[MS-SPSTWS]:

SharePoint Security Token Service Web Service Protocol

Revision Summary

Date	Revision History	Revision Class	Comments
7/13/2009	0.1	Major	Initial Availability
8/28/2009	0.2	Editorial	Revised and edited the technical content
11/6/2009	0.3	Editorial	Revised and edited the technical content
2/19/2010	1.0	Major	Updated and revised the technical content
3/31/2010	1.01	Major	Updated and revised the technical content
4/30/2010	1.02	Editorial	Revised and edited the technical content
6/7/2010	1.03	Editorial	Revised and edited the technical content
6/29/2010	1.04	Minor	Clarified the meaning of the technical content.
7/23/2010	1.04	None	No changes to the meaning, language, or formatting of the technical content.
9/27/2010	1.04	None	No changes to the meaning, language, or formatting of the technical content.
11/15/2010	1.04	None	No changes to the meaning, language, or formatting of the technical content.
12/17/2010	1.04	None	No changes to the meaning, language, or formatting of the technical content.
3/18/2011	1.04	None	No changes to the meaning, language, or formatting of the technical content.
6/10/2011	1.04	None	No changes to the meaning, language, or formatting of the technical content.
1/20/2012	1.5	Minor	Clarified the meaning of the technical content.
4/11/2012	1.5	None	No changes to the meaning, language, or formatting of the technical content.
7/16/2012	1.5	None	No changes to the meaning, language, or formatting of the technical content.
9/12/2012	1.5	None	No changes to the meaning, language, or formatting of the technical content.
10/8/2012	1.6	Minor	Clarified the meaning of the technical content.
2/11/2013	1.6	None	No changes to the meaning, language, or formatting of the technical content.
7/30/2013	1.6	None	No changes to the meaning, language, or formatting of the technical content.
11/18/2013	1.6	None	No changes to the meaning, language, or formatting of the technical content.
2/10/2014	1.6	None	No changes to the meaning, language, or formatting of the technical content.
4/30/2014	1.7	Minor	Clarified the meaning of the technical content.

Date	Revision History	Revision Class	Comments
7/31/2014	2.0	Major	Significantly changed the technical content.
10/30/2014	2.0	None	No changes to the meaning, language, or formatting of the technical content.
3/16/2015	3.0	Major	Significantly changed the technical content.
2/26/2016	4.0	Major	Significantly changed the technical content.
7/15/2016	4.0	None	No changes to the meaning, language, or formatting of the technical content.
9/14/2016	5.0	Major	Significantly changed the technical content.

Table of Contents

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 in Windows 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].

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.

MAY, SHOULD, MUST, SHOULD 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.

[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".

[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

[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

[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

[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

[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

[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

[WSSP1.2-2012] OASIS, "WS-SecurityPolicy 1.2", April 2012, http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.2/ws-securitypolicy.pdf

[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

[WSTrust1.4] OASIS Standard, "WS-Trust 1.4", February 2009, http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.doc

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

[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/

[XML] World Wide Web Consortium, "Extensible Markup Language (XML) 1.0 (Fourth Edition)", W3C Recommendation 16 August 2006, edited in place 29 September 2006, http://www.w3.org/TR/2006/REC-xml-20060816/

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], 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 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.

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.

Prefix	Namespace URI	Reference
wst	http://docs.oasis-open.org/ws-sx/ws-trust/200512	[WSTrust1.4]
wst14	http://docs.oasis-open.org/ws-sx/ws-trust/200802	[WSTrust1.4]
fed	http://docs.oasis-open.org/wsfed/federation/200706	[WSFederation]

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, 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 2.2.2.2.1.1.1 of this document.
- An **AttributeNamespace** attribute, as specified in [SAMLCore] section 2.4.4.1 and section 2.2.2.2.1.1.2 of this document.
- An **AttributeValue** element, as specified in [SAMLCore] section 2.4.4.1 and section 2.2.2.2.1.1.4 of this document.
- An **OriginalIssuer** attribute, as specified in section 2.2.2.2.1.1.3 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:

Issuer	Value
Windows	"windows"
Trusted Security	"TrustedProvider:" + STS name, where STS name is defined by an administrator when

Issuer	Value
Token Service	setting up the trust.
Claim Provider	"ClaimProvider:" + Name of claim provider, where name is defined by the administrator when registering the claim provider.
Forms Based Authentication	"Forms:" + 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.
Security Token Service	"SecurityTokenService"

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:

Claim type URI	Encoded character
"http://schemas.microsoft.com/sharepoint/2009/08/claims/audienceid"	"0"
"http://schemas.microsoft.com/sharepoint/2009/08/claims/organizationid"	"1"
"http://schemas.microsoft.com/sharepoint/2009/08/claims/useridentifier"	"""
"http://schemas.microsoft.com/sharepoint/2009/08/claims/userlogonname"	"#"
"http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider"	"!"
"http://schemas.microsoft.com/sharepoint/2009/08/claims/distributionlistsid"	"$"
"http://schemas.microsoft.com/sharepoint/2009/08/claims/farmid"	"%"
"http://schemas.microsoft.com/sharepoint/2009/08/claims/processidentitysid"	"&"
"http://schemas.microsoft.com/sharepoint/2009/08/claims/processidentitylogonname"	"`"
"http://schemas.microsoft.com/sharepoint/2009/08/claims/windowstoken/handle"	"A"
"http://sharepoint.microsoft.com/claims/2009/01/windowstoken/processid"	"B"
"http://sharepoint.microsoft.com/claims/2009/01/windowstoken/processid"	"C"
"http://schemas.microsoft.com/sharepoint/2009/08/claims/isauthenticated"	"("
"http://schemas.microsoft.com/sharepoint/2009/08/claims/provideruserkey"	"h"
IDFX and service model claim type URIs	

Claim type URI	Encoded character
"http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"	")"
"http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid"	"*"
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid"	"+"
"http://schemas.microsoft.com/ws/2008/06/identity/claims/role"	"-"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/anonymous"	"."
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication"	"/"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecision"	"0"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country"	"1"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth"	"2"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid"	"3"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns"	"4"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"	"5"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/gender"	"6"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"	"7"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/hash"	"8"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/homephone"	"9"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality"	"<"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone"	"="
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"	">"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"	"?"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone"	"@"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode"	"["
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier"	"\"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/rsa"	"]"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/sid"	"^"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/spn"	"_"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince"	"`"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress"	"a"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"	"b"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/system"	"c"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprint"	"d"

Claim type URI	Encoded character
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"	"e"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/uri"	"f"
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/webpage"	"g"

- 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	Encoded character
"http://www.w3.org/2001/XMLSchema#base64Binary"	"!"
"http://www.w3.org/2001/XMLSchema#boolean"	"""
"http://www.w3.org/2001/XMLSchema#date"	"#"
"http://www.w3.org/2001/XMLSchema#dateTime"	"$"
"http://www.w3.org/TR/2002/WD-xquery-operators-20020816#dayTimeDuration"	"%"
"http://www.w3.org/2001/XMLSchema#double"	"&"
"http://www.w3.org/2001/XMLSchema#hexBinary"	"("
"http://www.w3.org/2001/XMLSchema#integer"	")"
"http://www.w3.org/2000/09/xmldsig#KeyInfo"	"*"
"http://www.w3.org/2000/09/xmldsig#RSAKeyValue"	"-"
"http://www.w3.org/2000/09/xmldsig#DSAKeyValue"	"`"
"http://www.w3.org/2001/XMLSchema#string"	"."
"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:

Original issuer	Encoded character
Windows	"w"
Forms based authentication	"f"
Trusted STS	"t"
Personal InfoCard	"p"
Local STS	"s"
Claim provider	"c"

- 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.

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.

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:

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 (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:

```
<HttpRequest>
  <Method>POST</Method>
  <QueryString></QueryString>
  <WebHeaders>
    <Content-Length>1346</Content-Length>
    <Content-Type>application/soap+msbin1</Content-Type>
    <Authorization>Negotiate
TlRMTVNTUAADAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAANcKY4gYAchcAA
AAPk9yL+ts+ej9l3CqHBNl3Nw==</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
zLSDL7YLbny6PE5GmuzDmq9LjozTaApxpDJQAZlMi2CC8F5peYEewnVODojbotje/26JocdC+TNDFe3ycKv3aQ9Ks0qEx
k72ZzMnTS3/QEzLBJoL58QAgL7ydEvUann9A0gUXfj8Fs8DP552vpXWx3ped3N9092J2bXaOiFlVQ2yIhk8a//44KvyAs
N7HrOI2tuOFwE+whEn9DYSRaQJKCVQ96V/FzrsW3pkHVaMhBWu6Tc7ObMC9GCP4fd6p1R9slIFND9n2RpMm6Io0LosUj7
6oDVgyfz/aTOzsQi1eypvCfQoV8tXQdY3ikg91aIQ==,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>
```

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+Y0iRUG0lfwAZ5KRPAFjT5ZHd
l15RyvEOBqGjJ9/Odiic8MrgU5SqThWRB5+y/6lXUuhRE9Qpei4PkVNKsAfzYojTojxRaZ4lUaG0OMY1uo/PiYJpmvyuR
uDPov5DHZqBoq4fObUomGpZTIHP/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+yqm2lhySRxziOf7z8=</ds:DigestValue>
              </ds:Reference>
            </ds:SignedInfo>

<ds:SignatureValue>WvLnpnvqmc1z3ldNaT39wZCOAqtiWiQo/CvAWkYARcf1l8/WqY17gEaxsf9AppywD7h5dCb/cd
ES2Jex8llnUXdePZnGodz3Sa9uFAPnYfsfPmdpvJNtmDSaTiKF4dsWPUbKQeOK/yAy3Q6mgU4OTKjIGdwRNrPl3r+czrI
gg/GWqK4Xf31U42N4iwiMt9CaITxeNY9idYCB0qnp6d9ELB0LhLP1jP47TIk2lDbsRM5unjFLcTRHu+6eL2aqn5p7OpqS
l9O49SLT/I4g9Mn0fgxoH8E8KHvEgziOh8loFjnlj6O/woUGwGYDdWgURKN5V5hgmpFKLb4W1e3Ej9toSg==</ds:Sign
atureValue>
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
              <X509Data>

<X509Certificate>MIIERjCCAi6gAwIBAgIQ+BzA2uDkYKBI8psCB32xXTANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQG
```

```
EwJVUzESMBAGA1UEChMJTWljcm9zb2Z0MRMwEQYDVQQLEwpTaGFyZVBvaW50MSIwIAYDVQQDExlTaGFyZVBvaW50IFJvb
3QgQXV0aG9yaXR5MCAXDTEwMDEyNDE5MDYwN1oYDzk5OTkwMTAxMDAwMDAwWjBiMQswCQYDVQQGEwJVUzESMBAGA1UECh
MJTWljcm9zb2Z0MRMwEQYDVQQLEwpTaGFyZVBvaW50MSowKAYDVQQDEyFTaGFyZVBvaW50IFNlY3VyaXR5IFRva2VuIFN
lcnZpY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCeKuBBZa5n3RI1wCy4nLgFURUB88TI2MvGBbKvRtSX
GWjKMcmf0W/LS2OykTtUZXdyJqZ2iC/mHBevdWiimh+5Js9I5LSAMILzqpEinLXzIKW7M1sM2rB8QYqvK49lqBmpD66hs
HAdgsGO//ybBv/tmpyIIfSsKLcYJWyu+NbPAB7fUtnPugAolNk3Trv7zeJ8SnTi/xThaR7UJa5plTsB2CxFQo9Yy9MN/n
Z0KGFsipFZAwcKtH5wnkh2n6tz3pJ73ZIpmuawnc0JJhHghffBpPb/aqq8ltXuvZdap+zMLyh7bcegZXK24fgComH8KiS
n9N2OkUjWgcTdC7t77e5zAgMBAAEwDQYJKoZIhvcNAQEFBQADggIBAEHVCVBUjwbbTXfCnQ8Qe4eldfCisQJfg1t/HjO/
H1d0iF42bYv+DcfHMwYr6XPDNTx/nAdO2EfA6VUueTzy1vGynPgT0eLCUAA11X332wH9XVvMvgdW2d5b7O/rNy3Yoew/p
9S4nwboqgiuNk7rjHAyNtE7KXZyqT7kcwRCb1UmPgP+vxhRGJucfw7/hrn02bBkHRtB01jsH+LBotpZz0roA4PIxOySpP
hAvIzM1ApyfjY+pfkWyYk67c4Yf+KWwcGy6JDOwTaaflpyEM2NAWLNSjnba720efV14TMHZM1ArGcUVAfh0++0XyceReD
RcwW1isgpRlQJrtzYEDgPDNSmrq3vBFPzNlF8pvSYNPaXAfD4fiWRI5QkX5JUWOQC3xyEqV67OMnFXBuDZiCR2QFwoQEc
VR344quRPx+5bQUj35jdPBjwZFexL1YtJg8KOs5BCD87eMfc68NM9CL2QqZHvfwOyO5iAWfGbYsGxuQqXhLNq5tMgJTFn
u6UUZHSLgQwWOFHopu7QJFz0TAK9x4JC+KwbFGKC067x3Xl96NUf3e8WAVweUQwAPGnY+eUtZsBI/ltCzCTLd/9RSISSR
3wKqEz5jS7jAdfrGNUytlSmG0PXroz9wf0SIjZPovFevucg3BzvjoVRPI8T9ldRV4pQWGhh0EC37SwWTjl7XbM</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 **RequestSecurityToken** request 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
TlRMTVNTUAADAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAANcKY4gYAchcAA
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 **RequestSecurityTokenResponse**. 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: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,czhRNuPUw78kO1B8tNfnUKLDhd5xYPnTN2S
6Qu5DtXIQLjEEMnNPiuKpnMuwqeRxObyq4ycW08i+C63CGhp9EZca/1ZpgiqKfWCsB+x1MfspqYLurgphmkvz9uCkdFb0
QEOeYZXRf7OXYLGgCVdmbKwnG5M+j74wZq8l6MuE30+Ffb5kV14g2kg/7MApGZGEyQ4hwxEeZI0QdB/HFzyZkL81YQNWP
e+/O9dNUEMWLho/ws0kxhKSEHkuqaLLLkLMrEzPRsHdIKNSgmPq3kD3I+BIbaNvZW5IwXX2r4IJNMkLufiIshaRoKmveW
WsSO3ZYI2Ls34FxvH/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>
              <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="#_667b495b-bd0a-486f-b1fd-a754730e0b4b">
                <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>K2b6djB70uIBZcjCBhjzMMRYx25qPWcIoTFg9FlOIBs=</ds:DigestValue>
              </ds:Reference>
            </ds:SignedInfo>

<ds:SignatureValue>ExTNHbiSRiIZSF3zzTVtVrUaunYqhhUZZD7brFzZs2saqdY5JVjEG6renMcNO/oLVahvVE4Gt1
zMaN+Q061uyWUhO+kDfZhYdFl7xa6k5iVx47EMBdnd1mfws6zoiseScgTDsA/xHj2YmkH5dUt1lbtvXm/I6wGg9QrUmcC
JYK6/nRA67oN87LubvvsrQuTfg31NDP+ZkhdiILPLlIBvZvhgNE6irMix3HpXG37uJOqYy3S3uu4RebCQZo+DPl55KGm0
D+t+fzg1IZxq1jk6l9TvTKZu+g8Y7h+bXSE5HjPphaPAdhDYTOchnE/v1zBfLSNeL9kjGepHqimurgSfUg==</ds:Sign
atureValue>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>

<X509Certificate>MIIERjCCAi6gAwIBAgIQIpKr6+DF745AAUgms+NDuDANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQG
EwJVUzESMBAGA1UEChMJTWljcm9zb2Z0MRMwEQYDVQQLEwpTaGFyZVBvaW50MSIwIAYDVQQDExlTaGFyZVBvaW50IFJvb
3QgQXV0aG9yaXR5MCAXDTEwMDEzMTE3NTgyMFoYDzk5OTkwMTAxMDAwMDAwWjBiMQswCQYDVQQGEwJVUzESMBAGA1UECh
MJTWljcm9zb2Z0MRMwEQYDVQQLEwpTaGFyZVBvaW50MSowKAYDVQQDEyFTaGFyZVBvaW50IFNlY3VyaXR5IFRva2VuIFN
lcnZpY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCtEOD88wj3QfhNIWR1hmO3Dt6YTohjfy/5PpjvezbU
ud06cble90CyFqdg3ImE/T3PWLsU8mexFxzCuL5flqA9QYMSvhYZSDTWoy6MltMQlPRti7mqToH3dUGMFpD24DKGrXww6
ezMdNn1bi9PiQEr5a9JemeVxoPhvasT5C5fG5snXsbmh7JjKH46zaV1o7/8H7Nikp2aw0YOKMWqwllVed3o30k/jo06oH
GUiWqm3yVDvHUTb/RsK0LHUIySwXoakr45IWU5jJVsQD/8Zn8qaNLa3cNbnwIuBYneIICkNtIULO/qdbTXXiev04g3oez
gfvqMZRBCO02PQnSmNBFVAgMBAAEwDQYJKoZIhvcNAQEFBQADggIBAHx+Z9uj3lSzduTbhTVBKyf4kJUMYVQHRPnKDCEO
JfLDFEZ8u5GgoNLVJ9SmC3FVvdWPoD5qClE+sxtF/StkJXgN6dKrQE77EE5uMXQFq3eU8tJEqmW5TDY5J0GwdTWSVbwQk
eMD4q/+t+uNF5TqzF7sr5OZrhEl4ZUYh60vgPe52ZxXOsLIsP2jz4HPPCqSW1CgVD3TSu9w6ugH7HqlM0vDXGUG491CwS
Nt36E+RExzK2kIu6cX5AtXrVhv5QEkERb8A6JA95dPiEkdQSB8iBaogAh5IbAtYwg4fsXnX3JB6jhNOcp0DxNl9/+rC3M
th4N9kYodGnqzEVzlkBEZiwSVg7btOUeWCXEQEwWKrC2IUI0Ucayqm69QJ+fUsrKZ5jsJS479DUcdSjJc9HAsY4iS5S6H
J0zK+OMwDgw8XDTd5dH3ARqDgtJa891X5zMULHXFo7R/CBchYswd8xkUNhAmbuiWzNl5NjFdEhqSt0JBWw0ogWjC9sgme
sAO42xnBmxof0ASsuwerp152E8iWRB/wcBtk/cfaNFRh6/3UKSq5Fy41ae3mGPHTylxCHDHeXvmur96mdbyUHyvI2bnWX
```

```
0mN1WeuP3MF+jKFhvsACixgLFJy71wiDthd0aVEUUt4MTYMMsmshQQwLh0stpp3UD3y477dz5LN0yzN9VURfBu</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">_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: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 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 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:msc="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:wsu="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="AsymmetricWindowsHttp_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SymmetricBinding xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:SpnegoContextToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/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-sx/ws-
securitypolicy/200702">
          <wsp:Policy>
            <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never" wsp:Optional="true"/>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sp:Wss11 xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
          <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>
        <msb:BinaryEncoding
xmlns:msb="http://schemas.microsoft.com/ws/06/2004/mspolicy/netbinary1"/>
        <wsaw: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>
  <wsp:Policy wsu:Id="AsymmetricWindowsHttp_Trust13Renew_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_Trust13Renew_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_Trust13Validate_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_Trust13Validate_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>
  <wsdl:import
namespace="http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice"
location="http://example.com/_vti_bin/sts/spsecuritytokenservice.svc?wsdl"/>
  <wsdl:types/>
  <wsdl:binding name="AsymmetricWindowsHttp" type="i0:IWSTrust13Sync">
    <wsp:PolicyReference URI="#AsymmetricWindowsHttp_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>
        <wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Cancel_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Cancel_output_policy"/>
        <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>
        <wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Issue_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference URI="#AsymmetricWindowsHttp_Trust13Issue_output_policy"/>
        <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>
        <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">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Validate" style="document"/>
      <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 released service packs.

- 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

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

This section identifies changes that were made to this document since the last release. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- The removal of a document from the documentation set.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the technical content of the document is identical to the last released version.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.
- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.
- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated**.

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact dochelp@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
2.2.2.2.1.1 Attribute Element	Clarified the description to indicate that the Attribute element must contain several listed attributes and elements.	Y	Content update.

9 Index

S

T

V

W