Haka SAML 2.0 -profile 2.0

By defining sections of wide-ranging SAML 2.0 -standard, Haka SAML 2.0 -profile will ensure that services using SAML 2.0 protocol are compatible. In addition some implementation related details are defined to ensure compatibility.

The goal of the new profile is to harmonize the compatibility between eduGAIN and the Finnish public sector SAML 2.0 -profile (version 1.1). eduGAIN and the Finnish public sector profiles are all based on SAML2 Interoperable Profile version 0.2. Extensive compatibility will ease the work of system developers, software suppliers and organizations acquiring related information systems. Haka Operations Committee approved the proposed profile on 4th of October 2011.

Haka SAML 2.0 -profile version 2.0

The SAML 2.0 Web SSO -profile of Haka is based on the common SAML 2.0 profile of the Finnish public sector (ver 1.1). The general comments not targeting any federation in the third column apply to Haka as well. Haka profile additions are listed below.

Haka's additions and correctives to Finnish public sector profile

Haka's SAML profile additions to Finnish public sector SAML 2.0 -profile (version 1.1):

- IdP- and SP-servers registered to Haka are free to use any X.509 certificates (including self-signed certificates). Used RSA key must be at least 2048 bits.
- SAML-message exchange between IdP- and SP-servers must be secured byt using TLS/SLL protocol.
- Haka-metadata is signed with a certificate provided by Funet certificate service. In addtion to check the signature within the metadata, certificate revocation list must be monitored to detect if the certificate used for signing has been revocated.
- It is optional to implement Single logout defined in chapter Additional extensions.
- The attributes passed in Haka are described and defined in FunetEduPerson-schema.
- Scoped attributes. In FunetEduPerson-schema, two scoped attributes exist: eduPersonPrincipalName and eduPersonScopedAffiliation. Home organizations are allowed to populate the attributes only by using the scopes that they own (for example: ePPN account1@csc.fi is allowed only for IdP owned by CSC). It is recommended that services exploiting scoped attributes would verify this definition. The list of allowed scopes is published within Haka-metadata by the operator.

Effective date

New Haka profile will be effective on 1st of December 2011.