eGov Profile

SAML 2.0

Version 1.5 Draft E

Editor:

Kyle Meadors, Drummond Group Inc.

Abstract:

This document describes the eGovernment profile for SAML 2.0.

Filename:

LibertyAlliance_eGov_1.5_DraftE.odt

Notice

This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact the Liberty Alliance to determine whether an appropriate license for such use is available.

Implementation or use of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This Specification is provided "AS IS," and no participant in the Liberty Alliance makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Implementers of this Specification are advised to review the Liberty Alliance Project's website (http://www.projectliberty.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance Management Board.

Agency for Public Management and eGovernment, Norwegian Public Roads Administration, Novell, NRI Pacific, Office of the Information Privacy Commissioner of Ontario, Omnibranch, OpenIAM, Oracle USA, Inc., Organisation Internationale pour la Sécurité des Transactions Électroniques (OISTE), Oslo University, Our New Evolution, PAM Forum, Parity Communications, Inc., PayPal, Phase2 Technology, Ping Identity Corporation, Bob Pinheiro, Platinum Solutions, Postsecondary Electronic Standards Council (PESC), Purdue University, RSA Security, Mary Ruddy, SAFE Bio-pharma, SanDisk Corporation, Shidler Center for Law, Andrew Shikiar, Signicat AS, Singapore Institute of Manufacturing Technology, Software & Information Industry Association, Software Innovation ASA, Sprint Nextel Corporation, Studio Notarile Genghini-SNG, Sunderland City Council, SUNET, Sun Microsystems, SwissSign AG, Technische Universitat Berlin, Telefonica S.A., TeleTrusT, TeliaSonera Mobile Networks AB, TERENA, Thales e-Security, The Boeing Company, The Financial Services Roundtable/BITS, The Open Group, The University of Chicago as Operator of Argonne National Laboratory, TRUSTe, tScheme Limited, UNINETT AS, Universidad Politecnica de Madrid, University of Birmingham, University of Kent, University of North Carolina at Charlotte, University of Ottawa (TTBE), U.S. Department of Defense, VeriSign, Vodafone Group Plc, Web Services Competence Center (WSCC), Zenn New Media

Liberty Alliance Project
Licensing Administrator
c/o IEEE-ISTO
445 Hoes Lane
Piscataway, NJ 08855-1331, USA
info@projectliberty.org

Contents

Introduction

Overview of eGov Profile

The eGov profile is a Liberty Alliance defined 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.

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. Information on deployment level detail can be found in the "Comparison and Analysis" document produced by Liberty Alliance SIG-eGov group. This eGov profile *does* reflect the SAML features that vendors must implement within their product offerings to satisfy SP and IdP functionality necessary to be conformant to this profile.

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

Draft History

- Draft E

  Removed “TEST” bullets added in Draft D.

- Draft D

  Removed many requirements which were redundant to the base SAML requirements. Clarified other requirements. Removed the document defined key word “SUPPORT” and not only use RFC 2119 defined key words. Added “TEST” bullets stating how stated requirements are currently tested in the Liberty test plan and what new test specifications are needed.

- Draft C

  Defined constrained conformance requirements for complying SPs and IdPs.

- Draft B

  Based on initial feedback, this Draft placed requirements in align, nearly aligned and non-aligned groups to determine where the differences were in terms of expectations.

- Draft A

  First attempt to reconcile requirements of US, New Zealand and Denmark governments. Utilized the “Comparison and Analysis of Government Web Browser SSO Profiles” document produced by Liberty eGov SIG.

- eGov Profile 1.0

  The eGov Profile 1.0 follows the SAML 2.0 requirements for the General Service Administration (GSA) of the US Government. It was tested in the Liberty Alliance 2008 SAML 2.0 IOP event.

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.

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.
- *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.
- <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.
- Assertion MUST be encrypted when using POST binding.
- 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

Assertion

- Assertion MUST be signed.

- 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>.
- MUST support NameFormat of <Attribute> values of “basic”, “uri” and “unspecified”.
- <AttributeStatement> MUST use <Attribute> and MUST NOT use <EncryptedAttribute>.
- 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 Artifact.
- <LogoutRequest> MUST be signed.
- <LogoutResponse> MUST be signed.
- 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.
- 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.

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.

<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.

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 profile. 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.