

Asia: 888/00.01.00.01/2015

VAHTI 3/2017 Sähköisen asioinnin tietoturvallisuus -ohje

Lausunto - VAHTI 3/2017 Sähköisen asioinnin tietoturvallisuus-ohjeluonnokseen -
yleistä

Yleinen palaute

-

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Viestintävirasto katsoo, että ohje on kokonaisuudessaan kohtuullisen laaja ja raskaslukuinen. Tämä voi osaltaan aiheuttaa haasteita sen soveltamisessa käytäntöön.

Mitkä olivat ohjeen parhaita asioita?

Ohjeen parhaita puolia olivat selkeä rakenne ja erikseen kuvatut kokonaisuudet. Erityisesti sähköisene tunnistamiseen liittyvät asiat olivat ansiokkaasti ja selkeästi kuvattu.

Yksityiskohtaiset kommentit

Luku 1 Johdanto

-

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

Viestintävirasto ehdottaa, että säädöskuvauksessa mainittaisiin sähköistä allekirjoitusta ja sähköistä leimaa koskeva sääntely eIDAS-asetuksessa (EU) 910/2014 ja eIDAS-asetuksen nojalla annettu komission täytäntöönpanopäätös (EU) 2015/1506 eritelmien vahvistamisesta sellaisia kehittyneiden sähköisten allekirjoitusten ja kehittyneiden leimojen muotoja varten, jotka julkisen sektorin elinten on tunnustettava sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 27 artiklan 5 kohdan ja 37 artiklan 5 kohdan mukaisesti.

Nämä on mainittu myöhemmin ohjeessa, mutta viittaus voisi olla myös tässä kohtaa, koska eIDAS-asetuksessa säädetyillä edellytyksillä velvoitteet koskevat Suomen julkishallinnon viranomaisten sähköisiä asiointipalveluita.

Luku 3 Sähköiset asiointipalvelut

-

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

Tässä yhteydessä kannattaisi ohjeessa mainita myös se, että palvelun tilaajan on varmistauduttava palveluntoimittajien ja yhteistyökumppanien tekijänoikeuksista omiin tuotteisiinsa tai käyttämiinsä järjestelmäkomponentteihin. Mikäli järjestelmän osana käytetään komponenttia, jonka lisenssiehdoissa on mainittu esimerkiksi rajausta kaupallisessa toiminnassa käyttöön, voidaan riitatapauksessa pahimmillaan estää koko järjestelmän käyttö tai vaatia sen käytöstä huomattavia korvauksia.

Ohjeessa voisi ensisijaisesti suositella viranomaisen hyväksymiä salausmenetelmiä, jos sellaisia on tarjolla.

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

Ks. kohdassa 6 sanottu tunnistuspalveluiden varmuustasosta.

Viitearkkitehtuurissa olisi myös hyvä painottaa viranomaisen hyväksymiä salausratkaisuja, kun sellaisia on.

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

Vahvan sähköisen tunnistamisen sääntely ja valintaperusteet on kuvattu kaiken kaikkiaan hyvin ja selkeästi. Ohjeeseen voi harkita seuraavia tar-kennuksia:

Kohdan 6.2. taulukossa voi aiheuttaa sekaannusta suhteessa eIDAS-asetukseen se, että korkea varmuustaso yhdistetään substantial -tason riskiin asiointipalvelussa. eIDAS-asetuksen kielessä substantial vastaa kuitenkin korotettua tasoa ja high korkeaa tasoa. Todentamismekanismin sietokykyä tietoturvaaukia vastaan taas kuvataan eIDAS-säännöksissä asteikolla "enhanced-basic" (matala varmuustaso), "moderate" (korotettu varmuustaso) ja "high" (korkea varmuustaso).

Kohdan 6.2 lopussa mainitaan, että 1.5.2017 alkaen kansallisia tai eIDAS-notifioituja vahva sähköisen tunnistamisen menetelmiä ja palveluita voi tarjota vain tunnistamisen luottamusverkostoon liittynyt auditoitu toimija (ks. Suomi.fi-tunnistaminen). Kyseinen sääntely on jo voimassa, tunnistusvälineiden tarjonnan osalta sääntely on ollut voimassa jo vuodesta 2009 ja tunnistusväilyksen osalta 1.7.2016 lähtien. 1.5.2017 tulevat voimaan uudet yhteistyövelvoitteet luottamusverkostossa. Hienoisen epätarkkuuden voi korjata esimerkiksi jättämällä pois viittauksen päivämäärään.

Tässä kohdassa ja edellä kohdassa 5.3.1 Esimerkki 1 viitataan Suomi.fi -tunnistamiseen liitetyn tunnistuspalvelun varmuustasoon.

Viestintävirasto ehdottaa, että termi varmuustaso sidottaisiin aina sähköi- sessä tunnistamisessa selvyiden vuoksi yksiselitteisesti tunnistuslain ja eIDAS-asetuksen mukaiseen korotetun tai korkean varmuustason määrittelyyn. Toinen vaihtoehto on tarkentaa esim. "laissa säädetty varmuustaso" relevanteissa kohdissa.

Tietylle varmuustasolle rekisteröidyt tunnistuspalvelut ilmenevät Viestintäviraston tunnustuslain 12 §:n mukaisesta rekisteristä (<https://www.viestintavirasto.fi/kyberturvallisuus/sahkoinentunnistaminenjaallekirjoitus/rekisteritunnistamispalveluntarjoajista/rekisteritunnistamispalvelujentarjoajista.html>). Rekisterissä olevat tunnistuspalveluntarjoajat ovat jättäneet tunnustuslaissa säädetty ilmoitukset palvelunsa varmuustasosta 31.1.2017 mennessä ja Viestintävirasto arvioi parhaillaan, täyttävätkö ne ilmoittamansa varmuustason vaatimukset. Tieto merkitään rekisteriin.

On hyvä huomata, että rekisteriin tulee myös uusia vahvoja sähköisiä tunnistuspalveluita. Kohdassa 6.3 tulisi tasapuolisuuden vuoksi esim. mainita omana laatikkonaan "muu Viestintäviraston rekisterissä olevan vahva sähköinen tunnistusväline", jotta markkinoille tulijoiden vahvan sähköisen tunnistamisen palvelut näkyvät tasapuolisesti. Ohjeen liitteessä asia kylläkin huomioidaan.

Huomiona kohtaan 6.4.3 voi todeta, että toistaiseksi markkinoilla on vain luonnollisille henkilöille myönnettyjä vahvoja sähköisiä tunnistusvälineitä, mutta tunnustuslaki ja eIDAS mahdollistavat vahvan sähköisen tunnistusvälineen tuotteistamisen myös oikeushenkilölle.

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

Viestintävirasto pitää hyvänä sitä, että ohjeessa kuvataan eIDAS-asetuksessa määritellyt sähköisen allekirjoituksen tasot. Ohjeessa voisi mainita myös, että eIDAS-asetuksessa oikeushenkilön kohdalla sähköistä allekirjoitusta vastaa sähköinen leima, joka on teknisesti samanlainen kuin sähköinen allekirjoitus.

Kehittyntä sähköistä allekirjoitusta koskevana tarkennuksena komission täytäntöönpanoasetus (EU) 2015/1506 ei tarkenna geneerisesti kehittyneen sähköisen allekirjoituksen vaatimuksia vaan ainoastaan määrittelee tietyt kehittyneen sähköisen allekirjoituksen formaatit, joiden vastaanottamiseen julkisen sektorin elimillä olisi oltava valmiudet, jos ne vaativat kehittyneen sähköisen allekirjoituksen käyttämistä. EU:n komissiolla on myös tarjolla validointityökalu (nk. DSS-tool), jolla pystyy validoimaan nämä säädettyt formaatit.

Yleisesti kehittyneen sähköisen allekirjoituksen vaatimusten täyttäminen on vielä tarkemmin määrittelemättä. Tyypillisenä tapana toteuttaa kehittyneen sähköisen allekirjoituksen vaatimukset pidetään kuitenkin julkisen ja yksityisen avaimen PKI-arkkitehtuuria, jota Vahti-ohjeessa kuvataan digitaalisen allekirjoituksen otsakkeen 7.1.3 alla. Ko. kohdassa oleva kaaviokin (kuva 6) koskee kehittyneen sähköisen allekirjoituksen toimintaperiaatetta.

Ohjeesta ei käy ilmi, mikä erottaa digitaalisen allekirjoituksen kehittyneestä sähköisestä allekirjoituksesta tai sähköisestä leimasta.

Viestintävirasto saa säännöllisesti neuvontapyyntöjä sähköisestä allekirjoituksesta julkishallinnon toimijoilta ja yksityisen sektorin toimijoilta, jotka tarjoavat allekirjoituspalveluja. Niiden perusteella viranomaiset tarvitsisivat sähköisen allekirjoituksen suunnittelussa ja hankinnoissa tietoa siitä, millä perusteella ne tunnistavat kehittyneen sähköisen allekirjoituksen, vaikka säädettyjä velvoitteita sellaisen käyttämiseen onkin vähän. Viestintävirasto ehdottaa siksi, että ohjetta pyrittäisiin vielä selkeyttämään tältä osin suhteessa digitaaliseen allekirjoitukseen. Viestintävirasto valvoo pääosin eIDAS-asetuksen noudattamista, mutta sähköisten allekirjoitusten statuksen arviointi ei kuulu Viestintäviraston toimivaltaan ja Vahti-ohje olisi siksi tar-koituksen mukainen väline ohjata valtionhallinnon käytäntöjä.

Viestintävirasto pitää erittäin hyvänä ja tarpeellisena sitä, että ohjeessa on selvennetty sähköisen asioinnin lain 16 §:n vaatimusta viranomaisen päätöksen allekirjoittamisesta kehittyneellä sähköisellä allekirjoituksella tai muuten sellaisella tavalla, että asiakirjan alkuperäisyydestä ja eheydestä voidaan varmistautua. Edelleen on erittäin hyvä, että sähköisen asioinnin lain 20 §:ssä mainitun koneellisen allekirjoituksen suhteeseen sähköiseen leimaan otetaan kantaa.

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

-

Liite 1: Keskeinen sanasto

-

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

-

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

-

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

-

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

Viestintävirasto huomauttaa, että eIDAS-asetuksen nojalla annetussa nk. varmuustasoasetuksessa (EU:n komission täytäntöönpanoasetus (EU) 2015/1502 teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti) määritellään tekniset eritelmät ja menettelyt eri varmuustasoilla tunnistusmenetelmän koko elinkaaren ja hallinnan kannalta.

Näistä elinkaaren ja hallinnan vaatimuksista liitteen 5 taulukkoon on poi-mittu vain osa. Viestintävirasto ei ole arvioinut poiminnan tarkoituksenmukaisuutta tai tarkistanut poimittuja faktoja varmuustasoasetuksesta, mutta kiinnittää huomiota ainakin siihen, että korotetun varmuustason tunnistusmenetelmässä edellytetään kahta (ei yhtä) todentamistekijää (varmuustasoasetus liite kohta 2.2.1) ja lisäksi todentamismekanismita edellytetään dynaamisuutta (varmuustasoasetus liite kohta 2.3.1 ja liite kohta 1 määritelmät).

Viestintävirasto ehdottaa, että jos varmuustasoasetusta halutaan referoida liitteessä, listattaisiin esimerkiksi johdonmukaisesti kaikki varmuustasoasetuksen vaatimukset otsikkotasolla.

Vaihtoehtona on viitata suoraan varmuustasoasetukseen <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32015R1502&qid=1455478267718&from=FI>

Liite 6: Case-esimerkit

-

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

-

Muuta palautetta ohjeesta tai VAHTille?

-

Viitaila Mikko
Viestintävirasto