa”. Täytäntöönpanoasetus 2025/846 ja eIDAS-asetus antavat mahdollisuuden tarjota henkilöllisyyden linkityspalvelua myös luottaville osapuolille, jotka eivät ole julkisen sektorin organisaatioita.

Koska henkilöllisyyden linkittämisen osalta on päädytty toteuttamaan vain minimivaatimukset täyttävä järjestelmä, on ilmeistä, että uudistettu eIDAS-asetus ei Suomessa korjaa rajat ylittävän tunnistamisen nykyisiä puutteita. Esityksen mukainen ratkaisu johtaa siihen, että asiointipalvelujen on pyydettävä ja tallennettava käyttäjiltä suuri määrä yksilöiviä tietoja, joita ne eivät tarvitse muuhun käyttötarkoitukseen kuin henkilön tunnistamiseen. Täten eri asiointipalveluihin muodostuu rinnakkaisia rekisteri-identiteettejä mikä vaikeuttaa eri asiointipalveluiden yhteentoimivuutta.

Ehdotetun lain 14 § ei sisällä rajauksia siihen, mille tahoille linkityspalvelua voidaan tarjota tai siihen, voisiko se sisältää myös uusien identiteettien muodostamisen. Vaikka järjestelmän toteutuksessa lähdettäisiinkin liikkeelle minimitoteutuksella, hallituksen esitys tulisi kirjata sellaiseen muotoon, joka ei estä järjestelmän jatkokehittämistä ja tarjoamista laajemmalle käyttäjäkunnalle jatkossa. Lisäksi linkityspalvelun käytännön toteutuksen tulee tukea sekä julkisen että yksityisen sektorin käyttötapauksia ja tarjota koneellisesti integroitavat rajapinnat, jotta palvelu voidaan skaalata laajaan käyttöön.

Luottavien osapuolten rekisteröintiä tulisi selkeyttää

Eurooppalaisten digitaalisen identiteetin lompakoiden laaja käyttöönotto nojaa siihen, että lompakkoa hyödyntäviä palveluja on laajalti tarjolla. Lompakkoon luottavien osapuolten sääntelyyn liittyy vielä paljon epävarmuutta. Tällä hetkellä on vielä epäselvää kuinka helppoa ja automaattista luottavaksi osapuoleksi rekisteröityminen on tai millä edellytyksillä rekisteröityminen voitaisiin perua. Luottavan osapuolen pääsy- tai rekisteröintivarmenteen peruminen tulee vaikuttamaan merkittävästi luottavan osapuolen kykyyn tarjota digitaalisia palveluita. Näkemyksemme mukaan epäselvät keskeytys- ja peruutusehdot nostavat merkittävästi luottavien osapuolten kynnystä rekisteröityä.

Ehdotetun lain 13 §:ssä mainitaan, että Liikenne- ja viestintävirasto ylläpitää Suomessa eIDAS-asetuksen 5 b artiklassa tarkoitettua eurooppalaisen digitaalisen identiteetin lompakon luottavien osapuolten rekisteriä. Lain 35 §:ssä luetellaan Liikenne- ja viestintävirastolle maksettavia maksuja. Näissä maksuissa mainitaan hyväksytyn luottamispalvelun tarjoajan, vaatimustenmukaisuuden arviointilaitoksen ja sertifiointielimen suorittamista maksuista, mutta ei luottavan osapuolen rekisteröinnistä suoritettavaa maksua. Onko digitaalisen identiteetin lompakon luottavaksi osapuoleksi rekisteröityminen maksutonta vai voiko Liikenne- ja viestintävirasto periä rekisteröinnistä maksun?

Viraston tulisi järjestää rekisteröinti- ja ylläpitoprosessi itsepalveluperiaatteella sekä tarjottava sitä varten ihmis- ja koneluettavat rajapinnat. Viraston tulisi julkaista rekisteröinnin edellytykset, tarkastusrytmi sekä keskeytys- ja peruuttamisperusteet, samoin kuin mahdolliset maksut ja niiden määräytymisperusteet.

Luottavan osapuolen määritelmää olisi hyvä tarkentaa

Uudistetun eIDAS-asetuksen 3 artiklan kohdassa 16 mainitaan, että esimerkiksi “sähköisten attribuuttitodistusten myöntäminen” on asetuksen mukainen “luottamuspalvelu”.

Digitaalisen todisteiden myöntämiseen, hallintaan ja vastaanottamiseen on jo tarjolla runsaasti ratkaisuja, jotka toteuttavat samoja teknisiä määrityksiä kuin eurooppalaiset digitaalisen identiteetin lompakot ja niihin liittyvät sähköiset attribuuttitodistukset. Suurella osalla näiden ratkaisujen tarjoajista ja käyttäjistä ei todennäköisesti ole aikomusta rekisteröityä eurooppalaisen digitaalisen identiteetin lompakon tarjoajaksi tai luottavaksi osapuoleksi.

Kansallisessa lainsäädännössä olisi hyvä tarkentaa, että digitaalisten todisteiden myöntäjistä ja luottavista osapuolista tulee asetuksen tarkoittamia luottamuspalvelun tarjoajia vasta, kun ne rekisteröityvät eurooppalaisen digitaalisen identiteetin lompakon luottaviksi osapuoliksi eIDAS-asetuksen 5 b artiklan mukaisesti. Uudistetun eIDAS-asetuksen 19 artiklan ja ehdotetun lain 37 §:n tulisi koskea vain eIDAS-asetuksen 5 b artiklan mukaisesti rekisteröityneitä luottavia osapuolia.

Avoimen lähdekoodin kirjaus tulisi kirjata ymmärrettävään muotoon

8 §:n kirjaus “Eurooppalaisen digitaalisen identiteetin lompakon tarjoaja ei kuitenkaan saa luovuttaa lompakon lähdekoodia komponenteista, joita ei ole asennettu käyttäjän laitteeseen, jos sille on olemassa asianmukaisesti perusteltu syy.” pitäisi varmaankin olla kirjoitettu muotoon “Eurooppalaisen digitaalisen identiteetin lompakon tarjoaja ei kuitenkaan ole velvoitettu

luovuttamaan lompakon lähdekoodia komponenteista, joita ei ole asennettu käyttäjän laitteeseen, jos siihen on olemassa asianmukaisesti perusteltu syy.” Ehdotetun kirjauksen nykyinen muoto voi johtaa tulkintaan, jonka mukaan avoimen lähdekoodin ohjelmistoja tarjoavat yritykset rikkovat lakia julkaistessaan ohjelmistonsa lähdekoodin, vaikka tarkoituksena on ainoastaan mahdollistaa perusteltu rajoitus taustakomponenttien lähdekoodin luovuttamisen osalta. Tavoitteena tulee olla avoimen lähdekoodin hyödyntämisen mahdollistaminen vaarantamatta tietoturvaa.

Huomiot koskien digitaalista henkilöllisyystodistusta:

Biometristen tietojen käyttö jää epäselväksi

Lausuttavana olevan dokumentin sivulla 96 kerrotaan digitaaliseen henkilöllisyystodistukseen liittyvän käyttäjän kasvokuvan käytöstä:

”Käyttäjän tunnistaminen tapahtuisi luottavan osapuolen silmämääräisen arvion perusteella vastaavalla tavalla kuin perinteisten henkilöllisyystodistusten passin ja henkilökortin osalta. Tunnistamisessa ei käytettäisi teknisiä menetelmiä, vaan se perustuisi aina luonnollisen henkilön aistinvaraisesti tekemien havaintojen pohjalta tekemään punnintaan. Digitaalinen henkilöllisyystodistus ei mahdollistaisi erityisten teknisten menetelmien käyttöä henkilön tunnistamisessa. Digitaalista henkilöllisyystodistusta koskevassa ehdotuksessa valokuvien käsittelyn ei siten katsota olevan tietosuoja-asetuksen 9 artiklassa tarkoitettua biometristen tietojen käsittelyä henkilön yksiselitteistä tunnistamista varten.”

Jos esimerkiksi ravintola tai kauppa toteuttaa järjestelmän, joka pyytää henkilön lompakosta digitaalisena henkilöllisyystodistuksena käytettävästä sähköisestä attribuuttitodistuksesta henkilön nimeä, ikää ja kasvokuvaa, ja vertaa kasvokuvaa käyttäjästä otettavaan kuvaan, eikö tällaista järjestelmää pidettäisi biometristen tietojen käsittelynä henkilön yksiselitteistä tunnistamista varten?

Hallituksen esityksestä ei käy ilmi, miten erityisten teknisten menetelmien käyttö henkilön tunnistamisessa käytännössä estettäisiin. Ehdotamme, että sääntelyssä todetaan nimenomaisesti, että digitaalisen henkilöllisyystodistuksen yhteydessä esitettävää kasvokuvaa saa käyttää ainoastaan manuaaliseen, aistinvaraiseen vertailuun luottavan osapuolen toimesta. Automaattiset tai puoliautomaattiset tekniset menetelmät (esimerkiksi piirteiden poiminta, mallipohjainen vertailu tai kasvojentunnistus) eivät ole sallittuja, ellei erillisessä säännöksessä toisin nimenomaisesti säädetä. Mikäli tällainen tekninen käsittely myöhemmin sallitaan, edellytyksenä tulee olla täsmällinen oikeusperuste, vaikutustenarviointi, dokumentoitu tarkoitussidonnaisuus ja auditointivelvoite.

Terminologiaa olisi hyvä yksinkertaistaa

Ehdotetun lain 3 §:n määritelmä digitaalisesta henkilöllisyystodistuksesta on ongelmallinen. Siinä digitaalinen henkilötodistus määritellään oikeudeksi saada attribuuttitodistus.

Jos henkilö hakee Digi- ja väestötietovirastolta ”digitaalisena henkilöllisyystodistuksena käytettävää hyväksyttyä sähköistä attribuuttitodistusta” tai esimerkiksi verkkopalvelun tarjoaja pyytää henkilöä todistamaan ikänsä ”digitaalisena henkilöllisyystodistuksena käytettävän hyväksytyn sähköisen attribuuttitodistuksen” avulla, henkilö voi hämmentyä. Ymmärrettäviä ja helppokäyttöisiä asiointipalveluja tarjoavat tahot tuskin voivat käyttää laissa määriteltyjä termejä.

Olisi yksinkertaisempaa ja ymmärrettävämpää, mikäli laissa säädettäisiin erikseen (i) oikeudesta digitaaliseen henkilöllisyyteen, jonka myöntää Poliisi (3, 4, 5, 6 ja 8 §), sekä (ii) digitaalisesta henkilöllisyystodistuksesta, jonka myöntää Digi- ja väestötietovirasto (7 ja 8 §).

Raukeamisesta tulisi säätää tarkemmin

Ehdotetun lain 12 §:ssä säädetään digitaalisen henkilöllisyystodistuksen raukeamisesta. Pykälässä käytetty passiivimuoto voi olla ongelmallinen sillä raukeaminen tuskin tapahtuu itsestään. Lakia selkeyttäisi, jos pykälässä mainittaisiin, että toimivaltaisen viranomaisen tulee merkitä digitaalinen henkilöllisyys(todistus) rauenneeksi havaitessaan jonkin ehdoista täyttyvän. Selkeyden vuoksi pykälässä voisi mainita yhtenä raukeamisen ehtona voimassaoloajan päättymisen (joka muista ehdoista poiketen tapahtuu itsestään). Ehdotamme lisäksi, että sääntelyssä erotetaan selkeästi raukeaminen, peruuttaminen ja keskeytys, määritellään voimaantulon ajankohta ja todetaan, että raukeamisesta annetaan haltijalle todisteellinen tiedoksianto. Muutos tulee välittää reaaliaikaisesti luottaville osapuolille saatavan voimassaolorajapinnan kautta.

Sulkulistatarkistuksen vaikutukset tulee kuvata

Ehdotetun lain 15 §:ssä mainitaan oikeus tarkistaa todistuksen voimassaolo sulkulistan avulla. On hyvä, että kyseessä on oikeus eikä velvollisuus, mutta hallituksen esitykseen voisi lisätä maininnan, että jättämällä sulkulistatarkastuksen tekemättä luottava osapuoli hyväksyy riskit, jotka aiheutuvat siitä, että esitetty attribuuttitodistus on peruutettu tai rauennut.

Huomiot kansallisen vahvan sähköisen tunnistamisen turvallisuutta parantavista muutoksista:

Ensitunnistamisen kieltomahdollisuudella ei todennäköisesti saavuteta toivottuja tuloksia

Hallituksen esityksessä päivitetyn lain vahvasta sähköisestä tunnistamisesta uusi 18 a § mahdollistaisi tunnistusvälineen kieltämisen ensitunnistamiseen. Lain yksityiskohtaisissa perusteluissa (lausuttavana olevan luonnosdokumentin sivulla 79) mainitaan esimerkkinä anastetun tunnistusvälineen käyttö uuden tunnistusvälineen hankkimiseksi. Esimerkin mukaisessa tilanteessa tunnistusvälineen oikean haltijan vastuulla olisi ilmoittaa välineen tarjoajalle välineen anastamisesta ja välineen tarjoajan vastuulla olisi estää välineen käyttö kaikkeen tunnistamiseen – ei vain uusien tunnistusvälineiden hankkimiseen. Hallituksen esityksessä olisi hyvä kuvata annetun esimerkin sijaan tai lisäksi muita tapauksia, joissa tunnistusvälineen haltija haluaisi kieltää tunnistusvälineen käytön ensitunnistamisessa.

Arvioimme, että ensitunnistuskiellon ennakollinen käyttöönotto on vähäistä ja kiellon poistaminen monille hankalaa, minkä vuoksi toimenpiteen kokonaishyöty turvallisuuden kannalta jää rajalliseksi. Ensitunnistuksen turvallisuuden parantamiseksi ehdotettua kieltoa parempi menetelmä on vaatia ensitunnistuksen tekijää välittämään tunnistusvälineen käyttöön liittyvät tiedot varmistettua kanavaa pitkin (esimerkiksi Suomi.fi-viestinä tai kirjattuna kirjeenä väestötietoihin merkittyyn osoitteeseen). Vaikka paperiposti aiheuttaa prosessiin viivettä, aiheutuva kitka on perusteltua tunnistusvälineen hankintaan liittyvässä ensitunnistuksessa.

Tunnistamisvälineenä käyttämisen estämistä tulee selkeyttää

Lausuttavana olevan dokumentin sivulla 79 mainitaan: “Toisaalta sääntely ei myöskään velvoittaisi eurooppalaisen digitaalisen identiteetin lompakon tarjoajaa antamaan tarjoamaansa lompakkoon perustuvaa tunnistamista välitettäväksi tunnistusvälityspalvelun tarjoajalle.” Jos eurooppalaisen digitaalisen identiteetin lompakossa “olevien tietojen tulee siis olla käyttäjän yksinomaisessa hallinnassa ja täydessä määräysvallassa” (s. 55), on syytä täsmentää, mitä “estämisellä” tarkoitetaan. Ehdotamme, että perusteluissa todetaan selvästi: lompakon tarjoajaa ei velvoiteta tarjoamaan tunnistamista tunnistusvälityspalvelun kautta, mutta tarjoaja ei saa estää käyttäjää käyttämästä lompakkoa tunnistamiseen yhteensopivalla tavalla suoraan luottavan osapuolen kanssa. Käyttäjän yksinomainen määräysvalta tarkoittaa, että käyttäjä voi luovuttaa tietojaan valitsemalleen luottavalle osapuolelle, kun tekninen ja oikeudellinen yhteensopivuus täyttyy. Lompakon tarjoajan tulee dokumentoida tuetut tunnistusvirrat ja rajapinnat läpinäkyvästi.

Lausuttavana olevan dokumentin sivulla 79 todetaan, että ” oisaalta sääntely ei myöskään velvoittaisi eurooppalaisen digitaalisen identiteetin lompakon tarjoajaa antamaan tarjoamaansa lompakkoon perustuvaa tunnistamista välitettäväksi tunnistusvälityspalvelun tarjoajalle.”, kun taas sivulla 55 todetaan, että ”lompakossa olevien tietojen tulee olla käyttäjän yksinomaisessa hallinnassa ja täydessä määräysvallassa”. Näiden kirjausten välillä on tulkinnallinen ristiriita käyttäjän määräysvallan ja lompakon tarjoajan harkinnan välillä. Ehdotamme, että perusteluissa ratkaistaan tämä jännite selventämällä, mitä ”yksinomainen määräysvalta” käytännössä tarkoittaa suhteessa käyttäjän mahdollisuuteen esittää tunnistetietonsa tunnistusvälityspalvelujen kautta.

Huomiot koskien kansallista ekosysteemikuvausta:

Luotettavien osapuolten rekisteröintiä on hyödyllistä kuvata tarkemmin

Ekosysteemikuvauksessa todetaan, että “Luottavien osapuolten rekisterinpitäjä tekee myös toimenpiteitä varmistuakseen siitä, että rekisterin tiedot ovat ajantasaiset ja asianmukaiset.” Ilmaisu “asianmukaiset” jää tulkinnanvaraiseksi. On hyödyllistä avata, viitataanko tällä esimerkiksi yrityksen toimialan varmistamiseen, liittyvätkö yrityksen myöntämät tai pyytämät attribuutit sen toimintaan vai viitataanko ainoastaan yrityksen perustietojen (Y-tunnus ja virallinen nimi) oikeellisuuteen.

Ehdotamme, että ekosysteemikuvauksessa täsmennetään, että luottavien osapuolten rekisterinpitäjän rooli on rajattu ja tarkemmat tiedot tiettyjä todisteita myöntävistä ja niitä pyytävistä tahoista voidaan kirjata esimerkiksi eri toimialojen ja liiketoimintaverkostojen omiin luottamusrekistereihin.

Luottamusekosysteemin hallinto-organisaation rooli on hyödyllistä huomioida

Ehdotamme, että ekosysteemikuvaukseen lisätään luottamusekosysteemin hallinto-organisaation rooli. Luottamusekosysteemi on tietyn toimialan tai liiketoimintaverkoston toimijoiden muodostama kokonaisuus, jossa todisteiden myöntäjät, haltijat ja luottavat osapuolet hyödyntävät digitaalisia todisteita yhteisesti sovittujen sopimusten, sääntöjen ja määrittelyjen puitteissa. Hallinto-organisaation tehtävänä on varmistaa luottamusekosysteemin sääntöjen ajantasaisuus ja noudattaminen sekä sen yhteentoimivuus ja turvallisuus. Luottamusekosysteemin hallinto-organisaation koordinoi sääntöjen kehittämistä ja muutostenhallintaa, valvoo yhteentoimivuutta ja vaatimustenmukaisuutta, koordinoi uusien jäsenten liittymistä sekä fasilitoi riitatilanteiden ratkaisua.

Oikeushenkilölompakoiden luonne palvelinpohjaisina ratkaisuina on hyödyllistä kuvata kattavammin

Ehdotamme, että ekosysteemikuvauksessa tuodaan selkeämmin esiin oikeushenkilöiden lompakoiden mahdollinen luonne palvelinpohjaisena ratkaisuna, joka voidaan integroida organisaation liiketoimintajärjestelmiin ja -prosesseihin. Palvelinpohjainen lompakko mahdollistaa digitaalisten todisteiden vastaanoton, hallinnan ja esittämisen automaation eri käyttötarkoituksissa. Oikeushenkilölompakon haltijana on oikeushenkilö ja lompakkoa käyttävät valtuutetut edustajat ja/tai organisaation tietojärjestelmät organisaation sisäisen pääsynhallinnan ja roolipohjaisten käyttöoikeuksien puitteissa.

Hautala Markus
TietoEVRY - Tietoevry Create