Name Identifier Management in SAML 2.0

Working Draft 00, 25 August 2003

Document identifier:

draft-sstc-nameid-00

Location:

http://www.oasis-open.org/committees/security/docs

Editors:

Scott Cantor, individual <cantor.2@osu.edu>
John Linn, RSA Laboratories <jlinn@rsasecurity.com>

Contributors:

Abstract:

This document proposes candidate requirements for name identifier management in SAML 2.0. Subsequent versions will be augmented with use case and mechanism proposals.

Status:

Interim draft. Send comments to the editors.

Committee members should send comments on this specification to the security-services@lists.oasis-open.org list. Others should subscribe to and send comments to the security-services-comment@lists.oasis-open.org list. To subscribe, send an email message to security-services-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

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 Intellectual Property Rights section of the Security Services TC web page (http://www.oasis-open.org/committees/security/).
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>31</td>
<td>1.1 Notation</td>
<td>4</td>
</tr>
<tr>
<td>32</td>
<td>2 Candidate Name Identifier Requirements for SAML 2.0</td>
<td>6</td>
</tr>
<tr>
<td>33</td>
<td>2.1 Identity Federation</td>
<td>6</td>
</tr>
<tr>
<td>34</td>
<td>2.2 Representation of Federated Identities</td>
<td>6</td>
</tr>
<tr>
<td>35</td>
<td>2.3 Affiliations</td>
<td>7</td>
</tr>
<tr>
<td>36</td>
<td>2.4 Anonymous Session Identifiers</td>
<td>7</td>
</tr>
<tr>
<td>37</td>
<td>2.5 Name Identifier Encryption</td>
<td>8</td>
</tr>
<tr>
<td>38</td>
<td>2.6 Federation Management</td>
<td>8</td>
</tr>
<tr>
<td>39</td>
<td>3 Use Cases</td>
<td>10</td>
</tr>
<tr>
<td>40</td>
<td>4 Candidate Mechanisms</td>
<td>11</td>
</tr>
<tr>
<td>41</td>
<td>5 Security Considerations</td>
<td>12</td>
</tr>
<tr>
<td>42</td>
<td>6 References</td>
<td>13</td>
</tr>
<tr>
<td>43</td>
<td>Appendix A. Revision History</td>
<td>15</td>
</tr>
<tr>
<td>44</td>
<td>Appendix B. Notices</td>
<td>16</td>
</tr>
</tbody>
</table>
Introduction

This document proposes candidate requirements for name identifier management in SAML 2.0. Subsequent versions will be augmented with use case and mechanism proposals.

1.1 Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF RFC 2119. [RFC2119]

Listings of productions or other normative code appear like this.

Example code listings appear like this.

Note: Non-normative notes and explanations appear like this.

Conventional XML namespace prefixes are used throughout this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

- The prefix saml: stands for the SAML assertion namespace [SAMLCore].
- The prefix samlp: stands for the SAML request-response protocol namespace [SAMLCore].
- The prefix ds: stands for the W3C XML Signature namespace, http://www.w3.org/2000/09/xmldsig# [XMLSig].
2 Candidate Name Identifier Requirements for
SAML 2.0

This section proposes candidate name identifier requirements for SAML 2.0, including account
linking, pseudonyms, and anonymity facilities. Many of these requirements have been addressed
within the Liberty Alliance Identity Federation Framework (ID-FF) [LibBP] [LibPS], using
approaches that may also be suitable for integration within SAML.

ISSUE: SAML currently speaks in terms of authentication authorities and relying parties, but
Liberty speaks of identity providers and service providers. How should these terms be aligned?

2.1 Identity Federation

SAML 2.0 shall support the ability for authentication authorities to federate identities of principals,
so that a principal’s identity as demonstrated to the authentication authority can be persistently
linked to identifiers as presented to relying parties within authentication assertions.

2.2 Representation of Federated Identities

SAML 2.0 shall provide facilities enabling a federated principal’s identity to be indicated to a
relying party in a form that is specific and significant only to that relying party. In particular,
facilities must be provided so that provision of a globally significant principal identifier to relying
parties is not required, and possession of two or more identifiers generated by an authentication
authority must not provide sufficient information to determine whether more than one of the
identifiers corresponds to the same principal. (Comment: it is recognized, however, that colluding
relying parties may correlate patterns of accesses to their sites and thereby detect corresponding
identifiers, though possibly with some level of uncertainty.) While globally significant identifiers
may be permissible in some environments (e.g., within enterprises), and should be supported for
use as appropriate, facilities affording enhanced privacy assurance are also required.

SAML 2.0 shall enable a relying party to specify to an authentication authority the identifier that is
to be used to represent a federated principal to that relying party.

2.3 Affiliations

SAML 2.0 shall enable groups of relying parties to designate themselves as affiliations, with the
result that federation with the affiliation through any of its members will have the effect of
federating with all members. As a result, all affiliation members will receive the same identifier to
represent a federated principal. In environments where affiliations are used, principals shall be
able to determine that a prospective federation corresponds to an affiliation, and shall be able to
enumerate the affiliation’s membership.

2.4 Anonymous Session Identifiers

SAML 2.0 shall provide a facility enabling a principal’s identity to be reflected to relying parties
anonymously, using unique and non-persistent identifiers. Identifiers of this type may be obtained
upon relying party request; additionally, principals may designate that they are to be so
represented to relying parties within the scope of an authentication authority session. This facility
shall be applicable independent of whether or not the principal has a federation relationship
between the SAML authentication authority and any of the relying parties receiving assertions
within the session. Desirably, it should be possible for a principal to request and/or configure use of this facility at the granularity of individual relying parties.

2.5 Name Identifier Encryption

SAML 2.0 shall specify an interoperable means for name identifiers to be encrypted, so that they cannot be meaningfully interpreted at an intermediate entity. The form of encryption shall ensure that successive encryptions of a persistent identifier will yield distinct results that cannot be meaningfully correlated to one another.

2.6 Federation Management

SAML 2.0 shall provide facilities enabling principals to request initiation and termination of federation relationships between a SAML authentication authority and particular relying parties, which can be initiated either at the authentication authority or at a relying party.

Although relying parties may initiate federation requests, no federation shall be established without approval by the principal’s authentication authority, which is relied upon to act in accordance with a policy accepted by the principal. Means shall be specified enabling the authentication authority to obtain explicit confirmation by the principal before a federation is established.

While federations are normally terminated upon authenticated, confirmed principal request to an authentication authority or relying party, these processing entities may also initiate terminations unilaterally. An authentication authority, e.g., may act to terminate a principal’s federations when the principal’s account with the authentication authority is terminated.

Although outside protocol scope, SAML 2.0 authentication authorities should provide their principals with interfaces that allow them to display and manage their federations. In some environments, administrative access to such facilities may also be appropriate.
3 Use Cases

TBS.
4 Candidate Mechanisms

TBS.
5 Security Considerations

TBS.
6 References


[WS-Sec] Web Services Security (WS-Security) specifications, OASIS.

## Appendix A. Revision History

<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>By Whom</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>wd-00</td>
<td>2003-08-25</td>
<td>John Linn</td>
<td>Initial candidate requirements.</td>
</tr>
</tbody>
</table>
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.

Copyright © OASIS Open 2003. All Rights Reserved.

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 paragraph are included on all such copies and derivative works. However, this document itself does not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document 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 RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.