Liberty ID-WSF Security Mechanisms
Version: 1.0

Editors:
Gary Ellison, Sun Microsystems, Inc.

Contributors:
Robert Aarts, Nokia
Carolina Canales, Ericsson
Scott Cantor, The Ohio State University/Internet2
Frederick Hirsch, Nokia
Jeff Hodges, Sun Microsystems, Inc.
John Kemp, Liberty Alliance
John Linn, RSA Laboratories
Paul Madsen, Entrust
Jonathan Sergent, Sun Microsystems, Inc.
Greg Whitehead, Trustgenix

Abstract:
Specification from the Liberty Alliance Project Identity Web Services Framework for describing security mechanisms for authentication and authorization.

Filename: liberty-idwsf-security-mechanisms-v1.0.pdf
Notice

Copyright © 2003 America Online, Inc.; American Express Travel Related Services; Bank of America; Bell Canada;
Cingular Wireless; Cisco Systems, Inc.; Communicator, Inc.; Deloitte & Touche LLP; Earthlink, Inc.; Electronic
Data Systems, Inc.; Entrust, Inc.; Ericsson; Fidelity Investments; France Telecom; Gemplus; General Motors;
Hewlett-Packard Company; i2 Technologies, Inc.; Intuit Inc.; MasterCard International; NEC Corporation; Netegrity;
NeuStar; Nextel Communications; Nippon Telegraph and Telephone Corporation; Nokia Corporation; Novell, Inc.;
NTT DoCoMo, Inc.; OneName Corporation; Openwave Systems Inc.; PricewaterhouseCoopers LLP; Register.com;
Royal Mail; RSA Security Inc; Sabre Holdings Corporation; SAP AG; SchlumbergerSema; SK Telecom; Sony
Corporation; Sun Microsystems, Inc.; Symlabs, Inc.; Trustgenix; United Airlines; VeriSign, Inc.; Visa International;
Vodafone Group Plc; Wave Systems;. All rights reserved.

This specification document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to
use the document solely for the purpose of implementing the Specification. No rights are granted to prepare
derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other
uses must contact the Liberty Alliance to determine whether an appropriate license for such use is available.

Implementation of certain elements of this Specification may require licenses under third party intellectual property
rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are
not, and shall not be held responsible in any manner, for identifying or failing to identify any or all such third party
intellectual property rights. This Specification is provided "AS IS", and no participant in the Liberty Alliance
makes any warranty of any kind, express or implied, including any implied warranties of merchantability,
non-infringement of third party intellectual property rights, and fitness for a particular purpose. Implementors
of this Specification are advised to review the Liberty Alliance Project’s website (http://www.projectliberty.org/) for
information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance
Management Board.

Liberty Alliance Project
Licensing Administrator
c/o IEEE-ISTO
445 Hoes Lane
Piscataway, NJ 08855-1331, USA
info@projectliberty.org
# Contents

1. Abstract ................................................................. 4
2. Overview of Identity-Based Web Services Authorization (Informative) ............................................................................. 5
3. Notation and Terminology .................................................................................................................................. 6
4. Security Requirements (Informative) ......................................................................................................................... 8
5. Message Confidentiality and Privacy Mechanisms ..................................................................................................... 11
6. Authentication Mechanisms ..................................................................................................................................... 13
7. Supporting Schema ..................................................................................................................................................... 21
8. Message Authorization Model ................................................................................................................................ 25
9. Identity-Based Web Service Examples (Informative) ................................................................................................. 29
10. XSD ................................................................................................................................................................. 37
Bibliography ................................................................................................................................................................. 40
1. Abstract

This document specifies security protocol mechanisms for securing the consumption of identity-based web services. An identity-based web service is a particular type of a web service that acts upon some resource to either retrieve information about an identity, update information about an identity, or perform some action for the benefit of some identity. This document describes authentication mechanisms which are factored into the authorization decisions enforced by a given identity-based web service. The specified mechanisms provide for authentication, signing and encryption operations. XML-Signature ([XMLDsig]) and XML-Encryption ([xmlenc-core]) are utilized to provide the associated transformations and processing semantics to accommodate the message authentication and protection functionality. OASIS WS-Security ([wss-sms]) compliant header elements communicate the relevant security information, i.e., a SAML ([SAMLCore11]) assertion, along with the protected message.
2. Overview of Identity-Based Web Services Authorization (Informative)

This section provides a perspective of some of the authorization obligations an identity-based web service may assume.

An identity-based web service is a particular type of a web service that acts upon some resource to either retrieve information about an identity, update information related to an identity, or perform some action for the benefit of some identity. A resource is either data related to some identity or a service acting for the benefit of some identity.

Identity-based web services may be accessed by system entities. The access may be direct or with the assistance of an intermediary. To access an identity-based web service a system entity must interact with a specific service instance which exposes some resource.

Given the above description, we strongly believe that access control policies must be enforced by identity-based web services. The authorization decision to access an identity-based web service instance offering a specific resource may be made locally (that is at the entity hosting the resource) or remotely. Regardless of whether the policy decision point (PDP) is distributed or not a policy enforcement point (PEP) will likely be implemented by the entity hosting or exposing the resource.

In most cases, the service requester directly interacts with the identity-based web service, thus the identity-based web service may implement both the PEP and the PDP. Under these circumstances the authorization decision, at a minimum, should be based on the authenticated identity of the service requester and the resource for which access is being requested.

However, an identity-based web service may rely upon a trusted third party (TTP) to make coarse policy decisions. It is also likely that the TTP will act as a Policy Information Point (PIP) such that it can convey information regarding the resource and the policy it maintains. This scenario might be deployed in the event that the principal is unable to actively authenticate to the identity-based web service. One such scenario is where a TTP provides a bridge function to introduce new participants to the identity service. The result of any such policy decision made by the TTP must be presented to the entity hosting the identity-based web service. Of course this does not preclude the identity-based web service from making additional policy decisions based on other criteria.

Our definition of an identity-based web service mentioned the notion of the service performing an action for the benefit of an identity. To fully appreciate the possibilities this notion suggests one must recognize scenarios whereby peer entities may need to represent or perform actions on behalf of other system entities. It may also be the case that the identity-based web service must consider the status of the resource owner for a given request to access a resource.

To support the case where an intermediary accesses a resource on behalf of another system entity, the identity-based web service may rely upon a TTP to make policy decisions and issue statements which allow the service requester to act on behalf of a different system entity.
3. Notation and Terminology

This section specifies the notations, namespaces and and terminology used throughout this specification. This specification uses schema documents conforming to W3C XML Schema (see [Schema1]) and normative text to describe the syntax and semantics of XML-encoded messages.

3.1. Notational Conventions

Note: Phrases and numbers in brackets [ ] refer to other documents; details of these references can be found in Section 3 (at the end of this document).

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

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.

3.2. Namespace

The following namespaces are referred to in this document:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Namespace</th>
</tr>
</thead>
<tbody>
<tr>
<td>sec</td>
<td>urn:liberty:sec:2003-08</td>
</tr>
<tr>
<td>sb</td>
<td>urn:liberty:soap-bind:2003-05</td>
</tr>
<tr>
<td>disco</td>
<td>urn:liberty:disco:2003-08</td>
</tr>
<tr>
<td>ac</td>
<td>urn:liberty:ac:2003-08</td>
</tr>
<tr>
<td>lib</td>
<td>urn:liberty:iff:2003-08</td>
</tr>
<tr>
<td>md</td>
<td>urn:liberty:metadata:2003-08</td>
</tr>
<tr>
<td>saml</td>
<td>urn:oasis:names:tc:SAML:1.0:assertion</td>
</tr>
<tr>
<td>S</td>
<td><a href="http://www.w3.org/2002/12/soap-envelope">http://www.w3.org/2002/12/soap-envelope</a></td>
</tr>
<tr>
<td>ds</td>
<td><a href="http://www.w3.org/2000/09/xmldsig#">http://www.w3.org/2000/09/xmldsig#</a></td>
</tr>
<tr>
<td>xenc</td>
<td><a href="http://www.w3.org/2001/04/xmlenc#">http://www.w3.org/2001/04/xmlenc#</a></td>
</tr>
<tr>
<td>wsse:</td>
<td><a href="http://schemas.xmlsoap.org/ws/2003/06/secext">http://schemas.xmlsoap.org/ws/2003/06/secext</a></td>
</tr>
<tr>
<td>xs</td>
<td><a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a></td>
</tr>
<tr>
<td>xsi</td>
<td><a href="http://www.w3.org/2001/XMLSchema-instance">http://www.w3.org/2001/XMLSchema-instance</a></td>
</tr>
</tbody>
</table>

This specification uses the following typographical conventions in text: <Element>, <ns:ForeignElement>, Attribute, Datatype, OtherCode.

For readability, when an XML Schema type is specified to be xs:boolean, this document discusses the values as true and false rather than "1" and "0".

3.3. Terminology

Definitions for Liberty-specific terms can be found in [LibertyGloss].

The following terms are defined below as an aid in understanding the participants in the message exchanges:

- Recipient – entity which receives a message that is the ultimate processor of the message
- Sender – the initial SOAP sender. A sender is a proxy when its identity differs from the invocation identity.
• Proxy – entity whose authenticated identity, according to the recipient, differs from that of the entity making the invocation.

• Trusted Authority – a Trusted Third Party (TTP) which issues and vouches for SAML assertions

• Invocation Identity – party invoking a service.

• Service – invocation responder, providing a service. Ultimate message processor.
4. Security Requirements (Informative)

This section details the security requirements which this specification must support. This section first presents an use case scenarios envisioned for identity-based web services. We then followup the discussion with the requirements the usage scenarios prescribe.

4.1. Security Requirements Overview

There are multiple facets this security specification considers:

- Authentication of the sender
- When the sender is not the invocation identity, the proxy rights for sender to make a request on behalf of invocation identity
- Authentication of the response
- Authentication context and session status of the interacting entity
- Authorization of invocation identity to access service or resource

Note that the authorization mechanism draws a distinction between the invocation identity and the identity of the initial SOAP sender making a request to the identity web service. These two identities are referred to as the invocation identity and the sender identity, respectively. In effect, this enables a constrained proxy authorization model.

The importance of the distinction between invocation and sender identity lies in the service’s access control policies whereby the service’s decision to grant or deny access may be based on either or both identities. The degenerate case is where the invocation identity is the same as the sender identity, in which case no distinction need be made.

Note that a browser-based user agent interacting with some service provider does not necessarily imply that the service provider will use the user identity as the invocation identity. In some cases, the identity of the service provider may still be used for invocation.

The above scenarios suggest a number of requirements in order to secure the exchange of information between participants of the protocol. The following list summarizes the security requirements:

- Request Authentication
- Response Authentication
- Request/Response Correlation
- Replay Protection
- Integrity Protection
- Confidentiality Protection
- Privacy Protections
- Resource Access Authorization
- Proxy Authorization
- Mitigation of denial of service attack risks
4.2. Common Requirements

The following apply to all mechanisms in this specification, unless specifically noted by the individual mechanism.

- Messages may need to be kept confidential and inhibit unauthorized disclosure, either when in transit or when stored persistently. Confidentiality may apply to the entire message, selected headers, payload, or XML portions depending on application requirements.
- Messages need to arrive at the intended recipient with data integrity. SOAP intermediaries may be authorized to make changes, but no unauthorized changes should be possible without detection. Integrity requirements may apply to the entire message, selected headers, payload, or XML portions depending on application requirements.
- The authentication of a message sender and/or initial sender may be required by a receiver to process the message. Likewise, a sender may require authentication of the response.
- Message responses must correspond to message requests and attempts to replay requests or responses should be detected. Likewise the attempt to substitute requests or responses should be detected. Transaction integrity requires that messages be timely and related to each other.
- The privacy requirements of the participants with respect to how their information is shared or correlated must be ensured.

4.3. Peer Authentication Requirements

The security mechanisms supported by this framework must allow for active and passive intermediaries to participate in the message exchange between end entities. In some circumstances it is necessary to authenticate all active participants in a message exchange.

Under certain conditions, two separate identities must be authenticated for a given request: the invocation identity and the sender identity. The degenerate case is where the identity of the message sender is to be treated as the invocation identity, and thus, no distinction between invocation identity and sender identity is required. In support of this scenario the candidate mechanism to convey identity information is client-side X.509 v3 certificates based authentication over a SSL 3.0 (see [SSL]) or TLS 1.0 (see [RFC2246]) connection. Generally, this protocol framework may rely upon the authentication mechanism of the underlying transfer or transport protocol binding to convey the identity of the communicating peers.

However for scenarios where the senders messages are passing through one or more intermediaries, the sender must explicitly convey its identity to the recipient by using a WSSec token profile which specifies processing semantics in support of Proof-of-Possession. For example, the Web Services Security SAML Token Binding defines Proof-of-Possession processing semantics. Other possible bindings include Kerberos whereby the session key is used to sign the request.

4.4. Message Correlation Requirements

The messages exchanged between participants of the protocol MAY require assurance that a response correlates to its request.

4.5. Privacy Requirements

Adequate privacy protections must be assured so as to inhibit the unauthorized disclosure of personally identifiable information. In addition, controls must be established so that personally identifiable information is not shared without user notification and consent and that where applicable privacy regulations may be accommodated. This may require prescriptive steps to prevent collusion among participants in an identity network.
4.6. Service Availability

The system must maintain availability, requiring the implementation of techniques to prevent or reduce the risk of attacks to deny or degrade service.

4.7. Resource Access Authorization Requirements

Previously we mentioned the notion of conveying both a *sender identity* and an *invocation identity*. In doing so the framework accommodates a restricted proxy capability whereby a consumer of an identity-based web service (the intermediate system entity or proxy) can act on behalf of another system entity (the subject) to access an identity-based web service (the recipient.) To be granted the right to proxy for a subject, the intermediate system entity may need to interact with a trusted authority. Based on the authority’s access control policies, the authority may generate and distribute an assertion authorizing the intermediary to act on behalf of the subject to the recipient. This protocol framework can only convey authoritative information regarding the identities communicated to other system entities. Even with the involvement of a trusted authority acting as a proxy authorization policy decision point, the recipient must still implement some degree of policy decisions and enforcement.
5. Message Confidentiality and Privacy Mechanisms

Some of the service interactions described in this specification include the conveyance of information that is only known by a trusted authority and the eventual recipient of a resource access request. This section specifies the schema and measures to be employed to attain the necessary confidentiality controls.

5.1. Transport Layer Channel Protection

When communicating peers interact directly (i.e. no active intermediaries in the message path) then transport layer protection mechanisms may suffice to ensure the integrity and confidentiality of the message exchange. However, this mechanism may not fully address the privacy and confidentiality requirements of information supplied by a trusted authority. For example the authorization data may contain sensitive information. To accommodate this requirement the trusted authority and ultimate recipient MUST rely upon the mechanisms specified in Encrypted Name Identifiers [Section 5.3.1] and in Encrypted URI [Section 5.3.2].

- Messages between sender and recipient MUST have their integrity protected and confidentiality MUST be ensured. This requirement MUST be met with suitable SSL/TLS cipher suites. The security of the SSL or TLS session depends on the chosen cipher suite. An entity that terminates an SSL or TLS connection needs to offer (or accept) suitable cipher suites during the handshake. The following list of TLS 1.0 cipher suites (or their SSL 3.0 equivalent) is RECOMMENDED.

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA

The above list is not exhaustive. The recommended cipher suites are among the most commonly used. New cipher suites using the Advanced Encryption Standard have been standardized by the IETF [RFC3268] and are just beginning to appear in TLS implementations. It is anticipated that these AES-based cipher suites will be widely adopted and deployed.

- TLS_RSA_WITH_AES_CBC_SHA
- TLS_DHE_DSS_WITH_AES_CBC_SHA

For signing and verification of protocol messages, communicating entities SHOULD use certificates and private keys that are distinct from the certificates and private keys applied for SSL or TLS channel protection.

- Other security protocols (e.g. Kerberos, IPSEC) MAY be used as long as they implement equivalent security measures.
5.2. Message Confidentiality Protection

In the presence of intermediaries, communicating peers MUST ensure that sensitive information is not disclosed to unauthorized entities. To fulfill this requirement, peers MUST use the confidentiality mechanisms specified in [wss-sms] to encrypt the child elements of the <S:Body>.

Please note that this mechanism does not fully address the privacy and confidentiality requirements of information supplied by a trusted authority which is subsequently carried in the <S:Header> which is not to be revealed to the entity interacting with the recipient. For example the authorization data may contain sensitive information. To accommodate this requirement the trusted authority and ultimate recipient MUST rely upon the mechanisms specified in Encrypted Name Identifiers [Section 5.3.1] and in Encrypted URI [Section 5.3.2] SHOULD be used.

5.3. Identifier Privacy Protection

Under certain usage scenarios the information conveyed by the Trusted Authority for consumption by the identity-based web service may contain privacy sensitive data. However, this data generally passes through the system entity accessing the particular identity-based web service. One example is the name identifier from the federated namespace of the authority and the identity-based web service. Another sensitive data item may be the URI which has some association with the identity-based web service and the principal on whose behalf the sender is acting.

5.3.1. Encrypted Name Identifiers

The identity conveyed in the subject must be resolvable in the namespace of the consuming service instance. However, this requirement is in conflict with the need to protect the privacy of the identifier when the message passes through intermediaries. To accomplish this securely the <saml:Subject> MUST contain a <saml:NameIdentifier> following the processing rules in the NameIdentifier Encryption Profile specified in [LibertyBindProf].

5.3.2. Encrypted URI

At times it may be necessary to privacy protect the contents of a URI to deter the release of sensitive information to an intermediary. The [[LibertyDisco]] specification defines an encrypted form of a URI with the <disco:EncryptedResourceID> schema element. This specification relies upon the semantics defined in [[LibertyDisco]] to fulfill this privacy requirement. Thus the processing rules defined by [[LibertyDisco]] for the <disco:EncryptedResourceID> element MUST be followed.
6. Authentication Mechanisms

This specification defines a set of authentication mechanisms, their URIs, and the security properties they engender. The multiplicity of mechanisms specified is necessary to accommodate various deployment scenarios. Each identifier qualifies two security properties of the given mechanism:

- Peer Entity Authentication
- Message Authentication

For either of the properties a value of "null" indicates that the particular security property is not supported by the mechanism. For the peer entity authentication property, the qualifier indicates which actor(s) is authenticated in a given interaction. For the message authentication property the qualifier describes the security profile utilized to secure the message.

The following table summarizes the authentication mechanism identifiers and their security properties. Each URI is of the form urn:liberty:security:2003-08:peer mechanism:message mechanism.

<table>
<thead>
<tr>
<th>URI</th>
<th>Peer Entity</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:liberty:security:2003-08:null:null</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>urn:liberty:security:2003-08:null:X509</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>urn:liberty:security:2003-08:null:SAML</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>urn:liberty:security:2003-08:TLS:null</td>
<td>Recipient</td>
<td>No</td>
</tr>
<tr>
<td>urn:liberty:security:2003-08:TLS:X509</td>
<td>Recipient</td>
<td>Yes</td>
</tr>
<tr>
<td>urn:liberty:security:2003-08:TLS:SAML</td>
<td>Recipient</td>
<td>Yes</td>
</tr>
<tr>
<td>urn:liberty:security:2003-08:ClientTLS:null</td>
<td>Mutual</td>
<td>No</td>
</tr>
<tr>
<td>urn:liberty:security:2003-08:ClientTLS:X509</td>
<td>Mutual</td>
<td>Yes</td>
</tr>
<tr>
<td>urn:liberty:security:2003-08:ClientTLS:SAML</td>
<td>Mutual</td>
<td>Yes</td>
</tr>
</tbody>
</table>

6.1. Authentication Mechanism Overview (Informative)

The above table depicts the various authentication mechanism identifiers and the security properties they exhibit. A description of the setting in which a particular mechanism should be deployed is out of scope for this specification. However, this section describes the characteristics of the class of mechanism and general circumstances whereby the deployment of a given mechanism may be appropriate.

The identifier, urn:liberty:security:2003-08:null:null, does not exhibit any security properties and is basically defined here for completeness. However one can envision a deployment setting in which access to a resource does not require rigor in authenticating the entities involved in an interaction. For example, a weather reporting service.

The peer entity authentication mechanisms defined by this specification leverage the authentication features supplied by SSL 3.0 [[SSL]] or TLS 1.0 [[RFC2246]]. The mechanism identifier describes whether the recipient ("TLS") is unilaterally authenticated or whether each communicating peer ("ClientTLS") is mutually authenticated to the other peer. The peer entity authentication mechanisms [Section 6.2] are best suited for direct message exchanges between end systems and when the message exchange may be sufficiently trusted to not require additional attestation of the message payload. However this does not obviate the processing of subject confirmation obligations but rather enables alternative and potentially optimized processing rules. Such optimizations are a matter of security policy as it applies to the trust model in place between communicating entities.

The message authentication mechanisms indicate which attestation profile is utilized to ensure the authenticity of a message. The message level facilities aid the deployer in the presence of intermediaries. The X.509 v3 Certificate mechanism [Section 6.3.1] is suited for message exchanges which generally rely upon message authentication as the principle factor in making authorization decisions. The SAML Assertion mechanism [Section 6.3.2] is suited for
message exchanges which generally rely upon message authentication as well as the conveyance and attestation of authorization information.

Not all peer entity authentication and message authentication combinations make sense in a given setting. Again this is a matter of security policy and the trust model the policy accords. For example, in a conventional setting where peer entity authentication is relied upon to ensure the authenticity, confidentiality and integrity of the transport in combination with message authentication to assure message authorship, intent and retention of the act of attestation then the mechanism urn:liberty:security:2003-08:ClientTLS:X509 is relevant. However, such a combination may make little sense when peer entity authentication is relied upon to imply message authentication. For example, the mechanism urn:liberty:security:2003-08:ClientTLS:X509 seems equivalent to urn:liberty:security:2003-08:ClientTLS:null in such a setting. A similar argument can be made for the urn:liberty:security:2003-08:ClientTLS:SAML mechanism.

6.2. Peer Entity Authentication

The Peer entity authentication mechanisms prescribed by this specification rely upon the inherent security properties of the TLS/SSL protocol (sometimes referred to as transport-level security). The mechanisms described below have distinct security properties regarding which peers in a message exchange are authenticated. For the mechanisms which include both peer entity authentication and message authentication, optimizations regarding attestation MAY be employed. For example, in environments where the signature attesting to the authenticity of the message need not be retained, then it may be sufficient to rely upon the security properties of peer entity authentication to assure the integrity and authenticity of the message payload.

6.2.1. Unilateral Peer Entity Authentication

The following URIs support unilateral (recipient) peer entity authentication:

- urn:liberty:security:2003-08:TLS:null
- urn:liberty:security:2003-08:TLS:X509

The primary function of these mechanisms is to provide for the authentication of the receiving entity and to leverage confidentiality and integrity features at the transport layer.

The latter two mechanisms MAY be used in conjunction with message authentication mechanisms defined by this specification.

6.2.1.1. Processing Rules

These mechanisms MUST implement TLS/SSL end entity authentication in accordance with the TLS/SSL specifications and employing a cipher suite based on X.509 certificates, requiring the following:

- The sender MUST authenticate the recipient.
- The recipient MUST authenticate using X.509 v3 certificates by demonstrating possession of the key bound by its certificate in accordance with the processing rules and semantics of the TLS/SSL protocol.
6.2.2. Mutual Peer Entity Authentication

The following URIs support mutual (sender and recipient) peer entity authentication:

- urn:liberty:security:2003-08:ClientTLS:null
- urn:liberty:security:2003-08:ClientTLS:X509
- urn:liberty:security:2003-08:ClientTLS:SAML

The primary function of these mechanisms is to provide for the mutual authentication of the communicating peers and to leverage confidentiality and integrity features at the transport layer.

The latter two URIs indicate that the mechanism may be used in conjunction with message authentication mechanisms defined by this specification.

6.2.2.1. Processing Rules

These mechanisms MUST implement TLS/SSL end entity authentication in accordance with the TLS/SSL specifications and employing a cipher suite based on X.509 certificates, requiring the following:

- The sender MUST authenticate the recipient AND the recipient MUST authenticate the sender.
- The recipient MUST authenticate using X.509 v3 certificates by demonstrating possession of the key bound by its certificate in accordance with the processing rules and semantics of the TLS/SSL protocol.
- The sender MUST authenticate using X.509 v3 certificates by demonstrating possession of the key bound by its certificate in accordance with the processing rules and semantics of the TLS/SSL protocol.

6.3. Message Authentication

The message authentication mechanisms prescribed by this specification rely upon the integrity properties imbued by the application and verification of digital signatures over elements of the message payload. The mechanisms described below have distinct security properties regarding authenticity of a given message. For the mechanisms which include both peer entity authentication and message authentication, optimizations regarding attestation MAY be employed. For example, in environments where the signature attesting to the authenticity of the message need not be retained, then it may be sufficient to rely upon the properties of peer entity authentication to assure the integrity and authenticity of the message payload. Another example might be when unilateral peer entity authentication of the recipient can be combined with message authentication of the sender such that the response could be deemed trustworthy in the absence of a signature over the payload of said response.

6.3.1. X.509 v3 Certificate Message Authentication

The following URIs define X.509 based unilateral (sender) message authentication mechanisms:

- urn:liberty:security:2003-08:TLS:X509
- urn:liberty:security:2003-08:ClientTLS:X509
These mechanisms utilize the Web Services Security X.509 Certificate Token Profile [wss-x509] as the means by which the message sender authenticates to the recipient. These message authentication mechanisms are unilateral. That is only the author of the message is authenticated. It is not in the scope of this specification to suggest when response messages should be authenticated but it is worth noting that this mechanism could be relied upon to authenticate the response message as well. Deployers should recognize, however, that independent authentication of response messages does not provide the same message stream protection semantics as a mutual peer entity authentication mechanism would offer.

For deployment settings which require independent message authentication then the sending peer MUST perform message authentication by demonstrating proof of possession of a subject confirmation key. This key MUST be recognized by the recipient as belonging to the sending peer.

When the sender wields the subject confirmation key to sign elements of the message the signature ensures the authenticity and integrity of the elements covered by the signature. However, this alone does not mitigate the threat of replay, insertion and certain classes of message modification attacks. To secure the message from such threats, one of the mechanisms which support peer entity authentication (see Section 6.2) MAY be used or the underlying SOAP binding request processing model MUST address these threats.

### 6.3.1.1. Sender Processing Rules

- The construction and insertion of the `<wsse:Security>` element must adhere to the rules specified in the [wss-sms] and [wss-x509].
- The sender MUST demonstrate possession a subject confirmation key.
- For deployment settings which REQUIRE independent message authentication, the obligation MUST be accomplished by signing elements of the message and decorating the `<wsse:Security>` element with the signature.
- For deployment settings which DO NOT REQUIRE independent message authentication then the sender MUST accomplish this obligation by decorating the security header with a `<ds:KeyInfo>` element bearing the security token. This MUST be unambiguously verified to be the same certificate and key used in establishing peer entity authentication. This is necessary to mitigate the threat of a certificate substitution attack.
- If peer entity authentication is not in use and the message is bound with [LibertySOAPBinding] the sender MUST sign:
  - The `<sb:Correlation>` header block element.
  - All other header block elements which require the aforementioned security properties in accordance with the security requirements prescribed in their respective specification.
  - All sub-elements of the `<S:Body>`.
- If the message is signed then the sender MUST include the resultant XML signature in a `<ds:Signature>` element as a child of the `<wsse:Security>` header. The `<ds:Signature>` element MUST refer to the subject confirmation key with a `<ds:KeyInfo>` element.

### 6.3.1.2. Recipient Processing Rules

- The recipient MUST locate the `<wsse:Security>` element for which it is the target. This must adhere to the syntax and processing rules specified in [wss-sms] and [wss-x509].
• If the validation policy regards peer entity authentication sufficient for purposes of message authentication then the recipient MUST locate the \texttt{<ds:KeyInfo> element bearing a security token. This token MUST be unambiguously verified to be referring to the same certificate and key used in establishing peer entity authentication.}

• If the message has been signed then the recipient MUST locate the \texttt{<ds:Signature> element carried inside the \texttt{<wsse:Security> header.} The recipient MUST resolve the contents of the \texttt{<ds:KeyInfo> element carried within the \texttt{<ds:Signature> and use the key it describes for validating the signed elements.} This validation MUST conform to the core validation rules described in [XMLDsig]. Additionally, the recipient MUST determine that it trusts the key used to sign the message, and the recipient SHOULD validate the sender's certificate, verifying the certificate revocation status as appropriate to the risk of incorrect authentication.

• If peer entity authentication is not in use and the message is bound with [LibertySOAPBinding] the recipient MUST verify the signature covers the following elements:

  • The \texttt{<sb:Correlation> header block element.

  • All other header block elements which require the aforementioned security properties in accordance with the security requirements prescribed in their respective specification.

  • All sub-elements of the \texttt{<S:Body>.”}
6.3.1.3. Example X.509 v3 Message Authentication (Informative)

The following example demonstrates this message authentication mechanism.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/
 xmlns:ns="urn:liberty:soap-bind:2003-05"
 xmlns:idpp="urn:liberty:idpp:1.0"
 xmlns:sec="urn:liberty:security:2003-05">
  <s:Header>
    <ns:Correlation s:mustUnderstand="1"
      id="A13454...245"
      actor="http://schemas.../next"
      messageID="uuid:eefefef-aaaa-ffff-cccc-eeeeffffbbbb"
      time stamp="2112-03-15T11:12:12Z"/>
    <wsse:Security xmlns:wsse="...">
      <wsse:BinarySecurityToken ValueType="wsse:X509v3" wsu:Id="X509Token"
        EncodingType="wsse:Base64Binary">
        MIIB 9zCCAWgAwIBAgIQ...
      </wsse:BinarySecurityToken>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <!-- bind the correlation header -->
          <ds:Reference URI="#A13454...245">
            <ds:DigestValue>GuGsF0pi4xfPU...</ds:DigestValue>
          </ds:Reference>
          <!-- bind the security token (thwart cert substitution attacks) -->
          <ds:Reference URI="#X509Token">
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>Ru4cAfeBABE...</ds:DigestValue>
          </ds:Reference>
          <!-- bind the body of the message -->
          <ds:Reference URI="#MsgBody">
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>YgGfS0pi56pu...</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:KeyInfo>
          <wsse:SecurityTokenReference Usage="sec:MessageAuthentication">
            <wsse:Reference URI="#X509Token"/>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
        <ds:SignatureValue>
          HJJWbvqW8E84vJVQkj1LLA6nNvB7mY00TzhwBdFND1gscSXZ5Ekw==
        </ds:SignatureValue>
      </ds:Signature>
    </wsse:Security>
  </s:Header>
  <s:Body id="MsgBody">
    <idpp:Modify>
      <!-- this is an ID-PP Modify message -->
    </idpp:Modify>
  </s:Body>
</s:Envelope>
```

Figure 1.
6.3.2. SAML Assertion Message Authentication

The following URIs define SAML based unilateral (sender) message authentication mechanisms:

- urn:liberty:security:2003-08:ClientTLS:SAML

These mechanisms utilize the Web Services Security SAML Profile [wss-saml] as the means by which the message sender authenticates to the recipient. In general these mechanisms assume that a TTP issues an assertion which includes an `<saml:AuthenticationStatement>` which describes the authentication event to an authority and the subject confirmation obligations the subject must affirm its identity to a relying party.

These message authentication mechanisms are unilateral. That is only the author of the message is authenticated. It is not in the scope of this specification to suggest when response messages should be authenticated but it is worth noting that the mechanisms defined in Section 6.3.1 could be relied upon to authenticate the response message as well. Deployers should recognize, however, that independent authentication of response messages does not provide the same message stream protection semantics as a mutual peer entity authentication mechanism would offer.

For deployment settings which require independent message authentication then the sending peer MUST perform message authentication by demonstrating proof of possession of a subject confirmation key. This key MUST be recognized by the recipient as belonging to the sender.

When the sender wields the subject confirmation key to sign elements of the message the signature ensures the authenticity and integrity of the elements covered by the signature. However, this alone does not mitigate the threat of replay, insertion and certain classes of message modification attacks. To secure the message from such threats, one of the mechanisms which support peer entity authentication (see Section 6.2) MAY be used or the underlying SOAP binding request processing model MUST address these threats.

6.3.2.1. Sender Processing Rules

- The construction and decoration of the `<wsse:Security>` element must adhere to the rules specified in the [wss-sms] and [wss-saml].
- The sender MUST present the `<saml:Assertion>` (as security token) by inserting it as a child of `<wsse:Security>`.
- The sender MUST adhere to its subject confirmation obligation in accordance with the semantics of the confirmation method described by the `<saml:AuthenticationStatement>` bound to the `<saml:Assertion>.
- For deployment settings which DO NOT REQUIRE independent message authentication then for confirmation methods which require proof of possession the sender MUST accomplish this obligation when performing peer entity authentication. To accommodate this the assertion issuing authority MUST construct the assertion such that the confirmation key can be unambiguously verified to be the same certificate and key used in establishing peer entity authentication. This is necessary to mitigate the threat of a certificate substitution attack. It is RECOMMENDED that the certificate or certificate chain be bound to the subject confirmation key.
- If peer entity authentication is not in use and the message is bound with [LibertySOAPBinding] the sender MUST sign:
  - The `<sb:Correlation>` header block element.
6.3.2.2. Recipient Processing Rules

- The recipient MUST locate the `<wsse:Security>` element for which it is the target. This must adhere to the rules specified in the [wss-sms] and [wss-saml].

- The recipient MUST locate the `<saml:Assertion>` (security token) and the recipient MUST determine that it trusts the authority which issued the `<saml:Assertion>`.
  The recipient MUST validate the signature of the `<saml:Assertion>`. The recipient SHOULD validate the trust semantics of the signing key, as appropriate to the risk of incorrect authentication.

- If the validation policy regards peer entity authentication sufficient for purposes of message authentication then the recipient MUST locate the `<ds:KeyInfo>` element within `<saml:SubjectConfirmation>` element. This key MUST be unambiguously verified to be referring to the same certificate and key used in establishing peer entity authentication.

- If the message has been signed then the recipient MUST locate the `<ds:Signature>` element carried inside the `<wsse:Security>` header.
  The recipient MUST resolve the contents of the `<ds:KeyInfo>` element carried within the `<ds:Signature>` and use the key it describes for validating the signed elements.
  This validation MUST conform to the core validation rules described in [XMLDsig].

- The recipient MUST determine that it trusts the key used to sign the message. The recipient SHOULD validate the sender’s certificate and verify the certificate revocation status, as appropriate to the risk of incorrect authentication.

- If peer entity authentication is not in use and the message is bound with [LibertySOAPBinding] the recipient MUST verify the signature covers the following elements:
  - The `<sb:Correlation>` header block element.
  - All other header block elements which require the aforementioned security properties in accordance with the security requirements prescribed in their respective specification.
  - All sub-elements of the `<S:Body>`.
7. Supporting Schema

The authorization mechanism defined in this specification relies upon supporting XML Schema. The defined schema fosters the conveyance of authorization information within a given message exchange. This section defines new schema types as well as the utilization of schema elements defined in other specifications.

7.1. ProxySubject Schema

The `<ProxySubject>` is used to convey the identity of a proxy, the confirmation key and confirmation obligation the proxy must possess and demonstrate for authentication purposes. The following schema fragment describes the structure of the `<ProxySubject>` element:

```xml
<xs:element name="ProxySubject" substitutionGroup="saml:Subject"
            type="saml:SubjectType"/>
```

The construction of a `<ProxySubject>` element MUST adhere to the following constraints:

- The `<ProxySubject>` SHOULD include a `<saml:SubjectConfirmation>` element with a `<saml:ConfirmationMethod>` of `urn:oasis:names:tc:SAML:1.0:cm:holder-of-key`.
- The `<ProxySubject>` SHOULD specify the subject confirmation key by including a `<ds:KeyInfo>` element as a child of the `<saml:SubjectConfirmation>` element.

7.2. ProxyTransitedStatement Schema

The `<ProxyTransitedStatement>` is used to identify an entity which actively participated in the message exchanges leading up to a given resource access. Its intended usage is twofold. First, it MAY be used by the consumer of authorization data for conveyance to the assertion issuing authority. Second, the assertion issuing authority MAY propagate this information as advice within assertions it subsequently generates.

The following schema fragment describes the structure of the `<ProxyTransitedStatement>` element:

```xml
<xs:element name="ProxyTransitedStatement" type="saml:SubjectStatementAbstractType"/>
```

7.3. ProxyInfoConfirmationData Schema

The `<ProxyInfoConfirmationData>` is used to supply subject confirmation data which was demonstrated by a system entity to a trusted authority which resulted in propagating a resource access to a proxy.

The following schema fragment describes the structure of the `<ProxyInfoConfirmationData>` element:
ProxyInfoConfirmationData may be relied upon to corroborate the path information carried in a ProxyTransitedStatement.

Figure 4.

The semantics around the elements are as follows:

- The `<saml:AssertionIDReference>`, `<Issuer>` and `<IssueInstant>` are that of the `<saml:Assertion>` presented by the proxy subject.
- The OPTIONAL `<ds:Signature>` element is a digital signature created by the recipient which covers the child elements of `<ProxyInfoConfirmationData>` with the exclusion of itself. It is RECOMMENDED that the enveloped signature transform (see [XMLDsig]) be utilized to accomplish the element exclusion.

7.4. SessionContext Schema

The `<SessionContext>` element conveys session status of an entity to another system entity. In general it is supplied to a relying party to support policy enforcement.

The following schema fragment describes the structure of the `<SessionContext>` element:

Figure 5.

The contents of the `<SessionContext>` element MUST adhere to the following constraints:

- The `<saml:SessionSubject>` element MUST be constructed in such a way as to protect the privacy of the identifier it carries by adhering to the rules defined in Encrypted Name Identifiers [Section 5.3.1]. The identifier
MUST indicate (when decrypted) the identity of the subject with which the session applies. This identity MUST be resolvable in the namespace of the entity consuming the <SessionContext> element.

- The <ProviderID> element is a URI which indicates the entity (session holder) with which the session applies. <ProviderID> MUST correspond with the constraints for the <entityIDType> data type as specified in [LibertyMetadata].

- The <ac:AuthnContext> element depicts the authentication context which the session holder relied upon to create the session.

- The AuthenticationInstant attribute describes the time at which the subject of the session authenticated to an authority.

- The AssertionIssueInstant attribute is the time at which the assertion issuer generated an assertion for the provider.

### 7.5. SessionContextStatement Schema

The <SessionContextStatement> element conveys session status of an entity to another system entity within the body of an <saml:Assertion>.

The following schema fragment describes the structure of the <SessionContextStatement> element:

```xml
<xs:element name="SessionContextStatement"
    type="sec:SessionContextStatementType"
    substitutionGroup="saml:SubjectStatement"/>
<xs:complexType name="SessionContextStatementType">
    <xs:complexContent>
        <xs:extension base="saml:SubjectStatementAbstractType">
            <xs:sequence>
                <!-- This is the name of the proxy and it SHOULD carry SubjectConfirmation information to authorize the ProxySubject to act on behalf of the Subject inherited from SubjectStatementAbstractType -->
                <xs:element name="ProxySubject"
                    type="saml:SubjectType" minOccurs="0"/>
                <xs:element ref="sec:SessionContext"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

Figure 6.

The <SessionContextStatement> derives from <saml:SubjectStatementAbstractType> and MUST adhere to the following constraints:

- It MAY include a <ProxySubject> element which adheres to the structure and semantics described in this specification

- It MUST include a <SessionContext> element which adheres to the structure and semantics described in this specification
7.6. ResourceAccessStatement Schema

Resource access information is captured in a `<ResourceAccessStatement>` element. The purpose of this statement is to convey sufficient information regarding the accessing entity and the resource for which access is being attempted.

The following schema fragment describes the structure of the `<ResourceAccessStatement>` element:

```xml
<xs:element name="ResourceAccessStatement"
    type="sec:ResourceAccessStatementType"
    substitutionGroup="saml:SubjectStatement"/>
<xs:complexType name="ResourceAccessStatementType">
    <xs:complexContent>
        <xs:extension base="saml:SubjectStatementAbstractType">
            <xs:sequence>
                <xs:group ref="disco:ResourceIDGroup"/>
                <xs:sequence minOccurs="0">
                    <!-- This is the name of the proxy and it SHOULD carry SubjectConfirmation information to authorize the ProxySubject to act on behalf of the Subject inherited from SubjectStatementAbstractType -->
                    <xs:element name="ProxySubject" type="saml:SubjectType"/>
                    <xs:element ref="sec:SessionContext" minOccurs="0"/>
                </xs:sequence>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

Figure 7.

The `<ResourceAccessStatement>` derives from `<saml:SubjectStatementAbstractType>` and MUST adhere to the following constraints:

- It MUST contain either a `<disco:ResourceID>` or a `<disco:EncryptedResourceID>` element which adheres to the processing rules of [[LibertyDisco]]
- It MAY include a `<ProxySubject>` element which adheres to the structure and semantics described in this specification
- It MAY include a `<SessionContext>` element which adheres to the structure and semantics described in this specification
8. Message Authorization Model

The Message Authorization Model specifies OPTIONAL mechanisms to convey authorization and resource access information (supplied by a trusted third party) which may be necessary to access a service. This facility, incorporated for authorization purposes, serves a distinct and complementary function to the binding between subject and key which the subject accomplishes for authentication purposes. However, it is possible to optimize the processing when the message authentication mechanism utilizes the same subject confirmation key as the authorization mechanism and the key has successfully been applied to ensure the integrity and authenticity of the message payload.

8.1. Authorization Mechanism Overview (Informative)

The authorization mechanism defined by this specification formalizes the generation and conveyance of authorization information. In support of this mechanism a Trusted Third Party (TTP) may be relied upon to act as a Policy Decision Point (PDP) and potentially a coarse grained Policy Enforcement Point (PEP) to facilitate the exchange of resource access information to the relying party. As a PDP, the Trusted Third Party would adhere to the coarse access policies of the relying party insofar as ensuring which entities may attempt to access a given resource. This requires strong assurance as to the authenticity of a peer subject. Given the reliance of authorization upon authentication, this model aids in disseminating subject confirmation obligations, identity information and access authorization data.

The Sender may authenticate to the Recipient using one of three general methods Section 6. Using any of these methods, both the Access Authorization PDP and the Proxy Authorization PDP may be located either at the TTP or the recipient. Although in principle all permutations of authentication mechanism, Access Authorization PDP location, and Proxy Authorization PDP location are possible.

When the PDP is located at the TTP, the TTP must issue an assertion with respect to Sender authorizations for consumption by the Service - this assertion will likely be presented to the Sender/Proxy for inclusion in the request to the Recipient. Note that if the TTP policies do not grant access to the particular resource the TTP may also act as a PEP and not issue an assertion.

When the PDP for both types of authorization decisions is located at the TTP, the two different assertions issued by the TTP logically collapse into a single authorization assertion, e.g. ‘Invocation Identity can perform operation’ and ‘Sender can proxy for Invocation Identity’ collapses to ‘Sender can perform operation’. The authorization decision that the TTP creates could reflect this. It may still however be desirable for both assertions to be sent.

Authentication and authorization authorities may be co-located. When the Sender is relying on a particular TTP for both authentication (through SAML holder-of-key) and either types of authorization decision, some optimization may be possible through that TTP issuing ‘combined’ assertions.

8.2. Authorization Mechanism

It is RECOMMENDED that this mechanism utilize the Web Services Security SAML Profile [wss-saml] as the means by which the message sender authenticates to the recipient. Each communicating peer performs message level authentication by demonstrating proof of possession of a subject confirmation key. The assertion issuer binds the subject confirmation key to the assertion by signing the assertion. This attestation assures the consumer of the assertion that the subject confirmation key is that of the intended sender. Thus the senders subject confirmation key can be recognized by the recipient as belonging to the remote peer. Subsequent to the authentication of the sender the recipient can leverage this knowledge in support of the authorization model described below.

The authorization model supports the issuance of assertions which convey information regarding the resource to be accessed, the entity attempting to access the resource, the mechanism by which the accessing entity must use to demonstrate its identity to the recipient and the ability for the accessing entity to access the resource on behalf of another system entity. This latter facility suggests the need to verify two distinct identities in a given resource access message, the sender identity and the invocation identity. Thus the authorization model supports a constrained proxy mechanism which permits a proxy (the sender) to access the resource on behalf of some other system entity.
To aid in processing of the authorization information `<wsse:SecurityTokenReference>` elements MUST qualify their usage by specifying the `<wsse:Usage>` attribute with a QName value of `sec:RequestAuthorization`. If the processing rules specified in the subsequent sections are adhered to then the authorization usage qualifier would subsume `sec:MessageAuthentication`.

8.3. Authorization Data Generation

It is anticipated that a service exists which aids in the discovery of identity-based web services. In support of this, a Trusted Authority may issue an assertion which is subsequently used in conjunction with the accessing of the discovered identity-based web service.

In addition to managing the registration and discovery of identity-based web services the Trusted Authority may act as a centralized policy information and decision point. The authority may issue assertions regarding authentication and authorization policies enforced for a given identity-based web service, resource and the identity of the sender.

The makeup of this assertion reflects the information necessary to accommodate the authentication and authorization requirements.

8.3.1. Processing Rules

The following processing rules describe the steps the assertion issuing authority takes to generate an assertion. It is out of scope for this specification to describe how assertions are requested and distributed. However it is presumed that in order for assertions to be generated that the requester has been authenticated and that the assertion issuing authority has enforced the necessary access controls to ensure that the assertions are released to authorized entities.

Presuming the requesting entity meets the necessary authorization criteria, the assertion issuing authority constructs the assertion in accordance with the following rules:

- The assertion MUST include at most one of the following statements; `<SessionContextStatement>` or a `<ResourceAccessStatement>`.
- The `<saml:Subject>` element MUST describe the invocation identity. The invocation identity MUST be either that of the sender or another system entity on whose behalf the sender (as a proxy) is authorized to act.
- The assertion MUST describe the invocation identity within the `<saml:Subject>` element of the base statement.
- When the invocation identity is that of the sender the `<saml:Subject>` element of the base statement type MUST be constructed as follows:
  - The `<saml:Subject>` element MUST include a `<saml:SubjectConfirmation>` element with a `<saml:ConfirmationMethod>` of `urn:oasis:names:tc:SAML:1.0:cm:holder-of-key`.
  - The subject confirmation key MUST be specified within the `<saml:Subject>` element by including a `<ds:KeyInfo>` element in the `<saml:SubjectConfirmation>` element.
• When the invocation identity is NOT that of the sender the <saml:Subject> element of the base statement type MUST be constructed as follows:
  The assertion SHOULD protect the privacy of the named entity with a <lib:EncryptedNameIdentifier> element.
  The authority MUST include a <saml:SubjectConfirmation> element in this subject and specify that the sender will vouch for the subject by indicating a <saml:ConfirmationMethod> of urn:oasis:names:tc:SAML:1.0:cm:sender-vouches.
  D1Additionally, the assertion MUST identify the proxy and its confirmation requirements by including a <ProxySubject> element. This element MUST be constructed in accordance with the constraints defined in ProxySubject Schema [Section 7.1]. OPTIONALLY, the assertion issuer MAY include proxy chaining information in the <saml:Advice> element. It is RECOMMENDED that the <saml:Advice> be of Type <saml:Assertion> and that the contents of the assertion be comprised with statements of Type <ProxyTransitedStatement>. The issuer should include a <ProxyTransitedStatement> for each proxy which has participated in the message exchange. See Proxy Chaining [Section 8.3.2] for a recommendation on constructing the proxy chain.

• For statements of type <ResourceAccessStatement> the assertion issuing authority MUST adhere to the construction constraints described in ResourceAccessStatement Schema [Section 7.6].
  The assertion issuing authority MAY describe the authentication status of the interacting party by including a <SessionContext> element. The by <SessionContext> element MUST adhere to the construction constraints described in SessionContext Schema [Section 7.6].

• For statements of type <SessionContextStatement> the assertion issuing authority MUST adhere to the construction constraints described in SessionContextStatement Schema [Section 7.5] and SessionContext Schema [Section 7.6].

• The assertion MUST be signed by the assertion issuing authority in accordance with the signing requirements specified in [SAMLCore11].

8.3.2. Proxy Chaining

In some operational settings it may be necessary to carry the chain of proxies traversed. The following algorithm describes how an assertion issuing authority could formulate the proxy chain.

It is presumed that when an entity interacts with the assertion issuing authority that the requester will include a claim which bears a <ProxyTransitedStatement> which includes the necessary <ProxyInfoConfirmationData>.

The confirmation data includes the <saml:AssertionID> of the assertion which the proxy presented to the requester for authorization purposes. Thus, the assertion issuer could use this information to locate the original assertion. Given the assertion the proxy chain can be extracted and a new chain created by appending the newest proxy to the chain. The result will be an <saml:Assertion> comprised of <ProxyTransitedStatement> elements for each of the proxies transited.
8.4. Presenting Authorization Data

Interactions with identity-based web services may rely on the conveyance of authorization information. In general, the authorization data is issued by a trusted authority. In such a setting the authorization information would be sent along with the identity-based web service request to the recipient. See Authorization Data Generation [Section 8.3] for details as to how this data is acquired and formulated.

8.4.1. Processing Rules

• The sender MUST authenticate to the recipient using one of the SAML authentication mechanisms described in Message Authentication [Section 6.3]. It is RECOMMENDED that the sender authenticate using the SAML Assertion Message Authentication and specifically conform with the processing rules specified in [Section 6.3.2.1].

• In accordance with the above requirement the sender MUST include the resultant XML signature in a <ds:Signature> element. The signature element SHOULD be decorated with a ds:KeyInfo which MUST resolve to the subject confirmation key.

To assist the receiver in processing the authorization information, the sender decorates the <ds:Signature> with a <ds:KeyInfo> which SHOULD include a <wsse:SecurityTokenReference> element in accordance with the [wss-sms]. The <wsse:SecurityTokenReference> element MUST be qualified with usage information by specifying the <wsse:Usage> attribute. The value MUST be a QName value of sec:RequesterAuthorization.

8.5. Consuming Authorization Data

A recipient which exposes a resource typically makes access control decisions based on the invocation identity. Additionally the recipient may also predicate access control policies upon the sender identity. The semantics of resource access authorization are described in Presenting Authorization Data [Section 8.4].

The recipient determines the invocation identity by inspecting the <saml:Subject> element and the proxy identity by inspecting the <ProxySubject> if present. When the <ProxySubject> element is present it also describes the subject confirmation obligation of the proxy. Providing both the invocation identity and the proxy identity enables the recipient to tailor authorization policy to a finer degree of granularity. That is, the recipient generally uses the invocation identity to make its authorization decisions and potentially determine whether the proxy is permitted to access the resource on behalf of said invocation identity.

8.5.1. Processing Rules

• The recipient MUST authenticate the sender using one of the mechanisms described in Authentication Mechanisms.

It is RECOMMENDED that the sender authenticate using the SAML Assertion Message Authentication and specifically conform with the processing rules specified in [Section 6.3.2.2].

• The recipient MUST locate the <saml:Assertion> (security token) which conferred the subject confirmation key relied upon for sender authentication.

The recipient MUST corroborate that the bound subject confirmation key is the same key used to authenticate the communicating peer.

• The recipient MUST determine that it trusts the authority which signed the <saml:Assertion>. The recipient MUST validate the signature of the <saml:Assertion>. The recipient SHOULD validate the trust semantics of the signing key, as appropriate to the risk of incorrect authentication.
9. Identity-Based Web Service Examples (Informative)

The following are examples demonstrating the various use cases supported by this specification.

9.1. Conveyance of Sender as Invocation Identity

Recall that the authorization model describes a mechanism for an assertion issuing authority to bind the invocation identity to an assertion by specifying the invocation identity within the `<saml:Subject>`. The following example demonstrates the construction of a `<saml:Subject>` to accomplish this binding:

```xml
<Subject>
  <!-- the name identifier of the sender -->
  <NameIdentifier format="urn:liberty:iff:nameid:entity ID">
    http://serviceprovider.com/
  </NameIdentifier>
  <SubjectConfirmation>
    <ConfirmationMethod>
      urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
    </ConfirmationMethod>
    <!-- This keyinfo is the key by which the sender must prove possession. Note the KeyName MAY but is NOT REQUIRED to match the above NameIdentifier -->
    <ds:KeyInfo>
      <ds:KeyName>
        CN=serviceprovider.com,OU=Services R US,O=Service Nation,...
      </ds:KeyName>
      <ds:KeyValue>...
    </ds:KeyInfo>
  </SubjectConfirmation>
</Subject>
```

Figure 8.

Contents in the above example worth particular mention include:

- The assertion issuing authority specifies the `<saml:ConfirmationMethod>` with the value of `urn:oasis:names:tc:SAML:1.0:cm:holder-of-key`.
- The assertion issuing authority included a `<ds:KeyInfo>` element to indicate which key the `<saml:Subject>` must demonstrate possession of to meet the above confirmation obligation.

What follows is a more complete example which depicts a request to access an identity-based web service which carries authorization data to the recipient such that the sender identity and the invocation identity are the same. The resource for which the sender is attempting to access is described in an ResourceAccessStatement bound to the assertion.

The interpretation of the assertion can be expressed as follows:

According to the policies of the assertion issuing authority the sender must adhere to the confirmation requirements expressed in the encapsulated ResourceAccessStatement. To meet the obligation the message sender;

- must successfully demonstrate possession of the key referenced in the ResourceAccessStatement’s SubjectConfirmation element which is bound to the Assertion
- AND the message receiver has a trusted path from the signing certificate to an issuing Certification Authority.
Note that, while the assertion associates a subject’s name with a key, this association is made as a means to indicate the authorization of that subject, acting with that key, to invoke a service. This facility, incorporated for authorization purposes, serves a distinct and complementary function to the binding between subject and key which the subject’s certificate accomplishes for authentication purposes.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:sb="urn:liberty:soap-bind:2003-05"
  xmlns:idpp="urn:liberty:idpp:1.0"
  xmlns:sec="urn:liberty:security:2003-05">
  <s:Header>
    <sb:Correlation s:mustUnderstand="1"
      id="A13454...245"
      actor="http://schemas.../next"
      messageID="uuid:efefef-aaaa-ffff-cccc-eeeffffbbbb"
      timestamp="2112-03-15T11:12:12Z"/>

    <wsse:Security>
      <saml:Assertion
        xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
        MajorVersion="1" MinorVersion="0"
        AssertionID="2sxJu9g/vvLG9sAN9bKp/8g0KNU="
        Issuer="idp.example.com"
        IssueInstant="2003-09-09T16:58:33.173Z">
        <!-- The AuthenticationStatement carries information
          which describes the identity of the entity this assertion
          was issued too (the Subject) and the method the Subject
          authenticated to the assertion issuing authority -->
        <saml:AuthenticationStatement
          AuthenticationMethod="urn:ietf:rfc:2246"
          AuthenticationInstant="2003-09-09T16:57:30.000Z">
          <saml:Subject>
            <saml:NameIdentifier
              format="urn:liberty:iff:nameid:entityID"
              NameQualifier="http://AffiliationStation.com/">
              http://serviceprovider.com/
            </saml:NameIdentifier>
            <saml:SubjectConfirmation>
              <saml:ConfirmationMethod>
                urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
              </saml:ConfirmationMethod>
              <!-- This keyinfo is the key by which the sender must prove
                  possession. Note the KeyName MAY but is NOT REQUIRED to
                  match the above NameIdentifier -->
              <ds:KeyInfo>
                <ds:KeyName>
                  CN=serviceprovider.com,OU=Services R US,O=Service Nation,...
                </ds:KeyName>
                <ds:KeyValue>... </ds:KeyValue>
              </ds:KeyInfo>
            </saml:SubjectConfirmation>
          </saml:Subject>
        </saml:AuthenticationStatement>

        <!-- The Subject of the ResourceAccessStatement specifies use of
          holder-of-key which indicates the subject of the statement
          is the sender of the message and is to be treated as the
          invocation identity for any access control decisions -->

        <ResourceAccessStatement
          xmlns="urn:oasis:names:tc:SAML:1.0:assertion">
          <!-- the name identifier of the sender -->
          <saml:NameIdentifier format="urn:liberty:iff:nameid:entityID"
            http://serviceprovider.com/>
        </ResourceAccessStatement>
      </saml:Assertion>
    </wsse:Security>
  </s:Header>
</s:Envelope>
```
Liberty Alliance Project:  
Liberty ID-WSF Security Mechanisms

This authorization model supports environments where the sender of a message is acting as a proxy on behalf of another system entity. The following example demonstrates the construction of a `<ProxySubject>` to accomplish this binding:

```
<saml:ConfirmationMethod>
  <saml:KeyInfo>
    <ds:KeyName>
      CN=serviceprovider.com,OU=Services R US,O=Service Nation,...
    </ds:KeyName>
    <ds:KeyValue>...
  </ds:KeyInfo>
</saml:ConfirmationMethod>
```

```
<!-- This keyinfo is the key by which the sender must prove possession. Note the KeyName MAY but is NOT REQUIRED to match the above NameIdentifier -->
```

```
<ds:KeyInfo>
  <ds:KeyName>
    CN=serviceprovider.com,OU=Services R US,O=Service Nation,...
  </ds:KeyName>
  <ds:KeyValue>...
</ds:KeyInfo>
```

```
<!-- This ResourceID describes the resource for which the sender is attempting to access. -->
```

```
<disco:ResourceID>http://example.com/disco/d0CF8e1JTDLzmEo</disco:ResourceID>
```

```
<!-- This ResourceID describes the resource for which the sender is attempting to access. -->
```

```
<ds:KeyInfo>
  <wsse:SecurityTokenReference Usage="sec:RequestAuthorization">
    <wsse:Reference URI="#2sxJu9g/vvLG9aAN9bKp/8qDNKU=" />
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

```
<!-- this is the signature the sender generated to demonstrate holder-of-key the signature should cover the i,s header and body-->
```

```
<ds:KeyInfo>
  <wsse:SecurityTokenReference Usage="sec:RequestAuthorization">
    <wsse:Reference URI="#2sxJu9g/vvLG9aAN9bKp/8qDNKU=" />
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

```
<!-- this is the signature the sender generated to demonstrate holder-of-key the signature should cover the i,s header and body-->
```

```
<ds:SignedInfo>
  <ds:Reference URI="#AL3454...245">
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>GyGsF0Pi4xPU...</ds:DigestValue>
  </ds:Reference>
  <ds:Reference URI="#MsgBody">
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>YgGFp0p156pu...</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>
```

```
<ds:KeyInfo>
  <wsse:SecurityTokenReference Usage="sec:RequestAuthorization">
    <wsse:Reference URI="#2sxJu9g/vvLG9aAN9bKp/8qDNKU=" />
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

```
<ds:SignatureValue>
  HJJWbvqW9E84vJVQkJLLA6nVbX7mY00TtwBdFNE1gscSXZ5Ekw==
</ds:SignatureValue>
```

```
<ds:Signature>
  <ds:SignedInfo>
    <ds:Reference URI="#AL3454...245">
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <ds:DigestValue>GyGsF0Pi4xPU...</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#MsgBody">
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <ds:DigestValue>YgGFp0p156pu...</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
</ds:Signature>
```

Figure 9.

**9.2. Conveyance of Sender as Proxy**

This authorization model supports environments where the sender of a message is acting as a proxy on behalf of another system entity. The following example demonstrates the construction of a `<ProxySubject>` to accomplish this binding:
Contents in the above example worth particular mention include:

- The assertion issuing authority generated assertion indicates that the <saml:Subject> element is that of the system entity on whose behalf the sender is proxying.
- The assertion includes a <ProxySubject> element so as to convey the identity of the proxy to the relying party.
- The <ProxySubject> element specifies the <saml:ConfirmationMethod> with a value of urn:oasis:names:tc:SAML:1.0:cm:holder-of-key.
- The <saml:SubjectConfirmation> element includes a <ds:KeyInfo> element which indicates which key the proxy must prove possession of to meet the confirmation obligation.

The following example is a more complete demonstration of a request invoking an identity-based web service which carries authorization data to the recipient such that the sender can act as a proxy on behalf of the entity described in the subject of the resource access statement.
Liberty Alliance Project:
Liberty ID-WSF Security Mechanisms

1071 authenticated to the assertion issuing authority -->
1072 <saml:AuthenticationStatement
1073  <AuthenticationMethod="urn:ietf:rfc:2246"
1074  AuthenticationInstant="2003-09-09T16:57:30.000Z">
1075  <saml:Subject>
1076   <saml:NameIdentifier format="urn:liberty:iff:nameid:entityID">
1077     http://serviceprovider.com/
1078   </saml:NameIdentifier>
1079   <saml:SubjectConfirmation>
1080     <saml:ConfirmationMethod>
1081      urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
1082    </saml:ConfirmationMethod>
1083    <!-- This keyinfo is the key by which the sender must prove
1084    possession. Note the KeyName MAY but is NOT REQUIRED to
1085    match the above NameIdentifier -->
1086    <ds:KeyInfo>
1087      <ds:KeyName>
1088       CN=serviceprovider.com,OU=Services R US,O=Service Nation,...
1089      </ds:KeyName>
1090      <ds:KeyValue>...</ds:KeyValue>
1091    </ds:KeyInfo>
1092   </saml:SubjectConfirmation>
1093  </saml:Subject>
1094 </saml:AuthenticationStatement>

1096 <!-- Subject of the ResourceAccessStatement specifies a
1097 confirmation method of sender-vouches. This indicates that the
1098 subject of the statement is being vouched for by the sender of
1099 the message. The sender identity is conveyed in the
1100 ProxySubject element. In order for the ProxySubject to vouch
1101 for the Subject the ProxySubject must meet the holder-of-key
1102 confirmation obligation. The proxy does so by demonstrating
1103 possession of the described key. In this scenario the Subject of
1104 the message is to be treated as the invocation identity (for
1105 any access control decisions) -->
1106
1107 <ResourceAccessStatement xmlns="urn:oasis:names:tc:SAML:1.0:assertion">
1108  <saml:Subject>
1109    <!-- the name identifier of the interacting entity -->
1110    <saml:NameIdentifier ID="#abesyd"
1111       Format="urn:liberty:iff:nameid:encrypted">
1112       HJNWbqW9E84vJVQkjjLLA6nNvB7x7wDfNDElgscS XZ5EkwA3B45...C569UXR3==
1113    </saml:NameIdentifier>
1114    <SubjectConfirmation>
1115      <!-- The confirmed sender of this message vouches for the
1116      identity carried in this subject. -->
1117      <ConfirmationMethod>
1118        urn:oasis:names:tc:SAML:1.0:cm:sender-vouches
1119      </ConfirmationMethod>
1120    </SubjectConfirmation>
1121  </saml:Subject>
1122 <ProxySubject>
1123  <!-- the name identifier of the sender -->
1124  <NameIdentifier format="urn:liberty:iff:nameid:entityID">
1125     http://serviceprovider.com/
1126 </NameIdentifier>
1127  <SubjectConfirmation>
1128   <ConfirmationMethod>
1129      urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
1130    </ConfirmationMethod>
1131    <!-- This keyinfo is the key by which the sender must prove
1132    possession. -->
1133    <ds:KeyInfo>
1134      <ds:KeyName>
1135       CN=serviceprovider.com,OU=Services R US,O=Service Nation,...
1136    </ds:KeyName>
1137  </ResourceAccessStatement>
The following example is similar to the above example with the addition of conveying session context of the entity (principal) interacting with the message sender.

<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body id="MsgBody">
    <idpp:Modify>
      <!-- this is an ID-PP Modify message -->
    </idpp:Modify>
  </s:Body>
</s:Envelope>
<s:Header>
  <sb:Correlation s:mustUnderstand="1"
    id="A13454...245"
    actor="http://schemas .../next"
    messageID="uuid:efefefef-aaa-a-fff-cccc-eeeffbbbbb"
    timestamp="2112-03-15T11:12:12Z"/>
</wase:Security>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  AssertionID="2sxJu9g/vvLG9sAN9bKp/8q0NKU="
  Issuer="idp.example.com"
  IssueInstant="2003-09-09T16:58:33.173Z">
  <!-- The AuthenticationStatement carries information
      which describes the identity of the entity this assertion
      was issued too (the Subject) and the method the Subject
      authenticated to the assertion issuing authority -->
  <saml:AuthenticationStatement
    AuthenticationMethod="urn:ietf:rfc:2246"
    AuthenticationInstant="2003-09-09T16:57:30.000Z">
    <saml:NameIdentifier format="urn:liberty:iff:nameid:entityID">
      http://serviceprovider.com/
    </saml:NameIdentifier>
    <saml:Subject
      ConfirmationMethod="urn:oasis:names:tc:SAML:1.0:cm:holder-of-key"
      SubjectConfirmation
        ConfirmationMethod"
        SubjectConfirmation
        <ds:KeyInfo
          KeyName"
          KeyName"
          KeyValue">
            RS, O=Service Nation,...
          </KeyInfo>
          <saml:SubjectConfirmation
            ConfirmationMethod="urn:oasis:names:tc:SAML:1.0:cm:holder-of-key"
            SubjectConfirmation
        </ds:KeyInfo>
        <ds:KeyInfo
          KeyName">
            RS, O=Service Nation,...
          </KeyInfo>
          <saml:Subject
            ConfirmationMethod"
            SubjectConfirmation"
          <ds:KeyInfo
            KeyName">
              RS, O=Service Nation,...
            </KeyInfo>
            <saml:Subject
              ConfirmationMethod">
                RS, O=Service Nation,...
              </SubjectConfirmation>
            </saml:SubjectConfirmation>
          </saml:Subject>
        </ds:KeyInfo>
      </saml:AuthenticationStatement>
    </saml:Subject>
  </saml:Assertion>
</s:Header>
<!-- This ResourceID describes the resource for which
the sender is attempting to access. -->
<disco:ResourceID>http://foo.com/d0CQF8e1jTDLmzEo</disco:ResourceID>

<!-- The session context of the entity interacting with the
request sender -->
<SessionContext xmlns="urn:liberty:id-wsf:sec:1.0"

AuthenticationInstant="" AssertionIssueInstant="">
    <SessionSubject>
        <saml:NameIdentifier ID="#abesyd"
            Format="urn:liberty:iff:nameid:encrypted">
            HJJWbvqW9E84vJVQkjjLLA6nNV8X7mY00T7hwbFDNDElgsCSXZ5Ekw
            A23B45C569UKjJLLA6nNV8X7mY00T7hwbFDNDElgsCSXZ5Ekw89XR3==
        </saml:NameIdentifier>
    </SessionSubject>
    <AuthnContext
        xmlns="http://www.projectliberty.org/schemas/authctx/2002/05">
        ...
    </AuthnContext>
    <ProviderID>http://serviceprovider.com/</ProviderID>
</SessionContext>

<!-- signature by the authority over the assertion -->
<ds:Signature>...
</ds:Signature>
<!-- this is the signature the sender generated to demonstrate holder-of-key
the signature should cover the isf header and body-->
<ds:Signature>
    <ds:SignedInfo>
        <ds:Reference URI="#A13454...245">
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>GyGsF0Pi4xPU...</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:KeyInfo>
        <wsse:SecurityTokenReference Usage="sec:RequestAuthorization">
            <wsse:Reference URI="#2sxJu9g/vvLG9aAN9bKp/8qVNKU=" />
        </wsse:SecurityTokenReference>
    </ds:KeyInfo>
    <ds:SignatureValue>
        HJJWbvqW9E84vJVQkjjLLA6nNV8X7mY00T7hwbFDNDElgsCSXZ5Ekw==
    </ds:SignatureValue>
</ds:Reference>
</s:Body>
</s:Envelope>

Figure 12.
10. XSD

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:liberty:sec:2003-08"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
    xmlns:ac="urn:liberty:ac:2003-08"
    xmlns:lib="urn:liberty:iff:2003-08"
    xmlns:disco="urn:liberty:disco:2003-08"
    xmlns:md="urn:liberty:metadata:2003-08"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:sec="urn:liberty:sec:2003-08"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">
  <xs:import namespace="urn:oasis:names:tc:SAML:1.0:assertion"
      schemaLocation="oasis-ssts-c-saml-schema-assertion-1.1.xsd"/>
  <xs:import namespace="urn:liberty:iff:2003-08"
      schemaLocation="liberty-idff-protocols-schema-v1.2.xsd"/>
  <xs:import namespace="urn:liberty:disco:2003-08"
      schemaLocation="liberty-idwsf-disco-svc-v1.0.xsd"/>
  <xs:import namespace="urn:liberty:ac:2003-08"
      schemaLocation="liberty-authentication-context-v1.2.xsd"/>
  <xs:import namespace="urn:liberty:metadata:2003-08"
      schemaLocation="liberty-metadata-v1.0.xsd"/>
  <xs:import namespace="http://www.w3.org/2001/04/xmlenc#"
      schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd"/>
  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
      schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
  <xs:annotation>
    <xs:documentation>
      The source code in this XSD file was excerpted verbatim from:
      Liberty ID-WSF Security Mechanisms Specification
      Version 1.0
      12th November 2003
      Copyright (c) 2003 Liberty Alliance participants, see
      http://www.projectliberty.org/specs/idwsf_copyrights.html
    </xs:documentation>
    <xs:element name="MessageAuthentication" type="xs:QName"/>
    <xs:element name="RequesterAuthorization" type="xs:QName"/>
    <xs:element name="ValidityRestrictionCondition" type="sec:ValidityRestrictionConditionType"/>
    <xs:complexType name="ValidityRestrictionConditionType">
      <xs:extension base="saml:ConditionAbstractType">
        <xs:sequence>
          <xs:element name="NumberOfUses" type="xs:integer"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexType>
    <xs:element name="ProxySubject" substitutionGroup="saml:Subject"
      type="saml:SubjectType"/>
    <xs:annotation>
      <xs:documentation>ProxyTransitedStatement is a SubjectStatement which MAY carry specific subject confirmation data</xs:documentation>
  </xs:annotation>
</xs:schema>
```
ProxyInfoConfirmationData may be relied upon to corroborate the path information carried in a ProxyTransitedStatement.
<!-- This is the name of the proxy and it SHOULD carry
SubjectConfirmation information to authorize the
ProxySubject to act on behalf of the
Subject inherited from
SubjectStatementAbstractType -->
<xs:element name="ProxySubject" type="saml:SubjectType"/>
<xs:element ref="sec:SessionContext" minOccurs="0"/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:schema>
Bibliography

Normative


