22.2.2016

LVM LAUSUNTOPYYNTÖ LVM/2005/03/2015 (VAHVASTA SÄHKÖISESTÄ TUNNISTAMISESTA JA SÄHKÖISISTÄ ALLEKIRJOITUKSISTA ANNETUN LAIN SEKÄ ERÄIDEN SIIHEN LIITTYVIEN LAKIEN MUUTTAMISESTA)

OP Ryhmä kiittää mahdollisuudesta antaa lausunto koskien luonnosta Valtioneuvoston asetukseksi sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta.

Pykäläkohtaisia kommentteja

8b § Tunnistusmenetelmässä käytettävät todentamistekijät

Selkeyttävänä ehdotuksena mielestämme todentamistekijöiden luettelossa olisi hyvä mainita ensin periaate ja vasta sitten esimerkkejä menetelmistä,

1) tiedossa oloon perustuva todentamistekijä *(salasana tai jokin muu sellainen, mitä tunnistusvälineen haltija tietää);*

2) hallussapitoon perustuva todentamistekijä *(sirukortti tai jokin muu sellainen, mitä tunnistusvälineen haltijalla on hallussaan);*

3) luontainen todentamistekijä *(sormenjälki tai jokin muu tunnistusvälineen haltijan yksilöivä ominaisuus).*

Pykälä sisältää uutena vaatimuksena: "Jokaisessa tunnistusmenetelmässä on käytettävä sellaista dynaamista todentamistekijää, joka voidaan muuttaa jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamistapahtumassa". Dynaamisuus määritellään komission täytäntöönpanoasetuksessa (EU) 2015/1502 (sähköisen tunnistamisen varmuustasoasetus). Asetuksen määritelmä kuuluu: 'dynaamisella todentamisella' tarkoitetaan sähköistä prosessia, jossa käytetään salausta tai muita tekniikoita, joiden avulla voidaan pyynnöstä luoda sähköinen todiste siitä, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot, sekä muuttaa sitä jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa".

Vaatimus dynaamisen todentamistekijän käytöstä voi, tulkinnasta riippuen, olla ongelmallinen. Pankkien tällä hetkellä yleisesti hyödyntämissä nk. salasanalista-ratkaisuissa dynaamisuuden vaatimus toteutuu. Esim. OPn nykyisessä ratkaisussa yhteys palveluun on salattu ja varmenteella suojattu (eli käytetään salausta). Avainlukulistassa avainlukuhaaste poimitaan satunnaisesti ja avainluvut ovat kertakäyttöisiä (eli voidaan muuttaa jokaisessa todentamistapahtumassa) ja lisäksi voidaan pyytää dynaamisesti tekstiviestikanavaa pitkin (eli kyky hakea asetusta laajemmin lisävarmuus sille, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot). Lisäksi valvomme jatkuvasti tunnusten käyttöä ja reagoimme poikkeamiin.

Dynaamisuuden tulkinta voi olla haaste varmennepohjaisille ratkaisuille, sillä varmenteessa taustalla on julkiseen ja yksityiseen avaimeen perustuva ratkaisu, eivätkä nämä avaimet vaihdu joka todentamistapahtumalla, eikä se ole tarkoituksenmukaistakaan. Kotimaassa tällaisia ratkaisuja ovat esim. HST-kortti ja Mobiilivarmenne, sillä ne perustuvat muuttumattomiin tietoihin (varmenne ja PIN).

Jos varmennepohjaisesti (PKI) halutaan tehdä dynaaminen tunnistustapahtuma, tehdään itse asiassa todentamistekijän sähköinen allekirjoitus varmenteella. Ja todentamistekijä on tällöin esim. joku generoitu tieto (esim. one-time-password). Tekeminen edellyttää tällöin esim. mobiilivarmenteella allekirjoitus PIN:n käyttöä - ei tunnistus PIN:n. Tämän viestiminen asiakkaalle on haasteellista.

Käytännössä, ainakin ahtaasti tulkittuna, dynaamisen todentamistekijän vaatimus ohjaa käyttöä OTP tyyppisiin ratkaisuihin (mitä käytännössä myös avainlukulista on) tai muutamien sirukorttivalmistajien toteuttamiin OTP tyyppisiin haaste - vaste ratkaisuihin. Myös biometriikan hyödyntäminen olisi haastavaa, sillä nykyratkaisuissa ei toteudu tuo muuttuvan - dynaamisen todentamistekijän vaatimus.

Jokaisen vahvoja sähköisiä tunnisteita tarjoavan toimijan pitäisi saada selkeä arvio Viestintävirastolta vaatimuksenmukaisuudesta, sekä ohjausta millaisilla muutoksilla vaatimuksien täyttämiseen päästään ja millaisilla siirtymäajoilla muutoksia on tehtävä. On syytä huomata, että pankkien käyttämät tunnuslukulistaratkaisut poikkeavat toisistaan eli arviointi on tehtävä yritys ja ratkaisukohtaisesti.

16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä.

Pykälässä käsitellään velvollisuutta ilmoittaa palvelun toimivuuteen, tietoturvaan tai sähköisen identiteetin käyttöön kohdistuvista **merkittävistä** uhkista tai häiriöistä. Käytännössä valtaosa väärinkäytöksistä kohdistuu **yksittäisiin** ihmisiin ja lain pitäisi luoda mekanismi sille, miten yksittäisten identiteettivarkauksien uhrien osalta menetellään. Yksittäistapauksenkin pitää olla merkittävä. Olisi myös määriteltävä, mikä on tiedotuskynnyksen ylittävän merkittävän uhan tai häiriön raja, muutoin toteuttaminen voi muodostua haastavaksi ja kalliiksi

Käytännön toiminnan kannalta Valtiolla pitäisi olla tarjota luottamusverkoston jäsenille rekisteri, jonne voisi ilmoittaa kadonneista tai varastetuista tai kopioiduista fyysisistä tunnistamisasiakirjoista, sekä vääriin käsiin päätyneistä sähköisistä tunnisteista. Nykytilassa varastetulla passilla voi avata eri toimijoiden parissa lukuisia vahvoja sähköisiä tunnisteita. Myös pykälien 25 ja 26 tulisi ulottua myös passiin ja henkilökorttiin, sillä ne ovat kaikkein riskipitoisimmat dokumentit, jotka voivat kadota.

Olisi myös mahdollistettava se, että pankit voisivat vaihtaa luottamusverkostossa riskienhallinnallisesti tarpeellisia tietoja muiden verkoston jäsenten kanssa ilman, että pankkisalaisuuteen liittyvä säätelyä loukataan.

16 § keskittää organisoinnin Viestintävirastolle. Kun kyse on tietomurrosta, identiteettivarkaudesta tai vastaavasta rikoslakiin kirjatusta teosta, valtionhallinnon koordinoinnin pitäisi tapahtua esitutkintaviranomaisen taholta. Malli sisältää riskin siitä, että rikostutkintaan liittyviä tietoja päätyy tarpeettomasti Viestintäviraston ja luottamusverkoston jäsenten tietoon. Tulisi erottaa toisistaan tekninen häiriötilanne ja rikostutkinta.

17 §Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen

Näkökulmastamme on haasteellista, että sähköinen identiteetti on periaatteessa ikuinen, mutta fyysiset tunnistamisasiakirjat (passi, henkilökortti) ovat voimassa vain viisi vuotta. Mikäli tämä tarkoittaa, että ensitunnistamiset tulee tehdä viiden vuoden välein uusiksi, aiheuttaa se valtavan työ- ja kustannuspaineen fyysisestä ensitunnistamisesta vastaaville tahoille. Nykyinen fyysisten tunnistusasiakirjojen voimassaoloaika ja hintataso voivat olla haasteellisia joillekin kohderyhmille jos ajokortti rajataan pois.

Pankkien kannalta erityisen haasteen muodostava ne henkilöt, joille on toimialan erityssääntelyn – oikeus peruspankkipalveluihin eli nk. tilidirektiivi – myönnettävä perusmaksutili siihen liittyvine palveluineen. Miten toimitaan niiden henkilöiden osalta, joille on tarjottava peruspalvelut, mutta joilla ei ole mitään tunnistamisasiakirjaa?

Ensitunnistamista koskevassa 17 §:ssä on rajoitettu ensitunnistamiseen kelpaavia todentamisasiakirjoja. Ensitunnistamista koskevassa pykälässä on selvästi todettu, että tunnistusvälineen tarjoaja voi halutessaan hyväksyä ensitunnistamisessa myös muun

kuin ETA-alueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämät passit tai henkilökortit.

Lain ja lain perusteluiden mukaan tunnistusvälineen tarjoajan ei tarvitse hyväksyä muiden maiden viranomaisten myöntämiä passeja. Tästä nimenomaisesta säännöksestä huolimatta syrjintälautakunta (nyk. yhdenvertaisuuslautakunta) on todennut pankin syrjivän asiakasta, kun se ei ole hyväksynyt esitunnistamisessa hakijan esittämää muun kuin ETA-valtion, Sveitsin tai San Marinon viranomaisen myöntämää passia. Tunnistusvälineen tarjoajan näkökulmasta on kestämätöntä, että lain nimenomaisesta sanamuodosta riippumatta viranomainen voi tulkita sen noudattamisen syrjiväksi. Tämän vuoksi 17 §:n osalta tulee tarvittaessa hankkia lausunto siitä, voiko se yksittäistapauksissa olla syrjivä.

20 §Tunnistusvälineen myöntäminen

Luonnollisen henkilön ja oikeushenkilön tunnistusvälineiden kytkös on toteutettava sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdan 2.1.4 mukaisesti. Tunnistusvälineen on oltava henkilökohtainen. Tämä edellyttää, että tunnistusväline on aina kytkettävissä sekä oikeushenkilöön, sekä oikeushenkilöä edustavaan luonnolliseen henkilöön (tunnisteen haltija). Tällä voi olla merkittäviäkin vaikutuksia joidenkin prosessien osalta. Pahimmillaan tämä vaatimus voi johtaa siihen, että esim. meklarilla on 1-n tunnistusvälinettä, eli vähintään yksi / asiakasyritys.

26 § Tunnistusvälineen tarjoajan oikeus peruuttaa tai estää tunnistusvälineen käyttö.

Kokonaisuudessa pitäisi huomioida PSD2:n 3. osapuolien palveluntarjoajien asemoituminen, sekä EBAn SecuRE Internet ja Mobile Payments dokumenttien vaikutus. Mm. EBAn palvelun monitorointiin liittyvät velvoitteet ovat hankalasti yhtyeensovitettavissa luottamusverkostomalliin.

EBAn ohjeistuksen "Asiakkaalle toimitettaviin tunnistusvälineisiin ja/tai -ohjelmistoihin rekisteröityminen ja hankinta"- osiossa todetaan, että maksupalveluntarjoajan tulisi varmistaa, että internet-maksupalvelun käyttämiseksi vaadittavien tunnistusvälineiden, toimittaminen asiakkaille toteutetaan turvallisella tavalla (mukaan lukien maksamiseen liittyvät ohjelmistot). Yksittäinen toimija ei voi suoraan vaikuttaa muiden luottamusverkoston jäsenten tunnisteiden hankintaan ja jakeluun.

Lisäksi osiossa "Sisäänkirjautumisyritykset, istunnon aikakatkaisu, tunnistamisen voimassaolo" todetaan, että maksupalveluntarjoajan tulisi asettaa tietty raja sisäänkirjautumis- tai tunnistautumisyritysten lukumäärälle, määritellä säännöt internet-maksupalvelun aikakatkaisulle (time out) ja asettaa aikarajat tunnistamisen voimassaololle. Myös, kun tunnistamisessa käytetään kertakäyttösalasanoja, maksupalveluntarjoajan tulisi varmistaa, että salasanat ovat voimassa ainoastaan välttämättömän minimiajan.

Käytännössä yksittäinen toimija ei voi määritellä luottamusverkoston muiden jäsenten tunnistusvälineiden sisäänkirjautumis- ja tunnistautumisyritysten määriä eikä kertakäyttösalasanojen kestoja.

Kohdassa "Sisäänkirjautumisyritykset, istunnon aikakatkaisu, tunnistamisen voimassaolo" todetaan, että maksupalveluntarjoajan tulisi käyttää vilpillisten maksutapahtumien ennaltaehkäisyyn, tunnistamiseen ja torjuntaan tarkoitettuja seurantamekanismeja ennen maksutapahtuman lopullista hyväksyntää; epäilyttävät tai suuririskiset maksutapahtumat tulisi asettaa erityiseen seulonta- ja arviointimenettelyyn. Vastaavia tietoturvaseuranta- ja hyväksymismekanismeja tulisi käyttää myös sähköisten valtakirjojen antamista varten.

Maksutapahtumien seuraaminen, jos tunnistautuminen tehty jonkun muun myöntämällä välineellä, edellyttäisi reaaliaikaista pääsyä muiden luottamusverkoston jäsenten järjestelmiin, mikä on käytännössä hankala toteuttaa.

Lopuksi, on syytä huomata, että pankkiasioinnin turvallisuus ei rajaudu vain tunnistamiseen, vaan siinä myös istunnon aikainen tarkkailu ja tunnistus/vahvistustason nosto riskipitoisissa tapauksissa esim. maksun lisävahvistusviesti, ovat keskeisessä roolissa. Näitä ominaisuuksia ei voi välttämättä voi hyödyntää muiden myöntämillä tunnuksilla

Auditointivelvollisuus, 28 - 37 §

Auditointivelvollisuus voi tukea luottamusverkoston toimintaa takaamalla verkostoon mukaan hyväksyttävien tunnistusvälineiden laatua, mutta se voi liian raskaasti toteutettuna muodostua vaikeaksi ja kalliiksi operaatioksi joka käytännössä muodostaa markkinoille tulon esteen, koska auditointimaksut valvontamaksujen tavoin lisäävät toimijoiden kustannuksia.

Riskinä on, että lopputuloksena syntyy samankaltainen tilanne kuten PCI DSS – säädöksissä, eli markkinoilla on eri tasoisia auditoijia, mikä ei varmista auditoitavien yhdenmukaista kohtelua. Lisäksi on syytä varmistaa, ettei mahdollisessa auditoinnissa muodosteta raskaita kansallisia erityskriteereitä, jotka voisivat muodostua esteeksi eurooppalaiselle yhteentoimivuudelle. Nykyisten toimijoiden auditoinnille esitetty aikataulu tuntuu tilanteessa, jossa tarkat kriteerit puuttuvat, erittäin haasteelliselta.

Auditoinnissa tulisi kiinnittää myös erityistä huomiota kykyyn tehdä ensitunnistamiseen luotettavasti ja tunnusten käytön valvontaan. Koko luottamusverkosto rakentuu sen varaan että nämä perustekijät ovat kunnossa.

Muita kommentteja

Ensitunnistamisen ketjuttaminen

Tunnistusvälineiden vapaa ketjuttaminen voi aiheuttaa pitkän vastuuketjun, jossa ensitunnistamisen menetelmä voi olla mahdotonta selvittää. Ketjuttamisen tai ensitunnistamiseen vetoamisen tulee olla rajoitettu. Ketjuttaminen on ongelma suhteessa väärinkäytöstapauksiin, samoin suhteessa EBA:n ohjeisiin.

Muutokset lakiin rahanpesun ja terrorismin rahoittamisen estämiseksi

Osana muutoskokonaisuutta pakettia on esitys lain rahanpesun ja terrorismin rahoittamisen estämisestä muuttamiseksi. Esitys on lähtökohtaisesti kannatettava. Asiakkaan henkilöllisyys on voitava todentaa vahvalla sähköisellä tunnistusvälineellä tai vaihtoehtoisesti hyväksyttävällä asiakirjalla. Siten pelkän etätunnistamista koskevan rahanpesulain pykälän muuttaminen ei ole riittävää, vaan samassa yhteydessä on muutettava rahanpesulain 10 §:n vaatimukset säilytettävien tietojen osalta vastaamaan etätunnistamista koskevaa pykälää.

Lain soveltaminen yhteisön sisäisiin tunnuksiin

HE:n sivulla 16 todetaan soveltamisalaa koskien: "Tapauksiin, joissa yhteisö käyttää omaa vahvaa sähköistä tunnistusmenetelmäänsä omien asiakkaidensa tunnistamiseen omissa palveluissaan sovelletaan kuitenkin 3 §:n, 20 §:n 1 momentin, 21-22 §:n, 23 §:n 1 momentin, 25 §:n 1 momentin ja 2 momentin sekä 27 §:n 1 momentin, 2 momentin 1 kohdan ja 3 momentin säännöksiä."

Kyseiset säännökset liittyvät vastuukysymysten ratkaisemiseen. Koska tällaisessa palveluntarjonnassa ei ole kyse vahvan sähköisen tunnistuspalvelun tarjonnasta, Viestintäviraston 42 b §:ssä säädetty valvontatehtävä ei koske tällaista toimintaa. Muutoin säännöksellä on merkitystä lähinnä juuri vastuukysymyksiä esimerkiksi tuomioistuimissa ratkaistaessa. On selvää, että jos lain soveltamisalaan kuulumaton toimija haluaa vapaaehtoisesti noudattaa lain palveluntarjoajalle ja tarjottavalle palvelulle asetettuja laadullisia säännöksiä, ei oikeusjärjestyksessämme ole tälle mitään yleistä estettä. Tällaiset toimijat eivät luonnollisestikaan voi tehdä 10 §:ssä tarkoitettua rekisteröidyksi tai 12 a §:n mukaisesti luottamusverkoston jäseniksi. Niitä ei myöskään valvota 5 luvun mukaisesti.

Itse soveltamisalapykälässä kuitenkin todetaan ainoastaan, että "Lakia ei sovelleta yhteisön sisäiseen tunnistamiseen käytettävien palveluiden tarjontaan. Lakia ei sovelleta myöskään, jos yhteisö käyttää omaa tunnistusmenetelmäänsä omien asiakkaidensa tunnistamiseen omissa palveluissaan." Lakia ei tulisi soveltaa yhteisön omiin sisäisiin tunnisteisiin miltään osin, vaan esim. tunnusten luovuttaminen pitäisi tapahtua, kuten toimija omissa sopimusehdoissaan määrittelee. Samoin pankin pitää voida omassa palvelussaan päättää itse millaiset tunnukset se hyväksyy (pl. Secure Pay-sääntely).

OP Osuuskunta

Taina Kallio