Name Identifier Profiles and Management in SAML 2.0

Working Draft 07, 15 December 2003

Document identifier:
draft-sstc-nameid-07

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:
Liberty Alliance ID-FF Specification Contributors

Abstract:
This document proposes candidate requirements, use cases, and candidate solutions for name identifier profiles and management in SAML 2.0.

Status:
Working draft. Send comments to the mailing list.

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

1 Introduction

This document proposes candidate use cases, requirements, and solutions for name identifier profiles and management in SAML 2.0.

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 [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
- The prefix `samlp:` stands for the SAML request-response protocol namespace
- The prefix `ds:` stands for the W3C XML Signature namespace, `http://www.w3.org/2000/09/xmldsig#`
- The prefix `xenc:` stands for the W3C XML Encryption namespace, `http://www.w3.org/2001/04/xmlenc#`

2 Definitions

The following new terminology is used in this document:

Account

A formal business agreement for providing regular dealings and services between a Principal and identity or service providers.

Account Linkage

A method of relating accounts at two different providers that represent the same Principal so that the providers can communicate about the Principal. Account linkage can be established through the sharing of attributes or through Identity Federation.

Affiliation

An affiliation is a set of one or more entities who may perform interactions as a member of the set. Members of an affiliation may invoke services either as a member of the affiliation or individually. "Affiliation" and "affiliation group" are equivalent terms.

Federation

An association comprising any number of service providers and identity providers.

Identity Defederation

The elimination of the linkage between a Principal's accounts at an identity provider and a service provider, such that the identity provider no longer provides the associated identifier to the service provider, and the service provider will no longer accept the associated identifier from the identity provider.

Identity Federation

Linking accounts for a given Principal at a pair of providers within a federation by establishing (or using an existing) identifier to refer to the Principal.

Identity Provider

An entity that creates, maintains, and manages identity information for Principals and provides Principal authentication to other service providers within a federation, such as with web browser profiles.

Persistent Pseudonym

A privacy-preserving name identifier assigned by an identity provider or service provider to identify a Principal to a given relying party for an extended period of time that spans multiple sessions; can be used to represent an identity federation.

Service Provider

An entity that provides services to Principals.

Transient Pseudonym

A privacy-preserving name identifier assigned by an identity provider to identify a Principal to a given relying party for a relatively short period of time that need not span multiple sessions.

3 Name Identifier Requirements for SAML 2.0

This section proposes candidate name identifier requirements for SAML 2.0, including account linking, persistent pseudonyms, and single-use identifiers for anonymity to service providers. 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.

3.1 Account Linking with 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.

3.2 Representation of Federated Identities

SAML 2.0 shall provide facilities enabling a principal's federated 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 and should be considered as other profiles are defined.

SAML 2.0 shall also enable one relying party to specify to another relying party the identifier that is to be used to represent a principal's federated identity to it.

3.3 Affiliations

SAML 2.0 shall enable groups of relying parties to designate themselves as affiliations, with the result that identity 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 identity. In environments where affiliations are used, principals shall be able to determine that a prospective identity federation corresponds to an affiliation, and shall be able to enumerate the affiliation's membership.

3.4 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, unless the deployment specifically obviates the need for such privacy considerations.

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. For example, an authentication authority 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.

3.5 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.

The mechanism specified should enable entities that do not mutually have an identity federation with a principal, but who each share an identity federation with a common third entity (typically an authentication authority), to communicate about the principal, subject to appropriate policies and consent. In other words, an encrypted SAML name identifier must itself be an acceptable SAML name identifier.

3.6 Transient Identifiers

SAML 2.0 shall provide a facility enabling a principal's identity to be reflected to relying parties anonymously (in effect), using 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 a 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.

4 Use Cases

In the following scenarios, the actors are the principal/user, one or more service providers, and the identity provider.

4.1 Service Provider Initiates Identity Federation

4.1.1 Preconditions

1. The principal has an account at a service provider and an identity provider.
2. The principal has authenticated to the service provider and is visiting its site.

4.1.2 Flow

1. The principal indicates consent to federate his identity.
2. The service provider requests that the identity provider authenticate the principal and federate his identity.
3. The identity provider authenticates the principal (if it hadn't previously done so), generates a name identifier for the new identity federation, and records it for future use.
4. The identity provider issues an assertion to the principal to communicate the federated name identifier to the service provider.
5. The service provider establishes the identity federation by linking the name identifier to its local account identitier for the principal.

4.1.3 Postconditions

1. The service provider and identity provider share a common name identifier for the principal, linked to each provider's local identifier for him.

4.2 Identity Provider Initiates Identity Federation

4.2.1 Preconditions

1. The principal has an account at a service provider and an identity provider.
2. The principal has authenticated to the identity provider and is visiting its site.

4.2.2 Flow

1. The principal indicates consent to federate his identity.
2. The identity provider generates a name identifier for the new identity federation, and records it for future use.

3. The identity provider issues an assertion to the principal to communicate the federated name identifier to the service provider.

4. The service provider authenticates the principal and establishes the identity federation by linking the name identifier to its local account identitier for the principal.

4.2.3 Postconditions

1. The service provider and identity provider share a common name identifier for the principal, linked to each provider's local identifier for him.

4.3 Provider Requests a Name Identifier Change

4.3.1 Preconditions

1. The principal has an identity federation between a pair of providers.

2. One of the providers wishes to change the name identifier by which the other provider will communicate to it about the principal, such as during single sign-on.

4.3.2 Flow

1. The requesting provider generates a new name identifier and sends it with the original identifier to the other provider, registering it as the new value.

2. The receiving provider acknowledges the change.

4.3.3 Postconditions

1. The receiving provider has a new name identifier to use when communicating with the requesting provider about the principal, and will no longer use the old one.

4.4 Provider Terminates an Identity Federation

4.4.1 Preconditions

1. The principal has an identity federation between a pair of providers.

2. One of the providers wishes to terminate the federation, possibly because the principal has severed his relationship with it.

4.4.2 Flow

1. The terminating provider sends a notification of termination to the other provider.

2. The receiving provider acknowledges the termination.

4.4.3 Postconditions

241 1. The principal no longer has an identity federation between the providers.

242 4.5 Service Providers Communicate without Identity Federation

243 4.5.1 Preconditions

244 1. A service provider wants to communicate with another service provider regarding the principal,
245 for example to obtain attributes.

246 2. No identity federation for the principal exists between the service providers.

247 3. An identity provider shares an identity federation for the principal with both service providers.

248 4. The principal's and/or identity provider's policy dictates that a name identifier may be given to
249 the requesting service provider, but only in protected and time-limited fashion.

250 4.5.2 Flow

251 1. The requesting service provider asks the identity provider for the name identifier of the
252 principal in the context or namespace of the second service provider.

253 2. The identity provider encrypts the name identifier it shares with the second service provider,
254 such that only the second service provider can understand it, and returns it to the requester.

255 3. The requesting service provider uses the encrypted name identifier in its message to the
256 second service provider, as if an identity federation existed between them.

257 4. The receiving service provider decrypts the encrypted name identifier and fulfills the request
258 subject to appropriate policy.

259 4.5.3 Postconditions

260 1. The encrypted name identifier expires at some point such that it can no longer be used in
261 subsequent requests.

5 Candidate Mechanisms

The main limitation on name identifiers in SAML 1.1 is that they are placed in a simple string-valued element. The requirements laid out in this document can be met by a combination of new Format-based "profiles" on content and usage, new protocols to address identifier and federation management, and an enhanced schema for complex content in name identifiers to address advanced requirements such as encryption.

5.1 Revision to <NameIdentifier> Element

The following text and schema is proposed to replace [SAMLCore] §2.4.2.2:

The `<BaseNameIdentifier>` element serves as an extension point for new types of identifiers. Its **BaseNameIdentifierType** complex type is abstract; extension elements must use the `xsi:type` attribute to indicate the derived type, or be substitutable for this element. The following common attributes are defined for all name identifiers:

`NameQualifier` [Optional]
: The security or administrative domain that qualifies the name identifier of the subject. This attribute provides a means to federate names from disparate user stores without collision.

`SPNameQualifier` [Optional]
: Further qualifies a federated name identifier with the name of the service provider or affiliation of providers which has federated the principal's identity.

`NotBefore` [Optional]
: The date and time at which the name identifier becomes usable for referring to the subject. Generally used when encrypting the resulting element to indicate the time at which the encryption was performed, so that decrypting parties may enforce time-sensitive policies on use.

`NotOnOrAfter` [Optional]
: Indicates the time at which the identifier should no longer be used to refer to the subject. Generally used with encrypted or transient identifiers.

The `NotBefore` and `NotOnOrAfter` attributes do not impact or interact with the validity of an assertion whose subject contains a name identifier decorated with them. Rather, they represent the validity of the binding of the name identifier to the subject of the assertion.

The following schema fragment defines the `<BaseNameIdentifier>` element and its **BaseNameIdentifierType** complex type:

```
<element name="BaseNameIdentifier" type="saml:BaseNameIdentifierType"/>
<complexType name="BaseNameIdentifierType" abstract="true">
    <complexContent>
        <extension base="anyType">
            <attribute name="NameQualifier" type="string" use="optional"/>
            <attribute name="SPNameQualifier" type="string" use="optional"/>
            <attribute name="NotBefore" type="dateTime" use="optional"/>
            <attribute name="NotOnOrAfter" type="dateTime" use="optional"/>
       </extension>
    </complexContent>
</complexType>
```

The following text and schema is proposed for insertion into [SAMLCore] as §2.4.2.3:

The <NameIdentifier> element restricts a <BaseNameIdentifier> to simple string content in naming the subject. The <NameIdentifier> element contains the following defined additional attributes:

Format [Optional]
A URI reference representing the classification of string-based identifier information. See Section 7.3 for some URI references that MAY be used as the value of the Format attribute, and associated descriptions of the content, and processing rules. If the Format attribute is not included, the identifier urn:oasis:names:tc:SAML:1.0:nameid-format:unspecified (see Section 7.3.1) is in effect. If not otherwise specified by the format, issues of anonymity, pseudonymity, and the persistence of the identifier with respect to the asserting and relying parties are implementation-specific.

SPProvidedIdentifier [Optional]
The name identifier established by the service provider or affiliation of providers for the principal, if different from the primary identifier in the element content.

The following schema fragment defines the <NameIdentifier> element and its **NameIdentifierType** complex type:

```
<element name="NameIdentifier" type="saml:NameIdentifierType"
substitutionGroup="saml:BaseNameIdentifier"/>
<complexType name="NameIdentifierType" mixed="false">
    <simpleContent>
        <restriction base="saml:BaseNameIdentifierType">
            <simpleType>
                <restriction base="string"/>
            </simpleType>
            <attribute name="Format" type="anyURI" use="optional"/>
            <attribute name="SPProvidedIdentifier" type="string"
use="optional"/>
        </restriction>
    </simpleContent>
</complexType>
```

The following text and schema is proposed for insertion into [SAMLCore] as §2.4.2.4:

The <EncryptedNameIdentifier> element extends a <BaseNameIdentifier> such that it carries the content in encrypted fashion, as defined by **[XMLEnc]**. The <EncryptedNameIdentifier> element contains the following defined additional elements and attributes:

<xenc:EncryptedData> [Required]
The encrypted content and associated encryption details, as defined by **[XMLEnc]**. The encrypted content MUST be a <BaseNameIdentifier> element or a derivation of it.

<xenc:EncryptedKey> [Optional]
A wrapped decryption key, as defined by **[XMLEnc]**.

Encrypted identifiers are intended as a privacy protection when the plaintext value passes through an intermediary ; as such the ciphertext MUST be unique to any given encryption operation. For more on such issues, see **[XMLEnc] §6.3**.

The following schema fragment defines the <EncryptedNameIdentifier> element and its **EncryptedNameIdentifierType** complex type:

```
<element name="EncryptedNameIdentifier" type="saml:EncryptedNameIdentifierType"
substitutionGroup="saml:BaseNameIdentifier"/>
    <complexType name="EncryptedNameIdentifierType" mixed="false">
        <complexContent>
            <restriction base="saml:BaseNameIdentifierType">
                <sequence>
                    <element ref="xenc:EncryptedData"/>
                    <element ref="xenc:EncryptedKey" minOccurs="0"/>
                </sequence>
            </restriction>
    </complexContent>
</complexType>
```

5.2 Revision to Format Identifiers

The following text is proposed to replace [SAMLCore] §7.3:

The following identifiers MAY be used in the Format attribute of the `<NameIdentifier>` element (see Section 2.4.2.3) to refer to common formats for the content of the element and the associated processing rules, if any.

7.3.1 Unspecified

URI: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

The interpretation of the content of the element is left to individual implementations.

7.3.2 Email Address

URI: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Indicates that the content of the element is in the form of an email address, specifically "addr-spec" as defined in IETF RFC 2822 **[RFC 2822]** §3.4.1. An addr-spec has the form local-part@domain. Note that an addr-spec has no phrase (such as a common name) before it, has no comment (text surrounded in parentheses) after it, and is not surrounded by "<" and ">".

7.3.3 X.509 Subject Name

URI: urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName

Indicates that the content of the element is in the form specified for the contents of the `<ds:X509SubjectName>` element in the XML Signature Recommendation **[XMLSig]**. Implementers should note that the XML Signature specification specifies encoding rules for X.509 subject names that differ from the rules given in IETF RFC 2253 **[RFC 2253]**.

7.3.4 Windows Domain Qualified Name

URI: urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName

Indicates that the content of the element is a Windows domain qualified name. A Windows domain-qualified username is a string of the form "DomainName\UserName". The domain name and "\" separator MAY be omitted.

7.3.5 Provider Identifier

URI: urn:oasis:names:tc:SAML:2.0:nameid-format:provider

Indicates that the content of the element is the identifier of a provider of SAML-based services (such as a SAML authority) or a participant in SAML profiles (such as a service provider supporting the browser profiles). Such an identifier can be used to make assertions about system entities that can issue SAML requests, responses, and assertions.

7.3.6 Federated Identifier

URI: urn:oasis:names:tc:SAML:2.0:nameid-format:federated

Indicates that the content of the element is a persistent opaque identifier that corresponds to an identity federation between an identity provider and a service provider (or affiliation of service providers). Federated name identifiers generated by identity providers MUST be constructed using pseudo-random values that have no discernible correspondence with the subject's actual identifier (e.g., username). The intent is to create a non-public pseudonym to prevent the discovery of the subject's identity or activities. Federated name identifier values MUST NOT exceed a length of 256 characters.

The element's content MUST contain the most recent identifier of the subject set by the identity provider.

The element's `NameQualifier` attribute, if present, MUST contain the name of the identity provider participating in the identity federation. It MAY be omitted if the value can be derived from the context of the message containing the element, such as the issuer of an assertion.

The element's `SPNameQualifier` attribute, if present, MUST contain the name of the service provider or affiliation of providers participating in the identity federation. It MAY be omitted if the element is contained in a message intended only for consumption directly by the service provider, and the value would be the name of that service provider.

The element's `SPProvidedIdentifier` attribute MUST contain the alternative identifier of the subject most recently set by the service provider or affiliation, if any. If no such identifier has been established, than the attribute MUST be omitted.

Federated identifiers are intended as a privacy protection; as such they MUST NOT be shared in cleartext with providers other than the providers that have established the identity federation. Furthermore, they MUST NOT appear in log files or similar locations without appropriate controls and protections. Deployments without such requirements are free to use other kinds of identifiers in their SAML exchanges.

7.3.7 Transient Identifier

URI: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Indicates that the content of the element is an identifier with transient semantics and SHOULD be treated as an opaque and temporary value by the relying party. Transient identifier values MUST be generated in accordance with the rules for SAML identifiers (see Section 1.2.3), and MUST NOT exceed a length of 256 characters.

The `NameQualifier` and `SPNameQualifier` attributes MAY be used to signify that the identifier represents a transient and temporary identity federation, as described in **§7.3.6**. In such a case, they MAY be omitted in accordance with the rules specified in that section.

5.3 Revision to Existing Base Types

It is suggested that an optional `Issuer` attribute be added to both the `RequestAbstractType` and `ResponseAbstractType` types. This addition facilitates the identification of a message sender such that associated metadata about the sender can be easily referenced.

Alternatively, other use cases have suggested that a more complex identifier structure be used to represent issuers. Replacing the existing `Issuer` attribute with an `Issuer` element of `NameIdentifierType` would meet this use case.

5.4 Proposed Protocol and Schema for Identifier Management

It is suggested that [LibPS] **§3.3** be adopted for federated name identifier management in SAML, with the following general modifications:

- The `<ProviderID>` element is superfluous given the suggestion to add an `Issuer` attribute to the base request and response types.
- Using the related proposals in this document, it should be possible to consolidate the three elements in the Liberty request message to a pair, the old identifier and a new one.

5.5 Proposed Protocol and Schema for Federation Termination

It is suggested that [LibPS] **§3.4** be adopted for federated name identifier management in SAML, with the following general modifications:

- The `<ProviderID>` element is superfluous given the suggestion to add an `Issuer` attribute to the base request type.

6 References

[LibBP] Liberty Alliance Project, *Liberty ID-FF Bindings and Profiles Specification,* August 2003.

[LibPS] Liberty Alliance Project, *Liberty ID-FF Protocols and Schema Specification,* August 2003.

[LibGloss] Liberty Alliance Project, *Liberty Architecture Glossary*, August 2003.

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[SAMLCore] E. Maler, et al., *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)*, available from http://www.oasis-open.org/committees/security, OASIS, May 2003.

[SAMLBind] E. Maler, et al., *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)*, available from http://www.oasis-open.org/committees/security, OASIS, May 2003.

[SAMLSecure] E. Maler, et al., *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML),* OASIS, July 2003.

[XMLEnc] D. Eastlake et al., *XML Encryption Syntax and Processing*, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/, World Wide Web Consortium.

Appendix A.Revision History

Rev	Date	By Whom	What
wd-00	2003-08-25	John Linn	Initial candidate requirements.
wd-02	2003-09-24	Scott Cantor	Added some use cases and proposals.
wd-03	2003-10-12	Scott Cantor	Added text for new federation-related protocols.
wd-04	2003-10-22	Scott Cantor	Adjusted proposal on federated identifiers to reflect feedback.
wd-05	2003-10-27	Scott Cantor	Adjusted name of schema types, added glossary.
wd-07	2003-12-15	Scott Cantor	Glossary adjustments

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.