

Muistio 1-2015

Teknisen ryhmän kokous

Aika:	Torstai 10.9.2015 klo 13:55 - 15:20
Paikka:	Verkossa http://connect.funet.fi/haka
Osallistujat:	Haka-operaattori: Kari Laalo Keijo Korte Sami Silén Arto Tuomi Osallistujat Juha Nyholm Leena Heino Pekka Kuronen Reijo Rosti Jari Järvinen Veli-Matti Vimpari Tero Oinonen Mikael Linden Mika Tiainen Max Österman Viljo Viitanen Ismo Aulaskari Heikki Ruhanen Matti Tiitinen Jiri Sariola Mika Salo Markus Hagman Katarina Stubbe Sami Mäkinen Antto Sierla Heikki Ruhanen Janne Lauros Jouko Rintamäki Maarit Saaresto Toni Säämänen Sami Mäkinen Mikko Kuja-Lipasti

Kokousmuistio

- Kokouksen avaus
 - Kari Laalo avasi kokouksen klo. 13:55
- Valitaan puheenjohtaja ja sihteeri
 - Valittiin puheenjohtajaksi Kari Laalo ja sihteeriksi Keijo Korte.
- Todetaan läsnäolijat
 - Päätettiin, että läsnäolijat todetaan ACP-osallistujaluettelosta. Sovittiin, että mikäli esityksistä eroavia ehdotuksia ilmenee, on ne esitettävä ääneen sen riskin pienentämiseksi, että joku esiintyy väärällä nimellä.
- FunetEduPerson-skeeman (FEP) versio 2.2 käyttöönotto

a. Esittely:	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: https://confluence.csc.fi/x/yQwIAg. Keskeiset muutokset skeemaan on merkitty sinisellä värillä ja lueteltu changeLog-kappaleessa. Taustatietoa päivityksestä on wikin navigaatioissa versioluonnoksen yläsivuilla. 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.
--------------	---

Hak a- oper oinni n esity s:	Esitetään Haka ohjausryhmän 2.10.2015 pidettävälle kokoukselle 3/2015 funetEduPerson-skeeman version 2.2 vahvistamista käyttöön otettavaksi viimeistään maanantaina 4.1.2016. Tämän jälkeen skeemaversio 2.1 katsotaan vanhentuneeksi ja sitä ei pidä enää käyttää.
Kesk ustel u:	Leena Heino: FEP 2.2:n 2.1 changes osiossa typo funetEduPersoLearnerId, Person sanasta puuttuu n-kirjain. Jari Järvinen: Tekstin muuttaminen siten että attribuutin "funetEduPersonProgram" osalta viittaus tilastokeskuksen ensisijaisuuden poistetaan. Leena Heino: Pienet tekniset muutokset tai selvennykset kannattaa varmaan tehtä operaattorin toimesta ilman sen suurempaa hyväksymisprosessia.
Päät ös:	18 / 27 osallistujaa kannattaa uuden FEP-skeeman käyttöönottoa. Kukaan ei vastustanut. Päätettiin ottaa käyttöön uusi FEP-skeema operoinnin esittämän aikataulun mukaisesti operaattorin tehtyä keskustelussa esiintulleet vähäiset korjaukset.

5. SHA2-allekirjoitusalgoritmin käyttöön siirtyminen

a. Esit tely:	SHA1-allekirjoitusalgoritmi on tunnistettu heikoksi jo vuonna 2005. OWASP-säätiö kehottaa välttämään heikkojen salausalgoritmien käyttöä. 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. Google on ilmoittanut 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 tiedottanut. 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. Hakassa käytettävä SAML-profiili 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 siirtyä SHA2-varmenteiden käyttöön myös Hakassa käytettävässä HTTPS-viestinnässä. Funet varmennepalvelusta on saatavilla SHA2-menetelmällä allekirjoitettuja palvelinvarmenteita.
Hak a- ope roin nin esit ys:	Päätetään, että Hakassa käytettyjen SAML-viestien allekirjoittamisessa on käytettävä vähintään SHA2-vahvuista allekirjoitusmenetelmää viimeistään vuoden 2016 toisesta vuosineljänneksestä alkaen. Päätetään, että Hakassa SAML-viestien välittämiseen käytettävien HTTPS-päätepisteiden suojaamiseen on käytettävä vähintään SHA2-vahvuisella menetelmällä allekirjoitettuja varmenteita viimeistään vuoden 2016 toisesta vuosineljänneksestä alkaen.
Kes kus telu	Viljo Viitanen: Hakassa mukana olevilla ei ole valtiotason uhkaajia toivottavasti (jotka sha1:n ehkä murtavat nyt). Kerron jo nyt että vastustan noita aikoja, ovat tarpeettoman tiukat. Voisi olla 2017 alkaen kuten valtaselaimilla. (Chromessa 2016 loppuun voimassa olevat sha1 varmenteet ovat ok) Leena Heino: Kun web ja haka-varmenteet on erotettu, niin tuo sha2 muutos on mennyt aika kivuttomasti.
Pä ätö s:	Päätettiin, että Hakassa käytettyjen SAML-viestien allekirjoittamisessa on käytettävä vähintään SHA2-vahvuista allekirjoitusmenetelmää viimeistään vuoden 2016 toisesta vuosineljänneksestä alkaen. Toistaiseksi ei oteta kantaa SAML-viestien allekirjoittamisessa käytettyyn allekirjoitusalgoritmiin. 17 / 27 osallistujaa kannattaa päätöstä. Kukaan ei vastustanut.

6. Muut keskusteluasiat

- Kirjautumistilastojen kehittäminen
 - Todettiin, että kirjautumistilastoihin voi suhtautua lähtökohtaisesti julkisena tietona, joskin materiaalista on yksilönsuojan turvaamiseksi suodatettava pois sellaiset tilastorivit, joissa on vain yksittäisiä kirjautumisia yksittäisiin palveluihin.
- Mikael Lindén muistutti eduGain + Geant käyttöönotoista + Tietosuojakäytäntö.

7. Kokouksen päättäminen

- Puheenjohtaja päätti kokouksen klo. 15:20