Shibboleth Architecture

Conformance Requirements

10 September 2005

Document identifier:
internet2-mace-shibboleth-arch-conformance-200509

Location:
http://shibboleth.internet2.edu/shibboleth-documents.html

Editors:
Scott Cantor (cantor.2@osu.edu), The Ohio State University

Contributors:
RL "Bob" Morgan, University of Washington
Tom Scavo, NCSA

Abstract:
This specification provides the technical requirements for Shibboleth conformance. Shibboleth is itself built on the OASIS SAML 1.1 specification (http://www.oasis-open.org/committees/security). Readers should be familiar with that specification before reading this document.

Status:
Please submit comments to the shibboleth-dev mailing list (see http://shibboleth.internet2.edu/ for subscription details).

Table of Contents

1 Introduction

This normative specification describes features that are mandatory and optional for implementations claiming conformance to the *Shibboleth Architecture: Protocols and Profiles* specification [ShibProt].

1.1 Notation

This specification uses normative text to describe the use of SAML 1.1 and additional Shibboleth profiles.

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.

2 Profiles and Conformance Requirements

2.1 Shibboleth Profiles

The following set of profiles comprise the Shibboleth architecture [ShibProt]:

- Authentication Request
- Browser/POST Authentication Response
- Browser/Artifact Authentication Response
- Attribute Exchange
- Transient NameIdentifier Format
- Metadata

2.2 Conformance

This section describes the technical conformance requirements for Shibboleth implementations. General conformance requirements for Shibboleth are derived from SAML 1.1 conformance requirements [SAMLConf]. Where Shibboleth makes use of a SAML protocol or profile (such as Browser/POST or Browser/Artifact), the conformance requirements established by [SAMLConf] are assumed unless otherwise noted.

2.2.1 Roles

The roles that a software component can play in conforming to Shibboleth are as follows:

- Identity Provider (IdP)
- Service Provider (SP)

2.2.2 Feature Matrix

The following matrix identifies basic conformance requirements in terms of which profiles must (or need not) be supported by particular components.

Profile/Protocol	**IdP**	**SP**
Authentication Request	MUST	MUST
Browser/POST Authentication Response	MUST	MUST
Browser/Artifact Authentication Response	MUST	MUST
Attribute Exchange	MUST	OPTIONAL
Transient NameIdentifier Format	MUST	MUST
Metadata Profile	MUST	MUST

2.2.3 SAML Binding and Profile Requirements

Implementations of the Attribute Exchange and the Browser/Artifact profiles MUST support the SOAP 1.1 SAML binding [SAMLBind] and MUST adhere to its conformance requirements. In particular, implementations MUST support the mandatory authentication, confidentiality, and integrity mechanisms required by [SAMLBind].

Implementations of the Browser/Artifact profile MUST support the type 0x0001 artifact format defined by [SAMLBind].

Identity provider implementations of the browser profiles SHOULD support the ability to deliver attributes with the authentication response (attribute-push). Service provider implementations MUST support this on the receiving end.

2.2.4 Metadata Profile Requirements

It is difficult to describe clear conformance requirements for the support of metadata. In the interest of interoperability, the intent of this requirement is to ensure that a consistent approach to the public exchange of configuration and trust information is possible.

Support for the Shibboleth metadata profile does not require that implementations provide native support for or configure themselves via this format. They must only provide a reasonable mechanism to produce and consume it in some fashion in order to establish the necessary configuration that enables partnering deployments to successfully make use of the other Shibboleth profiles.

It is specifically OPTIONAL to support the dynamic acquisition and use of metadata in real time through the resolution of URL-based entity identifiers described in [ShibProt].

3 References

The following works are cited in the body of this specification.

3.1 Normative References

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

[ShibProt] S. Cantor et al. *Shibboleth Architecture: Protocols and Profiles*. Internet2-MACE, September 2005. Document ID internet2-mace-shibboleth-arch-protocols. http://shibboleth.internet2.edu/shibboleth-documents.html.

[SAMLBind] E. Maler et al. *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)*. OASIS, September 2003. Document ID oasis-sstc-saml-bindings-profiles-1.1. http://www.oasis-open.org/committees/security/.

[SAMLConf] E. Maler et al. *Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML)*. OASIS, September 2003. Document ID oasis-sstc-saml-conform-1.1. http://www.oasis-open.org/committees/security/.

3.2 Non-Normative References

[SAML2Conf] P. Mishra et al. *Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID oasis-sstc-saml-conform-2.0. http://www.oasis-open.org/committees/security/.