Tunnistaminen ja luottamuspalvelut

Pääryhmän toinen kokous

1.4.2016

Viestintävirasto
Kyberturvallisuuskeskus

Esityslista

Adobe Acrobat
Document

Edellisen kokouksen pöytäkirja

- Pöytäkirja

Adobe Acrobat Document

- Asetus/laki päivän tilanne

Selvitys luottamusverkoston vahingonkorvausoikeudellisista kysymyksistä
Professori Olli Norros

Selvityksen tausta

- Tavoitteena on ollut laatia selvitys luottamusverkoston vahingonkorvausoikeudellisista kysymyksistä
  - » Kuvataan periaatteet, joiden perusteella vahinkoja arvioidaan luottamusverkostossa.
  - » Käydään läpi Viestintäviraston esiselvityksessä kuvattuja vahinkotilanteita ja mahdollisia muita vahinkotilanteita.
  - » Kuvataan erityisesti sopimuksen ulkopuolisiin vastuisiin liittyviä kysymyksiä.
  - » Laaditaan mahdollisuuksien mukaan mallisopimuslausekkeita, joita voidaan sisällyttää luottamusverkoston käytännesääntöihin ja hyödyntää toimijoiden kahdenvälisissä sopimuksissa.
- Selvitys jaetaan työryhmän jäsenille, kun se on valmis

Määräyksen tilannekatsaus

Kokous 1.3 - Rajapinnat

- Pääasiat
  - Rajapinnat
    - SAML
    - Open ID Connect
    - TUPAS
  - Rajapinnoissa välitettävät tiedot
    - Minimi datasetti
    - Muut välitettävät tiedot
- Keskeneräiset asiat
  - TUPAS-protokollan heikkouksien parantaminen ja siirtymäaika
  - TUPAS: välitettävä varmuustaso
  - Vähimmäisvaatimukset salaus- ja tiivistealgoritmeille sekä avainpituudet
  - VRK kortin istuminen luottamusverkostomalliin

Kokous 17.3 - auditointikriteerit

- Pääasiat
  - Työn pohjana toimijoilta pyydetty auditointiselvitys
  - Työryhmälle esitettiin kaksi vaihtoehtoa määräyksen tarkkuustasosta
  - Ei löydy yhtä yleisesti tunnettua standardia, joka kattaisi tunnistuspalvelun luotettavuuden kokonaisuudessaan – tarvitaan siis useampia
  - KATAKRIa ei vaadita
- Merkittävät muutokset aiempaan
  - KATAKRIA ei vaadita
  - Viestintäviraston määräyksessä on yleiset vaatimukset palvelun luotettavuudelle.
  - Viestintävirastolta esimerkkikriteeristö, joka kelpaa auditointikriteeristöksi myös rajat ylittävässä tunnistamisessa.
  - Viestintäviraston rekisteriin ei tule tietoa toimijoiden käyttämistä standardeista
- Keskeneräiset asiat
  - Palvelun hallintaan käytettävien työasemien eriyttäminen korotetulla ja korkealla tasolla
  - Hallintaverkon ja tuotantoverkon eriyttäminen toimistoverkosta korotetulla ja korkealla tasolla

Kokous 24.3 – rajat ylittävä tunnistaminen ja ilmoitukset

- Pääasiat
  - julkishallinnon asiointipalveluiden kustannuksista vastaa valtio
  - Kansallinen solmupiste PEPS tukee kaikkia luottamusverkostossa hyödynnettäviä protokollia
  - Ilmoitukset: nykyiset toimijat tekevät muutosilmoituksen 31.8.2016 mennessä
  - Ilmoitukset: tavoitteena, että tunnistus- ja luottamuspalveluille olisi yhtenäiset vaatimukset häiriöilmoittamisesta
- Keskeneräiset asiat
  - Rajat ylittävä tunnistaminen: miten rahaliikenne kulkee, jos kyseessä on yksityinen asiointipalvelu (ei ole määräysasia).
  - Häiriöilmoitusten välittäminen luottamusverkostossa (ei ole määräysasia)

Tulevat kokoukset

- 12.4 Arviointielimet ja välineiden sertifioijat
  - mitä vaatimuksia arviointilaitokselle asetetaan määräyksessä
  - mitä vaatimuksia arviointielimelle/sisäiselle tarkastuslaitokselle asetetaan määräyksessä
  - mitä vaatimuksia on tarpeen asettaa sertifioijalle (jotta voidaan nimetä), sertifiointimenettelylle ja luontivälineelle
- 2.5 Hyväksytyt luottamuspalvelut
  - Mitä Eidas-asetusta ja komission täytäntöönpanopäätöksiä täydentäviä vaatimuksia (standardiviittauksia) määräykseen otetaan palveluntarjoajalle ja palvelulle
- 9.5 Koko määräyksen läpikäynti
  - Määräysluonnos
  - MPS-luonnos
  - Luettelo tarvittavista suosituksista/ohjeista
- 10.6 lausuntojen läpikäynti
  - Lausuntoyhteenveto
  - Tehdyt määräys- ja MPS- muutokset

Kansainvälisten kokousten asiat

ENISA workshop on Security Certification of ICT products in Europe 16.3.2016

- Yleistä:
  - Teollisuus: tietoturvasertifikaattien oltava globaaleja (CCRA - Common Criteria Recognition Arrangement) – Venäjä ja Kiina mukaan
  - Komissio: tavoite hyvä, mutta ei voida odottaa (muutkaan eivät odota) – jatketaan eurooppalaisia hankkeita
- eIDAS –sertifiointi:
  - eIDAS - kaksi sertifiointia - palvelu/väline
  - luottamuspalvelut - asetus on selvä (accreditation framework)
  - luontivälineet - eIDAS säädäntöpohja ei määrittele, miten sertifioidaan
  - nykyisten sertifiointiskeemojen hyödyntäminen – SOGIS-MRA - toimijat hyväksytään sellaisenaan?
  - kansallinen asia nimetä

ENISA Art 19 17.3.2016

- eIDAS art 19 mukaiset luottamuspalveluiden vika- ja häiriöilmoitukset ENISAlle ja muille jäsenvaltioille
- kynnysarvot - high, medium, low
  - » voiko low nousta high-tasolle, jos kesto/vaikutus on laaja?
- esimerkkitaulukko: updated list of scenarios/examples
  - » määrittely H, M, L
- CIRAS-T Mock up
  - » tekeillä työkalu, jolla jäsenvaltiot voivat tehdä ilmoitukset

ENISA Trusted Services 17.3.2016

- uusi ryhmä: lähtökohta - TSP guidelines puuttuu
- ryhmässä ei secondary legislation asioita tai standardiasioita
- kohteena luottamuspalveluiden tarjoajat, valvontaelimet, luottavat osapuolet
- tavoite: vuoden loppuun mennessä kaksi ohjedokumenttia
- Aiheet (ENISA laatii ehdotuksen, esillä vahvimmin seuraavat):
  - » luottamuspalveluiden valvonnan prosessit
  - » CAB-toiminnan/auditoinnin ohjeistus

ETSI ESI tilanne (1)

- julkaistu helmikuussa 2016
  - **EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers**
  - **EN 319 411-1 v1.1.1 General requirements**
  - **EN 319 411-2 v2.1.1 Requirements for trust service providers issuing EU qualified certificates**
  - **EN 319 421 v1.1.1 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps**
  - **EN 319 412-1 v1.1.1 Overview and common data structures**
  - **EN 319 412-2 v2.1.1 Certificate profile for certificates issued to natural persons**
  - **EN 319 412-3 v1.1.1 Certificate profile for certificates issued to legal persons**
  - **EN 319 412-4 v1.1.1 Certificate profile for web site certificates issued to organisations**
  - **EN 319 412-5 v2.1.1 QCStatements**
  - **EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles**

ETSI ESI tilanne (2)

- äänestyksessä huhtikuussa 2016
  - **EN 319 122-1 v1.1.0 CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures**
  - **EN 319 122-2 v1.1.0 CAdES digital signatures; Part 2: Extended CAdES signatures**
  - **EN 319 132-1 v1.1.0 XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures**
  - **EN 319 132-2 v1.1.0 XAdES digital signatures; Part 2: Extended XAdES signatures**
  - **EN 319 142-1 v1.1.0 PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures**
  - **EN 319 142-2 v1.1.0 PAdES digital signatures; Part 2: Additional PAdES signatures profiles**
  - **EN 319 102-1 Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation**
  - **EN 319 162-1 Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers**
  - **EN 319 162-2 Associated Signature Containers (ASiC); Part 2: Additional ASiC containers**

ETSI ESI tilanne (3)

- muita hyväksyttyjä/julkaistuja
  - **TS 119 172-1 Signature policies; Part 1: Building blocks and table of contents for human readable signature policy documents**
  - **TS 119 612 v2.1.1 Trusted Lists. An update of TS 119 612 was approved at ESI#54 (26-28 January 2016).**
  - **TR 119 300 Business guidance on cryptographic suit**es

ETSI ESI tilanne (4)

- Uusia työkohteita
  - study for standardization of long term data preservation services, including preservation of/with digital signatures
  - Update policies for TSP issuing certificate to take into account requirement of eIDAS eID assurance levels particularly for enrolment / registration
  - How to express eID minimum attribute set using 319 412-2/3 certificate profile
  - Requirements for CRL / OCSP services beyond the validity of certificates
  - Policy requirements for TSP issuing code signing certificates
  - Maintaining alignment of 411-1 to CAB-Forum requirements
  - DTR/ESI-0019500 Business Driven Guidance for Trust Application Service Providers (Registered Electronic Delivery and Registered Electronic Mail)

Viestintä

Teemakuukausi

- Ti 5.4 Viestintäviraston uutinen ja 1. teema julkaisu
- Loput julkaisut vähintään kerran viikossa huhtikuun ajan
- Sisältö:
  - » Kansallinen tunnistaminen
    - Mihin vahvaa sähköistä tunnistamista tarvitaan
    - Mikä tekee tunnistuspalvelusta vahvan
    - Mitä on tarjolla käyttäjille nyt
    - Välityspalvelut
    - Tunnistamisen välittäminen julkishallinnossa
  - » Rajat ylittävä tunnistaminen
    - Miten toimii (Espanja-Suomi pilotti)
    - Mistä luottamus syntyy
    - Millaisiin palveluihin voi tunnistautua
  - » Luottamuspalvelut

KIITOKSET KAIKILLE TEKSTINTUOTTAJILLE!

Muut asiat: Käytännesäännöt

Käytännesääntökokous 12.4.2016

- Odotetaan työryhmältä viimeistään 4.4. tietoa
  - mitä käytännesääntöjen kohtia kokouksessa on tarpeen käsitellä
  - yleistason tai yksityiskohtaiset näkökohdat em. kohdista
  - => Laadimme kokouksen esityslistan em. perusteella
- Voitte erittäin mielellään tarjoutua myös alustamaan tai vetämään keskustelun jonkin kohdan osalta

Sisällys

1. Johdanto ja ohjeen tarkoitus
2. Aikataulu ja eIDAS
3. Määritelmät
4. Säännöshierarkia

5. Sopimusmallit

5.1 Sopijaosapuolet

5.2 Tunnistuspalveluntarjoajan omalle vastuulle ja luottamusverkoston yhteistyövastuulle kuuluvat asiat

5.3 Tunnistuksen varmuustasot

5.4 Tekniset rajapinnat ja tunnistamistietojen vähimmäissisältö ("minimum data set")

5.5 Tietoturvahäiriöt

5.6 Toimivuus: käytettävyys, huoltokatkot, vikatilanteet ja muutokset

5.7 Tunnistustapahtumien välittämisen keskeyttäminen

5.8 Yhteistyö virhetilanteiden selvittämiseksi

5.9 Tietosuoja

5.10 Tunnistusverkostopalvelun käyttöön liittyvät maksut

5.11 Sopijapuolten keskinäinen vastuunjako (vahingonkorvaukset)

5.12 Salassapito

5.14 Sopimusmallin muuttaminen

5.13 Sopimuksen siirtäminen ja päättyminen

5.14 Riitaisuuksien ratkaiseminen

[5.] Sopimusmallit

- Sopimusvelvoitteet yleisellä tasolla:

1. **Tunnistusvälineen tarjoajan** on tarjottava välineensä kaikille välityspalveluille välitettäväksi näiden niin halutessa.
2. **Välityspalvelulla** ei ole ehdotonta laissa säädettyä pakkoa välittää kaikkia tunnistusvälineitä.
   - Lain tavoite on, että asiointipalveluita tarjoavat toimijat voisivat hankkia tunnistuspalvelut halutessaan vain yhdeltä toimijalta.
3. **Sama toimija** voi toimia sekä tunnistusvälineen tarjoajana että välityspalvelun tarjoajana.
   - Jos tunnistusvälineen tarjoaja myös "välittää" omaa tunnistustaan, toiminta kuuluu luottamusverkostoon, mutta ei siis velvoita välittämään kaikkien muiden tunnuksia (mutta ks. kohta 1, on tarjottava välineensä kaikille välityspalveluille)
4. **(Uusi) Tunnistuspalveluntarjoaja** voi pyytää Tunnistuspalveluntarjoajaa tekemään sopimuksia laissa ja näissä käytännesäännöissä kuvatuilla ehdoilla

Muut asiat: eDuuni

eDuuni

- Luottamusverkoston käytännesääntöjen valmistelu ...
- Vivin määräystyöryhmän (M72) kokoukset ...
- Vivin määräys- ja ohjevalmistelun taustadokumentit ...
- Vivin määräysvalmistelu M72 luonnokset ...
- Viestintäviraston tunnistus- ja luottamuspäätyöryhmän kokoukset ...

Muut asiat: ???

Seuraavat kokoukset

Seuraavat kokoukset

- Käytännesääntökokous
  - » TI 12.4.2016 klo 9-12
- Määräystyöryhmä
  - » TI 12.4.2016 klo 13-15.30
- Päätyöryhmä 3/2016
  - » KE 1.6. klo 12.30-15.30

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi