

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 terveystietoja kyselevä luottava osapuoli on varmasti terveydenhuollon toimija.

Asetuksen mukaisen eIDAS-luottamuskehyksen lisäksi tarvitaan täydentävää luottamusinfrastruktuuria. Ekosysteemikohtaisia luottamusrekistereitä voidaan toteuttaa esimerkiksi OpenID Federation -protokollaan liittyen. Findy-verkoston luottamusrekisteri on esimerkki tällaisesta toteutuksesta.

Tätä täydentävää luottamusinfrastruktuuria ei ole tarvetta säädellä osana lausuttavana olevaa lakipakettia. Täydentävä luottamusinfrastruktuuri voi perustua pitkälti sopimusoikeuteen ja toimijoiden keskenään sopimiin sääntökirjoihin.

Digitaalinen identiteetti tulee tarjota kaikille organisaatioille

Hallituksen esityksessä todetaan useaan kertaan olevan ”ilmeistä, ettei [oikeushenkilön] tunnistetietoja voitaisi aluksi tarjota kuin keskeisille oikeushenkilömuodoille, kuten osakeyhtiölle.” Emme löytäneet hallituksen esityksestä kuvausta siitä, miksi oikeushenkilömuotoja koskeva rajoite on ilmeinen.

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

On valitettavaa, että oikeushenkilön tunnistetietojen tietolähteeksi on valittu Yritys- ja yhteisötietojärjestelmän sijaan Kaupparekisteri, ja että esimerkiksi toiminimellä toimiva yrittäjä ei voi saada yritykselleen organisaation tunnistetietoja. Ymmärrämme, että 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.

Uskoaksemme olisi lain hengen mukaista myöntää yrityksen tunnistetiedot kaikille yrityksille, joilla on Y-tunnus.

Hallituksen esityksessä tulisi arvioida, minkälaiset vaikutukset esitetyllä lailla olisi yhdistysten, kuntien, asunto-osakeyhtiöiden, oppilaitosten, toiminimien yms. mahdollisuuksiin osallistua digitaaliseen yhteiskuntaan. Jos oikeushenkilön tunnistetiedot voidaan myöntää vain keskeisille oikeushenkilömuodoille, tulisi kuvata, miten muut organisaatiot voivat hyödyntää digitaalisia palveluja.

Findynetin mielestä olisi tärkeää, että kaikki toimijat, joilla on yritys- ja yhteisötunnus, voisivat käyttää digitaalisia ja todisteita. Tämä tulisi mahdollistaa antamalla Patentti- ja rekisterihallitukselle tehtäväksi myöntää digitaalinen Y-tunnustodiste. Todiste voitaisiin myöntää tahoille, jotka pystyvät luotettavalla tavalla todistamaan olevansa oikeutettuja edustamaan kyseistä Y-tunnusta vastaavaa organisaatiota. Tällainen todiste voitaisiin myöntää myös muihin lompakoihin kuin eurooppalaisiin digitaalisen identiteetin lompakoihin, jolloin niistä olisi hyötyä kansainvälisesti toimiville tai kansainvälistä yhteistyötä tekeville organisaatioille.

Julkisen hallinnon toimijoita tulee velvoittaa todisteiden myöntämiseen

Digitaalisten lompakoiden käyttöönottoon vaikuttaa se, mitä niillä voi tehdä. Jos lompakkoon ei ole saatavilla todisteita tai niihin saatavia todisteita ei voi käyttää mihinkään, lompakoita ei oteta käyttöön eikä eIDAS-asetuksen tai kansallisen lainsäädännön tavoitteita saavuteta.

Osana kansallista lainsäädäntöä tulisi velvoittaa keskeiset julkisen sektorin toimijat sekä myöntämään hallussaan olevia tietoja digitaalisina todisteina että hyväksymään digitaalisen lompakon avulla esitettäviä tietoja. Toimijoiden velvollisuuksia ei tarvitsisi kirjata suoraan lakiin,

mutta kansallisen lainsäädännön tulisi mahdollistaa sellaisten säädösten antaminen, joiden perusteella julkisen sektorin toimijat pystyvät edistämään todisteiden myöntämistä ja hyödyntämistä. Valitettavan moni julkishallinnon organisaatio kokee voivansa tehdä vain asioita, joihin niillä on lakisääteinen velvollisuus.

Uudistetun eIDAS-asetuksen 45 e artiklan mukaisesti jäsenvaltioiden on varmistettava, että toteutetaan toimenpiteitä, joiden avulla hyväksytyt todisteiden myöntäjät voisivat tarkastaa tiettyjen attribuuttien aitouden. Asetuksen liitteessä VI on luettelo tällaisista attribuuteista. Kansallisen lainsäädännön yhteydessä tulisi osoittaa, miten asetuksen edellyttämiä toimenpiteitä toteutetaan.

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 antaisivat mahdollisuuden tarjota henkilöllisyyden linkityspalvelua myös luottaville osapuolille, jotka eivät ole julkisen sektorin elimiä.

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 mihinkään muuhun tarkoitukseen kuin henkilön tunnistamiseen. Eri asiointipalveluihin muodostuu rinnakkaisia rekisteri-identiteettejä, mikä haittaa tietojärjestelmien yhteentoimivuutta.

Ehdotetun lain 14 § ei sisällä rajoituksia siihen, kenelle linkityspalvelua voidaan tarjota tai siihen, voisiko se sisältää myös uusien identiteettien muodostamisen. Vaikka järjestelmän toteutuksessa haluttaisiin lähteä liikkeelle minimitoteutuksella, hallituksen esitys tulisi kirjoittaa sellaiseen muotoon, joka ei estä järjestelmän jatkokehittämistä ja tarjoamista laajemmalle käyttäjäkunnalle jatkossa.

Luottavien osapuolten rekisteröintiä tulisi selkeyttää

Eurooppalaisten digitaalisen identiteetin lompakoiden käyttöönotto riippuu pitkälti siitä, mihin lompakoita voi käyttää, eli mitä lompakoihin tukeutuvia palveluja on tarjolla. Lompakkoon luottavien osapuolten lainsäädäntöön liittyy vielä paljon epävarmuutta. Ei ole selvyyttä, kuinka helppoa ja automaattista luotettavaksi osapuoleksi rekisteröityminen olisi tai millä edellytyksillä rekisteröityminen voitaisiin perua. Luottavan osapuolen pääsy- tai rekisteröintivarmenteen peruminen vaikutta merkittävästi luottavan osapuolen kykyyn tarjota digitaalista palvelua. Luottavien osapuolten halua rekisteröityä voi rajoittaa, jos näillä ei ole riittävästi tietoa ehdoista, joiden perusteella rekisteröinti voidaan poistaa tai keskeyttää.

Ehdotetun eIDAS-lain 13 §:ssä mainitaan, että Liikenne- ja viestintävirasto ylläpitää Suomessa eIDAS-asetuksen 5 b artiklassa tarkoitettua eurooppalaisen digitaalisen identiteetin lompakon luottavien osapuolten rekisteriä. Saman ehdotetun 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 luotettavaksi osapuoleksi rekisteröityminen maksutonta vai voiko Liikenne- ja viestintävirasto periä rekisteröinnistä maksun?

Luottavan osapuolen määritelmää olisi hyvä tarkentaa

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

Digitaalisen todisteiden myöntämiseen, hallintaan ja vastaanottamiseen on jo tarjolla runsaasti ohjelmistoja, jotka toteuttavat samoja teknisiä määrittämiä kuin eurooppalaiset digitaalisen identiteetin lompakot ja niihin liittyvät sähköiset attribuuttitodistukset. Suurella osalla näiden ohjelmistojen tarjoajista ja käyttäjistä ei välttämättä ole aikomusta rekisteröityä eurooppalaisen digitaalisen identiteetin lompakon tarjoajiksi tai luottaviksi osapuoliksi.

Ehdotetun eIDAS-lain tulkitsijalle voi jäädä epäselväksi, onko kuka tahansa, joka kokeilee digitaalisen todisteen myöntämistä johonkin lompakkoon tai todisteen pyytämistä jostain lompakosta, automaattisesti ”ei-hyväksytyn luottamuspalvelun tarjoaja”.

Kansallisessa lainsäädännössä olisi hyvä tarkentaa, että digitaalisten todisteiden myöntäjistä ja vastaanottajista tulee asetuksen tarkoittamia luottamuspalvelun tarjoajia vasta, kun ne rekisteröityvät eurooppalaisen digitaalisen identiteetin lompakon luottaviksi osapuoliksi eIDAS-asetuksen 5 b artiklan mukaisesti. (Ilman kyseistä rekisteröitymistä toimijoilla ei ole pääsyä eurooppalaisen digitaalisen identiteetin lompakoihin tai niissä hallittaviin sähköisiin

attribuuttitodistuksiin.) Uudistetun eIDAS-asetuksen 19 artiklan ja ehdotetun eIDAS-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 sille on olemassa asianmukaisesti perusteltu syy." Ehdotetun kirjauksen mukaan avoimen lähdekoodin ohjelmistoja tarjoavat yritykset voisivat katsoa rikkovansa lakia julkaistessaan ohjelmistonsa lähdekoodin.

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.

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, jos laissa puhuttaisiin digitaalisesta henkilöllisyydestä, jonka myöntää Poliisi (3, 4 5, 6 ja 8 §) sekä digitaalisesta henkilöllisyystodistuksesta (7 ja 8 §), jonka myöntää Digi- ja väestötietovirasto.

Raukeamisesta tulisi säätää tarkemmin

Ehdotetun lain 12 §:ssä säädetään digitaalisen henkilöllisyystodistuksen raukeamisesta. Pykälässä käytetty passiivimuoto voi olla ongelmallinen. Raukeaminen tuskin tapahtuu itsestään. Lakia selkeyttäisi, jos pykälässä mainittaisiin, että Poliisin tulee merkitä digitaalinen henkilöllisyys(todistus) rauenneeksi havaitessaan jonkin ehdoista täyttyvän. Selkeyden vuoksi pykälässä voisi mainita yhtenä raukeamisen ehtona voimassaoloajan täyttymisen (joka muista ehdoista poiketen tapahtuu itsestään).

Sulkulistatarkistuksen vaikutuksia voisi avata

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 sulkulistatarkistuksen 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 luultavasti saavutettaisi 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.

Kovin moni tuskin asettaisi ensitunnistuskieltoa päälle ennakoivasti tai varmuuden vuoksi, etenkin koska kiellon peruminen ei välttämättä olisi täysin suoraviivaista. Ensitunnistuksen turvallisuuden

parantamiseksi ehdotettua kieltoa parempi menetelmä voisi olla vaatia ensitunnistuksen tekijää välittämään tunnistusvälineen käyttöön liittyvät tiedot varmennettua kanavaa pitkin. Esimerkiksi Digi- ja väestötietovirasto sekä pankit toimittavat tunnistusvälineiden käyttöön tarvittavia tietoja postitse välineen hakijan väestörekisteriin kirjattuun viralliseen osoitteeseen. Vaikka paperipostin käyttö aiheuttaa prosessiin viivettä, aiheutuva kitka voi olla perusteltua tunnistusvälineen hankkimiseen liittyvän ensitunnistuksen osalta.

Tunnistamisvälineenä käyttämisen estämistä tulisi 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” (lausuttavana olevan dokumentin s. 55), miten lompakon tarjoaja voisi estää lompakkoon perustuvan tunnistamisen välittämisen tunnistusvälityspalvelun tarjoajalle?

Huomiot koskien kansallista ekosysteemikuvausta:

Luotettavien osapuolten rekisteröintiä voisi tarkentaa

Ekosysteemikuvauksessa kerrotaan: ”Luottavien osapuolten rekisterinpitäjä tekee myös toimenpiteitä varmistuakseen siitä, että rekisterin tiedot ovat ajantasaiset ja asianmukaiset.” Kuvauksesta jää epäselväksi, mitä tarkoittavat ”asianmukaiset” tiedot? Pyritäänkö esim. tarkastamaan yrityksen toimiala ja liittyvätkö sen myöntämät tai pyytämät attributit sen toimintaan? Vai tarkoitetaanko asianmukaisilla tiedoilla vain sitä, että Y-tunnus on oikea ja voimassa sekä vastaa organisaation nimeä?

Ekosysteemikuvaukseen voisi tarkentaa, että luottavien osapuolten rekisterinpitäjän rooli on rajattu, ja että tarkempia tietoja todisteita myöntävistä ja niitä pyytävistä tahoista voidaan kirjata esimerkiksi toimialojen tai luottamusverkostojen omiin luottamusrekistereihin.

Kuvausta voisi täydentää hallinto-organisaation roolilla

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. Ainakin jotkut luottamusekosysteemit voivat edellyttää jokin toimijan toimimista luottamusekosysteemin hallinto-organisaationa. Hallinto-organisaation tehtävänä on varmistaa luottamusekosysteemin sääntöjen ajantasaisuus ja noudattaminen sekä yhteentoimivuus ja turvallisuus. Luottamusekosysteemin hallinto-organisaation koordinoi sääntöjen kehittämistä ja muutostenhallintaa, valvoo yhteentoimivuutta ja vaatimustenmukaisuutta, koordinoi uusien jäsenten liittymistä sekä fasilitoi riitatilanteiden ratkaisua.

Rinnetmäki Samuel
Findynet Osuuskunta