Kantara Initiative eGov 2.0 Profile Draft

This document is in DRAFT form.

Follow this link to access the eGovernment SAML 2.0 Implementation Profile as an official Kantara approved report.

eGov Profile
SAML 2.0

Version 2.0

Editors:

- TBD
- TBD

Abstract:
This document describes the eGovernment "Conformance (or Interoperability)" profile for SAML 2.0.

Filename:
Kantara_Initiative_eGov_2.0_Draft.doc

Contents

Considerations for Version 2

⚠ **This document is in DRAFT form**

Introduction

Overview of eGov Profile

The Kantara Initiative eGov profile is a ~~Kantara Initiative~~ 2 part Profile.

Part 1 is entitled interoperability profile for implementations. It defines SAML 2.0 conformance specification for SP and IdP applications operating in approved eGovernment federations and deployments. The eGov profile is based on the SAML 2.0 specifications created by the Security Services Technical Committee (SSTC) of OASIS. It constrains the base SAML 2.0 features, elements, attributes and other values required for approved eGovernment federations and deployments. Unless otherwise specified, SAML operations and features follow those found in the OASIS SAML 2.0 specifications.

~~PM 'Constrains the base features' makes this sound like an interop profile, but the sentence following argues not...~~

Part 2 is entitled Interoperability Profiles for deployers. Idealistically, the long term goal is to converge towards one agreed deployment for government worldwide. Realistically there may be several deployments along the path to that long term goal. These profiles are the range of constraints/rules/actions /processes 'rule set' that we deployers have agreed on. They may consist of one or more specifications to guide product configuration, federation operations, and to test deployments against.

~~This eGov profile *does not* reflect which aspects of SAML the individual governments must utilize in their respective federations. Thus, it is not a deployment level profile.~~ Detailed information on deployment level detail can be found in the "Comparison and Analysis" document originally produced by Liberty Alliance SIG-eGov group.

In summary, this eGov profile therefore ~~*does*~~ reflects

(a) the SAML features that vendors [CW 10-01-20: and open source developers] must implement within their product offerings to satisfy SP and IdP functionality necessary to be conformant to this profile

[(b) CW 10-01-20: the confluence of the deployment operational criteria of the governments of the USA, Denmark, New Zealand ..and Canada?, Finland? that use products and/or features that have been accepted as "implementation" level criteria in (a) above]

Document References

[SAMLAuthnCxt]	J. Kemp et al, "Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf
[SAMLBind]	Scott Cantor et al, "Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
[SAMLConf]	Prateek Mishra et al, "Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005). http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf.
[SAMLCore]	S. Cantor et al, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.
[SAMLErrata]	Jahan Moreh, "Errata for the OASIS Security 2 Assertion Markup Language (SAML) V2.0, Working Draft 28," OASIS SSTC (May 8, 2006), http://www.oasis-open.org/committees/download.php/18070/sstc-saml-errata-2.0-draft-28.pdf
[SAMLMeta]	S. Cantor et al, "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.
[SAMLMetaExt]	Tom Scavo et al, "SAML Metadata Extension for Query Requesters, Committee Draft 01", OASIS SSTC (March 2006), http://www.oasis-open.org/committees/download.php/18052/sstc-saml-metadata-ext-query-cd-01.pdf
[SAMLProf]	S. Cantor et al, "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.
[SAMLSec]	Frederick Hirsch et al, "Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf
[CW 10-01-20: SAMLIDAss]	'Bob' Morgan et al, "Expressing Identity Assurance in SAML V2.0", OASIS SSTC (XXX 2010) url to come
[CW: 10-01-20: SAMLMetaIOPProf]	S.Cantor, SAML V2.0 Metadata Interoperability Profile version 1.0, OASIS SSTC, (August 2009) http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop-cs-01.pdf

Draft History

- Draft X TBD

Key Words

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 RFC 2119.

This document is in DRAFT form

Part 1: Interoperability Profile for Implementations

Conformance Requirements

Web SSO

- SSO profile in [SAMLProf] MUST be supported by both SP and IdP with both capable of initiation. Unsolicited IdP <Response> messages MUST be supported.

IdP Discovery

- IdP Discovery MUST be supported.
- If a CDC exists the SP MUST SUPPORT functionality of presenting the user with a tailored list of compatible Identity Providers featuring, at a minimum, the compatible Identity Providers in the CDC.

SP Authentication Request

- MUST be communicated using HTTP Redirect binding. [PM : this is a deployment stipulation]
- *isPassive* MUST be supported. It MAY be used when the IdP is not to take direct control. If *isPassive* is true, the Identity Provider and client MUST NOT take over the user interface.
- *ForceAuthn* MUST be supported. It MAY be used to require the IdP to force the end user to authenticate.
- <AuthnRequest> MUST be signed. [PM : this is a deployment stipulation]
- <NameIDPolicy> MUST be supported and MUST SUPPORT formats of 'persistent', 'transient' and 'unspecified'.
- <RequestedAuthnContext> MUST be supported. IdP MUST recognize *Comparison* field and evaluate the requested context classes.

IdP Authentication Response

- MUST be communicated using HTTP POST binding or SOAP Artifact binding. [PM : this is a deployment stipulation]
- MUST be produced and sent regardless of the success or failure of the <AuthnRequest> [i.e. the IdP may not logically abandon the <AuthnRequest> under any circumstances in its control]
- Assertion MUST be encrypted when using POST binding. [PM : this is a deployment stipulation]
- The *Consent* attribute MUST be supported. The *Consent* values which MUST be supported, but not limited to, are:
    - urn:oasis:names:tc:SAML:2.0:consent:obtained
    - urn:oasis:names:tc:SAML:2.0:consent:prior
    - urn:oasis:names:tc:SAML:2.0:consent:current-implicit
    - urn:oasis:names:tc:SAML:2.0:consent:current-explicit
    - urn:oasis:names:tc:SAML:2.0:consent:unspecified

Comment: what does it mean to 'support' one of these consent values? Not choke? or differentiate based on them?

Assertion

- Assertion MUST be signed. [PM : this is a deployment stipulation]
- MUST have one <AuthnStatement> present. SessionIndex parameter MUST be present and SessionNotOnOrAfter MUST NOT be present.
- MUST support <AttributeStatement> and MAY contain up to one <AttributeStatement>. [PM : this is a deployment stipulation]
- MUST support NameFormat of <Attribute> values of "basic", "uri" and "unspecified".
- <AttributeStatement> MUST use <Attribute> and MUST NOT use <EncryptedAttribute>. [PM : this is a deployment stipulation]
- The <SubjectConfirmationData> attributes *NotOnOrAfter* MUST be supported.
- The <Conditions> attributes *NotBefore* and *NotOnOrAfter* MUST be supported.
- The <Conditions> element <AudienceRestriction> MUST be supported.

Single Logout

- SP-initiated Single Logout and IdP-initiated Single Logout MUST be supported.
- Single Logout binding MAY be HTTP Redirect or SOAP. [PM : this is a deployment stipulation]
- <LogoutRequest> MUST be signed. [PM : this is a deployment stipulation]

- <LogoutResponse> MUST be signed. [PM : this is a deployment stipulation]
- SP MUST offer user choice between local logout from SP only or SLO.
- User SHOULD confirm logout. If Single Logout is unsuccessful, user MUST be informed.

Security

- The minimum requirements for algorithm, key length and other security requirements are defined in Section 4 of [SAMLConf]. eGov applications and deployments MUST follow those minimum requirements. [PM : this is a deployment stipulation]
- Utilization of a certificate authority and other security practices not defined in this profile are deployment decisions outside the scope of this profile.
- <AuthnRequest>, <SingleLogoutRequest> and <SingleLogoutResponse> messagesSHOULD use HTTPS over SSL (v3.0 or higher) or TLS (v1.0 or higher) to establish a security context with the user agent (web browser) but earlier versions of SSL are permissible.

This document is in DRAFT form

Metadata

The choice of Metadata information is largely a deployment level decision. However, all conformant SP and IdP implementations MUST support the consumption and proper use of all Metadata elements, attributes and specifications listed in this section.

General Metadata

- SP and IdP SHOULD authenticate metadata before using it.
- ~~The exchange of metadata is outside the scope of this profile.~~
- Signing of Metadata MUST be supported.
- MUST support root elements of <EntityDescriptor> or <EntitiesDescriptor>.
- <Organization> MUST be supported.
- Attributes *validUntil* AND *cacheDuration* MUST be supported.
- Certificates consumption and use in metadata MUST be supported.
- Certificate revocation methods of CDP Extention, OSCP and CRL MUST be supported.
- IDPs MAY? advertise the levels of assurance they can meet through their metadata

<SPSSODescriptor>

- <KeyDescriptor> MUST be supported.
- <SingleLogOutService> MUST be supported.
- *WantAssertionSigned* MUST be supported.
- *AuthnRequestsSigned* MUST be supported.

<IDPSSODescriptor>

- <KeyDescriptor> MUST be supported.
- *WantAuthnRequestsSigned* MUST be supported.
- <SingleLogOutService> MUST be supported.
- <SingleSignOnService> MUST be supported.

<AttributeAuthorityDescriptor>

- <AttributeAuthorityDescriptor> MUST be supported.

This document is in DRAFT form

Part 2: Interoperability Profiles for Deployments

Requirements under consideration for future versions ~~Considerations for Version 2.0~~

This section is a "catch all" for pertinent issues that need to be addressed in the next version of the eGov profile. They are not required for adoption of eGov ~~1.5~~ 2.0 profiles. These bullet points exist as reminders and placeholders for future discussion.

- Some don't consider CDC approach to IdP discovery to be an effective model. Suggest putting on roadmap consideration for moving to other discovery service approach.
- On a deployment level, we had stated that optional metadata elements <RoleDescriptor>, <AuthnAuthorityDescriptor>, <PDFDescriptor>, <AffiliationDescriptor> and <AdditionalMetadataLocation> SHOULD NOT be used. However, it is not necessary or particularly wise to state for vendors that they are NOT to support certain elements.
- Metadata and PKI methods need to be better specified to insure interoperability.
- Version 1.5 was a hybrid of implementation conformance and deployment interoperability requirements. Should these be broken apart in V 2? Or at least a) remove the current text that suggests there are no deployment requirements and b) better differentiate the two types of requirements
- We need a way to send the user's (not the browser's) current language preference from the RP to the IdP and from the IdP to the RP in all cases, even when authentication fails and an assertion is not produced. Canada currently plans to do this by using the "Extensions" in the RequestAbstractType and the StatusResponseType.

Draft Issues Task List

eGov 2.0 Profile Draft Issues

Joni: Create tracking page to track Draft Issues for resolution