LIIKENNE- JA VIESTINTÄMINISTERIÖLLE

ASIA:

LAUSUNTO ASIASSA LVM/1518/03/2014:

HALLITUKSEN ESITYS VAHVASTA SÄHKÖISESTÄ TUNNISTAMISESTA JA SÄHKÖISESTÄ ALLEKIRJOITUKSESTA ANNETUN LAIN MUUTTAMISEKSI

LAUSUNNON ANTAJA: **AKTIA PANKKI OYJ**

Kiitämme mahdollisuudesta osallistua asian valmisteluun ja lausumme asiassa seuraavaa:

Lausunnon sisältö tiivistettynä pääpiirteissään

Katsomme jäljempänä esitetyin perustein ehdotetun hallituksen esityksen (jälj. Esitys) epäonnistuvan yrityksessä saattaa Suomen kansallinen vahvan sähköisen tunnistamisen järjestelmä vastaamaan Euroopan parlamentin ja neuvoston asetuksen (910/2014; jälj. Asetus) Suomelle jäsenvaltiona asettamia vaatimuksia. Esityksen tärkeimpänä ajurina vaikuttaa olevan julkisen sektorin kulujen pienentäminen, joka sinänsä yleisesti kannatettavana ajatuksena, ei kuitenkaan tässä tapauksessa vastaa Asetuksen tavoitteita eikä Esitys tule johtamaan Asetuksen vaatimusten täyttymiseen. Mikäli Esityksen tarkoituksena on ensisijaisesti rikkoa nykyinen vahvan tunnistamisen infrastruktuuri Suomessa, niin tässä muodossaan Esitys siinä todennäköisesti onnistuisi. Valitettavasti Esitys ei kuitenkaan sisällä työkaluja tai riittävää perustaa uuden toimivan infrastruktuurin rakentamiselle.

Esitys rakentuu ajatukselle luottamusverkostosta ja sähköisen ensitunnistamisen ketjuttamisesta, joita ei kuitenkaan ole käytännössä mahdollista toteuttaa Suomessa nykyisin käytössä olevan vahvan tunnistamisen infrastruktuurin puitteissa. Esityksen toteuttaminen ehdotetulla tavalla ei loisi Suomeen uutta Asetuksen edellyttämää toimivaa järjestelmää, vaan vaarantaisi vakavalla tavalla nykyisen järjestelmän jatkuvuuden ilman riittävää siirtymäaikaa korvaavaan järjestelmään.

Lisäksi katsomme, että Esitykseen sisältyy ehdotuksia, jotka ovat voimassaolevan lainsäädännön kannalta ongelmallisia, käytännössä mahdottomia toteuttaa esitetyssä aikataulussa sekä osin jopa ristiriidassa Asetuksen kanssa.

Oikeudelliset ja riskienhallinnalliset ongelmat

Vahvan sähköisen tunnistamisen järjestelmä perustuu Suomessa nykyisellään pitkälti talletuspankkien asiakkailleen tarjoamiin pankkitunnuksiin, joihin voidaan liittää ja käytännössä usein liitetään ns. Tupas-tunnistuspalvelu. Pankkitunnukset ovat kuitenkin lähtökohtaisesti asiakkaiden tilinkäyttöväline, jolla asiakkaat käyttävät oman pankkinsa verkkopankkipalveluita tai suorittavat sähköisiä verkkomaksupalveluja. Tunnistuspalvelut ovat lisäpalvelu, joita sähköisten palveluiden tarjoajista hyödyntävät julkisen sektorin toimijat, sekä lisäksi rajoitetusti lähinnä rahoitus- ja vakuutusalan toimijat sekä yksityiset terveysalan toimijat. Järjestelmä on toiminut hyvin eikä pankin kuluttaja-asiakkailta ole tullut kielteistä palautetta. Julkinen sektori on käytännössä ainoa, joka on esittänyt kritiikkiä sopimushallinnan monimutkaisuudesta, mutta tähänkin on ala tarjonnut jo aiemmin muita ratkaisumalleja.

Talletuspankit eivät käsityksemme mukaan voi kuitenkaan toimia Esityksen mukaisina luottamusverkoston jäseninä, sikäli kuin tämä edellyttää sähköisen tunnisteen myöntämistä jonkun toisen tekemän ensitunnistamisen perusteella. Tämä ei täytä luottolaitoksille asetettuja asiakkaan tunnistamisen ja tuntemisen edellytyksiä, joita mm. rahanpesun ja terrorismin rahoituksen estämiseksi annettu lainsäädäntö edellyttää.

Luottamusverkoston jäsenten väliset vastuukysymykset jäävät Esityksessä avoimiksi. Luottolaitoksille asetetut riskienhallintaa koskevat säädökset tekevät käsityksemme mukaan niin ikään mahdottomaksi talletuspankille olla mukana Esityksen mukaisessa luottamusverkostossa. Luottolaitosten toiminnan ulkoistamiselle ja ulkoistetun toiminnan auditoinnille asetetut vaatimukset jäävät Esityksessä täysin huomiotta.

Vastuu jonkun muun virheellisestä ensitunnistamisesta voi luoda vaikeasti ennakoitavia tilanteita, joiden vahingot voivat nousta erittäin suuriksi. Esimerkkinä voidaan mainita terrorismista epäillyn henkilön sähköisesti toteuttamat liiketoimet toisessa valtiossa, joka voisi johtaa pankin koko rahaliikenteen pysäyttämiseen tässä valtiossa sekä mahdollisiin korvausvaatimuksiin ja takavarikoihin. Esityksen mukaan ko. pankille olisi käytännössä erittäin vaikeaa saada virheellisen tunnistamisen alun perin tehnyttä tahoa vastuuseen, koska ketjutus voi olla toimijasta toiseen hyvinkin pitkä ja Esitys ei sisällä vaatimusta ketjutuksen rekisteröinnistä. Vastaavasti potentiaalinen virhe ensitunnistamisessa voisi aiheuttaa tunnistuksen tehneelle taholle täysin kestämättömän vahingonkorvausriskin, ellei korvausvastuun rajoittaminen ole mahdollista.

Esitys jättää vastuiden sopimusperusteisen hallinnan ja jakamisen luottamusverkoston jäsenten väliseksi asiaksi. Tämä ei ole mikään ratkaisu, sillä nykyisenkin lain 17 §:n mukaan ensitunnistamisen ketjuttamisesta on voinut sopia osapuolten kesken. Käsityksemme mukaan tällaisia sopimuksia ei ole juurikaan tehty, johtuen juuri vahinkojen ennakoimisen ja

rajoittamisen vaikeudesta. Säätämällä osapuolia velvoittava laki maininnalla, että osapuolten asiana on sopia vastuunjaosta keskenään tai säätämällä asetuksella ns. yleiset ehdot, ei ole toimiva ratkaisu. Se johtaa siihen, että toimijat joutuvat toteamaan, etteivät ne voi jatkaa osapuolina. Ratkaisuna voisi olla lähinnä se, että kaikki mahdolliset osapuolille syntyvät vahingot kanavoidaan valtiolle, joka toimisi ensikäteisenä vastuutahona ja joka hoitaisi regressivaatimukset todellista vahingonaiheuttajaa kohtaan myöhemmin.

Ajatus sähköisen ensitunnistamisen ketjuttamisesta on muutenkin outo eikä Esityskään pysty tuomaan esiin, mikä on tarve ensitunnistamisen ketjuttamiselle ja onko missään muussa maassa päädytty tällaiseen ratkaisuun. Asetuksen asettamat vaatimukset, esim. julkisen sektorin sähköisten palveluiden avaamisesta muiden jäsenvaltioiden hyväksymille tunnuksille, ei käsityksemme mukaan edellytä ensitunnistamisen ketjuttamista.

Esitys on ongelmallinen myös ns. identiteettivarkauksien osalta, jos henkilön vahva tunniste joutuu luvattomiin käsiin. Tätä on pankkitunnusten kohdalla sattunut käytännössä joskus, mutta näissä vahingot ovat tähän asti kohdistuneet ja rajoittuneet lähinnä henkilön varallisuuteen ko. pankissa tai velanottoon henkilön nimissä pikavippiyhtiöiden kautta. Koska tunniste on pankkikohtainen, se on ollut helppo sulkea ja poistaa käytöstä ja asiakas on saanut uudet toimivat tunnisteet. Jos sallitaan Esityksen mukainen ensitunnistamisen ketjuttaminen, niin luvaton käyttäjä voisi "monistaa" henkilöllisyyden läpi koko luottamusverkoston, minkä jälkeen sulkeminen (kun rekisteröintivelvoitetta ei ole) ei olekaan enää yksinkertaista. Henkilöllisyyden sulkeminen koko verkostossa ja oikean henkilön identiteetin uudelleen avaaminen jää Esityksessä kokonaan avoimeksi.

Koska Esityksen mukaiseen luottamusjärjestelmään sisältyy osapuolille riskejä, joiden ennakointi ja hallinnointi tulisi olemaan vaikeaa, nämä riskit joudutaan hinnoittelemaan käyttäjien maksettaviksi. Käyttäjiä ovat tällöin sekä yksittäiset kuluttajat että sähköisten tunnistuspalveluiden käyttäjät, lähinnä siis julkinen sektori. Tämän vuoksi hinnoittelun sääntely lailla tai asetuksella ei ole toimiva ratkaisu. Jos palvelu ei ole markkinaehtoisesti hinnoiteltavissa, markkinaehtoisia toimijoita ei tule järjestelmään osallistumaan.

Kiinnitämme vielä lainvalmistelijoiden huomiota Asetuksen resitaalin 37 sanamuotoon, jonka mukaan toimijoilla tulee olla mahdollisuus asettaa palveluilleen rajoituksia, jotta ne voivat hallinnoida mahdollisia niille Asetuksen perusteella syntyviä vastuita. Lisäksi artiklan 24 mukaan erilaiset ensitunnistamisen tavat ovat mahdollisia eikä artikla käsityksemme mukaan velvoita toimijaa hyväksymään kaikkia Asetuksen mahdollistamia tunnistamistapoja omassa toiminnassaan. Nämä Asetuksen sitovat säännökset osaltaan johtavat käsityksemme mukaan siihen, että Esitykseen sisältyvät velvoittavat määräykset sähköisen ensitunnistamisen ketjuttamisesta ja luottamuksesta muihin toimijoihin ovat jo sinänsä mahdottomia säädettäväksi kansallisessa lainsäädännössä.

Tekniset ongelmat

Esityksen mukainen siirtymäaika on mahdoton, koska Esitys jättää kaikki yksityiskohdat avoimeksi liittyen luottamusverkostosopimukseen sekä teknisiin rajapintoihin. Tämä

tarkoittaa, että sovittujen asioiden tekniseen toteuttamiseen, omaan ja luottamusverkoston väliseen testaamiseen sekä jalkauttamiseen nykyisille tai tuleville palveluntarjoajille ei jää riittävästi aikaa. Siirtymäajan tulisi olla vähintään kolme vuotta, jotta toimivia palveluita voitaisiin teknisesti järjestää.

Esityksestä ja siihen liittyvästä asetusehdotuksesta aiheutuvat kustannukset nykyiselle vahvan sähköisen tunnistuspalvelun tarjoajalle eivät ole arvioitavissa millään tavoin. Varsinkin kun esitetään, että nykyisten tunnistusvälineiden turvatasoja tarkastetaan 1.7.2016 voimaan astuvaa Euroopan parlamentin ja neuvoston asetusta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla vasten. Tunnistusvälineiden turvatasoja määritettäessä tulisi huomioida, että eri toimijoilla voi olla eritasoisia vaatimuksia turvatasojen suhteen, riippuen tarjottavista palveluista ja käytettävistä päätelaitteista.

Väestörekisterikeskuksen aseman monopolisointi datan toimittajana on ongelmallinen paitsi juridisesti niin myös teknisesti, mikäli Esityksen tarkoituksena on sulkea pois kaikki sellaiset kaupalliset toimittajat, jotka sinänsä perustavat datan väestörekisterin tietoihin, mutta voivat edelleen jalostaa välitettävää dataa. Esimerkiksi toimijat joutuisivat itse rakentamaan kaikki varmennepolitiikan prosessit itse, kun Väestörekisterikeskus ei niitä tarjoa. Kaupallisilta varmennepalvelujentarjoajilta nämä olisivat ostettavissa valmiina.

Helsingissä lokakuun 30. päivänä

AKTIA PANKKI OYJ

Jarl Sved
varatoimitusjohtaja

Kari Lähteenmäki
lakimies