ETÄTUNNISTAMISEN MENETELMÄT ASIAKKAAN TUNNISTAMISESSA JA HENKILÖLLISYYDEN TODENTAMISESSA

Etätunnistaminen

Tarve digitaaliselle etätunnistamiselle on kasvanut jo pitkään, kun palveluita tarjotaan digitaalisesti sekä kotimaassa että rajat yli tapahtuvana palveluntarjontana. Tämänhetkinen sosiaalisen etäisyyden ylläpitäminen on omiaan kiihdyttämään kehitystä entisestään.

Etätunnistamistilanteessa asiakas ei ole fyysisesti läsnä asiakkuuden alkamishetkellä tai liiketoimen suorittamisen yhteydessä. Tällöin ilmoitusvelvollinen tunnistaa asiakkaan hankkimalla asiakkaan tuntemistietoja ja todentamalla tämän henkilöllisyyden valitsemaansa etätuntemisen menetelmää tai useampia menetelmiä hyödyntäen.

Riskiperusteinen lähestymistapa

Ilmoitusvelvollinen luo riskiperusteisen lähestymistavan perusteella omat asiakkaan tuntemiseen liittyvät menettelytapansa ja vähimmäiskriteerit, joita se noudattaa asiakassuhteissaan. Etätunnistamisen riskiperusteisessa arvioinnissa ilmoitusvelvollisen tulee kiinnittää huomiota erityisesti oman toiminnan luonteeseen ja toimialansa riskillisyyteen, sekä toiminnan laajuuteen ja asiakkaiden maantieteelliseen sijaintiin. Ilmoitusvelvollisen tulee riskiarviointiin perustuen arvioida, mitkä rahanpesulaissa säädetyt etätunnistamiseen liittyvät tehostetut tuntemisvelvollisuuden lisätoimet ovat tarpeen, jotta ilmoitusvelvollinen voi vähentää etätunnistamiseen mahdollisesti liittyvää suurempaa rahanpesun ja terrorismin rahoituksen riskiä.

Etätunnistamiseen liittyvä tehostettu tuntemisvelvollisuus

Jos asiakas ei ole läsnä tunnistettaessa ja henkilöllisyyttä todennettaessa (etätunnistaminen) ilmoitusvelvollisen tulee rahanpesun ja terrorismin rahoittamisen riskin vähentämiseksi

- todentaa asiakkaan henkilöllisyys hankkimalla lisäasiakirjoja tai -tietoja luotettavasta lähteestä
- varmistaa, että liiketoimeen liittyvä suoritus tulee luottolaitoksen tililtä tai se maksetaan tilille, joka on aiemmin avattu asiakkaan nimiin
- todentaa asiakkaan henkilöllisyys laissa[1] tarkoitetulla tunnistusvälineellä tai sähköisen allekirjoituksen hyväksytyllä varmenteella[2] tai muun sähköisen tunnistamistekniikan avulla, joka on tietoturvallinen ja todisteellinen.

Etätunnistamistilanteissa luotettava asiakkaan tunnistaminen ja henkilöllisyyden todentaminen saattaa edellyttää useiden eri menetelmien yhdistämistä ja lisätietojen pyytämistä asiakkaalta sekä luotettavista lähteistä varsinkin silloin, kun kyseessä on rajat yli tapahtuva palveluntarjonta ja asiakassuhde aloitetaan toisessa valtiossa olevan asiakkaan kanssa. Ilmoitusvelvollisen vastuulla on arvioida tarpeelliset tehostetun tuntemisvelvollisuuden lisätoimenpiteet.

[1] Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
[2] Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta

Etätunnistamisen menetelmiä

Asiakkuuden perustamisvaiheessa asiakas etätunnistetaan ja hänen henkilöllisyytensä todennetaan jotain etätunnistamisen menetelmää tai useamman menetelmän yhdistelmää hyödyntäen. Ilmoitusvelvollisella tulee olla käytössään menetelmiä, joilla se voi tarkistaa asiakkaan etätunnistamisen välityksellä antamia tietoja. Asiakkaan antamia tuntemistietoja voi tarkistaa luotettaviksi lähteiksi luokitelluista julkisista rekistereistä saatavien tietojen avulla. Tällaisia rekistereitä ovat esimerkiksi

- Patentti- ja rekisterihallituksen ylläpitämät rekisterit, kuten kaupparekisteri ja yhdistysrekisteri
- Digi- ja väestöviraston ylläpitämä väestötietorekisteri
- Suomen asiakastieto Oy:n ylläpitämä luottotietorekisteri[3].

Ilmoitusvelvollisen on syytä huomioida, että muissa valtioissa ei aina ole saatavilla tietoa vastaavista julkisista rekistereistä. Mikäli tietoa on saatavilla, ilmoitusvelvollisen tulee arvioida ulkomaisesta rekisteristä saadun tiedon ajantasaisuutta, luotettavuutta ja käytettävyyttä. Luotettavista lähteistä saatujen selvitysten lisäksi asiakkaan tuntemisessa voidaan hyödyntää ilmoitusvelvollisen riskiarvioon perustuen esimerkiksi yksityisen palveluntarjoajan tarjoamia sosiaalisen median tunnuksia, sähköpostiosoitetta, puhelinnumeroa sekä palvelua, jossa toinen palveluntarjoaja on jo tunnistanut asiakkaan esimerkiksi luottokorttitietoja hyödyntäen.

Tunnistuslain mukaiset vahvat sähköiset tunnistusvälineet

Liikenne- ja viestintävirasto Traficom valvoo tunnistuslain[4]noudattamista. Vahvoja sähköisiä tunnistuspalveluita ovat tällä hetkellä

- pankkien verkkopankkitunnukset
- teleyritysten mobiilivarmenteet
- Digi- ja väestötietoviraston kansalaisvarmenne poliisin myöntämällä henkilökortilla
- eräät muut tunnistusvarmenteet
- erilaisilla organisaatiokorteilla rekisteröidyt tunnistusvälityspalvelut.

Vahvoille sähköisille tunnistusvälineille on säädetty tarkat vaatimukset, kuten esimerkiksi velvollisuus tehdä ilmoitus ennen toiminnan aloittamista Traficomille, auditointivelvollisuus ja häiriöilmoitusvelvollisuus. Traficom pitää yllä luetteloa lain vaatimukset täyttävistä tunnistuspalveluista.[5]

Muu sähköinen tunnistamistekniikka

Teknologian kehittymisen myötä etätunnistamisratkaisuissa on mahdollista hyödyntää esimerkiksi tekoälyä sekä lohkoketjuteknologian käyttöä, mikä mahdollistaa uudenlaisia tapoja rakentaa palveluita ja tallettaa dataa. Asiakkaan etätunnistamisessa tulisi hyödyntää eri datalähteistä saatuja tietoja vertailemalla ja yhdistelemällä niitä asiakkaalta saatuihin tietoihin sekä luotettavien lähteiden kautta saatuihin tietoihin.

[3] luottotietolain (527/2007) mukaisissa tarkoituksissa.
[4] laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009
[5] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

Tekoälyä hyödynnetään tällä hetkellä ainakin jo kasvojen tunnistamisessa ja fyysisten henkilöpapereiden oikeellisuuden todentamisessa. Digitaalisessa ensitunnistamisessa[6] asiakkaat voivat tunnistaa itsensä mobiililaitteella, passilla (tai jollain muulla henkilöllisyystodistuksella) ja omilla kasvoillaan. Markkinoilla on sovelluksia, jotka todentavat henkilöllisyystodistuksien aitoutta tarkastamalla turvaominaisuuksia, kuten hologrammien aitoutta. Biometrisistä passeista sovelluksen on mahdollisuus lukea passin siru. Sovellus todentaa asiakkaan kasvot asiakkaan ottamasta kasvokuvasta, ja asiakkaan elävyys tunnistetaan liikkuvan kuvan avulla.

Etätunnistamisprosessin läpinäkyvyys ja tunnistamistietojen säilyttäminen

Etätunnistamisprosessin tulee olla läpinäkyvä (tietoturvallista ja todisteellista) ja sen jälkikäteisen tarkastelun on oltava mahdollista. Asiakkaan tietoja tulee säilyttää rahanpesulaissa säädetyn säilytysajan mukaisesti huomioiden tietosuoja ja tietoturva (luottamuksellisuus, eheys ja saatavuus). Tunnistettavan henkilön tulee antaa suostumuksensa etätunnistamiseen, ja myös suostumus tulee säilyttää. Ilmoitusvelvollisen tulee harkita tarkkaan rajaus siitä, mitkä henkilöllisyyden todentamisasiakirjat ja -tiedot hyväksytään etätunnistamisessa, ja varmistua siitä, että asiakirjat ovat vahingoittumattomia ja muokkaamattomia. Riskiperusteiseen arviointiin pohjautuen, etätunnistamisessa voi olla perusteltua pyytää joiltakin asiakkailta laajemmin lisäselvityksiä ja tarkempia tietoja.

Etätunnistamisen ulkoistaminen

Etätunnistamista ostetaan usein alihankintana ulkoiselta palveluntarjoajalta. Etätunnistamisen ulkoistaminen edellyttää ilmoitusvelvolliselta aina etätunnistamiseen liittyvien riskien arviointia ja huolellista suunnittelua. Sopimuksissa tulee sopia sekä menettelytavoista että kunkin osapuolen tehtävistä ja vastuista. Lisäksi ilmoitusvelvollisen tulee edellyttää, että asiakassuhdetta koskeva dokumentaatio toimitetaan ilmoitusvelvolliselle tai se on ilmoitusvelvollisen saatavilla viivytyksettä koko asiakassuhteen ja rahanpesulaissa säädetyn säilytysajan.

Ilmoitusvelvollisen on huolehdittava riittävästä omasta teknisestä osaamisesta, johdon ymmärryksestä ja jatkuvuuden hallinnasta etätunnistamisen ulkoistamisessa. Tällöin ilmoitusvelvollisella tulee olla teknistä taitoa ja osaamista ohjata ja valvoa ulkoistettua toimintoa. Ilmoitusvelvollisella tulee olla myös riittävä ymmärrys ulkoistetusta toiminnosta, jotta se voi tarvittaessa ottaa ulkoistetun etätunnistamisen itselle hoidettavakseen tai siirtää sen uudelle palveluntarjoajalle. Ilmoitusvelvollinen on vastuussa ulkoistamansa palvelun laadun seuraamisesta.

Vastuu asiakkaan tuntemisesta sekä jatkuvan seurannan ja selonotto- ja ilmoitusvelvollisuuden noudattamisesta säilyy ilmoitusvelvollisella kaikissa tilanteissa.

Tämä asiakirja on laadittu rahanpesun ja terrorismin rahoittamisen estämisen kansallisen viranomaisyhteistyöryhmän perustamassa rahanpesulain mukaisten valvojien alatyöryhmässä 29.6.2021. Lisätietoja asiakirjan sisällöstä antaa Finanssivalvonta. Jos sinulla on muuta kysyttävää aiheesta, käänny oman rahanpesulain mukaisen valvojasi puoleen.

[6] *ensitunnistamisella* tarkoitetaan tunnistusvälineen hakijan henkilöllisyyden todentamista välineen hankkimisen yhteydessä. Katso laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (7.8.2009/617)