

# Esityslista 1-2015

## Teknisen ryhmän kokous

|               |                                                                                             |
|---------------|---------------------------------------------------------------------------------------------|
| Aika:         | Torstai 10.9.2015 klo 14:00 - 15:45                                                         |
| Paikka:       | Verkossa <a href="http://connect.funet.fi/haka">http://connect.funet.fi/haka</a>            |
| Osallistujat: | Jokaisella luottamusverkoston jäsennalla on oikeus asettaa edustajansa tekniseen tyoryhmaan |



Verkkokokous tallennetaan. Tallennetta käytetään läsnäolijoiden toteamiseen ja tukena muistion kirjoittamiselle. Tallennetta ei julkaista.

## Esityslista

1. Kokouksen avaus
2. Valitaan puheenjohtaja ja sihteeri
3. Todetaan läsnäolijat
4. FunetEduPerson-skeeman (FEP) versio 2.2 käyttöönotto

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a. Esittely:                                | <p>FEP-päivitystä on valmisteltu ohjausryhmän 1/2013 kokouksen toimeksiannosta. Huhtikuussa 2015 päivittyi schac-skeema, johon FEP tukeutuu. Haka-operointi on valmistellut päivitystä yhteistyössä IAM-verkoston kanssa. Esitys FEP versioksi 2.2 löytyy Haka-wikistä osoitteella: <a href="https://confluence.csc.fi/x/yQwIAg">https://confluence.csc.fi/x/yQwIAg</a>.</p> <p>Keskeiset muutokset skeemaan on merkitty sinisellä värillä ja lueteltu changeLog-kappaleessa. Taustatietoa päivityksestä on wikin navigaatioissa versioluonnoksen yläsivuilla.</p> <p>Skeemamuutoksen lisäksi Hakan IdP-ympäristön muutokseen vaikuttaa keväällä 2015 julkaistu Shibboleth IdP ohjelmiston versiotason 3 valmistuminen. Organisaatiot joutuvat päivittämään IdP:nsä uuteen versioon syksyn aikana tai viimeistään keväällä 2016. Tällä perusteella Haka-operointi esittää uuden skeemaversion käyttöönottamista viimeistään 4.1.2016 mennessä, jonka jälkeen skeemaversio 2.1 katsottaisiin vanhentuneeksi.</p> |
| Hak a-<br>oper<br>oinni<br>n<br>esity<br>s: | <p>Esitetään Haka ohjausryhmän 2.10.2015 pidettävälle kokoukselle 3/2015 funetEduPerson-skeeman version 2.2 vahvistamista käyttöönotettavaksi viimeistään maanantaina 4.1.2016. Tämän jälkeen skeemaversio 2.1 katsotaan vanhentuneeksi ja sitä ei pidä enää käyttää.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Päätös:                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

5. SHA2-allekirjoitusalgoritmin käyttöön siirtyminen

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a. Esittely: | <p>SHA1-allekirjoitusalgoritmi on <b>tunnistettu</b> heikoksi jo vuonna 2005. OWASP-säätiö <b>kehottaa</b> välttämään heikkojen salausalgoritmien käyttöä.</p> <p>Hakassa SHA hajautusalgoritmi on käytössä palvelun (SP) tuottaman autentikaatiopyynnön ja tunnistuslähteen (IdP) tuottaman autentikaatiovastauksen allekirjoituksissa. Edellisten lisäksi algoritmia käytetään HTTPS-liikenteen suojaamiseen käytettyjen varmenteiden allekirjoituksissa.</p> <p>Google on <b>ilmoittanut</b> suhtautuvansa SHA1-algoritmiin vanhentuneena ja varoittaa käyttäjiä turvattoman algoritmin käytöstä Chrome-selaimessaan. Shibboleth-konsortio on julkaissut aikataulun IdP-ohjelmiston versiotasoon 3 siirtymiselle ja Haka-operointi on tästä erikseen <b>tiedottanut</b>.</p> <p>Hakassa yleisesti käytössä oleva Shibboleth SP-ohjelmiston viimeisin versio (kirjoittaessa V2.5.5) tukee sellaisenaan uudempaa SHA2-algoritmia. Hakassa yleisesti käytetty Shibboleth IdP-ohjelmiston versiotason 2 haaran viimeisin versio (kirjoitettaessa V2.4.4) pystyy tarkistamaan SHA2-allekirjoituksen ja ulkopuolisella laajennuksella myös tuottamaan SHA2-allekirjoituksia. Shibboleth IdP versiotason 3 haaran viimeisin versio (kirjoitettaessa V3.1.1) pystyy tarkistamaan ja tuottamaan SHA2-allekirjoituksia sellaisenaan.</p> <p>Hakassa käytettävä <b>SAML-profiili</b> velvoittaa käyttämään suojattuja HTTPS-päätepisteitä autentikaatioviestien välittämisessä. Mm. phishing- ja man-in-the-middle -hyökkäyksien ehkäisemiseksi HTTPS-liikenteessä ei pitäisi käyttää heikompia algoritmeja, mitä on käytössä SAML-viestien suojaamiseen. Näin ollen on perusteltua siirtä SHA2-varmenteiden käyttöön myös Hakassa käytettävässä HTTPS-viestinnässä. Funet <b>varmennepalvelusta</b> on saatavilla SHA2-menetelmällä allekirjoitettuja palvelinvarmenteita.</p> |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hak<br>a-<br>ope<br>roin<br>nin<br>esit<br>ys: | <p>Päätetään, että Hakassa käytettyjen SAML-viestien allekirjoittamisessa on käytettävä vähintään SHA2-vahvuista allekirjoitusmenetelmää viimeistään vuoden 2016 toisesta vuosineljänneksestä alkaen.</p> <p>Päätetään, että Hakassa SAML-viestien välittämiseen käytettävien HTTPS-päätepisteiden suojaamiseen on käytettävä vähintään SHA2-vahvuisella menetelmällä allekirjoitettuja varmenteita viimeistään vuoden 2016 toisesta vuosineljänneksestä alkaen.</p> |
| Pä<br>ätö<br>s:                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

6. Muut keskusteluasiat
7. Kokouksen päättäminen