

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 kattava ja laaja kokonaisuus, jota pystyvät parhaiten kokonaisuudessaan hyödyntämään pääkohderyhmiksikin nimetyt asiantuntijat. Julkisen hallinnon organisaatioissa on lisäksi paljon sellaisia tahoja, jotka tarvitsevat tietoa sähköisen asioinnin tietoturvallisuudesta, mutta ei näin syvälle menevänä tietona. Lopputuloksesta näkee, että sitä valmisteltu asiantuntijavoimin. Tekijät ovat itse mitä todennäköisimmin hyvin selvillä yksityiskohdista, jotka eivät kaikilta osin ehkä avaudu lukijoille.

Tulevaisuuden lisääntyvien sähköisten palvelujen ja tietoturvasoltaan korkealaatuisten sekä yhtenäisten toteutusten kannalta ohje on ehdottomasti tarpeen.

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Ohje on melko raskaslukuinen ja oppikirjamainen, joka ei kaikkia houkuttele lukemaan sitä, vaikka se sisällöltään onkin hyvä. Huomioitavaksi myös, että se on rakennettu niin, että se saattaa "vanheta" nopeastikin, joten sen ajan tasalla pitäminen vaatii melko jatkuvaa työtä. Ohjeesta voisi irrottaa ns. yleiset asiat omaksi helppolukuisemmaksi kokonaisuudekseen (näitäkin tietoja siellä on) ja teknisemmät osuudet ja yksityiskohdat omaksi kokonaisuudekseen.

Termistöt yhtenäisiksi kautta linjan – samat asiat yhdellä ilmauksella (tai esim. suluissa tarpeen mukaan rinnakkaiset termit). Vaatii vielä tekijöiltään läpilukemisen kirjoitusvirheiden korjaamiseksi ja lauserakenteiden selkiyttämiseksi.

Mitkä olivat ohjeen parhaita asioita?

Vaikka ohje on tekstiosuuksiltaan raskaslukuinen, sen rakenne hyvine kuvineen ja taulukkomaisine asiakoosteineen selventää kokonaisuutta ja helpottaa myös asioihin palaamista. Suomi.fi-kooste (luku 8) oli hyvin toteutettu. Myös lakikoosteet olivat tarpeelliset - toisaalta esim. tämä kohta voi olla useinkin muuttuva ja päivittämistä vaativa, joten sen toteutus mieluummin liitteenä.

Yksityiskohtaiset kommentit

Luku 1 Johdanto

Selkeä kooste ja johdattelu sisältöön.

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

Tärkeä osa asiaa, mutta toimisi ehkä paremmin liitteenä (päivitystarve huomioiden). Lukijan täytyy melko pitkälti voida luottaa koosteen sisältöön niin, että se sisältää tärkeimmät ja merkittävimmät kohdat <-- vaatii tekijöiltään ammattitaitoa.

Luku 3 Sähköiset asiointipalvelut

Yhteisen ymmärtämisen lisäämiseksi käsitteiden määrittely on tärkeää (esim. uhkatilanteet). Taulukon 1 esimerkit tietoturva vaatimuksineen ovat erittäin hyviä. *-merkkien selvennykset/selitykset puuttuvat.

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

Alakohdat eri kohderyhmille suunnattuja. Taulukkomainen rakenne tässäkin hyvä.

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

Laaja ja tärkeä kokonaisuus sisältäen paljon yksityiskohtia, joita kuvat selventävät. Pääosin erityisasiantuntijoille, taulukoiden esimerkit avaavat asiaa.

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

Ei lausuttavaa.

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

Ei lausuttavaa.

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

Tärkeä ja ajankohtainen osa ohjetta selkeästi esitettynä. Kohdassa 8.6 huomioitavaksi: kesäkuussa on 30 päivää (ei 31)--> PTV-tiedot oltava tallennettuna 30.6.2017 mennessä.

Liite 1: Keskeinen sanasto

Sanastossa pitää olla selkeät selitykset siinä oleville termeille/sanoilla - ei siis vain viittauksia Vahti-ohjeisiin. Sanasto on suppea - varmasti tarpeen lisätä siihen termejä. Esim. aikaisemmin ohjeessa viitataan esim. suojaustasoihin lyhenteillä ST (I-IV). Esim. nämä myös tähän mukaan. Yhtenäinen

termien käyttö tärkeää ja sen pitää toteutua jo ohjeessa eli terminologian pitää olla yhtenäinen ohjeen sisälläkin tai vähintään samaa tarkoittavat termit rinnalla ilmaistuna.

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

Ei lausuttavaa

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

Ei lausuttavaa

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

Hyvä tarkistuslista

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

Ei sellaisenaan selkeä ja vaikuttaa keskeneräiseltä. Tarkennusta ja esimerkkejä vaativa

Liite 6: Case-esimerkit

Muuhun ohjeeseen nähden eri tasolla ja näkökulma käyttäjän. Käytännön tarve niilläkin on, koska ovat helppolukuiset ja selkeät.

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

Koulutuksia eri kohderyhmille sisältö rakentuen ryhmän mukaan. Toteutuksia myös verkkokoulutuksina ja/tai webinaareina.

Muuta palautetta ohjeesta tai VAHTille?

Tiivistelmien ja koosteiden toteuttamista kannattaa miettiä.

Tillström Anne
Kouvola kaupunki - Tietohallinto