Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.

- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.

- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.

- **Patents.** Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.

- **License Programs.** To see all of the protocols in scope under a specific license program and the associated patents, visit the Patent Map.

- **Trademarks.** The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.

- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

**Reservation of Rights.** All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

**Tools.** The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

**Support.** For questions and support, please contact dochelp@microsoft.com.
## Revision Summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision History</th>
<th>Revision Class</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/13/2009</td>
<td>0.1</td>
<td>Major</td>
<td>Initial Availability</td>
</tr>
<tr>
<td>8/28/2009</td>
<td>0.2</td>
<td>Editorial</td>
<td>Revised and edited the technical content</td>
</tr>
<tr>
<td>11/6/2009</td>
<td>0.3</td>
<td>Editorial</td>
<td>Revised and edited the technical content</td>
</tr>
<tr>
<td>2/19/2010</td>
<td>1.0</td>
<td>Major</td>
<td>Updated and revised the technical content</td>
</tr>
<tr>
<td>3/31/2010</td>
<td>1.01</td>
<td>Major</td>
<td>Updated and revised the technical content</td>
</tr>
<tr>
<td>4/30/2010</td>
<td>1.02</td>
<td>Editorial</td>
<td>Revised and edited the technical content</td>
</tr>
<tr>
<td>6/7/2010</td>
<td>1.03</td>
<td>Editorial</td>
<td>Revised and edited the technical content</td>
</tr>
<tr>
<td>6/29/2010</td>
<td>1.04</td>
<td>Minor</td>
<td>Clarified the meaning of the technical content.</td>
</tr>
<tr>
<td>7/23/2010</td>
<td>1.04</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>9/27/2010</td>
<td>1.04</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>11/15/2010</td>
<td>1.04</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>12/17/2010</td>
<td>1.04</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>3/18/2011</td>
<td>1.04</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>6/10/2011</td>
<td>1.04</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>1/20/2012</td>
<td>1.5</td>
<td>Minor</td>
<td>Clarified the meaning of the technical content.</td>
</tr>
<tr>
<td>4/11/2012</td>
<td>1.5</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>7/16/2012</td>
<td>1.5</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>9/12/2012</td>
<td>1.5</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>10/8/2012</td>
<td>1.6</td>
<td>Minor</td>
<td>Clarified the meaning of the technical content.</td>
</tr>
<tr>
<td>2/11/2013</td>
<td>1.6</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>7/30/2013</td>
<td>1.6</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>11/18/2013</td>
<td>1.6</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>2/10/2014</td>
<td>1.6</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>4/30/2014</td>
<td>1.7</td>
<td>Minor</td>
<td>Clarified the meaning of the technical content.</td>
</tr>
<tr>
<td>Date</td>
<td>Revision History</td>
<td>Revision Class</td>
<td>Comments</td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>7/31/2014</td>
<td>2.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>10/30/2014</td>
<td>2.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>3/16/2015</td>
<td>3.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>2/26/2016</td>
<td>4.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>7/15/2016</td>
<td>4.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>9/14/2016</td>
<td>5.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>1/12/2017</td>
<td>5.1</td>
<td>Minor</td>
<td>Clarified the meaning of the technical content.</td>
</tr>
<tr>
<td>6/20/2017</td>
<td>6.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>7/24/2018</td>
<td>7.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>10/1/2018</td>
<td>8.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>12/11/2018</td>
<td>8.1</td>
<td>Minor</td>
<td>Clarified the meaning of the technical content.</td>
</tr>
<tr>
<td>6/18/2019</td>
<td>8.1</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
</tbody>
</table>
# Table of Contents

1 Introduction ......................................................................................... 6
   1.1 Glossary .................................................................................. 6
   1.2 References .............................................................................. 7
      1.2.1 Normative References .................................................... 7
      1.2.2 Informative References .................................................. 9
   1.3 Overview .................................................................................. 9
   1.4 Relationship to Other Protocols ............................................... 9
   1.5 Prerequisites/Preconditions ..................................................... 10
   1.6 Applicability Statement .......................................................... 10
   1.7 Versioning and Capability Negotiation ................................... 10
   1.8 Vendor-Extensible Fields ......................................................... 10
   1.9 Standards Assignments .......................................................... 10

2 Messages .......................................................................................... 11
   2.1 Transport .............................................................................. 11
   2.2 Common Message Syntax ...................................................... 11
      2.2.1 Namespaces ..................................................................... 11
      2.2.2 Messages ....................................................................... 12
         2.2.2.1 RST .......................................................................... 13
         2.2.2.2 RSTR ......................................................................... 13
            2.2.2.2.1 Security Element .................................................. 13
               2.2.2.2.1.1 Attribute Element ........................................... 13
                  2.2.2.2.1.1.1 AttributeName ............................................. 14
                  2.2.2.2.1.1.2 AttributeNamespace .................................... 14
                  2.2.2.2.1.1.3 OriginalIssuer ............................................. 14
                  2.2.2.2.1.1.4 AttributeValue .......................................... 14
      2.2.3 Elements .......................................................................... 18
      2.2.4 Complex Types .................................................................. 18
         2.2.4.1 ServiceContext (from namespace
               http://schemas.microsoft.com/sharepoint/servicecontext) .. 18
      2.2.5 Simple Types ................................................................... 18
      2.2.6 Attributes ........................................................................ 18
      2.2.7 Groups ............................................................................ 19
      2.2.8 Attribute Groups ............................................................ 19
      2.2.9 Common Data Structures ............................................... 19

3 Protocol Details .............................................................................. 20
   3.1 Server Details ......................................................................... 20
      3.1.1 Abstract Data Model ...................................................... 20
      3.1.2 Timers ............................................................................. 20
      3.1.3 Initialization ................................................................. 20
      3.1.4 Message Processing Events and Sequencing Rules ............ 20
      3.1.5 Timer Events ............................................................... 20
      3.1.6 Other Local Events ........................................................ 20
   3.2 Client Details .......................................................................... 20
      3.2.1 Abstract Data model ....................................................... 20
      3.2.2 Timers ............................................................................ 20
      3.2.3 Initialization ................................................................. 20
      3.2.4 Message Processing Events and Sequencing Rules ............ 21
      3.2.5 Timer Events ............................................................... 21
      3.2.6 Other Local Events ........................................................ 21

4 Protocol Examples ............................................................................ 22
   4.1 Security Token Request .......................................................... 22
   4.2 Security Token Containing a Compressed Sid Claim ................ 25
1 Introduction

The SharePoint Security Token Service Web Service Protocol defines restrictions for several related protocols and enables interoperability and authentication with Web services that are provided by protocol servers.

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

1.1 Glossary

This document uses the following terms:

authentication: The act of proving an identity to a server while providing key material that binds the identity to subsequent communications.

claim: A statement that one subject makes about itself or another subject. For example, the statement can be about a name, identity, key, group, privilege, or capability. Claims have a provider that issues them, and they are given one or more values. They are also defined by a claim value type and, possibly, associated metadata.

claim type: A statement that is part of a claim and provides context for a claim value. It represents the type of claim and is typically a Uniform Resource Identifier (URI). Examples include FirstName and Role.

claim value: A string that represents the value of a statement in a claim. It specifies what is being asserted by a claim.

culture name: A part of a language identification tagging system, as described in [RFC1766]. Culture names adhere to the format "<languagecode2>-<country/regioncode2>." If a two-letter language code is not available, a three-letter code that is derived from [ISO-639] is used.

group object: A database object that represents a collection of user and group objects and has a security identifier (SID) value.

request identifier: A GUID that is used to identify a specific action or procedure that is sent to a protocol server or a protocol client.

security identifier (SID): An identifier for security principals that is used to identify an account or a group. Conceptually, the SID is composed of an account authority portion (typically a domain) and a smaller integer representing an identity relative to the account authority, termed the relative identifier (RID). The SID format is specified in [MS-DTYP] section 2.4.2; a string representation of SIDs is specified in [MS-DTYP] section 2.4.2 and [MS-AZOD] section 1.1.1.2.

security token service (STS): A web service that issues claims and packages them in encrypted security tokens.

site subscription: A logical grouping of site collections that share a common set of features and service data.

site subscription identifier: A GUID that is used to identify a site subscription.

SOAP message: An XML document consisting of a mandatory SOAP envelope, an optional SOAP header, and a mandatory SOAP body. See [SOAP1.2-1/2007] section 5 for more information.

Uniform Resource Identifier (URI): A string that identifies a resource. The URI is an addressing mechanism defined in Internet Engineering Task Force (IETF) Uniform Resource Identifier (URI): Generic Syntax [RFC3986].
Web Services Description Language (WSDL): An XML format for describing network services as a set of endpoints that operate on messages that contain either document-oriented or procedure-oriented information. The operations and messages are described abstractly and are bound to a concrete network protocol and message format in order to define an endpoint. Related concrete endpoints are combined into abstract endpoints, which describe a network service. WSDL is extensible, which allows the description of endpoints and their messages regardless of the message formats or network protocols that are used.

WSDL message: An abstract, typed definition of the data that is communicated during a WSDL operation [WSDL]. Also, an element that describes the data being exchanged between web service providers and clients.

XML schema: A description of a type of XML document that is typically expressed in terms of constraints on the structure and content of documents of that type, in addition to the basic syntax constraints that are imposed by XML itself. An XML schema provides a view of a document type at a relatively high level of abstraction.

MAY, SHOULD, MUST NOT, MUST NOT: These terms (in all caps) are used as defined in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the Errata.

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information.


1.2.2 Informative References

[MS-OFBA] Microsoft Corporation, "Office Forms Based Authentication Protocol".

1.3 Overview

This protocol specifies restrictions for a set of protocols and provides clarifications that enable interoperability when invoking Web services that are provided by the protocol server. See section 1.2 of this document for the references of the related protocols. This protocol and the related protocols can be used by protocol clients and protocol servers to implement authentication.

This protocol uses the model described in [WSTrust] and restricts messages as described in [SAMLCore].

In addition, this protocol relies on several underlying protocols. The exchanged messages are based on SOAP, as described in [SOAP1.1] and [SOAP1.2-1/2007], over XML, as described in [XML]. This protocol also requires a transport. This document does not specify which transport to use. However, this protocol does depend on the transport to help provide message integrity and protection.

For NTLM authentication, this protocol refers to the [MS-TNAP] protocol specification, which describes the NTLM authentication method.

1.4 Relationship to Other Protocols

Other than the normative references this protocol doesn’t use any other protocols.

1.5 Prerequisites/Preconditions

Clients that need to request a SharePoint token SHOULD use the following endpoints:

- To request a token using Windows as an authentication method with a security token service (STS), the endpoint URL is exposed through the site URL under http[s]://host:port/site/_vti_bin/sts/spsecuritytokenservice.svc/windows
  - NTLM authentication is out of scope of this document and is described in [MS-TNAP].

- To request a token using an authenticated session cookie as a method of authentication with an STS, the endpoint URL is exposed through the site URL under http[s]://host:port/site/_vti_bin/sts/spsecuritytokenservice.svc/cookie
To use the STS Windows endpoint, the web application that hosts the site is required to have NTLM authentication enabled.

To use an STS cookie endpoint, the web application that hosts the site is required to have forms-based authentication enabled.

The authenticated session cookie has to be requested, as specified in the [MS-OFBA] protocol standard.

When a SAML token is presented to SharePoint for the purposes of authenticating, the token conforms to the [SAMLCore] specification, uses the [WSFederation] protocol standard and follows the [WSTrust1.4] protocol.

In the server scenarios, SharePoint services consumers request the tokens from the local computer STS via the SharePoint object model. No endpoint is used, although this document describes the token that the local computer STS creates to access SharePoint services.

The transport protocol has to use TCP.

### 1.6 Applicability Statement

This protocol is applicable when interoperability with Web service implementations provided by the protocol server require both claims based authentication and to interoperate with external web services configured to use [WSFederation] with SharePoint.

### 1.7 Versioning and Capability Negotiation

None.

### 1.8 Vendor-Extensible Fields

None.

### 1.9 Standards Assignments

None.
2 Messages

2.1 Transport

This document does not define how SOAP messages are transmitted over a network. However, this protocol does depend on a transport to help protect messages. Refer to section 3 for more information about the security of the messages.

2.2 Common Message Syntax

This section contains common definitions that are used by this protocol. The syntax of the definitions uses XML schema, as specified in [XMLSCHEMA1/2] and [XMLSCHEMA2/2], and WSDL, as specified in [WSDL].

2.2.1 Namespaces

The following namespaces are defined by this document. These namespaces are used to identify the claim types created by the STS.

  - Prefix: spuid
  - Description: URI for the user’s unique identifier claim type.
  - Prefix: spuln
  - Description: URI for the user logon name claim type.
  - Prefix: spip
  - Description: URI for the identity provider claim type.
  - Prefix: spdl
  - Description: URI for the distribution list security identifier (SID) claim type.
  - Prefix: spfid
  - Description: URI for the farm identifier claim type.
  - Prefix: sppsid
  - Description: URI for the process identity SID claim type.
  - Prefix: sppln
- **Description:** URI for the process logon name claim type.

This specification defines and references various XML namespaces using the mechanisms specified in [XMLNS]. Although this specification associates a specific XML namespace prefix for each XML namespace that is used, the choice of any particular XML namespace prefix is implementation-specific and not significant for interoperability.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Namespace URI</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>trust</td>
<td><a href="http://docs.oasis-open.org/ws-sx/ws-trust/200512">http://docs.oasis-open.org/ws-sx/ws-trust/200512</a></td>
<td>[WSTrust1.4]</td>
</tr>
<tr>
<td>wsdl</td>
<td><a href="http://schemas.xmlsoap.org/wsd/">http://schemas.xmlsoap.org/wsd/</a></td>
<td>[WSDL]</td>
</tr>
<tr>
<td>xsd</td>
<td><a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a></td>
<td>[XMLSCHEMA1/2] [XMLSCHEMA2/2]</td>
</tr>
<tr>
<td>soapenc</td>
<td><a href="http://schemas.xmlsoap.org/soap/encoding/">http://schemas.xmlsoap.org/soap/encoding/</a></td>
<td>[SOAP1.1]</td>
</tr>
<tr>
<td>soap</td>
<td><a href="http://schemas.xmlsoap.org/wsd/soap/">http://schemas.xmlsoap.org/wsd/soap/</a></td>
<td>[SOAP1.1]</td>
</tr>
<tr>
<td>tns</td>
<td><a href="http://tempuri.org/">http://tempuri.org/</a></td>
<td></td>
</tr>
<tr>
<td>wsam</td>
<td><a href="http://www.w3.org/2007/05/addressing/metadata">http://www.w3.org/2007/05/addressing/metadata</a></td>
<td>[WSADDR-Metadata]</td>
</tr>
<tr>
<td>soap12</td>
<td><a href="http://schemas.xmlsoap.org/wsd/soap12/">http://schemas.xmlsoap.org/wsd/soap12/</a></td>
<td>[SOAP1.2-1/2007] [SOAP1.2-2/2007]</td>
</tr>
<tr>
<td>wsa10</td>
<td><a href="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing</a></td>
<td>[WSA10]</td>
</tr>
<tr>
<td>wsaw</td>
<td><a href="http://www.w3.org/2006/05/addressing/wsd/">http://www.w3.org/2006/05/addressing/wsd/</a></td>
<td>[WSADDRCORE]</td>
</tr>
<tr>
<td>i0</td>
<td><a href="http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice">http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice</a></td>
<td></td>
</tr>
<tr>
<td>wsu</td>
<td><a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecol-utility-1.0.xsd">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecol-utility-1.0.xsd</a></td>
<td>[WSS]</td>
</tr>
</tbody>
</table>

### 2.2.2 Messages

This section defines restrictions to SOAP extensions, as specified for the [WSS], [WSFederation], [WSTrust], and [SAMLCore]. This section contains two subsections. Section 2.2.2.1 specifies restrictions on RequestSecurityToken (RST) messages, as specified in [WSTrust], [WSSC], and [WSSC1.3]. Section 2.2.2.2 specifies restrictions on RequestSecurityTokenResponse (RSTR) messages, as specified in [WSTrust], [WSSC], and [WSSC1.3].

This document considers [WSSE 1.0], [WSS], [BSP], [WSSC], [WSSC1.3] and [SAMLCore] to be normative, unless otherwise specified in sections 2.2.2.1 and 2.2.2.2 of this document. <1>
2.2.2.1 RST

WS-Trust specifies the framework for requesting and returning security tokens using RequestSecurityToken (RST) and RequestSecurityTokenResponse (RSTR) messages. An RST message provides the means for requesting a security token from a security token service (STS) or a protocol server (as defined in [WSS]). It has an extensible format (as defined in [WSFederation]) that allows the protocol client to specify a range of parameters that the security token MUST satisfy.

The body of an RST message MUST contain exactly one RequestSecurityToken element, as specified in [WSTrust] sections 3, 5.1, and 6.1.

The AppliesTo element (as defined in [WS-Trust1.3]) MUST be used.

The RequestSecurityToken element MUST NOT be signed.

2.2.2.2 RSTR

A RequestSecurityTokenResponse (RSTR) message returns a token in response to a request from a protocol client. The requested token and supporting state are returned by the protocol server without any intermediate exchanges of trust messages.

The RSTR message body MUST contain exactly one RequestSecurityTokenResponse element, as specified in [WS-Trust1.3] sections 3.2 and 4.4.

The RequestSecurityTokenResponse element MUST be contained in a RequestSecurityTokenResponseCollection element, as specified in [WS-Trust1.3] section 4.3. The RequestSecurityTokenResponseCollection element MUST NOT contain more than one RequestSecurityTokenResponse element.

The RequestedSecurityToken element MUST contain one or more SAML (Security Assertion Markup Language) security assertion.

The RequestedSecurityToken element MUST contain a saml:AuthenticationStatement Assertion as defined in [SAMLCore] with a Subject element that specify the principal that is the subject of the statement. It MUST contain one NameIdentifier element as defined in [SAMLCore] section 2.4.2.2. The principal specified in the NameIdentifier assertion MUST be equal to the claim specified by an administrator as an user identity claim, as specified in section 2.2.1.

2.2.2.2.1 Security Element

The Security element is specified in [WSSE 1.0] section 5, [WSS] section 5, and [BSP] section 5. It is a container element that is used when adding or verifying authentication for a protocol client. The element binds a user's proof of authentication, in the form of tokens and signatures, to a SOAP message.

The Security element, when it is used to add authentication data to a SOAP request message, consists of a combination of child elements. It MUST contain only one Assertion element, as defined in [WSSE 1.0] section 5. It MUST also contain zero, one, or multiple Attribute elements.

2.2.2.2.1.1 Attribute Element

The Attribute element is specified in [SAMLCore] section 2.4.4. The Attribute element MUST contain the following attributes and elements:

- An AttributeName attribute, as specified in [SAMLCore] section 2.4.4.1 and section 2.2.2.1.1.1 of this document.
- An AttributeNamespace attribute, as specified in [SAMLCore] section 2.4.4.1 and section 2.2.2.1.1.2 of this document.
- An **AttributeValue** element, as specified in [SAMLCore] section 2.4.4.1 and section 2.2.2.1.1.4 of this document.
- An **OriginalIssuer** attribute, as specified in section 2.2.2.1.1.3 of this document.

### 2.2.2.2.1.1.1 AttributeName

The value of the **AttributeName** attribute MUST be an identifier that uniquely identifies the user.

### 2.2.2.2.1.1.2 AttributeNamespace

The value of the **AttributeNamespace** attribute MUST be "http://schemas.microsoft.com/sharepoint/2009/08/claims".

### 2.2.2.2.1.1.3 OriginalIssuer

All the claim assertions made about the user MUST contain an **OriginalIssuer** attribute.

The value of the **OriginalIssuer** attribute MUST be one of the values specified in the following table:

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>&quot;windows&quot;</td>
</tr>
<tr>
<td>Trusted Security Token Service</td>
<td>&quot;TrustedProvider:&quot; + STS name, where STS name is defined by an administrator when setting up the trust.</td>
</tr>
<tr>
<td>Claim Provider</td>
<td>&quot;ClaimProvider:&quot; + Name of claim provider, where name is defined by the administrator when registering the claim provider.</td>
</tr>
<tr>
<td>Forms Based Authentication</td>
<td>&quot;Forms:&quot; + Name of the membership provider or name of the role provider, where name is defined by the administrator when configuring forms based authentication identity provider.</td>
</tr>
<tr>
<td>Security Token Service</td>
<td>&quot;SecurityTokenService&quot;</td>
</tr>
</tbody>
</table>

The XML namespace for the **OriginalIssuer** attribute MUST be "http://schemas.microsoft.com/ws/2008/06/identity".

### 2.2.2.2.1.1.4 AttributeValue

The **AttributeValue** element is encoded as follows:

- Character 1 MUST be "i" for an identity **claim** (unique identifier for a user) or "c" for all other claims.
- Character 2 MUST be ":" (colon).
- Character 3 MUST be "0" (zero).
- Character 4 MUST be the encoded character for the **claim type**. The claim type **URIs** and their encoded characters are specified in the following table:

<table>
<thead>
<tr>
<th>Claim type URI</th>
<th>Encoded character</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;<a href="http://schemas.microsoft.com/sharepoint/2009/08/claims/audienceid">http://schemas.microsoft.com/sharepoint/2009/08/claims/audienceid</a>&quot;</td>
<td>&quot;0&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.microsoft.com/sharepoint/2009/08/claims/organizationid">http://schemas.microsoft.com/sharepoint/2009/08/claims/organizationid</a>&quot;</td>
<td>&quot;1&quot;</td>
</tr>
<tr>
<td>Claim type URI</td>
<td>Encoded character</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider">http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider</a>&quot;</td>
<td>&quot;!&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.microsoft.com/sharepoint/2009/08/claims/distributionlistsid">http://schemas.microsoft.com/sharepoint/2009/08/claims/distributionlistsid</a>&quot;</td>
<td>&quot;$&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://sharepoint.microsoft.com/claims/2009/01/windowstoken/processid">http://sharepoint.microsoft.com/claims/2009/01/windowstoken/processid</a>&quot;</td>
<td>&quot;B&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://sharepoint.microsoft.com/claims/2009/01/windowstoken/processid">http://sharepoint.microsoft.com/claims/2009/01/windowstoken/processid</a>&quot;</td>
<td>&quot;C&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.microsoft.com/sharepoint/2009/08/claims/provideruserkey">http://schemas.microsoft.com/sharepoint/2009/08/claims/provideruserkey</a>&quot;</td>
<td>&quot;h&quot;</td>
</tr>
<tr>
<td>IDFX and service model claim type URIs</td>
<td></td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid">http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid</a>&quot;</td>
<td>&quot;)&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid">http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid</a>&quot;</td>
<td>&quot;***&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid">http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid</a>&quot;</td>
<td>&quot;+&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.microsoft.com/ws/2008/06/identity/claims/role">http://schemas.microsoft.com/ws/2008/06/identity/claims/role</a>&quot;</td>
<td>&quot;+&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/anonymous">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/anonymous</a>&quot;</td>
<td>&quot;:.&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication</a>&quot;</td>
<td>&quot;/&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecision">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecision</a>&quot;</td>
<td>&quot;0&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country</a>&quot;</td>
<td>&quot;:1&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth</a>&quot;</td>
<td>&quot;:2&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid</a>&quot;</td>
<td>&quot;:3&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns</a>&quot;</td>
<td>&quot;:4&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a>&quot;</td>
<td>&quot;:5&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/gender">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/gender</a>&quot;</td>
<td>&quot;:6&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a>&quot;</td>
<td>&quot;:7&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/hash">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/hash</a>&quot;</td>
<td>&quot;:8&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/homephone">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/homephone</a>&quot;</td>
<td>&quot;:9&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality</a>&quot;</td>
<td>&quot;:&lt;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone</a>&quot;</td>
<td>&quot;:=&quot;</td>
</tr>
</tbody>
</table>
### Claim type URI

<table>
<thead>
<tr>
<th>Claim type URI</th>
<th>Encoded character</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a>&quot;</td>
<td>&quot;&gt;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</a>&quot;</td>
<td>&quot;)&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone</a>&quot;</td>
<td>@&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode</a>&quot;</td>
<td>&quot;}&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier</a>&quot;</td>
<td>&quot;)&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone</a>&quot;</td>
<td>@&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone</a>&quot;</td>
<td>@&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/spn">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/spn</a>&quot;</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince</a>&quot;</td>
<td>&quot;)&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress</a>&quot;</td>
<td>&quot;a&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</a>&quot;</td>
<td>&quot;b&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/system">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/system</a>&quot;</td>
<td>&quot;c&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprint">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprint</a>&quot;</td>
<td>&quot;d&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn</a>&quot;</td>
<td>&quot;e&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/webpage">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/webpage</a>&quot;</td>
<td>&quot;f&quot;</td>
</tr>
</tbody>
</table>

- Character 5 MUST be the encoded character for claim value type. The claim value types and their encoded characters are specified in the following table:

### Claim value type URI

<table>
<thead>
<tr>
<th>Claim value type URI</th>
<th>Encoded character</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;<a href="http://www.w3.org/2001/XMLSchema#base64Binary">http://www.w3.org/2001/XMLSchema#base64Binary</a>&quot;</td>
<td>&quot;)&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/2001/XMLSchema#boolean">http://www.w3.org/2001/XMLSchema#boolean</a>&quot;</td>
<td>&quot;)&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/2001/XMLSchema#date">http://www.w3.org/2001/XMLSchema#date</a>&quot;</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/2001/XMLSchema#dateTime">http://www.w3.org/2001/XMLSchema#dateTime</a>&quot;</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/TR/2002/WD-xquery-operators-20020816#dayTimeDuration">http://www.w3.org/TR/2002/WD-xquery-operators-20020816#dayTimeDuration</a>&quot;</td>
<td>&quot;)&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/2001/XMLSchema#double">http://www.w3.org/2001/XMLSchema#double</a>&quot;</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/2001/XMLSchema#hexBinary">http://www.w3.org/2001/XMLSchema#hexBinary</a>&quot;</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/2001/XMLSchema#integer">http://www.w3.org/2001/XMLSchema#integer</a>&quot;</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/2000/09/xmldsig#KeyInfo">http://www.w3.org/2000/09/xmldsig#KeyInfo</a>&quot;</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/2000/09/xmldsig#RSAKeyValue">http://www.w3.org/2000/09/xmldsig#RSAKeyValue</a>&quot;</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/2000/09/xmldsig#DSAKeyValue">http://www.w3.org/2000/09/xmldsig#DSAKeyValue</a>&quot;</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>&quot;<a href="http://www.w3.org/2001/XMLSchema#string">http://www.w3.org/2001/XMLSchema#string</a>&quot;</td>
<td>&quot;&quot;</td>
</tr>
</tbody>
</table>
Claim value type URI | Encoded character
---|---
"http://www.w3.org/2001/XMLSchema#time" | "/" 
"http://www.w3.org/TR/2002/WD-xquery-operators-20020816#yearMonthDuration" | "1" 
X500Name | "0" 
Rfc822Name | "+" 

- Character 6 MUST be "w", "f", "t", "p", "s", or "c". This character represents the encoded original issuer. The list of provider types is specified in the following table:

<table>
<thead>
<tr>
<th>Original issuer</th>
<th>Encoded character</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>&quot;w&quot;</td>
</tr>
<tr>
<td>Forms based authentication</td>
<td>&quot;f&quot;</td>
</tr>
<tr>
<td>Trusted STS</td>
<td>&quot;t&quot;</td>
</tr>
<tr>
<td>Personal InfoCard</td>
<td>&quot;p&quot;</td>
</tr>
<tr>
<td>Local STS</td>
<td>&quot;s&quot;</td>
</tr>
<tr>
<td>Claim provider</td>
<td>&quot;c&quot;</td>
</tr>
</tbody>
</table>

- If the original issuer is not Windows or the local STS, the next character MUST be "|" (pipe), then the name of the original issuer MUST begin at this point. If the original issuer is Windows or local STS, there MUST NOT be any character.

- If the identity provider is not Windows or local STS, the next character MUST be "|" (pipe). If the identity provider is Windows or local STS, there MUST NOT be any character.

- Next character after "|" - This character MUST be the claim value. If the claim is encoded, as described at the beginning of this section, then the casing for encoded claims MUST be lower and invariant culture,
  - upper case MUST NOT be used.
  - Claim value, Provider type and original issuer are not case sensitive.
  - Characters %, :, ;, | MUST be HTML encoded.

The preceding encoded strings have the following restrictions:

- Characters 1 through 5 are case-sensitive.
- Claim value, provider type, and original issuer are not case-sensitive.

These restrictions apply only to the encoded claims string. Non-encoded claims are not case sensitive. The total length of the claim value MUST NOT exceed 255 characters.

In the SAML token, the casing for the claim value of the claim type NameIdentifier MUST be lower and invariant culture. This claim MUST be on the header of the SAML token as specified by the [SAMLToken1.1].
All tokens issued for SharePoint MUST contain one FarmId claims with the SharePoint farm identifier for which the token was issued.

### 2.2.3 Elements

This specification does not define any common XML schema element definitions.

### 2.2.4 Complex Types

The following table summarizes the set of common XML schema complex type definitions defined by this specification. XML schema complex type definitions that are specific to a particular operation are described with the operation.

<table>
<thead>
<tr>
<th>Complex type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceContext</td>
<td>Common properties that are sent with a web service request.</td>
</tr>
</tbody>
</table>

#### 2.2.4.1 ServiceContext (from namespace http://schemas.microsoft.com/sharepoint/servicecontext)

The ServiceContext element specifies common properties that are sent with a web service request.

```xml
<xs:element name="ServiceContext">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="correlationId" minOccurs="1" maxOccurs="1"
      type="q13:guid"/>
      <xs:element name="language" minOccurs="1" maxOccurs="1" type="xs:string"/>
      <xs:element name="region" minOccurs="1" maxOccurs="1" type="xs:string"/>
      <xs:element name="siteSubscriptionId" minOccurs="1" maxOccurs="1"
      type="q14:guid"/>
      <xs:attribute name="nil" type="xs:string" use="optional" fixed="true" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

correlationId: The request identifier for the current request.

language: The culture name that corresponds to the language used by the request.

region: The culture name that corresponds to the regional settings used by the request.

siteSubscriptionId: A site subscription identifier that corresponds to the site that the request originated from. If the site does not have a site subscription, the nil attribute MUST be specified.

#### 2.2.5 Simple Types

This specification does not define any common XML schema simple type definitions.

#### 2.2.6 Attributes

This specification does not define any common XML schema attribute definitions.
2.2.7 Groups
This specification does not define any common XML schema group definitions.

2.2.8 Attribute Groups
This specification does not define any common XML schema attribute group definitions.

2.2.9 Common Data Structures
This specification does not define any common XML schema data structures.
3 Protocol Details

The protocol details for the messages defined in section 2.2.2.1 of this document are specified in [WSSE 1.0], [WSS], [SAMLCore], [SAMLToken1.1], [BSP], [WSSC], and [WSSC1.3]. The protocol details for the messages defined in section 2.2.2.2 of this document are specified in [WS-Trust1.3], [WSSC], [WSFederation], and [WSSC1.3]. This document does not specify any unique protocols.

The protocol described in this document implements only one of the operations defined in [WS-Trust1.3] as specified in section 3.1.4 of this document.

3.1 Server Details

3.1.1 Abstract Data Model

None.

3.1.2 Timers

None.

3.1.3 Initialization

None.

3.1.4 Message Processing Events and Sequencing Rules

This protocol only implements the Issuance Binding operation as defined in [WS-Trust1.3]. It provides abstract methods of Cancel, Renew, and Validate binding operations.

3.1.5 Timer Events

None.

3.1.6 Other Local Events

None.

3.2 Client Details

3.2.1 Abstract Data model

None.

3.2.2 Timers

None.

3.2.3 Initialization

None.
3.2.4 Message Processing Events and Sequencing Rules

Group SID (Security Identifier) claims MUST be compressed in the issued tokens, see the following for details of the compression algorithm.

Claim is defined in [WSFederation] specification’s terminology section and Group SID is a SID that identifies a group object.

To calculate the Transformed SID from a GroupSidClaim, replace the last instance of the character '-' (dash) with the character ';' (semi-colon).

For each set S of GroupSidClaim claims that share an Original Issuer replace those claims with a new claim, constructed as follows:

2. Claim value type set to "group claim value type"
3. Original Issuer set to the Original Issuer that are common to Set S
4. Claim value set to a semi-colon-separated list of Transformed SIDs for each claim in Set S.

The term Original Issuer refers to the name of the security token service (STS) that issued these claims.

For each set S of GroupSidClaim claims that group by domain SID, use the character '|' (vertical bar) to separate them.

When receiving a token with compressed group SID claim, the opposite process MUST be used to build the original claim set that stores one group SID per claim.

3.2.5 Timer Events

None.

3.2.6 Other Local Events

None.
4 Protocol Examples

4.1 Security Token Request

In this example, the protocol client requests a security token from the protocol server using a username and password combination. Consider the following WSDL message which is sent by the protocol client:

```xml
<HttpRequest>
  <Method>POST</Method>
  <QueryString></QueryString>
  <WebHeaders>
    <Content-Length>1346</Content-Length>
    <Content-Type>application/soap+xml</Content-Type>
    <Authorization>Negotiate TlRMTVNTUAADAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAAAAAACy4YAcchAA AAPk9ylts:e1913CqHBN13Nw==</Authorization>
    <Expect>100-continue</Expect>
    <Host=localhost:32843</Host>
  </WebHeaders>
</HttpRequest>

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope">
  <s:Header>
    <a:MessageID>urn:uuid:0c9b2158-be51-4222-afa8-b55036b5a6df</a:MessageID>
    <a:ReplyTo>
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1">http://localhost:32843/SecurityTokenServiceApplication/securitytoken.svc</a:To>
  </s:Header>
  <s:Body>
        <a:Address>http://server.example.com/</a:Address>
      </wsp:AppliesTo>
      <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</trust:KeyType>
      <trust:OnBehalfOf>
          <Username>0#.f|ldapmembershipprovider|user1</Username>
          <Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">0#.f|ldapmembershipprovider|user1,129091469640504627,mOUexpCMZkX024dk2g7wQ z1LSDL7Yn6P565muzDmgv91joxTaApxpDQ4AD1M12CC8F5peY6ewnVDoJbotje/26JocdcY+TNDPe3ycV3aQKa0qEx k72zzmT5T3/QFZLB6oL58 OgAg7yA7evUann90agUXYfj8Fs80P5S2vpXWx3ped3N992J2bXaO1F1VQ2yhk8a/44KyvAs NTHk012tuOFwI+wEn9HYSRaQK7CYvQ96yFZzsw3pKvHmBH6TuF7C70bMC9GC4fPd6p1R5s1F4NDnR2pN66Io0LosUj7 6oDVgyfz/aTOs91iyrvCFQoV8tXqdySt31kg91aIQ==</Password>
        </UsernameToken>
      </trust:OnBehalfOf>
      <trust:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</trust:RequestType>
    </trust:RequestSecurityToken>
  </s:Body>
</s:Envelope>
```
The protocol server responds with a Security Token Response that matches the user requested. Consider the following WSDL message which contains this response:

```xml
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns="http://www.w3.org/2003/05/soap-envelope">
  <s:Header>
    <a:Action s:mustUnderstand="1">http://docs.oasis-open.org/ws-
trust/200512/RSTRC/IssueFinal</a:Action>
    <ActivityId CorrelationId="f1d13f52-af2c-46dd-9f73-67b6ef08543"
xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">00d96a84-2caaa45bb-
bb11-e843e2197471</ActivityId>
  </s:Header>
  <s:Body>
    <trust:RequestSecurityTokenResponseCollection
xmlns:trust="http://docs.oasis-
open.org/wss/ws-trust/200512">
      <trust:RequestSecurityTokenResponse>
        <trust:Lifetime>
          <wsu:Created xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd">2010-
01-28T00:19:34.264Z</wsu:Created>
          <wsu:Expires xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd">2010-
01-28T10:19:34.264Z</wsu:Expires>
        </trust:Lifetime>
          <a:EndpointReference>
            <a:Address>http://server.example.com/</a:Address>
          </a:EndpointReference>
        </wsp:AppliesTo>
        <trust:RequestedSecurityToken>
          <saml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="_40e2d2b1-6da1-46bc-
9a2c-769c03d21d32" Issuer="SharePoint" IssueInstant="2010-01-28T00:19:34.315Z"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
            <saml:Conditions NotBefore="2010-01-28T00:19:34.264Z" NotOnOrAfter="2010-01-
28T10:19:34.264Z">
              <saml:AudienceRestrictionCondition>
                <saml:Audience
http://server.example.com/</saml:Audience>
              </saml:AudienceRestrictionCondition>
            </saml:Conditions>
            <saml:AttributeStatement>
              <saml:Subject>
                <saml:NameIdentifier>user1</saml:NameIdentifier>
                <saml:SubjectConfirmation>
                  <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>
                </saml:SubjectConfirmation>
                <s:Attribute Name="role"
Namespace="http://schemas.microsoft.com/ws/2008/06/identity/claims"/>
                <s:Attribute Name="userlogonname"
                <s:Attribute Name="userid"
                <s:Attribute Name="name"
Namespace="http://schemas.microsoft.com/wss/2005/05/identity/claims"/>
              </s:Subject>
            </saml:AttributeStatement>
          </saml:Assertion>
        </trust:RequestedSecurityToken>
      </trust:RequestSecurityTokenResponse>
    </trust:RequestSecurityTokenResponseCollection>
  </s:Body>
</s:Envelope>
```
In the following example, the protocol client issues a RequestSecurityToken request for a user who has GroupSidClaims. Consider the following WSDL message for this request:

```xml
<HttpRequest>
  <Method>POST</Method>
  <QueryString/>
  <WebHeaders>
    <Content-Length>510</Content-Length>
    <Content-Type>application/soap+xml</Content-Type>
    <Authorization>Negotiate TlRMTVNTUAADAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAANcKY4gYAhcAA
      AP4dX8Niq7yPVRkkRs9JHMbw==</Authorization>
    <Expect>100-continue</Expect>
    <Host>localhost:32843</Host>
  </WebHeaders>
</HttpRequest>

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <trust:RequestedSecurityToken xmlns:trust="urn:oasis:names:tc:SAML:2.0:protocol">
      <trust:RequestedAttachedReference/>
      <trust:RequestedUnattachedReference/>
      <trust:TokenType>urn:oasis:names:tc:SAML:1.0:assertion</trust:TokenType>
      <trust:RequestType>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd</trust:RequestType>
      <trust:KeyType>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd</trust:KeyType>
      <trust:RequestSecurityTokenResponseCollection/>
    </trust:RequestedSecurityToken>
  </s:Header>
  <s:Body>
  </s:Body>
</s:Envelope>
```

### 4.2 Security Token Containing a Compressed Sid Claim

In the following example, the protocol client issues a RequestSecurityToken request for a user who has GroupSidClaims. Consider the following WSDL message for this request:

```xml
<HttpRequest>
  <Method>POST</Method>
  <QueryString/>
  <WebHeaders>
    <Content-Length>510</Content-Length>
    <Content-Type>application/soap+xml</Content-Type>
    <Authorization>Negotiate TlRMTVNTUAADAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAANcKY4gYAhcAA
      AP4dX8Niq7yPVRkkRs9JHMbw==</Authorization>
    <Expect>100-continue</Expect>
    <Host>localhost:32843</Host>
  </WebHeaders>
</HttpRequest>

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <trust:RequestedSecurityToken xmlns:trust="urn:oasis:names:tc:SAML:2.0:protocol">
      <trust:RequestedAttachedReference/>
      <trust:RequestedUnattachedReference/>
      <trust:TokenType>urn:oasis:names:tc:SAML:1.0:assertion</trust:TokenType>
      <trust:RequestType>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd</trust:RequestType>
      <trust:KeyType>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd</trust:KeyType>
      <trust:RequestSecurityTokenResponseCollection/>
    </trust:RequestedSecurityToken>
  </s:Header>
  <s:Body>
  </s:Body>
</s:Envelope>
```
The protocol server responds with the following RequestSecurityTokenResponse. This response contains an example of GroupSidClaims.

```xml
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope">
  <s:Header>
    <a:Action s:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</a:Action>
    <a:MessageID>urn:uuid:f1ff81d7-3e43-43f4-b7fc-b5fa6d6d8dc5</a:MessageID>
    <a:ReplyTo>
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1">http://localhost:32843/SecurityTokenServiceApplication/securitytoken.svc</a:To>
  </s:Header>
  <s:Body>
      <trust:RequestSecurityTokenResponse>
        <trust:Lifetime>
        </trust:Lifetime>
          <a:EndpointReference>
            <a:Address>https://server.example.com</a:Address>
          </a:EndpointReference>
        </wsp:AppliesTo>
        <trust:RequestedSecurityToken>
          <saml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="_667b495b-bd0a-486f-b1fd-a754730e0b4b" Issuer="SharePoint" IssueInstant="2010-02-05T17:41:25.444Z" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
            <saml:Conditions NotBefore="2010-02-05T17:41:24.310Z" NotOnOrAfter="2010-02-06T03:41:24.310Z">
              <saml:AudienceRestrictionCondition>
                <saml:Audience>https://server.example.com</saml:Audience>
              </saml:AudienceRestrictionCondition>
            </saml:Conditions>
            <saml:AttributeStatement>
              <saml:Subject>
                <saml:NameIdentifier>domain\user1</saml:NameIdentifier>
              </saml:Subject>
              <saml:SubjectConfirmation>
                <saml:Inference>http://www.w3.org/2001/04/xsysubjectassertion</saml:Inference>
              </saml:SubjectConfirmation>
            </saml:AttributeStatement>
          </saml:Assertion>
        </trust:RequestedSecurityToken>
      </trust:RequestSecurityTokenResponse>
      <trust:RequestSecurityTokenResponseCollection>
        <trust:RequestSecurityTokenResponse>
          <trust:Lifetime>
          </trust:Lifetime>
            <a:EndpointReference>
              <a:Address>https://server.example.com</a:Address>
            </a:EndpointReference>
          </wsp:AppliesTo>
          <trust:RequestedSecurityToken>
            <saml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="_667b495b-bd0a-486f-b1fd-a754730e0b4b" Issuer="SharePoint" IssueInstant="2010-02-05T17:41:25.444Z" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
              <saml:Conditions NotBefore="2010-02-05T17:41:24.310Z" NotOnOrAfter="2010-02-06T03:41:24.310Z">
                <saml:AudienceRestrictionCondition>
                  <saml:Audience>https://server.example.com</saml:Audience>
                </saml:AudienceRestrictionCondition>
              </saml:Conditions>
              <saml:AttributeStatement>
                <saml:Subject>
                  <saml:NameIdentifier>domain\user1</saml:NameIdentifier>
                </saml:Subject>
                <saml:SubjectConfirmation>
                  <saml:Inference>http://www.w3.org/2001/04/xsysubjectassertion</saml:Inference>
                </saml:SubjectConfirmation>
              </saml:AttributeStatement>
            </saml:Assertion>
          </trust:RequestedSecurityToken>
        </trust:RequestSecurityTokenResponse>
      </trust:RequestSecurityTokenResponseCollection>
    </trust:RequestSecurityTokenResponseCollection>
  </s:Body>
</s:Envelope>
```
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>

<saml:SubjectConfirmation>
  <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>
    <saml:AttributeValue>S-1-5-21-1217521184-1604012920-1887927527-66602</saml:AttributeValue>
  </saml:Attribute>
    <saml:AttributeValue>pkmacct@microsoft.com</saml:AttributeValue>
  </saml:Attribute>
    <saml:AttributeValue>DOMAIN\USER1</saml:AttributeValue>
  </saml:Attribute>
    <saml:AttributeValue>0#.w\domain\user1</saml:AttributeValue>
  </saml:Attribute>
    <saml:AttributeValue>0#.w\domain\user1</saml:AttributeValue>
  </saml:Attribute>
    <saml:AttributeValue>windows</saml:AttributeValue>
  </saml:Attribute>
    <saml:AttributeValue>True</saml:AttributeValue>
  </saml:Attribute>
    <saml:AttributeValue>1e5a76e4-7c6c-43b3-a5cf-a8e617962fc6</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute AttributeName="tokenreference" AttributeNamespace="http://sharepoint.microsoft.com/claims/2009/08">
    <saml:AttributeValue>0#.w\domain\user1,12909012852708179,czhRNuFWw79ko1B8tM6nUKLDhd5xYPnTN2S64uS5DTXQ1LEmNPqPwqwgRw0rbhlyNlcF0bC63Cghp9EZDa/12p1qXhFwC6h1xMFspQgLqpgmnpvuxZvSUCkYwB0QEoeYXK77l0XYLqGcMhXWmSri5j+74w2g816MuE30+FhbbV14g2kg/7MqGZ3Ey4hqExZ1OdB/HfzyZk18YQNWPet/9dUnV3ivsLho/wsOhxKSEhkuqaLlkkLMezFpsHdIJKN5mgPq3kD31+BIlaNzV3twXXr41JNKnLuf1IshaRoKmveWwsO2Y12l3A4FxVH/qbmpXlKWA==,https://server.example.com</saml:AttributeValue>
  </saml:Attribute>
    <saml:AttributeValue>0#.w\domain\user1</saml:AttributeValue>
  </saml:Attribute>
</saml:SubjectConfirmation>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:trust="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-protocol-1.0.xsd">
  <s:Body>
    <trust:RequestSecurityTokenResponseCollection>
      <trust:RequestSecurityTokenResponse>
        <trust:RequestedSecurityToken>
          <saml:Assertion />
          <trust:RequestedAttachedReference>
            <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
              <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID">_667b495b-bd0a-486f-b1fd-a754730e0b4b</o:KeyIdentifier>
            </o:SecurityTokenReference>
          </trust:RequestedAttachedReference>
          <trust:RequestedUnattachedReference>
            <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
              <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID">_667b495b-bd0a-486f-b1fd-a754730e0b4b</o:KeyIdentifier>
            </o:SecurityTokenReference>
          </trust:RequestedUnattachedReference>
        </trust:RequestedSecurityToken>
        <trust:TokenType>urn:oasis:names:tc:SAML:1.0:assertion</trust:TokenType>
        <trust:RequestType>http://docs.oasis-open.org/wss/sx/sst/200512/Issue</trust:RequestType>
        <trust:KeyType>http://docs.oasis-open.org/wss/sx/sst/200512/Bearer</trust:KeyType>
      </trust:RequestSecurityTokenResponse>
    </trust:RequestSecurityTokenResponseCollection>
  </s:Body>
</s:Envelope>
5 Security

5.1 Security Considerations for Implementers

Security assumptions and considerations for this protocol are specified in the following documents:

- [WSFederation] section 16
- [WSSC] section 11
- [WSSE 1.0] section 13
- [WSS] section 13
- [BSP] section 17
- [WSSKTP1.1] section 4
- [SAMLToken1.1] section 4
- [WSTrust] section 14
- [WS-Trust1.3] section 12
- [WSTrust1.4] section 12
- [WSSC1.3] section 10
- [MS-TNAP] section 5

Message integrity assumptions and considerations for this protocol are specified in following documents:

- [WS-Trust1.3] section 4.5
- [WSSP1.2-2012] section 4.1

Message confidentiality assumptions and considerations for this protocol are specified in following documents:

- [WSFederation] section 12
- [WSS] section 15

This protocol uses a range of cryptographic algorithms. Some of these algorithms can be considered weak depending on the security threats for specific usage scenarios. This specification neither classifies nor prescribes cryptographic algorithms for specific usage scenarios.

When implementing and using this protocol, one has to make every effort to ensure that the result is not vulnerable to any one of the wide range of attacks.

Encryption and message signing assumptions and considerations for this protocol are specified in the following documents:

- [WSS] section 8
- [WS-Trust1.3] sections 4.4 and 8.2 and 9.2

When selecting the encryption mechanism, the following restrictions have to be considered:

For SharePoint services SAML tokens, the following rules have to be followed:
The cryptographic algorithm for signing the SAML token header is required to be SHA1.

The cryptographic algorithm for signing the SAML token date value is required to be SHA256.

For external services SAML tokens, the following rules have to be followed:

- The cryptographic algorithm for signing the SAML token header is required to be SHA256.
- The cryptographic algorithm for signing the SAML token date value is required to be SHA256.

All tokens are required to not encrypt the message.

5.2 **Index of Security Parameters**

None.
6 Appendix A: Full WSDL

For ease of implementation, the full WSDL and schema is provided in this appendix.

```xml
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions targetNamespace="http://tempuri.org/
 xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/
 xmlns:soap="http://schemas.xmlsoap.org/soap/
 xmlns:tns="http://tempuri.org/
 xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
 xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/
 xmlns:wsa10="http://www.w3.org/2005/08/addressing"
 xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
 xmlns:i0="http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice"
 xmlns:xws="http://schemas.xmlsoap.org/soap/
 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
 wssecurity-utility-1.0.xsd"
 xmlns:trust="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
 trust/200512"
 wsp:Policy wsu:Id="AsymmetricWindowsHttp_policy">
 <wsp:ExactlyOne>
 <wsp:All>
 <sp:SymmetricBinding xmlns:sp="http://docs.oasis-open.org/ws-
 securitypolicy/200702">
 <wsp:Policy>
 <sp:ProtectionToken>
 <wsp:Policy>
 <sp:SpnegoContextToken sp:IncludeToken="http://docs.oasis-open.org/ws-
 securitypolicy/200702/IncludeToken/AlwaysToRecipient">
 <wsp:Policy>
 <sp:RequireDerivedKeys/>
 <sp:MustNotSendCancel/>
 <sp:MustNotSendAmend/>
 <sp:MustNotSendRenew/>
 </wsp:Policy>
 </sp:SpnegoContextToken>
 </wsp:Policy>
 </sp:ProtectionToken>
 <sp:AlgorithmSuite>
 <wsp:Policy>
 <sp:Basic256Sha256/>
 </wsp:Policy>
 </sp:AlgorithmSuite>
 <sp:Layout>
 <wsp:Policy>
 <sp:Strict/>
 </wsp:Policy>
 </sp:Layout>
 <sp:IncludeTimestamp/>
 <sp:EncryptSignature/>
 <sp:OnlySignEntireHeadersAndBody/>
 </wsp:Policy>
 </sp:SymmetricBinding>
 <sp:EndorsingSupportingTokens xmlns:sp="http://docs.oasis-open.org/ws-
 securitypolicy/200702">
 <wsp:Policy>
 <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-
 securitypolicy/200702/IncludeToken/AlwaysToRecipient" wsp:Optional="true"/>
 </wsp:Policy>
 </sp:EndorsingSupportingTokens>
 <sp:Ws11 xmlns:sp="http://docs.oasis-open.org/ws-
 securitypolicy/200702">
 <wsp:Policy>
 <sp:EndorsingSupportingTokens/>
 </wsp:Policy>
 </sp:Ws11>
</wsp:Policy>
</wsp:Policy>
</sp:Wss11>
</wsam:Addressing>
</wsdl:definitions>
```
<sp:Trust13 xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
  <sp:Policy>
    <sp:MustSupportIssuedTokens/>
    <sp:RequireClientEntropy/>
    <sp:RequireServerEntropy/>
  </sp:Policy>
</sp:Trust13>


<wsp:UsingAddressing/>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>

<wsp:Policy wsu:Id="AsymmetricWindowsHttp_Trust13Cancel_Input_policy">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:SignedParts xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <sp:Body/>
        <sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="FaultTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="ReplyTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="MessageID" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="RelatesTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="Action" Namespace="http://www.w3.org/2005/08/addressing"/>
      </sp:SignedParts>
      <sp:EncryptedParts xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <sp:Body/>
      </sp:EncryptedParts>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>

<wsp:Policy wsu:Id="AsymmetricWindowsHttp_Trust13Cancel_output_policy">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:SignedParts xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <sp:Body/>
        <sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="FaultTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="ReplyTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="MessageID" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="RelatesTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="Action" Namespace="http://www.w3.org/2005/08/addressing"/>
      </sp:SignedParts>
      <sp:EncryptedParts xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <sp:Body/>
      </sp:EncryptedParts>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>

<wsp:Policy wsu:Id="AsymmetricWindowsHttp_Trust13Issue_Input_policy">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:SignedParts xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <sp:Body/>
        <sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="FaultTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="ReplyTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="MessageID" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="RelatesTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="Action" Namespace="http://www.w3.org/2005/08/addressing"/>
      </sp:SignedParts>
      <sp:EncryptedParts xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <sp:Body/>
      </sp:EncryptedParts>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>

<wsp:Policy wsu:Id="AsymmetricWindowsHttp_Trust13Issue_output_policy">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:SignedParts xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <sp:Body/>
        <sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="FaultTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="ReplyTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="MessageID" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="RelatesTo" Namespace="http://www.w3.org/2005/08/addressing"/>
        <sp:Header Name="Action" Namespace="http://www.w3.org/2005/08/addressing"/>
      </sp:SignedParts>
      <sp:EncryptedParts xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <sp:Body/>
      </sp:EncryptedParts>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
<sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing"/>
<sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing"/>
<sp:Header Name="FaultTo" Namespace="http://www.w3.org/2005/08/addressing"/>
<sp:Header Name="ReplyTo" Namespace="http://www.w3.org/2005/08/addressing"/>
<sp:Header Name="MessageID" Namespace="http://www.w3.org/2005/08/addressing"/>
<sp:Header Name="RelatesTo" Namespace="http://www.w3.org/2005/08/addressing"/>
<sp:Header Name="Action" Namespace="http://www.w3.org/2005/08/addressing"/>
</sp:SignedParts>
</sp:EncryptedParts>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
<wsdl:types/>
<wsdl:binding name="AsymmetricWindowsHttp" type="i0:IWSTrust13Sync">
<wsp:PolicyReference URI="#AsymmetricWindowsHttp_policy"/>
<soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
</wsdl:binding>
<wsdl:operation name="Trust13Cancel">
<wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Cancel_Input_policy"/>
</wsdl:operation>
<wsdl:operation name="Trust13Issue">
<wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Issue_Input_policy"/>
</wsdl:operation>
<wsdl:operation name="Trust13Renew">
<wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Renew_Input_policy"/>
<wsdl:input>
  <wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Renew_Input_policy"/>
  <soap12:body use="literal"/>
</wsdl:input>
<wsdl:output>
  <wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Renew_output_policy"/>
  <soap12:body use="literal"/>
</wsdl:output>
</wsdl:operation>
<wsdl:operation name="Trust13Validate">
  <wsdl:input>
    <wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Validate_Input_policy"/>
    <soap12:body use="literal"/>
  </wsdl:input>
  <wsdl:output>
    <wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Validate_output_policy"/>
    <soap12:body use="literal"/>
  </wsdl:output>
</wsdl:operation>
</wsdl:binding>
</wsdl:definitions>
7 Appendix B: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include updates to those products.

- Microsoft Lync 2010
- Microsoft Lync Client 2013/Skype for Business
- Microsoft FAST Search Server 2010
- Microsoft Office 2010 suites
- Microsoft Office 2013
- Microsoft Search Server 2010
- Microsoft SharePoint Designer 2010
- Microsoft SharePoint Designer 2013
- Microsoft SharePoint Foundation 2010
- Microsoft SharePoint Foundation 2013
- Microsoft SharePoint Server 2010
- Microsoft SharePoint Server 2013
- Microsoft SharePoint Workspace 2010
- Microsoft Visio 2010
- Microsoft Visio 2013
- Microsoft Office 2016
- Microsoft Visio 2016
- Microsoft SharePoint Server 2016
- Microsoft Office 2019
- Microsoft SharePoint Server 2019
- Microsoft Visio 2019

Exceptions, if any, are noted in this section. If an update version, service pack or Knowledge Base (KB) number appears with a product name, the behavior changed in that update. The new behavior also applies to subsequent updates unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms "SHOULD" or "SHOULD NOT" implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term "MAY" implies that the product does not follow the prescription.

<1> Section 2.2.2: When authenticating to SharePoint Server 2010 with SAML 1.1 tokens, assumptions and considerations for this protocol are specified in the [WSFederation] document section 13.
8 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.
Index

A
Abstract data model
  client 20
  server 20
Applicability 10
Attribute groups 19
Attributes 18

C
Capability negotiation 10
Change tracking 38
Client
  abstract data model 20
  initialization 20
  local events 21
  message processing 21
  overview 20
  sequencing rules 21
  timer events 21
  timers 20
Common data structures 19
Complex types 18
  ServiceContext (from namespace
    http://schemas.microsoft.com/sharepoint/servicecontext) 18

D
Data model - abstract
  client 20
  server 20

E
Events
  local - client 21
  local - server 20
  timer - client 21
  timer - server 20
Examples
  security token containing a compressed Sid claim 25
  security token request 22

F
Fields - vendor-extensible 10
Full WSDL 32

G
Glossary 6
Groups 19

I
Implementer - security considerations 30
Index of security parameters 31
Informative references 9
Initialization

9

client 20
server 20

Introduction 6

L
Local events
  client 21
  server 20

M
Message processing
  client 21
  server 20
Messages
  attribute groups 19
  attributes 18
  common data structures 19
  complex types 18
  elements 18
  enumerated 12
  groups 19
  namespaces 11
  RST 13
  RST message 13
  RSTR 13
  RSTR message 13
  ServiceContext (from namespace
    http://schemas.microsoft.com/sharepoint/servicecontext) complex type 18
  simple types 18
  syntax 11
  transport 11

N
Namespaces 11
Normative references 7

P
Parameters - security index 31
Preconditions 9
Prerequisites 9
Product behavior 37
Protocol Details
  overview 20

R
References 7
  informative 9
  normative 7
Relationship to other protocols 9

S