CSC-Tieteen tietotekniikan keskus Oy

Lausunto

17.02.2017

Asia: 888/00.01.00.01/2015

VAHTI 3/2017 Sähköisen asioinnin tietoturvallisuus -ohje

Lausunto - VAHTI 3/2017Sähköisen asioinnin tietoturvallisuus-ohjeluonnokseen

Yleistä

Yleinen palaute

Tietoturvallisuus on keskeisimpiä menestystekijöitä sähköisessä asioinnissa. Turvallisuuteen liittyvät riskit tulee torjua tai lieventää riittävän kattavasti, mutta palvelun tehokkuutta ja käytettävyyttä ei kuitenkaan saa vaarantaa liian jäykillä turvallisuuskontrolleilla.

On positiivista, että hallitusohjelmankin kannalta erittäin keskeisistä toiminnoista julkaistaan ohje, jonka avulla voidaan tukea hyvien turvallisuuskäytäntöjen toteuttamista riskienhallinnan kannalta parhaalla mahdollisella tavalla.

Ohjeluonnoksessa käydään läpi keskeisiä hyviä turvallisuuskäytäntöjä, mutta seuraavat seikat luonnoksessa kaipaavat vielä korjauksia ja selvennyksiä:

- Mitkä osat ohjeessa ovat opastuksia hyviin käytäntöihin, mitkä osat ovat vaatimuksia?
- Miten ohje suhtautuu Viestintäviraston arviointivaatimuksiin (Ohje tietoturvallisuuden arviointilaitoksille)? Entä muihin ohjeisiin:
    - KATAKRI
    - Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010)
    - Sisäverkko-ohje (VAHTI 3/2010)
    - Teknisen ICT-ympäristön tietoturvataso-ohje (VAHTI 3/2012)
    - Sovelluskehityksen tietoturvaohje (VAHTI 1/2013)
    - Valtionhallinnon toimitilojen tietoturvaohje (VAHTI 2/2013)
    - Päätelaitteiden tietoturvaohje (VAHTI 5/2013)
- Eri VAHTI-ohjeet voivat olla keskenään päällekkäisiä tai ristiriitaisia, miten tätä pitää tulkita erityisesti vaatimusten osalta?
- VAHTI 3/2017 -ohje sähköisen asioinnin tietoturvallisuudesta tulisi integroida VAHTI:n ”beta-ohjeisiin”, ks. https://beta.vahtiohje.fi
- Tietyillä erityissektoreilla on sektorikohtaisia erityistarpeita sekä -ratkaisuja. Esimerkiksi kaikki suomalaiseet korkeakoulut ovat käyttäneet luotettavaa ja laadukasta Haka-luottamusverkostoa jo yli 10 vuoden ajan. Sen piirissä on liki 300 palvelua, joihin

kirjaudutaan vuosittain n. 30 miljoonaa kertaa. Haka tulisi mainita lopullisessa ohjeessa suositeltuna valmiina ja tehokkaana ratkaisuna korkeakoulutukseen sekä tutkimukseen liittyvien palveluiden osalta.

- Ohjeluonnoksen liite 2 ”Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista” on hyvä lähtökohta vaatimusten konkretisointiin, mutta luonteeltaan vielä varsin yleinen. Tavoitteena tulisi olla selkeä ja konkreettinen vaatimuslista, jonka voisi liittää esim. vaatimusmäärittelyn tai hankintasopimuksen osaksi.
- Eri toimijoiden välisiä rooleja ja vastuita olisi hyvä tuoda ohjeissa selkeästi esille laatimalla esimerkiksi vastuutaulukko palvelun tilaajan, kehittäjän sekä tuottajan kesken.

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Ohjeesta jää epäselväksi, mitkä konkreettiset asiat ovat suosituksia. Suositukset tulisi yksilöidä selkeästi esim. graafisin elementein. Toivottavaa olisi myös esim. liitteenä annettava tiivis luettelo, jossa ohjeessa edellä kuvatut suositukset on koottu yhteen niin, että luettelon suositukset voi liittää esimerkiksi järjestelmähankinnan vaatimusmäärittelyyn (vrt. Haka-luottamusverkoston määrittäminen kilpailutuksessa: https://wiki.eduuni.fi/x/BYigAQ).

Mitkä olivat ohjeen parhaita asioita?

-

Yksityiskohtaiset kommentit

Luku 1 Johdanto

-

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

-

Luku 3 Sähköiset asiointipalvelut

Sivulla 9 ’sähköinen asiointipalvelu’ määritellään verkkopalveluksi, jossa asiakkaat voivat asioida viranomaisen kanssa tietoverkon avulla. Suomessa valtion ja kuntien viranomaiset vastaavat mm. koulutuksesta, joissa sähköinen asiointi on nopeasti yleistymässä. Olisi hyödyllistä tarkentaa, missä määrin tämä VAHTI 3/2017 -ohje ja sähköisen asioinnin kansalliset tukipalvelut koskevat oppilaitoksia, jotka käyttävät yhä enenevässä määrin sähköisiä asiointipalveluita (digitaalisia oppimateriaaleja) opetuksessa.

Nykymuotoinen suomi.fi-tunnistus sopii huonosti perusopetuksen tarpeisiin, koska a) opetuksessa ei pääsääntöisesti tarvita vahvaa tunnistamista, b) alaikäisillä ei ole vahvoja tunnistusvälineitä (esim. pankkitunnuksia tai mobiilivarmennetta), ja c) asiointipalvelut tarvitsevat tunnistuksen ja yksilöinnin lisäksi tietoja myös

oppilaan oppilaitoksesta, luokka-asteesta, ryhmästä yms., joita ei ole saatavissa suomi.fi-tunnistuksen yhteydessä. CSC – Tieteen tietotekniikan keskus Oy on kehittänyt vuosina 2015–2016 opetus- ja

kulttuuriministeriön rahoituksella ja ohjauksessa erityisesti perusopetuksen tarpeisiin sähköisen tunnistamisen tukipalvelua (lisätietoa osoitteessa www.mpass.fi), joka pyrkii ratkaisemaan sähköisten asiointipalveluiden haasteita opetustoimessa. Olisi tärkeää kartoittaa mahdolliset yhteistyö- ja synergiamahdollisuudet MPASS-tunnistusratkaisun ja suomi.fi.-tunnistuksen välillä.

Huomionarvoista myös on, että korkeakoulujen näkökulmasta on usein ongelmallista tulkita, mikä toiminta on viranomaistehtävää ja mikä ei. Tietohallinnon näkökulmasta ei liene tarkoituksenmukaista eikä tehokasta, että viranomaistehtäviä varten käytetään eri tukipalveluita (esim. tunnistamiseen) kuin muussa korkeakoulujen toiminnassa.

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

Ehdotamme lisättäväksi luvun neljä johdantokappaleeseen: ”Hyvän tiedonhallintatavan mukaisesti alla lueteltujen tietoturvaperiaatteiden toteutumistapa on syytä kirjata lyhyt muistio hanke- tai palvelukohtaisesti. Tällä tavoin esimerkiksi turvallisuusarvionnissa voi osoittaa, että periaatteita on pyritty soveltamaan käytäntöön.

Teknisten ratkaisujen osalta olisi hyvä myös lisätä viittaus Kyberturvallisuuskeskuksen julkaisemaan luetteloon hyväksytyistä salauskäytännöistä, koska tilanne näiden osalta voi muuttua nopeasti.

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

-

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

Lopullisen VAHTI 3/2017 -ohjeen terminologiassa tulee pyrkiä yhdenmukaisuuteen. Nyt erityisesti tunnistamiseen liittyvässä käsitteistössä on vaihtelevuutta läpi tekstin. Liitteen 1 sanastossa on kevyesti avattu tunnistamisen käsitteistöä, mutta selkeyden takaamiseksi sitä olisi kuitenkin syytä syventää. Korkeakoulukentällä toimii käyttäjähallinnan asiantuntijoiden muodostama identiteetinhallinnan hyviä käytänteitä yhteistyössä kehittävä vertaisryhmäperiaatteella toimiva korkeakoulujen IAM-verkosto, joka on laatinut mm. organisaatioiden identiteetinhallinnan ja tunnistamisen sanaston. IAM-verkoston sanastotyöryhmän sanasto on saatavilla verkoston wiki-sivuilta (vaatii tunnistautumisen): https://confluence.csc.fi/display/IAM/Sanasto.

VAHTI 3/2017 -ohjeluonnoksessa on omaksuttu eIDAS-asetuksen termi ’sähköisen tunnistamisen menetelmän varmuustaso’. Korkeakoulujen kielenkäytössä on englanninkielisestä termistä ’Level of Assurance’ totuttu käyttämään suomenkielistä termiä ’tunnistamisen vahvuus’.

Edellä mainitun IAM-verkoston näkemyksen mukaan termejä ’tunnistaminen’ ja ’tunnistautuminen’ ei pitäisi käyttää toistensa synonyymeina. Tiivistäen IAM-verkoston sanastosta, tunnistamisella tarkoitetaan henkilön identiteetin toteamista perustuen yhteen tai useampaan tunnistustekijään. Tunnistaminen on siis asiointipalvelun käynnistämä prosessi. Sen sijaan tunnistautuminen kuvaa varsinaista tunnistustapahtumaa käyttäjän näkökulmasta. Vastaavasti eri asioita kuvaavia termejä ’tunnistusmenetelmä’ ja ’tunnistamismenetelmä’ ei voi käyttää toistensa vaihtoehtoina.

Yleisenä suuntauksena viime vuosina on ollut siirtyä pois yksiulotteisesta ajattelusta, jossa tunnistamisen vahvuutta voidaan ilmaista skalaarisella suureella (esim. matala-korotettu-korkea). Sen sijaan tunnistamista on alettu ajatella moniulotteisena mallina, jossa ensitunnistusta ilmaistaan yhdellä suureella ja sähköistä tunnistusta toisella. Tämä malli mahdollistaa esimerkiksi pseudonyymin käyttäjän vahvan tunnistamisen. Tälle on tarvetta erityisesti silloin, kun käyttäjän henkilöllisyydellä ei ole palvelun kannalta merkitystä, mutta palvelun tulee varmistaa, että käyttäjä on sama henkilö, joka palvelussa on aiemmin vieraillut. Kiinnostavia edistysaskeleita tässä suhteessa ollaan ottamassa Yhdysvalloissa, jossa "VAHTI-suositus" NIST SP-800-63-3 on lausuntokierroksella (https://pages.nist.gov/800-63-3/).

Sivulla 43 kerrotaan, että suomi.fi-tunnistus tarjoaa kansalaisille "vahvan tunnistusmenetelmän sekä muita tunnistusmenetelmiä kuin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (533/2016) tarkoitettua vahvaa sähköistä tunnistamista." Tällä hetkellä suomi.fi-tunnistuksessa ei kuitenkaan liene muita vahvaa heikompia tunnistusvälineitä kuin Verohallinnon Katso-tunnisteet. Mikäli myöhemmin on tarkoitus mahdollistaa muita vahvaa heikompia tunnistusvälineitä, olisi syytä pohtia samassa yhteydessä, kuinka hyödyllisiä pelkät vahvaa heikommat tunnistusvälineet ovat yksinään. Samalla tulisi selvittää, olisiko syytä mahdollistaa suomi.fi-tunnistuksen kytkeminen erilaisiin käyttäjän ominaisuuksia (käyttäjäattribuutteja) sisältäviin tietovarantoihin niin, että suomi.fi-tunnistus voisi välittää eri julkisten palveluiden (esim. koulutus, sote) tarvitsemia tietoja käyttäjästä tunnistuksen yhteydessä. Käyttäjätietojen päälle olisi mahdollista rakentaa tehokkaita attribuuttipohjaisia valtuutusratkaisuja, kuten esimerkiksi: ”tätä oppimateriaalia saavat lukea kaikki kunnan X 1.–3. luokka-asteen oppilaat”.

Näin toimitaan esimerkiksi Virtu-luottamusverkostossa, johon viitataan ohjeluonnoksen sivulla 43. Virtu-luottamusverkostossa välitetään kirjautumisen yhteydessä tietoa käyttäjän ominaisuuksista (esim. käyttäjän organisaatio ja tehtävä), joiden perusteella palvelu tekee päätöksen siitä, mitä käyttäjä saa palvelussa tehdä. VAHTI 3/2017 -ohjeluonnoksessa kuvataan kuitenkin harhaanjohtavasti, että Virtussa välitettäisiin suoraan tieto käyttövaltuudesta. Tämä on teknisesti mahdollista, mutta näin ei Virtussa tällä hetkellä toimita, vaan palvelu päättelee käyttövaltuuden käyttäjäattribuuttien perusteella.

Lopullisessa ohjeessa tulisi selkeästi suosittaa välttämään palvelukohtaiseen käyttäjätunnukseen ja salasanaan perustuvaa tunnistamista. Sen sijaan sähköiset asiointipalvelut tulisi aina, kun se vain on mahdollista, liittää joko suomi.fi-tunnistukseen tai Virtu-luottamusverkostoon, jotta käyttäjän ei tarvitsisi hallita useita salasanoja.

Ohjeluonnoksessa on myös kuvattu erilaisia tunnistamisen menetelmiä, mutta joitakin olennaisia ja yleisesti käytettyjä tunnistamismenetelmiä on jäänyt mainitsematta. Yksityishenkilöiden tunnistamisessa ohje sivuuttaa vahvaa heikommat tunnistusmenetelmät, joskin näiden käyttöön suomi.fi-tunnistuksen kautta viitataan. Tunnistusmenetelminä mainitsematta jää vajaa 30 miljoonaa tunnistustapahtumaa vuodessa kattava korkeakoulujen ja tutkimuslaitosten Haka-luottamusverkosto. Hakassa kehitetään myös vahvempaa tunnistamista. Kehityksessä huomioidaan erilaiset käyttötapaukset, joissa voidaan mm. yhdistää tunnistaminen, käyttäjäattribuuttien nouto ja käyttövaltuuden selvittäminen yhteen tunnistustapahtumaan keräämällä tarpeellisia tietoja eri lähteistä (kuvaus käyttötapauksista Hakan wikissä: https://wiki.eduuni.fi/x/RwLGAQ). Koululaisten tunnistamisessa on mahdollista hyödyntää MPASS-tunnistusratkaisua (lisätietoa osoitteessa www.mpass.fi). Täysi-ikäisten yksityishenkilöiden tunnistamisesta vahvaa heikommassa käyttötapauksessa on mahdollista myös esim. Yle-tunnuksen tai sosiaalisen median tunnisteiden avulla.

Suomessa käytettäviä tunnistusratkaisuja olisi hyödyllistä konsolidoida suuntaan, jossa käyttäjä voi valita haluamansa tunnistusmenetelmän ja sama menetelmä hyväksyttäisiin useissa eri palveluissa. Tilanne, jossa käyttäjällä on kymmeniä huonolaatuisia käyttäjätunnuksia ja salasanoja muistilapuille kirjoitettuna on käytettävyyden ja tietoturvan näkökulmasta kestämätön. Tämä on mahdollista, jos yhteen tunnistustapahtumaan yhdistetään tunnistaminen, henkilön yksilöiminen ja hänen henkilötietojensa (käyttäjäattribuuttien) selvittäminen useista lähteistä yhtenä prosessina. Tulisi selvittää, voidaanko suomi.fi-tunnistusta kehittää siihen suuntaan, että se linkittäisi julkisten palveluiden kannalta olennaiset käyttäjän identiteetit eri tietolähteistä.

Asiointipalvelussa ja yhtenäisen tunnistuspalvelun kehittämisessä tulisi kiinnittää huomiota käyttäjän yksilöimisessä käytettävään tunnisteeseen. On olennaista varmistaa, että käyttäjä pääsee asiointipalvelussa samaan käyttäjäprofiiliin riippumatta käytetystä tunnistusmenetelmästä. Henkilötunnus on yleisesti asiointipalveluissa käytetty tunniste, mutta sen käyttämiseen liittyy HetiL:n määrittämiä rajoituksia. Sähköisen asiointitunnisteen käyttöä rajoittaa myös Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (21.8.2009/661). Tulisi pohtia, voisiko henkilötunnuksen tai sähköisen asiointitunnisteen käyttöä henkilön yksilöimisessä lainsäädännöllisesti vapauttaa tai vaihtoehtoisesti määritellä muu saatavilla oleva, yhtenäinen ja yleiskäyttöinen, mielellään yksinään käyttäjän ominaisuuksia paljastamaton tunniste.

Sivulla 45 todetaan: "Näissä järjestelmäintegraatioissa tulee käyttää oletusarvoisesti vahvasti todennettua käyttäjäidentiteettiä sekä vahvaa sähköistä tunnistamista esimerkiksi seuraavien integraatiopalveluiden yhteydessä." Käytettyjä käsitteitä tulisi kuitenkin tarkentaa, sillä ’vahvasti todennettu käyttäjäidentiteetti’ ja ’vahva sähköinen tunnistaminen’ (ks. tunnistuslaki) viittaavat perinteisesti luonnollisen henkilön tunnistamiseen. Luvussa 6.4.4. kuvataan kuitenkin tietojärjestelmiä ja oletettavasti järjestelmien välisessä tunnistamisessa tunnistetaan järjestelmä (esimerkiksi palvelinvarmenteella), ei luonnollinen henkilö.

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

Luvussa 7.1.3. kuvataan digitaalista allekirjoitusta. Tulisi kuitenkin tarkentaa, voidaanko symmetriseen salausmenetelmään perustuvaa allekirjoitusta kutsua digitaaliseksi allekirjoitukseksi, sillä tällöin käytännössä allekirjoituksen luontivälineet olisivat useamman tahon hallussa.

Yleisesti ottaen voidaan todeta, että ohjeen tavoitteet sähköisestä allekirjoituksesta ovat hyviä, mutta toimivat käytännön tekniset menetelmät sähköisen allekirjoituksen tuottamiseen ovat vielä kehitysasteella. Tämä onkin yksi olennaisin kehityskohta asiointipalvelujen ja tukipalvelujen kehittämisessä, jotta luotettavaa sähköistä viranomaisasiointia voidaan aidosti edistää. Menetelmien suunnittelussa on huomioitava yleinen tekninen kehitys, jossa kansalaisella ei välttämättä ole käytössään perinteistä työasemaa, johon esim. HST-kortin saa liitettyä, vaan allekirjoituksen tuottamisen on oltava mahdollista kansalaisen mobiilipäätelaitteella.

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

Kansallisten tukipalveluiden keskeinen tehtävä on tunnistaa suositellut kansalliset tukipalvelut, kuten Suomi.fi-palveluväylä, Virtu ja Haka.

Ehdotamme muutettavaksi otsikkoa 8.2.2 ”Standardinmukainen tietoturvallisuus” muotoon ”Hyvien teknisten käytäntöjen ja standardien mukainen tietoturvallisuus”.

Liite 1: Keskeinen sanasto

-

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

Tarkistuslista on erittäin kannatettava, mutta toteutus jää vielä ylimalkaiseksi. Ehdotamme täydennystä listaan niin, että huomioitavien asioiden kohdalla on selkeitä tehtäviä tai vaatimuksia:

- Mitä vaatimuksia palveluun kohdistuu?
- Palveluntarjoaja pystyy esittämään sertifikaatin tai lausunnon palveluidensa tietoturvallisuudesta (kyllä/ei)?
- Miten tiedon luottamuksellisuus suojataan?

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

-

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

-

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

-

Liite 6: Case-esimerkit

-

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Paljon.

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

-

Muuta palautetta ohjeesta tai VAHTIlle?

-

Kaila Urpo
CSC-Tieteen tietotekniikan keskus Oy - Urpo Kaila