SAML-profiili

Haka SAML 2.0 -profiili 2.0

SAML 2.0 -profiililla varmistetaan SAML 2.0 -protokollaa käyttävien palveluiden yhteensopivuus määrittämällä käytettävät osat laajasta SAML 2.0 -standardista. Lisäksi määritetään joitakin implementointiin liittyviä yksityiskohtia yhteensopivuuden takaamiseksi.

Hakan uuden profiilin tavoitteena on yhteensopivuus sekä eduGAIN-palvelun käyttämän profiilin että julkishallinnon yhteisen SAML 2.0 -profiilin (ver 1.1) kanssa. eduGAIN:n ja julkishallinnon profiilit perustuvat SAML2 Interoperable Profile versioon 0.2. Laajalla yhteensopivuudella helpotetaan järjestelmäkehittäjien, ohjelmistotoimittajien ja järjestelmiä hankkivien organisaatioiden tehtäviä.

Hakan teknisen ryhmän kokous 4.10.2011 hyväksyi ehdotetun SAML 2.0 profiilin:

Haka SAML 2.0 -profiili versio 2.0

Hakan SAML 2.0 Web SSO -profiili perustuu julkishallinnon yhteiseen SAML 2.0 -profiiliin (ver 1.1). Julkishallinnon profiilin kolmannen sarakkeen yleiset kommentit koskevat myös Hakaa. Hakan lisäykset profiiliin on lueteltu alla.

Hakan lisäykset ja tarkennukset julkishallinnon profiiliin

Hakan SAML-profiili täydentää julkishallinnon yhteistä SAML 2.0 -profiilia (ver 1.1) seuraavilla lisäyksillä:

- Hakaan rekisteröidyt IdP- ja SP-palvelimet voivat käyttää kaikkien varmentajien X.509 -varmenteita (mukaanlukien itseallekirjoitetut varmenteet). Varmenteessa käytetyn RSA-avaimen minimikoko on 2048 bittiä.
- SP:n ja IdP:n SAML-viestien vaihtoon rekisteröidyt osoitteet tulee suojata TLS/SSL protokollalla.
- Haka-metadata on allekirjoitettu Funet-varmennepalvelun antamalla varmenteella. Metadatan käyttäjän tulee varmistaa allekirjoituksen lisäksi, ettei käytetty varmenne ole sulkulistalla.
- Kappaleessa Additional extensions määritellyn Single logout:in totetuttaminen on valinnaista.
- Hakassa välitettävät attribuutit on kuvattu ja määritelty FunetEduPerson-skeemassa.
- Rajatut attribuutit (scoped attributes). FunetEduPerson skeemassa on kaksi rajattua attribuuttia: eduPersonPrincipalName ja eduPersonScopedAffiliation. Kotiorganisaatiot saavat populoida rajatut attribuutit vain omistamillaan rajauksilla (esim. ePPN jalauros@csc.fi vain CSC:n IdP:n toimesta). Rajattua attribuuttia hyödyntävän tahon olisi suositeltavaa tarkistaa että rajaus on sallittu. Haka- operaattori julkaisee listan sallituista kotiorganisaatioiden rajauksista osana Haka-metadataa.

Voimaantulo

Profiili astui voimaan 1.12.2011.