SAML V2.0 Information Card Token Profile

Working Draft 02, 8 August 2008

Specification URIs:
TBD

Technical Committee:
OASIS Security Services TC

Chair(s):
Hal Lockhart, BEA Systems, Inc.
Brian Campbell, Ping Identity Corporation

Editors:
Scott Cantor, Internet2

Abstract:
This profile describes a set of rules for identity providers and relying parties to follow when using SAML V2.0 assertions as managed information card security tokens, so that interoperability and security is achieved commensurate with other SAML authentication profiles.

Status
This document was last revised or approved by the SSTC on the above date. The level of approval is also listed above. Check the current location noted above for possible later revisions of this document. This document is updated periodically on no particular schedule.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC by using the "Send A Comment" button on the TC's web page at http://www.oasis-open.org/committees/security.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the IPR section of the TC web page (http://www.oasis-open.org/committees/security/ipr.php).

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/security.

Notices

Copyright © OASIS Open 2008. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction

Microsoft has defined a set of profiles for acquring and delivering security tokens, collectively referred to as "Information Card" technology. These profiles are agnostic with respect to the format and semantics of a security token, but interoperability between issuing and relying parties cannot be achieved without additional rules governing the creation and use of the tokens exchanged. This document describes a set of rules for the use of SAML V2.0 assertions, as defined in [SAML2Core], as security tokens within the Information Card architecture.

1.1 Notation

This specification uses normative text.

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 [RFC2119]:

> …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:

Prefix	XML Namespace	Comments
saml:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Core].
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification [SAML2Meta].
ic:	http://schemas.xmlsoap.org/ws/2005/05/identity	This is the Infocard namespace defined in the Identity Selector Interoperability Profile [ISIP].
wsa:	http://www.w3.org/2005/08/addressing	This is the WS-Addressing namespace defined in the WS-Addressing specification [WS-Addr].
wsp:	http://schemas.xmlsoap.org/ws/2004/09/policy	This is the WS-Policy namespace defined in the March 2006 WS-Policy specification [WS-Policy].
sp:	http://schemas.xmlsoap.org/ws/2005/07/securitypolicy	This is the WS-SecurityPolicy namespace defined in the July 2005 WS-SecurityPolicy specification [WS-SecPol].
wst:	http://schemas.xmlsoap.org/ws/2005/02/trust	This is the WS-Trust namespace defined in the February 2005 WS-Trust specification [WS-Trust].

Prefix	XML Namespace	Comments
ds:	http://www.w3.org/2000/09/xmldsig#	This is the XML Signature namespace [XMLSig].
xsd:	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.
xsi:	http://www.w3.org/2001/XMLSchema-instance	This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].

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

1.2 Normative References

126 **[ISIP]**   A. Nanda. *Identity Selector Interoperability Profile V1.0*. Microsoft, April 2007.
127   http://www.microsoft.com/downloads/details.aspx?
128   FamilyID=b94817fc-3991-4dd0-8e85-b73e626f6764.

129 **[RFC2119]**   S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
130   RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

131 **[SAML2Core]**   S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion
132   Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID
133   saml-core-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-
134   core-2.0-os.pdf.

135 **[SAML2Meta]**   S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language
136   (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-
137   os. See http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

138 **[SAML2Prof]**   S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language
139   (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-profiles-2.0-os.
140   See http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

141 **[Schema1]**   H. S. Thompson et al. *XML Schema Part 1: Structures.* World Wide Web
142   Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-
143   xmlschema-1-20010502/. Note that this specification normatively references
144   [Schema2], listed below.

145 **[Schema2]**   Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide Web
146   Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-
147   xmlschema-2-20010502/.

148 **[WS-Addr]**   M. Gudgin et al. *WS-Addressing 1.0 Core*. World Wide Web Consortium
149   Recommendation, May 2006. See http://www.w3.org/TR/2006/REC-ws-addr-
150   core-20060509/.

151 **[WS-Policy]**   *Web Services Policy Framework, Version 1.2*. March 2006. See
152   http://specs.xmlsoap.org/ws/2004/09/policy/ws-policy.pdf.

153 **[WS-SecPol]**   *Web Services Security Policy Language*. July 2005. See
154   http://specs.xmlsoap.org/ws/2005/07/securitypolicy/ws-securitypolicy.pdf.

155 **[WS-Trust]**   *Web Services Trust Language*. February 2005. See http://specs.xmlsoap.org/ws/
156   2005/02/trust/WS-Trust.pdf.

157 **[XMLSig]**   D. Eastlake et al. *XML-Signature Syntax and Processing*. World Wide Web
158   Consortium Recommendation, February 2002. See
159   http://www.w3.org/TR/xmldsig-core/.

1.3 Conformance

1.3.1 SAML V2.0 Information Card Token Profile

An identity provider implementation conforms to this profile if it can produce assertions consistent with the normative text in section 2.3.

A relying party implementation conforms to this profile if it can accept assertions consistent with the normative text of section 2.4.

Use of SAML V2.0 metadata [SAML2Meta] per section 2.5 is OPTIONAL.

2 SAML V2.0 Information Card Token Profile

2.1 Required Information

Identification: `urn:oasis:names:tc:SAML:2.0:profiles:Infocard`

Contact information: security-services-comment@lists.oasis-open.org

Description: Given below.

Updates: None.

2.2 Profile Overview

Identity providers and relying parties employing the Identity Selector Interoperability Profile [ISIP] to request and exchange security tokens are able to use arbitrary token formats, provided there is agreement on the token's syntax and semantics, and a way to connect the token's content to the supported protocol features.

This profile provides a set of requirements and guidelines for the use of SAML V2.0 assertions as security tokens that, where possible, emulates existing SAML V2.0 authentication profiles [SAML2Prof] so as to limit the amount of new work that must be done by existing software to support the use of Information Cards. It also provides for the use of SAML assertions in this new context that is safe and consistent with best practices in similar contexts.

This profile does not seek to alter the required behavior of existing identity selector software, or conflict with the profiles defined by [ISIP].

2.3 Identity Provider Requirements

While the SAML V2.0 specification [SAML2Core] defines an identity provider solely in terms of the SAML Authentication Request protocol, the term is generally applicable to an entity that issues authentication assertions by means of other, similar protocols. In this case, the identity provider functions as an Identity Provider/Security Token Service (IP/STS) in the Information Card vocabulary, and issues assertions in response to `<wst:RequestSecurityToken>` messages [WS-Trust].

As defined by [ISIP], the request contains information that provides input into the assertion creation process. The following sections outline requirements for interpreting this input and the resulting assertion content.

2.3.1 Token Type

The token type string used with SAML V2.0 assertions MUST be `urn:oasis:names:tc:SAML:2.0:assertion`.

This string appears in various content produced and consumed by an identity provider, such as (but not limited to) the `<wst:TokenType>` element.

2.3.2 Identifying Token Issuers

Information cards produced by identity providers MUST contain the identity provider's unique name as the value of the `<ic:Issuer>` element. This name corresponds to the SAML concept of an "entityID" and may correspond to an actual entityID in the SAML sense of the term, or a logically equivalent name for the identity provider.

2.3.3 General Assertion Requirements

Assertions issued in accordance with this profile MUST contain a single `<saml:AuthnStatement>` that reflects the authentication of the token requester to the identity provider. It MAY contain a single `<saml:AttributeStatement>` that carries one or more `<saml:Attribute>` elements reflecting the claims requested by the relying party, in the manner specified by [ISIP].

When satisfying these requested claims, the resulting `<saml:Attribute>` element's `NameFormat` XML attribute MUST be `urn:oasis:names:tc:SAML:2.0:attrname-format:uri` and its `Name` XML attribute MUST correspond to the requested claim type's URI value (e.g., in `<ic:ClaimType>` elements).

A `<saml:NameID>` element MAY be included in the assertion's `<saml:Subject>` element. If the requested claim types include a claim type with a URI corresponding to a SAML name identifier format known to the identity provider, it may satisfy that claim request by including a `<saml:NameID>` element of the proper format in the assertion's subject. If more than one claim type corresponding to a name identifier format is requested, the identity provider MAY fault the request or choose any requested format, at its discretion. If two such claim types are "required" by the relying party, a fault MUST be generated.

The assertion's `<saml:Subject>` element MUST contain at least one `<saml:SubjectConfirmation>` element, the details of which are defined in section 2.3.4 below.

Finally, the assertion MUST be signed.

2.3.4 Proof Keys and Subject Confirmation

[ISIP] defines three classes of "proof keys" that bind the issued token to key material controlled by the client: symmetric, asymmetric, and no key. The notion of a proof key maps directly to a `<saml:SubjectConfirmation>` element in the issued assertion.

If a token request does not include a `<wst:KeyType>` element, the identity provider SHOULD assume that an asymmetric proof key is required.

Both symmetric and asymmetric proof key types correspond to the "holder-of-key" confirmation method defined in section 3.1 of [SAML2Prof]. The resulting assertion MUST contain a `<saml:SubjectConfirmation>` element with a `Method` of `urn:oasis:names:tc:SAML:2.0:cm:holder-of-key`, as defined in that section. The accompanying `<ds:KeyInfo>` element MUST identify the proof key. In the case of an asymmetric proof key, the key SHOULD be represented as a `<ds:RSAKeyValue>` element within a `<ds:KeyValue>` element.

The "no key" proof key type corresponds to the "bearer" confirmation method defined in section 3.3 of [SAML2Prof]. The resulting assertion MUST contain a `<saml:SubjectConfirmation>` element with a `Method` of `urn:oasis:names:tc:SAML:2.0:cm:bearer`, as defined in that section.

In the case of bearer assertions, the `<saml:SubjectConfirmation>` element MUST include a `<saml:SubjectConfirmationData>` element containing a `NotOnOrAfter` XML attribute to limit their use, typically to a very short window of time, although the exact duration may be use case dependent. The attribute MAY be included for "holder-of-key" assertions, at the discretion of the identity provider.

The `<saml:SubjectConfirmationData>` element, if present, MUST NOT contain a `NotBefore` or `Recipient` XML attribute. The `Address` XML attribute MAY be included to indicate the expected network address of the client to the relying party.

Finally, note that other `<saml:SubjectConfirmation>` elements MAY be included at the discretion of the identity provider.

2.3.5 Conditions

Assertions MAY contain a `<saml:Conditions>` element with `NotBefore` and `NotOnOrAfter` attributes. This validity period can be independent of the window during which the client can present the assertion to a relying party as a security token (see section 2.3.4).

If the request contains a `<wsp:AppliesTo>` element, then a `<saml:AudienceRestriction>` containing a `<saml:Audience>` element MUST be included with the value of that element.

Other conditions MAY be included at the discretion of the identity provider.

2.3.6 Encryption

If a suitable key belonging to the relying party is known, the identity provider SHOULD encrypt the resulting assertion in accordance with section 6 of [SAML2Core], and return the result to the requester in the form of a `<saml:EncryptedAssertion>` element.

If a public key belonging to the relying party is communicated to the identity provider in the `<wst:RequestSecurityToken>` request message in the `<wsp:AppliesTo>` element, this key SHOULD be used in preference to any other key known to the identity provider through others means (e.g., SAML V2.0 metadata).

2.4 Relying Party Requirements

A relying party uses the mechanisms defined by [ISIP] to request security tokens in the form of SAML2.0 assertions issued by particular or arbitrary identity providers. The following sections outline requirements for describing a relying party's needs based on this profile.

2.4.1 Token Type

The token type string used with SAML V2.0 assertions MUST be `urn:oasis:names:tc:SAML:2.0:assertion`.

This string appears in various content produced by a relying party, such as (but not limited to) the `<wst:TokenType>` element.

2.4.2 IdentifyingToken Issuers

When identifying a requirement for a specific token issuer, the relying party SHOULD use the identity provider's unique name (i.e., its "entityID").

2.4.3 Identifying Relying Parties

If the relying party provides security policy metadata (see section 3.1 of [ISIP]), it MAY include a `<wsp:AppliesTo>` element inside a `<sp:RequestSecurityTokenTemplate>` element that refers to its own unique name (i.e., its "entityID") in the `<wsa:Address>` element.

If it does include a `<wsp:AppliesTo>` element, it SHOULD NOT identify itself using the location of its endpoint, as this complicates the identity provider's ability to identify the relying party. A logical name SHOULD be used instead.

2.4.4 Identifying Claim Types

SAML attributes required or desired by the relying party are identified by using the SAML attribute's `Name` XML attribute in various places, such as the `<ic:ClaimType>` element's `Uri` XML attribute. Such SAML attributes MUST have a `NameFormat` XML attribute of `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

A claim type URI corresponding to a SAML name identifier format MAY be used to request a particular type of `<saml:NameID>` element in the resulting assertion. A relying party MUST NOT request more than one "required" claim type corresponding to a name identifier format.

2.4.5 Assertion Validity

Relying parties SHOULD evaluate assertions using the rules defined by [SAML2Core] (and [SAML2Prof] in the case of the defined subject confirmation methods). Invalid assertions SHOULD NOT be used to authenticate clients that present them.

In assessing validity, a relying party MUST verify the signature over the assertion, evaluate any conditions present, and successfully evaluate at least one `<saml:SubjectConfirmation>` element in the assertion based on the presentation of the assertion. This may include verifying that the `NotOnOrAfter` attribute in the `<saml:SubjectConfirmationData>` (if present) has not passed, subject to allowable clock skew between it and the identity provider.

If the `<saml:SubjectConfirmationData>` includes an `Address` attribute, the relying party MAY check the client address against it.

In the case of the "holder-of-key" method, the relying party MUST establish proof of possession by the client of the key identified by the accompanying `<ds:KeyInfo>` element, such as through the use of a message signature or authentication over a secure transport. The exact means are out of scope.

In the case of the "bearer" method, the relying party MUST ensure that assertions are not replayed, by maintaining the set of used `ID` values for the length of time for which the assertion would be considered valid based on the `NotOnOrAfter` attribute in the `<saml:SubjectConfirmationData>` element.

2.5 Use of SAML Metadata

While not required, sites exchanging SAML assertions based on this profile MAY rely on SAML V2.0 metadata [SAML2Meta] as a way of deriving information about endpoints and keys, to supplement mechanisms that exist within [ISIP]. Where similarities or overlaps exist, precedence MUST be given to metadata information exchanged using the mechanisms defined by [ISIP].

When referring to token issuers or relying parties by "logical" names, in the manner described by [ISIP], the names used SHOULD correspond to the "entityID" values used in SAML metadata.

The value `urn:oasis:names:tc:SAML:2.0:profiles:Infocard` MUST be used in the `protocolSupportEnumeration` attribute to identify support for this profile within a `<md:IDPSSODescriptor>` or `<md:SPSSODescriptor>` role.

If `<md:SingleSignOnService>` or `<md:AssertionConsumerService>` endpoints supporting this profile are included, the same value MUST be used as the value of the `Binding` attribute. In addition, a `<wsa:EndpointReference>` element MAY be included within an endpoint element to describe the endpoint and its security policy in accordance with [ISIP].

2.6 Security Considerations

The Information Card model's support for hiding the identity of the relying party from the identity provider, combined with constraints on the implementation of the model for use with web browsers, leads to requests for "unconstrained" bearer assertions with no audience or subject confirmation conditions on use. This is **extremely** dangerous and insecure, even if assertion validity is extremely short term. This profile recommends against such a practice and urges implementations, if they do support such behavior, to enable deployers to disable it by requiring requests for bearer assertions be accompanied by the identity of the relying party.

Identity providers should generally make every attempt to encrypt the assertions they produce if a key for the relying party can be established. If encryption is not used, then the identity provider should be aware of the potential for exposure of the assertion's contents, both to the requester and potentially to network observers if TLS/SSL is not used (particularly between the requester and the eventual relying party).

Caution, however, should be exercised in relying solely on the TLS/SSL certificate found at a relying party's endpoint to identify the key. In particular, the key has to be authenticated in order to ensure that it actually belongs to the eventual endpoint used by the client. Furthermore, there can be no guarantee that the software responsible for decrypting the security token will have access to the corresponding private key.

Appendix A. Acknowledgments

The editors would like to acknowledge the contributions of the OASIS Security Services Technical Committee, whose voting members at the time of publication were:

- TBD

The editor would also like to acknowledge the following contributors:

- Jim Fox, University of Washington

Appendix B. Revision History

342

- Draft 01.

- Draft 02; incorporate feedback, refine Recipient/Audience rules, add signing requirement, enumerate assertion validation processing rules.