

Muistio 1-2018

Aika:	27.4.2018 klo 09:30-10:30
Paikka:	Videokokous Huom! Liittyessä videokokoukseen kirjaa osallistujanimesi: Etunimi Sukunimi (Organisaatio), jotta osallistajat voidaan todeta asiakohdassa 3. Join from PC, Mac, Linux, iOS or Android: https://cscfi.zoom.us/j/898981760 Or an H.323/SIP room system: H.323: 109.105.112.236 or 109.105.112.235 Meeting ID: 898 981 760 SIP: 898981760@109.105.112.236 or 898981760@109.105.112.235
Osallistujat:	Kari Laalo (CSC) Arto Tuomi (CSC) Timo Mustonen (CSC) Pasi Tukiainen (Haaga-Helia) Kari Kumpulainen (Pelastusopisto) Satu Torikka (CSC) Mika Tiainen (Saimaan AMK) Barbro Sjöblom (Åbo) Markku Hihnala (Oulun yliopisto) Jussi Tirkkonen (TTY) Reijo Rosti (Certia) Joona Rantapere (Turun AMK) Sami Mäkinen (JAMK) Jussi Saine (Polamk) Ville Liukkonen (Xamk) Scott Alexander (Humak) Elina Toivanen (Turun yliopisto) Mika Salo (Laurea) Kenneth Mattson (Novia)



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

Esityslista

1. Kokouksen avaus
 - Kari Laalo avasi kokouksen klo. 9:32
2. Valitaan puheenjohtaja ja sihteeri
 - Valittiin puheenjohtajaksi Kari Laalo ja sihteeriksi Timo Mustonen
3. Todetaan läsnäolijat
 - Päätettiin, että läsnäolijat todetaan Zoom-videoneuvotteluhuoneen osallistujaluettelosta
4. FunetEduPerson-skeeman (FEP) versio 2.3 käyttöönotto

Esi tel y:	Hakan IAM-verkostossa ja eriässä Haka-kirjautumiseen tukeutuissa palveluissa on noussut esille tarve muuttaa Hakassa yleisesti käytetty henkilötunniste eduPersonPrinsipalName (eppn) pysyväksi. Hakassa on määritelty, että palvelun on oletettava tietyn tunnisteiden haltijan vaihtuneen, jos tunnisteella ei olla kirjaututtu palveluun 24 kk:n kuluessa. On syntynyt epäilystä, noudattavatko kaikki palvelut tätä vaatimusta. Toisaalta, esimerkiksi Refeds Assurance Framework kehityksessä on otettu lähtökohdaksi pysyvät eppn-tunnisteet (katso Mikael Lindenin esitys IAM-verkoston tapaamisessa 19.4.2018) IAM-verkoston kokouksessa 10.10.2017 päätettiin aikataulusta, jolla ehdotettiin muutosta edistettävän. Koska Hakassa on ollut mahdollista kierrättää tunnisteita uudelle käyttäjälle kahden vuoden varoajalla, on pysyväksi siirtymisessä noudatettava aikataulua, joka huomioi kierrättämisen mahdollisuuden. IAM-verkosto päätti ehdottaa aikataulua: • päätöksen prosessointi Hakan toimielimissä: viimeistään kesällä 2018 • Organisaatiot lakkaavat eppn-tunnisteiden kierrättämisen: viimeistään 1.1.2019 • Palvelut voivat luottaa eppn-tunnisteiden pysyvyyteen: aikaisintaan 1.1.2021 Muutosta on käsitelty IAM-verkoston tapaamisissa ja siitä on tiedotettu Hakan viestintäkäytäntöjen mukaisesti Hakan blogissa. Operointi on valmistellut funetEduPerson-skeemasta luonnoksen versiolla 2.3. Luonnos löytyy tästä linkistä. Luonnoksessa on huomioitu IAM-verkoston suunnittelema aikataulu ja uuden version voi asettaa astumaan voimaan välittömästi.
Ha ka- op ero inni n esit ys:	Esitetään Haka-ohjausryhmälle operoinnin valmisteleman funetEduPerson-skeeman version 2.3 vahvistamista käyttöön otettavaksi. Versiomuutos tulee voimaan välittömästi päätöksen yhteydessä.
Ke sku stel u:	Kari Laalo avasi operaattorin esitystä, operaattorin tekemää esitystä puollettiin. Keskusteltiin lyhyesti aikataulusta ja Haka-kotiorganisaatioihin kohdentuvista muutostoimenpiteistä, operaattori tähdensi että eppn-attribuutin kierrätyksen tulee loppua viimeistään 1.1.2019.
Pä ätö s:	Kukaan ei vastustanut, päätettiin edetä operaattorin esityksen mukaisesti.

5. Uusien SAML-käyttäjätunnisteiden omaksuminen Hakaan

Esittely:	SAML2-standardin osaksi on tulossa uusi tapa esittää käyttäjätunniste (https://wiki.oasis-open.org/security/SAMLSubjectIDAttr). Hakassa käyttäjätunnisteina käytetään tällä hetkellä EduPersonPrincipalName- (EPPN) ja EduPersonTargetedId-attribuutteja (EPTID) sekä NameID:na esitettäviä transientid:ta ja persistentid:ta. Korkeakoulut Suomessa ovat havainneet ongelmaksi EPPN-attribuutin mahdollisen kierrättämisen uusille käyttäjille ja sopineet sitoutuvansa sen pysyvyyteen. EduPersonTargetedId:n käyttämiseen on alusta asti liittynyt ongelmia, joten se ei ole yleistynyt käyttöön. Uudet esitellyt tunnisteet ovat General Purpose Subject Identifier ja Pairwise Subject Identifier. Ensimmäisen ollessa käyttäjälle muuttumaton tunnisteen kaikissa käyttäjän käyttämässä palveluissa, jälkimmäinen tunnisteen on käyttäjä- ja palvelukohtainen. Muistuttavat siis hyvin paljon EPPN- ja EPTID-tunnisteita.
Haka- operoin nin esitys:	Annetaan Haka-operoinnille tehtäväksi valmistella uusien käyttäjätunnisteiden omaksumista Hakan käyttöön siten, että ne on otettavissa käyttöön Haka-kirjautumisessa, kun ao. SAML profiililuonnos vahvistetaan.
Keskust elu:	Arto Tuomi avasi operaattorin esitystä. Keskusteltiin lyhyesti EduPersonTargetedId:n käyttöön liittyvistä ongelmista, Arto Tuomi suositteli kaikkia asiasta enemmän kiinnostuneita tutustumaan Shibboleth-ohjelmiston wiki-sivuun , jossa kyseisen attribuutin käyttöön liittyviä ongelmia on kuvattu seikkaperäisesti.
Päätös:	Kukaan ei vastustanut, päätettiin edetä operaattorin esityksen mukaisesti.

6. Tiedotusasiat

- [SAML-vastausviestien salaaminen muuttumassa pakolliseksi](#)
- [Avoimen opiskelijat sisällytettäväksi affiliation student-arvoon](#)
- [Hakan keskitetyn vahvemman tunnistamisen palvelun uudet ominaisuudet 1-2018](#)

7. Muut keskusteluasiat

- Hakan metatiedossa olevien varmenteiden use-attribuuttimäärityksen uupuminen
 - Keskusteltiin ongelmasta liittyen Hakan resurssirekisteri-työkaluun ja metatietoon, joissa ei tällä hetkellä tueta use-attribuutin määrittämistä käytetyille varmenteille. Operaattori lisää tarkentavia ohjeita resurssirekisteri-työkaluun väärinkäsitysten minimoimiseksi tulevaisuudessa. Operaattori myös jatkoselvittää tarpeen use-attribuutin käyttöönotolle Haka-luottamuverkossa ja sen metatiedossa.

8. Kokouksen päätös

- Kari Laalo päätti kokouksen klo. 10:22