

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

Ohje on kokonaisuutena kattava ja hyvin hyödynnettävissä. Tietoturvan kokonaiskuva tulisi kuitenkin kirkastaa ja lisätä ohjeeseen mm. jatkuvuusasiat omana osionaan sekä vastuut kehittäjien, palvelutuottajien ja yhteisten palvelujen osalta.

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Sähköisen asioinnin tietoturvaohjeesta tulisi laatia myös selkeä riittävän yksityiskohtainen soveltamisohje, jota sähköisen asioinnin kehittäjät ja palvelutuottajat (esim. eri viranomaiset) pystyvät suoraan hyödyntämään oman palvelutoiminnan edellyttämälle tietoturvatasolle.

Ohje voisi koostua kahdesta kokonaisuudesta:

1. Johdanto-osuus, johon on sisällytetty tietoturvan kokonaiskuvaus ja sen hallintaan liittyvät vastuut valtionhallinnossa
2. Varsinainen ohje ja sen liitteet

Mitkä olivat ohjeen parhaita asioita?

Kokonaisuus on kattava ja kuvat ovat havainnollisia.

Yksityiskohtaiset kommentit

Luku 1 Johdanto

Edellä mainitun johdanto-osuuden sisällyttäminen tähän ohjeeseen.

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

Kehitysehdotus:

Alussa voisi olla lista lainsäädännöstä, jotka koskevat sähköistä asiointia.

Tämän jälkeen asiointi olisi kuvattu prosessina. Prosessin eri vaiheisiin tulisi kiinnittää vaiheittain säätelevät lait ja asetukset vaatimuksineen.

Luku 3 Sähköiset asiointipalvelut

Asiakkuuksien osalta rekisteröidyt yhdistykset tulisi sisällyttää ohjeistuksen piiriin.

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

Ohjeessa tulisi ottaa kantaa siihen, mitkä ovat eri tietoturvasojen osalta turvalliset tekniset ratkaisut.

Valtiolla tulisi olla myös kevyt auditointi- tai tarkastuspalvelu sähköisen asioinnin kehittämisen tueksi. Tukipalvelu, jonka toimesta arvioidaan esitetyn ratkaisun riittävyys/vältetään ylimitoitusta.

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

Viitearkkitehtuuri kuvaus on laadittu hyvin kattavasti. Ehdotetaan että ohjeeseen sisällytetään kannanotto viitearkkitehtuuri-kontrollin lisäämisestä kehitysprojektin hyväksymiskriteeriksi (hanke palaa valmisteluun, jollei tietosuojan vaatima viitearkkitehtuuri toteudu).

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

Eri tunnistautumismenetelmien (HST-kortti, verkkopankkitunnukset...) käyttökelpoisuus varmuustasoihin nähden on vaikeaselkoinen/puuttuu esityksestä?

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

Aihealue on esitetty hyvin kattavasti ja yksityiskohtaisesti. Esimerkkien käyttö voisi helpottaa ohjeen hyödyntämistä viranomaisen käyttötarvetta vastaavaksi.

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

Asiointivaltuudet -palvelun käyttöönoton aikataulu on jätetty auki. Pelkkä tunnistautuminen ei riitä esimerkiksi viitearkkitehtuurin mukaisten suojaustasojen toteuttamiseen kehittyneellä tavalla.

Liite 1: Keskeinen sanasto

Viittauksien sijaan sanastossa tulisi suoraan esittää kuvaus. (minimissään URL-linkki viitattuun esitykseen)

Lisäksi sanasto voisi olla kattavampi.

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

Ohjeen voisi tältä osin täydentää suoraan vaatimusmäärittelytasolle, jossa on eritelty suojaustasoja vastaavat vaatimukset.

(Hankintojen tueksi)

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

Ei kommentoitavaa.

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

Ei kommentoitavaa.

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

Ei kommentoitavaa.

Liite 6: Case-esimerkit

Voisiko olla case-esimerkkejä tyypillistä puutteista, joihin tulisi kiinnittää huomiota sähköistä asiointiympäristöä kehitettäessä.

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

Toivotaan tiivistelmää, jossa kokonaisuus on huomioitu, kehittämisprojektien valmistelun ja määrittelyn tueksi.

Muuta palautetta ohjeesta tai VAHTille?

-

Isosuo Tuula-Kaarina
Etelä-Suomen aluehallintovirasto

Taipale Anu
Etelä-Suomen aluehallintovirasto - Hallinto- ja kehittämispalvelut/AVI:n
yhteinen lausunto