Metadata Discovery Protocols for SAML 2.0 Web Browser SSO Profiles

Working Draft 00, 01 October 2003

Document identifier:
sstc-saml-MetadataDiscoveryProtocols-2.0-draft-00

Location:

http://www.oasis-open.org/apps/org/workgroup/security/download.php

Editor:
Jahan Moreh, Sigaba <jmoreh@sigaba.com>

Abstract:

The SAML Web Browser SSO Profiles require agreements between source and destination sites about supported protocols, service end points, supported profiles, source and destination IDs, certificates, cryptographic keys, and so forth. Metadata definitions are useful for describing this information in a standardized way. Moreover, it is desirable for assertion producers and consumers to have standard ways for discovering metadata about each other. This document describes a proposal for Metadata Discovery Protocol. The proposal described in this document borrows extensively from the metadata discovery protocol defined in the draft Liberty Alliance 1.2 specifications [**libMD**].

Status:

This document is a solution proposal for SAML 2.0 Work Item W-3 specified in [**SAML2.0Work**] (action item #0064). The final, accepted proposal will be incorporated into the document entitled Metadata for SAML 2.0 Web Browser Profiles [**SAMLMetaData**].

For information on whether any patents have been disclosed that may be essential to implementing this proposal, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Security Services TC web page (http://www.oasis open.org/committees/security/).

Table of Contents

1 Summary

The SAML Web Browser SSO Profiles **[SAMLBind]** require agreement between source and destination sites about supported protocols, service end points, supported profiles, source and destination IDs, certificates, cryptographic keys, and so forth. Sources and destinations of SAML Web Browser SSO Profiles can exchange this information via a set of metadata as proposed in [**SAMLMetaData**]. The current version of [**SAMLMetaData**] leaves unspecified the protocol for discovering the location of metadata. A discovery protocol enables real-time communication of metadata and eliminates the need for out-of-band exchange of metadata.

The Liberty Alliance 1.2 draft specifications include metadata description and discovery protocols (see **[libMD]**). This proposal **recommends that SAML 2.0 adopt the Liberty Metadata Discovery Protocols** and incorporate that specification into the document *Metadata for SAML 2.0 Web Browser Profiles.* The resulting document would be entitled *Metadata Description and Discovery Protocols for SAML 2.0 Web Browser Profiles*.

2 Liberty Metadata Discovery

Liberty metadata discovery envisions two methods for *providers* to discover metadata about each other. Liberty uses the terms *Service Providers* and *Identity Providers* as roughly equivalent to SAML Assertion Consumers and Assertion Producers.

The first method uses a provider's mandatory element `providerID`. A `providerID` is a URI and is used to uniquely identify each provider. There is precedence in SAML specifications for requiring distinct provider IDs (see line 588 of [**SAMLBind**). This first method states that the URI is a URL that can be de-referenced to obtain the provider's metadata. This is a simple method and should work in many situations. It also has a benefit in that it does not require provisioning the network infrastructure.

The second method uses DNS to publish metadata locations. Using existing DNS protocols and discovery methods, one can determine the location of the provider's metadata. Dynamic Delegation Discovery System [**RFC 3403**] defines a specific DNS resource record called Naming Authority Pointer (NAPTR) resource record [**RFC 2915**]. A NAPTR record specifies a regular expression for so-called re-writing rules. A simple example follows.

Assume a `providerID` URI of `http://samlprovider.com/saml/consumer/cs`. A possible regular expression and replacement string could be like:

```
!^([^:/?#]+:)?/*([^:/?#]*@)?(([^/?:#]*\.)*(([^/?#:\.]+)\.([^/?#:\.]+)))(:\d+)?([
^?#]*)(\?[^#]*)?(#.*)?$!\3!
```

This expression extracts the FQDN (i.e., `samlprovider.com`), which is "subexpression" #3. The FQDN is used as the *replacement* string. Next, the requestor performs a DNS NAPTR query to the domain samlprovider.com. It may get a response like:

```
!^.*$!https://samlprovider.com/metadata/cs/consumer.xml!
```

This replacement string states that the data should be replaced with `https://samlprovider.com/metadata/cs/consumer.xml`.

DDDS and NAPTR provide a way to inform the requestor if the replacement string is "terminal" or not. This is accomplished using a flag (not shown in the examples).

DDDS has a specific initial regular expression for parsing URNs (see [**RFC 3403**), which Liberty has adopted. Also, DNS Security Extensions [**RFC 2535**] along with SSL/TLS [**RFC 2246**] are recommended for ensuring integrity of DNS records as well as that of the final metadata document.

3 Metadata Communication Protocol

In addition to the location of metadata, the protocols proposed in this document provide for discovery of the communication protocols as follows:

- Well-known URL method includes the communication protocol (e.g., https).
- A NAPTR record includes a *service field*, which specifies the communication protocol.

SAML entities are free to exchange metadata using other protocols (including an out-of-band method). However, SAML 2.0 should not make any recommendations regarding these other possible protocols.

4 References

[**SAMLBind**] E. Maler, P. Mishra, R. Philpott (Editors), Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) 1.1, Committee Specification, 18 July 2003.

[**libMD**] P. Davis (Editor), Liberty Metadata Description and Discovery Specification. Version 1.0-08; July 2003.

[**SAMLMetaData**] J. Moreh (Editor), Metadata for SAML 2.0 Web Browser SSO Profiles, Working Draft 00, 15 September 2003.

[**SAML2.0Work**] S. Cantor, P. Mishra, E. Maler (Editors) SAML Version 2.0 Scope and Work Items. Draft 08. 30 September 2003.

[**RFC 3403**] M. Mealing, Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database.

[**RFC 2915**] M. Mealing and R. Daniel, The Naming Authority Pointer (NAPTR) DNS Resource Record

[**RFC 2535**] D. Eastlake, Domain Name System Security Extensions.

[**RFC 2246**] T. Dierks and C. Allen, The TLS Protocol, Version 1.0

Appendix A. Revision History

Rev	Date	By Whom	What
00	2003-10-01	Jahan Moreh	Initial draft based on Liberty Metadata Description and Discovery Protocols.

Appendix B. Notices

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's procedures with respect to rights in OASIS specifications can be found at 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 implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.