

Haka SAML 2.0 profile



Version	Date	Editor	Change
0.1	14.1.2010	Mikael Linden	Taken Virtu federation's SAML2 profile as a basis, and - dropped authentication context - advisory committee approves the CAs - Shibboleth-style scoping of attributes
0.2	22.1.2010	Arto Tuomi	- Universal scoping - Added Requested Attributes definition - validUntil attribute requirement for root element
0.3	25.1.2010	Mikael Linden	- clarifications
1.0	19.2.2010	Mikael Linden	- Approved by Haka operations committee 19.2.2010

Table of Contents

1. Introduction.....	2
2. SAML 2.0 profile for Web Single-sign on	2
2.1. SAML 2.0 deployment profile	2
2.2. Single Logout (optional).....	2
2.3. Identity Provider Discovery	3
3. Use of SAML 2.0 metadata	3
3.1. SAML 2.0 Metadata profile.....	3
3.2. Scoping of identities	3
3.3. Requested Attributes.....	4
Bibliography	4

Appendix A: Interoperable SAML 2.0 Web Browser SSO Deployment Profile, version 0.1 stable

1. Introduction

This document defines the SAML 2.0 profile for Haka federation, the identity federation for the Finnish higher education and research. Haka federation is operated by CSC, the Finnish IT Center for Science Ltd.

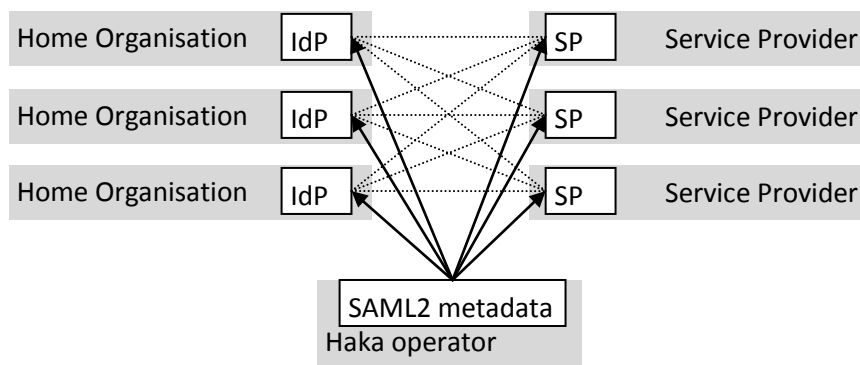


Figure 1. The technical architecture of Haka federation consists of SAML 2.0 Identity Providers (IdP) operated by end users' home organisations, SAML 2.0 Service Providers (SP) operated by organizations providing services to the end users and the SAML 2.0 metadata managed by the federation operator.

The technical architecture (Figure 1) of Haka federation is based on a full mesh of Identity Providers (IdP) and Service Providers (SP) who exchange SAML 2.0 assertions directly. As the operator of Haka federation, CSC manages and distributes the federation's SAML 2.0 metadata containing the Providers registered to the federation.

Attributes that the IdPs may deliver to the SPs are defined in the funetEduPerson (CSC, 2008) schema definition.

2. SAML 2.0 profile for Web Single-sign on

2.1. SAML 2.0 deployment profile

Haka federation uses the "SAML2Int" Interoperable SAML 2.0 Web Browser SSO Deployment Profile (Solberg;Maler;Cantor;& Johansson, 2009). The profile is available in Appendix A.

However, following amendments are made to the profile

- A secure transport connection (SSL/HTTPS) MUST be used for transporting authentication requests and responses. The operator of Haka federation will register only https endpoints (e.g. SingleSignInService, AssertionConsumerService) to the federation.

2.2. Single Logout (optional)

Identity and Service Providers MAY support the Single Logout protocol of SAML 2.0 as defined in section 3.7 of (Cantor;Kemp;Philpott;& Maler, 2005). Providers manifest their support to Single Logout by registering a Single Logout endpoint to the federation metadata. All Service Providers

that support Single Logout MUST both be able to initiate a logout, send a Logout request to the Identity Provider, as well as handle an incoming Logout request from the Identity Provider.

HTTP-REDIRECT binding MUST be used for logout requests and responses. Logout requests and responses MUST be signed.

To ensure the user experience, an Identity Provider registering a Single Logout endpoint MUST provide means for a user to assure of a successful logout. In the event of an unsuccessful logout request from an Identity Provider to a Service Provider, the Identity Provider MUST instruct the user of the steps involved in finishing the logout process. A Service Provider SHOULD register a Single Logout endpoint only if it can make sure that the end user's session is terminated in the application level, as well.

2.3. Identity Provider Discovery

In Haka federation, it is a responsibility of the Service Provider to decide, to which Identity Provider the end user is redirected for authentication. To assist the Service Provider in the decision, the Haka federation operator provides an Identity Provider Discovery service, which uses available means (typically, presents the end user a dialogue) to deduce the end user's Identity Provider.

The Identity Provider Discovery service implements the Identity Provider Discovery Service Protocol and Profile (Widdowson & Cantor, 2008).

3. Use of SAML 2.0 metadata

3.1. SAML 2.0 Metadata profile

Haka federation uses the SAML 2.0 Metadata interoperability profile version 1.0 (Cantor, SAML v2.0 Metadata Interoperability Profile Version 1.0, 2009).

However, following amendments are made to the profile

- when SAML assertions are signed and/or encrypted by an Identity or a Service Provider, a valid certificate issued by a CA approved by the federation's advisory committee¹ MUST be used. The operator of Haka federation will register to the federation metadata only certificates issued by an approved CA.
- metadata root element MUST contain a validUntil attribute

It is RECOMMENDED, that the Providers use certificates recognized by common web browsers (IE, Mozilla) in the browser facing https traffic.

3.2. Scoping of identities

For the security model of Haka federation, it is necessary to bind the end user's unique identifier to his/her home organisation in order to ensure that only his/her home organisation's Identity Provider(s) is (are) authoritative to claim his/her identity in the authentication response.

¹ Current list available in <http://www.csc.fi/haka/>

In scoped attributes, '@' sign is used to delimit the scope (the right hand side) from the rest of the attribute value. Currently, funetEduPerson (CSC, 2008) defines following scoped attributes

- eduPersonPrincipalName (e.g. bsmith@example.org)
- eduPersonScopedAffiliation (e.g. student@example.org)

The Haka federation operator provides a list of the scope values permitted for each Identity Provider². The list is provided using format(s) deemed currently appropriate.

Example (informative):

Suppose idp.example.org is the Example university's Identity Provider. Example university uses two scope values, "example.org" for employees and "student.example.org" for students. Following entry in the Shibboleth SAML2 metadata expresses the university's scopes

```
<EntityDescriptor entityID="https://idp.example.org/">
  <IDPSSODescriptor ...>
    <Extensions>
      <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
        regexp="false">example.org</shibmd:Scope>
      <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
        regexp="false">student.example.org</shibmd:Scope>
    </Extensions>
  </IDPSSODescriptor>
</EntityDescriptor>
```

When a Service Provider receives a scoped attribute from idp.example.org, it SHOULD ensure that scoped attributes, if any, carry either of the two scopes.

Examples of valid scoped attribute values from idp.example.org:

- eduPersonPrincipalName="bobsmith@student.example.org"
- eduPersonScopedAffiliation="employee@example.org"

Examples of invalid scoped attribute values from idp.example.org:

- eduPersonPrincipalName="bobsmith@staff.example.org"
- eduPersonPrincipalName="johndoe@bad-example.org"

3.3. Requested Attributes

One or several RequestedAttribute elements MAY be incorporated to SPSSODescriptor elements in the Haka federation metadata. Identity Provider SHOULD release to a Service Provider only attributes defined in metadata for each Service Provider entry.

Bibliography

Cantor, S. (2009). *SAML v2.0 Metadata Interoperability Profile Version 1.0*. OASIS.

² Current list available in <http://www.csc.fi/haka/>

Cantor, S., Kemp, J., Philpott, R., & Maler, E. (2005). *Assertions and Protocols for the OASIS Secure Assertion Markup Language (SAML) V2.0*.

CSC. (2008). *funetEduPerson schema*.

Solberg, A., Maler, E., Cantor, S., & Johansson, L. (2009, 11 2). *SAML2Int: Interoperable SAML 2.0 Web Browser SSO Deployment Profile ver 0.1 Stable (2.11.2009)*. Retrieved from <http://saml2int.org/profile/0.1>

Widdowson, R., & Cantor, S. (2008). *Identity Provider Discovery Service Protocol and Profile. Committee Specification 01*. OASIS.

Interoperable SAML 2.0 Web Browser SSO Deployment Profile

Versions

current
0.1 stable
Working draft

This deployment profile of SAML 2.0 Web Browser SSO defines a minimal set of requirements that entities need to support in order to be interoperable.

Service Providers and Identity Providers implementing this profile may interoperate with other entities implementing the same profile, as well as with entities that honor the conformance guidelines of Liberty Alliance for SP, SP-Lite, IdP and IdP-Lite.

```
$Id: saml2int-0.1.txt 165 2009-11-02 14:24:05Z andreas $
```

[Version history](#)

Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119](#).

Introduction

This deployment profile of SAML 2.0 Web Browser SSO defines a minimal set of requirements that entities need to support in order to be interoperable. The goals of this profile include:

- Easy implementation that can be based on available SAML libraries.
- Good support in current available SAML 2.0 software implementations.
- Minimal effort required to configure entities to support this profile from a default installation.
- Increased interoperability between SAML 2.0 implementations and deployment environments, thanks to a very limited set of required options.

This profile draws upon operational experience of several SAML-based federations in the higher-education and research community and reflects best current practice of a wide range of deployments involving web single sign-on. The authors believe that this profile has broad applicability outside the scope of education and research.

Interoperability

One of the main goals of this profile is to increase interoperability between deployments, as well as across SAML 2.0 implementations.

Service Providers and Identity Providers implementing this profile may interoperate with other entities implementing the same profile.

Specification Scope

The scope of this specification is a SAML 2.0 deployment profile, "Single Sign-On Profile", that limits the options available in SAML 2.0 SSO to increase interoperability between deployments.

References to SAML 2.0 specification

When referring to elements from the SAML 2.0 core specification [saml2-core](#), the following syntax is used:

`<samlp:ProtocolElement>` - for elements from the SAML 2.0 Protocol namespace.
`<saml:AssertionElement>` - for elements from the SAML 2.0 Assertion namespace.

When referring to elements from the SAML 2.0 metadata specification [saml2-metadata](#), the following syntax is used:

`<samlmd:MetadataElement>`

This profile is a normative deployment profile for the SAML 2.0 Web Browser SSO Profile ([urn:oasis:names:tc:SAML:2.0:profiles:SSO:browser](#)), as specified in [saml2-profiles](#). Text from [saml2-profiles](#), [saml2-core](#), [saml2-bindings](#) and [saml2-metadata](#) is background material, and is not repeated in this document.

Single Sign-On Profile

This deployment profile of SAML 2.0 Single Sign-On (SSO) defines a set of requirements that entities need to support in order to be interoperable with other entities.

SAML 2.0 Metadata

All entities supporting this profile MUST provide SAML 2.0 Metadata following the *SAML V2.0 Metadata Interoperability Profile* [saml2-metadata-profile](#) specification.

The Authentication Request

The `<samlp:AuthnRequest>` MUST include a `<saml:Issuer>` including the EntityID of the Service Provider.

The `<samlp:AuthnRequest>` MUST NOT include `<saml:Subject>`, `<saml:Conditions>`.

The Identity Provider MUST provide a reasonable user experience when the Service Provider is not including a `<samlp:Scoping>` element. The use of `<samlp:Scoping>` requires the Service Provider to know something about what is behind the Identity Provider, something that may be used in some local environments, but is not reasonable to assume when cross-connecting existing federation.

The Identity Provider MUST interpret `@ForceAuthN="true"`, and return a SAML Error if forced re-authentication is not supported. The Identity Provider MUST interpret `@IsPassive="true"`, and return a SAML Error if it does not support the passive behavior.

The `<samlp:AuthnRequest>` MUST contain an `<samlp:AssertionConsumerServiceURL>`. The Identity Provider MUST verify that the value of `<samlp:AssertionConsumerServiceURL>` exactly matches the `<samlmd:AssertionConsumerURL>` in the metadata corresponding to the Service Provider.

To increase the chance of interoperability the `<samlp:AuthnRequest>` SHOULD NOT include a

<samlp:RequestedAuthnContext> element. The support for different authentication context classes, and the semantics around the different classes may be interpreted differently and may potentially cause interoperability problems. If the <samlp:RequestedAuthnContext> is included in the request, the participating entities SHOULD have a already established agreement upon which authentication context classes that are available.

A <samlp:NameIDPolicy> element SHOULD be included in the <samlp:AuthnRequest> with the AllowCreate attribute set to "true".

If the Service Provider includes a NameIDPolicy@Format in the <samlp:AuthnRequest>, it SHOULD be set to either of:

```
urn:oasis:names:tc:SAML:2.0:nameid-format:transient
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.
```

The Identity Provider MUST support the transient NameID format.

The <samlp:AuthnRequest> issued by the Service Provider MUST be sent to the Identity Provider using the HTTP-REDIRECT binding.

The Service Provider SHOULD NOT sign the <samlp:AuthnRequest>. If the Service Provider is signing the request, it MUST NOT assume that the Identity Provider is validating the signature unless an explicit agreement is made about doing so.

As this profile only allows the HTTP-POST binding for the <samlp:Response>, the <samlp:AuthnRequest> MUST either have the @ProtocolBinding attribute to be set to urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST, or omitted.

The Response

The Service Provider MUST support both unsolicited responses and responses mapped to an <samlp:AuthnRequest> .

The <samlp:Response> MUST include a <saml:Issuer> element as a child to the <samlp:Response> element including the EntityID of the Identity Provider.

The <samlp:Response> MUST be sent using the HTTP-POST binding [saml2-bindings](#).

The Assertion

If successful, the <samlp:Response> MUST contain one <saml:Assertion>. The Assertion MUST contain one <saml:AuthnStatement> and zero or one <saml:AttributeStatement>-s. Each <saml:AttributeStatement> MAY contain any number of <saml:Attribute>-s, which MAY contain any number of <saml:AttributeValue>-s.

The Assertion MUST contain a <saml:Subject> and the <saml:Subject> MUST contain a <saml:NameID>.

If the request did not include a NameIDPolicy@NameIDFormat the NameID@Format in the response MUST be either of:

```
urn:oasis:names:tc:SAML:2.0:nameid-format:transient
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.
```

The Identity Provider MUST include a <saml:Conditions> element. Conditions restricting the

period when the assertion is valid, the @NotBefore and @NotOnOrAfter MUST be included.

<saml:Attribute> elements SHOULD carry a NameFormat attribute of urn:oasis:names:tc:SAML:2.0:attrname-format:uri. It is RECOMMENDED that the I2MI SAML 2.0 attribute profile MACE-attributes be used.

Encoding attribute values as plain strings is strongly RECOMMENDED. Past experience has shown that using simple strings eases interoperation between different products compared to other encoding methods.

Encryption of the Response

The content of the Assertion MUST be protected against eavesdropping, either by encrypting the assertion, or by ensuring that the response is sent on a secure transport.

The Service Provider MUST either support decrypting <saml:EncryptedAssertion>, or the AssertionConsumerService endpoint MUST use a secure transport connection (SSL/HTTPS).

The Identity Provider MUST NOT send an unencrypted Assertion to an unprotected (HTTP) AssertionConsumerService endpoint, or present the <form> containing the response on an unprotected (HTTP) XHTML/HTML page.

If the Service Provider uses SSL/HTTPS and supports decrypting assertions, the Identity Provider MAY encrypt the assertion. The Service Provider will implicitly indicate to the Identity Provider whether it supports decrypting assertions or not. By including a <samlmd:KeyDescriptor> with use=encryption or with the use attribute left out, the Service Provider indicates that it supports decrypting assertions. If the Service Provider metadata contains no <samlmd:KeyDescriptor> at all, or only a <samlmd:KeyDescriptor> with use="signing" the Service Provider indicates it does not support decrypting assertions.

Security Considerations

As this profile does not require validation of signed authentication request messages, the Service Provider cannot assume that the content of the request has not been tampered with. Consequences of this include:

If the Service Provider included a <saml:RequestedAuthnContext> element in the request, it cannot rely on the Identity Provider to honor the requirements. It should only consider the required authentication context as guidance, and instead verify the <saml:AuthnContext> provided in the <samlp:Response>. This approach also makes it easier to support unsolicited responses.

If the Service Provider requires the user to present a fresh authentication, and sends a request with ForceAuthn="true", it SHOULD verify the AuthnInstant attribute in the Response.

This profile does not allow an authentication response to be sent unencrypted over the network. Either the <saml:Assertion> is encrypted end-to-end, or all endpoints are required to use encrypted transport. When the <saml:Assertion> is not encrypted, the content will be exposed in the user's web-browser. The content cannot be tampered with by the user, because the message is signed. However, the user may be able to decode and view attributes sent in the <samlp:Response>.

Normative References

- [RFC2119] Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, March 1997.
[saml2-core] OASIS, "SAML 2.0 Core".

[saml2-bindings] [OASIS, "SAML 2.0 Bindings"](#).
[saml2-profiles] [OASIS, "SAML 2.0 Profiles"](#).
[saml2-metadata-profile] [OASIS, "SAML 2.0 Metadata"](#)
[saml2-metadata-profile] [OASIS, "Interoperable SAML 2.0 Metadata Deployment Profile"](#).

Informative References

[MACE-attributes] [MACE, "MACE: Attribute schemes"](#).

Authors' addresses

Andreas Åkre Solberg, UNINETT, andreas.solberg@uninett.no
Scott Cantor, Ohio State University, cantor.2@osu.edu
Eve Maler, Sun Microsystems, eve.maler@sun.com
Leif Johansson, Stockholm University, leifj@it.su.se

[HTML](#) [CSS](#)