

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:

Ulosottolaitos / valtakunnanvoudin kanslia kiittää mahdollisuudesta lausua luonnoksesta hallituksen esitykseksi eduskunnalle sähköisestä tunnistamisesta, luottamuspalveluista ja eurooppalaisesta digitaalisesta identiteetistä annettua EU:n asetusta täydentäväksi lainsäädännöksi.

Hallituksen esitysluonnoksessa pidetään tarkoituksenmukaisena, että kansalliset vahvan sähköisen tunnistamisen vaatimukset ja eIDAS-asetukseen liittyvä täydentävä sääntely säädetään erillisissä laeissa. Kannatettavaa on, kuten hallituksen esitysluonnoksen lain säännöskohtaisissa perusteluissa (s. 44) esitetään, että eIDAS-asetusta täydentävä kansallinen sääntely koskien rajat ylittävää sähköistä tunnistamista, sähköisiä luottamuspalveluja sekä eurooppalaista digitaalista lompakkoa kootaan uuteen eIDAS-lakiin. Tällainen lainsäädännön rakenne tukee sääntelyn selkeyttä, parantaa lain soveltajien oikeusvarmuutta ja helpottaa eri sääntelykokonaisuuksien erottamista toisistaan.

Hallituksen esitysluonnoksen (s. 51) säädöskohtaisissa perusteluissa 2 §:n ("Määritelmät") 8 kohdassa määritellään tekninen alusta. Määritelmässä sillä tarkoitetaan eurooppalaisen digitaalisen identiteettilompakon käyttäjän mobiililaitetta tai muuta laitetta, johon lompakko on otettu käyttöön. Esimerkkinä mainitaan matkapuhelin. Määritelmän osalta olisi kuitenkin hyvä huomioda, että termillä "tekninen alusta" viitataan yleensä virtuaaliseen ohjelmisto- tai järjestelmäympäristöön, joka ei ole sidottu fyysiseen laitteeseen. Teknisen alustan päälle rakennetaan muita sovelluksia tai palveluita, ja tekninen alusta voi olla esimerkiksi käyttöjärjestelmä tai ohjelmistoalusta, joka mahdollistaa esimerkiksi lompakkosovelluksen toiminnan. Sen sijaan matkapuhelin on fyysinen laite, joka käyttää yhtä tai useampaa teknistä alustaa. Edellä esitetyn perusteella olisi hyvä muokata tätä määritelmää siten, että tekninen alusta ei rinnastu suoraan fyysiseen laitteeseen. Siten esimerkiksi matkapuhelin on enemmänkin laitteistoalusta, joka käyttää

tekniistä alustaa, ja matkapuhelin voi sisältää useita teknisiä alustoja, joilla viitataan ohjelmisto- tai järjestelmäympäristöön, jossa esimerkiksi lompakko toimii. Laitteistoalustan käyttötarkoitus on siis mahdollistaa ohjelmistojen ja käyttöjärjestelmien toiminta fyysisessä ympäristössä.

Huomiot koskien digitaalista henkilöllisyystodistusta:

Poliisihallituksen tuottama digitaalinen henkilöllisyystodistus, jonka myöntäminen ei nykyisen lainsäädännön mukaan ole viranomaisille mahdollista, voisi selkeyttää henkilöllisyyden osoittamista erilaisissa asiointitilanteissa ja vähentää epäselvyyksiä siitä, milloin mikäkin tunnistusasiakirja on hyväksyttävä, tukea sähköisen asioinnin sujuvuutta ja tehostaa tunnistamisprosesseja.

On kuitenkin tärkeää huomioida, kuten hallituksen esitysluonnoksessa (s. 34) todetaan, että kansalaisten mahdollisuudet ja halukkuus hyödyntää digitaalista henkilöllisyystodistusta vaihtelevat. Uuden tunnistusratkaisun käyttöönottoon voi liittyä erilaisia vaatimuksia ja edellytyksiä, jotka voivat vaikuttaa sen saavutettavuuteen ja käyttöön eri käyttäjäryhmien keskuudessa.

Huomiot kansallisen vahvan sähköisen tunnistamisen turvallisuutta parantavista muutoksista:

eIDAS-muutosasetus (hallituksen esitysluonnos, s. 10) velvoittaa julkisen sektorin sähköisiä asiointipalveluja hyväksymään eurooppalaisen digitaalisen identiteettilompakon käytön vahvan sähköisen tunnistamisen välineenä. On tärkeää varmistaa, että lompakko täyttää korkean varmuustason vaatimukset eli mahdollisimman korkean luotettavuuden ja tietoturvallisuuden tason (hallituksen esitysluonnos, s. 97).

Kuten hallituksen esitysluonnoksessa (s. 17, 26 ja 78) todetaan, lompakko ei ole pelkästään tunnistusväline, vaan osa laajempaa digitaalisen identiteetin kokonaisuutta. Tämän vuoksi olisi myös perusteltua, että tunnistusvälineiden tarjoajille asetetaan jatkossa velvollisuus, eikä pelkästään nykyistä oikeutta, tarkistaa poliisin tietojärjestelmästä passin tai henkilökortin voimassaolo silloin, kun niitä käytetään ensitunnistuksessa eli luonnollisen henkilön tunnistamisessa vahvan sähköisen tunnistusvälineen hankkimisen yhteydessä. Tarkistus poliisin tietojärjestelmästä on tunnistusvälineen tarjoajille maksutonta, ja sen tekninen toteutus edellyttää ainoastaan kansallisen palveluväylän liityntäpalvelimen käyttöönottoa (hallituksen esitysluonnos, s. 30). Vaikka em. käyttöönotto voi aiheuttaa kertaluonteisia kustannuksia toimijalle, ei niitä voida pitää kohtuuttomina, kun otetaan huomioon muutoksen merkitys vahvan sähköisen tunnistamisen turvallisuuden parantamisessa. Tämä tarkistustoimenpide lisäisi myös luottamusta sekä eIDAS-muutosasetuksen mukaisten luottavien osapuolten kuten sähköisten asiointipalvelujen tarjoajien että lompakon käyttäjien keskuudessa, kun henkilöllisyys asiointipalveluissa perustuu lompakosta saataviin tietoihin. Ja kuten hallituksen luonnosesityksessäkin todetaan (s. 30), niin ehdotetuilla muutoksilla ei arvioida olevan merkittäviä taloudellisia vaikutuksia tunnistusvälineiden tarjoajille.

Huomiot koskien kansallista ekosysteemikuvausta:

Tietojen itsehallittavuus:

Kuten hallituksen esitysluonnoksessakin (s. 42) todetaan, tietojen valikoiva osoittaminen on kannatettava toimintamalli, sillä se tukee yleisen tietosuoja-asetuksen mukaista tietojen minimointiperiaatetta.

Lompakon käyttö perustuu itsehallittavaan identiteettiin ja tiedonhallintaan, jolloin käyttäjä hallitsee joko itseltään tai luotettavalta kolmannelta taholta lähtöisin olevia omia tietojaan valitsemalla, mitä tietoja hän jakaa ja kenelle. Tämä huomioon ottaen tulisi asiointipalveluilla olla mahdollisuus käytännössä rajata niille toimitettavia tietoja, koska niiden tulee kerätä käyttäjältä vain palvelun tarjoamisen kannalta välttämättömät tiedot, jotka ne ovat rekisteröinnin yhteydessä ilmoittanut ja toimittanut (hallituksen esitysluonnos, s. 9) rekisterin ylläpitäjälle eli Liikenne- ja viestintävirastolle.

Lisäksi on syytä huomioida, että mitä enemmän käyttäjä voi omatoimisesti kerätä ja tallentaa lompakkoonsa tietoja, joita asiointipalvelut eivät välttämättä edellytä, sitä suurempi on mahdollinen vahinko tietoturvaloukkauksen sattuessa. Tämän vuoksi on tärkeää, että lompakon suunnittelussa ja käytössä otetaan huomioon myös tietojen tarpeellisuus ja riskienhallinta.

Raportointi tietosuojaviranomaiselle ja tietojen poistaminen:

Kuvauksessa (s. 11, ja myös hallituksen esitysluonnoksessa sivulla 42) todetaan, että lompakon käyttäjä voi käyttää yleisen tietosuoja-asetuksen mukaista oikeuttaan pyytää asiointipalvelua häntä koskevien tietojen poistamiseen. Lompakkopalvelun tarjoajan tulee tarjota käyttäjille mahdollisuus pyytää suoraan tietojen poistamista asiointipalveluilta, joille käyttäjä on jakanut tietojaan. Asiointipalveluja tarjoavien luottavien osapuolten tulisi taas mahdollistaa rajapinta, jonka kautta sitä voidaan informoida pyynnöstä poistaa käyttäjään liittyvät tiedot. Näiden edellä esitettyjen edellytysten osalta olisi tarkoituksenmukaista, jotta lompakon käyttäjät eivät ymmärtäisi henkilötietojen poisto-oikeutta väärin ja asiointipalvelut eivät kuormittuisi perusteettomista tietojen poistopyynnöistä, tarkentaa lompakkopalvelussa, missä tilanteissa tätä oikeutta voi käyttää. Poisto-oikeuden soveltaminen riippuu muun muassa siitä, millä oikeusperusteella henkilötietoja käsitellään asiointipalveluissa. Rekisteröidyllä ei ole oikeutta vaatia henkilötietojensa poistamista esimerkiksi silloin, kun niiden käsittely perustuu Ulosottolaitoksen lakisääteisten tehtävien hoitamiseen.

Kuvauksen (s. 12) mukaan lompakko antaa käyttäjälle myös mahdollisuuden ilmoittaa kansalliselle tietosuojaviranomaiselle tilanteista, joissa voidaan epäillä asiointipalvelulta tulleen tietopyynnön olevan lainvastainen tai epäilyttävä. Mikäli tällä tietopyynnöllä tässä tarkoitetaan esimerkiksi tietojen kalasteluyritystä, niin todettakoon, että tämä tieto on myös asiointipalvelun tarjoajalle erittäin tärkeää tietoa saada mahdollisimman pian, kun se havaitaan, jotta tapahtumaa voidaan alkaa tutkia ja aloittaa mahdolliset tarpeelliset toimenpiteet ko. asiointipalvelun tarjoajan omien sisäisten prosessien mukaisesti. Tämä asia tulisi ottaa huomioon, kun lompakon palvelun sisältöä lompakon käyttäjille suunnitellaan.

Lompakossa olevien tietojen hallinnan osalta hallituksen esitysluonnoksen (s. 42) mukaan eurooppalaiset digitaaliset identiteettilompakot rakentuvat pääsääntöisesti tiedonvaihtoon perustuvaan malliin, jossa käyttäjät antavat nimenomaisen suostumuksensa tietojen luovuttamiseen asiointipalveluille. On tärkeää huomioida, että viranomaisten tarjoamissa asiointipalveluissa suostumus ei useinkaan ole soveltuva oikeusperuste henkilötietojen käsittelylle, kun viranomainen toimii rekisterinpitäjänä ja se käsittelee henkilötietoja lakisääteisen velvoitteen tai muun julkisen tehtävän perusteella, jolloin ei ole kyse lompakon käyttäjän tietojen itsehallittavuuden piiriin kuuluvasta tietojen käytöstä. Näin ollen viranomaispalveluissa ei pääsääntöisesti kerätä eikä hallinnoida käyttäjien suostumuksia. Myös tämä seikka on tärkeä ottaa huomioon lompakon käyttötapauksia ja teknisiä toteutuksia suunniteltaessa.

Lompakoiden sertifiointi:

Vaatimustenmukaisuuden varmistaminen voi käytännössä olla haasteellista, kun Digi- ja väestötietoviraston lisäksi myös yksityiset toimijat alkavat tarjota omia lompakkoratkaisujaan. Haasteita voi aiheutua sen takia, että jäsenvaltiot ovat vasta kehittämässä kansallisia sertifiointijärjestelmiä, joihin sisällytetään nyt myös kyberturvallisuusvaatimukset, koska eurooppalaista kyberturvallisuuden sertifiointijärjestelmää ei ole vielä käytössä (kuten hallituksen esitysluonnoksessa asiasta todetaan, s. 9, 10 ja 37). Tässä yhteydessä olisi erityisen tärkeää varmistaa, että kansalliset vaatimukset vastaavat riittävällä tasolla tulevia eurooppalaisia tasovaatimuksia.

Ekosysteemi ja täydentävä materiaali:

Asiointipalveluiden näkökulmasta mahdollisia lisäkustannuksia aiheuttavia tekijöitä ovat tekniset muutokset ja asiakkaiden neuvonta ja ohjaus.

Digi- ja väestötietovirasto vastaa lompakon teknisestä toteutuksesta ja käyttöönotosta sekä toimii kansallisen lompakon tarjoajana, mutta tekniset muutokset aiheuttavat mahdollisesti kustannuksia myös julkisen sektorin asiointipalveluille, kun esimerkiksi testataan järjestelmien yhteensopivuutta digitaalisen identiteettilompakon kanssa. Tiedonvaihdon toteutustapojen arviointi voi aiheuttaa myös uudelleensuunnittelua.

Kuvauksessa viitattiin teknisiin standardeihin (s. 14), jotka osaltaan voivat vaikuttaa sähköisten asiointipalvelujen kustannuksiin, kun asiointipalvelujen yhteensopivuutta varmistetaan näiden standardien kanssa. Vaikka nämä standardit parantavat yhteentoimivuutta ja turvallisuutta, niiden käyttöönotto voi aiheuttaa merkittäviä alkuinvestointeja asiointipalveluille riippuen palvelun arkkitehtuurista.

Käytännössä Digi- ja väestötietovirasto on päävastuussa käyttäjien neuvonnasta, mutta myös muut viranomaiset ja asiointipalvelut osallistuvat neuvontaan omien palveluidensa osalta. Tämä voi sisältää ohjeistuksia ja asiakastukea kuten asiakkaiden neuvontaa asioinnin osalta, viraston oman henkilöstön koulutusta uuden prosessin osalta ja tukipalveluiden vahvistamista lisäämällä resursseja.

Vaikka Digi- ja väestötietovirastolla on keskeinen rooli käyttäjien ohjeistamisessa ja tukipalveluissa, asiointipalveluja tarjoavat viranomaiset, jotka hyödyntävät lompakkoa ovat vastuussa omien palveluidensa osalta siitä, että käyttäjät saavat riittävästi tietoa ja tukea uuden tunnistustavan käytössä. Tämä on tärkeää, jotta kansalaiset osaavat käyttää digitaalista identiteettilompakkoa sujuvasti eri tilanteissa, jotta palvelu olisi myös kustannustehokasta.

Blomqvist Mia
Ulosottolaitos - valtakunnanvoudin kanslia