

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

Sähköisen asioinnin ohje on hyvin tarpeellinen. Tällaisen ohjeen avulla koko sähköisen asioinnin palvelua tuottava työryhmä pystyy yhdessä ymmärtämään millaisia asioita on otettava huomioon palvelun toteutuksessa.

Ohje on asiantuntijalukijoille sopivaa kieltä. Asiat on esitetty ymmärrettävästi. Kuvitus jäsentää tekstiä hyvin.

On oikein hyvä, että ohjeessa esitetään myös sähköisen asiointipalvelun käyttäjää koskevia asioita, jotka palvelua kehittävän työryhmän on syytä huomioida.

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Sähköisen asiointipalvelun kehittäjiä varten olisi hienoa olla sellaisten tietojärjestelmien rakentamisen suuntaa antava toimintakaavio, jolla jäsennetään kuinka palvelua kehitettäessä tietoturva tulee huomioitua sopivimmissa työvaiheissa. Tällainen prosessikaavio voisi olla vaikka liitteenä.

Myös suoranaisia esimerkkiratkaisuita turvalliseen asiakasviestintään turvapostilla, sähköisen allekirjoituksen vaihtoehtoihin ja muihin vastaaviin olisi hyvä saada joko tässä ohjeessa tai uusissa VAHTI-ohjekorteissa.

Verkkolähteet voisi koota sähköisessä julkaisussa sanastoliitteessä tai omana liitteenään kokoelmaksi. Ohjeen käsittämä aihepiiri vaatii siihen syventyvältä monien muiden lähteiden käyttöä ja asian jäsentämistä tukisi verkkolähteiden luettelo.

Vaikkakin tekstin kohderyhmä on asiantuntijat, niin silti joissakin tekstikohdissa lukemista häiritsee kieliasu. Julkaisun kielenhuollossa tekstin luettavuutta voi varmaan vielä parantaa.

Mitkä olivat ohjeen parhaita asioita?

Ohje auttaa ymmärtämään kuinka laaja-alaista osaamista työryhmä tarvitsee luotettavien, toimivien sähköisen asioinnin palveluiden kehittämisessä.

Ohje soveltuu kunnan ja kumppaneidensa sähköisen asioinnin palveluiden kehittämisen osaamisen lisäämiseen suomenkielisenä, avoimesti saatavilla olevana lähdelukemistona. Viittaukset muihin avoimiin aineistoihin auttavat löytämään syventävää tietoa.

Yksityiskohtaiset kommentit

Luku 1 Johdanto

Oikein hyvä, että jo alussa (sivu 4) tuodaan esille sähköiseen asiointipalveluun kohdistuviin uhkiin varautumisen tärkeys.

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

Keskeisten asioiden nostot lain kohdista auttavat ymmärtämään millaisia lakivelvoitteita on muistettava sähköisen asioinnin palvelua kehitettäessä.

Tämä luku sopisi myös selvittämään uuden EU tietosuoja-asetuksen suhdetta ”privacy shield”-sopimuksiin. Mukana olisi hyvä olla myös viite aiheetta syventäviin lähdeaineistoihin, joilla sähköistä asiointipalvelua kehittävä työryhmä voi ymmärtää voimaan astuvan EU tietosuoja-asetuksen ja ”privacy shield”-sopimusten keskinäisiä vaikutuksia.

Luku 3 Sähköiset asiointipalvelut

Kappaleen 3.2 kuvaus uhkaympäristöstä on oikein riittävä tässä ohjeessa.

Julkaisutekniikka näyttää aiheuttaneen alaviitteiden kanssa ongelmia. Taulukon 1 X* ja X** viitteiden merkitys jäi auki.

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

Luku antaa oikein hyvän kuvan siitä, kuinka vaativa tehtävä on toteuttaa luotettava, toimiva sähköinen asiointipalvelu jo pelkästään tietoturvaa koskevien tavoitteiden kannalta.

Luvun taulukot auttavat sähköistä asiointipalvelua toteuttavaa työryhmää muistamaan mitkä asiat tulee muistaa huomioida. On myös hyvä, että mukana on muistutus avoimen lähdekoodin komponenttien kanssa huomioitavista asioista.

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

Luku arkkitehtuurista tuntuu riittävältä tähän ohjeeseen. Luvun kuvitus on onnistunut ja tukee tekstiä. Erityisesti kuva 4 auttaa hyvin jäsentämään sähköisen asiointipalvelun toteuttamisen vaatimuksia.

Sivulla 20 suojaustason IV ja III vyöhykkeistä puhumisen sijaan tai rinnalla voisi harkita käytettäväksi yleisempiä ilmauksia. Esimerkiksi ”perustaso” ja ”korotetun turvallisuuden taso” tai ”korkeamman turvatason vyöhyke” tai jotain muuta vastaavaa.

Sivulla 23 analytiikkapalveluita kuvaavaan esimerkkiin voisi liittää arkkitehtuurikuvan, jossa näkyy miten henkilötieto voi analyysin lähtötietona ajautua palveluketjun läpi EU:n ulkopuoliseen tallennuspaikkaan, vaikka analyysipalvelu hankitaan suomalaiselta toimijalta. Tällainen kuva voisi auttaa palvelun omistajaa tunnistamaan esimerkiksi uuden EU tietosuoja-asetuksen velvoitteisiin kohdistuvan vaaran.

Kappaleessa 5.3.4 käsitellään asiakasviestinnän luottamuksellisuutta. Tässä kohden kaivattaisiin esimerkkejä, joiden avulla kehittäjätyöryhmä voi ymmärtää millaisia tietoja saa välittää millaisilla ratkaisulla. Syventävinä viitteinä voi antaa lähdeaineistoja, joista voi löytää julkishallinnolle annettuja suosituksia turvapostiratkaisuista ja vastaavista. Esimerkkien olisi tarpeen olla tietosisältöä kuvaavia, esimerkiksi viitaten ministeriöiden tai hallinnonalojen antamiin määräyksiin tai suosituksiin.

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

Luvussa 6 tai 7 tai liitteessä voisi esitellä hiukan tarkemminkin mitä muita vaihtoehtoja on tarjolla sähköiseen allekirjoittamiseen esimerkiksi markkinaehtoisilta toimijoilta. Esittelyssä voi viitata sopiviin syventäviin lähteisiin sekä mitä sellaisten vaihtoehtojen allekirjoituspalveluiden tai niitä tarjoavien palvelutoimittajien kanssa on erityisesti huomioitava.

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

Luku 7 kuvaa aihepiiriä yleisesti. Tässä luvussa esitettyjen seikkojen huomioiminen käytännöllisessä sähköisen asiointipalvelun kehittämisessä kaipaa tukimateriaaleja. Luvussa voisi viitata avoimesti saatavilla oleviin tukimateriaaleihin tai niitä voisi esittää VAHTI-ohjekorteissa tai kansalliseen palveluväylään liittyvissä toteutusohjeissa.

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

Sivulla 49 kannustetaan sähköisen asioinnin järjestämisestä vastaavia tahoja seuraamaan tukipalveluiden kehittymistä. Tähän kohtaan sopisi hyvin viite lähteeseen, jota kannattaa seurata.

Luvun 8 sisältö sopii ohjeeseen hyvin.

Liite 1: Keskeinen sanasto

Viittaukset EU-tietosuojan kokonaisuudistus VAHTI 1/2016 ohjeeseen voisi kohdentaa sanastoon.

Viittaus eIDAS asetuksen selitteeseen sähköisestä allekirjoituksesta olisi hyödykästä viitata verkkolähteeseen.

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

Kaupallisten tukipalveluiden hankintaan liittyvä ohjeistus on tarpeellinen.

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

-

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

Sähköisen asiointipalvelun suunnittelun ohjeistus on tarpeellinen.

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

Viittaus yksityiskohtaiseen lähteeseen sopisi tähän kohtaan.

Liite 6: Case-esimerkit

Uusissa VAHTI-ohjekorteissa voi jatkossa viitata artikkeleihin, joista löytää lisää käytännön esimerkkejä onnistuneista sähköisistä asiointipalveluista.

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

Puolen päivän esittelytilaisuus verkko-osallistumisen mahdollisuudella.

Verkostoitumistilaisuus, jossa sekä sähköisen asioinnin järjestämisestä vastaavat, projektihenkilöstö että palvelutoimittajan toteuttajat voisivat oppia samassa tilaisuudessa sähköisen asioinnin toteuttamista tämän ohjeen läpikäynnin kautta. Tilaisuus voi sisältää tuote- ja ratkaisuesittelyitä.

Muuta palautetta ohjeesta tai VAHTille?

Tällaisten suomenkielisten ohjeistojen tarjoaminen avoimesti saataville tukee Helsingin digitaalisten palveluiden järjestämistä.

Aaro Antero Hallikainen
Helsingin kaupunki, tietotekniikka- ja viestintäosasto