

[MS-SPSTWS]: SharePoint Security Token Service Web Service Protocol Specification

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **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 may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft [Open Specification Promise](#) or the [Community Promise](#). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events 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 specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do 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 are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Preliminary Documentation. This Open Specification provides documentation for past and current releases and/or for the pre-release (beta) version of this technology. This Open Specification is final documentation for past or current releases as specifically noted in the document, as applicable; it is preliminary documentation for the pre-release (beta) versions. Microsoft will release final documentation in connection with the commercial release of the updated or new version of this technology. As the documentation may change between this preliminary version and the final version of this technology, there are risks in relying on preliminary documentation. To the extent that you incur additional development obligations or any other costs as a result of relying on this preliminary documentation, you do so at your own risk.

Revision Summary

Date	Revision History	Revision Class	Comments
07/13/2009	0.1	Major	Initial Availability
08/28/2009	0.2	Editorial	Revised and edited the technical content
11/06/2009	0.3	Editorial	Revised and edited the technical content
02/19/2010	1.0	Major	Updated and revised the technical content
03/31/2010	1.01	Major	Updated and revised the technical content
04/30/2010	1.02	Editorial	Revised and edited the technical content
06/07/2010	1.03	Editorial	Revised and edited the technical content
06/29/2010	1.04	Minor	Clarified the meaning of the technical content.
07/23/2010	1.04	No change	No changes to the meaning, language, or formatting of the technical content.
09/27/2010	1.04	No change	No changes to the meaning, language, or formatting of the technical content.
11/15/2010	1.04	No change	No changes to the meaning, language, or formatting of the technical content.
12/17/2010	1.04	No change	No changes to the meaning, language, or formatting of the technical content.
03/18/2011	1.04	No change	No changes to the meaning, language, or formatting of the technical content.
06/10/2011	1.04	No change	No changes to the meaning, language, or formatting of the technical content.
01/20/2012	1.5	Minor	Clarified the meaning of the technical content.
04/11/2012	1.5	No change	No changes to the meaning, language, or formatting of the technical content.
07/16/2012	1.5	No change	No changes to the meaning, language, or formatting of the technical content.

Date	Revision History	Revision Class	Comments
09/12/2012	1.5	No change	No changes to the meaning, language, or formatting of the technical content.

Preliminary

Table of Contents

1 Introduction	6
1.1 Glossary	6
1.2 References	6
1.2.1 Normative References	6
1.2.2 Informative References	8
1.3 Protocol Overview (Synopsis)	8
1.4 Relationship to Other Protocols	8
1.5 Prerequisites/Preconditions	8
1.6 Applicability Statement	9
1.7 Versioning and Capability Negotiation	9
1.8 Vendor-Extensible Fields	9
1.9 Standards Assignments	9
2 Messages	10
2.1 Transport	10
2.2 Common Message Syntax	10
2.2.1 Namespaces	10
2.2.2 Messages	11
2.2.2.1 RST	11
2.2.2.2 RSTR	11
2.2.3 Elements	12
2.2.4 Complex Types	12
2.2.4.1 ServiceContext (from namespace http://schemas.microsoft.com/sharepoint/servicecontext)	12
2.2.5 Simple Types	12
2.2.6 Attributes	13
2.2.7 Groups	13
2.2.8 Attribute Groups	13
2.2.9 Common Data Structures	13
3 Protocol Details	14
3.1 Server Details	14
3.1.1 Abstract Data Model	14
3.1.2 Timers	14
3.1.3 Initialization	14
3.1.4 Message Processing Events and Sequencing Rules	14
3.1.5 Timer Events	14
3.1.6 Other Local Events	14
3.2 Client Details	14
3.2.1 Abstract Data model	14
3.2.2 Timers	14
3.2.3 Initialization	14
3.2.4 Message Processing Events and Sequencing Rules	15
3.2.5 Timer Events	15
3.2.6 Other Local Events	15
4 Protocol Examples	16
4.1 Security Token Request	16
4.2 Security Token Containing a Compressed Sid Claim	20
5 Security	25

5.1 Security Considerations for Implementers	25
5.2 Index of Security Parameters	26
6 Appendix A: Full WSDL	27
7 Appendix B: Product Behavior	30
8 Change Tracking.....	31
9 Index	32

Preliminary

1 Introduction

This document specifies the SharePoint Security Token Service Web Service Protocol, which defines restrictions for several related protocols and enables interoperability and authentication with Web services that are provided by protocol servers.

Sections 1.8, 2, and 3 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in RFC 2119. Sections 1.5 and 1.9 are also normative but cannot contain those terms. All other sections and examples in this specification are informative.

1.1 Glossary

The following terms are defined in [\[MS-GLOS\]](#):

**authentication
security identifier (SID)**

The following terms are defined in [\[MS-OFCGLOS\]](#):

**culture name
request identifier
security token service (STS)
site subscription
site subscription identifier
SOAP message
Web Services Description Language (WSDL)
XML schema**

The following terms are specific to this document:

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

1.2 References

References to Microsoft Open Specifications documentation do not include a publishing year because links are to the latest version of the technical documents, which are updated frequently. References to other documents include a publishing year when one is available.

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. Please check the archive site, <http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624>, as an additional source.

[BSP] McIntosh, M., Gudgin, M., Morrison, K.S., et al., "Basic Security Profile Version 1.0", March 2007, <http://www.ws-i.org/profiles/basicsecurityprofile-1.0.html>

[MS-TNAP] Microsoft Corporation, "[Telnet: NT LAN Manager \(NTLM\) Authentication Protocol Specification](#)".

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.rfc-editor.org/rfc/rfc2119.txt>

[SAMLCore] Maler, E., Mishra, P., Philpott, R., et al., "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1", September 2003, <http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf>

[SAMLToken1.1] Lawrence, K., Kaler, C., Monzillo, R., et al., "Web Services Security: SAML Token Profile 1.1", February 2006, <http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf>

[SOAP1.1] Box, D., Ehnebuske, D., Kakivaya, G., et al., "Simple Object Access Protocol (SOAP) 1.1", May 2000, <http://www.w3.org/TR/2000/NOTE-SOAP-20000508/>

[SOAP1.2/1] Gudgin, M., Hadley, M., Mendelsohn, N., Moreau, J., and Nielsen, H.F., "SOAP Version 1.2 Part 1: Messaging Framework", W3C Recommendation, June 2003, <http://www.w3.org/TR/2003/REC-soap12-part1-20030624>

[WSDL] Christensen, E., Curbera, F., Meredith, G., and Weerawarana, S., "Web Services Description Language (WSDL) 1.1", W3C Note, March 2001, <http://www.w3.org/TR/2001/NOTE-wsdl-20010315>

[WSFederation] Kaler, C., Nadalin, A., Bajaj, S., et al., "Web Services Federation Language (WS-Federation)", Version 1.1, December 2006, <http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf>

If you have any trouble finding [WSFederation], please check [here](#).

[WSS] OASIS, "Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", February 2006, <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>

[WSSC] OpenNetwork, Layer7, Netegrity, Microsoft, Reactivity, IBM, VeriSign, BEA Systems, Oblix, RSA Security, Ping Identity, Westbridge, Computer Associates, "Web Services Secure Conversation Language (WS-SecureConversation)", February 2005, <http://schemas.xmlsoap.org/ws/2005/02/sc>

[WSSC1.3] Lawrence, K., Kaler, C., Nadalin, A., et al., "WS-SecureConversation 1.3", March 2007, <http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.html>

[WSSE 1.0] Nadalin, A., Kaler, C., Hallam-Baker, P., and Monzillo, R., Eds., "Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", OASIS Standard 200401, March 2004, <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf>

[WSSKTP1.1] Lawrence, K., Kaler, C., Nadalin, A., et al., "Web Services Security Kerberos Token Profile 1.1", November 2005, <http://www.oasis-open.org/committees/download.php/16788/wss-v1.1-spec-os-KerberosTokenProfile.pdf>

[WSSP1.2] OASIS Standard, "WS-SecurityPolicy 1.2", July 2007, <http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf>

[WSTrust] IBM, Microsoft, Nortel, VeriSign, "WS-Trust V1.0", February 2005, <http://specs.xmlsoap.org/ws/2005/02/trust/WS-Trust.pdf>

[WS-Trust1.3] Nadalin, A., Goodner, M., Gudgin, M., Barbir, A., Granqvist, H., "WS-Trust 1.3", OASIS Standard 19 March 2007, <http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html>

[XML] World Wide Web Consortium, "Extensible Markup Language (XML) 1.0 (Fourth Edition)", W3C Recommendation, August 2006, <http://www.w3.org/TR/2006/REC-xml-20060816/>

[XMLNS] Bray, T., Hollander, D., Layman, A., et al., Eds., "Namespaces in XML 1.0 (Third Edition)", W3C Recommendation, December 2009, <http://www.w3.org/TR/2009/REC-xml-names-20091208/>

[XMLSCHEMA1] Thompson, H.S., Ed., Beech, D., Ed., Maloney, M., Ed., and Mendelsohn, N., Ed., "XML Schema Part 1: Structures", W3C Recommendation, May 2001, <http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/>

[XMLSCHEMA2] Biron, P.V., Ed. and Malhotra, A., Ed., "XML Schema Part 2: Datatypes", W3C Recommendation, May 2001, <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>

1.2.2 Informative References

[MS-GLOS] Microsoft Corporation, "[Windows Protocols Master Glossary](#)".

[MS-OFBA] Microsoft Corporation, "[Office Forms Based Authentication Protocol Specification](#)".

[MS-OFCGLOS] Microsoft Corporation, "[Microsoft Office Master Glossary](#)".

1.3 Protocol Overview (Synopsis)

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 [\[SOAP1.2/1\]](#), 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 MUST have NTLM authentication enabled.

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

The authenticated session cookie MUST 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 [WSTrust1.3] 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 MUST 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 [5](#) 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 [\[XMLSCHEMA1\]](#) and [\[XMLSCHEMA2\]](#), 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.

- <http://schemas.microsoft.com/sharepoint/2009/08/claims/useridentifier>
 - Prefix: spuid
 - Description: URI for the user's unique identifier claim type.
- <http://schemas.microsoft.com/sharepoint/2009/08/claims/userlogonname>
 - Prefix: spuln
 - Description: URI for the user logon name claim type.
- <http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider>
 - Prefix: spip
 - Description: URI for the identity provider claim type.
- <http://schemas.microsoft.com/sharepoint/2009/08/claims/distributionlistsid>
 - Prefix: spdl
 - Description: URI for the distribution list **security identifier (SID)** claim type.
- <http://schemas.microsoft.com/sharepoint/2009/08/claims/farmid>
 - Prefix: spfid
 - Description: URI for the farm identifier claim type.
- <http://schemas.microsoft.com/sharepoint/2009/08/claims/processidentitysid>
 - Prefix: sppsid
 - Description: URI for the process identity SID claim type.
- <http://schemas.microsoft.com/sharepoint/2009/08/claims/processidentitylogonname>

- Prefix: sppln
- Description: URI for the process logon name claim type.

The following namespaces are referenced by this document.

Prefix	Namespace URI	Reference
wst	http://docs.oasis-open.org/ws-sx/ws-trust/200512	[WSTRUST]
wst14	http://docs.oasis-open.org/ws-sx/ws-trust/200802	[WSTRUST]
fed	http://docs.oasis-open.org/wsfed/federation/200706	[WS-FEDERATION]

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.

When authenticating to SharePoint 2010 with SAML 1.1 tokens, assumptions and considerations for this protocol are specified in the [\[WSFederation\]](#) document section 13.

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 3.1, 3.3, 5.1, and 5.3

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, 3.3, 5.2, and 5.3.

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 [\[SAMLToken1.1\]](#) section 2.4.2.1. 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](#).

2.2.3 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.

Complex type	Description
ServiceContext	Common properties that are sent with a web service request.

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.

```
<xs:element name="ServiceContext">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="correlationId" minOccurs="1" maxOccurs="1"
xmlns:q13="http://schemas.microsoft.com/2003/10/Serialization/" 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"
xmlns:q14="http://schemas.microsoft.com/2003/10/Serialization/" 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.

Preliminary

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 [WS-Federation] specification's terminology section and Group SID is a SID, which is defined in [MS-GLOS], that identifies a group object, which is defined in [MS-GLOS].

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:

- 1.Claim type set to http://schemas.microsoft.com/sharepoint/2009/08/claims/SidCompressed
- 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 that issued these claims.

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:

```
<HttpRequest>
  <Method>POST</Method>
  <QueryString></QueryString>
  <WebHeaders>
    <Content-Length>1346</Content-Length>
    <Content-Type>application/soap+xml</Content-Type>
    <Authorization>Negotiate
TlRMTVNTUADAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAAAAAAFgAAAAAAAAWAAAAAAAABYAAAAANCKY4gYAchcAA
AAPk9yL+ts+ej913CqHBNl3Nw==</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>
    <a:Action s:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</a:Action>
    <a:MessageID>urn:uuid:0c9b2158-be51-4222-afa8-b55036b5aedf</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:RequestSecurityToken xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-
trust/200512">
      <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <a:EndpointReference>
          <a:Address>http://server.example.com/</a:Address>
        </a:EndpointReference>
      </wsp:AppliesTo>
      <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</trust:KeyType>
      <trust:OnBehalfOf>
        <UsernameToken b:Id="LDAPMembershipProvider:LDAPRoleProvider"
xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:b="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
          <Username>0#.f|ldapmembershipprovider|user1</Username>
          <Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-
token-profile-
1.0#PasswordText">0#.f|ldapmembershipprovider|user1,129091469640504627,mOUexpCMCzkI024dk2g7wQ
zLSDL7YLbny6PE5GmuzDmq9LjzTaApxpDJQAZlMi2CC8F5peYEewnVODoJbotje/26JocdC+TNDFe3ycKv3aQ9Ks0qEx
k72ZzMnTS3/QEzLBJoL58QAgL7ydeVUann9A0gUXfj8Fs8DP552vpXWx3ped3N9092J2bXaOiF1VQ2yIhk8a//44KvyAs
N7HrOI2tuOFwE+whEn9DYSRaQJKCVQ96V/FzrsW3pkHVaMhBWu6Tc7ObMC9GCP4fd6p1R9s1IFND9n2RpMm6Io0LosUj7
6oDVgyfz/aTOzsQileyvCfQoV8tXQdY3ikg91aIQ==,http://server.example.com/</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>
```



```
</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:

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
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/RSTRC/IssueFinal</a:Action>
    <ActivityId CorrelationId="f1d13f52-af2c-46dd-9f73-67b68ef08543"
xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">00d96a84-2caa-45bb-
bbb1-e843e2197471</ActivityId>
  </s:Header>
  <s:Body>
    <trust:RequestSecurityTokenResponseCollection xmlns:trust="http://docs.oasis-open.org/ws-
sx/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>
        <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
          <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>
              </saml:Subject>
              <saml:Attribute AttributeName="role"
AttributeNamespace="http://schemas.microsoft.com/ws/2008/06/identity/claims"
a:OriginalIssuer="Forms:LDAPRoleProvider"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
                <saml:AttributeValue>USERS</saml:AttributeValue>
                <saml:AttributeValue>EXAMPLE-ROLE-RW</saml:AttributeValue>
              </saml:Attribute>
              <saml:Attribute AttributeName="userlogonname"
AttributeNamespace="http://schemas.microsoft.com/sharepoint/2009/08/claims">
```

```

a:OriginalIssuer="Forms:LDAPMembershipProvider"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
  <saml:AttributeValue>user1</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute AttributeName="userid"
AttributeNamespace="http://schemas.microsoft.com/sharepoint/2009/08/claims"
a:OriginalIssuer="SecurityTokenService"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
  <saml:AttributeValue>0#.f|ldapmembershipprovider|user1</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute AttributeName="name"
AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
a:OriginalIssuer="SecurityTokenService"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
  <saml:AttributeValue>0#.f|ldapmembershipprovider|user1</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute AttributeName="identityprovider"
AttributeNamespace="http://schemas.microsoft.com/sharepoint/2009/08/claims"
a:OriginalIssuer="SecurityTokenService"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
  <saml:AttributeValue>forms:LDAPMembershipProvider</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute AttributeName="isauthenticated"
AttributeNamespace="http://sharepoint.microsoft.com/claims/2009/08"
a:OriginalIssuer="SecurityTokenService"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
  <saml:AttributeValue>True</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute AttributeName="farmid"
AttributeNamespace="http://schemas.microsoft.com/sharepoint/2009/08/claims"
a:OriginalIssuer="ClaimProvider:System"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
  <saml:AttributeValue>568e7577-e4e6-4bb1-a8d8-7058ac50f5aa</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute AttributeName="tokenreference"
AttributeNamespace="http://sharepoint.microsoft.com/claims/2009/08">
  <saml:AttributeValue>0#.f|ldapmembershipprovider|user1,129091475742945006,JpbKq4NnifCahSpPqxn
MzMO++E0cG0QWt4rLDDh/Ig2oR+gFN8hqQ5oB1nI7NW9kz5EVoQAF6AzPx2D8WcPOPhg+Y0iRUG01fwAZ5KRPAFjT5ZHd
115RyvEOBqGjJ9/Odiic8MrgU5SqThWRB5+y/6lXUuhRE9Qpei4PkVnKsAfzYojTojxRaZ41UaG00MY1uo/PiYJpmvYuR
uDPov5DHZqBoq4fObUomGpZTTHP/9Prh7U0QJkjCaHdzjps6aNPUnMjr3LDH44myTsOiLc7PYhWFD/Zay4yBpFwrMzXzv
xmAt0ABdyTfNDlGtHzfMe2m8VFteYIds9uTJ25sv9S0Q==,http://server.example.com/</saml:AttributeValu
e>
</saml:Attribute>
</saml:AttributeStatement>
<saml:AuthenticationStatement AuthenticationMethod="urn:federation:authentication:password"
AuthenticationInstant="2010-01-28T00:19:34.315Z">
  <saml:Subject>
    <saml:NameIdentifier>domain\user1</saml:NameIdentifier>
    <saml:SubjectConfirmation>
      <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>
    </saml:SubjectConfirmation>
  </saml:Subject>
</saml:AuthenticationStatement>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></ds:CanonicalizationMethod>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"></ds:SignatureMethod>

```

```
<ds:Reference URI="#_40e2d2b1-6da1-46bc-9a2c-769c03d21d32">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></ds:Transform>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></ds:Transform>
  </ds:Transforms>
  <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></ds:DigestMethod>
  <ds:DigestValue>CtNDDf6s4vSMxJBr7EhBxFrtX+yqm2lhySRxi0f7z8=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>WvLnpnvqmc1z3ldNaT39wZCOAqtiWiQo/CvAWkYARcf118/WqY17gEaxsf9AppyWd7h5dCb/cd
ES2Jex81lnUXdePZnGodz3Sa9uFAPnYfsfPmdpvJntmDSaTiKF4dsWPubKQeOK/yAy3Q6mgU40TKjIGdWRNrP13r+cZrI
gg/GwQK4Xf31U42N4iwiMt9CaITxeNY9idYCB0qnp6d9ELB0LhLP1jP477TiK21DbsRM5unjFLcTRHu+6eL2aqn5p7OpqS
19049SLT/I4g9Mn0fgxOH8E8KHvEgziOh8loFjn1j60/woUGwGYDdWgURKN5V5hgmpFKLb4Wle3Ej9toSg=</ds:Sign
atureValue>

  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <X509Data>

<X509Certificate>MIERjCCAi6gAwIBAgIQ+BzA2uDKYKBI8psCB32xXTANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQG
EwJVUzESMBAGAlUEChMJTlWlJcm9zb2Z0MRMwEQYDVQQLEWpTaGFyZVBvaW50MSIwIAYDVQQDEeI1TaGFyZVBvaW50IFJvb
3QgQXV0aG9yaXR5MCAXDTEwMDEyNDUyN1oYDzK5OTkwMTAxMDAwMDAwWjBiMQswCQYDVQQGEwJVUzESMBAGAlUECh
MJTlWlJcm9zb2Z0MRMwEQYDVQQLEWpTaGFyZVBvaW50MSowKAYDVQQDEyFTaGFyZVBvaW50IFNlY3VyaXR5IFRva2VuIFN
lcnZpY2UwggiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCeKuBBZa5n3RI1wCy4nLgFURUB88TI2MvGBbKvRtSX
GWjKcmf0W/LS2OykTtUZxYdYjQz2iC/mHBEvdWiimh+5Js9I5LSAMILzqpEiNLXzIKW7M1sM2rB8QYqvK49lqBmpD66hs
HADgsGO//ybBv/tmpyIIfSsKLCYJWyu+NbPAB7fUtnPugAolNk3Trv7zeJ8SnTi/xThaR7UJa5p1TsB2CxFQo9Y9MN/n
Z0KGFsifFZAwcKtH5wnkh2n6tz3pJ73ZIpmauawnc0JjhHghffBpPb/aqg8ltXuvZdap+zMLyh7bcegZXK24fgComH8KiS
n9N2OkUjWgcTdc7t77e5zAgMBAAEwDQYJKoZIhvcNAQEFBQADggIBAETHVVCVBUjwbbTXfCnQ8Qe4eldfCisQJfg1t/HjO/
H1d0iF42bYv+DcFHMwYr6XPdNTx/nAdO2Efa6VUueTzy1vGynPgT0eLCUAA11X332wH9XVvMvgdW2d5b70/rNy3Yoew/p
9S4nwboggiuNk7rjHAYntE7KXZyqT7kwcRCb1UmPgP+vxhRGJucfw7/hrn02bBkHRtB01jsH+LBotpZz0roA4PIxOySpP
hAvIzM1ApyfjY+pfkWyYk67c4Yf+KWwGy6JDOWTaaflpyEM2NAWLNSjnba720efV14TMHZM1ArGcUVAfh0++0XyceReD
RcwWl1sgpRlQJrtzYEDgPDNSmrq3vBFPzNLF8pvsYNPaXAFD4fiWRI5QkX5JUWOQC3xyEqV670MnFXBuDZiCR2QFwoQEc
VR344quRpx+5bQUj35jdPbjwzFexL1YtJg8KOs5BCD87emfc68NM9CL2QqZHVfwoY05iAWfGbySgXuQqXhLNq5tMgJTFn
u6UUZHSLGQwWOFHopu7QJFz0TAK9x4JC+KwbFGK067x3X196NUf3e8WAVwUQwAPGnY+eUtZsBI/ltCzCTLd/9RSISSR
3wKqEz5jS7jAdfrGNUyt1SmG0PXroz9wF0SIjZPovFevucg3BzvjoVRPI8T9lDRV4pQWGHh0EC37SwWTj17XbM</X509C
ertificate>

    </X509Data>
  </KeyInfo>
</ds:Signature>
</saml:Assertion>
</trust:RequestedSecurityToken>
<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">_40e2d2b1-6da1-46bc-9a2c-769c03d21d32</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">_40e2d2b1-6da1-46bc-9a2c-769c03d21d32</o:KeyIdentifier>
  </o:SecurityTokenReference>
</trust:RequestedUnattachedReference>
<trust:TokenType>urn:oasis:names:tc:SAML:1.0:assertion</trust:TokenType>
<trust:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</trust:RequestType>
<trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Bearer</trust:KeyType>
```

```

    </trust:RequestSecurityTokenResponse>
  </trust:RequestSecurityTokenResponseCollection>
</s:Body>
</s:Envelope>

```

4.2 Security Token Containing a Compressed Sid Claim

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

```

<HttpRequest>
  <Method>POST</Method>
  <QueryString></QueryString>
  <WebHeaders>
    <Content-Length>510</Content-Length>
    <Content-Type>application/soap+msbin1</Content-Type>
    <Authorization>Negotiate
TlRMTVNTUAAADAAAAAAAAAFgAAAAAAAAWAAAAAAAAABYAAAAAAAAAFgAAAAAAAAWAAAAAAAAABYAAAAANcKY4gYAChcAA
AAP4dX8Niq7yPURkkRs9JHMBw==</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>
    <a:Action s:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/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:RequestSecurityToken xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-
trust/200512">
      <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <a:EndpointReference>
          <a:Address>https://server.example.com/</a:Address>
        </a:EndpointReference>
      </wsp:AppliesTo>
      <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</trust:KeyType>
      <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 the following SecurityTokenRequestResponse. This response contains an example of GroupSidClaims.

```

<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
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/RSTRC/IssueFinal</a:Action>
    <ActivityId CorrelationId="58984e0d-ffb8-4643-a0f9-6aa89ce42bd8"
xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">cce14abf-a3b0-4f06-
82bf-396f0aefab59</ActivityId>
  </s:Header>
<s:Body>
  <trust:RequestSecurityTokenResponseCollection xmlns:trust="http://docs.oasis-open.org/ws-
sx/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">2010-02-05T17:41:24.310Z</wsu:Created>
        <wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2010-02-06T03:41:24.310Z</wsu:Expires>
      </trust:Lifetime>
      <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <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:SubjectConfirmation>
                <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>
                </saml:SubjectConfirmation>
              </saml:Subject>
              <saml:Attribute AttributeName="primarysid"
AttributeNamespace="http://schemas.microsoft.com/ws/2008/06/identity/claims"
a:OriginalIssuer="Windows" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
                <saml:AttributeValue>S-1-5-21-2127521184-1604012920-1887927527-
66602</saml:AttributeValue>
              </saml:Attribute>
              <saml:Attribute AttributeName="primarygroupsid"
AttributeNamespace="http://schemas.microsoft.com/ws/2008/06/identity/claims"
a:OriginalIssuer="Windows" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
                <saml:AttributeValue>S-1-5-21-2127521184-1604012920-1887927527-
513</saml:AttributeValue>
              </saml:Attribute>
              <saml:Attribute AttributeName="upn"
AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
a:OriginalIssuer="Windows" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
                <saml:AttributeValue>pkmacct@microsoft.com</saml:AttributeValue>
              </saml:Attribute>
              <saml:Attribute AttributeName="userlogonname"
AttributeNamespace="http://schemas.microsoft.com/sharepoint/2009/08/claims"
a:OriginalIssuer="Windows" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
                <saml:AttributeValue>DOMAIN\USER1</saml:AttributeValue>
              </saml:Attribute>
            </saml:Subject>
          </saml:AttributeStatement>
        </trust:RequestedSecurityToken>
      </trust:RequestSecurityTokenResponse>
    </trust:RequestSecurityTokenResponseCollection>
  </s:Body>

```

```

    <saml:Attribute AttributeName="userid"
AttributeNamespace="http://schemas.microsoft.com/sharepoint/2009/08/claims"
a:OriginalIssuer="SecurityTokenService"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
    <saml:AttributeValue>0#.w|domain\user1</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="name"
AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
a:OriginalIssuer="SecurityTokenService"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
    <saml:AttributeValue>0#.w|domain\user1</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="identityprovider"
AttributeNamespace="http://schemas.microsoft.com/sharepoint/2009/08/claims"
a:OriginalIssuer="SecurityTokenService"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
    <saml:AttributeValue>windows</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="isauthenticated"
AttributeNamespace="http://sharepoint.microsoft.com/claims/2009/08"
a:OriginalIssuer="SecurityTokenService"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
    <saml:AttributeValue>True</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="farmid"
AttributeNamespace="http://schemas.microsoft.com/sharepoint/2009/08/claims"
a:OriginalIssuer="ClaimProvider:System"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
    <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\user1,129099012852708179,czhRNuPUw78k01B8tNfnUKLDhd5xYPnTN2S
6Qu5DtXIQlJEE MnPIuKpnMuwqerXObYq4ycW08i+C63CGhp9EZca/lZpgiqKfWCsB+xlMfspqYLurgphmkvz9uCKdFb0
QEOeYZXRf7OXYLGgCVdmbKwnG5M+j74wZq816MuE30+FFb5kV14g2kg/7MApGZGEyQ4hwxEeZIQDb/HFzyZkL81YQNWP
e+/O9dNUEMWLho/ws0kxhKSEHKuqaLLLkLMrEzPRsHdIKNSgmPq3kD3I+BIbaNvZW5IwXX2r4IJNMkLufiIshaRoKmvEw
WsSO3ZYI2Ls34FvxH/qbmppXlkWA==,https://server.example.com/</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="SidCompressed"
AttributeNamespace="http://schemas.microsoft.com/sharepoint/2009/08/claims"
a:OriginalIssuer="Windows" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
    <saml:AttributeValue>S-1-5-21-2127521184-1604012920-
1887927527;513;1495408;5576293;1874606;5317986;634623;5317941;5154286;4751181;1921737;3487562
;5413290;3061541;4746090;5301610;4933277;1421044;3698337;5782818;1348243;3688791;326949;50053
50;2115484;705229;5974845;1821296;4855650;2268910;5687401;5124256;1929380;1684156;3191140;345
7293;2347842;175772;2361615;650727;547378;547376;771043;547375;3452120;1700934;2547081;236161
4;2749268;664781;2671629;2289587;332924;2347844;3457290;5421060;4968904;3457292;1247867;54737
4;1378086;1944152;2932750;2015134;2671626;1908118;1378084;1944303;1472082;158181;2464244;5473
77;547379;556526;771112;2289588;1472089;5107804;1390170;2361613;1908116;725547;1378088;722103
;5107803;754149;3457291;1908117;1908121;2984327;571;2347847;576701;2361612;1174182;1378091;18
97219|S-1-1;0|S-1-5-21-258540387-1499065276-4212630864;1010;1011;1012|S-1-5-
32;544;568;558;545|S-1-5;2;11;15|S-1-5-21-1721254763-462695806-
1538882281;2369298;2649140;2358360;2982283;2793640|S-1-5-21-2146773085-903363285-
719344707;859159;750693|S-1-5-21-57989841-823518204-1644491937;46661|S-1-5-21-124525095-
708259637-1543119021;926551;926563|S-1-5-64;10|</saml:AttributeValue>
    </saml:Attribute>
    </saml:AttributeStatement>
    <saml:AuthenticationStatement
AuthenticationMethod="urn:federation:authentication:windows" AuthenticationInstant="2010-02-
05T17:41:24.281Z">
    <saml:Subject>
    <saml:NameIdentifier>domain\user1</saml:NameIdentifier>

```



```
<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:TokenType>urn:oasis:names:tc:SAML:1.0:assertion</trust:TokenType>
<trust:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</trust:RequestType>
  <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/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 12
- [\[WSSC\]](#) section 11
- [\[WSSC1.3\]](#) section 10
- [\[MS-TNAP\]](#) section 5

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

- [\[WSTrust\]](#) section 4.5
- [\[WSSP1.2\]](#) 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 MUST 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
- [\[WSTrust\]](#) sections 4.4 and 8.2 and 9.2

When selecting the encryption mechanism, the following restrictions MUST be considered:

For SharePoint services SAML tokens, the following rules MUST be followed:

- The cryptographic algorithm for signing the SAML token header MUST be SHA1.
- The cryptographic algorithm for signing the SAML token date value MUST be SHA256.

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

- The cryptographic algorithm for signing the SAML token header MUST be SHA256.
- The cryptographic algorithm for signing the SAML token date value MUST be SHA256.

All tokens MUST 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 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/wsdl/soap/" xmlns:tns="http://tempuri.org/"
xmlns:microsoft="http://schemas.microsoft.com/ws/2005/12/wsdl/contract"
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:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
xmlns:i0="http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice"
xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex"
xmlns:wsap="http://schemas.xmlsoap.org/ws/2004/08/addressing/policy"
xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
  <wsp:Policy wsu:Id="AsymmetricNtlm_policy">
    <wsp:ExactlyOne>
      <wsp>All>
        <msb:BinaryEncoding
xmlns:msb="http://schemas.microsoft.com/ws/06/2004/mspolicy/netbinary1" />
        <sp:TransportBinding xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken />
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256Sha256 />
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict />
              </wsp:Policy>
            </sp:Layout>
            <sp:IncludeTimestamp />
          </wsp:Policy>
        </sp:TransportBinding>
        <sp:EndorsingSupportingTokens xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
          <wsp:Policy>
            <sp:SpnegoContextToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <wsp:Policy>
                <sp:MustNotSendCancel />
                <sp:MustNotSendAmend />
                <sp:MustNotSendRenew />
              </wsp:Policy>
            </sp:SpnegoContextToken>
            <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/Never" wsp:Optional="true" />
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
      </wsp>All>
    </wsp:ExactlyOne>
  </wsp:Policy>

```

```

        <sp:SignedParts>
            <sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing" />
        </sp:SignedParts>
    </wsp:Policy>
</sp:EndorsingSupportingTokens>
<sp:Wss11 xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
    <wsp:Policy>
        <sp:MustSupportRefKeyIdentifier />
        <sp:MustSupportRefIssuerSerial />
        <sp:MustSupportRefThumbprint />
        <sp:MustSupportRefEncryptedKey />
    </wsp:Policy>
</sp:Wss11>
<sp:Trust13 xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
    <wsp:Policy>
        <sp:MustSupportIssuedTokens />
        <sp:RequireClientEntropy />
        <sp:RequireServerEntropy />
    </wsp:Policy>
</sp:Trust13>
    <wsaw:UsingAddressing />
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
<wsdl:import
namespace="http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice"
location="https://example.com/_vti_bin/sts/spsecuritytokenservice.svc?wsdl" />
<wsdl:types />
<wsdl:binding name="AsymmetricNtlm" type="i0:IWSTrust13Sync">
    <wsp:PolicyReference URI="#AsymmetricNtlm_policy" />
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="Trust13Cancel">
        <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Cancel" style="document" />
        <wsdl:input>
            <soap12:body use="literal" />
        </wsdl:input>
        <wsdl:output>
            <soap12:body use="literal" />
        </wsdl:output>
    </wsdl:operation>
    <wsdl:operation name="Trust13Issue">
        <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue" style="document" />
        <wsdl:input>
            <soap12:body use="literal" />
        </wsdl:input>
        <wsdl:output>
            <soap12:body use="literal" />
        </wsdl:output>
    </wsdl:operation>
    <wsdl:operation name="Trust13Renew">
        <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Renew" style="document" />
        <wsdl:input>
            <soap12:body use="literal" />
        </wsdl:input>
        <wsdl:output>
            <soap12:body use="literal" />
        </wsdl:output>
    </wsdl:operation>

```

```
</wsdl:output>
</wsdl:operation>
<wsdl:operation name="Trust13Validate">
  <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Validate" style="document" />
  <wsdl:input>
    <soap12:body use="literal" />
  </wsdl:input>
  <wsdl:output>
    <soap12:body use="literal" />
  </wsdl:output>
</wsdl:operation>
</wsdl:binding>
</wsdl:definitions>
```

Preliminary

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 released service packs:

- Microsoft® Lync™ 2010
- Microsoft® Lync® 2013 Preview
- Microsoft® FAST™ Search Server 2010
- Microsoft® Office 2010 suites
- Microsoft® Office 2013 Preview
- Microsoft® Search Server 2010
- Microsoft® SharePoint® Designer 2010
- Microsoft® SharePoint® Designer 2013 Preview
- Microsoft® SharePoint® Foundation 2010
- Microsoft® SharePoint® Foundation 2013 Preview
- Microsoft® SharePoint® Server 2010
- Microsoft® SharePoint® Server 2013 Preview
- Microsoft® SharePoint® Workspace 2010
- Microsoft® Visio® 2010
- Microsoft® Visio® 2013 Preview

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product 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.

8 Change Tracking

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

Preliminary

9 Index

A

Abstract data model
[server](#) 14
[Applicability](#) 9
[Attribute groups](#) 13
[Attributes](#) 13

C

[Capability negotiation](#) 9
[Change tracking](#) 31
Client
[initialization](#) 14
[local events](#) 15
[message processing](#) 15
[overview](#) 14
[sequencing rules](#) 15
[timer events](#) 15
[timers](#) 14
[Common data structures](#) 13
[Complex types](#) 12
[ServiceContext \(from namespace <http://schemas.microsoft.com/sharepoint/servicecontext>\)](#) 12

D

Data model - abstract
[server](#) 14

E

Events
[local - client](#) 15
[local - server](#) 14
[timer - client](#) 15
[timer - server](#) 14

Examples

[security token containing a compressed Sid claim](#)
20
[security token request](#) 16

F

[Fields - vendor-extensible](#) 9
[Full WSDL](#) 27

G

[Glossary](#) 6
[Groups](#) 13

I

[Implementer - security considerations](#) 25
[Index of security parameters](#) 26
[Informative references](#) 8
Initialization

[client](#) 14
[server](#) 14
[Introduction](#) 6

L

Local events
[client](#) 15
[server](#) 14

M

Message processing
[client](#) 15
[server](#) 14
Messages
[attribute groups](#) 13
[attributes](#) 13
[common data structures](#) 13
[complex types](#) 12
[elements](#) 12
[enumerated](#) 11
[groups](#) 13
[namespaces](#) 10
[RST](#) 11
[RST message](#) 11
[RSTR](#) 11
[RSTR message](#) 11
[ServiceContext \(from namespace <http://schemas.microsoft.com/sharepoint/servicecontext>\)](#) [complex type](#) 12
[simple types](#) 12
[syntax](#) 10
[transport](#) 10

N

[Namespaces](#) 10
[Normative references](#) 6

O

[Overview \(synopsis\)](#) 8

P

[Parameters - security index](#) 26
[Preconditions](#) 8
[Prerequisites](#) 8
[Product behavior](#) 30

R

[References](#) 6
[informative](#) 8
[normative](#) 6
[Relationship to other protocols](#) 8

S

Security
[implementer considerations](#) 25
[parameter index](#) 26
[Security token containing compressed Sid claim example](#) 20
[Security token request example](#) 16
Sequencing rules
[client](#) 15
[server](#) 14
Server
[abstract data model](#) 14
[initialization](#) 14
[local events](#) 14
[message processing](#) 14
[overview](#) 14
[sequencing rules](#) 14
[timer events](#) 14
[timers](#) 14
[ServiceContext \(from namespace http://schemas.microsoft.com/sharepoint/servicecontext\) complex type](#) 12
[Simple types](#) 12
[Standards assignments](#) 9
Syntax
[messages - overview](#) 10

T

Timer events
[client](#) 15
[server](#) 14
Timers
[client](#) 14
[server](#) 14
[Tracking changes](#) 31
[Transport](#) 10
Types
[complex](#) 12
[simple](#) 12

V

[Vendor-extensible fields](#) 9
[Versioning](#) 9

W

[WSDL](#) 27