

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 laaja, erittäin hyödyllinen ja hyvin valmisteltu. Se auttaa ymmärtämään sen, mitä kaikkea asiantuntijoiden pitäisi huomioida mm. kehittämistyössä ja hankinnoissa. Toisaalta yksityiskohtaisuudessaan se ei aina kaikilta osin avaudu EI asiantuntijalle.

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Yleisenä huomiona, että vuosien 2018-19 aikana tulee viranomaisille käyttöön yhteinen kenttäjärjestelmä KEJO, johon liittyy kansallinen sähköinen ensihoitokertomus.

KEJOn ja ensihoitokertomuksen myötä mobiililaitteiden käyttö TUVEssa ensihoitopalvelussa ja myöhemmin sosiaalitoimessa tulee merkittävästi lisääntymään.

Ohjeita tulisi miettiä myös sen käyttäjäkunnan näkökulmasta (ensihoitopalvelussa pelkästään 4000-5000 käyttäjää). Ohje tulee pitää yleisilmaisultaan sellaisena, että siitä on suurta hyötyä myös suurelle toimijajoukolle.

Asiointipalvelun omistajalle ohjeen hyödyntämisen ja periaatteiden noudattamisen voi tehdä hankalaksi se, että vaikutusmahdollisuudet valtion yhteisiin palveluihin ovat vähäiset ja tiedonsaanti varsinkin käyttöpalveluista ja tietoliikenteestä on ohjeen tarkkuudella vielä vaikeaa.

Onko ohjeesta mahdollista tuottaa lyhennetty versio (tietokortti-tyyppinen), joita esim. kehittäjien/päätöksentekijöiden/yrittäjien olisi hyvä vähintään huomioida työssään?

Mitkä olivat ohjeen parhaita asioita?

Ohje on käytännönläheinen ja selkeästi kirjoitettu. Käytännön esimerkit ja listaukset huomioitavista asioista ovat hyviä ja helpottavat jatkossa palvelujen hankintaa.

Ohje on erittäin yksityiskohtaisesti laadittu ja sisältää paljon alan asiantuntijoille suunnattua tietoa. Kuvat, taulukot ja case-esimerkit ansaitsevat kiitokset. Ohje tarjoaa konkreettisia ohjeita kaikille julkisen hallinnon sähköisten asiointipalvelujen hankintaan, suunnitteluun, toteuttamiseen, kehittämiseen ja ylläpitoon osallistuville päätöksentekijöille ja asiantuntijoille.

Yksityiskohtaiset kommentit

Luku 1 Johdanto

-

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

-

Luku 3 Sähköiset asiointipalvelut

Kirjoitustekninen kysymys luku 3.3. taulukossa on * ja ** merkintä, mutta mikä niiden merkitys on epäselvä

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

Tietoturva on tärkeä asia ja sen merkitys korostuu koko ajan. Ihmisten informointi ja tietoisuuden lisääminen on ensiarvoisen tärkeää.

Täydellisen tietoturvan tavoittelu ei kuitenkaan saa johtaa siihen, että sähköiset palvelut ovat liian vaikeakäyttöisiä esim vanhuksille. Lisäksi vanhuksien tai sairaiden henkilöiden kyky tai mahdollisuus antaa valtakirja sähköisessä järjestelmässä voi olla heikko tai sitä ei ole. Siten valtakirjan antamiseen tulee olla myös joku vaihtoehtoinen keino, joka ei edellytä sähköistä tunnistamista, jos henkilö ei sitä kykene tekemään.

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

Ohjeen luvun 5.3.4 mukaan ei-julkisen tiedon välittämiseen tulee käyttää ainoastaan sellaisia asiointipalvelun ulkopuolisia viestintäkanavia, joiden tietoturvallisuudesta palvelun omistaja voi varmistua. Erityistä varovaisuutta tulee ohjeen mukaan noudattaa sähköpostin, pilvipalvelupohjaisten ja sosiaalisen median viestintäratkaisujen käytössä. Normilla ei tarkoitettane, että asiointipalvelun ulkopuolisten järjestelmien käyttöä suosittaisiin tai sitä haluttaisiin laajentaa?

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

-

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

-

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

Taulukko 6 p.o Palvelutietovaranto ei palelutietovaranto

Liite 1: Keskeinen sanasto

Kun sanastossa viitataan selityskentässä muihin Vahti-ohjeisiin, olisi tarpeen olla linkki ko. ohjeeseen.

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

Korotetun ja korkean varmuustason vaatimuksia pitäisi selittää ja selventää tarkemmin vaikka esimerkein. Liite vaikuttaa keskeneräiseltä.

Liite 6: Case-esimerkit

-

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

Ohjeen sisällöstä kannattaisi tehdä eri kohderyhmille (kansalainen, yritys, hankintapäätöksen tekijä, kehittäjä jne.) koulutusaineistoa, joka pitäisi olla verkossa avoimesti saatavilla. Lisäksi kannattaisi järjestää verkossa toteuttavaa avointa ohjattua koulutusta. Koulutus kannattaisi jaotella useampaan osaan. Tästä koulutuksesta kannattaisi tehdä myös "kansalaistaito" tyyppinen koulutus, jolla varmistettaisiin se, että tämä osaaminen olisi tulevaisuudessa osa työelämävalmiuksia.

Muuta palautetta ohjeesta tai VAHTIille?

-

Puhto Maarit
Sosiaali- ja terveysministeriö - Tietoyksikkö