Dnro
TRAFICOM/461816/04.04.04.01/2020
1.6.2021

Traficomin muistio puolesta-asioijan luotettavuuden arviointikriteereistä

Sisällysluettelo

1 Muistion tarkoitus ja tausta

Liikenteen palveluista annetun lain (liikennepalvelulain) mukaan puolesta-asiointirajapinnan avaamisvelvollisilla (avaamisvelvollisilla) on oikeus asettaa ennakolta arviointikriteerejä, joiden perusteella voivat ne arvioida puolesta-asioinnin rajapinnan avaamista pyytävien toimijoiden (puolesta-asioijien) luotettavuutta.

Tämän muistion tarkoitus on selventää, miten Liikenne- ja viestintävirasto Traficom (jäljempänä Traficom) toimivaltaisena valvovana viranomaisena tulkitsee edellä mainittua avaamisvelvollisten oikeutta arviointikriteerien asettamiseen.

Traficomin muistiolla on tarkoitus muun muassa tunnistaa minkä tyyppisillä eri kriteereillä avaamisvelvolliset voisivat arvioida puolesta-asioijan luotettavuutta ja auttaa toimijoita tunnistamaan millaiset arviointikriteerit ovat oikeudenmukaisia, kohtuullisia ja syrjimättömiä. Traficom kuitenkin arvioi toimijoiden laatimien arviointikriteereiden lainmukaisuutta tapauskohtaisesti.

Muistio ei ole mallipohja arviointikriteereiksi ja toimijat itse vastaavat omien arviointikriteeriensä asettamisesta. Muistio ei ole myöskään tyhjentävä luettelo arviointikriteereistä, eivätkä tässä esitellyt kriteerit muodosta yhtenäistä kokonaisuutta.

Traficom valvoo puolesta-asiointia koskevaa tietosuojaa niiltä osin, kun kyse on tietosuojaa koskevien arviointikriteerien ja sopimusehtojen oikeudenmukaisuudesta, kohtuullisuudesta ja syrjimättömyydestä. Lisäksi Traficom valvoo, että avaamisvelvoitetut toimijat täyttävät liikennepalvelulaissa asetetun velvoitteen avata puolesta-asiointirajapinta tietosuoja huomioiden.

Muistion tekemisen tueksi Traficom on järjestänyt viisi työpajaa, joissa toimijat ovat voineet esittää näkemyksiään arviointikriteereistä. Traficom lähetti 6.11.2020 muistioluonnoksen arviointikriteereistä toimijoille lausuttavaksi. Määräaikaa lausunnon antamiselle oli 27.11.2020 saakka ja Traficom sai asiassa 19 lausuntoa. Lausunnoissa kiinnitettiin erityisesti huomiota tietosuojakysymyksiin Traficomin näkemyksen mukaisessa puolesta-asioinnin toteuttamismallissa, jossa käyttäjätilien tietoja vertailemalla tunnistetaan asiakas.

Lausuntopalaute huomioitiin uudessa luonnosversiossa, joka lähetettiin toimijoille lausuttavaksi 10.5.2021 ja hankkimalla alla mainittu tietosuojaselvitys. Määräaikaa lausunnon antamiselle oli 26.5.2021 saakka ja Traficom sai asiassa 11 lausuntoa.

Muistiossa on pyritty huomioimaan kaikki prosessin aikana saatu palaute.

Traficom hankki Bird & Bird Asianajotoimistolta selvityksen tietosuojalainsäädännön asettamista vaatimuksista, jotka rekisterinpitäjän tulee ottaa huomioon puolesta-asiointiin liittyvän vertailumallin toteuttamisessa.[1]

Selvitys koskee tietosuojalainsäädännön rekisterinpitäjälle asettamia vaatimuksia. Selvityksessä ei oteta kantaa liikennepalvelulain velvoitteiden tulkintaan. Traficom ei valvo rekisterinpitäjän velvoitteiden toteutumista tietosuojalainsäädännön näkökulmasta. Selvitys ja sen lopputulos eivät ole Traficomin valvontatyökalu tai tulkintakannanotto.

Muistion valmisteluprosessia on kuvattu yllä olevassa kuvassa.

2 Mitä puolesta-asiointi tarkoittaa?

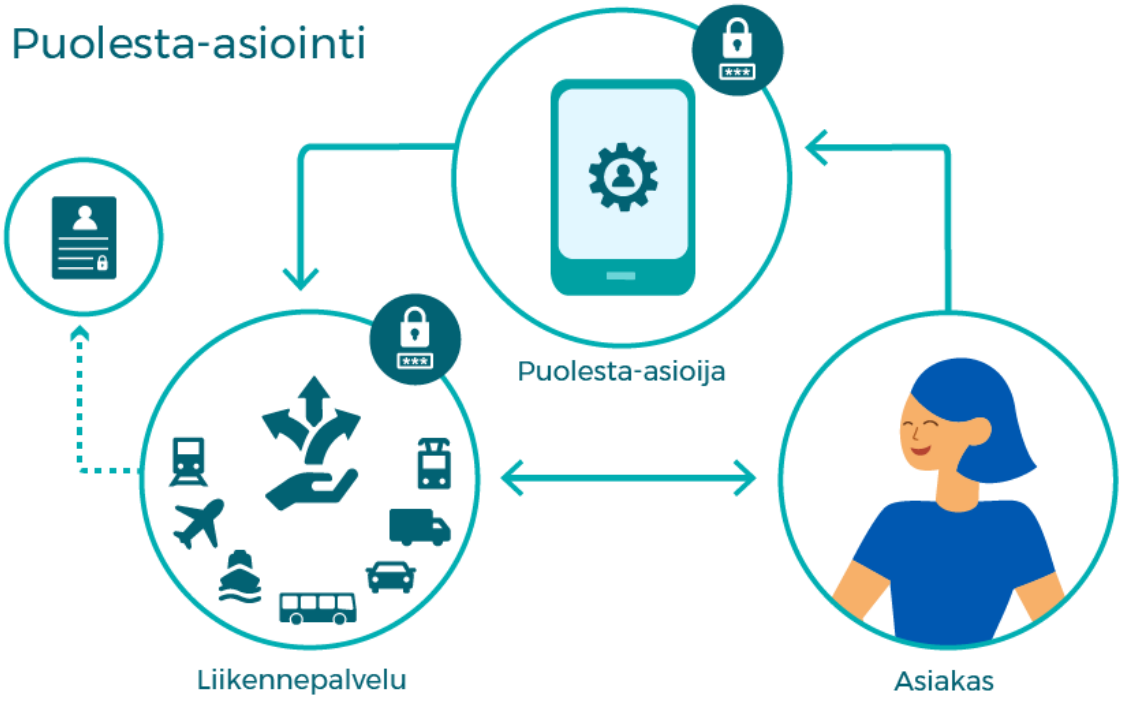
Liikenteen palveluista annetun lain 156 §:n mukaan liikkumis- tai yhdistämispalvelun, jolla on käyttäjätilijärjestelmä, on avattava toiselle liikkumis- tai yhdistämispalvelulle pääsy myyntirajapintaansa ja mahdollistettava sille hankkia palvelun käyttäjän toimeksiannosta hänen puolestaan alennuksen, korvauksen tai muun erityisehdon käyttämiseen oikeuttavia lipputuotteita tai muita palvelun käyttöön oikeuttavia tuotteita hyödyntäen palvelun käyttäjän palvelussa olevia tunniste- ja käyttäjätietoja.

[1] https://liikkumisenrajapinnat.fi/sites/default/files/media/file/Puolesta-asioinnin%20vertailumallin%20tietosuojavelvoitteet%20%202021%2004%2014.pdf

Liikennepalvelulain mukaisella puolesta-asiointivelvoitteella (puolesta-asioinnilla) tarkoitetaan sitä, että liikkumis- tai yhdistämispalvelu voi hankkia toiselta liikkumis- tai yhdistämispalvelulta kyseisen palvelun asiakkaan henkilökohtaisia ja käyttäjätiliin sidottuja matkustusoikeuksia tai muita liikkumispalveluun käyttöön oikeuttavia tuotteita. Henkilökohtaiset matkustusoikeudet ja muut liikkumispalvelutuotteet perustuvat asiakkaalla olemassa olevaan rajapinnan avaamisvelvollisen palvelussa olevaan käyttäjätiliin. Puolesta-asioija ei siis voi vaatia puolesta-asioinnin perusteella mitään sellaisia etuja, joita palvelun asiakas itsekään ei saa. Avaamisvelvollisen ei siis liikennepalvelulain velvoitteen perusteella tarvitse puolesta-asioinnin kautta myydä tuotteita palvelun asiakkaalle tarjottua hintaa halvemmalla tai maksaa puolesta-asioijalle komissiota. Osapuolet voivat sopia lain velvoitetta laajemmasta yhteistyöstä puolesta-asioinnissa.

Puolesta-asioinnissa on siten kyse siitä, että asiakas pyytää puolesta-asioijan hyödyntämään toisessa palvelussa olevia asiakkaan käyttäjätilin tietoja. Puolesta-asioinnissa on kyse kuitenkin aina kahden liikkumis- tai yhdistämispalvelun välisestä oikeustoimesta, joka perustuu toimijoiden väliseen sopimukseen kyseessä olevan rajapinnan hyödyntämisestä. Puolesta-asioinnin vertailumallia on kuvattu tarkemmin Traficomin puolesta-asioinnin vertailumallin kuvauksessa[2].

Alla on kaaviokuva puolesta-asioinnista.



[2] https://www.liikkumisenrajapinnat.fi/sites/default/files/media/file/Liite%201.1.%20Puolesta-asiointi%20vertailumallin%20kuvaus_.pdf

3 Mitä arviointikriteerit ovat?

Lainsäädännöllinen perusta arviointikriteereille on liikenteen palveluista annetun lain 156 §:n 4 momentissa, jonka mukaan […] edellä 1 momentissa tarkoitetulla liikkumis- tai yhdistämispalvelun tarjoajalla ja näiden puolesta lippu- ja maksujärjestelmästä vastaavalla toimijalla sekä 2 momentissa tarkoitetulla liikkumispalveluun liittyvän alennuksen, korvauksen tai erityisehdon sisältävän lipun liikkeelle laskijalla on kuitenkin oikeus arvioida pääsyyn oikeutetun liikkumis- tai yhdistämispalvelun tarjoajan luotettavuus ennalta asetettujen arviointikriteerien ja ehtojen mukaan. Pääsyä tietoihin ei saa evätä, jos pääsyä hakevalla toimijalla on toimintaan viranomaisen tai viranomaisen valtuuttaman kolmannen osapuolen vastaavaa tarkoitusta varten myöntämä lupa, hyväksyntä, auditointi tai sertifiointi tai sen toiminnan on muutoin osoitettu vastaavan yleisesti käytettyä standardia tai alan yleisesti hyväksyttyjä ehtoja. Jos pääsy evätään, on pääsyä hakevalle toimijalle esitettävä asianmukaisesti perustellut epäämisen syyt.

Edellä mainitun puolesta-asiointivelvoitteen rajapinnan avaamisvelvollisen eli sen toimijan, jonka on avattava myyntirajapintansa, on liikenteen palveluista annetun lain 158 §:n mukaan huolehdittava siitä, että rajapinnan avaaminen voi tapahtua palvelun tietoturvan ja yksityisyyden suojan vaarantumatta.

Jotta avaamisvelvollinen voi täyttää edellä mainitun lain 158 § vaatimukset sekä varmistaa muutoinkin toimivan ja turvallisen puolesta-asioinnin, sillä on oikeus arvioida puolesta-asioijan luotettavuus ennalta asetettujen arviointikriteerien ja ehtojen mukaan.

Avaamisvelvollisen tulee asettaa arviointikriteerinsä ennalta ja niiden tulee olla oikeudenmukaisia, kohtuullisia ja syrjimättömiä. Nämä vaatimukset koskevat sekä yksittäistä luotettavuuden arviointikriteeriä että arviointikriteerejä kokonaisuudessaan. Avaamisvelvollisen pitää pystyä osoittamaan ja perustelemaan, että sen arviointikriteerit ovat tarpeen puolesta-asioijan luotettavuuden arvioinnissa. Jos avaamisvelvollinen epää pääsyä hakevan pyynnön, sen on esitettävä asianmukaisesti perustellut epäämisen syyt pääsyä hakevalle toimijalle.

Arviointikriteerit helpottavat pääsyä hakevaa toimijaa ymmärtämään jo etukäteen, mitä ehtoja sen pitää täyttää, jotta se voisi toimia puolesta-asioijana kyseisen avaamisvelvollisen palvelussa.

Arviointikriteerejä voi myös muuttaa esimerkiksi tilanteessa, jos avaamisvelvollisen omat järjestelmät muuttuvat ja se vaikuttaa puolesta-asioijien luotettavuuden arviointiin. Muutostenkin täytyy täyttää oikeudenmukaisuuden, kohtuullisuuden ja syrjimättömyyden vaatimukset.

4. Esimerkkejä puolesta-asioijan luotettavuuden arviointikriteereistä

Traficomin näkemyksen mukaan avaamisvelvolliset voisivat pääsyä hakevan puolesta-asioijan luotettavuutta arvioidessaan käyttää esimerkiksi seuraavanlaisia arviointikriteereitä:

- Puolesta-asioijan asiakkaiden tunnistamisen luotettavuus
- Puolesta-asioijan käyttäjätilien luotettavuus vertailussa:
  - Tietosisältöjen soveltuvuus vertailuun
  - Tietosisältöjen oikeellisuus/tietojen varmentaminen
- Puolesta-asioijan tietoturva
- Puolesta-asioijan taloudellinen tilanne
- Puolesta-asioijan maine

Edellä luetellut kriteerit eivät muodosta yhtä kokonaisuutta, vaan niitä voi käyttää soveltuvin osin. Luettelo ei ole myöskään tyhjentävä, vaan toimija voi käyttää myös muita kriteereitä, joita katsoo tarpeelliseksi ja välttämättömiksi luotettavuuden arvioimiseksi.

Tietosuojan osalta arviointikriteereissä voidaan edellyttää sitä, että puolesta-asioija pystyy osoittamaan, millaisia toimenpiteitä se on toteuttanut yleisen tietosuoja-asetuksen vaatimusten toteuttamiseksi, esimerkiksi rekisteröityjen informoinnin ja rekisteröityjen muiden oikeuksien toteuttamisesta puolesta-asioijan palvelussa.

4.1 Puolesta-asioijan tunnistamisen luotettavuus

4.1.1 Yleistä tunnistamisesta puolesta-asioinnissa

Liikenteen palveluista annetun lain 156 §:n 3 momentin mukaan edellä 1 ja 2 momentissa tarkoitetun puolesta-asiointitapahtuman yhteydessä saa henkilötietoja käsitellä ainoastaan siinä määrin kuin on tarpeen henkilöllisyyden varmistamiseksi ja puolesta-asiointitapahtuman toteuttamiseksi. Sen lisäksi, mitä muualla laissa säädetään, henkilöllisyys on voitava varmistaa erityisen luotettavalla tavalla, kun puolesta-asiointisuhde perustetaan tai sitä muutetaan olennaisesti. Myös puolesta-asiointitapahtuman yhteydessä henkilöllisyys on voitava varmistaa.

Lainkohtaa koskevassa hallituksen esityksessä HE (145/2017 vp s.237) henkilöllisyyden varmistamisesta lausutaan seuraavaa: "Ehdotetussa 3 momentissa edellytettäisiin, että asiakassuhdetta perustettaessa ja sitä olennaisesti muutettaessa olisi henkilöllisyydestä voitava varmistua erityisen huolellisesti. Myös kunkin puolesta-asiointitapahtuman yhteydessä olisi tämän henkilöllisyyden oikeellisuudesta voitava varmistua. Teknisessä mielessä tähän voitaneen käyttää erilaisia ratkaisuja, kuten tunnisteita, varmenteita tai pseudonyymeja. Toisin kuin PSD2:ssa, vahvaa tunnistamista ei siis vaadittaisi. Lisäksi on kuitenkin huomattava, että

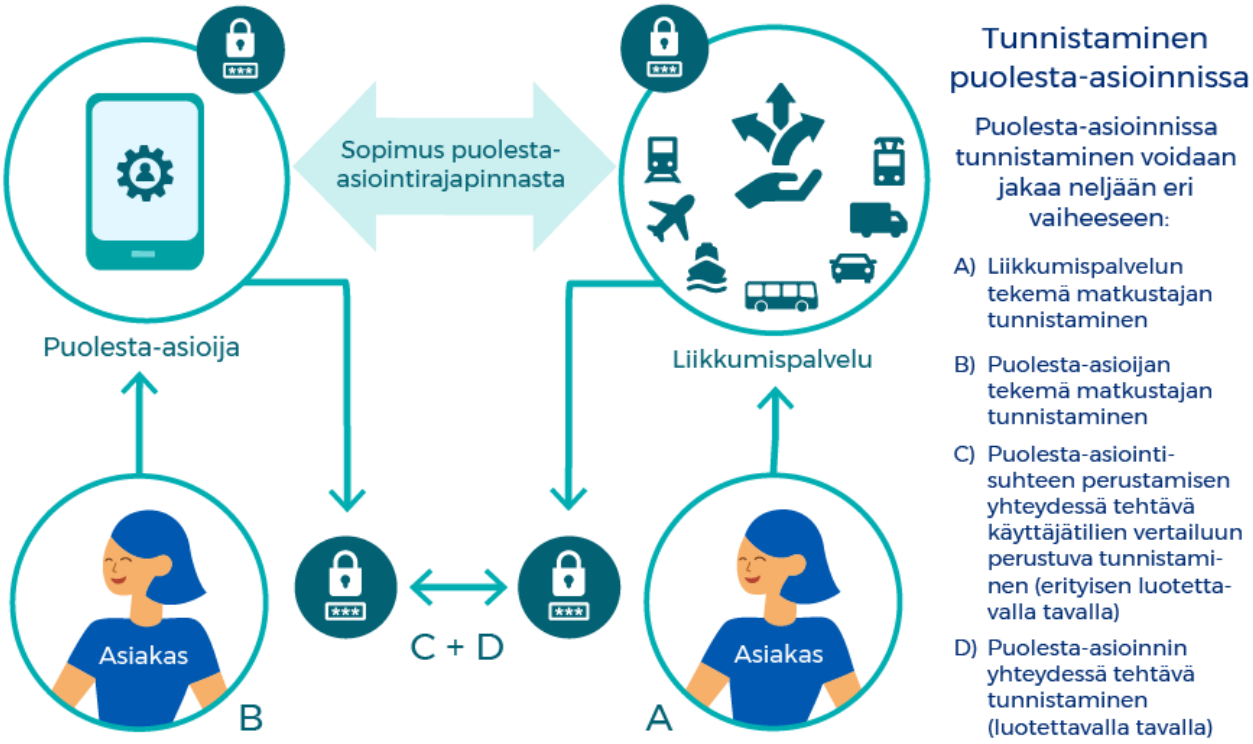
esimerkiksi maksupalveludirektiivi saattaa edellyttää vahvaa sähköistä tunnistamista, mikäli kyse on maksutoimeksiannosta."

Helsingin hallinto-oikeus on 10.12.2020 päätöksellään 20/1905/3 katsonut, että puolesta-asiointivaltuutuksen antamiseen liittyvää vahvaa tunnistamista on voitu pitää kiellettynä kohtuuttomana käyttöehtona.

Liikenteen palveluista annetun lain mukaisen puolesta-asioinnin perusedellytys on, että asiakkaalla on käyttäjätili avaamisvelvollisen palvelussa ja puolesta-asioijalla (HE 145/2017, s.236). Tilejä avatessaan ja myöhempien toimenpiteiden yhteydessä toimijat ovat tunnistaneet asiakkaan.

Tätä perusasetelmaa hyödyntäen puolesta-asiointisuhteen perustaminen onnistuu, jos kahden käyttäjätilin tietoja vertailemalla voidaan asiakkaan henkilöllisyys varmistaa erityisen luotettavalla tavalla hyödyntäen samalla avaamisvelvollisen ja puolesta-asioijan tekemiä asiakkaan tunnistamisia. Puolesta-asioinnissa tunnistaminen tapahtuu siis käyttäjätilien tietoja vertailemalla.

Havainnekuva tunnistamisen eri vaiheista puolesta-asioinnissa.



4.1.2 Puolesta-asioijan tekemän asiakkaan tunnistamisen luotettavuus

Avaamisvelvollinen voi vaatia puolesta-asioijalta riittävää asiakkaan tunnistamisen tasoa, jotta varmistetaan osaltaan oikeiden tilien yhdistyminen, minimoidaan epäonnistuneet vertailut ja mahdolliset väärinkäytökset. Mikäli puolesta-asioijan tekemä asiakkaan tunnistaminen ei täytä ennalta asetettuja luotettavuuden kriteerejä, ei puolesta-asioinnissa voida varmistaa asiakkaan henkilöllisyyttä lain edellyttämällä erittäin luotettavalla tavalla.

Tunnistamisen luotettavuuden kriteereiden on oltava oikeudenmukaisia, kohtuullisia ja syrjimättömiä.

Pääperiaate on, että rajapinnan avaamisvelvollinen voi edellyttää asiakkaan tunnistamiseen käytettäviltä tiedoilta korkeintaan sitä luotettavuuden tasoa, jota itse asiakkailtaan vaatii. Esimerkiksi, jos rajapinnan avaamisvelvollisen käyttäjätileillä asiakkaan tunnistaminen perustuu nimeen ja (varmennettuihin) puhelinnumeroon sekä sähköpostiin, ei puolesta-asioijalta voida vaatia tämän enempää.

Rajapinnan avaamisvelvollisen täytyy avata rajapinta vasta kun puolesta-asioijan tunnistaminen täyttää vaadittavan luotettavuuden tason.

4.2. Puolesta-asioijan käyttäjätilien luotettavuus vertailussa

4.2.1 Yleistä

Kuten edellä on mainittu Traficomin tulkinnan mukaan palvelun käyttäjä ja hänen asiakastilinsä tunnistetaan hyödyntämällä puolesta-asioijan ja rajapinnan avaamisvelvollisen tekemiä tunnistamisia sekä heidän käyttäjätiliensä tietojen vertailua lain edellyttämällä erittäin luotettavalla tavalla.

Puolesta-asioinnissa tulee käsitellä niin vähän henkilötietoja kuin mahdollista, mutta kuitenkin niin, että liikennepalvelulain edellyttämän henkilöllisyyden varmistaminen "erityisen luotettavalla tavalla" ei vaarannu.

Avaamisvelvollisella on oikeus varmistua arviointikriteerien avulla puolesta-asioijan luotettavuus myös käyttäjätilien tietosisältöjen osalta, jotta puolesta-asioinnissa yhdistetään varmasti saman asiakkaan tilit.

Tätä arviointia voidaan tehdä kahdesta eri tarkastelukulmasta: 1) Onko puolesta-asioijalla sellaisia tietosisältötyyppejä, joita voidaan vertailla avaamisvelvollisen käyttäjätileihin? ja 2) Miten näiden tietosisältöjen oikeellisuus varmistetaan?

4.2.2 Puolesta-asioijan käyttäjätilien tietosisältöjen soveltuvuus vertailuun

Jotta vertailu olisi mahdollista, tulisi puolesta-asioijalla on joitain sellaisia asiakasta koskevia tietosisältöjä, jotka ovat myös avaamisvelvollisen käyttäjätileillä. Lisäksi tietosisältöjen pitäisi olla riittävän erottelukykyisiä, jotta ne yksilöivät oikean tilinhaltijan.

Kun arviointikriteerien tulee olla kohtuullisia, ei rajapinnan avaamisvelvollinen voi vaatia useampaa tietosisältöä puolesta-asioijalta kuin on välttämätöntä asiakkaan yksilöimiseksi. Lisäksi toimijoiden täytyy huomioida EU:n yleisen tietosuoja-asetuksen tietojen minimointiperiaate, joka rajoittaa toimijoiden mahdollisuuksia kerätä käyttäjien henkilötietoja.

Avaamisvelvollisen laatiessa arviointikriteerejä vaadittavien tietosisältöjen osalta olisi huomioitava myös asiakkaan käyttökokemus puolesta-asioijan palvelussa. Esimerkiksi avaamisvelvollisen oman palvelun pitkien asiakasnumeroiden, vaatimista vertailutietona voitaisiin lähtökohtaisesti pitää kohtuuttomana, jos asiakas saa selville vain käymällä omalla avaamisvelvollisen palvelussa olevalla käyttäjätilillään.

Eli vertailun tulee tapahtua asiakkaan käyttökokemus huomioon ottaen mahdollisimman pienellä määrällä tietosisältölajeja, mutta näiden vertailuun käytettävien tietosisältöjen pitää yksilöidä asiakas tehokkaasti.

4.2.3 Puolesta-asioijan tietosisältöjen oikeellisuus ja tietojen varmentaminen

Edellä mainitun vertailun toimivuuden edellytys on se, että käyttäjätilien vertailuun käytettävät tiedot ovat oikeita ja ajantasaisia, jotta vertailussa saadaan yhdistettyä saman asiakkaan tietosisällöt toisiinsa. Siten avaamisvelvollinen voi vaatia, että ainakin yhden tietosisällön tulisi olla varmennettu puolesta-asioijan tekemässä tunnistamisessa tai sen yhteydessä. Varmentaminen voi tapahtua eri tavoin riippuen tietotyypistä. Esimerkiksi puhelinnumeron hallinnan voi varmentaa SMS-viestillä, kun taas osoitetiedon voi varmentaa väestötietojärjestelmästä.

Käyttäjätilien tietojen oikeellisuuteen ja ajantasaisuuteen velvoittaa rekisterinpitäjiä myös yleisen tietosuoja-asetuksen vaatimus tietojen täsmällisyydestä.

4.2.4 Avaamisvelvollisen omat tietosisällöt ja niiden varmentaminen

Liikennepalvelulaissa avaamisvelvollista ei velvoiteta muuttamaan käyttäjätiliensä tietosisältöjä tai niiden varmentamistapoja. Lähtökohtana voidaan siten pitää sitä, että avaamisvelvollisen käyttäjätilien tietosisällöt sellaisenaan mahdollistavat myös puolesta-asioinnin. Siten

avaamisvelvollinen ei voi kieltäytyä puolesta-asioinnin toteuttamisesta vedoten siihen, etteivät sen käyttäjätilien tietosisällöt mahdollista puolesta-asiointia tietoturvaa ja tietosuojaa vaarantamatta.

Avaamisvelvollinen voi kuitenkin, esimerkiksi tietosuojasyistä, nähdä tarpeelliseksi parantaa omia puolesta-asiointiin käytettäviä käyttäjätilejään esimerkiksi tietojen varmentamisen taikka tietosisältöjen osalta. Tietosuojalainsäädäntö edellyttää sekä tietojen minimointia, mutta samalla myös tietojen eheyttä sekä luottamuksellisuutta ja täsmällisyyttä. Tietosuojalainsäädäntö ei estä sitä, että mikäli käyttäjätileillä jo olevien tietojen ei voida katsoa täyttävän liikennepalvelulain vaatimusta asiakkaan henkilöllisyyden varmistamisesta, voidaan puolesta-asioinnin toteuttamiseksi käsitellä myös uusia, mutta vain välttämättömiä tietosisältöjä.

4.3 Puolesta-asioijan tietoturva arviointikriteerinä

4.3.1 Luottamuksellisuus, eheys ja saatavuus

Tietoturvallisuuden ylläpidolla tarkoitetaan niitä teknisiä ja organisatorisia toimenpiteitä, joita toimija toteuttaa verkko- ja tietojärjestelmien eheyden, käytettävyyden ja tiedon luottamuksellisuuden turvaamiseksi.

Luottamuksellisuus (confidentiality) tarkoittaa sitä, että tietoon pääsevät käsiksi vain siihen oikeutetut. Tämä edellyttää käytännössä sekä tietojen että tietoon oikeutettujen määrittelyä riittävällä tasolla.

Eheys (integrity) tarkoittaa sitä, että tietoa tai järjestelmää ei päästä muuttamaan tai hävittämään oikeudettomasti koko sen elinkaaren aikana ja että mahdolliset oikeudettomat muutokset havaitaan.

Saatavuus (availability) tarkoittaa sitä, että tieto tai järjestelmä on käytettävissä silloin, kun sitä tarvitaan. Saatavuus tarkoittaa myös käyttötarpeeseen nähden riittävää kapasiteettia, sekä tarvittaessa myös suojautumista tahattomilta ja tahallisilta palvelunestohyökkäyksiltä.

4.3.2 Puolesta-asioijan tietoturvan tason vaikuttavat tekijät

Suojattavan tiedon tunnistaminen ja riski

Jotta tietoa ja tietojärjestelmiä pystyy suojaamaan tehokkaasti ja taloudellisesti, on tunnistettava mitkä ovat keskeiset suojattavat asiat ja toisaalta niihin kohdistuvat olennaiset uhkat. Kaiken suojaaminen kaikilta uhkilta on mahdotonta ja/tai liian kallista. Tietoturva- ja tietosuojakontrollien oikeaan mitoittamiseen tarvitaankin järjestelmällistä

uhka-analyysiä, jossa arvioidaan toimintaan liittyviä riskejä tyypillisesti niiden todennäköisyyksien ja seurausten vakavuuksien kautta.

Avaamisvelvollinen voi edellyttää puolesta-asioijalta teknisiä ja organisatorisia toimenpiteitä tietoturvan ylläpitämiseksi suhteutettuna uhan vakavuuteen ja todennäköisyyteen, toimenpiteistä aiheutuviin kustannuksiin sekä käytettävissä oleviin teknisiin ja organisatorisiin kontrolleihin uhan torjumiseksi. Riskejä ei yleensä voi vaatia kokonaan poistettavaksi, mutta sen voi vaatia laskettavan hyväksyttävälle tasolle (jäännösriski).

Uhan vakavuuden arvioinnissa on otettava huomioon ainakin:

1. Suojattavan tiedon luonne (esimerkiksi henkilötietojen käsittelyn tai sertifikaattien avaintenhallinnan vaatimukset),

2. suojattavan toiminnon kriittisyys järjestelmän eheyden kannalta ja

3. mahdollisten henkilötietovahinkojen sekä taloudellisten ja muiden vahinkojen suuruus uhan toteutuessa.

Uhan todennäköisyyden arvioinnissa on otettava huomioon ainakin:

1. Vallitseva ajantasainen tietämys online-verkkopalveluista,

2. sekä niiden taustalla olevaan alustainfrastruktuuriin kohdistuvista tietoturvauhkista.

Mitä suojataan erityisesti puolesta-asioinnissa?

Käyttäjätilien vuoksi asiakkaiden henkilötietojen luottamuksellisuutta luottamuksellisuuden ja eheyttä eheyden suojaaminen korostuvat puolesta-asioinnissa (tietosuoja). Erityispiirteenä on asiakkaiden tilien yhteenkytkemisen kohdistuminen puolesta-asioijan ja liikkumispalvelun tarjoajan välillä oikein.

Muita suojattavia hyveitä voivat olla esimerkiksi järjestelmien sisältämät liikesalaisuudet ja rahaliikenteen eheys, ylipäänsä tietojärjestelmien eheinä säilyminen myös virhetilanteissa ja vähintäänkin tavanomaisissa verkkohyökkäyksissä. Tietojärjestelmien ja palveluiden saatavuuden tavoitetason määrittämisessä on usein hyödyllistä ajatella katkostilanteista aiheutuvien vahinkojen (esim. taloudelliset ja/tai mainetappiot) suuruutta ja suhteuttaa saatavuuden suojaustoimenpiteet sen mukaisesti. Kuten jäännösriskiäkään ei yleensä ole järkevää viedä nollaan, ei 100% saatavuuttakaan yleensä kannata mm. siitä aiheutuvista kustannuksista johtuen tavoitella.

4.3.3 Mitä avaamisvelvollinen voi arviointikriteereissä vaatia puolesta-asioijan tietoturvallisuudelta?

Vaatimukset voi karkeasti jakaa kahteen osa-alueeseen: turvallisuuden huomioimiseen yleisesti organisaation toiminnassa (hallinnollinen turvallisuus) ja puolesta-asiointiin liittyvien tietojärjestelmien tekniseen turvallisuuteen.

1) Hallinnolliselle puolelle voidaan katsoa kuuluvan oman toiminnan realistisen ja systemaattisen uhka-analyysinä, jonka perusteella jäännösriskit on saatu laskettua hyväksyttävälle tasolle. Organisaatiolla tulee mm. olla turvallisuuteen liittyen keskeiset vastuuhenkilöt ja toimintaprosessit määriteltynä ja jalkautettuna päivittäiseen toimintaan.

2) Puolesta-asiointiin liittyvien tietojärjestelmien tekniseltä turvallisuudelta voidaan vaatia yleisten hyvien tietoturvakäytäntöjen noudattamista konkreettisella tasolla. Tällaisiin sisältyy yleisellä tasolla mm. seuraavia (listaus ei ole tyhjentävä):

   - Ajantasaiset tietoturvapäivitykset järjestelmissä
   - Käyttöoikeuksien hallinnan hyvät käytännöt
   - Asianmukaiset tietoturvakovennukset ja ylläpitokäytännöt
   - Tietoliikenteen riittävä suojaus (salaus/luottamuksellisuus, eheys, vastapuolen luotettava tunnistus)
   - Selkeästi määritellyt, turvalliset, robustit, ja testatut rajapintatoteutukset

Yllä mainittujen vaatimusten täyttymisestä on mahdollista myös vaatia näyttöä puolesta-asioijalta. Tällaisena näyttönä voi toimia esimerkiksi kohtuullisen tuoreet itsearvioinnit tai kolmansien osapuolien tekemät arvioinnit. (Puoli)automaattisten tietoturvatyökalujen tuottamat raportit voivat myös olla yksi tapa osoittaa teknistä turvallisuustasoa.

Kumpikaan osapuoli ei kuitenkaan voi ulkoistaa omia tietoturva- ja tietosuojavastuita toiselle osapuolelle. Esimerkiksi avaamisvelvoitetun on huolehdittava oman rajapintatoteutuksensa suojaamisesta asianmukaisesti.

Tietoturvallisuuden arviointikriteeristöt

Tietoturvallisuuden arvioinnin kattavuuden ja vertailtavuuden vuoksi on mahdollista käyttää hyödyksi jo olemassa olevia kriteeristöjä ja työkaluja. Näitä löytyy sekä yleisluontoisempia hallinnollisen turvallisuuden varmistamiseen suunniteltuja, että teknisempiä tietojärjestelmien tarkastukseen suunniteltuja kriteeristöjä.

Esimerkkejä yleisluontoisemmista ovat muun muassa:

- ISO 27000 -sarja
- Traficom Kybermittari

Esimerkkejä teknisemmistä ovat muun muassa:

- OWASP Top Ten Web Application Security Risks, Mobile Security Testing Guide
- PCI DSS

Valtionhallinto on julkaissut myös kriteeristöjä ja ohjeita, joiden lähtökohtana on tyypillisesti viranomaisen luokitteleman tiedon suojaaminen. Näitä ovat mm. Kansallinen turvallisuusauditointikriteeristö (KATAKRI), Pilvipalveluiden turvallisuuden auditointikriteeristö (PiTuKri) ja lukuisat VAHTI-ohjeet. Sellaisenaan näiden soveltuvuus puolesta-asioijan tietoturvan arviointiin on kuitenkin rajallinen em. kriteeristöjen paikoitellen korkean vaatimustason vuoksi.

4.4 Taloudelliset arviointikriteerit

Taloudellisten arviointikriteerien tarkoituksena on varmistua siitä, että rajapintojen avaamista pyytävällä on riittävät taloudelliset resurssit puolesta-asioinnin turvalliseen toteuttamiseen.

4.4.1 Elinkeinonharjoittajaksi rekisteröitymisen vaatimus arviointikriteerinä

Lähtökohtaisesti laissa on velvollisuus avata rajapinta kaikille, mutta avaamisvelvoitetulla on kuitenkin oikeus arvioida toisen toimijan luotettavuutta taloudellisesta näkökulmasta.

Rajapintojen avaamista pyytävällä yritykseltä voidaan vaatia Y-tunnusta Suomessa tai muuta osoitusta siitä, että yritys on rekisteröitynyt elinkeinonharjoittajaksi muualla EU-alueella. EU:ssa on ainakin käytössä ns. VAT -numero, jolla voidaan tunnistaa hakijan ALV -velvollisuus. Verohallinnon ohjeiden mukaisesti "Kun arvonlisäverovelvollinen yritys käy kauppaa toisessa EU:n jäsenvaltiossa arvonlisäverovelvolliseksi rekisteröityneen yrityksen kanssa, yritys merkitsee laskuun Y-tunnuksensa lisäksi alv-numeronsa."

Suomessa toimivan yrityksellä tai yhteisöllä on velvollisuus ilmoittaa perustamisesta sekä toiminnan aikana tapahtuvista muutoksista ja toiminnan lopettamisesta Patentti ja rekisterihallitukseen (PRH) ja Verohallintoon (PRH:n kaupparekisteriin, yhdistysrekisteriin tai säätiörekisteriin +verohallinnon arvonlisäverovelvollisten rekisteriin, ennakkoperintärekisteriin ja työnantajarekisteriin).

Edellä mainituista PRH:n ja verohallinnon rekistereistä saatavat otteet ja todistukset antavat viitteitä toimijan luotettavuudesta myös taloudellisesta näkökulmasta.

4.4.2 Riittävät taloudelliset resurssit puolesta-asioinnin toteuttamiseen

Puolesta-asioijalta voidaan vaatia riittäviä taloudellisia edellytyksiä harjoittaa turvallisesti toimintaa, jota varten rajapinnat avataan. Riittävien taloudellisten resurssien arvioinnissa voidaan käyttää esimerkiksi seuraavia kriteerejä:

> Yrityksellä ei ole todennäköisiä taloudellisia edellytyksiä harjoittaa toimintaa mikäli:
>
> - Yhtiö on menettänyt yli puolet merkitystä osakepääomastaan (osakeyhtiö) tai yli puolet tilinpäätöksen mukaisista omista varoistaan (ay tai ky) kertyneiden tappioiden vuoksi.
>
> - Yhtiö on asetettu konkurssi- tai yrityssaneerausmenettelyyn maksukyvyttömyyden vuoksi, taikka se voitaisiin tilanteensa johdosta sellaiseen asettaa.

4.5 Yrityksen maine luotettavuuden arviointikriteerinä

Yrityksen maineeseen perustuvat arviointikriteerit voivat osaltaan varmistaa, ettei puolesta-asioijan toimintaan liity väärinkäytöksiä tai vakavia puutteita.

Yrityksen mainetta arvioivissa kriteereissä korostuu avaamisvelvollisen näyttövelvollisuus, jos se kieltäytyy avaamasta rajapintaa puolesta-asioijalle näillä perusteilla. Tältäkin osin kriteerien tulee olla oikeudenmukaisia, kohtuullisia ja syrjimättömiä. Esimerkiksi harkinnassa saa ottaa huomioon virheitä tai laiminlyöntejä vain kohtuullisen pituiselta ajanjaksolta. Maineeseen kohdistuvilla kriteereillä on yhtymäkohtia hankintalain harkinnanvaraisiin poissulkemisperusteisiin.

Yrityksen maineetta arvioivat kriteerit voidaan jakaa yleisiin ja kahdenvälisiin perusteisiin olla avaamatta rajapintaa vastapuolen maineen perusteella.

Avaamisvelvollisen on katsottava puolesta-asioija kuitenkin luotettavaksi toimijaksi, jos puolesta-asioija on toteuttanut konkreettiset tekniset sekä organisaatioon ja henkilöstöön liittyvät toimenpiteet, joilla voidaan estää uudet rangaistavat teot, virheet tai laiminlyönnit. Tästä näyttövelvollisuus on puolesta-asioijalla.