



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/>).

28 **Table of Contents**

29 1 Summary..... 3
30 2 Liberty Metadata Discovery 4
31 3 Metadata Communication Protocol..... 5
32 4 References..... 6
33 Appendix A. Revision History 7
34 Appendix B. Notices 8

35

36

1 Summary

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

44

45 The Liberty Alliance 1.2 draft specifications include metadata description and discovery protocols
46 (see **[libMD]**). This proposal **recommends that SAML 2.0 adopt the Liberty Metadata**
47 **Discovery Protocols** and incorporate that specification into the document *Metadata for SAML*
48 *2.0 Web Browser Profiles*. The resulting document would be entitled *Metadata Description and*
49 *Discovery Protocols for SAML 2.0 Web Browser Profiles*.

2 Liberty Metadata Discovery

50

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

54

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

61

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

67

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

70

71

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

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

75

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

76

77

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

78

79

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).

80

81

82

83

84

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.

85 **3 Metadata Communication Protocol**

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

- 88
- Well-known URL method includes the communication protocol (e.g., https).
 - A NAPTR record includes a *service field*, which specifies the communication protocol.
- 89

90

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

94

4 References

- 95
- 96 **[SAMLBind]** E. Maler, P. Mishra, R. Philpott (Editors), Bindings and Profiles for the
97 OASIS Security Assertion Markup Language (SAML) 1.1, Committee
98 Specification, 18 July 2003.
99
- 100 **[libMD]** P. Davis (Editor), Liberty Metadata Description and Discovery
101 Specification. Version 1.0-08; July 2003.
102
- 103 **[SAMLMetaData]** J. Moreh (Editor), Metadata for SAML 2.0 Web Browser SSO Profiles,
104 Working Draft 00, 15 September 2003.
105
- 106 **[SAML2.0Work]** S. Cantor, P. Mishra, E. Maler (Editors) SAML Version 2.0 Scope and
107 Work Items. Draft 08. 30 September 2003.
108
- 109 **[RFC 3403]** M. Mealing, Dynamic Delegation Discovery System (DDDS) Part Three:
110 The Domain Name System (DNS) Database.
111
- 112 **[RFC 2915]** M. Mealing and R. Daniel, The Naming Authority Pointer (NAPTR) DNS
113 Resource Record
114
- 115 **[RFC 2535]** D. Eastlake, Domain Name System Security Extensions.
116
- 117 **[RFC 2246]** T. Dierks and C. Allen, The TLS Protocol, Version 1.0

118 **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.

119

120

121

Appendix B. Notices

122 OASIS takes no position regarding the validity or scope of any intellectual property or other rights
123 that might be claimed to pertain to the implementation or use of the technology described in this
124 document or the extent to which any license under such rights might or might not be available;
125 neither does it represent that it has made any effort to identify any such rights. Information on
126 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS
127 website. Copies of claims of rights made available for publication and any assurances of licenses
128 to be made available, or the result of an attempt made to obtain a general license or permission
129 for the use of such proprietary rights by implementors or users of this specification, can be
130 obtained from the OASIS Executive Director.

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

134 Copyright © OASIS Open 2003. *All Rights Reserved.*

135 This document and translations of it may be copied and furnished to others, and derivative works
136 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,
137 published and distributed, in whole or in part, without restriction of any kind, provided that the
138 above copyright notice and this paragraph are included on all such copies and derivative works.
139 However, this document itself does not be modified in any way, such as by removing the
140 copyright notice or references to OASIS, except as needed for the purpose of developing OASIS
141 specifications, in which case the procedures for copyrights defined in the OASIS Intellectual
142 Property Rights document must be followed, or as required to translate it into languages other
143 than English.

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

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