Vaana

Lausunto

08.02.2019

Asia: VM068:00/2017

Kuuleminen henkilötunnuksen uudistamista koskevan työryhmän johtoryhmän väliraportista

Nykytilan ongelmat

Onko työryhmä mielestänne tunnistanut oikeat haasteet nykyjärjestelmässä? Onko tiedossanne sellaisia ongelmia, jotka tulisi näiden lisäksi huomioida?

-

Onko järjestelmässä sellaisia elementtejä, joista ei mielestänne saisi luopua?

-

Tulevaisuuden näkymät ja haasteet

Millaisten ilmiöiden oletatte vaikuttavan henkilön yksilöinnin ja identiteetin tarpeisiin tulevaisuudessa? Onko joihinkin muutostrendeihin reagoiminen erityisen kriittistä tulevaa ratkaisua suunniteltaessa?

Identiteettiverkkojen (esim. Hyperledger Indyn päälle rakentuva Sovrin) tarjoamat mahdollisuudet henkilökohtaisen tiedon yksityisyyden varmistamiseksi ovat erittäin mielenkiintoisia puhuttaessa digitaalisten palveluiden käytöstä tulevaisuudessa. Mahdollisuudet eivät rajoitu vain yksityishenkilöihin vaan myös yhteisöihin.

Nämä mallit vähentävät tarvetta identiteetille ja sen sijaan korostavat digitaalisesti varmennettavien väittämien (claim tai credential) käyttöä. Käytännössä esimerkiksi Poliisilaitos voi luovuttaa digitaalisesti allekirjoitetun väittämän yksityishenkilölle joka todistaa että kyseinen henkilö saa ajaa autoa. Maistraatti voi luovuttaa samalle henkilölle toisen väittämän joka todistaa että henkilö asuu Helsingissä. Kansainvälinen standardointiryhmä W3C tekee työtä väittämien standardoimiseksi: https://www.w3.org/community/credentials/

Väittämiä käyttäen yksityishenkilö voi todistaa asuvansa Helsingissä ilman että hänen tarvitsee paljastaa itsestään muuta, tarkoitusta varten epärelevanttia, tietoa. Erityisesti tämä vapauttaa sekä järjestelmät että henkilöt identiteetin käytöstä ja sen käyttöön liittyvistä haasteista. Identiteettien

käyttö on esimerkiksi tietomurtotapauksissa vaarallista. Mikäli hyökkääjä murtautuu rekisteriin jossa ylläpidetään osoitteita ja toiseen rekisteriin jossa ylläpidetään potilastietoa pystyy hän yhdistämällä tietoa eri rekistereistä tunnistamaan potilaan. Vastaavaa tietojen yhdistelemistä rekistereiden yli ei voi tehdä mikäli järjestelmät toimivat perustuen digitaalisiin väittämiin identiteettien sijaan.

Miten näette nykyisen henkilötunnusjärjestelmän mahdollisuudet vastata tulevaisuuden haasteisiin?

Äärimmäisen huonona.

Sen lisäksi että nykyiset henkilötunnukset paljastavat tietoa kansalaisesta (esimerkiksi syntymäaika ja sukupuoli) ne on myös helppoja arvata. Mikäli tiedetään henkilön syntymäaika ja sukupuoli ei jää enää kuin yksilönumero joka tarvitsee arvata. Tämän on numero välillä 002–899. Kyseisen arvoavaruuden läpikäynti esimerkiksi naiivilla brute-force menetelmällä on helppoa.

Tämän lisäksi arvoavaruuden pienuuden takia henkilötunnukset kärsivät myös törmäysongelmista (collision) yksisuuntaisten kryptografisten hajautusfunktioiden parametreina (one-way cryptographic hash function) joka mahdollistaisi henkilötunnuksen tallentamisen niin että ainoastaan taho joka tietää alkuperäisen henkilötunnuksen voisi osoittaa sen olevan sama kuin tallennettu tunnus.

Oletteko tunnistaneet sellaisia jo olemassa olevia tarpeita, joihin väliraportissa esitetyt ratkaisumallit eivät kykene vastaamaan?

-

Biometria

Miten näette biometrian hyödyntämismahdollisuudet uudistuksessa?

Biometriaa voidaan käyttää hyödyksi henkilön tunnistamisessa jotta henkilö voisi esimerkiksi välittää edellisissä vastauksissa käsiteltyjä väittämiä palvelun tuottajille.

Millaisia mahdollisuuksia biometria tarjoaa?

-

Millaisia riskejä näette biometrian hyödyntämisessä?

-

Ratkaisumallien arviointi

Kommentteja minimimallista

-

Kommentteja keskitetystä mallista

-

Kommentteja hajautetusta mallista

Tässä on havaittavissa yhteneväisyyttä filosofioihin joihin identiteettiverkotkin perustuvat. Väliraportissa puhutaan kuitenkin identiteettitiedoista. Parempaa yksityisyyttä voitaisiin mielestäni saavuttaa väittämillä. Sen lisäksi mallissa puhutaan mahdollisuuksista tietojen linkittämiseen. Tämä tulisi kuitenkin olla mahdollista ainoastaan kansalaisen suostumuksesta tai julkisen toimijan kriittisen toiminnon pakottamana. Mikäli linkittämiseen mahdollistavaa tietoa on tallennettu keskitettyihin tietovarantoihin avataan aina mahdollisuus riskille että tietoa linkitetään vastoin kansalaisen tahtoa ja vääriin tarkoituperiin.

Millä tavalla työtä tulisi mielestänne jatkossa suunnata? Mitkä elementit esitetyistä malleista ovat mielestänne tarkoituksenmukaisia jatkoselvityksen kannalta?

-

Mitä elementtejä malleista puuttuu tai haluaisitteko esittää kokonaan toisenlaista ratkaisumallia?

-

Vaikutukset

Miten vaikutusarviointia olisi mielestänne tarkoituksenmukaista tehdä, kun jatkoselvityksen kohde on konkretisoitunut?

-

Mitä tahoja olisi mielestänne tärkeää kuulla vaikutuksia arvioitaessa?

-

Miten arivioisitte vaikutuksia järjestelmiinne tai toimintaanne seuraavissa tilanteissa, olettaen mahdollisuuden kohtuulliseen siirtymäaikaan:
A) henkilötunnuksen välimerkki muutetaan tai lisätään uusi välimerkki
B) henkilötunnuksesta poistetaan sukupuolitieto
C) henkilötunnuksesta poistetaan syntymäaika
D) henkilötunnuksen muoto muutetaan kokonaisuudessaan erilaiseksi merkkisarjaksi

Järjestelmätoimittajan edustajana näen että uudistustyöhön käytettävän ajan suuruudessa sillä muutetaanko olemassa olevaa henkilötunnusta paljon vai vähän on pieni ero.

Näkisin että koska työhön henkilöiden tunnistamiseen ja henkilöihin liittyvien tietojen välittämiseen on ryhdytty kannattaisi suunnitella muutokset niin että ne ovat kauaskantoisia. Tähän liittyen kannatta harkita uudelleen koko nykyinen järjestelmä joka perustuu henkilötietojen keskitettyyn tallentamiseen sekä yhteen tunnukseen joka johtaa siihen että samalla tunnisteella pystyy löytämään samasta henkilöstä tietoa useasta eri tietovarannosta.

Muut kommentit

Muita kommentteja väliraportista tai selvityksen kohteesta

-

Avoin vastauskenttä

Tähän voitte kirjoittaa vapaasti jäsennellyn avovastauksen

-

Parpala Matti
Vaana Oy

Järvensivu Tuomas
Vaana