eIDAS ja PSD2/RTS -tarkastelu

Viestintäviraston ja Fivan arvio sähköisen tunnistamismenetelmän vaatimusten yhteensopivuudesta

Viestintävirasto

Tausta

- Sähköistä pankkitunnistusta käytetään Suomessa tunnistamiseen pankkien omissa pankkipalveluissa JA tarjotaan yleisesti käytettäväksi vahvaan sähköiseen tunnistamiseen muissa palveluissa
  - » Tunnistusmenetelmää koskee tällöin kahden sääntelyn vaatimukset
  - » Toimijat ovat esittäneet viranomaisille huolia, että vaatimukset voivat olla ristiriitaisia ja sama tunnistusmenetelmä ei voisi välttämättä täyttää molempia vaatimuksia
- Viestintävirasto ja Finanssivalvonta ovat vertailleet tunnistusmenetelmän vaatimuksia.
  - » Tarkoituksena on selvittää, onko esteitä käyttää samaa tunnistusmenetelmää molemmissa säädöskehikoissa vai onko eriytettävä menetelmät.
  - » Kysymystä on käsitelty myös pankkien kanssa Viestintäviraston työryhmissä.
- Vivin ja Fivan arviosta pyydetään nyt näkemyksiä

Säädökset

Yleinen vahva sähköinen tunnistus

- (eIDAS-asetus (EU) 910/2014, erityisesti 8 artikla)
- eIDAS LOA = komission täytäntöönpanoasetus (EU) 2015/1502 sähköisen tunnistamisen menetelmien varmuustasoista
- Tunnistus- ja luottamuspalvelulaki = laki vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista (617/2009)
- M72 = Viestintäviraston määräys 72A/2018 M vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista

PSD2 vahva tunnistus

- Maksupalvelulaki (290/2010)
- RTS = komission delegoitu asetus (EU) 2018/389 tekninen sääntelystandardi mm. asiakkaan vahvasta tunnistamisesta

Toimijoiden havaintoja pyydetään

Lausuntopyyntö

- Vivi ja Fiva pyytävät toimijoilta kommentteja nyt esiteltävistä teknisistä päätelmistä
  - » Kalvojen lisäksi vaatimuksista on laadittu säännösvertailuexcel
- Lausuntopyyntö lähetetään Fivan PSD2-seurantaryhmälle sekä Viestintäviraston eIDAS-ryhmälle ja tunnistuspalveluiden luottamusverkoston yhteistoimintaryhmälle.

Lisäksi tiedoksi

- Viestintävirasto käynnistää 2018 aikana mobiilisovellusten arviointikriteeristön laatimisen
  - » Fiva seuraa työtä, RTS pyritään huomioimaan.
  - » Vivi kutsuu valmisteluun työryhmän.
  - » Kysymyksessä on Vivin suosituksen 211/2016 S täydennys/päivitys.
  - » Pohjaksi otetaan OWASP, Mobile AppSec Verification

Muut kuin tekniset seikat

- Viestintävirasto ja Finanssivalvonta ovat arvioineet yhdessä ministeriöiden ja KKV:n kanssa tunnistuslain ja maksupalvelulain oikeudellista suhdetta
- Arvio on julkaistu muistiossa 6.7.2017 dnro 1044/620/2017 *Viestintäviraston ja Finanssivalvonnan muistio: maksupalvelulain ja tunnistuslain suhde avattaessa rajapinta ja tunnistus TPP:lle PSD2:n edellyttämällä tavalla*
- *https://www.viestintavirasto.fi/attachments/tietoturva/Viestintaviraston_ja_Finanssivalvonnan_muistio_maksupalvelulaki_tunnistu....pdf*

Tunnistusmenetelmän tekniset vaatimukset

Tarkastellut vaatimukset ja päätelmät

- Sääntelyn vaatimukset ovat vähimmäisvaatimuksia
- Jos toisessa säännöskehyksessä on joltain osin tarkempia tai tiukempia vaatimuksia, täyttämällä nämä täyttää varsin todennäköisesti myös tältä osin yleisluonteisemmat toisen sääntelyn vaatimukset
- Vaatimukset on säädöksissä ryhmitelty eri tavalla.

➢ Tarkastelussa ei ole tunnistettu vaatimuksia, jotka estäisivät teknisesti saman tunnistusmenetelmän tarjoamisen molempien sääntelyjen mukaisena

1) Todentamistekijät
2) Todentamismekanismi
3) Henkilökohtaisten turvatunnusten/tunnistusvälineen luomisen ja elinkaaren vaatimukset
4) Salausvaatimukset
5) Rajapintavaatimukset
6) Auditointivaatimukset

1) ja 2) Todentamistekijät ja todentamismekanismi

- Todentamistekijät
  - vaaditut todentamistekijät ovat samat
  - vähintään 2 tekijää eri ryhmistä
  - RTS 4.1, MPL 8 § ja eIDAS LOA 2.2.1
- Todentamismekanismi
  - Tunnistustapahtuman uniikkius
  - eIDAS LOA dynaamisen todentamisen vaatimus vastaa RTS tunnistamiskoodin muodostamisen vaatimuksia
  - RTS 4.2 ja TunnL 8 §, eIDAS LOA 2.3.1
- Vaatimukset tekijöiden turvallisuudelle ja riippumattomuudelle
  - RTS 6-9 artiklat, todentamistekijöiden vaatimukset ja riippumattomuus
  - eIDAS LOA vastaavat vaatimukset:
  - 2.2.1 menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.
  - 2.3.1 turvatoimenpiteet menetelmän varmentamiseksi arvaamista, salakuuntelua, toistoa tai manipulointia vastaan

3) Turvatunnusten/tunnistusvälineen luominen ja elinkaari

- Yhdistäminen henkilöön
  - Säädösten painotukset eroavat, mutta ei ristiriitoja
  - Tunnistussääntelyssä lisäksi erityisesti henkilöllisyyden todistamiseen liittyviä vaatimuksia
  - RTS:ssä erityisesti yhdistämistapahtuman vaatimuksia (Tunnusten/välineen luomisen turvallisuus)
  - RTS 24 ja eIDAS LOA 2.2.1

4) ja 5) salaus- ja rajapintavaatimukset

- Istuntojen eli tunnistustapahtumien (tietoliikenteen) tietoturvallisuutta edellytetään molemmissa sääntelyissä
- Turvallisuusvaatimuksia on vertailtu erityisesti tietoliikenteen salausvaatimusten näkökulmasta
  - eIDAS 2.3.1 (todentamismekanismin hyökkäyksenkestävyys)
  - Vivi M72A 7 § (liikenteen, sanomien ja säilytettävän tiedon salaus)
  - RTS johdantokappale 26 (salaus rajapinnoissa toimijoiden välillä),
  - RTS art. 2 yleiset tunnistamisvaatimukset (haittaohjelmien havainnointi),
  - RTS art. 4 Tunnistamiskoodi (viestintäistuntojen suoja)
  - RTS art. 35 Viestintäistuntojen turvallisuus (vahvat ja yleisesti tunnustetut salaustekniikat)
- Muita relevantteja salausteknisen aineiston turvallisuus ja turvatunnusten/henkilötietojen turvallisuus

6) Auditointivaatimukset

- Molemmissa vaatimukset säännöllisestä vaatimustenmukaisuuden arvioinnista tietoturvallisuuden kannalta
  - » RTS 3.1 ja eIDAS LOA 2.4.7 säännöllinen riippumaton arviointi
  - » TunnL 28 §, 29 §, 31 § ja 33 § arviointielimen vaatimukset ja tarkastuskertomus
  - » eIDAS korotetulla varmuustasolla riittää sisäisen tarkastuslaitoksen riippumaton arviointi
- Edellytyksenä molemmissa asiantuntemus tietoturvallisuudesta
- Tunnistusääntelyssä kansallisesti yksityiskohtaisemmat säännökset arviointielimen riippumattomuudesta, pätevyydestä ja tarkastuskertomuksen syklistä
- Sääntely tukee sitä, että esim. pankkien sisäinen tarkastus kelpaa myös tunnistuslain mukaiseen riippumattomaan arviointiin, kunhan pätevyyden näkökulmasta tietoturvallisuusasiantuntemus ilmenee tarkastuskertomuksesta tai sitä on tarvittaessa täydennetty ulkoisesti

Vrt. RTS dynaaminen yhdistäminen

- RTS 5 art.:
  - ...4 artiklan vaatimusten lisäksi toteutettava turvatoimenpiteet, jotka täyttävät kaikki seuraavat vaatimukset:
  - a) maksajalle ilmoitetaan maksutapahtuman määrä ja maksunsaaja;
  - b) tunnistamiskoodi tuotetaan tiettyä maksutapahtuman määrää ja tiettyä maksunsaajaa varten, jotka maksajan on hyväksynyt käynnistäessään tapahtuman;
  - c) maksupalveluntarjoajan hyväksymä tunnistamiskoodi vastaa alkuperäistä maksutapahtuman määrää ja maksunsaajan henkilöllisyyttä, jotka maksaja on hyväksynyt;
  - d) määrän tai maksunsaajan muutokset johtavat tuotetun tunnistamiskoodin mitätöintiin.
  - 2. Sovellettaessa 1 kohtaa maksupalveluntarjoajien on toteutettava turvatoimenpiteet, joilla varmistetaan kaikkien seuraavien tietojen luottamuksellisuus, aitous ja eheys:
  - a) maksutapahtuman määrä ja maksunsaaja kaikissa tunnistamisen vaiheissa;
  - b) maksajalle näytetyt tiedot kaikissa tunnistamisen vaiheissa, tunnistamiskoodin tuottaminen, lähettäminen ja käyttö mukaan luettuina.

Arvio RTS art. 5 vaatimuksesta suhteessa tunnistuslakiin

- Viville ja Fivalle on esitetty, että RTS:n dynaamisen yhdistämisen vaatimusta ei voi toteuttaa tunnistusmenetelmällä, joka täyttää eIDAS-vaatimukset
- Seuraavaa arviota on käsitelty viestintäviraston M72A-työpajassa 26.3.2018
- Artikla 5, tunnistamiskoodi ja dynaaminen yhdistäminen maksutapahtuman tietoihin
  - » Toimintoa ei puhtaissa yleiskäyttöisissä tunnistusvälineissä lähtökohtaisesti ole eikä tarvita
  - » Maksupalveluntarjoajan (= pankin) tuotettava ja sidottava tunnistamiskoodi maksunsaajaan ja summaan. Voinee katsoa, että käyttäjä vahvistaa tunnistamiskoodilla toimeksiannon maksutapahtuman suorittamisen.
  - » Tunnistamiskoodi voidaan täten tuottaa vasta kun maksun saaja ja summa ovat tiedossa ja käyttäjä on vahvasti tunnistettu
    - esimerkiksi mobiilipankkisovellus/erillinen laite/verkkopankki, joille tavalla tai toisella on kommunikoitu maksun saaja ja summa
  - » → Ei ristiriitaa, tunnistamiskoodin luonti seuraa vahvan tunnistamisen jälkeen? Tai erillisessä rajapinnassa, joka sisältää sekä tunnistamisen, että maksupalveluiden tarvitsemat ominaisuudet

Muita vaatimuksia

- Tunnistusmenetelmien sääntelyn lähtökohdat eroavat
  - » TunnL, eIDAS: käyttötarkoituksesta riippumaton yleiskäyttöinen sähköinen tunnistusmenetelmä ja sen tarjonta yleisesti
  - » "sähköinen henkilötodistus"
  - » MPL, PSD2, RTS: käyttäjän tunnistaminen maksutilin etäkäytössä ja maksutapahtuman vahvistus
- Eri sääntelytarkoituksen takia palveluntarjoajan vaatimukset yms. säännellään yleisessä tunnistusääntelyssä kokonaisuutena ja maksupalvelusääntelyssä eri osissa sääntelykokonaisuutta
  - » säännösvertailuexcelissä keskitytään tunnistusmenetelmään
  - » ei tarvetta tarkastella elinkeinotoimintaan kohdistuvia muita vaatimuksia

www.viestintävirasto.fi