Kantara Initiative
eGovernment Profiles of SAML 2.0

Version 2.0

Working Draft 01
February 16, 2010

Document identifier:
draft-kantara-egov-saml2-profiles-2.0

Location:
TBD

Editors:
Scott Cantor, Internet2

Contributors:
Kantara eGovernment WG
Andreas Åkre Solberg, UNINETT

Abstract:
This document contains implementation and deployment profiles for eGovernment use of SAML V2.0, suitable for the purposes of developing a conformance program.

Table of Contents

1 Introduction

SAML V2.0 is a rich and extensible standard that must be profiled to be used interoperably, and the profiles that typically emerge from the broader standardization process usually remain fairly broad and include a number of options and features that increase the burden for implementers and make deployment-time decisions more difficult.

The Kantara Initiative eGovernment profiles make up a SAML V2.0 conformance specification for Identity Provider and Service Provider implementations operating in eGovernment federations and deployments. The profiles are based on the SAML V2.0 specifications created by the Security Services Technical Committee (SSTC) of OASIS, and related specifications approved by that body. It constrains and supplements the base SAML V2.0 features, elements, and attributes required for eGovernment federations and deployments.

It is divided into *implementation* and *deployment* profiles. Implementation profiles define the features that implementations must support within their product offerings such that deployers can be assured of the ability to meet their own (possibly varied) deployment requirements. Deployment profiles define specific options and constraints to which deployments are required to conform; they guide product configuration and federation operations, and provide criteria against which actual deployments may be tested.

1.1 Notation

This specification uses normative text to describe the use of SAML capabilities.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in [RFC 2119]:

> …they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)…

These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

```
Listings of XML schemas appear like this.
```

```
Example code listings appear like this.
```

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

- The prefix `saml2:` stands for the SAML 2.0 assertion namespace, `urn:oasis:names:tc:SAML:2.0:assertion`
- The prefix `saml2p:` stands for the SAML 2.0 protocol namespace, `urn:oasis:names:tc:SAML:2.0:protocol`
- The prefix `md:` stands for the SAML 2.0 metadata namespace, `urn:oasis:names:tc:SAML:2.0:metadata`
- The prefix `idpdisc:` stands for the Identity Provider Discovery Service Protocol and Profile [IdPDisco] namespace, `urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol`
- The prefix `mdattr:` stands for the Metadata Extension for Entity Attributes Version 1.0 [MetaAttr] namespace, `urn:oasis:names:tc:SAML:metadata:attribute`

This specification uses the following typographical conventions in text: `<ns:Element>`, `Attribute`, **Datatype**, `OtherCode`.

1.2 Normative References

[RFC 2119] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997. http://www.ietf.org/rfc/rfc2119.txt

[RFC2616] IETF RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1*, June 1999. http://www.ietf.org/rfc/rfc2616.txt

[RFC2818] IETF RFC 2818, *HTTP Over TLS*, May 2000. http://www.ietf.org/rfc/rfc2818.txt

[IdPDisco] OASIS Committee Specification, *Identity Provider Discovery Service Protocol and Profile*, March 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf

[MetaAttr] OASIS Committee Specification, *SAML V2.0 Metadata Extension for Entity Attributes Version 1.0*, August 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf

[MetaIOP] OASIS Committee Specification, *SAML V2.0 Metadata Interoperability Profile Version 1.0*, August 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf

[SAML2Core] OASIS Standard, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML2Meta] OASIS Standard, *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SAML2Bind] OASIS Standard, *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

[SAML2Prof] OASIS Standard, *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[SAML2Err] OASIS Approved Errata, *SAML V2.0 Errata*. http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf

[SAML-X500] OASIS Committee Specification, *SAML V2.0 X.500/LDAP Attribute Profile*, March 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500.pdf

Non-Normative References

[eGov15] Kyle Meadors, *Liberty Alliance eGov Profile for SAML 2.0 Version 1.5*.

2 SAML V2.0 Browser SSO/SLO Implementation Profile

This profile specifies behavior and options that implementations of the SAML V2.0 Web Browser SSO and Single Logout Profiles [SAML2Prof] are required to support. The requirements specified are *in addition to* all normative requirements of the original profiles, as modified by the Approved Errata [SAML2Err], and readers should be familiar with all relevant reference documents. Any such requirements are not repeated here except where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in errata, but remain implied.

SAML leaves substantial latitude to implementations with regard to how software is architected and combined with authentication and application infrastructure. Where the terms "Identity Provider" and "Service Provider" are used, they should be understood to include the total software footprint intended to provided the desired functionality; no specific assumptions are made as to how the required features are exposed to deployers, only that there is some method for doing so.

2.1 Required Information

Identification: TBD

Contact information: TBD

Description: Given below

Updates: Liberty Alliance eGov Profile for SAML 2.0 [eGov15]

2.2 Metadata and Trust Management

Identity Provider, Service Provider, and Discovery Service implementations MUST support the use of SAML V2.0 Metadata [SAML2Meta] in conjunction with their support of the SAML V2.0 Web Browser SSO Profile [SAML2Prof]. Additional expectations around the use of particular metadata elements related to profile behavior may be encountered in subsequent sections.

Implementations MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP].

Implementations MUST support the **TBD: insert profile for PKI here**

It is OPTIONAL for implementations to support the generation, publication, or exportation of metadata, but implementations MUST support the following mechanisms for the importation of metadata:

- local file
- remote resource at fixed location accessible via HTTP 1.1 [RFC2616] or HTTP 1.1 over TLS/SSL [RFC2818]

In the case of HTTP resolution, implementations MUST support use of the "ETag" header for cache management; other cache control support is OPTIONAL. Implementations SHOULD support the use of more than one fixed location for the importation of metadata, but MAY leave their behavior unspecified if a single entity's metadata is present in more than one source.

In accordance with [MetaIOP], importation of multiple entities' metadata contained within an `<md:EntitiesDescriptor>` element MUST be supported.

Verification of metadata, if supported, MUST include XML signature verification at least at the root element level, and SHOULD support the following mechanisms for signature key trust establishment:

- direct comparison against known keys

- some form of path-based certificate validation against one or more trusted root certificates and certificate revocation lists

The latter mechanism does not impose a particular profile for certificate validation, as no such profile has wide enough adoption across tools and libraries to warrant such a requirement, but should be understood as being consistent with the "usual" practices encountered in the implementation of certificate validation. Where possible, implementations SHOULD document known limitations of the mechanisms they employ.

Implementations SHOULD support the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 [MetaAttr] and provide policy controls on the basis of SAML attributes supplied via this extension mechanism.

Finally, implementations SHOULD allow for the automated updating/reimportation of metadata without substantial disruption of services.

2.2.1 Conformance Assertions

TBD

2.3 Identity Provider Discovery

Service Provider and Discovery Service implementations MUST support the Identity Provider Discovery Service Protocol Profile in conformance with section 2.4.1 of [IdPDisco].

TBD: Maintain MUST for CDC profile?

2.3.1 Conformance Assertions

TBD

2.4 Name Identifiers

Identity Provider and Service Provider implementations MUST support the following SAML V2.0 name identifier formats, in accordance with the normative obligations associated with them by [SAML2Core]:

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

Support for other formats is OPTIONAL.

2.4.1 Conformance Assertions

TBD

2.5 Attributes

Identity Provider and Service Provider implementations MUST support the generation and consumption of `<saml2:Attribute>` elements that conform to the SAML V2.0 X.500/LDAP Attribute Profile [SAML-X500].

TBD: Should support for more than simple strings be required or recommended?

2.5.1 Conformance Assertions

TBD

2.6 Single Sign-On

2.6.1 Authentication Requests

2.6.1.1 Binding and Security Requirements

Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect binding [SAML2Bind] for the transmission of `<saml2p:AuthnRequest>` messages, including the generation or verification of signatures in conjunction with this binding.

Support for other bindings is OPTIONAL.

2.6.1.1.1 Conformance Assertions

TBD

2.6.1.2 Message Content

In addition to standard core- and profile-driven requirements, Service Provider implementations MUST support the inclusion of at least the following `<saml2p:AuthnRequest>` child elements and attributes (when appropriate):

- `AssertionConsumerServiceURL`
- `ProtocolBinding`
- `ForceAuthn`
- `IsPassive`
- `AttributeConsumingServiceIndex`
- `<saml2p:RequestedAuthnContext>`
- `<saml2p:NameIDPolicy>`

Identity Provider implementations MUST support all `<saml2p:AuthnRequest>` child elements and attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate errors when confronted by particular request options. However, implementations SHOULD fully support the options enumerated above. Implementations MAY limit their support of the `<saml2p:RequestedAuthnContext>` element to the value "exact" for the `Comparison` attribute.

2.6.1.2.1 Conformance Assertions

TBD

2.6.2 Responses

2.6.2.1 Binding and Security Requirements

Identity Provider and Service Provider implementations MUST support the use of the HTTP-POST binding [SAML2Bind] for the transmission of `<saml2p:Response>` messages.

Support for other bindings is OPTIONAL.

Identity Providers and Service Providers MUST support the generation and consumption of unsolicited `<saml2p:Response>` messages (i.e., responses that are not the result of a `<saml2p:AuthnRequest>` message).

Identity Provider and Service Provider implementations MUST support the signing of `<saml2:Assertion>` elements in responses; support for signing of the `<saml2p:Response>` element is OPTIONAL.

Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the `<saml2:EncryptedAssertion>` element; support for the `<saml2:EncryptedID>` and `<saml2:EncryptedAttribute>` elements is OPTIONAL.

2.6.2.1.1 Conformance Assertions

TBD

2.6.2.2 Message Content

The Web Browser SSO Profile allows responses to contain any number of assertions and statements. Identity Provider implementations MUST allow the number of `<saml2:Assertion>`, `<saml2:AuthnStatement>`, and `<saml2:AttributeStatement>` elements in the `<saml2p:Response>` message to be limited to one.

In turn, Service Provider implementations MAY limit support to a single instance of those elements when processing `<saml2p:Response>` messages.

Identity Provider implementations MUST support the inclusion of a `Consent` attribute in `<saml2p:Response>` messages, and a `SessionIndex` attribute in `<saml2:AuthnStatement>` elements.

Service Provider implementations that provide some form of session semantics MUST support the `<saml2:AuthnStatement>` element's `SessionNotOnOrAfter` attribute.

2.6.2.2.1 Conformance Assertions

TBD

2.7 Single Logout

2.7.1 Logout Requests

2.7.1.1 Binding and Security Requirements

Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect binding [SAML2Bind] for the transmission of `<saml2p:LogoutRequest>` messages, including the generation or verification of signatures in conjunction with this binding.

Support for other bindings is OPTIONAL.

Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the `<saml2:EncryptedID>` element.

2.7.1.1.1 Conformance Assertions

TBD

2.7.1.2 User Interface Behavior

Identity Provider and Service Provider implementations MUST support "local" logout as well as initiation of Single Logout, subject to deployer and user option.

2.7.1.2.1 Conformance Assertions

TBD

2.7.2 Logout Responses

2.7.2.1 Binding and Security Requirements

Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect binding [SAML2Bind] for the transmission of `<saml2p:LogoutResponse>` messages, including the generation or verification of signatures in conjunction with this binding.

Support for other bindings is OPTIONAL.

2.7.2.1.1 Conformance Assertions

TBD

3 SAML V2.0 Browser SSO/SLO Deployment Profile

This profile specifies behavior and options that deployments of the SAML V2.0 Web Browser SSO Profile [SAML2Prof] are required or permitted to rely on. The requirements specified are *in addition to* all normative requirements of the original profile, as modified by the Approved Errata [SAML2Err], and readers should be familiar with all relevant reference documents. Any such requirements are not repeated here except where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in errata, but remain implied.

This profile addresses the content, exchange, and processing of SAML messages only, and does not address deployment details that go beyond that scope. Furthermore, nothing in the profile should be taken to imply that disclosing personally identifiable information, or indeed any information, is *required* from an Identity Provider with respect to any particular Service Provider. That remains at the discretion of applicable settings, user consent, or other appropriate means in accordance with regulations and policies.

Note that SAML features that are optional, or lack mandatory processing rules, are assumed to be optional and out of scope of this profile if not otherwise precluded or given specific processing rules.

3.1 Required Information

Identification: TBD

Contact information: TBD

Description: Given below

Updates: Liberty Alliance eGov Profile for SAML 2.0 [eGov15]

3.2 Metadata and Trust Management

TBD: Any agreement on the profile of metadata IdPs and SPs should supply?

If a Service Provider forgoes the use of TLS/SSL for its Assertion Consumer Service endpoints, then its metadata MUST include a `<md:KeyDescriptor>` suitable for XML Encryption. Note that use of TLS/SSL is RECOMMENDED.

If a Service Provider plans to utilize an external Discovery Service supporting the Identity Provider Discovery Service Protocol Profile [IdPDisco], then its metadata MUST include one or more `<idpdisc:DiscoveryResponse>` elements in the `<md:Extensions>` element of its `<md:SPSSODescriptor>` element.

3.3 Name Identifiers

Identity Providers MUST support the `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` name identifier format [SAML2Core]. They SHOULD support the `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` name identifier format [SAML2Core]. Support for other formats is OPTIONAL.

Service Providers, if they rely at all on particular name identifier formats, MUST support one of the following:

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

Reliance on other formats by Service Providers is NOT RECOMMENDED.

Note that these requirements are reflected in additional constraints on message content in subsequent sections.

3.4 Attributes

Any `<saml2:Attribute>` elements exchanged via any SAML 2.0 messages, assertions, or metadata MUST contain a `NameFormat` of `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

The use of LDAP/X.500 attributes, and the SAML V2.0 X.500/LDAP Attribute Profile [SAML-X500] is RECOMMENDED where possible.

It is RECOMMENDED that the content of `<saml2:AttributeValue>` elements exchanged via any SAML 2.0 messages, assertions, or metadata be limited to a single child text node (i.e., a simple string value).

3.5 Single Sign-On

3.5.1 Authentication Requests

3.5.1.1 Binding and Security Requirements

The `<saml2p:AuthnRequest>` message issued by a Service Provider MUST be communicated to the Identity Provider using the HTTP-REDIRECT binding [SAML2Bind].

The endpoints at which an Identity Provider receives a `<saml2p:AuthnRequest>` message, and all subsequent exchanges with the user agent, SHOULD be protected by TLS/SSL.

3.5.1.2 Message Content

The `<saml2p:AuthnRequest>` message issued by a Service Provider MUST contain an `AssertionConsumerServiceURL` attribute identifying the desired response location. The `ProtocolBinding` attribute, if present, MUST be set to `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`.

The `<saml2p:AuthnRequest>` message MUST NOT contain a `<saml2:Subject>` element.

The `<saml2p:AuthnRequest>` message SHOULD contain a `<saml2p:NameIDPolicy>` element with an `AllowCreate` attribute of "true". Its `Format` attribute, if present, SHOULD be set to one of the following values:

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

The `<saml2p:AuthnRequest>` message MAY contain a `<saml2p:RequestedAuthnContext>` element, but SHOULD do so only in the presence of an arrangement between the Identity and Service Providers regarding the Authentication Context definitions in use. The `Comparison` attribute SHOULD be omitted or be set to "exact".

3.5.2 Responses

3.5.2.1 Binding and Security Requirements

The `<saml2p:Response>` message issued by an Identity Provider MUST be communicated to the Service Provider using the HTTP-POST binding [SAML2Bind].

The endpoint(s) at which a Service Provider receives a `<saml2p:Response>` message SHOULD be protected by TLS/SSL. If this is not the case, then Identity Providers MUST utilize XML Encryption and return a `<saml2:EncryptedAssertion>` element in the `<saml2p:Response>` message. The `<saml2:EncryptedID>` and `<saml2:EncryptedAttribute>` elements MUST NOT be used.

Whether encrypted or not, the `<saml2:Assertion>` element issued by the Identity Provider MUST itself be signed directly using a `<ds:Signature>` element within the `<saml2:Assertion>`.

Service Providers MUST support unsolicited `<saml2p:Response>` messages (i.e., responses that are not the result of an earlier `<saml2p:AuthnRequest>` message).

3.5.2.2 Message Content

Assuming a successful response, the `<saml2p:Response>` message issued by an Identity Provider MUST contain exactly one assertion (either a `<saml2:Assertion>` or an `<saml2:EncryptedAssertion>` element). The assertion MUST contain exactly one `<saml2:AuthnStatement>` element and MAY contain zero or one `<saml2:AttributeStatement>` elements.

The `<saml2:AuthnStatement>` element of the assertions issued by an Identity Provider MUST contain a `SessionIndex` attribute.

The `<saml2:Subject>` element of the assertions issued by an Identity Provider SHOULD contain a `<saml2:NameID>` element. It MUST NOT contain a `<saml2:EncryptedID>` or `<saml2:BaseID>` element. In the absence of a `<saml2p:NameIDPolicy>` `Format` attribute in the Service Provider's `<saml2p:AuthnRequest>` message, or a `<md:NameIDFormat>` element in the Service Provider's metadata, the `Format` of the `<saml2:NameID>` SHOULD be set to `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`.

3.6 Single Logout

3.6.1 Logout Requests

3.6.1.1 Binding and Security Requirements

The `<saml2p:LogoutRequest>` message issued by an Identity Provider or Service Provider MUST be communicated using the HTTP-REDIRECT binding [SAML2Bind]. The message MUST be signed.

The endpoints at which an Identity Provider or Service Provider receives a `<saml2p:LogoutRequest>` message SHOULD be protected by TLS/SSL.

TBD: Use of encryption?

3.6.2 Logout Responses

3.6.2.1 Binding and Security Requirements

The `<saml2p:LogoutResponse>` message issued by an Identity Provider or Service Provider MUST be communicated using the HTTP-REDIRECT binding [SAML2Bind]. The message MUST be signed.

The endpoints at which an Identity Provider or Service Provider receives a `<saml2p:LogoutResponse>` message SHOULD be protected by TLS/SSL.

Appendix A. Open Issues

- Need an alternative to IOP, or agreement to drop PKI outside of metadata exchange. Alternative needs to specify PKI to some degree AND address the exact content and semantics of metadata as relates to runtime certificate evaluation and/or identity of SAML peer.
- Should CDC discovery profile remain MTI?
- Should responses via artifact remain MTI?
- Dropped "unspecified" and "basic" formats for names and attribute naming.
- Need for non-trivial attribute value support?
- Need for more than exact AuthnContext matching?
- Noted specific AuthnRequest content to support, needs review.
- Need for specific MTI behavior on ACS checking?
- Added constraint on number of assertions and statements.
- Added requirement for SP support of SessionNotOnOrAfter.
- Added Encryption as MTI for logout.
- Need some clarification of some of the original single logout language around user consent.
- Is SSL a MUST for deployers? If so, why require encryption?
- Updated crypto algorithm conformance rules for implementers and deployers?
- Populate with conformance assertions/tests.