Web Single Sign-On Interoperability Profile

April 2005

Authors

Rajeev Angal, Sun Microsystems
Chris Kaler, Microsoft
Hubert Le Van Gong, Sun Microsystems
Eve Maler, Sun Microsystems
Ari Medvinsky, Microsoft
John Shewchuk, Microsoft

Copyright Notice

Abstract

This document defines an interoperability profile of the web single sign-on metadata exchange protocol [WSSOMEX] that allows using either Liberty Identity Federation or WS-Federation based Identity Providers to interact with a service. It defines how the service determines the protocols supported by the client's identity provider thereby allowing identity processing to occur.

Status

This specification is an initial public draft release and is provided for review and evaluation only. The authors hope to solicit your contributions and suggestions in the near future. The authors make no warrantees or representations regarding the specifications in any manner whatsoever.

Table of Contents

1. Introduction

This document describes a set of protocol suites that can be used with the Web Single Sign-On Metadata Exchange Protocol.

It defines a notion of Target Service compliance and Identity Provider compliance.

2. Notations and Terminology

This section specifies the notations, namespaces, and terminology used in this specification.

2.1. Notational Conventions

The keywords "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 [RFC 2119].

2.1.1. Normative Outlines

This specification uses the following syntax to define normative outlines for messages:

The syntax appears as an XML instance, but values in italics indicate data types instead of values.

Characters are appended to elements and attributes to indicate cardinality:

"?" (0 or 1)

"*" (0 or more)

"+" (1 or more)

The character "|" is used to indicate a choice between alternatives.

The characters "[" and "]" are used to indicate that contained items are to be treated as a group with respect to cardinality or choice.

An ellipsis (i.e. "...") indicates a point of extensibility that allows other child or attribute content. Additional children and/or attributes MAY be added at the indicated extension points but MUST NOT contradict the semantics of the parent and/or owner, respectively. If an extension is not recognized it SHOULD be ignored.

XML namespace prefixes (see [XML-ns]) are used to indicate the namespace of the element being defined.

Additionally, normative text is provided describing elements and attributes, their expected values, and any usage expectations and restrictions. Normative text within this specification takes precedence over normative outlines, which in turn take precedence over any XML Schema and WSDL descriptions that are provided here or referenced from other specifications.

2.2. XML Namespaces

The XML namespace URI that MUST be used by implementations of this specification is:

```
http://schemas.xmlsoap.org/ws/2005/04/ssi
```

where ssi refers to Single Sign-on Interoperability.

The following table lists XML namespaces that are used in this specification. The choice of any namespace prefix is arbitrary and not semantically significant.

Prefix	XML Namespace	Specification(s)
ssi	http://schemas.xmlsoap.org/ws/2005/04/ssi	This document
xs	http://www.w3.org/2001/XMLSchema	XML Schema [Part 1, 2]

2.3. Compliance

A target service or identity provider is not compliant with this profile if it fails to satisfy one or more of the MUST or REQUIRED level requirements defined herein. A SOAP Node MUST NOT use the XML namespace identifier for this specification (listed in Section 2.2) within SOAP Envelopes unless it is compliant with this specification.

This specification references a number of other specifications (see the table above). In order to comply with this specification, an implementation MUST implement the portions of referenced specifications necessary to comply with the required provisions of this profile. Additionally, the implementation of the portions of the referenced specifications that are specifically cited in this specification MUST comply with the rules for those portions as established in the referenced specification. It is not necessary for

compliance with this specification to implement portions of referenced specifications that are not (directly or transitively) identified by this specification.

Additionally normative text within this specification takes precedence over normative outlines (as described in section 2.1.1), which in turn take precedence over the XML Schema [XML Schema Part 1, Part 2] and WSDL [WSDL 1.1] descriptions. That is, the normative text in this specification further constrains the schemas and/or WSDL that are part of this specification; and this specification contains further constraints on the elements defined in referenced schemas.

3. Protocol Suite Profile

The following sections provide specific details and restrictions on the indicated specifications to support the model defined in the Web Single Sign-On Metadata Exchange Protocol [WSSOMEX].

This profile defines a subset of mechanisms for interoperability between WS-Federation and Liberty Identity Federation (ID-FF) based applications.

Specifically:

- Section 3.1 describes a set of required protocol suites.
- Section 3.2 describes an interoperable subset of the SAML profile that a compliant implementation MUST support
- Section 3.3 describes an interoperable subset of Liberty ID-FF protocols that a compliant implementation MUST support
- Section 3.4 describes an interoperable subset of the WS-Federation Passive Requestor Profile that a compliant implementation MUST support

This profile brings into scope the following specifications:

- Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V1.1 [SAML]
- WS-Addressing [WS-Addressing]
- Liberty ID-FF Bindings and Profiles Specification, Version 1.2 [IDFFBP]
- WS-Federation Passive Requestor Profile [WSFRP]
- WS-MetadataExchange [MEX]
- WS-Security [WS-Security]

3.1. Protocol Suites

The following protocol identifiers are defined:

Identifier	Meaning
`<ssi:ID-FF_12/>`	The Liberty 1.2 identity establishment and verification protocols are supported as profiled below.
`<ssi:WSFed_10/>`	The WS-Federation 1.0 identity establishment and verification protocols are supported as profiled below.

A compliant target service implementation MUST support both protocol suites; this ensures maximum reach for the target service.

A compliant identity provider implementation MUST support both protocol suites; this ensures maximum reach for the identity provider.

Note that as described in the WebSSO metadata exchange protocol [WSSOMEX] in the case where both the target service and the identity provider support both protocol suites it is up to the target service to select its preferred protocol.

3.2. SAML Profile

Identification: http://schemas.xmlsoap.org/ws/2005/04/ssi

Contact Information: webssoq@Microsoft.com, Eve.Maler@Sun.COM

SAML Confirmation Method Identifiers: urn:oasis:names:tc:SAML:1.0:cm:bearer.

Description: Given below.

Updates: None.

In order to facilitate interoperability, this profile uses SAML assertions to convey identity information, as defined in [SAML] and profiled here.

Only identity and name/value type claims are supported. The notion of "claims" is modeled in SAML as an "assertion statement". So an "identity claim" is expressed via an AuthenticationStatement, and a "name/value" claim is expressed via an AttributeStatement. The SAML assertion issued by the assertion provider in this profile must carry an identity claim in the *AuthenticationStatement* (via the Subject/NameIdentifier element) and may carry any number of name/value type claims in the *AttributeStatement*.

To express Group claim semantics, the name/value claim syntax MUST be used as described in the below:

#	*Claim Definition*	*Claim usage in SAML*

1	**Claim name:** group
	
	URL: http://schemas.xmlsoap.org/2004/06/webSSO/group
	
	Description: the group claim. The group claim can only be carried in the attribute element of AttributeStatement. (It is never used in the Subject/NameIdentifier element).
		SAML Example:
		
		`<AttributeStatement>`
		`<Subject>...</Subject>`
		`<Attribute AttributeName="group"`
		`AttributeNamespace="http://schemas.xmlsoap.org/2004/06/webSSO/group">`
		`<AttributeValue>Managers</AttributeValue>`
		`</Attribute>`
		`</AttributeStatement>`

It should be noted that if there are privacy concerns around passing identity or any statements made, care should be taken to protect this information.

The error codes defined in SAML, WS-Security, and SOAP are possible within this profile.

The following rules are established:

R-01) Assertion providers MUST support, at a minimum, SAML 1.1 security tokens

R-02) SAML assertions MUST carry an identity claim in the authentication statement via the Subject/NameIdentifier

R-03) SAML assertions MAY carry any number of name/value type claims in the AttributeStatement

R-04) Group claims MUST use the syntax indicated in this document

R-05) The <saml:ConfirmationMethod> element of the assertion MUST be set to the SAML V1.1 "Bearer" method: urn:oasis:names:tc:SAML:1.0:cm:bearer

3.3. Liberty Identity Federation Profile

The interoperable profile of the Liberty Identity Federation browser federation protocol is the Liberty Identity Federation Browser POST Profile, as described in section 3.2.3 of [IDFFBP], with the restriction that WML is not supported.

The SAML assertion used is subject to the constraints defined above.

The following rules are established:

R-06) The Liberty Identity Federation Browser POST Profile MUST be supported

R-07) Support for WML is excluded from this profile

3.4. WS-Federation Passive Requestor Profile

The interoperable subset of WS-Federation Passive Profile is defined in the WS-Federation Passive Requestor Interoperability Profile [WSFIP] document.

The WS-Federation Passive Requestor Interoperability Profile is a further constraint to the Passive Requestor Profile [WSFRP].

The SAML assertion used is subject to the constraints defined above.

As defined in WS-Federation Passive Requestor Interoperability Profile to conform to this specification, messages 1, 4, 7 & 10 must be supported. All other message exchanges are implementation specific and are only provided in [WSFRP] for guidance.

The following rules are established:

R-08) The WS-Federation Passive Requestor Profile MUST be supported

R-09) The Passive Requestor Profile is further restricted to the subset identified in WSFRP

4. Security Considerations

It is strongly recommended that the messages exchanged by Web services be secured using WS-Security-based [WS-Security] mechanisms. In order to properly secure a message, the SOAP body and all relevant SOAP header blocks need to be explicitly included in the signature's "signed data". Specifically, any standard messaging header blocks, such as those from WS-Addressing [WS-Addressing], need to be included in the same signature as the SOAP body in order to "bind" them all together.

Additionally, different security mechanisms may be desired depending on the frequency of message transmission. For example, for infrequent messages, public key technologies applied to individual messages, as described above, may be adequate. However, for high-frequency message transmissions, it may be more performant to establish a security context between the endpoints. If a shared secret is used, it is RECOMMENDED that derived keys be used to strengthen the secret.

Requests for metadata that are not available to anonymous parties are strongly RECOMMENDED to require usage of WS-Security so that the requester can be authenticated and authorized to access the indicated metadata. Similarly, integrity and confidentiality SHOULD be used whenever metadata has restricted access.

Recipients of metadata are RECOMMENDED to validate the signature to authenticate and verify the integrity of the data. Specifically, recipients SHOULD verify that the sender

has the right to "speak" for the metadata. This is important because some metadata, such as schemas, have embedded target URIs that might be outside the scope of the sender.

If a metadata request results in a reference to another location, care should be taken if that location is in a different security domain or realm from that of the original request target.

It should be noted that when using URL parameters to indicate the identity providers there is the possibility of a redirect attack by inserting a different identity provider that the requestor expected (because the URL parameters are often not verified by users). Constraints on the identity provider, additional security mechanisms, and/or user interface should be used to mitigate against such attacks

The following list summarizes common classes of attacks that apply to this protocol and identifies the mechanism to prevent/mitigate the attacks:

Message alteration – Alteration can be prevented through including signatures of the message information using WS-Security mechanisms.

Message disclosure – Confidentiality can be preserved by encrypting sensitive data using WS-Security mechanisms.

Key integrity – Key integrity can be maintained by using the strongest algorithms possible.

Authentication – Authentication of messages can be established using the mechanisms described in WS-Security.

Accountability – Accountability is a function of the type of and strength of the key and algorithms being used. In many cases, a strong symmetric key provides sufficient accountability. However, in some environments, strong PKI signatures are required.

Availability – Metadata services are subject to a variety of availability attacks such as application-level denial of service. It is recommended that the mechanisms described in WS-Security be considered as mitigations for some forms of attacks. Other attacks, such as network-level denial of service, are harder to avoid. Note that both of these classes of attack are outside the scope of this specification.

Replay – Messages may be replayed for a variety of reasons. To detect and eliminate this attack, mechanisms should be used to identify replayed messages such as the timestamp/nonce outlined in WS-Security. Alternatively, and optionally, other technologies, such as sequencing, can also be used to prevent replay of application messages.

Privacy - Adequate privacy protections should be assured so as to inhibit the unauthorized disclosure of personally identifiable information. In addition, controls should be established so that personally identifiable information is not shared without user notification and consent and that where applicable privacy regulations may be accommodated.

5. Acknowledgements

This specification has been developed as a result of joint work with many individuals and teams, including:

Qingwen Cheng (Sun)
Gary Ellison (Former co-author)

Jeff Hodges (Former co-author)
Chuck Mortimore
Jeffrey Schlimmer (Microsoft)
Don Schmidt (Microsoft)
Wei Sun (Sun)
Emily Xu (Sun)

6. References

[IDFF]
Liberty ID-FF Architecture Overview, Version 1.2

[IDFFBP]
Liberty ID-FF Bindings and Profiles Specification, Version 1.2

[IDFFPS]
Liberty ID-FF Protocols and Schema Specification, Version 1.2

[MEX]
Keith Ballinger, et al, "Web Services Metadata Exchange (WS-MetadataExchange)", September 2004.

[RFC 2119]
S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, Harvard University, March 1997.

[RFC 2616]
R. Fielding, et al, "Hypertext Transfer Protocol -- HTTP/1.1," RFC 2616, UC Irvine, June 1999.

[SAML]
Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V1.1

[SOAP 1.1]
D. Box, et al, "Simple Object Access Protocol (SOAP) 1.1," May 2000.

[SOAP 1.2]
M. Gudgin, et al, "SOAP Version 1.2 Part 1: Messaging Framework," June 2003.

[WS-Addressing]
D. Box, et al, "Web Services Addressing (WS-Addressing)," August 2004.

[WS-Policy]
S. Bajaj, et al, "Web Services Policy Framework (WS-Policy)," September 2004.

[WS-Security]
A. Nadalin, et al, "Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)," March 2004.

[WSDL 1.1]
E. Christensen, et al, "Web Services Description Language (WSDL) 1.1," March 2001.

[XML Schema, Part 1]
H. Thompson, et al, "XML Schema Part 1: Structures," May 2001.

[XML Schema, Part 2]
P. Biron, et al, "XML Schema Part 2: Datatypes," May 2001.

[WSFED]
S. Bajaj, et al, "Web Services Federation Language (WS-Federation)")

[WSFRP]
S. Bajaj, et al, "WS-Federation Passive Requestor Profile"

[WSFIP]
WS-Federation Passive Requestor Interoperability Profile (as Passive Federation Interop Scenario.doc)

[WSSAML]
OASIS Web Services Security: SAML Token Profile

[WSSOMEX]
Web Single Sign-On Metadata Exchange Protocol

[WSX]
OASIS Web Services Security: X.509 Certificate Token Profile; Errata

[XML-ns]
W3C Recommendation, "Namespaces in XML," 14 January 1999