[MS-CTAP]:
CardSpace Token Acquisition Protocol Specification

Revision Summary

Date	Revision History	Revision Class	Comments
06/20/2008	0.1		Initial Availability
07/25/2008	0.1.1	Editorial	Revised and edited the technical content.
10/24/2008	0.1.2	Editorial	Revised and edited the technical content.
12/05/2008	0.2	Minor	Updated the technical content.
01/16/2009	0.3	Minor	Updated the technical content.
02/27/2009	1.0	Major	Updated and revised the technical content.
04/10/2009	2.0	Major	Updated and revised the technical content.
05/22/2009	2.1	Minor	Updated the technical content.
07/02/2009	3.0	Major	Updated and revised the technical content.
08/14/2009	4.0	Major	Updated and revised the technical content.
09/25/2009	5.0	Major	Updated and revised the technical content.
11/06/2009	5.1	Minor	Updated the technical content.
12/18/2009	5.2	Minor	Updated the technical content.
01/29/2010	5.3	Minor	Updated the technical content.
03/12/2010	5.3.1	Editorial	Revised and edited the technical content.
04/23/2010	5.4	Minor	Updated the technical content.
06/04/2010	6.0	Major	Updated and revised the technical content.
07/16/2010	7.0	Major	Significantly changed the technical content.
08/27/2010	7.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	7.0	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	7.1	Minor	Clarified the meaning of the technical content.
01/07/2011	7.2	Minor	Clarified the meaning of the technical content.
02/11/2011	7.2	No change	No changes to the meaning, language, or formatting of the technical content.

Contents

1 Introduction

The CardSpace Token Acquisition Protocol defines restrictions on the Web Services (WS) MetadataExchange [WSMETA] and WS-Trust [WSTrust1.3] protocols. The protocol is used by clients to obtain a **security token** from a **Security Token Service (STS)**.

This protocol is based on Web Services (WS) Metadata Exchange and Trust protocols.

1.1 Glossary

The following terms are defined in [MS-GLOS]:

base64
Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)
.NET Framework
Secure Sockets Layer (SSL)
signature
SOAP
SOAP body
SOAP envelope
SOAP fault
SOAP header
symmetric key
Transport Layer Security (TLS)
URI
X.509

The following terms are specific to this document:

claim: A statement made about one subject such as a user, service or other resource by another subject. Examples are name, e-mail address, key, group membership, privilege, capability, etc. For more information, see WS-Trust [WSTrust1.3] section 2.4.

endpoint: WS-Addressing Endpoint References and Identity, a (referenceable) entity, processor, or resource where Web service messages can be targeted. WS-Addressing Endpoint references convey the information needed to reference a Web service **endpoint**, and may be used in several different ways; **endpoint** references are suitable for conveying the information needed to access a Web service **endpoint**, but are also used to provide addresses for individual messages sent to and from Web services. For more information, see [WSAIdentity].

relying party (RP): A Web application or service that consumes **security tokens** issued by a **Security Token Service (STS)**. For more information, see WS-Federation [WSFederation] sections 1.6 and 2.

Security Assertion Markup Language (SAML): A standard XML framework for exchanging security information between business partners over the Internet. SAML was created by the Organization for the Advancement of Structured Information Standards (OASIS).

security token: A collection of one or more **claims**. A **security token** may be signed to preserve its integrity and to identify the asserting party. For more information, see Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) [WSS] section 2.4 and 6.

Security Token Service (STS): A Web service that issues **security tokens**. The **STS** makes assertions based on evidence that it **trusts** to whoever else that trusts the **STS**. For more information, see WS-Trust [WSTrust1.3].

trust: A characteristic that one entity is willing to rely upon a second entity to execute a set of actions and/or to make set of assertions about a set of subjects and/or scopes.

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

1.2 References

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.

[Excl-C14N] Boyer, J., Eastlake 3rd, D. E., and Reagle, J., "Exclusive XML Canonicalization Version 1.0", July 2002, http://www.w3.org/TR/xml-exc-c14n/

[IMI] OASIS Standard, "Identity Metasystem Interoperability V1.0", July 2009, http://docs.oasis-open.org/imi/identity/v1.0/identity.html

[MS-WSPOL] Microsoft Corporation, "Web Services: Policy Assertions and WSDL Extensions", September 2009.

[RFC1738] Berners-Lee, T., Masinter, L., and McCahill, M., "Uniform Resource Locators (URL)", RFC 1738, December 1994, http://www.ietf.org/rfc/rfc1738.txt

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

[RFC2246] Dierks, T., and Allen, C., "The TLS Protocol Version 1.0", RFC 2246, January 1999, http://www.ietf.org/rfc/rfc2246.txt

[RFC2396] Berners-Lee, T., Fielding, R., and Masinter, L., "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998, http://www.ietf.org/rfc/rfc2396.txt

[RFC2478] Baize, E., and Pinkas, D., "The Simple and Protected GSS-API Negotiation Mechanism", RFC 2478, December 1998, http://www.ietf.org/rfc/rfc2478.txt

[RFC2616] Fielding, R., Gettys, J., Mogul, J., et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, http://www.ietf.org/rfc/rfc2616.txt

[RFC3986] Berners-Lee, T., Fielding, R., and Masinter, L., "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005, http://www.ietf.org/rfc/rfc3986.txt

[SAMLASchema] OASIS Standard, "Security Assertion Markup Language (SAML) V1.1 XML Schema", September 2003, http://www.oasis-open.org/committees/download.php/3408/oasis-sstc-saml-schema-assertion-1.1.xsd

[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

[SOAP1.2-1/2007] Gudgin, M., Hadley, M., Mendelsohn, N., et al., "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) ", W3C Recommendation 27, April 2007, http://www.w3.org/TR/2007/REC-soap12-part1-20070427/

[SOAP1.2-2/2007] Gudgin, M., Hadley, M., Mendelsohn, N., et al., "SOAP Version 1.2 Part 2: Adjuncts (Second Edition)", W3C Recommendation, April 2007, http://www.w3.org/TR/2007/REC-soap12-part2-20070427

[WSA] Gudgin, M., Hadley, M., and Rogers, T., "Web Services Addressing 1.0 - Core", W3C Recommendation, May 2006, http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/

[WSAIdentity] Alexander, J., Della-Libera, G., Gudgin, M., et al., "Application Note: Web Services Addressing Endpoint References and Identity", August 2008, http://schemas.xmlsoap.org/ws/2006/02/addressingidentity/WS-AddressingAndIdentity.pdf

[WSAWSDL] World Wide Web Consortium, "Web Services Addressing 1.0 - WSDL Binding", May 2006, http://www.w3.org/TR/2006/CR-ws-addr-wsdl-20060529/

[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

[WSMETA] Ballinger, K., Bissett, B., Box, D., et al., "Web Services Metadata Exchange (WS-MetadataExchange)", Version 1.1, August 2006, http://specs.xmlsoap.org/ws/2004/09/mex/WS-MetadataExchange.pdf

[WS-Policy] Siddharth, B., Box, D., Chappell, D., et al., "Web Services Policy 1.2 - Framework (WS-Policy)", April 2006, http://www.w3.org/Submission/2006/SUBM-WS-Policy-20060425/

[WSPolicyAtt] BEA Systems, IBM, Microsoft Corporation, SAP, Sonic Software, VeriSign, "Web Services Policy 1.2 - Attachment (WS-PolicyAttachment)", April 2006, http://www.w3.org/Submission/WS-PolicyAttachment/

[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

[WSSKerb] OASIS, "Web Services Security Kerberos Token Profile 1.1", February 2006, http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-KerberosTokenProfile.pdf

[WSSP] Della-Libera, G., Gudgin, M., Hallam-Baker, P., et al., "Web Services Security Policy Language (WS-SecurityPolicy)", July 2005, http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-secpol/ws-secpol.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

[WSTrust1.3] Lawrence, K., Kaler, C., Nadalin, A., et al., "WS-Trust 1.3", March 2007, http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html

[WSTSPNego] Alexander, J., Gajjala, V., Gavrylyuk, K., et al., "Application Note: Using WS-Trust for Simple and Protected Negotiation Protocol", September 2007, http://schemas.xmlsoap.org/ws/2005/02/trust/spnego/WSTrustForSPNego.pdf

[WSSUTP] OASIS Standard, "Web Services Security UsernameToken Profile 1.0", March 2004, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf

[WSSX509TP] OASIS Standard, "Web Services Security X.509 Certificate Token Profile", March 2004, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf

[WXFR] Alexander, J., Box, D., Cabrera, L.F., et al., "Web Services Transfer (WS-Transfer)", September 2006, http://www.w3.org/Submission/2006/SUBM-WS-Transfer-20060927/

[X509] ITU-T, "Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks", Recommendation X.509, August 2005, http://www.itu.int/rec/T-REC-X.509/en

Note There is a charge to download the specification.

[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/

[XMLDSig/2002] Bartel, M., Boyer, J., Fox, B., LaMacchia, B., and Simon, E., "XML-Signature Syntax and Processing", February 2002, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[XMLEnc] Imamura, T., Dillaway, B., and Simon, E., "XML Encryption Syntax and Processing", W3C Recommendation, December 2002, http://www.w3.org/TR/xmlenc-core/

[XMLNS-2ED] World Wide Web Consortium, "Namespaces in XML 1.0 (Second Edition)", August 2006, http://www.w3.org/TR/2006/REC-xml-names-20060816/

[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", March 2007.

[RFC2246] Dierks, T., and Allen, C., "The TLS Protocol Version 1.0", RFC 2246, January 1999, http://www.ietf.org/rfc/rfc2246.txt

[RFC3546] Blake-Wilson, S., Nystrom, M., Hopwood, D., et al., "Transport Layer Security (TLS) Extensions", RFC 3546, June 2003, http://www.ietf.org/rfc/rfc3546.txt

[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.

1.3 Overview

The [WSTrust1.3] specification defines a standard mechanism that may be used by a client to acquire a security token from a Security Token Service (STS). Acquiring a security token is designed to address two problems related to communicating user information to remote applications and services.

First, in order to properly control access to information or resources in remote applications, those applications must have information about the users that are accessing them. Previous solutions required the application to identify the user and use that identity to access additional information about the user. Second, users were forced to be prompted multiple times to supply credentials (for example, supply user names and passwords) to securely identify themselves and authenticate to multiple applications.

Implementations of [WSTrust1.3] solve these problems by moving the responsibility for authenticating the user away from the remote application to an STS that already has an account for the user. The STS issues security tokens that contain information about the user in the form of **claims**. When accessing an application, the user's client agent presents a security token that is obtained from an STS to the application. The **signature** in the security token allows the application to verify its validity, and the claims in the security token convey relevant user information to the application. These claims can then be used for making authorization decisions by the application. In this scenario, the application is a **relying party (RP)** that relies upon the claim information that is issued by the STS.

The CardSpace Token Acquisition Protocol increases interoperability of [WSTrust1.3] by restricting the protocol options and the variations of security tokens that may be included in [WSTrust1.3]. This protocol also adds optional parameters to address existing limitations to the protocol.

The CardSpace Token Acquisition Protocol is used by a client to acquire a security token from a Security Token Service (STS). The underlying protocols that are used by this protocol enable the STS to specify how messages must be structured and secured via Service Metadata Exchange messages. The STS and the client can further negotiate the user authentication and message protection cryptography using Message Protection Negotiation messages. Finally, the client uses [WSTrust1.3] to request the token from the STS according to the results of the previous capability and security negotiations.

This protocol specification describes restrictions on the choice of message transport that is allowed for all the request messages in section 2.1. Section 2.2 specifies restrictions imposed on the request and response message syntax in order to aid interoperability by reducing the possible variations in this protocol; the restrictions are specified for obtaining service metadata information, performing message protection negotiation, and acquiring a security token. Additional parameters are described for communicating user pseudonym information, communicating client state, and requesting and returning a user readable description of the security token contents.

The protocol specification describes the message processing model in section 3 for the client and the STS to successfully emit or consume protocol messages that are created in accordance with section 2.

1.4 Relationship to Other Protocols

The CardSpace Token Acquisition Protocol defines restrictions on the Web Services (WS) MetadataExchange [WSMETA] and WS-Trust [WSTrust1.3] protocols. The CardSpace Token Acquisition Protocol uses standard Web protocols. The reader should be familiar with the IETF specifications:

- Hypertext Transfer Protocol (HTTP), as specified in [RFC2616].

- Uniform Resource Identifiers (URIs), as specified in [RFC2396].
- Uniform Resource Locators (URLs), as specified in [RFC1738].

URLs and URIs are used to describe the data used in the protocol.

The CardSpace Token Acquisition Protocol uses Extensible Markup Language (XML); the following specifications are used to describe the requirements for the XML syntax involved in the protocol. The reader should be familiar with the following W3C specifications:

- Exclusive XML Canonicalization Version 1.0, as specified in [Excl-C14N].
- Extensible Markup Language (XML) 1.0 (Fourth Edition), as specified in [XML].
- Namespaces in XML, as specified in [XMLNS-2ED].
- SOAP Version 1.2, as specified in [SOAP1.2-1/2007] and [SOAP1.2-2/2007].
- XML Encryption Syntax and Processing, as specified in [XMLEnc].
- XML Schema Part 1: Structures Second Edition, as specified in [XMLSCHEMA1].
- XML Schema Part 2: Datatypes Second Edition, as specified in [XMLSCHEMA2].
- XML-Signature Syntax and Processing, as specified in [XMLDSig/2002].

The CardSpace Token Acquisition Protocol uses WS-MetadataExchange [WSMETA] for Web services capability negotiation. The protocol also uses WS-Trust [WSTrust1.3] for security token issuance. On the whole, the reader should be familiar with the following WS-* specifications:

- WS-Addressing, as specified in [WSA].
- WS-MetadataExchange, as specified in [WSMETA].
- WS-Policy, as specified in [WS-Policy].
- WS-SecureConversation as specified in [WSSC].
- WS-Security Policy as specified [WSSP].
- WS-Security: SOAP Message Security 1.1 as specified in [WSS].
- WS-Transfer as specified in [WXFR].
- WS-Trust, as specified in [WSTrust1.3].
- Using WS-Trust for SPNego as specified in [WSTSPNego].

The protocol uses Security Assertion Markup Language (SAML) v1.1 Assertions to communicate security tokens. The reader should be familiar with the OASIS specification for SAML v1.1 Assertions (as specified in [SAMLCore]) and the SAML v1.1 XML Schema (as specified in [SAMLASchema]).

1.5 Prerequisites/Preconditions

It is a requirement that, before the protocol is invoked, a CardSpace Token Acquisition Protocol client has obtained both the Service Metadata Exchange endpoint URL for the server it wants to communicate with and the Security Token Service (STS) endpoint URL. How a client obtains these URLs is not addressed in this specification.

1.6 Applicability Statement

The CardSpace Token Acquisition Protocol is used by a client who needs to present user information to a relying party in the form of a security token that has been signed by a Security Token Service (STS). This protocol is applicable for HTTP-based applications and agents running on the client's behalf.

1.7 Versioning and Capability Negotiation

1.7.1 Versioning

This protocol uses the versioning mechanisms defined in the following specifications:

- Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1 [SAMLCore] for syntax and semantics for XML-encoded assertions about authentication, attributes and authorization.
- WS-MetadataExchange [WSMETA] for endpoints description with various authentication types.
- WS-SecureConversation [WSSC] for providing secure communication across messages.
- WS-Security Policy [WSSP] for using security policy assertions with WS-Policy [WS-Policy] with respect to security features provided in WS-Security: SOAP Message Security 1.1 [WSS], WS-Trust [WSTrust1.3], and WS-SecureConversation [WSSC].
- WS-Security: SOAP Message Security 1.1 [WSS] for conducting secure SOAP message exchanges.
- WS-Transfer [WXFR] for accessing XML representations of Web Service-based resources.
- WS-Trust [WSTrust1.3] for security token request and response message exchange.
- Using WS-Trust for SPNego [WSTSPNego] for establishing of a shared security context.
- XML Encryption Syntax and Processing [XMLEnc] for encrypting data and representing the result in XML.
- XML-Signature Syntax and Processing [XMLDSig/2002] for XML digital signature processing rules and syntax.

This document does not introduce any additional versioning mechanism.

1.7.2 Capability Negotiation

This protocol uses the capability negotiation mechanisms defined in the following specifications:

- WS-MetadataExchange [WSMETA] for communicating WS-Policy and WS-SecurityPolicy capability requirements and descriptions.
- WS-Policy [WS-Policy] for asserting capability requirements and descriptions of the service.
- WS-Security Policy [WSSP] for asserting security specific capability requirements and descriptions of the service.
- Using WS-Trust for SPNego [WSTSPNego] for negotiating a shared security token to secure protocol messages by tunneling SPNego through WS-Trust.

- WS-SecureConversation [WSSC] for negotiating a shared security token to secure protocol messages.

This document does not introduce any additional capability negotiation mechanism.

1.8 Vendor-Extensible Fields

As specified in section 2, the CardSpace Token Acquisition Protocol uses the SAML 1.1 token format, as specified in [SAMLCore]. Vendors MAY extend the SAML Advice element to contain additional information. The XML elements placed under the SAML 1.1 Advice element may be guaranteed to be unique if the vendor registers the XML namespace URN with the Internet Assigned Numbers Authority (IANA).

As specified in section 2, the CardSpace Token Acquisition Protocol uses SOAP messages for communication, as specified in [SOAP1.2-1/2007]. Core functionality of SOAP is to provide extensibility as specified in section 3 of the [SOAP1.2-1/2007] — that section contains detail discussion on SOAP messaging framework extensibility model.

As specified in section 2, the CardSpace Token Acquisition Protocol uses the Security, SecurityTokenReference, and BinarySecurityToken elements in WS-Trust request and response messages. Refer to [WSS] for the extensibility mechanism for the aforementioned elements.

As specified in section 2, the CardSpace Token Acquisition Protocol uses various assertions stated in the Security Assertion Model of [WSSP]. Vendor-extensible fields in [WS-Policy] are applicable since [WSSP] defines security policy assertions for using [WS-Policy] framework.

As specified in section 2, the CardSpace Token Acquisition Protocol uses RequestSecurityToken and RequestSecurityTokenResponse elements respectively, as specified in sections 3 and 4 of [WSTrust1.3]. Both RequestSecurityToken and RequestSecurityTokenResponse elements allow additional child elements to be added to contain additional information; refer to [WSTrust1.3] for details on extending the elements.

As specified in section 2, the CardSpace Token Acquisition Protocol uses Security Context Token (SCT), as specified in [WSSC]. Vendors can extend the SecurityContextToken element to contain additional information; refer to [WSSC] for details on extending the element.

Vendors may use these existing extensibility points as specified in the CardSpace Token Acquisition Protocol and the protocols referenced above.

1.9 Standards Assignments

There are no standards assignments for the WS-Trust: CardSpace Token Acquisition Extensions protocol beyond those defined in the following specifications:

- Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1, as specified in [SAMLCore].
- SOAP 1.2, as specified in [SOAP1.2-1/2007] and [SOAP1.2-2/2007].
- WS Policy 1.2 - Attachment, as specified in [WSPolicyAtt].
- WS-Addressing, as specified in [WSA].
- WS-MetadataExchange, as specified in [WSMETA].
- WS-Policy, as specified in [WS-Policy].

- WS-SecureConversation, as specified in [WSSC].
- WS-SecurityPolicy, as specified [WSSP].
- WS-Security: SOAP Message Security 1.1, as specified in [WSS].
- WS-Transfer, as specified in [WXFR].
- WS-Trust, as specified in [WSTrust1.3].
- Using WS-Trust for SPNego, as specified in [WSTSPNego].
- XML Encryption Syntax and Processing, as specified in [XMLEnc].
- XML-Signature Syntax and Processing, as specified in [XMLDSig/2002].
- Unless otherwise indicated, MSFT implementation follows all RECOMMENDED, SHOULD, MUST, MUST NOT, and SHOULD NOT behavior of the specifications above.

2 Messages

This section specifies the transport and syntax of request and response messages in normative detail.

2.1 Transport

All of the request and response messages described in sections 3.1.4.4 and 2.2 MUST use the **SOAP** HTTP binding described in section 7 of [SOAP1.2-2/2007].

For WS-MetadataExchange and **HTTPS** GET requests, the client MUST authenticate the IP/STS using **Secure Sockets Layer (SSL)**/**Transport Layer Security (TLS)** transport security (for more information, see [RFC2246] and [RFC3546]) and **X.509** certificates (as specified in [X509]).

2.2 Common Message Syntax

This section contains common definitions used by this protocol. The syntax of the definitions uses XML Schema as defined in [XMLSCHEMA1] and [XMLSCHEMA2], and Web Services Description Language as defined in [WSDL].

2.2.1 Namespaces

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
wsdl	"http://schemas.xmlsoap.org/wsdl/"	[WSDL]
xsd	"http://www.w3.org/2001/XMLSchema"	[XMLSCHEMA1]
t	"http://schemas.xmlsoap.org/ws/2005/02/trust"	This specification.
soapenc	"http://schemas.xmlsoap.org/soap/encoding/"	[SOAP1.2-1/2007]
tns	"http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice"	This specification.
wsam	"http://www.w3.org/2007/05/addressing/metadata"	[WSA]
soap12	"http://schemas.xmlsoap.org/wsdl/soap12/"	[SOAP1.2-1/2007]
wsa10	"http://www.w3.org/2005/08/addressing"	[WSA]
wsa	"http://schemas.xmlsoap.org/ws/2004/08/addressing"	[WSA]
wsaw	"http://www.w3.org/2006/05/addressing/wsdl"	[WSAWSDL]
wsx	"http://schemas.xmlsoap.org/ws/2004/09/mex"	[WSMETA]
wsap	"http://schemas.xmlsoap.org/ws/2004/08/addressing/policy"	[WS-Policy]

Prefix	Namespace URI	Reference
wsu	"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"	[WSS]
trust	"http://docs.oasis-open.org/ws-sx/ws-trust/200512"	[WSTrust1.3]
wsp	"http://schemas.xmlsoap.org/ws/2004/09/policy"	[WS-Policy]
sp	"http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"	This specification
sp	"http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"	[WSSP]

2.2.2 Messages

This protocol does not contain any WSDL messages that are used in more than one operation.

2.2.3 Elements

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

2.2.4 Complex Types

This specification does not define any common XML Schema complex type definitions.

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.

3 Protocol Details

The protocol specifies three distinct roles for the entities that emit, transport, and consume protocol messages. Only the client and Security Token Service (STS) roles directly participate in the protocol interaction. The relying party role consumes tokens, but is not involved in this protocol. The client and the STS roles are described below in separate subsections.

3.1 Common Details

This section describes protocol details that are common between multiple port types.

3.1.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

3.1.1.1 Claims

Security tokens provide a data structure for communicating sets of claims. The claims are encoded in the security token as pairs of a claim type and value. Each security token has an issuer and a subject (who the claims are about). The security token thus provides a way to communicate the claims about a subject while retaining the data about the issuer of those claims. This model is useful for communicating user identity information across **trust** boundaries. As described in sections 3.7.4.1.2.1.6, 3.6.4.1.2.23, and 3.7.3, requests for specific claim types are included in the overall request sent from the client to the Security Token Service (STS).

The Token Acquisition message that is sent from the client also serves to authenticate the client user to the STS. Once authenticated, the claims present in any security tokens present are available to be used by the STS when issuing its token. The STS may also use data from the authenticated claims to look up more information about a user that is maintained by the STS or its affiliates. The STS then uses both the claims present from incoming security tokens and the claims obtained from cached data to issue a token. The STS may maintain local policy for which claims are issued. This policy defines business logic for what claims may be accepted from other STSs and affiliates, and how those claims map to claims issued by the STS.

3.1.1.2 Abstract Interface for Initiating Protocol

The client initiates the protocol when a higher laver on the client system calls the client implementation to obtain a token. The higher layer can pass the following data: the **Relying Party URI**, the **Relying Party X509 Certificate**, a **Requested Key Type**, a set of **Requested Claim Types**, the **STS Service Metadata Exchange Endpoint**, and the **STS Token Acquisition Endpoint**. The semantics of these values and their mapping to message syntax are specified in section 3.7.1. All values are optional. If the **STS Service Metadata Exchange Endpoint** are omitted, the client must have a corresponding endpoint by some other means (such as configuration); otherwise, there is not sufficient information to initiate the protocol.

When the protocol completes, the client returns the contents of the <RequestedSecurityToken> element (section 3.6.4.1.2.28) to the higher layer. If the protocol does not have a <RequestedSecurityToken> element (section 3.6.4.1.2.28) or results in a fault, a fault is returned to the higher layer.

3.1.2 Timers

The security tokens that are transported in protocol messages have a specific time interval during which they are considered to be valid. The Security Token Service (STS) that issues the security tokens MUST set the time interval by using the **NotBefore** and **NotOnOrAfter** attributes of the <Conditions> element. For more details, see [SAMLCore] section 2.3.2.1.1.

Timers are not used to determine when validity intervals expire. The **NotBefore** and **NotOnOrAfter** values that are obtained from the received security tokens MUST be explicitly checked for validity.

3.1.3 Initialization

Initialization is specific to the client and server details of each port type.

3.1.4 Message Processing Events and Sequencing Rules

The following sections detail common sequencing, structure and error conditions.

3.1.4.1 Client Message Sequencing Requirements Across Port Types

The protocol begins with an exchange of Security Token Service (STS) metadata using Prerequisite Service Metadata Exchange endpoint URL, followed by an optional exchange of Message Protection Negotiation message, and end with a Token Acquisition exchange. This sequencing is detailed in the subsequent sections, grouped by the type of exchange that occurs.

The sequence for messages in the protocol MUST be as follows:

1. Service Metadata Exchange request.
2. Service Metadata Exchange response.
3. (Optionally) Message Protection Negotiation request/responses.
4. Token Acquisition request.
5. Token Acquisition response.

The data obtained by the client in the Service Metadata Exchange response enables the client to appropriately format the Token Acquisition request for the STS. The data from the Service Metadata Exchange response also determines the method used to prove the identity of the client user to the STS. The remainder of the Token Acquisition Request Message is determined by the pre-existing relying party data described in section 3.7.3. The Token Acquisition Response Message contains the security token for the client to be able to use. The client then submits the token to the relying party to prove the identity of the user to the relying party. The submission of the token to the relying party is outside the scope of this protocol.

The client MUST fault in either of these conditions:

- The client does not receive a Token Acquisition Response from the Security Token Service.
- The client does not receive a Service Metadata Exchange response from the Security Token Service.

When the client receives a server response that violates a MUST of the protocol, the client MUST fault unless otherwise noted.

3.1.4.2 Server Message Sequencing Requirements Across Port Types

The protocol MUST begin with an exchange of Security Token Service (STS) service metadata, followed by Message Protection Negotiation message exchange(s), and end with a Token Acquisition exchange. The client role controls the sequencing of the messages. The server role requires only that if a Token Acquisition request message needs to refer to the result of a Message Protection Negotiation message exchange, that Message Protection Negotiation message exchange MUST be completed prior to receiving the Token Acquisition request message. If the server receives a Token Acquisition request message referring to the result of a Message Protection Negotiation message exchange that has not yet occurred or completed, it MUST fault. There are no further requirements for the server role on the expected sequence of receiving request message types. This sequencing is detailed in the subsequent sections, grouped by the type of exchange that occurs.

When the server receives a client request that violates a MUST of the protocol, the server MUST fault unless otherwise noted.

3.1.4.3 Message Structure

All protocol messages MUST be well-formed XML placed within a **SOAP envelope** conforming to [SOAP1.2-1/2007] section 5.1.

3.1.4.4 Error Handling

When a malformed message is received, the server MUST respond with a SOAP fault conforming to [SOAP1.2-1/2007] section 5.4.

3.1.5 Timer Events

There are no protocol-specific timer events that are serviced by an implementation. This protocol does not require timers except those that may be used by the underlying transport to transmit and receive messages over HTTP. The protocol does not include provisions for time-based retry for sending protocol messages.

3.1.6 Other Local Events

This protocol does not have dependencies on any transport protocols other than HTTP 1.1. This protocol relies on this transport mechanism for the correct and timely delivery of protocol messages. The protocol does not take action in response to any changes or failure in machine state or network communications.

3.2 Service Metadata Exchange Server Details

The following sections detail the server details for Service Metadata Exchange port type. The port type name for Service Metadata Exchange is MetadataExchange.

3.2.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

Section 3.3.1 of the abstract data model for clients applies equally well to the abstract data model for servers.

3.2.2 Timers

There are no protocol-specific timer events that are serviced by an implementation. The protocol does not include provisions for time-based retry for sending protocol messages.

3.2.3 Initialization

There are no server specific initialization requirements.

3.2.4 Message Processing Events and Sequencing Rules

Service Metadata Exchange messages can be sent by using HTTPS GET, or by using SOAP messages, as specified by [WSMETA] and further specified below. For further details on how an implementation chooses which messages to use, refer to section 3.3.3.

Simple HTTPS GET avoids using SOAP-based WS-MetadataExchange to obtain the WSDL metadata described below. The request message MUST be an HTTPS GET message to the URL that supports providing WSDL metadata. The response message MUST contain an HTTP status code of 200, with the WSDL metadata in the body of the response.

The following table summarizes the list of WSDL operations as defined by this specification:

Operation	Description
GetMetadata	Used to obtain the WSDL of a service.

3.2.4.1 Get Metadata

The first message of the protocol MUST be a Service Metadata Exchange request message conforming to section 3.2.4.1.1.1. This message MUST be sent to the STS's Service Metadata Exchange endpoint. An STS Implementation SHOULD choose to implement either HTTPS GET and/or WS-MetadataExchange types of messages.<1> The response to this request message MUST be the Service Metadata Exchange response corresponding to the type of request message originally sent. If an HTTPS GET Service Metadata Exchange request message was sent, an HTTPS GET Service Metadata Exchange response message MUST be sent in response. If a WS-MetadataExchange Service Metadata Exchange request message was sent, a WS-MetadataExchange Service Metadata Exchange response message MUST be sent in response.

Simple HTTPS GET avoids using SOAP-based WS-MetadataExchange to obtain the WSDL metadata described in section 3.2.4.1.2.3. The request message MUST be an HTTPS GET message to the URL that supports providing WSDL metadata. The response message MUST contain an HTTP status code of 200, with the WSDL metadata in the body of the response.

The STS MUST respond to this message with a Service Metadata Exchange response message conforming to section Using WS-MetadataExchange for Service Metadata Exchange Messages. The Service Metadata Exchange response message contains the WSDL document for the STS as specified in section Using WS-MetadataExchange for Service Metadata Exchange Messages. Each <wsdl:port> element defines an endpoint that references a <wsdl:binding> element.

The content of these <Policy> elements MUST affect the content and sequencing of future messages as described in section 3.2.4.1.1.2.1.

3.2.4.1.1 Messages

The following table summarizes the set of WSDL message definitions that are specific to this operation.

Message	Description
GetMetadataMSg	Requests the WSDL
GetMetadataResponseMsg	A response containing the WSDL

3.2.4.1.1.1 GetMetadataMsg

This message MUST be a WS-Transfer Get message as described in [WSMETA] section 5.1. The message MUST conform to the WS-Transfer Get message described in [WXFR] section 3.1 and the schema found in [WXFR] Appendix I - XSD.

3.2.4.1.1.2 GetMetadataResponseMsg

This message MUST be a response to the WS-Transfer Get message described in section 3.2.4.1. The message MUST conform to the WS-Transfer Get response message detailed in [WXFR] section 3.1. The SOAP body is specified in section 5.1 of [WSMETA]. The first element of the SOAP body of the WS-Transfer Get MUST be a Web service <Metadata> element conforming to [WSMETA] section 4.

3.2.4.1.1.2.1 Effects of Policy Elements with Endpoint Policy Subject

[WSSP] defines the effects of security policy assertions with endpoint policy subject for the protocol. The policy assertions returned in the WSDL of a Service Metadata Exchange response are determined by the configuration of the STS. The relevant policy assertions for this protocol, and their impacts on the final token request, are listed here. Policy assertion IDs (PAXX) are included to allow referencing specific policy assertions within this specification. For convenience, the sp: prefix used in [WSSP] is repeated here before the policy assertion elements. The impact of these assertions on the request and response message formats is discussed in detail in section 3.3.4.1.

PA01: Policy Assertion **/sp:TransportBinding**

Overview: Presence of this assertion indicates that the message protection and security correlation will be provided by means other than those defined in [WSS]. Specifically for this protocol, this assertion indicates that the message is protected using the means provided by transport layer. The actual transport layer mechanism used is determined by PA02 and PA03.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the new format changes and implementing transport layer protections required by PA03 (if present), no further behavior changes are required.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the new format changes and implementing transport layer protections required by PA03 (if present), no further behavior changes are required.

PA02: Policy Assertion **/sp:TransportBinding/wsp:Policy/sp:TransportToken**

Presence of this assertion indicates that the token(s) used to protect the final token request and response messages will be restricted. Only nested assertions have a direct impact on the final token request and response.

PA03: Policy Assertion
/sp:TransportBinding/wsp:Policy/sp:TransportToken/wsp:Policy/sp:HttpsToken

Presence of this assertion indicates that the transport layer MUST use of HTTPS and TLS as described in [RFC2246] to protect the messages. The **RequireClientCertificate** attribute MUST be false.

PA04: Policy Assertion **/sp: TransportBinding /wsp:Policy/sp:AlgorithmSuite**

Presence of this assertion indicates that the cryptographic algorithms will be restricted. Only nested assertions have a direct impact on the final token request and response.

PA05: Policy Assertion **/sp: TransportBinding**
/wsp:Policy/sp:AlgorithmSuite/wsp:Policy/sp:Basic256

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion, if algorithms not corresponding to the Basic256 AlgorithmSuite specified in section 7.1 of [WSSP] are used to perform cryptographic operations on the message then the STS SHOULD fault.

Impact on Token Acquisition Response Message Processing: When the STS includes this policy assertion, the STS MUST use the algorithms that correspond to the Basic256 AlgorithmSuite specified in section 7.1 of [WSSP] for cryptographic operations on the message sent to the client.

PA06: Policy Assertion **/sp: TransportBinding**
/wsp:Policy/spAlgorithmSuite/wsp:Policy/sp:TripleDes

Overview: Presence of this assertion indicates that all referenced algorithm URIs in the Token Acquisition messages MUST be one of the URIs corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion, if algorithms not corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1 are used to perform cryptographic operations on the messages, then the STS SHOULD fault.<2>

Impact on Token Acquisition Response Message Processing: When the STS includes this policy assertion, the STS MUST use the algorithms that correspond to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1 for cryptographic operations on the messages sent to the client. If the STS receives a request using an algorithm that does not correspond to the TripleDes AlgorithmSuite specified in section 7.1 of [WSSP], the STS MUST fault.

PA07: Policy Assertion **/sp: TransportBinding /wsp:Policy/sp:Layout**

Presence of this assertion indicates that the layout of the <Security> Header element defined by [WSS] is restricted. Only nested assertions have a direct impact on the final token request and response.

PA08: Policy Assertion **/sp: TransportBinding**
/wsp:Policy/sp:Layout/wsp:Policy/sp:Strict

Overview: Presence of this assertion indicates that the layout of the <Security> Header element defined by [WSS] MUST conform to the strict layout rules defined in [WSSP] section 7.7.1.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

PA09: Policy Assertion **/sp:TransportBinding/wsp:Policy/sp:IncludeTimestamp**

Overview: Presence of this assertion indicates that a wsu:TimeStamp MUST be present in the <Security> Header element defined by [WSS]. This policy assertion is described in [WSSP] section 7.2.

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion, the timestamp in the <Created> element MUST be the time (GMT) that the message was created. The timestamp in the <Expires> element SHOULD be the time (GMT) when the message SHOULD be ignored by a recipient.<3>

Impact on Token Acquisition Response Message Processing: When the STS includes this policy assertion, the timestamp in the <Created> element MUST be the time (GMT) that the message was created. The timestamp in the <Expires> element SHOULD be the time (GMT) when the message SHOULD be ignored by a recipient.<4>

PA10: Policy Assertion **/sp:SymmetricBinding**

Presence of this assertion indicates that the same set of tokens MUST secure both requests and responses. Only nested assertions have a direct impact on the final token request and response.

PA11: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken**

Presence of this assertion indicates that the token(s) used to protect the final token request and response messages will be restricted. Only nested assertions have a direct impact on the final token request and response.

PA12: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/sp:X509Token**

Overview: Presence of this assertion indicates that a binary Security Token carrying an X.509 token MUST be used for protecting the final token request and response messages. This policy assertion is described in [WSSP] section 6.3.3. Nested assertions further restrict the usage of X.509 tokens. When this assertion is present, the <EndpointReference> element of each corresponding <wsdl:port> MUST contain an <Identity> element (specified in [WSAIdentity]) that contains a <KeyInfo> child element (specified in section 4.4. of [XMLDSig/2002]).

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion, the STS MUST use an X.509 certificate to verify the protection on the message as described in section 3.6.4.1.1.1.1.

Impact on Token Acquisition Response Message Processing: When this policy assertion is present, the protection mechanism for the Token Acquisition response message MUST use the **symmetric key** from the Token Acquisition request to protect the response message.

PA13: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/sp:X509Token/wsp:Policy/sp:RequireDerivedKeys**

Overview: Presence of this assertion indicates that derived keys MUST be used as defined in [WSSC]. This policy assertion is described in [WSSP] section 6.2.1.

Impact on Token Acquisition Request Message Processing: If a <DerivedKeyToken> element is not used in the response, or the request <EncryptedData> and <Signature> elements do not reference the <DerivedKeyToken> element, the STS MUST fault. If multiple <DerivedKeyToken> elements are found in the request, the STS SHOULD NOT require that particular <EncryptedData> and <Signature> elements reference a particular <DerivedKeyToken> element.

Impact on Token Acquisition Response Message Processing: Any <EncryptedData> and <Signature> elements in the response MUST reference a <DerivedKeyToken> element.

PA14: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/sp:X509Token/wsp:Policy/sp:RequireThumbprintReference

Overview: Presence of this assertion indicates that a thumbprint reference MUST be used when referencing this token. This policy assertion is described in [WSSP] section 6.3.3.

Impact on Token Acquisition Request Message Format: The <KeyInfo> element described in 3.6.4.1.2.6 MUST use a <KeyIdentifier> element 3.6.4.1.2.13 conforming to [WSS] within a <SecurityTokenReference> element conforming to [WSS]. The <KeyIdentifier> element MUST have a **ValueType** attribute equal to "http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1".

Impact on Token Acquisition Response Message Format: None, the X.509 certificate is not referred to in the response as noted above.

Impact on Token Acquisition Request Message Processing: The client MUST calculate the thumbprint reference using a SHA1 hash over the certificate file. That thumbprint is then included as described above.

Impact on Token Acquisition Response Message Processing: None, the X.509 certificate is not referred to in the response as noted above.

PA15: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/sp:X509Token/wsp:Policy/sp:WssX509V3Token10

Overview: Presence of this assertion indicates that an X.509 Version 3 token should be used as defined in [WSSX509TP]. This policy assertion is described in [WSSP] section 6.3.3.

Impact on Token Acquisition Request Message Format: When this assertion is present, the format and references to the X.509 certificate in the message MUST conform to [WSSX509TP].

Impact on Token Acquisition Response Message Format: None. The X.509 certificate is not referred to in the response as noted above.

Impact on Token Acquisition Request Message Processing: None, this impacts message formatting only.

Impact on Token Acquisition Response Message Processing: None, the X509 certificate is not referred to in the response as noted above.

PA16: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/sp:SpnegoContextToken

Overview: Presence of this assertion indicates that a <SecurityContextToken> obtained by executing an n-leg RST/RSTR SPNEGO binary negotiation protocol with the service MUST be used for protecting the final token request and response messages. This policy assertion is described in [WSSP] section 6.3.5. Nested assertions further restrict the usage of SPNego context tokens. When this assertion is present, the <EndpointReference> element of each corresponding <wsdl:port> element in the Service Metadata Exchange response message MUST contain an <Identity> element (specified in [WSAIdentity]) that contains an <Spn> element (specified in section 3.2 of [WSAIdentity]).<5>

Impact on Token Acquisition Request Message Format: When this policy assertion is present, the <SecurityContextToken> element described in section 3.6.4.1.2.9 MUST be present in the Token Acquisition request message. The <EncryptedKey> element described in section 3.6.4.1.2.6 is not used with a <SecurityContextToken> element and MUST NOT be present in the <Security> (3.6.4.1.2.2.2) element. If <DerivedKeyToken> elements are used, then the <SecurityTokenReference> child elements of the <DerivedKeyToken> elements in the response MUST reference the value of the <Identifier> child element of the <SecurityContextToken> element. If <DerivedKeyToken> elements are not used, then the <SecurityTokenReference> child elements of the <EncryptedData> and Signature elements in the response MUST reference the value of the <DerivedKeyToken> child element of the <SecurityContextToken> element present in the request.

Impact on Token Acquisition Response Message Format: If <DerivedKeyToken> elementsare used, then the <SecurityTokenReference> child elements of the <DerivedKeyToken> elements in the response MUST reference the value of the <Identifier> child element of the <SecurityContextToken> element present in the request when this policy assertion is present. If <DerivedKeyToken> elements are not used, then the <SecurityTokenReference> child elements of the <EncryptedData> and <Signature> elements in the response MUST reference the value of the <Identifier> child element of the <SecurityContextToken> element present in the request.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the protection mechanism for the Token Acquisition request message MUST use a <SecurityContextToken> element obtained from a WS-TrustForSPNego message protection negotiation as described in section 3.5.4 to protect the message as described in section 3.7.4.1.1.1.

Impact on Token Acquisition Response Message Processing: When this policy assertion is present, the protection mechanism for the Token Acquisition Response Message MUST use the <Identifier> from the <SecurityContextToken> element present in the request to verify protection on the message as described in section 3.7.4.1.1.1.

PA17: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/sp:SpnegoContextToken/wsp:Policy/sp:RequireDerivedKeys

Overview: Presence of this assertion indicates that derived keys MUST be used as defined in [WSSC]. This policy assertion is described in [WSSP] section 6.2.1.

Impact on Token Acquisition Response Message Format: When the STS includes this policy assertion, the <DerivedKeyToken> element described in section 3.6.4.1.2.7 MUST be present in the response message. All <EncryptedData> and <Signature> elements in the message that would reference the <SecurityContextToken> element from the request MUST now

reference a <DerivedKeyToken> element that MUST reference the <SecurityContextToken> element from the request. More than one <DerivedKeyToken> element SHOULD be used.<6>

Impact on Token Acquisition Request Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

PA18: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:AlgorithmSuite**

Presence of this assertion indicates that the cryptographic algorithms will be restricted. Only nested assertions have a direct impact on the final token request and response.

PA19: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:AlgorithmSuite/wsp:Policy/sp:Basic256**

Overview: Presence of this assertion indicates that all referenced algorithm URIs in the Token Acquisition messages MUST be one of the URIs corresponding to the Basic256 AlgorithmSuite specified in section 7.1 of [WSSP].

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion, if the STS receives a request using an algorithm that does not correspond to the Basic256 AlgorithmSuite specified in section 7.1 of [WSSP], then the STS MUST fault.<7>

Impact on Token Acquisition Response Message Processing: When the STS includes this policy assertion, the STS MUST use the algorithms that correspond to the Basic256 AlgorithmSuite specified in section 7.1 of [WSSP] for cryptographic operations on the message sent to the client.

PA20: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:AlgorithmSuite/wsp:Policy/sp:TripleDes**

Overview: Presence of this assertion indicates that all referenced algorithm URIs in the Token Acquisition messages MUST be one of the URIs corresponding to the TripleDes AlgorithmSuite specified in section 7.1 of [WSSP].

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion, if the STS receives a request using an algorithm that does not correspond to the TripleDes AlgorithmSuite specified in section 7.1 of [WSSP], then the STS MUST fault.<8>

Impact on Token Acquisition Response Message Processing: When the STS includes this policy assertion, the STS MUST use the algorithms that correspond to the TripleDes AlgorithmSuite specified in section 7.1 of [WSSP] for cryptographic operations on the message sent to the client.

PA21: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:Layout**

Presence of this assertion indicates that the layout of the <Security> Header element defined by [WSS] is restricted. Only nested assertions have a direct impact on the final token request and response.

PA22: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:Layout/wsp:Policy/sp:Strict**

Overview: Presence of this assertion indicates that the layout of the <Security> Header element defined by [WSS] MUST conform to the strict layout rules defined in [WSSP] section 7.7.1.

Impact on Token Acquisition Request Message Processing: The server MUST fault if the strict rules defined in [WSSP] section 7.7.1 are not met. No further behavior changes are required.

Impact on Token Acquisition Response Message Processing: The server MUST enforce the strict rules defined in [WSSP] section 7.7.1 for response messages. No further behavior changes are required.

PA23: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:IncludeTimestamp**

Overview: Presence of this assertion indicates that a wsu:TimeStamp MUST be present in the <Security> Header element defined by [WSS]. This policy assertion is described in [WSSP] section 7.2.

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion, the timestamp in the <Created> element MUST be the time (GMT) that the message was created. The timestamp in the <Expires> element SHOULD be the time (GMT) when the message SHOULD be ignored by a recipient.<9>

Impact on Token Acquisition Response Message Processing: When the STS includes this policy assertion, the timestamp in the <Created> element MUST be the time (GMT) that the message was created. The timestamp in the <Expires> element SHOULD be the time (GMT) when the message SHOULD be ignored by a recipient.<10>

PA24: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:EncryptSignature**

Overview: Presence of this assertion indicates that the primary signature and any signature confirmation elements MUST be encrypted as described in [WSSP] section 7.4.

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion, the message protection processing MUST encrypt the required signatures according to the formats and mechanism described in [XMLEnc], and only using the algorithms allowed by PA11. Request messages received without encrypted signature will cause the STS to issue a SOAP fault.

Impact on Token Acquisition Response Message Processing: When the STS includes this policy assertion, the STS MUST encrypt each message signature according to the formats and mechanism described in [XMLEnc], and only using the algorithms allowed by PA11.

PA25: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:OnlySignEntireHeadersAndBody

Overview: Presence of this assertion indicates that signature digests MUST only be over the entire SOAP body element, first descendents of the SOAP <Header> element, and/or first descendants of the <Security> Header element. This policy assertion is described in [WSSP] section 7.6.

Impact on Token Acquisition Request Message Processing: The server MUST check whether the signature of the request message conforms to the rules defined in [WSSP] section 7.6 and fault if the signature is incorrect. No further behavior is changed.

Impact on Token Acquisition Response Message Processing: The server MUST follow the signature rules defined in [WSSP] section 7.6 for response messages. No further behavior is changed.

PA26: Policy Assertion **/sp:EndorsingSupportingTokens**

Presence of this assertion indicates the presence of endorsing tokens that sign the message signature. The nested assertions specify the tokens and message impact for the final token request and response.

PA27: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:X509Token**

Overview: Presence of this assertion indicates that a binary Security Token carrying an X.509 token MUST be used by the client to prove the identity of the user. This policy assertion is described in [WSSP] section 6.3.3. Nested assertions further restrict the usage of X.509 tokens.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST use the private key associated with an X.509 certificate to prove the identity of the user to the STS. The STS verifies the identity as described in section 3.6.4.1.1.1.1.

Impact on Token Acquisition Response Message Processing: None.

PA28: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:X509Token/wsp:Policy/sp:RequireThumbprintReference**

Overview: Presence of this assertion indicates that a thumbprint reference MUST be supported when the X.509 token is not included in the message but is referenced from the message. When an X.509 token is included in the message instead of referenced, this PA has no effect.<11> This policy assertion is described in [WSSP] section 6.3.3.

Impact on Token Acquisition Request Message Processing: None, thumbprint reference cannot be used because the client MUST include the X.509 token in the message since the STS does not have access to the full X.509 token prior to receiving the request.

Impact on Token Acquisition Response Message Processing: None, the X.509 certificate is not referred to in the response as noted above.

PA29: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:X509Token/wsp:Policy/sp:WssX509V3Token10**

Overview: Presence of this assertion indicates that an X.509 Version 3 token should be used as defined in [WSSX509TP]. This policy assertion is described in [WSSP] section 6.3.3.

Impact on Token Acquisition Request Message Processing: None, this impacts message formatting only.

Impact on Token Acquisition Response Message Processing: None, the X.509 certificate is not referred to in the response as noted above.

PA30: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:SpnegoContextToken**

Overview: Presence of this assertion indicates that a <SecurityContextToken> element obtained by executing an n-leg RST/RSTR SPNEGO binary negotiation protocol with the service MUST be used by the client to prove the identity of the user. This policy assertion is described in [WSSP] section 6.3.5. Nested assertions further restrict the usage of SPNego context tokens. When this assertion is present, the <EndpointReference> element of each corresponding <wsdl:port> element MUST contain an <Identity> element (specified in [WSAIdentity]) containing an <Spn> element (specified in section 3.2 of [WSAIdentity]).

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the Token Acquisition request message MUST use a <SecurityContextToken> element obtained from a WS-Trust for SPNego message protection negotiation as described in section 3.5.4 to prove the user's identity as described in section 3.7.4.1.1.2.1. If the key obtained from SPNego is not used to sign the required parts of the message (as specified in PA22) the STS MUST fault. The STS MUST also support receiving and responding to WS-Trust for SPNego messages.

Impact on Token Acquisition Response Message Processing: None.

PA31: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:SignedParts**

Presence of this assertion indicates that the section contains policy for elements that MUST be signed. Only nested assertions have a direct impact on the final token request and response. This policy assertion is described in [WSSP] section 5.1.1.

PA32: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:SignedParts/sp:Header**

Overview: Presence of this assertion indicates that the specific SOAP <Header> element that is defined by an XML attribute on the assertion MUST be signed for integrity protection. This policy assertion is described in [WSSP] section 5.1.1.

Impact on Token Acquisition Request Message Processing: The specified <Header> element MUST be signed as part of the digital signature present in the message. The STS MUST return a **SOAP fault** if the <Header> element is not signed.

Impact on Token Acquisition Response Message Processing: The specified <Header> element MUST be signed as part of the digital signature present in the message.

PA33: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:KerberosToken**

Overview: Presence of this assertion indicates that a Kerberos token MUST be used by the client to prove the identity of the user. This policy assertion is described in [WSSP] section 6.3.4. Nested assertions further restrict the usage of issued tokens.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST use the key associated with a Kerberos token to prove the identity of the user. The STS verifies the identity as described in section 3.6.4.1.1.1.

Impact on Token Acquisition Response Message Processing: None.

PA34: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/mssp:RsaToken**

Overview: Presence of this assertion indicates that if the client is requesting an asymmetric key in the Security Token, the client must prove possession of the private key corresponding to the public key that is present in the <UseKey> element of the request.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present and the client requests a Security Token with an asymmetric key, the server MUST validate the client's signature using the public key that is present in the <UseKey> element of the request to prove that the user has access to the private key.

Impact on Token Acquisition Response Message Processing: None.

PA35: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:IssuedToken**

Overview: Presence of this assertion indicates that an issued token MUST be used by the client to prove the identity of the user. This policy assertion is described in [WSSP] section 6.3.2. Nested assertions further restrict the usage of issued tokens.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST use the key associated with an issued token to prove the identity of the user to the STS. The STS verifies the identity as described in section 3.6.4.1.1.1.1.

Impact on Token Acquisition Response Message Processing: None.

PA36: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:IssuedToken/sp:RequestSecurityTokenTemplate/t:KeyType**

Overview: Presence of this assertion indicates that the corresponding <KeyType> element MUST be used when requesting a conformant issued token from a different STS.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST use the private or symmetric key associated with the issued token to prove the identity of the user to the STS. The STS verifies the identity as described in section 3.6.4.1.1.1.1.

Impact on Token Acquisition Response Message Processing: None.

PA37: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:IssuedToken/wsp:Policy/sp:RequireDerivedKeys**

Overview: Presence of this assertion indicates that derived keys MUST be used as defined in [WSSC]. This policy assertion is described in [WSSP] section 6.2.1.

Impact on Token Acquisition Request Message Processing: If a <DerivedKeyToken> element is not used in the response, or the request <EncryptedData> and <Signature> elements do not reference the <DerivedKeyToken> element, the STS MUST fault. If multiple <DerivedKeyToken> elements are found in the request, the STS SHOULD NOT require that particular <EncryptedData> and <Signature> elements reference a particular <DerivedKeyToken> element.

Impact on Token Acquisition Response Message Processing: None.

PA38: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:IssuedToken/wsp:Policy/sp:RequireInternalReference**

Overview: Presence of this assertion indicates that an internal reference to the issued token MUST be used when referencing the issued token. This policy assertion is described in [WSSP] section 6.3.2.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST place the username and password in the <UsernameToken> element to prove the identity of the user to the STS as described in section 3.6.4.1.2.11.

Impact on Token Acquisition Response Message Processing: None.

PA39: Policy Assertion **/sp:SignedSupportingTokens**

Presence of this assertion indicates that signed tokens are included in the message signature. The nested assertions specify the tokens and message impact for the final token request and response.

PA40: Policy Assertion **/sp:SignedSupportingTokens/wsp:Policy/sp:UsernameToken**

Overview: Presence of this assertion indicates that a username token MUST be used by the client to prove the identity of the user. This policy assertion is described in [WSSP] section 6.3.1. Nested assertions further restrict the usage of username tokens.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST place the username and password in the <UsernameToken> element to prove the identity of the user to the STS. The STS verifies the identity as described in section 3.6.4.1.1.1.1.

Impact on Token Acquisition Response Message Processing: None.

PA41: Policy Assertion **/sp:SignedSupportingTokens/wsp:Policy/sp:UsernameToken/wsp:Policy/sp:WssUsernameToken10**

Overview: Presence of this assertion indicates that a username token should be used as defined in [WSSUTP]. This policy assertion is described in [WSSP] section 6.3.1.

Impact on Token Acquisition Request Message Processing: None, this impacts message formatting only.

Impact on Token Acquisition Response Message Processing: None, the username token is not referred to in the response as noted above.

PA42: Policy Assertion **/sp:Wss11**

Presence of this assertion indicates that the use of WS-Security 1.1 described in [WSS] is restricted. Only nested assertions have a direct impact on the final token request and response. This policy assertion is described in [WSSP] section 10.

PA43: Policy Assertion **/sp:Wss11/wsp:Policy/sp:MustSupportRefKeyIdentifier**

Overview: Presence of this assertion indicates that the initiator and recipient MUST be able to process key-specific identifier token references. This policy assertion is described in [WSSP] section 10.

Impact on Token Acquisition Response Message Format: When the STS includes this policy assertion in PA12 or PA27, the response message SHOULD contain a key specific identifier as part of a <SecurityTokenReference> inside any element under the <Security> element of the **SOAP header** in the response message.<12>

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion and the client includes this type of reference, the STS MUST be able to accept and resolve a key specific identifier used in the request message.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the message format for key specific identifiers and generating those identifiers, no further behavior changes are required to emit key specific identifier references.

PA44: Policy Assertion **/sp:Wss11/wsp:Policy/sp:MustSupportRefIssuerSerial**

Overview: Presence of this assertion indicates that the initiator and recipient MUST be able to process references using the issuer and token serial number.

Impact on Token Acquisition Response Message Format: When the STS includes this policy assertion in PA12 or PA27, the response message SHOULD contain an <X509IssuerSerial> element as part of a <SecurityTokenReference> element inside any element under the <Security> element of the SOAP header in the response message.<13>

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion and the client includes this type of reference, the STS MUST be able to accept and resolve an issuer and serial number reference used in the request message.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the message format for key specific identifiers and generating those identifiers, no further behavior changes are required to emit an issuer and serial number reference in the response message.

PA45: Policy Assertion **/sp:Wss11/wsp:Policy/sp:MustSupportRefThumbprint**

Overview: Presence of this assertion indicates that the initiator and recipient MUST be able to process references using token thumbprints. This policy assertion is described in [WSSP] section 10.

Impact on Token Acquisition Response Message Format: When the STS includes this policy assertion in PA12 or PA27, the response message SHOULD contain a thumbprint reference as part of a <SecurityTokenReference> element inside any element under the <Security> element of the SOAP header in the response message.<14>

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion and the client includes this type of reference, the STS MUST be able to accept and resolve the thumbprint reference used in the request message.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the message format for key specific identifiers and generating those identifiers, no further behavior changes are required to emit a thumbprint reference in the response message.

PA46: Policy Assertion **/sp:Wss11/wsp:Policy/sp:MustSupportRefEncryptedKey**

Overview: Presence of this assertion indicates that the initiator and recipient MUST be able to process references using <EncryptedKey> element references. This policy assertion is described in [WSSP] section 10.

Impact on Token Acquisition Response Message Format: When the STS includes this policy assertion in PA12 or PA27, the response message SHOULD reference an <EncryptedKey> element that is not contained in the message (but that is understood by the context of the message) as part of a <SecurityTokenReference> inside any element under the <Security> element of the SOAP header in the response message.<15>

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion and the client includes this type of reference, the STS MUST be able to accept and resolve the <EncryptedKey> element reference used in the request message. The STS

MUST preserve the value of the <EncryptedKey> element and its identifier from the request for use in the response.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the message format for key specific identifiers and generating those identifiers, no further behavior changes are required to emit an <EncryptedKey> element reference in the response message.

PA47: Policy Assertion **/sp:Wss11/wsp:Policy/sp:RequireSignatureConfirmation**

Overview: Presence of this assertion indicates that <wsse11:SignatureConfirmation> elements should be used as defined in [WSS]. This policy assertion is described in [WSSP] section 10.

Impact on Token Acquisition Response Message Format: When the STS includes this policy assertion, the <Security> element of the SOAP header in the response message MUST contain a <SignatureConfirmation> element for each incoming Signature element of the request. If policy assertion PA15 is in effect, each <SignatureConfirmation> element will be found encrypted inside an <EncryptedData> element.

Impact on Token Acquisition Request Message Processing: The STS MUST preserve the values of each <SignatureValue> element in the request for use in the response.

Impact on Token Acquisition Response Message Processing: When the STS includes this policy assertion, the value of the <SignatureValue> element for each <Signature> element in the incoming request MUST be copied into a corresponding <SignatureConfirmation> element for the response. If PA15 applies to the STS endpoint used by the request, each <SignatureConfirmation> element MUST be encrypted in an <EncryptedData> element according to [XMLEnc].

PA48: Policy Assertion **/sp:Trust10**

Presence of this assertion indicates that the use of WS-Trust as described in [WSTrust1.3] is restricted. The XML namespace for WS-Trust requests and responses MUST be "http://schemas.xmlsoap.org/ws/2005/02/trust". The value of the <wsa:Action> element for a WS-Trust request MUST be "http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue". The value of the <wsa:Action> element for a WS-Trust response MUST be "http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue". This policy assertion is described in [WSSP] section 11.

PA49: Policy Assertion **/sp:Trust10/wsp:Policy/sp:RequireClientEntropy**

Overview: Presence of this assertion indicates that client entropy MUST be used as key material for a requested symmetric key proof token. This policy assertion is described in [WSSP] section 11.

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion, the client MUST include a cryptographically random number in the request message to the STS as part of the <Entropy> element described in sections 3.7.4.1.2.3.3 and 3.6.4.1.1.2.2.9.

Impact on Token Acquisition Response Message Processing: If PA25 applies to the STS endpoint used by the request, the STS MUST combine its entropy with the client's entropy using the PSHA1 algorithm as specified in [WSSC]. The result is the symmetric key included in the proof token and the Security Token. If PA25 does not apply to the endpoint used in the request, the STS uses the client entropy as the symmetric key.

PA50: Policy Assertion **/sp:Trust10/wsp:Policy/sp:RequireServerEntropy**

Overview: Presence of this assertion indicates that server entropy MUST be used as key material for a requested symmetric key proof token. This policy assertion is described in [WSSP] section 11.

Impact on Token Acquisition Request Message Processing: None.

Impact on Token Acquisition Response Message Processing: If PA24 applies to the STS endpoint used by the request, the STS MUST combine its entropy with the client's entropy using the PSHA1 algorithm as specified in [WSSC]. The result is the symmetric key included in the proof token and the Security Token. If PA24 does not apply to the endpoint used in the request, the STS uses its own entropy as the symmetric key.

PA51: Policy Assertion **/sp:Trust10/wsp:Policy/sp:MustSupportIssuedTokens**

Overview: Presence of this assertion indicates that the wst:IssuedTokens header is supported as described in WS-Trust.

Impact on Token Acquisition Request Message Processing: None, the wst:IssuedTokens header is not used for messages of this protocol.

Impact on Token Acquisition Response Message Processing: None, the wst:IssuedTokens header is not used for messages of this protocol.

PA52: Policy Assertion **/sp:Trust13**

Presence of this assertion indicates that the use of WS-Trust as described in [WSTrust1.3] is restricted. The XML namespace for WS-Trust requests and responses MUST be "http://docs.oasis-open.org/ws-sx/ws-trust/200512". The value of the <wsa:Action> element for a WS-Trust request MUST be "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue". The value of the <wsa:Action> element for a WS-Trust response MUST be "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Issue" or "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal".<16> This policy assertion is described in [WSSP1.2] section 10.

PA53: Policy Assertion **/sp:Trust13/wsp:Policy/sp:RequireClientEntropy**

Overview: Presence of this assertion indicates that client entropy MUST be used as key material for a requested symmetric key proof token. This policy assertion is described in [WSSP] section 11.

Impact on Token Acquisition Request Message Processing: When the STS includes this policy assertion, the client MUST include a cryptographically random number in the request message to the STS as part of the <Entropy> element described in sections 3.6.4.1.1.2.2.9 and 3.7.4.1.2.3.3.

Impact on Token Acquisition Response Message Processing: If PA25 applies to the STS endpoint used by the request, the STS MUST combine its entropy with the client's entropy using the PSHA1 algorithm as specified in [WSSC]. The result is the symmetric key included in the proof token and the Security Token. If PA25 does not apply to the endpoint used in the request, the STS uses the client entropy as the symmetric key.

PA54: Policy Assertion **/sp:Trust13/wsp:Policy/sp:RequireServerEntropy**

Overview: Presence of this assertion indicates that server entropy MUST be used as key material for a requested symmetric key proof token. This policy assertion is described in [WSSP] section 11.

Impact on Token Acquisition Request Message Processing: None.

Impact on Token Acquisition Response Message Processing: If PA24 applies to the STS endpoint used by the request, the STS MUST combine its entropy with the client's entropy using the PSHA1 algorithm as specified in [WSSC]. The result is the symmetric key included in the proof token and the Security Token. If PA24 does not apply to the endpoint used in the request, the STS uses its own entropy as the symmetric key.

PA55: Policy Assertion **/sp:Trust13/wsp:Policy/sp:MustSupportIssuedTokens**

Overview: Presence of this assertion indicates that the wst:IssuedTokens header is supported as described in WS-Trust.

Impact on Token Acquisition Request Message Processing: None, the wst:IssuedTokens header is not used for messages of this protocol.

Impact on Token Acquisition Response Message Processing: None, the wst:IssuedTokens header is not used for messages of this protocol.

PA56: Policy Assertion **/wsaw:UsingAddressing**

Overview: Presence of this assertion indicates that services MUST use WS-Addressing for request messages and use of the message addressing properties MUST be fully compliant with this specification; in particular, senders MUST use all message addressing properties mandated by [WSA], applicable WS-Addressing protocol bindings, and MUST follow all applicable WS-Addressing normative requirements. This policy assertion is described in [WSAWSDL] section 3.1.

Impact on Token Acquisition Request Message Processing: The STS MUST preserve the value of the <MessageID> element from the request message for use in the response message. Beyond accommodating the new message format and saving this value, no further behavior changes are required.

Impact on Token Acquisition Response Message Processing: The STS MUST use the <MessageID> element value from the incoming request as the value for the <RelatesTo> element described in section 3.6.4.1.2.1.2.

3.2.4.1.1.2.2 Effects of Policy Elements with Message Policy Subject

[WSSP] defines the effects of security policy assertions with message policy subject for the protocol. The policy assertions returned in the WSDL of a Service Metadata Exchange response are determined by the configuration of the STS. The relevant policy assertions for this protocol are listed here. Policy assertion IDs (PAXX) are included to allow referencing specific policy assertions within this specification. For convenience, the sp: prefix used in [WSSP] is repeated here before the policy assertion elements. The impact of these assertions on the request and response message formats is discussed in detail in section 3.3.4.2.

PA57: Policy Assertion **/sp:SignedParts**

Presence of this assertion indicates that the section contains policy for elements that MUST be signed. Only nested assertions have a direct impact on the final token request and response. This policy assertion is described in [WSSP] section 5.1.1.

PA58: Policy Assertion **/sp:SignedParts/sp:Body**

Overview: Presence of this assertion indicates that the entire <s:Body> element, its attributes and content, MUST be signed for integrity protection. This policy assertion is described in [WSSP] section 5.1.1.

Impact on Token Acquisition Request Message Processing: The body MUST be signed as part of the digital signature present in the message. The STS MUST return a SOAP fault if the body is not signed.

Impact on Token Acquisition Response Message Processing: The body MUST be signed as part of the digital signature present in the message.

PA59: Policy Assertion **/sp:SignedParts/sp:Header**

Overview: Presence of this assertion indicates that the specific SOAP <Header> element that is defined by an XML attribute on the assertion MUST be signed for integrity protection. This policy assertion is described in [WSSP] section 5.1.1.

Impact on Token Acquisition Request Message Processing: The specified <Header> element MUST be signed as part of the digital signature present in the message. The STS MUST return a SOAP fault if the <Header> element is not signed.

Impact on Token Acquisition Response Message Processing: The specified <Header> element MUST be signed as part of the digital signature present in the message.

PA60: Policy Assertion **/sp:EncryptedParts**

Presence of this assertion indicates that the section contains policy for elements that MUST be encrypted. Only nested assertions have a direct impact on the final token request and response. This policy assertion is described in [WSSP] section 5.2.1.

PA61: Policy Assertion **/sp:EncryptedParts/sp:Body**

Overview: Presence of this assertion indicates that the entire <s:Body> element, its attributes and content, MUST be encrypted for confidentiality protection. This policy assertion is described in [WSSP] section 5.2.1.

Impact on Token Acquisition Request Message Processing: The body MUST be encrypted. The STS MUST return a SOAP fault if the body is not encrypted.

Impact on Token Acquisition Response Message Processing: The body MUST be encrypted.

3.2.4.1.2 Elements

The following table summarizes the XML Schema element definitions that are specific to this operation. Elements are included below if they are not specified in normative references, or if this protocol restricts the contents of the element. Elements that are fully specified in normative references and that are not restricted in this protocol are not detailed below.

Element	Description
Metadata	Specified in [WSMETA] section 4
MetadataSection	Specified in [WSMETA] section 4

Element	Description
definitions	Specified in [WSDL] section 2.1
EndpointReference	Specified in [WSA] section 2
Policy	Specified in [WS-Policy] section 4
UsingAddressing	Specified in [WSAWSDL] section 3.1
Wss11	Specified in [WSSP] section 10.2
TransportBinding	Specified in [WSSP] section 8.3
SymmetricBinding	Specified in [WSSP] section 8.4
EndorsingSupportingTokens	Specified in [WSSP] section 9.3
SignedSupportingTokens	Specified in [WSSP] section 9.2
Trust10	Specified in [WSSP] section 11.1
Trust13	Specified in [WSSP] section 10.1
TransportToken	Specified in [WSSP] section 8.3
AlgorithmSuite	Specified in [WSSP] section 8.1
Layout	Specified in [WSSP] section 8.2
HttpsToken	Specified in [WSSP] section 6.3.10
ProtectionToken	Specified in [WSSP] section 8.4
SPNegoContextToken	Specified in [WSSP] section 6.3.5
X509token	Specified in [WSSP] section 6.3.3
IssuedToken	Specified in [WSSP] section 6.3.2
RequestSecurityTokenTemplate	Specified in [WSSP] section 6.3.2
KerberosToken	Specified in [WSSP] section 6.3.4
RsaToken	Specified below in section X.
SignedParts	Specified in [WSSP] section 5.1.1
EncryptedParts	Specified in [WSSP] section 5.2.1

3.2.4.1.2.1 Metadata

The <Metadata> element MUST have one or more <MetadataSection> child elements. The first <MetadataSection> child element MUST have a **Dialect** attribute that equals "http://schemas.xmlsoap.org/wsdl".

3.2.4.1.2.2 MetadataSection

The first <MetadataSection> element MUST contain a <definitions> element as specified in [WSDL] section 2.1, and as described in section 3.2.4.1.2.3. If further <MetadataSection> elements are present, they MUST be referenced by the WSDL content contained in the first <MetadataSection> element as described in [WSDL].

3.2.4.1.2.3 Definitions

This element MUST describe the service to be used for the Token Acquisition requests and responses detailed in sections 3.6.4.1.2.1.1 and 3.6.4.1.2.1.2.

The <EndpointReference> element (section 3.6.4.1.2.24) of a particular <wsdl:port> MAY<17> contain an <Identity> element specified in [WSAIdentity]. This <Identity> element MUST contain either a <KeyInfo> element specified in [XMLDSig/2002] section 4.4, or a <Dns> element specified in [WSAIdentity] section 3.1, or a <Spn> element specified in [WSAIdentity] section 3.2, or a Upn element specified in [WSAIdentity] section 3.3. For further details on when this element is present, see sections 3.3.4.1 and 3.2.4.1.1.2.1.

[WSPolicyAtt] section 4 defines how policy content conforming to [WS-Policy] may be attached to a WSDL 1.1 structure [WSDL]. Specifically, [WSPolicyAtt] identifies the following four types of Policy Subjects:

- Endpoint Policy Subject
- Operation Policy Subject
- Message Policy Subject
- Service Policy Subject

[WSSP] does not define any assertions with a scope of service policy subject. [WSSP] section 4.2 restricts <Policy> elements that address the preceding Policy Subjects to only be used in specific sections of the WSDL <definitions> element [WSDL]. In addition to the attachment requirements of [WSSP] section 4.2, <Policy> elements with the Endpoint Policy Subject MUST be referenced from a <wsdl:binding> element.

Each <wsdl:binding> element MUST contain <PolicyReference> elements referencing <Policy> elements with Endpoint Policy Subject and Message Policy Subject. The content of these <Policy> elements MUST conform to the descriptions in the following sections. The <Policy> elements in each binding MUST conform to the specifications in [WSSP] section 2. The XML namespace used by the elements defined in [WSSP] MUST be either "http://schemas.xmlsoap.org/ws/2005/07/securitypolicy" or "http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702".

3.2.4.1.2.4 EndpointReference

The <EndpointReference> element is specified in [WSA] section 2 and MAY contain an <Identity> element specified in [WSAIdentity] section 2. The <Identity> element MUST contain a <KeyInfo> element specified in [XMLDSig/2002] section 4.4, or a <Dns> element specified in [WSAIdentity] section 3.1, or a <Spn> element specified in [WSAIdentity] section 3.2, or a Upn element specified in [WSAIdentity] section 3.3.

3.2.4.1.2.5 Policy

The <Policy> element is specified in [WS-Policy] section 4.3.2. The content of the <Policy> element varies based on the policy subject. The requirements for the <Policy> elements under top level policy subjects are discussed in the contained sections below. Requirements for the <Policy> elements under other policy assertions are discussed in the element definitions for those assertions.

3.2.4.1.2.5.1 Endpoint Policy Subject

The <Policy> element MUST contain only one WS-Policy <All> element. The WS-Policy <All> element MUST contain the following elements:

- A <UsingAddressing> element that MUST conform to the guidance in section 3.2.4.1.2.6.
- A <Wss11> element that MUST conform to the guidance in section 3.2.4.1.2.7.

The WS-Policy <All> element MAY contain the following elements:

- A <TransportBinding> element that MUST conform to the guidance in section 3.2.4.1.2.8.
- A <SymmetricBinding> element that MUST conform to the guidance in section 3.2.4.1.2.9.
- An <EndorsingSupportingTokens> element that MUST conform to the guidance in section 3.2.4.1.2.10.
- A <SignedSupportingTokens> element that MUST conform to the guidance in section 3.2.4.1.2.11.
- A <Trust10> element that MUST conform to the guidance in section 3.2.4.1.2.12.
- A <Trust13> element that MUST conform to the guidance in section 3.2.4.1.2.13.

For further details on how the contents of the <Policy> element are determined, see section 3.2.4.1.1.2.1.

3.2.4.1.2.5.2 Message Policy Subject for wsd:input

The <Policy> element MUST contain only one WS-Policy <All> element. The WS-Policy <All> element MUST contain a SignedParts Element (section 3.2.4.1.2.25) and an EncryptedParts Element (section 3.2.4.1.2.26). The SignedParts Element MUST conform to the guidance in section 3.2.4.1.2.25. The EncryptedParts Element MUST conform to the guidance in section 3.2.4.1.2.26.

3.2.4.1.2.5.3 Message Policy Subject for wsdl:output

The format and content of this element MUST be identical to the <Policy> element defined in section 3.2.4.1.2.5.2.

3.2.4.1.2.6 UsingAddressing

This element MUST be empty and MUST have no attributes.

3.2.4.1.2.7 Wss11

The <Wss11> element MUST only contain a <Policy> element. This element MUST contain the following elements:

- <MustSupportRefKeyIdentifier> element as specified in [WSSP] section 10.2.
- <MustSupportRefIssuerSerial> element as specified in [WSSP] section 10.2.
- <MustSupportRefThumbprint> element as specified in [WSSP] section 10.2.
- <MustSupportRefEncryptedKey> element as specified in [WSSP] section 10.2.

The WS-Policy <Policy> element SHOULD contain a <RequireSignatureConfirmation> element conforming to [WSSP] section 10.2. For further details on how the content of this element is determined, see section 3.2.4.1.1.2.1.

3.2.4.1.2.8 TransportBinding

The <TransportBinding> element MUST only contain a <Policy> element. This element MUST contain the following elements:

- A <TransportToken> element that MUST conform to the guidance in section 3.2.4.1.2.14.
- An <AlgorithmSuite> element that MUST conform to the guidance in section 3.2.4.1.2.15.
- A <Layout> element that MUST conform to the guidance in section 3.2.4.1.2.16.
- An <IncludeTimestamp> element as specified in [WSSP] section 8.4.

3.2.4.1.2.9 SymmetricBinding

The <SymmetricBinding> element MUST only contain a <Policy> element. This element MUST contain the following elements:

- A <ProtectionToken> element that MUST conform to the guidance in section 3.2.4.1.2.18.
- An <AlgorithmSuite> element that MUST conform to the guidance in section 3.2.4.1.2.15.
- A <Layout> element that MUST conform to the guidance in section 3.2.4.1.2.16.
- An <IncludeTimestamp> element as specified in [WSSP] section 8.4.
- An <EncryptSignature> element as specified in [WSSP] section 8.4.
- An <OnlySignEntireHeadersAndBody> element as specified in [WSSP] section 8.4.

3.2.4.1.2.10 EndorsingSupportingTokens

The <EndorsingSupportingTokens> element MUST contain a <Policy> element. The <Policy> element MUST contain one of the following elements:

- An <X509Token> element that MUST conform to section 3.2.4.1.2.20.1.
- An <IssuedToken> element that MUST conform to section 3.2.4.1.2.21.
- An <SpnegoContextToken> element that MUST conform to section 3.2.4.1.2.19.2.
- A <KerberosToken> element that MUST conform to section 3.2.4.1.2.23.

In addition to one of the elements above, the <EndorsingSupportingTokens> element can contain an <RsaToken> element that MUST conform to section 3.2.4.1.2.24.

For further details on how the presence and contents of this element are determined, see section 3.2.4.1.1.2.1.

3.2.4.1.2.11 SignedSupportingTokens

The <SignedSupportingTokens> element MUST contain only a <Policy> element.

The <Policy> element MUST contain only a <UsernameToken> element specified in [WSSP] section 6.3.1. The <UsernameToken> element MUST have an IncludeToken attribute equal to "http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient". The <UsernameToken> element MUST contain only a <Policy> element. The <Policy> element MUST contain only a <WssUsernameToken10> element specified in [WSSP] section 6.3.1. The <Policy> element MUST NOT contain any other elements.

For further details on how the presence of this element is determined, see section 3.2.4.1.1.2.1.

3.2.4.1.2.12 Trust10

The <Trust10> element MUST only contain a <Policy> element. This element MUST contain the following elements:

- <RequireClientEntropy> element as specified in [WSSP] section 11.1.
- <RequireServerEntropy> element as specified in [WSSP] section 11.1.
- <MustSupportIssuedTokens> element as specified in [WSSP] section 11.1.

3.2.4.1.2.13 Trust13

The <Trust13> element MUST only contain a <Policy> element. This element MUST contain the following elements:

- <RequireClientEntropy> element as specified in [WSSP] section 10.1.
- <RequireServerEntropy> element as specified in [WSSP] section 10.1.
- <MustSupportIssuedTokens> element as specified in [WSSP] section 10.1.

3.2.4.1.2.14 TransportToken

The <TransportToken> element is specified in [WSSP] section 8.3. The <TransportToken> element MUST only contain a <Policy> element. The <Policy> element MUST contain an <HttpsToken> element. The <Policy> element MUST NOT contain any other elements.

3.2.4.1.2.15 AlgorithmSuite

The <AlgorithmSuite> element MUST only contain a <Policy> element. The WS-Policy <Policy> element MUST contain either only a <Basic256> element (described in [WSSP] section 8.1) or only a <TripleDes> element (described in [WSSP] section 8.1).

3.2.4.1.2.16 Layout

The <Layout> element MUST only contain a <Policy> element. The WS-Policy <Policy> element MUST contain only the <Strict> element specified in [WSSP] section 8.2.

3.2.4.1.2.17 HttpsToken

The <HttpsToken> element MUST have a **RequireClientCertificate** attribute equal to "false". The <HttpsToken> element MUST NOT contain a child element.

3.2.4.1.2.18 ProtectionToken

The <ProtectionToken> element is specified in [WSSP] section 8.4. The <ProtectionToken> element MUST only contain a <Policy> element. The <Policy> element SHOULD contain an <SpnegoContextToken> element conforming to section 3.2.4.1.2.19.1. If the <Policy> element does not contain an <SpnegoContextToken> element, the <Policy> element MUST contain an <X509Token> element conforming to 3.2.4.1.2.20.1. The <Policy> element MUST NOT contain any other elements.

For further details on how the contents of this element are determined, see section 3.2.4.1.1.2.1.

3.2.4.1.2.19 SPNegoContextToken

The SPNegoContextToken element is used differently depending on which policy assertion element it falls under. The following sections describe the restrictions.

3.2.4.1.2.19.1 Part of SymmetricBinding

The <SpnegoContextToken> element is specified in [WSSP] section 6.3.5. The <SpnegoContextToken> element MUST have an **IncludeToken** attribute equal to "http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient". The <SpnegoContextToken> element MUST contain only a <Policy> element. That <Policy> element MUST contain only a <RequireDerivedKeys> element conforming to [WSSP] section 6.3.5. For further details on how the presence of this element is determined, see section 3.2.4.1.1.2.1.

3.2.4.1.2.19.2 Part of EndorsingSupportingTokens

The <SpnegoContextToken> element MUST have an IncludeToken attribute equal to "http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient". The <SpnegoContextToken> element MUST contain only a <Policy> element. That <Policy> element MUST not contain any child elements. For further details on how the presence of this element is determined, see section 3.2.4.1.1.2.1.

3.2.4.1.2.20 X509token

The X509token element is used differently depending on which policy assertion element it falls under. The following sections describe the restrictions.

3.2.4.1.2.20.1 Part of SymmetricBinding

The <X509Token> element MUST have an **IncludeToken** attribute equal to "http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never". The <X509Token> element MUST contain only a <Policy> element. The <Policy> element MUST contain the following three elements:

- A <RequireDerivedKeys> element as specified in [WSSP] section 6.3.3.
- A <RequireThumbprintReference> element as specified in [WSSP] section 6.3.3.
- A <WssX509V3Token10> element as specified in [WSSP] section 6.3.3.

For further details on how the presence of this element is determined, see section 3.2.4.1.1.2.1.

3.2.4.1.2.20.2 Part of EndorsingSupportingTokens

The <X509Token> element is specified in [WSSP] section 6.3.3. The <X509Token> element MUST have an IncludeToken attribute equal to "http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient". The <X509Token> element MUST contain only a <Policy> element. The <Policy> element MUST contain only the following two elements:

- <RequireThumbprintReference> element as specified in [WSSP] section 6.3.3.
- <WssX509V3Token10> element as specified in [WSSP] section 6.3.3.

For further details on how the presence of this element is determined, see section 3.3.4.1.

3.2.4.1.2.21 IssuedToken

The <IssuedToken> element is specified in [WSSP] section 6.3.2. The <IssuedToken> element MUST have an **IncludeToken** attribute equal to "http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient". The <IssuedToken> element MUST contain a <RequestSecurityTokenTemplate> element specified in [WSSP] section 6.3.2. The <RequestSecurityTokenTemplate> element MUST contain a <KeyType> element specified in [WSTrust1.3] section 9.2. The <KeyType> element MUST equal one of the following values:

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey
- http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey
- http://schemas.xmlsoap.org/ws/2005/02/trust/Bearer
- http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey

The <IssuedToken> element MUST also contain a <Policy> element. The <Policy> element MUST contain only the following two elements:

- <RequireDerivedKeys> element as specified in [WSSP] section 6.3.2
- <RequireInternalReference> element as specified in [WSSP] section 6.3.2

For further details on how the presence of this element is determined, see section 3.2.4.1.1.2.1.

3.2.4.1.2.22 RequestSecurityTokenTemplate

The <RequestSecurityTokenTemplate> element MUST contain a <KeyType> element specified in [WSTrust1.3] section 9.2. The <KeyType> element MUST equal one of the following values:

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey

- http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey
- http://schemas.xmlsoap.org/ws/2005/02/trust/Bearer
- http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey

3.2.4.1.2.23 KerberosToken

The <KerberosToken> element MUST have an IncludeToken attribute equal to "http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Once". The <KerberosToken> element MUST contain only a <Policy> element. That <Policy> element MUST contain a single <WssGssKerberosV5ApReqToken11> child element. For further details on how the presence of the <KerberosToken> element is determined, see section3.2.4.1.1.2.1.

3.2.4.1.2.24 RsaToken

The <RsaToken> element MUST be in the XML namespace "http://schemas.microsoft.com/ws/2005/07/securitypolicy". The <RsaToken> element MUST have an IncludeToken attribute conforming to [WSSP] section 6.1. The IncludeToken attribute MUST equal "http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never". The <RsaToken> element MUST have an **Optional** attribute specified in [WS-Policy] section 4.3.1. The **Optional** attribute MUST equal "true".

3.2.4.1.2.25 SignedParts

The element MUST contain the following elements:

- An empty <Body> element as specified in [WSSP] section 5.1.1.
- An empty <Header> element as specified in [WSSP] section 5.1.1. A **Header** attribute MUST be present and MUST equal "To". A **Namespace** attribute MUST be present and MUST equal "http://www.w3.org/2005/08/addressing".
- An empty <Header> element as specified in [WSSP] section 5.1.1. A **Header** attribute MUST be present and MUST equal "From". A **Namespace** attribute MUST be present and MUST equal "http://www.w3.org/2005/08/addressing".
- An empty <Header> element as specified in [WSSP] section 5.1.1. A **Header** attribute MUST be present and MUST equal "FaultTo". A **Namespace** attribute MUST be present and MUST equal "http://www.w3.org/2005/08/addressing".
- An empty <Header> element as specified in [WSSP] section 5.1.1. A **Header** attribute MUST be present and MUST equal "ReplyTo". A **Namespace** attribute MUST be present and MUST equal "http://www.w3.org/2005/08/addressing".
- An empty <Header> element as specified in [WSSP] section 5.1.1. A **Name** attribute MUST be present and MUST equal "MessageID". A **Namespace** attribute MUST be present and MUST equal "http://www.w3.org/2005/08/addressing".
- An empty <Header> element as specified in [WSSP] section 5.1.1. A **Name** attribute MUST be present and MUST equal "RelatesTo". A **Namespace** attribute MUST be present and MUST equal "http://www.w3.org/2005/08/addressing".

The <SignedParts> element MUST NOT contain any other elements.

3.2.4.1.2.26 EncryptedParts

The element MUST contain an empty <Body> element conforming to [WSSP] section 5.1.1. The element MUST NOT contain any other elements.

3.2.4.1.3 Complex Types

There is no XML Schema defined to specify the schema types that govern the XML elements of the protocol beyond the XML schemas that are defined by existing normative documents. Those normative documents are referenced in the Elements section above.

3.2.4.1.4 Simple Types

There is no XML Schema defined to specify the schema types that govern the XML elements of the protocol beyond the XML schemas that are defined by existing normative documents. Those normative documents are referenced in the Elements section above.

3.2.4.1.5 Attributes

The following table summarizes the XML Schema attribute definitions that are specific to this operation. Attributes are included below if they are not specified in normative references.

Attribute	Description
IncludeToken	Uses the same syntax and semantics as that specified in [WSSP] section 6.1.
Optional	Uses the same syntax and semantics as that specified in [WSSP] section 6.1.

3.2.4.1.5.1 IncludeToken

This attribute is specified in [WSSP] section 6.1, and is used on the RsaToken element defined in this protocol. This usage is not defined elsewhere in normative documentation. Other uses of this attribute in this protocol are defined in other normative documents as described in the Elements section above.

3.2.4.1.5.2 Optional

This attribute is specified in [WS-Policy] section 4.3.1, and is used on the RsaToken element defined in this protocol. This usage is not defined elsewhere in normative documentation.

3.2.5 Timer Events

There are no protocol-specific timer events that are serviced by an implementation. This protocol does not require timers except those that may be used by the underlying transport to transmit and receive messages over HTTP. The protocol does not include provisions for time-based retry for sending protocol messages.

3.2.6 Other Local Events

This protocol does not have dependencies on any transport protocols other than HTTP 1.1. This protocol relies on this transport mechanism for the correct and timely delivery of protocol messages. The protocol does not take action in response to any changes or failure in machine state or network communications.

3.3 Service Metadata Exchange Client Details

The following sections detail the client details for service metadata exchange port type. The port type name for Service Metadata Exchange is MetadataExchange.

3.3.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

STS Service Metadata Exchange Endpoint: To initiate the protocol by sending a Service Metadata Exchange request, the client must know the endpoint URL to which to send the request.

STS Token Acquisition Endpoint: The **STS Token Acquisition Endpoint** may be used to distinguish the appropriate WS-SecurityPolicy for the token acquisition endpoint from the Service Metadata Response message.

Service Metadata Exchange Request Type: This value can be "GET" or "WS-MEX" and determines the type of Service Metadata Exchange request that will be used to initiate the protocol. A value of "GET" indicates that the HTTPS GET specified in section 3.2.4.1 will be used. A value of "WS-MEX" indicates that the WS-MetadataExchange [WSMETA] SOAP message specified in section 3.2.4.1.1.1 will be used.

3.3.2 Timers

Clients SHOULD fault if a Service Metadata Exchange Response Message is not received within 1 minute after a Service Metadata Exchange Request Message is issued to the server role.

There are no other protocol-specific timer events that are serviced by an implementation. The protocol does not include provisions for time-based retry for sending protocol messages.

3.3.3 Initialization

The Prerequisite Security Token Service (STS) endpoint URL is used for WS-MetadataExchange requests (section 3.2.4.1.1.1). It is implementation-specific<18> whether the client uses HTTPS GET requests or WS-MetadataExchange requests.The client MAY have the STS endpoint URL that will be used for WS-Trust requests, as specified in [WSTrust1.3], prior to sending the first protocol message. Section 3.1.1.2 describes the abstract interface for how these values may be provided to the client role implementation.

3.3.4 Message Processing Events and Sequencing Rules

The metadata exchange messages allow the Security Token Service (STS) to indicate to the client how to structure and secure messages to the STS. The first message of the protocol MUST be a Service Metadata Exchange request message. As mentioned in section 3.3.3, the client MUST know the type of Service Metadata Exchange requests to use prior to sending the first Service Metadata Exchange request message. This request message MUST be sent to the Service Metadata Exchange endpoint known before initiating the protocol, as specified in item 2 of section 3.7.3. The response to this message MUST be the Service Metadata Exchange response corresponding to the type of request message originally sent. If an HTTPS GET Service Metadata Exchange request message was sent, an HTTPS GET Service Metadata Exchange response message MUST be sent in response. If a

WS-MetadataExchange Service Metadata Exchange request message was sent, a WS-MetadataExchange Service Metadata Exchange response message MUST be sent in response. If a mismatched response is received, the client MUST fault.

The client MUST look up the appropriate <wsdl:binding> element using the value of the binding attribute of the <wsdl:port> whose endpoint reference address sub-element has the same value as the STS endpoint described in section 3.7.3.

The content of the <Policy> elements in the <wsdl:binding> applies to the endpoint and MUST affect the content and sequencing of future messages, as described in section 3.3.4.1.

3.3.4.1 Effects of Policy Elements with Endpoint Policy Subject

[WSSP] defines the effects of security policy assertions with endpoint policy subject for the protocol. For details on how the content of the [WSDL] metadata content of the Service Metadata Exchange response is determined, see section 4.2. The relevant policy assertions for this protocol, and their impacts on the request and response message formats, are listed here. Policy assertion IDs (PAXX) are included to allow referencing specific policy assertions within this specification. For convenience, the sp: prefix used in [WSSP] is repeated here before the policy assertion elements. The impact of these assertions on the final token request is discussed in detail in section 3.2.4.1.1.2.1.

Overview: Presence of this assertion indicates that the message protection and security correlation will be provided by means other than those defined in [WSS]. Specifically for this protocol, this assertion indicates that the message is protected using the means provided by transport layer. The actual transport layer mechanism used is determined by PA02 and PA03.

PA01: Policy Assertion **/sp:TransportBinding**

Overview: Presence of this assertion indicates that the message protection and security correlation will be provided by means other than those defined in [WSS]. Specifically for this protocol, this assertion indicates that the message is protected using the means provided by transport layer. The actual transport layer mechanism used is determined by PA02 and PA03.

Impact on Token Acquisition Request Message Format: When message protection is provided by the transport layer, confidentiality and integrity mechanisms are not needed within the Token Acquisition request SOAP message. Thus the <EncryptedKey> element, <ReferenceList> element, and <DerivedKeyToken> element described in section 3.6.4.1.2.2.1 are not used. In addition, the SOAP <Body> element will be unencrypted as described in section 3.6.4.1.2.1.1.

Impact on Token Acquisition Response Message Format: When message protection is provided by the transport layer, confidentiality and integrity mechanisms are not needed within the Token Acquisition request SOAP message. Thus the <ReferenceList> and <DerivedKeyToken> elements described in section 3.6.4.1.2.2.2 are not used. In addition, the SOAP <Body> element will be unencrypted as described in section 3.6.4.1.2.1.2.

PA02: Policy Assertion **/sp:TransportBinding/wsp:Policy/sp:TransportToken**

Presence of this assertion indicates that the token(s) used to protect the final token request and response messages will be restricted. Only nested assertions have a direct impact on the final token request and response.

PA03: Policy Assertion **/sp:TransportBinding/wsp:Policy/sp:TransportToken/wsp:Policy/sp:HttpsToken**

Presence of this assertion indicates that the transport layer MUST use HTTPS and TLS as specified in [RFC2246] to protect the messages. The **RequireClientCertificate** attribute SHOULD be false; otherwise, if it is true, the client MUST fault.

PA04: Policy Assertion **/sp: TransportBinding /wsp:Policy/sp:AlgorithmSuite**

Presence of this assertion indicates that the cryptographic algorithms will be restricted. Only nested assertions have a direct impact on the final token request and response.

PA05: Policy Assertion **/sp: TransportBinding /wsp:Policy/sp:AlgorithmSuite/wsp:Policy/sp:Basic256**

Overview: Presence of this assertion indicates that all referenced algorithm URIs in the Token Acquisition messages MUST be one of the URIs corresponding to the Basic256 AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Request Message Format: When this assertion is present, algorithm URIs mentioned in the SOAP header MUST be one of the URIs corresponding to the Basic256 AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Response Message Format: When this assertion is present, algorithm URIs mentioned in the SOAP header MUST be one of the URIs corresponding to the Basic256 AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Request Message Processing: Algorithms not corresponding to the Basic256 AlgorithmSuite specified in [WSSP] section 7.1 MUST NOT be used to perform cryptographic operation on the message to send to the Security Token Service (STS).

Impact on Token Acquisition Response Message Processing: The client need not expect to process algorithms not corresponding to the Basic256 AlgorithmSuite specified in [WSSP] section 7.1 for cryptographic operations on the message received from the STS. If the client receives a message using algorithms other than the specified algorithms, the client MUST fault.

PA06: Policy Assertion **/sp: TransportBinding /wsp:Policy/spAlgorithmSuite/wsp:Policy/sp:TripleDes**

Overview: Presence of this assertion indicates that all referenced algorithm URIs in the Token Acquisition messages MUST be one of the URIs corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Request Message Format: When this assertion is present, the **Algorithm** attribute of each of the <EncryptionMethod>, <DigestMethod>, <CanonicalizationMethod>, <SignatureMethod>, and <Transform> elements in the SOAP header MUST be one of the URIs corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Response Message Format: When this assertion is present, the Algorithm attribute of each of the <EncryptionMethod>, <DigestMethod>, <CanonicalizationMethod>, <SignatureMethod>, and <Transform> elements in the SOAP header MUST be one of the URIs corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Request Message Processing: Algorithms not corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1 MUST NOT be used to perform cryptographic operations on the message to send to the STS.

Impact on Token Acquisition Response Message Processing: The client need not expect to process algorithms not corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1 for cryptographic operations on the message received from the STS. If the client receives a response using an algorithm that does not correspond to the TripleDes AlgorithmSuite specified in section 7.1 of [WSSP], the client MUST fault.

PA07: Policy Assertion **/sp: TransportBinding /wsp:Policy/sp:Layout**

Presence of this assertion indicates that the layout of the <Security> Header element (section 3.6.4.1.2.2.1) defined by [WSS] is restricted. Only nested assertions have a direct impact on the final token request and response.

PA08: Policy Assertion **/sp: TransportBinding /wsp:Policy/sp:Layout/wsp:Policy/sp:Strict**

Overview: Presence of this assertion indicates that the layout of the <Security> Header element defined by [WSS] MUST conform to the strict layout rules defined in [WSSP] section 7.7.1.

Impact on Token Acquisition Request Message Format: The impact to message formatting is thoroughly described in [WSSP] section 7.7.1.

Impact on Token Acquisition Response Message Format: The impact to message formatting is thoroughly described in [WSSP] section 7.7.1.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the new message format, no further behavior changes are required. If the client receives a Token Acquisition response from the server that does not conform to the strict layout rules defined in [WSSP] section 7.7.1, the client MUST fault.

PA09: Policy Assertion **/sp:TransportBinding/wsp:Policy/sp:IncludeTimestamp**

Overview: Presence of this assertion indicates that a wsu:TimeStamp MUST be present in the <Security> Header element defined by [WSS]. This policy assertion is described in [WSSP] section 7.2.

Impact on Token Acquisition Request Message Format: The <Timestamp> element MUST be included in the request message.

Impact on Token Acquisition Response Message Format: The <Timestamp> element MUST be included in the response message.

Impact on Token Acquisition Request Message Processing: The Timestamp in the <Created> element MUST be the time (GMT) that the message was created. The Timestamp in the <Expires> element SHOULD be the time (GMT) when the message SHOULD be ignored by a recipient.<19>

Impact on Token Acquisition Response Message Processing: The Timestamp in the <Created> element MUST be the time (GMT) that the message was created. The Timestamp in the <Expires> element SHOULD be the time (GMT) when the message SHOULD be ignored by a recipient.<20> When the client receives a message without a Timestamp, the client MUST fault. When the client receives a message with a time in <Created> greater than the current time, the client SHOULD fault. When the client receives a message with a time in <Expires> less than the current time, the client SHOULD fault.

PA10: Policy Assertion **/sp:SymmetricBinding**

Presence of this assertion indicates that the same set of tokens MUST secure both requests and responses. Only nested assertions have a direct impact on the final token request and response.

PA11: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken**

Presence of this assertion indicates that the token(s) used to protect the final token request and response messages will be restricted. Only nested assertions have a direct impact on the final token request and response.

PA12: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/wsp:Policy/sp:X509Token

Overview: Presence of this assertion indicates that a binary Security Token carrying an X.509 token MUST be used for protecting the final token request and response messages. This policy assertion is described in [WSSP] section 6.3.3. Nested assertions further restrict the usage of X.509 tokens. When this assertion is present, the <EndpointReference> element of each corresponding <wsdl:port> MUST contain an <Identity> element (specified in [WSAIdentity]) that contains a <KeyInfo> child element ([XMLDSig/2002] section 4.4).

Impact on Token Acquisition Request Message Format: The <EncryptedKey> element described in section 3.6.4.1.2.6 MUST be used to encrypt the symmetric key for the message with the public key from service's X.509 certificate. The <EncryptedKey> element MUST be present in the Security element. The ADM element for the symmetric key is described in section 3.7.1.

Impact on Token Acquisition Response Message Format: No optional elements are included beyond what is required by other policy assertions. The symmetric key used in the request is used for the response as well, and referred to by the <DerivedKeyToken> or <EncryptedData> elements using the key.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the protection mechanism for the Token Acquisition request message MUST use an X.509 certificate to protect the message as described in section 3.7.4.1.1.1.3.

Impact on Token Acquisition Response Message Processing: When this policy assertion is present, the protection mechanism for the Token Acquisition Response Message (section 3.6.4.1.2.1.2) MUST use the symmetric key from the request to protect the message.

PA13: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/wsp:Policy/sp:X509Token/wsp:Policy/sp:RequireDerivedKeys

Overview: Presence of this assertion indicates that derived keys MUST be used as defined in [WSSC]. This policy assertion is described in [WSSP] section 6.2.1.

Impact on Token Acquisition Request Message Format: The <DerivedKeyToken> element described in section 3.6.4.1.2.7 MUST be present in the request message. All <EncryptedData> and <Signature> (section 3.6.4.1.2.8) elements in the message that would reference the symmetric key wrapped by the X.509 certificate MUST now reference a <DerivedKeyToken> element. The <DerivedKeyToken> element MUST reference the symmetric key. More than one <DerivedKeyToken> element SHOULD be used.<21>

Impact on Token Acquisition Response Message Format: The <DerivedKeyToken> element described in section 3.6.4.1.2.7 MUST be present in the response message. All

<EncryptedData> and <Signature> elements in the message that would reference the symmetric key from the request MUST now reference a <DerivedKeyToken> element. The <DerivedKeyToken> element MUST reference the symmetric key from the request. More than one <DerivedKeyToken> element SHOULD be used.<22>

Impact on Token Acquisition Request Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

PA14: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/wsp:Policy/sp:X509Token/wsp:Policy/sp:RequireThumbprintReference

Overview: Presence of this assertion indicates that a thumbprint reference MUST be used when referencing this token. This policy assertion is described in [WSSP] section 6.3.3.

Impact on Token Acquisition Request Message Format: The <KeyInfo> element described in section 3.6.4.1.2.6 MUST use a <KeyIdentifier> element (section 3.6.4.1.2.13) conforming to [WSS] within a <SecurityTokenReference> element conforming to [WSS]. The <KeyIdentifier> element MUST have a **ValueType** attribute equal to "http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1".

Impact on Token Acquisition Response Message Format: None, the X.509 certificate is not referred to in the response as noted above.

Impact on Token Acquisition Request Message Processing: The client must calculate the thumbprint reference using a SHA1 hash over the certificate file. That thumbprint is then included as above.

Impact on Token Acquisition Response Message Processing: None, the X.509 certificate is not referred to in the response as noted above.

PA15: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/wsp:Policy/sp:X509Token/wsp:Policy/sp:WssX509V3Token10

Overview: Presence of this assertion indicates that an X.509 Version 3 token should be used as defined in [WSSX509TP]. This policy assertion is described in [WSSP] section 6.3.3.

Impact on Token Acquisition Request Message Format: When this assertion is present, the format and references to the X.509 certificate in the message MUST conform to [WSSX509TP].

Impact on Token Acquisition Response Message Format: None. The X.509 certificate is not referred to in the response as noted above.

Impact on Token Acquisition Request Message Processing: None, this impacts message formatting only.

Impact on Token Acquisition Response Message Processing: None, the X.509 certificate is not referred to in the response as noted above.

PA16: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/wsp:Policy/sp:SpnegoContextToken

Overview: Presence of this assertion indicates that a <SecurityContextToken> element obtained by executing an n-leg RST/RSTR SPNEGO binary negotiation protocol with the service MUST be used for protecting the final token request and response messages. This policy assertion is described in [WSSP] section 6.3.5. Nested assertions further restrict the usage of SPNego context tokens. When this assertion is present, the <EndpointReference> element of each corresponding <wsdl:port> element in the Service Metadata Exchange response message MUST contain an <Identity> element (specified in [WSAIdentity]) that contains an <Spn> element (specified in section 3.2 of [WSAIdentity]).<23>

Impact on Token Acquisition Request Message Format: When this policy assertion is present, the <SecurityContextToken> element described in section 3.6.4.1.2.9 MUST be present in the Token Acquisition request message. The <EncryptedKey> element described in section 3.6.4.1.2.6 is not used with a <SecurityContextToken> element and MUST NOT be present in the <Security> (section 3.6.4.1.2.2.2) element. If <DerivedKeyToken> elements are used, then the <SecurityTokenReference> child elements of the <DerivedKeyToken> elements in the response MUST reference the value of the <Identifier> child element of the <SecurityContextToken> element. If <DerivedKeyToken> elements are not used, then the <SecurityTokenReference> child elements of the <EncryptedData> and <Signature> elements in the response MUST reference the value of the <Identifier> child element of the <SecurityContextToken> element present in the request.

Impact on Token Acquisition Response Message Format: If <DerivedKeyToken> elements are used, then the <SecurityTokenReference> child elements of the <DerivedKeyToken> elements in the response MUST reference the value of the <Identifier> child element of the <SecurityContextToken> element present in the request when this policy assertion is present. If <DerivedKeyToken> elements are not used, then the <SecurityTokenReference> child elements of the <EncryptedData> and <Signature> elements in the response MUST reference the value of the <Identifier> child element of the <SecurityContextToken> element present in the request.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the protection mechanism for the Token Acquisition request message MUST use a <SecurityContextToken> element obtained from a WS-TrustForSPNego message protection negotiation as described in section 3.5.4 to protect the message as described in section 3.7.4.1.1.1. If the client receives a response message with <EncryptedData> elements that do not refer to the <Identifier> element of the <SecurityContextToken>, the client MUST fault.

Impact on Token Acquisition Response Message Processing: When this policy assertion is present, the protection mechanism for the Token Acquisition Response Message MUST use the <Identifier> from the <SecurityContextToken> element present in the request to verify protection on the message as described in section 3.7.4.1.1.1.

PA17: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/wsp:Policy/sp:SpnegoContextToken/wsp:Policy/sp:RequireDerivedKeys

Overview: Presence of this assertion indicates that derived keys MUST be used as defined in [WSSC]. This policy assertion is described in [WSSP] section 6.2.1.

Impact on Token Acquisition Request Message Format: The DerivedKeyToken element described in section 3.6.4.1.2.7 MUST be present in the request message. All <EncryptedData> and <Signature> elements in the message that would reference the <SecurityContextToken> element MUST now reference a <DerivedKeyToken> element. The <DerivedKeyToken> element MUST reference the <SecurityContextToken> element. More than one <DerivedKeyToken> element SHOULD be used.<24>

Impact on Token Acquisition Response Message Format: The <DerivedKeyToken> element described in section 3.6.4.1.2.7 MUST be present in the response message. All <EncryptedData> and <Signature> elements in the message that would reference the <SecurityContextToken> element from the request MUST now reference a <DerivedKeyToken> element. The <DerivedKeyToken> element MUST reference the <SecurityContextToken> element from the request. More than one <DerivedKeyToken> element SHOULD be used, see section 3.2.4.1.1.2.1.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

PA18: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:AlgorithmSuite**

Presence of this assertion indicates that the cryptographic algorithms will be restricted. Only nested assertions have a direct impact on the final token request and response.

PA19: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:AlgorithmSuite/wsp:Policy/sp:Basic256

Overview: Presence of this assertion indicates that all referenced algorithm URIs in the Token Acquisition messages MUST be one of the URIs corresponding to the Basic256 AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Request Message Format: When this assertion is present, the **Algorithm** attribute of each of the <EncryptionMethod>, <DigestMethod>, <CanonicalizationMethod>, <SignatureMethod>, and <Transform> elements in the SOAP header MUST be one of the URIs corresponding to the Basic256 AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Response Message Format: When this assertion is present, the **Algorithm** attribute of each of the <EncryptionMethod>, <DigestMethod>, <CanonicalizationMethod>, <SignatureMethod>, and <Transform> elements in the SOAP header MUST be one of the URIs corresponding to the Basic256 AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Request Message Processing: Algorithms not corresponding to the Basic256 AlgorithmSuite specified in [WSSP] section 7.1 MUST NOT be used to perform cryptographic operation on the message to send to the STS.

Impact on Token Acquisition Response Message Processing: The client need not expect to process algorithms not corresponding to the Basic256 AlgorithmSuite specified in [WSSP] section 7.1 for cryptographic operations on the message received from the STS. If the client receives a response using an algorithm that does not correspond to the Basic256 AlgorithmSuite specified in section 7.1 of [WSSP], the client MUST fault.

PA20: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:AlgorithmSuite/wsp:Policy/sp:TripleDes

Overview: Presence of this assertion indicates that all referenced algorithm URIs in the Token Acquisition messages MUST be one of the URIs corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Request Message Format: When this assertion is present, the **Algorithm** attribute of each of the <EncryptionMethod>, <DigestMethod>,

<CanonicalizationMethod>, <SignatureMethod>, and <Transform> elements in the SOAP header MUST be one of the URIs corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Response Message Format: When this assertion is present, the **Algorithm** attribute of each of the <EncryptionMethod>, <DigestMethod>, <CanonicalizationMethod>, <SignatureMethod>, and <Transform> elements in the SOAP header MUST be one of the URIs corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1.

Impact on Token Acquisition Request Message Processing: Algorithms not corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1 MUST NOT be used to perform cryptographic operation on the message to send to the STS.

Impact on Token Acquisition Response Message Processing: The client need not expect to process algorithms not corresponding to the TripleDes AlgorithmSuite specified in [WSSP] section 7.1 for cryptographic operations on the message received from the STS. If the client receives a response using an algorithm that does not correspond to the TripleDes AlgorithmSuite specified in section 7.1 of [WSSP], the client MUST fault.

PA21: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:Layout**

Presence of this assertion indicates that the layout of the <Security> Header element (section 3.6.4.1.2.2.1) defined by [WSS] is restricted. Only nested assertions have a direct impact on the final token request and response.

PA22: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:Layout/wsp:Policy/sp:Strict**

Overview: Presence of this assertion indicates that the layout of the <Security> Header element defined by [WSS] MUST conform to the strict layout rules defined in [WSSP] section 7.7.1.

Impact on Token Acquisition Request Message Format: The impact to message formatting is thoroughly described in [WSSP] section 7.7.1.

Impact on Token Acquisition Response Message Format: The impact to message formatting is thoroughly described in [WSSP] section 7.7.1.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

Impact on Token Acquisition Response Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

PA23: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:IncludeTimestamp**

Overview: Presence of this assertion indicates that a wsu:TimeStamp MUST be present in the <Security> Header element defined by [WSS]. This policy assertion is described in [WSSP] section 7.2.

Impact on Token Acquisition Request Message Format: The Timestamp MUST be included in the request message.

Impact on Token Acquisition Response Message Format: The Timestamp MUST be included in the request message.

Impact on Token Acquisition Request Message Processing: The Timestamp in the <Created> element MUST be the time (GMT) that the message was created. The Timestamp in the <Expires> element SHOULD be the time (GMT) when the message SHOULD be ignored by a recipient.<25>

Impact on Token Acquisition Response Message Processing: The Timestamp in the <Created> element MUST be the time (GMT) that the message was created. The Timestamp in the <Expires> element SHOULD be the time (GMT) when the message SHOULD be ignored by a recipient.<26> When the client receives a message without a Timestamp, the client MUST fault. When the client receives a message with a time in <Created> greater than the current time, the client SHOULD fault. When the client receives a message with a time in <Expires> less than the current time, the client SHOULD fault.

PA24: Policy Assertion **/sp:SymmetricBinding/wsp:Policy/sp:EncryptSignature**

Overview: Presence of this assertion indicates that the primary signature and any signature confirmation elements MUST be encrypted as described in [WSSP] section 7.4.

Impact on Token Acquisition Request Message Format: Every <Signature> element present in the request message <Security> element of the SOAP <Header> element prior to encryption MUST be encrypted inside an <EncryptedData> element present in the request message <Security> element after encryption is performed. <Signature> elements MUST NOT be present in the <Security> element unless encrypted inside an <EncryptedData> element.

Impact on Token Acquisition Response Message Format: Every <Signature> element present in the request message <Security> element of the SOAP <Header> prior to encryption MUST be encrypted inside an <EncryptedData> element present in the request message <Security> element after encryption is performed. <Signature> elements MUST NOT be present in the <Security> element unless encrypted inside an <EncryptedData> element.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the message protection processing MUST encrypt the required signatures according to the formats and mechanism described in [XMLEnc], and only using the algorithms allowed by PA11. Further details on Token Acquisition request message protection processing are described in section 3.7.4.1.1.1.

Impact on Token Acquisition Response Message Processing: For further details on STS processing for this policy assertion, see section 3.2.4. When this policy assertion is present, response messages received without encrypted signatures MUST be rejected by the client.

PA25: Policy Assertion
/sp:SymmetricBinding/wsp:Policy/sp:OnlySignEntireHeadersAndBody

Overview: Presence of this assertion indicates that signature digests MUST only be over the entire SOAP body element, first descendents of the SOAP <Header> element, and/or first descendants of the <Security> Header element. This policy assertion is described in [WSSP] section 7.6.

Impact on Token Acquisition Request Message Format: When this policy assertion is present, Reference elements found in the <SignedInfo> element described in 3.6.4.1.2.14 MUST contain only references to the <Body> element, direct children of the <Header> element or direct children of the <Security> element.

Impact on Token Acquisition Response Message Format: When this policy assertion is present, Reference elements found in the <SignedInfo> element described in 3.6.4.1.2.14

MUST contain only references to the <Body> element, direct children of the <Header> element or direct children of the <Security> element.

Impact on Token Acquisition Request Message Processing: This policy assertion limits how the signature can be applied. Beyond that, no further behavior is changed.

Impact on Token Acquisition Response Message Processing: This policy assertion limits how the signature can be applied. Beyond that, no further behavior is changed.

PA26: Policy Assertion **/sp:EndorsingSupportingTokens**

Presence of this assertion indicates the presence of endorsing tokens that sign the message signature. The nested assertions specify the tokens and message impact for the final token request and response.

PA27: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:X509Token**

Overview: Presence of this assertion indicates that a binary Security Token carrying an X.509 token MUST be used by the client to prove the identity of the user. This policy assertion is described in [WSSP] section 6.3.3. Nested assertions further restrict the usage of X.509 tokens.

Impact on Token Acquisition Request Message Format: When this policy assertion is present, the <BinarySecurityToken> element described in section 3.6.4.1.2.10 MUST be present in the Token Acquisition request message. The **ValueType** attribute of the <BinarySecurityToken> element MUST be equal to "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3". Also, an additional <Signature> element will be present in the SOAP <Header> element under the <Security> element as specified in section 3.6.4.1.2.2.2.

Impact on Token Acquisition Response Message Format: None.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST use the private key associated with an X.509 certificate to prove the identity of the user to the STS as described in section 3.7.4.1.1.2.3.

Impact on Token Acquisition Response Message Processing: None.

PA28: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:X509Token/wsp:Policy/sp:RequireThumbprintReference**

Overview: Presence of this assertion indicates that a thumbprint reference MUST be supported when the X.509 token is not included in the message but is referenced from the message. This policy assertion is described in [WSSP] section 6.3.3.

Impact on Token Acquisition Request Message Format: None, thumbprint reference cannot be used because the client MUST include the X.509 token in the message since the STS does not have access to the full X.509 token prior to receiving the request.

Impact on Token Acquisition Response Message Format: None, the X.509 certificate is not referred to in the response as noted above.

Impact on Token Acquisition Request Message Processing: None, thumbprint reference cannot be used because the STS does not have access to the full X.509 token.

Impact on Token Acquisition Response Message Processing: None, the X.509 certificate is not referred to in the response, as noted above.

PA29: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:X509Token/wsp:Policy/sp:WssX509V3Token10**

Overview: Presence of this assertion indicates that an X.509 Version 3 token should be used as defined in [WSSX509TP]. This policy assertion is described in [WSSP] section 6.3.3.

Impact on Token Acquisition Request Message Format: When this assertion is present, the format and references to the X.509 certificate in the message MUST conform to [WSSX509TP].

Impact on Token Acquisition Response Message Format: None, the X.509 certificate is not referred to in the response, as noted above.

Impact on Token Acquisition Request Message Processing: None, this impacts message formatting only.

Impact on Token Acquisition Response Message Processing: None, the X.509 certificate is not referred to in the response, as noted above.

PA30: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:SpnegoContextToken**

Overview: Presence of this assertion indicates that a <SecurityContextToken> element obtained by executing an n-leg RST/RSTR SPNEGO binary negotiation protocol with the service MUST be used by the client to prove the identity of the user. This policy assertion is described in [WSSP] section 6.3.5. Nested assertions further restrict the usage of SPNego context tokens. When this assertion is present, the <EndpointReference> element of each corresponding <wsdl:port> element MUST contain an <Identity> element (specified in [WSAIdentity]) containing an <Spn> element (specified in section 3.2 of [WSAIdentity]).

Impact on Token Acquisition Request Message Format: When this policy assertion is present, the <SecurityContextToken> element in section 3.6.4.1.2.9 MUST be present in the Token Acquisition request message.

Impact on Token Acquisition Response Message Format: None.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the Token Acquisition request message MUST use a <SecurityContextToken> element obtained from a WS-Trust for SPNego message protection negotiation as described in section 3.4.4.1.1.1 to prove the user's identity as described in section 3.7.4.1.1.2.

Impact on Token Acquisition Response Message Processing: None.

PA31: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:SignedParts**

Presence of this assertion indicates that the section contains policy for elements that MUST be signed. Only nested assertions have a direct impact on the final token request and response. This policy assertion is described in [WSSP] section 5.1.1.

PA32: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:SignedParts/sp:Header**

Overview: Presence of this assertion indicates that the specific SOAP <Header> element that is defined by an XML attribute on the assertion MUST be signed for integrity protection. This policy assertion is described in [WSSP] section 5.1.1.

Impact on Token Acquisition Request Message Format: The <Signature> element described in section 3.6.4.1.2.8 MUST be present in the <Security> element of the SOAP header. A <Reference> element conforming to section 3.6.4.1.2.15 referring to the specified SOAP <Header> element MUST be present in the <SignedInfo> element described in section 3.6.4.1.2.14 of that <Signature> element.

Impact on Token Acquisition Response Message Format: None.

Impact on Token Acquisition Request Message Processing: The specified <Header> element MUST be signed as part of the digital signature present in the message.

Impact on Token Acquisition Response Message Processing: None.

PA33: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:KerberosToken**

Overview: Presence of this assertion indicates that a Kerberos token MUST be used by the client to prove the identity of the user. This policy assertion is described in [WSSP] section 6.3.4. Nested assertions further restrict the usage of issued tokens.

Impact on Token Acquisition Request Message Format: When this policy assertion is present, the <BinarySecurityToken> element described in section 3.6.4.1.2.10 MUST be present in the Token Acquisition request message.

Impact on Token Acquisition Response Message Format: None.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST use the key associated with a Kerberos token to prove the identity of the user to the STS as described in section 3.7.4.1.1.2.2.

Impact on Token Acquisition Response Message Processing: None.

PA34: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/mssp:RsaToken**

Overview: Presence of this assertion indicates that if the client is requesting an asymmetric key in the security token, the client must prove possession of the private key corresponding to the public key that is present in the <UseKey> element of the request.

Impact on Token Acquisition Request Message Format: When this policy assertion is present, an additional <Signature> element will be present in the SOAP <Header> element under the <Security> element as specified in section 3.6.4.1.2.2.2.

Impact on Token Acquisition Response Message Format: None.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST use the private key that is associated with the public key that is present in the <UseKey> element of the request to prove that the user has access to the private key.

Impact on Token Acquisition Response Message Processing: None.

PA35: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:IssuedToken**

Overview: Presence of this assertion indicates that an issued token MUST be used by the client to prove the identity of the user. This policy assertion is described in [WSSP] section 6.3.2. Nested assertions further restrict the usage of issued tokens.

Impact on Token Acquisition Request Message Format: When this policy assertion is present, the Assertion element described in section 3.6.4.1.2.16 MUST be present in the Token Acquisition request message.

Impact on Token Acquisition Response Message Format: None.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST use the key associated with an issued token to prove the identity of the user to the STS as described in section 3.7.4.1.1.2.5.

Impact on Token Acquisition Response Message Processing: None.

PA36: Policy Assertion
/sp:EndorsingSupportingTokens/wsp:Policy/sp:IssuedToken/sp:RequestSecurityTokenTemplate/t:KeyType

Overview: Presence of this assertion indicates that the corresponding KeyType element MUST be used when requesting a conformant issued token from a different STS.

Impact on Token Acquisition Request Message Format: If the <KeyType> element of the assertion is equal to "http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey" or "http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey", then the issued token that is used to verify the user's identity MUST contain an asymmetric key. If the <KeyType> element of the assertion is equal to "http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey" or "http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey", then the issued token that is used to verify the user's identity MUST contain a symmetric key.

Impact on Token Acquisition Response Message Format: None.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST use the private or symmetric key associated with the issued token to prove the identity of the user to the STS as described in section 3.7.4.1.1.2.5.

Impact on Token Acquisition Response Message Processing: None.

PA37: Policy Assertion
/sp:EndorsingSupportingTokens/wsp:Policy/sp:IssuedToken/wsp:Policy/sp:RequireDerivedKeys

Overview: Presence of this assertion indicates that derived keys MUST be used as defined in [WSSC]. This policy assertion is described in [WSSP] section 6.2.1.

Impact on Token Acquisition Request Message Format: The <DerivedKeyToken> element described in section 3.6.4.1.2.7 MUST be present in the request message. All <EncryptedData> and <Signature> elements in the message that would reference the issued token MUST now reference a <DerivedKeyToken> element. The <DerivedKeyToken> element MUST reference the SAML <Assertion> element described in section 3.6.4.1.2.16. More than one <DerivedKeyToken> element SHOULD be used.<27>

Impact on Token Acquisition Response Message Format: None, see section 3.2.4.1.1.2.1.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the new message format, no further behavior changes are required.

Impact on Token Acquisition Response Message Processing: None.

PA38: Policy Assertion **/sp:EndorsingSupportingTokens/wsp:Policy/sp:IssuedToken/wsp:Policy/sp:RequireInternalReference**

Overview: Presence of this assertion indicates that an internal reference to the issued token MUST be used when referencing the issued token. This policy assertion is described in [WSSP] section 6.3.2.

Impact on Token Acquisition Request Message Format: None.

Impact on Token Acquisition Response Message Format: When this policy assertion is present, the <RequestedAttachedReference> element (section 3.6.4.1.1.2.2.4) MUST be present in the Token Acquisition Response Message.

Impact on Token Acquisition Request Message Processing: None.

Impact on Token Acquisition Response Message Processing: If the response does not contain the <RequestedAttachedReference> element, the client MUST fault.

PA39: Policy Assertion **/sp:SignedSupportingTokens**

Presence of this assertion indicates that signed tokens are included in the message signature. The nested assertions specify the tokens and message impact for the final token request and response.

PA40: Policy Assertion **/sp:SignedSupportingTokens/wsp:Policy/sp:UsernameToken**

Overview: Presence of this assertion indicates that a username token MUST be used by the client to prove the identity of the user. This policy assertion is described in [WSSP] section 6.3.1. Nested assertions further restrict the usage of username tokens.

Impact on Token Acquisition Request Message Format: When this policy assertion is present, the <UsernameToken> element described in section 3.6.4.1.2.11 MUST be present in the Token Acquisition Request Message. The <UsernameToken> element MUST contain a <Username> element and a <Password> element.

Impact on Token Acquisition Response Message Format: None.

Impact on Token Acquisition Request Message Processing: When this policy assertion is present, the client MUST place the username and password in the <UsernameToken> element to prove the identity of the user to the STS as described in section 3.7.4.1.1.2.4.

Impact on Token Acquisition Response Message Processing: None.

PA41: Policy Assertion **/sp:SignedSupportingTokens/wsp:Policy/sp:UsernameToken/wsp:Policy/sp:WssUsernameToken10**

Overview: Presence of this assertion indicates that a username token should be used as defined in [WSSUTP]. This policy assertion is described in [WSSP] section 6.3.1.

Impact on Token Acquisition Request Message Format: When this assertion is present, the format and references to the username token in the message MUST conform to [WSSUTP].

Impact on Token Acquisition Response Message Format: None, the username token is not referred to in the response as noted above.

Impact on Token Acquisition Request Message Processing: None, this impacts message formatting only.

Impact on Token Acquisition Response Message Processing: None, the username token is not referred to in the response as noted above.

PA42: Policy Assertion **/sp:Wss11**

Presence of this assertion indicates that the use of WS-Security 1.1 described in [WSS] is restricted. Only nested assertions have a direct impact on the final token request and response. This policy assertion is described in [WSSP] section 10.

PA43: Policy Assertion **/sp:Wss11/wsp:Policy/sp:MustSupportRefKeyIdentifier**

Overview: Presence of this assertion indicates that the initiator and recipient MUST be able to process key-specific identifier token references. This policy assertion is described in [WSSP] section 10.

Impact on Token Acquisition Request Message Format: When this policy assertion is present with PA12 or PA27, the request message SHOULD contain a key specific identifier as part of a <SecurityTokenReference> inside any element under the <Security> element of the SOAP header.<28>

Impact on Token Acquisition Response Message Format: When this policy assertion is present with PA12 or PA27, the response message SHOULD contain a key specific identifier as part of a <SecurityTokenReference> element inside any element under the <Security> element of the SOAP header in the response message. See section 3.2.4.1.1.2.1 for details on whether the STS uses key identifiers in response messages.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the message format for key specific identifiers and generating those identifiers, no further behavior changes are required to emit key specific identifier references. For the STS message processing behavior, see section 2.

Impact on Token Acquisition Response Message Processing: When this policy assertion is present, the client MUST be able to accept and resolve a key specific identifier used in the response message. For the STS message processing behavior, see section 2.

PA44: Policy Assertion **/sp:Wss11/wsp:Policy/sp:MustSupportRefIssuerSerial**

Overview: Presence of this assertion indicates that the initiator and recipient MUST be able to process references using the issuer and token serial number.

Impact on Token Acquisition Request Message Format: When this policy assertion is present with PA12 or PA27, the request message SHOULD contain an <X509IssuerSerial> element as part of a <SecurityTokenReference> element inside any element under the <Security> element of the SOAP header.<29>

Impact on Token Acquisition Response Message Format: When this policy assertion is present with PA12 or PA27, the response message SHOULD contain an <X509IssuerSerial>

element as part of a <SecurityTokenReference> inside any element under the <Security> element of the SOAP header in the response message. See section 3.2.4.1.1.2.1 for details on whether the STS uses <X509IssuerSerial> elements in response messages.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the message format for issuer and serial number identifiers and generating those identifiers, no further behavior changes are required to emit issuer and serial number references. For the STS message processing behavior, see section 2.

Impact on Token Acquisition Response Message Processing: When this policy assertion is present, the client MUST be able to accept and resolve an issuer and serial number identifier used in the response message. For the STS message processing behavior, see section 2.

PA45: Policy Assertion **/sp:Wss11/wsp:Policy/sp:MustSupportRefThumbprint**

Overview: Presence of this assertion indicates that the initiator and recipient MUST be able to process references using token thumbprints. This policy assertion is described in [WSSP] section 10.

Impact on Token Acquisition Request Message Format: When this policy assertion is present in PA12 or PA27, the request message SHOULD contain a thumbprint reference as part of a <SecurityTokenReference> inside any element under the <Security> element of the SOAP header.<30>

Impact on Token Acquisition Response Message Format: When this policy assertion is present in PA12 or PA27, the response message SHOULD contain a thumbprint reference as part of a <SecurityTokenReference> inside any element under the <Security> element of the SOAP header in the response message. See section 3.2.4.1.1.2.1 for details on whether the STS uses thumbprint references in response messages.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the message format for a thumbprint reference and generating that reference, no further behavior changes are required to emit a thumbprint reference in the request message. For the STS message processing behavior, see section 2.

Impact on Token Acquisition Response Message Processing: When this policy assertion is present, the client MUST be able to accept and resolve a thumbprint reference used in the response message. For the STS message processing behavior, see section 2.

PA46: Policy Assertion **/sp:Wss11/wsp:Policy/sp:MustSupportRefEncryptedKey**

Overview: Presence of this assertion indicates that the initiator and recipient MUST be able to process references using <EncryptedKey> element references. This policy assertion is described in [WSSP] section 10.

Impact on Token Acquisition Request Message Format: When this policy assertion is present in PA12 or PA27, the request message SHOULD reference an <EncryptedKey> element that is not contained in the message (but that is understood by the context of the message) as part of a <SecurityTokenReference> inside any element under the <Security> element of the SOAP header.<31>

Impact on Token Acquisition Response Message Format: When this policy assertion is present in PA1 or PA27, the response message SHOULD reference an <EncryptedKey> element that is not contained in the message (but that is understood by the context of the message) as part of a <SecurityTokenReference> inside any element under the <Security> element of the SOAP header in the response message.

See section 3.2.4.1.1.2.1 for details on whether the STS uses the <EncryptedKey>.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the message format a thumbprint reference and generating that reference, no further behavior changes are required to emit a reference to an <EncryptedKey> element not present in the message. For the STS message processing behavior, see section 2.

Impact on Token Acquisition Response Message Processing: When this policy assertion is present, the client MUST be able to accept and resolve a reference to an <EncryptedKey> element not present in the response message. The referenced <EncryptedKey> element SHOULD be identical to the <EncryptedKey> element from the request message that the response message is responding to. For the STS message processing behavior, see section 2.

PA47: Policy Assertion **/sp:Wss11/wsp:Policy/sp:RequireSignatureConfirmation**

Overview: Presence of this assertion indicates that <wsse11:SignatureConfirmation> elements should be used as defined in [WSS]. This policy assertion is described in [WSSP] section 10.

Impact on Token Acquisition Request Message Format: None.

Impact on Token Acquisition Response Message Format: When this policy assertion is present, the <Security> element of the SOAP header in the response message MUST contain a <SignatureConfirmation> element as described in 3.6.4.1.2.2.2 for each incoming <Signature> element of the request. If policy assertion PA15 is in effect, each <SignatureConfirmation> element will be found encrypted inside an <EncryptedData> element.

Impact on Token Acquisition Request Message Processing: None.

Impact on Token Acquisition Response Message Processing: When this policy assertion is present, the client MUST validate that the value of each <Signature> element sent in the request has been copied into a corresponding <SignatureConfirmation> element for the response.

PA48: Policy Assertion **/sp:Trust10**

Presence of this assertion indicates that the use of WS-Trust as described in [WSTrust1.3] is restricted. The XML namespace for WS-Trust requests and responses MUST be "http://schemas.xmlsoap.org/ws/2005/02/trust". The value of the <wsa:Action> element for a WS-Trust request MUST be "http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue". The value of the <wsa:Action> element for a WS-Trust response MUST be "http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue". This policy assertion is described in [WSSP] section 11.

PA49: Policy Assertion **/sp:Trust10/wsp:Policy/sp:RequireClientEntropy**

Overview: Presence of this assertion indicates that client entropy MUST be used as key material for a requested symmetric key proof token. This policy assertion is described in [WSSP] section 11.

Impact on Token Acquisition Request Message Format: The <Entropy> element described in sections 3.7.4.1.2.3.3 and 3.6.4.1.1.2.2.9 MUST be included in the request message.

Impact on Token Acquisition Response Message Format: None.

Impact on Token Acquisition Request Message Processing: The client MUST compute a cryptographically random number to include in the request message to the STS as part of the <Entropy> element. For the STS message processing behavior, see section 2.

Impact on Token Acquisition Response Message Processing: None.

PA50: Policy Assertion **/sp:Trust10/wsp:Policy/sp:RequireServerEntropy**

Overview: Presence of this assertion indicates that server entropy MUST be used as key material for a requested symmetric key proof token. This policy assertion is described in [WSSP] section 11.

Impact on Token Acquisition Request Message Format: None.

Impact on Token Acquisition Response Message Format: If a symmetric key token is requested and client entropy was used as described in PA49 and section 3.7.4.1.2.3.3, the response message MUST contain the <ComputedKey> and <Entropy> elements as described in section 3.6.4.1.1.2.2.8. If no client entropy was used, the policy assertion has no impact on the response message.

Impact on Token Acquisition Request Message Processing: None.

Impact on Token Acquisition Response Message Processing: If client entropy was used as described in PA49 and section 3.7.4.1.2.3.3, the response message MUST contain the <ComputedKey> and <Entropy> elements as described in section 3.6.4.1.1.2.2.8. The actual <RequestedProofToken> MUST be calculated from these values as well as the entropy sent from the client. Otherwise, the entropy from the server MUST be the value of the key inside the proof token.

PA51: Policy Assertion **/sp:Trust10/wsp:Policy/sp:MustSupportIssuedTokens**

Overview: Presence of this assertion indicates that the wst:IssuedTokens header is supported as described in WS-Trust.

Impact on Token Acquisition Request Message Format: None, the wst:IssuedTokens header is not used for messages of this protocol.

Impact on Token Acquisition Response Message Format: None, the wst:IssuedTokens header is not used for messages of this protocol.

Impact on Token Acquisition Request Message Processing: None, the wst:IssuedTokens header is not used for messages of this protocol.

Impact on Token Acquisition Response Message Processing: None, the wst:IssuedTokens header is not used for messages of this protocol.

PA52: Policy Assertion **/sp:Trust13**

Presence of this assertion indicates that the use of WS-Trust as described in [WSTrust1.3] is restricted. The XML namespace for WS-Trust requests and responses MUST be "http://docs.oasis-open.org/ws-sx/ws-trust/200512". The value of the <wsa:Action> element for a WS-Trust request MUST be "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue". The value of the <wsa:Action> element for a WS-Trust response MUST be "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Issue", or "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal". This policy assertion is described in [WSSP1.2] section 10.

PA53: Policy Assertion **/sp:Trust13/wsp:Policy/sp:RequireClientEntropy**

Overview: Presence of this assertion indicates that client entropy MUST be used as key material for a requested symmetric key proof token. This policy assertion is described in [WSSP] section 11.

Impact on Token Acquisition Request Message Format: The <Entropy> element described in sections 3.7.4.1.2.3.3 and 3.6.4.1.1.2.2.9 MUST be included in the request message.

Impact on Token Acquisition Response Message Format: None.

Impact on Token Acquisition Request Message Processing: The client MUST compute a cryptographically random number to include in the request message to the STS as part of the <Entropy> element described in section 3.6.4.1.1.2.2.9. For the STS message processing behavior, see section 2.

Impact on Token Acquisition Response Message Processing: None.

PA54: Policy Assertion **/sp:Trust13/wsp:Policy/sp:RequireServerEntropy**

Overview: Presence of this assertion indicates that server entropy MUST be used as key material for a requested symmetric key proof token. This policy assertion is described in [WSSP] section 11.

Impact on Token Acquisition Request Message Format: None.

Impact on Token Acquisition Response Message Format: If a symmetric key token is requested and client entropy was used as described in PA53 and section 3.7.4.1.2.3.3, the response message MUST contain the <ComputedKey> and <Entropy> elements as described in section 3.6.4.1.1.2.2.8. If no client entropy was used, the policy assertion has no impact on the response message.

Impact on Token Acquisition Request Message Processing: None.

Impact on Token Acquisition Response Message Processing: If client entropy was used as described in PA53 and section 3.7.4.1.2.3.3, the response message MUST contain the <ComputedKey> and <Entropy> elements as described in section 3.6.4.1.1.2.2.8. The actual RequestedProofToken MUST be calculated from these values as well as the entropy sent from the client. Otherwise, the entropy from the server MUST be value of the key inside the proof token.

PA55: Policy Assertion **/sp:Trust13/wsp:Policy/sp:MustSupportIssuedTokens**

Overview: Presence of this assertion indicates that the wst:IssuedTokens header is supported as described in [WSTrust1.3].

Impact on Token Acquisition Request Message Format: None, the wst:IssuedTokens header is not used for messages of this protocol.

Impact on Token Acquisition Response Message Format: None, the wst:IssuedTokens header is not used for messages of this protocol.

Impact on Token Acquisition Request Message Processing: None, the wst:IssuedTokens header is not used for messages of this protocol.

Impact on Token Acquisition Response Message Processing: None, the wst:IssuedTokens header is not used for messages of this protocol.

PA56: Policy Assertion **/wsaw:UsingAddressing**

Overview: Presence of this assertion indicates that services MUST use WS-Addressing for request messages and use of the message addressing properties MUST be fully compliant with this specification; in particular, senders MUST use all message addressing properties mandated by [WSA], applicable WS-Addressing protocol bindings, and MUST follow all applicable WS-Addressing normative requirements. This policy assertion is described in [WSAWSDL] section 3.1.

Impact on Token Acquisition Request Message Format: The WS-Addressing fields described in section 3.6.4.1.2.2.1 MUST be present in the SOAP header. The value of the <To> element MUST be the STS endpoint described in section 3.3.3. The value of the <MessageID> element MUST be a random globally unique identifier for the message.

Impact on Token Acquisition Response Message Format: The WS-Addressing fields described in section 3.6.4.1.2.2.2 MUST be present in the SOAP header. The value of the <RelatesTo> element MUST be the value of the <MessageID> element in the corresponding request.

Impact on Token Acquisition Request Message Processing: Beyond accommodating the new message format and generating the required values, no further behavior changes are required.

Impact on Token Acquisition Response Message Processing: The client MUST verify that the value of the <RelatesTo> element matches the value of the <MessageID> element used in the request message. If the value does not match, the client MUST reject the message and display an error to the user. Beyond accommodating the new message format and validating this value, no further behavior changes are required.

3.3.4.2 Effects of Policy Elements with Message Policy Subject

[WSSP] defines the effects of security policy assertions with message policy subject for the protocol. The relevant policy assertions for this protocol are listed here. Policy assertion IDs (PAXX) are included to allow referencing specific policy assertions within this specification. For convenience, the sp: prefix used in [WSSP] is repeated here before the policy assertion elements.

PA57: Policy Assertion **/sp:SignedParts**

Presence of this assertion indicates that the section contains policy for elements that MUST be signed. Only nested assertions have a direct impact on the final token request and response. This policy assertion is described in [WSSP] section 5.1.1.

PA58: Policy Assertion **/sp:SignedParts/sp:Body**

Overview: Presence of this assertion indicates that the entire <s:Body> element, its attributes and content, MUST be signed for integrity protection. This policy assertion is described in [WSSP] section 5.1.1.

Impact on Token Acquisition Request Message Format: The Signature element MUST be present in the Security element of the SOAP header. A Reference element referring to the SOAP body MUST be present in the SignedInfo element of that <Signature> element.

Impact on Token Acquisition Response Message Format: The <Signature> element MUST be present in the <Security> element of the SOAP header. A <Reference> element referring to the SOAP body MUST be present in the <SignedInfo> element of that <Signature> element.

Impact on Token Acquisition Request Message Processing: The body MUST be signed as part of the digital signature present in the message.

Impact on Token Acquisition Response Message Processing: The body MUST be signed as part of the digital signature present in the message. The client MUST reject the message if the body is not signed.

PA59: Policy Assertion **/sp:SignedParts/sp:Header**

Overview: Presence of this assertion indicates that the specific SOAP <Header> element that is defined by an XML attribute on the assertion MUST be signed for integrity protection. This policy assertion is described in [WSSP] section 5.1.1.

Impact on Token Acquisition Request Message Format: The <Signature> element MUST be present in the <Security> element of the SOAP header. A <Reference> element referring to the specified SOAP <Header> element MUST be present in the <SignedInfo> element of that <Signature> element.

Impact on Token Acquisition Response Message Format: The <Signature> element MUST be present in the <Security> element of the SOAP header. A <Reference> element referring to the specified SOAP <Header> element MUST be present in the <SignedInfo> of that <Signature> element.

Impact on Token Acquisition Request Message Processing: The specified <Header> element MUST be signed as part of the digital signature present in the message.

Impact on Token Acquisition Response Message Processing: The specified <Header> element MUST be signed as part of the digital signature present in the message. The client MUST reject the message if the specified <Header> element is not signed.

PA60: Policy Assertion **/sp:EncryptedParts**

Presence of this assertion indicates that the section contains policy for elements that MUST be encrypted. Only nested assertions have a direct impact on the final token request and response. This policy assertion is described in [WSSP] section 5.2.1.

PA61: Policy Assertion **/sp:EncryptedParts/sp:Body**

Overview: Presence of this assertion indicates that the entire <s:Body> element, its attributes and content, MUST be encrypted for confidentiality protection. This policy assertion is described in [WSSP] section 5.2.1.

Impact on Token Acquisition Request Message Format: The <EncryptedData> element described in section 3.6.4.1.2.2.1 MUST be the only root element present in the SOAP <Body> element. The entire contents of the SOAP <Body> element MUST be encrypted inside the <CipherValue> element of the <EncryptedData> element.

Impact on Token Acquisition Response Message Format: The <EncryptedData> element described in section 3.6.4.1.2.2.1 MUST be the only root element present in the SOAP <Body> element. The entire contents of the SOAP <Body> element MUST be encrypted inside the <CipherValue> element of the <EncryptedData> element.

Impact on Token Acquisition Request Message Processing: The body MUST be encrypted.

Impact on Token Acquisition Response Message Processing: The body MUST be encrypted. The client MUST reject the message if the body is not encrypted.

3.3.5 Timer Events

There are no protocol-specific timer events that are serviced by an implementation. This protocol does not require timers except those that may be used by the underlying transport to transmit and receive messages over HTTP. The protocol does not include provisions for time-based retry for sending protocol messages.

3.3.6 Other Local Events

This protocol does not have dependencies on any transport protocols other than HTTP 1.1. This protocol relies on this transport mechanism for the correct and timely delivery of protocol messages. The protocol does not take action in response to any changes or failure in machine state or network communications.

3.4 Message Protection Negotiation Port Type Server Details

This port type uses the protocol defined in [WSTSPNego] to negotiate message protection. The port type name for Message Protection Negotiation is defined as SecurityTokenService in [WSTSPNego].

3.4.1 Abstract Data Model

No abstract data model is defined beyond that defined in [WSTSPNego] for this port type.

3.4.2 Timers

There are no protocol-specific timer events that are serviced by an implementation. The protocol does not include provisions for time-based retry for sending protocol messages.

3.4.3 Initialization

To service protocol messages, an STS MUST be listening for requests at the endpoint URLs being used by the client.

The protocol does not require specific initialization on receipt of a protocol message.

To service Token Acquisition request messages, an STS may need to access one or more local or remote sources of user data. If one or more of these sources is unavailable, the STS MAY fault.<32>

3.4.4 Message Processing Events and Sequencing Rules

The following table summarizes the list of WSDL operations as defined by this specification:

Operation	Description
RequestSecurityToken	This is the operation for protection negotiation specified in [WSTSPNego] section 3.

3.4.4.1 RequestSecurityToken

The following sections describe semantics for the message protection negotiation messages that are specified in section 3.4.4.1.1 and briefly outlined in section 3. Message protection negotiation MUST use WS-Trust for SPNego.

As described in policy assertion PA08 above, if the sp:SpnegoContextToken policy assertion is the only assertion under the /sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/ assertion, then a token obtained using the WS-Trust for SPNego protocol MUST be used for securing the message from the client. If the /sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/ assertion does not contain the sp:SpnegoContextToken policy assertion, the WS-Trust for SPNego exchange MUST NOT occur. In this case the next message received by the STS from the client MUST be the Token Acquisition request.

The WS-Trust for SPNego protocol is described in [WSTSPNego] section 3. As described in [WSTSPNego], the WS-Trust for SPNego protocol uses the WS-Trust protocol defined in [WSTrust1.3], to tunnel SPNego messages defined in [RFC2478]. The number of message request and response pairs MUST be determined by the mechanics of the actual SPNego messages exchanged, as described in [RFC2478]. In addition, the presence of the WS-Trust <BinaryExchange> element in the last message MUST be determined by the actual SPNego messages that are exchanged. Finally, the generated key MUST match any key size specified in the WS-Trust for SPNego Initial Request Message.

3.4.4.1.1 Messages

The following table summarizes the set of WSDL message definitions that are specific to this operation.

Message	Description
RequestSecurityTokenMsg	This is the message type for request messages specified in [WSTSPNego] section 3.
RequestSecurityTokenResponseMsg	This is the message type for response messages specified in [WSTSPNego] section 3.

3.4.4.1.1.1 RequestSecurityTokenMsg

WS-TrustForSPNego defines a set of message Protection Negotiation messages. The following messages are specified in [WSTSPNego] section 3.

3.4.4.1.1.1.1 Initial Request

This message MUST conform to Message 1 described in [WSTSPNego] section 3.

[WSTSPNego] offers two choices for the value of the <Action> element in the SOAP header. Since WS-Trust 1.3 is not used, the <Action> element in the SOAP header MUST equal "http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue".

[WSTSPNego] offers two choices for the value of <RequestType> element within the <RequestSecurityToken> element. Since WS-Trust 1.3 is not used, the <RequestType> element in the <RequestSecurityToken> element MUST equal "http://schemas.xmlsoap.org/ws/2005/02/trust/Issue".

[WSTSPNego] offers two choices for the value of <TokenType> element within the <RequestSecurityToken>. Since WS-SecureConversation 1.3 is not used, the <TokenType> element in the <RequestSecurityToken> element MUST equal "http://schemas.xmlsoap.org/ws/2005/02/sc/sct".

An <AppliesTo> element MUST NOT be included.

3.4.4.1.1.1.2 Continued Negotiation Request

This message MUST conform to Message 3 described in [WSTSPNego] section 3.

[WSTSPNego] offers two choices for the value of the <Action> element in the SOAP header conforming to [WSA]. Since WS-Trust 1.3 is not used, the <Action> element in the SOAP header MUST equal "http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue".

3.4.4.1.1.2 RequestSecurityTokenResponseMsg

WS-TrustForSPNego defines a set of message Protection Negotiation messages. The following messages are specified in [WSTSPNego] section 3.

3.4.4.1.1.2.1 Continued Negotiation Response

This message MUST conform to Message 2 described in [WSTSPNego] section 3.

[WSTSPNego] offers two choices for the value of the <Action> element in the SOAP header. Since WS-Trust 1.3 is not used, the <Action> element in the SOAP header MUST equal "http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue".

3.4.4.1.1.2.2 Final Response

This message MUST conform to Message 4 described in [WSTSPNego] section 3.

[WSTSPNego] offers two choices for the value of the <TokenType> element within the <RequestSecurityTokenResponse> element. Since [WSTrust1.3] is not used, the <TokenType> element in the <RequestSecurityTokenResponse> element MUST equal "http://schemas.xmlsoap.org/ws/2005/02/sc/sct".

[WSTSPNego] offers two choices for the value of the <Action> element in the SOAP header conforming to [WSA]. Since WS-Trust 1.3 ([WSTrust1.3]) is not used, the <Action> element in the SOAP header MUST equal "http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue".

3.4.5 Timer Events

There are no protocol-specific timer events that are serviced by an implementation. This protocol does not require timers except those that may be used by the underlying transport to transmit and receive messages over HTTP. The protocol does not include provisions for time-based retry for sending protocol messages.

3.4.6 Other Local Events

This protocol does not have dependencies on any transport protocols other than HTTP 1.1. This protocol relies on this transport mechanism for the correct and timely delivery of protocol messages. The protocol does not take action in response to any changes or failure in machine state or network communications.

3.5 Message Protection Negotiation Port Type Client Details

This port type uses the protocol defined in [WSTSPNego] to negotiate message protection. The port type name for Message Protection Negotiation is defined as SecurityTokenService in [WSTSPNego].

3.5.1 Abstract Data Model

No abstract data model is defined beyond that defined in [WSTSPNego] for this port type.

3.5.2 Timers

Clients SHOULD fault if a Message Protection Negotiation Response Message is not received within 1 minute after a Message Protection Negotiation Request Message is issued to the server role.

There are no other protocol-specific timer events that are serviced by an implementation. The protocol does not include provisions for time-based retry for sending protocol messages.

3.5.3 Initialization

There is no specific initialization required by clients.

3.5.4 Message Processing Events and Sequencing Rules

The Message Protection Negotiation messages MAY be used by the client and Security Token Service (STS) to further negotiate the cryptographic keys that should be used to protect the Token Acquisition messages. The following sections describe semantics for the message protection negotiation messages that are specified in section 3.4.4.1.1. Message protection negotiation MUST be WS-Trust for SPNego message protection negotiation, as described in section 3.5.4.

As described in policy assertion PA16, if the sp:SpnegoContextToken policy assertion is the only assertion under the /sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/ assertion, then a token obtained using the WS-TrustForSPNego protocol MUST be used for securing the message to the STS. If the /sp:SymmetricBinding/wsp:Policy/sp:ProtectionToken/ assertion does not contain the sp:SpnegoContextToken policy assertion, the WS-TrustForSPNego exchange MUST NOT occur. In this case the next message sent by the client MUST be the Token Acquisition request.

The WS-TrustForSPNego protocol is described in [WSTSPNego] section 3. As described in [WSTSPNego], the WS-TrustForSPNego protocol uses the WS-Trust protocol defined in [WSTrust1.3], to tunnel SPNego messages defined in [RFC2478]. The number of message request and response pairs MUST be determined by the mechanics of the actual SPNego messages exchanged, as described in [RFC2478]. In addition, the presence of the [WSTrust1.3] <BinaryExchange> element in the last message MUST be determined by the actual SPNego messages that are exchanged.

The SecurityContextToken element of the final WS-TrustForSPNego exchange response message MUST be included in the Token Acquisition request message as described in section 3.7.4.

3.5.5 Timer Events

There are no protocol-specific timer events that are serviced by an implementation. This protocol does not require timers except those that may be used by the underlying transport to transmit and receive messages over HTTP. The protocol does not include provisions for time-based retry for sending protocol messages.

3.5.6 Other Local Events

This protocol does not have dependencies on any transport protocols other than HTTP 1.1. This protocol relies on this transport mechanism for the correct and timely delivery of protocol messages. The protocol does not take action in response to any changes or failure in machine state or network communications.

3.6 Token Acquisition Server Details

This port type uses the protocol defined in [WSTrust1.3] to send/receive a security token. The protocol uses port types IWSTrustFeb2005Async and IWSTrust13Async for Token Acquisition. The port types implement substantially the same protocol, and so are documented in a single section. Differences are called out inline.

3.6.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

Section 3.7.1 of the abstract data model for clients applies equally well to the abstract data model for servers.

Chosen Token Acquisition Endpoint: The **STS Token Acquisition Endpoint** used by the client for the Token Acquisition message exchange. This endpoint determines the policy assertions that are in effect at the server.

ServerPAInEffect: The policy assertions in effect for the server depend on the **Chosen Token Acquisition Endpoint**. This element is an array of Boolean values to track which policy assertions are in effect for a particular Token Acquisition request. The index to the array represents the assertion number, and the array is initialized to false.

STS Service Metadata Exchange Client Request Type: Section 3.2.4.1 describes two types of requests that may be issued to begin the protocol. The server implementation must preserve which request type was used by the client in order to respond using the same type.

X.509 Session Key: When clients authenticate with an X.509 certificate, a symmetric session key is used in the Token Acquisition request as described in section 3.6.4.1.1.2.1.3. This value is used in the response as well, so it must be preserved. This value is a 256-bit binary value used as a symmetric key.

X.509 Session Key Identifier: When clients authenticate with an X.509 certificate, a symmetric session key is used in the request as described in section 3.6.4.1.1.2.1.3. This value is identified in the response as well, so the identifier of the key must be preserved. This value is a string identifier for the symmetric key.

ClientSignatureValues: This element is an array of incoming client signature values. As described for PA47 in section 3.2.4.1.1.2.1, when PA47 is in effect, the server must include the signature values received from the client in the response to the client. The length of the array is determined by the number of signatures received from the client.

3.6.2 Timers

There are no protocol-specific timer events that are serviced by an implementation. The protocol does not include provisions for time-based retry for sending protocol messages.

3.6.3 Initialization

Before any protocol messages can be exchanged, an STS SHOULD exchange metadata with relying parties and other STSs.<33>

To service protocol messages, an STS MUST be listening for requests at the endpoint URLs being used by the client.

To service Token Acquisition request messages, an STS SHOULD have network access to the Certificate Revocation List (CRL) Distribution Point contained in any X509 certificates used to secure the message or sign the token that is used to secure the message.<34>

To service Token Acquisition request messages, an STS may need to access one or more local or remote sources of user data. If one or more of these sources is unavailable, the STS MAY fault.<35>

The protocol does not require specific initialization on receipt of a protocol message.

3.6.4 Message Processing Events and Sequencing Rules

The following table summarizes the list of WSDL operations as defined by this specification:

Operation	Description
Trust13IssueAsync	Used to issue a security token. This is the operation for port type.
TrustFeb2005IssueAsync	Used to issue a security token. This is the operation for port type.

3.6.4.1 Trust13IssueAsync and TrustFeb2005IssueAsync

These operations are used to issue security tokens to clients.

3.6.4.1.1 Messages

The following table summarizes the set of WSDL message definitions that are specific to this operation.

Message	Description
IWSTrust13Async_Trust13IssueAsync_InputMessage	Used to request a security token.This is the name of the request message in operation Trust13IssueAsync.
IWSTrust13Async_Trust13IssueAsync_OutputMessage	Used to receive a security token.This is the name of the response message in operation Trust13IssueAsync.
IWSTrustFeb2005Async_TrustFeb2005IssueAsync_InputMessage	Used to request a security token. This is the name of the request message in operation TrustFeb2005IssueAsync.
IWSTrustFeb2005Async_TrustFeb2005IssueAsync_OutputMessage	Used to receive a security token. Used to request a security token. This is the name of the response message in operation TrustFeb2005IssueAsync.

3.6.4.1.1.1 IWSTrust13Async_Trust13IssueAsync_InputMessage and IWSTrustFeb2005Async_TrustFeb2005IssueAsync_InputMessage

The following sections describe the aspects of processing a request message.

3.6.4.1.1.1.1 SOAP Header Processing

The first processing step on receipt of a request message MUST be to verify the protection of the response message. To verify the protection of the message, the STS MUST:

- If PA56 is in effect, the STS MUST successfully decrypt the message to remove any confidentiality protections.
- If PA53 is in effect, the STS MUST successfully check the integrity of the message protection mechanisms to ensure the message has not been altered in transit.
- The STS MUST verify the identity of the client that sent the message is the claimed identity. To verify that the identity of the client user is the claimed identity, the STS MUST use the X509 certificate, username, SPNego context token, Kerberos token, or SAML token and evaluate the proof of possession that the client provided in the SOAP header.
- Optionally, if the client is requesting an asymmetric token, verify that the client has possession of the private key corresponding to the public key in the <UseKey> element.

Once these steps are complete, the request body MUST be processed.

3.6.4.1.1.1.2 SOAP Body Processing

The following sections describe the processing rules for the SOAP body of the incoming Token Acquisition request message sectioned by the elements that are present in the body.

3.6.4.1.1.1.2.1 <RequestType> Element

As stated in section 3.4.4.1.1.1.1, the <RequestType> element MUST be present and its value MUST equal http://schemas.xmlsoap.org/ws/2005/02/trust/Issue. If the element is missing or has a different value, the STS MUST return a SOAP fault.

3.6.4.1.1.1.2.2 <Claims> Element

The contents of this element describe the requested claims by claim type **URI**. The claims issued in the Security Token MUST be equal to or a superset of the requested claims. If the STS cannot issue one of the requested claim types for any reason, the STS SHOULD return a SOAP fault.<36>

<ClaimType> elements with values for the **Uri** attribute that are not valid URIs MUST be ignored.

3.6.4.1.1.1.2.3 <KeyType> Element

The <KeyType> element indicates the type of proof key that the client is requesting for the Security Token. The <KeyType> element MUST equal one of the following values:

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey

- http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey
- http://schemas.xmlsoap.org/ws/2005/02/trust/Bearer
- http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey

If any other value for the <KeyType> element is received, the STS MUST return a SOAP fault.

3.6.4.1.1.1.2.4 <KeySize> Element

If the key type requested is a symmetric key, the value of this element indicates the size of the requested symmetric key in bytes. If the key type requested is an asymmetric key, this indicates the size of the public key requested for the token. If the <UseKey> element is used, this value MUST reflect the size of the key found in <UseKey>. If no proof key is requested, this element MUST be ignored. If this element is missing for a symmetric key request, the STS SHOULD default to a value for key size.<37>

3.6.4.1.1.1.2.5 <UseKey> Element

This element contains the key that the client requests for the Security Token. If this element is missing for a symmetric key request, the STS SHOULD generate a key.<38>

3.6.4.1.1.1.2.6 <EncryptWith> Element

The <EncryptWith> element specifies an encryption algorithm that the key in the Security Token SHOULD support.<39>

3.6.4.1.1.1.2.7 <SignWith> Element

The <SignWith> element specifies a signature algorithm that the key in the Security Token SHOULD support.<40>

3.6.4.1.1.1.2.8 <EncryptionAlgorithm> Element

The <EncryptionAlgorithm> element specifies the symmetric encryption algorithm that SHOULD be used when encrypting the Security Token to the relying party.<41>

3.6.4.1.1.1.2.9 <CanonicalizationAlgorithm> Element

The <CanonicalizationAlgorithm> element specifies the XML canonicalization algorithm that SHOULD be used when signing the Security Token.<42>

3.6.4.1.1.1.2.10 <RequestDisplayToken> Element

If a <RequestDisplayToken> element is present in the request, then the STS SHOULD generate a <RequestDisplayToken> element for the response. The **lang** attribute SHOULD be used to localize the language specific descriptions in the <RequestDisplayToken> element.<43>

If the **lang** attribute is missing, the server MUST NOT fault.

3.6.4.1.1.1.2.11 <InformationCardReference> Element

The <InformationCardReference> element informs the STS of the identifier and version of the information card the client is using. The STS SHOULD use this information to change its issuance behavior.<44>

3.6.4.1.1.1.2.12 <ClientPseudonym> Element

The value <ClientPseudonym> element SHOULD be used by the STS in generating a pseudonym for the request.<45>

3.6.4.1.1.1.2.13 <OnBehalfOf> Element

The <OnBehalfOf> element SHOULD be used by the STS to generate claims for the issued token.<46>

3.6.4.1.1.1.2.14 <AppliesTo> Element

The <AppliesTo> element indicates to the STS the identity of the relying party. The STS SHOULD have issuance policy for relying parties such that it alters the claims issued based on the identity of the relying party. The STS SHOULD use the URL provided and/or the Security Token provided in the <Identity> element. If this element is missing, the STS SHOULD issue the Security Token without claims specific to a particular relying party.<47>

3.6.4.1.1.2 IWSTrust13Async_Trust13IssueAsync_OutputMessage and IWSTrustFeb2005Async_TrustFeb2005IssueAsync_OutputMessage

The following sections describe the processing rules for the SOAP header and body of the outgoing Token Acquisition response message.

3.6.4.1.1.2.1 SOAP Header Processing

The Token Acquisition response MUST be formatted as described by the requirements of the policy assertions that apply to the endpoint where the request message was sent. The formatting and message processing requirements of those policy assertions are described above in section 3.3.4.1.

The STS MUST set the value of the <RelatesTo> element to be equal to the value of the <MessageID> element used in the Token Acquisition request. If <SignatureConfirmation> is required by the endpoint policy, then the STS MUST copy each <SignatureValue> element from the Token Acquisition request into the corresponding <SignatureConfirmation> elements of the Token Acquisition response.

As described in the policy assertions above, one of the following mechanisms MUST be used to protect the message. The mechanism chosen will influence the content of the SOAP <Header> element.

3.6.4.1.1.2.1.1 Protection Using Transport Layer Security

If the policy assertion PA01 is present and applies to the endpoint being used for the Token Acquisition request message, then the STS MUST use TLS as described in [RFC2246] to protect the response message.

3.6.4.1.1.2.1.2 Protection Using Windows Authentication

If the policy assertion PA16 is present and applies to the endpoint used for the Token Acquisition request message, then the STS MUST use the existing SPNego context token from Windows authentication to protect the message from the STS. Thus the token obtained by the mechanism described in section 3.5.4 MUST be used to secure the response as indicated in section 3.5.4.

3.6.4.1.1.2.1.3 Protection Using the STS X509 Certificate

If the policy assertion PA12 is present and applies to the endpoint being used for the Token Acquisition request message (section 3.6.4.1.2.1.1), then the symmetric key used by the request MUST be used again by the Token Acquisition response (section 3.6.4.1.2.1.2). The symmetric key MUST be used for encrypting and signing the message parts required by PA25, PA57, and PA60. The <EncryptedKey> element from the request MUST be referred to in the response. If PA13 is present and applies to the endpoint, derived key tokens generated from the original symmetric key must be used for the encryption and signing.

3.6.4.1.1.2.2 SOAP Body Processing

The following sections describe the processing rules for the SOAP body of the outgoing Token Acquisition response message sectioned by the elements that may be present in the body.

3.6.4.1.1.2.2.1 <RequestedSecurityToken> Element

The content of this element is opaque to the protocol and need only be read by the relying party. It is therefore outside of the scope of this protocol.

The contents of the <RequestedSecurityToken> element SHOULD be encrypted for the relying party service if the STS has been configured with key material for the relying party. If this is the case, the emitted content will be an <EncryptedData> element as described in section 3.6.4.1.2.28.<48>

3.6.4.1.1.2.2.2 <Lifetime> Element

When a SAML 1.1 token is used, the value of the <Created> element MUST be equal to the value of the **NotBefore** attribute of the <Conditions> element in the SAML 1.1 token. The value of the <Expires> element MUST be equal to the value of the **NotOnOrAfter** attribute of the <Conditions> element in the SAML 1.1 token.

3.6.4.1.1.2.2.3 <RequestedDisplayToken> Element

If the Token Acquisition request contained a <RequestDisplayToken>, then the STS MUST include a <RequestDisplayToken> element in the Token Acquisition response message. The <DisplayToken> child element of <RequestDisplayToken> MUST contain a <DisplayClaim> element for every claim type returned in the Security Token. The **Uri** attribute of the <DisplayClaim> element is the URI of the claim type in the Security Token as specified in section 3. One <DisplayClaim> element MUST be emitted for each **<Attribute>** element in the Security Token.

3.6.4.1.1.2.2.4 <RequestedAttachedReference> Element

When a SAML 1.1 token is used, the value of the <KeyIdentifier> child element of the <SecurityTokenReference> element MUST be the same value as the **AssertionID** attribute of the SAML <Assertion> element.

3.6.4.1.1.2.2.5 <RequestedUnattachedReference> Element

When a SAML 1.1 token is used, the value of the <KeyIdentifier> child element of the <SecurityTokenReference> element MUST be the same value as the **AssertionID** attribute of the SAML <Assertion> element.

3.6.4.1.1.2.2.6 <TokenType> Element

The value of the <TokenType> element MUST equal the value urn:oasis:names:tc:SAML:1.0:assertion.

3.6.4.1.1.2.2.7 <KeyType> Element

The value of the <KeyType> element returned MUST be identical to the value of the <KeyType> element in the Token Acquisition request message.

3.6.4.1.1.2.2.8 <RequestedProofToken> Element

The <RequestedProofToken> element described in section 3.6.4.1.2.29 MUST be sent in the Token Acquisition response message if the <KeyType> element included in the request was equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey or http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey.

When the Token Acquisition request included a <KeyType> element equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey or http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey and included client entropy as described in section 3.6.4.1.2.6 and section 3, the STS MUST include a <ComputedKey> element conforming to [WSTrust1.3] section 4.4.3 within the <RequestedProofToken> element of the response message with a value of http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1 or http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1. The value of the <Entropy> element described below is used along with the value of the submitted entropy and the PSHA1 algorithm to construct the symmetric key proof token.

When the Token Acquisition request included a <KeyType> element equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey or http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey and no client entropy was included in the request, the STS MUST return the symmetric key in a <BinarySecret> child element as specified in [WSTrust1.3] section 3.3.

3.6.4.1.1.2.2.9 <Entropy> Element

When the Token Acquisition request included a <KeyType> element equal to http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey or http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey and <KeyType> included client entropy as described in section 3.6.4.1.2.6 and section 3, the STS MUST include an <Entropy> element specified in [WSTrust1.3] section 4.4. The <Entropy> element MUST contain a <BinarySecret> element specified in [WSTrust1.3] section 3.3. The value of the <BinarySecret> element is used along with the value of the client's submitted entropy and the PSHA1 algorithm to construct the symmetric key proof token.

3.6.4.1.1.2.2.10 <KeySize> Element

If a Token Acquisition request requires a proof key, a <KeySize> can be returned in the Token Acquisition response. If a <KeySize> is not specified in the request, then a <KeySize> MUST be included in the response. If a <KeySize> is specified in the request and the STS overrides the requested key size with a different value, then the new <KeySize> MUST be included in the response. If the <KeySize> is omitted from the response, then the requested key size is assumed. The <KeySize> element MUST NOT be present when a <RequestedProofToken> element is not returned.

3.6.4.1.2 Elements

The following table summarizes the XML Schema element definitions that are specific to this operation. Elements are included below if they are not specified in normative references, or if this protocol restricts the contents of the element. Elements that are fully specified in normative references and that are not restricted in this protocol are not detailed below.

Element	Description
Header	Specified in section 5.2 [SOAP1.2-1/2007]
Security	specified in section 5 of [WSS]
Body	Specified in section 5.3 [SOAP1.2-1/2007]
RequestSecurityToken	specified in sections 3 and 4 of [WSTrust1.3]
Timestamp	specified in section 10 of [WSS]
EncryptedKey	specified in section 2.2.2 of [XMLEnc]
DerivedKeyToken	specified in section 8 of [WSSC]
Signature	specified in section 4.0 of [XMLDSig/2002]
SecurityContextToken	specified in section 3 of the [WSSC]
BinarySecurityToken	specified in section 6.3 of [WSS]
UsernameToken	specified in section 6.2 of [WSS]
EncryptionMethod	specified in section 3.2 of [XMLEnc]
KeyIdentifier	specified in section 7.3 of [WSS]
SignedInfo	specified in section 4.3 of [XMLDSig/2002]
Reference	specified in section 4.3.3 of [XMLDSig/2002]
Assertion	specified in [SAMLCore] section 2.3.2
Conditions	specified in section 2.3.2.1.1 of [SAMLCore]
AttributeStatement	specified in section 2.4.4 of [SAMLCore]
Subject	specified in section 2.4.2.1 of [SAMLCore]
RequestDisplayToken	Defined below in section 3.6.4.1.2.20
InformationCardReference	Defined below in section 3.6.4.1.2.21
Claims	specified in section 3 of [WSTrust1.3]
ClaimType	Defined below in section 3.6.4.1.2.23
EndpointReference	specified in [WSA] section 2
ClientPseudonym	Defined below in section 3.6.4.1.2.25
RequestSecurityTokenResponse	specified in section 3 and 4 of WS-Trust [WSTrust1.3]

Element	Description
Lifetime	specified in sections 3.2 and 4.4 of [WSTrust1.3]
RequestedSecurityToken	specified in sections 3.2 and 4.4 of [WSTrust1.3]
RequestedProofToken	specified in section 4.4 of [WSTrust1.3]
RequestedDisplayToken	Defined below in section 3.6.4.1.2.30
DisplayToken	Defined below in section 3.6.4.1.2.31
DisplayClaim	Defined below in section 3.6.4.1.2.32

3.6.4.1.2.1 Header

The contents of the SOAP <Header> element are restricted based on whether they are contained in the request or the response, as detailed in the following sections.

3.6.4.1.2.1.1 Request Messages

The SOAP <Header> element MUST contain the following child elements:

- An <Action> element as specified in section 3.1 of [WSA] and section 4 of [WSTrust1.3]. This element MUST equal "http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue" or "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue". For further details on the <Action> element value, see sections 3.3.4.1 and 3.2.4.1.1.2.1.
- A <ReplyTo> element as specified in section 3.2 of [WSA]. This element MUST have a value of "http://www.w3.org/2005/08/addressing/anonymous".
- A <To> element as specified in 3.2 of [WSA].
- A <MessageID> element as specified in section 3.2 of [WSA].
- A <Security> element that MUST conform to section 3.6.4.1.2.2.1.

3.6.4.1.2.1.2 Response Messages

The SOAP <Header> element MUST contain the following child elements:

- An <Action> element that MUST conform to section 4 of [WSTrust1.3] and section 3.1 of [WSA]. This element MUST equal "http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue" or "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal". For further details on the <Action> element value, see sections 3.3.4.1 and 3.2.4.1.1.2.1.
- A <RelatesTo> element that MUST conform to section 3.1 of [WSA]. For further details on how the value of this element is determined, see section 3 of [WSA].
- A <Security> element that MUST conform to section 3.6.4.1.2.2.2.

3.6.4.1.2.2 Security

The contents of the <Security> element are restricted based on whether they are contained in the request or the response, as detailed in the following sections.

3.6.4.1.2.2.1 Request Messages

The <Security> element is specified in section 5 of [WSS]; for further details on how the format of this element is determined, see section 3.3.4.1. The <Security> element MAY contain the following child elements:

- A <Timestamp> element that MUST conform to section 3.6.4.1.2.5.
- An <EncryptedKey> element that MUST conform to section 3.6.4.1.2.6; for further details on how the presence of this element is determined, see sections 3.7.4.1.1.1.2 and 3.6.4.1.1.2.1.2.
- One or more <DerivedKeyToken> elements that MUST conform to section 3.6.4.1.2.7; for further details on how the cardinality of this element is determined, see section 3.3.4.1.
- A <ReferenceList> element as specified in sections 2.2.2 and 3.6 of [XMLEnc]; for further details on how the presence of this element is determined, see sections 3.3.4.1 and 3.3.4.2.
- One or more <EncryptedData> elements as specified in section 2.2 of [XMLEnc]; for further details on how the cardinality of this element is determined, see section 3.3.4.1.
- One or more <Signature> elements that MUST conform to section 3.6.4.1.2.8; for further details on how the cardinality of this element is determined, see section 3.7.4.1.1.1.
- A <SecurityContextToken> element that MUST conform to section 3.6.4.1.2.9.
- A <BinarySecurityToken> element that MUST conform to section 3.6.4.1.2.10.
- A <UsernameToken> element that MUST conform to section 3.6.4.1.2.11.

3.6.4.1.2.2.2 Response Messages

For further details on how the format of this element is determined, see section 3.2.4.1.1.2.1. The <Security> element can contain the following child elements:

- A <Timestamp> element that MUST conform to section 3.6.4.1.2.5.
- A <DerivedKeyToken Element> element that MUST conform to section 3.6.4.1.2.7.
- A <ReferenceList> element as specified in sections 2.2.2 and 3.6 of [XMLEnc]. For further details on how the presence of this element is determined, see sections 3.2.4.1.1.2.1 and 3.2.4.1.1.2.2.
- One or more <EncryptedData> elements as specified in section 2.2 of [XMLEnc]. For further details on how the cardinality of this element is determined, see section 3.2.4.1.1.2.1.
- One Signature element that MUST conform to section 3.6.4.1.2.8.
- One or more <SignatureConfirmation> elements as specified in section 8.5 of [WSS]; for further details on how the cardinality of this element is determined, see section 3.2.4.1.1.2.1.

3.6.4.1.2.3 Body

The contents of the SOAP <Body> element are restricted based on whether they are contained in the request or the response, as detailed in the following sections.

3.6.4.1.2.3.1 Request Messages

The SOAP <Body> element MUST contain only one of the following elements; for further details on how the format of the SOAP <Body> element is determined, see section 3.2.4.1.1.2.2:

- An <EncryptedData> element as specified in section 2.2 of XML Encryption Syntax and Processing [XMLEnc].
- A <RequestSecurityToken> element that MUST conform to section 3.6.4.1.2.4.

3.6.4.1.2.3.2 Response Messages

The SOAP <Body> element MUST contain one of the following elements:

- An <EncryptedData> element that MUST conform to section 2.2 of [XMLEnc].
- A <RequestSecurityTokenResponse> element that MUST conform to section 3.6.4.1.2.26.
- A <RequestSecurityTokenResponseCollection> element containing a <RequestSecurityTokenResponse> that MUST conform to section 3.6.4.1.2.26.

3.6.4.1.2.4 RequestSecurityToken

The <RequestSecurityToken> element is specified in sections 3 and 4 of [WSTrust1.3]. The XML namespace of the WS-Trust elements used by this protocol MUST be either "http://schemas.xmlsoap.org/ws/2005/02/trust" or "http://docs.oasis-open.org/ws-sx/ws-trust/200512". For further details on protocol behavior for namespaces, see sections 3.3.4.1 and 3.2.4.1.1.2.1. The <RequestSecurityToken> element SHOULD contain the following child elements:

- A <RequestType> element that MUST conform to section 4.1 of [WSTrust1.3], and MUST have a value equal to http://schemas.xmlsoap.org/ws/2005/02/trust/Issue or http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue.
- An <AppliesTo> element that MUST contain the <EndpointReference> element that MUST conform to section 3.6.4.1.2.24. For further details on how the presence and value of this element is determined, see section 3.7.4.1.2.1.1.

The <RequestSecurityToken> element can contain the following child elements:

- A <KeyType> element that MUST conform to section 9.2 of [WSTrust1.3]. For further details on how the value of this element is determined, see sections 3.7.4.1.2.2, 3.7.4.1.2.3, and 3.7.4.1.2.4. This element MUST equal one of the following values:
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey
  - http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey
  - http://schemas.xmlsoap.org/ws/2005/02/trust/Bearer
  - http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey
- A <KeySize> element that MUST conform to section 9.2 of [WSTrust1.3]; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.3.4.

- An <EncryptWith> element that MUST conform to section 9.2 of [WSTrust1.3]; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.3.1.
- A <SignWith> element that MUST conform to section 9.2 of [WSTrust1.3]; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.3.2.
- An <EncryptionAlgorithm> element that MUST conform to section 9.2 of [WSTrust1.3]; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.1.2.
- A <CanonicalizationAlgorithm> element that MUST conform to section 9.2 of [WSTrust1.3]; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.1.5.
- An <Entropy> element that MUST conform to section 4.4.3 of [WSTrust1.3]; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.3.3.
- An <Entropy> element that MUST conform to section 4.4.3 of [WSTrust1.3]; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.3.3.
- A <UseKey> element that MUST conform to section 9.2 of [WSTrust1.3]; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.2.3.
- A Claims element MUST conform to section 3.6.4.1.2.22; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.1.6.
- An <InformationCardReference> element that MUST conform to section 3.6.4.1.2.21; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.1.3.
- A <RequestDisplayToken> element that MUST conform to section 3.6.4.1.2.20; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.1.4.
- A ClientPseudonym element that MUST conform to section 3.6.4.1.2.25; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.1.7.
- An <OnBehalfOf> element that MUST conform to section 9.1 of [WSTrust1.3]; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.1.8.

3.6.4.1.2.5 Timestamp

The <Timestamp> element is specified in section 10 of [WSS]. The element MUST contain the following child elements:

- The <Created> element.
- The <Expires> element.

3.6.4.1.2.6 EncryptedKey

The <EncryptedKey> element is specified in section 2.2.2 of [XMLEnc]. This element MUST contain the following child elements:

- An <EncryptionMethod> element MUST conform to section 3.6.4.1.2.12.
- A <KeyInfo> element as specified in section 4.4 of [XMLDSig/2002]. The element MUST contain a <SecurityTokenReference> element specified in section 7 of [WSS]. The

<SecurityTokenReference> element MUST contain a single <KeyIdentifier> element that MUST conform to section 3.6.4.1.2.13.

For further details on how the presence of this element is determined, see Protection Using Message Level X509 Certificate (section 3.7.4.1.1.1.3) and Protection Using the STS X509 Certificate (section 3.6.4.1.1.2.1.3).

3.6.4.1.2.7 DerivedKeyToken

The <DerivedKeyToken> element is specified in section 8 of WS-SecureConversation [WSSC]. The element MUST contain the following child elements:

- A <SecurityTokenReference> element as specified in section 7 of [WSS]. The element MUST contain a <Reference> child element specified in section 7.2 of [WSS] or a <KeyIdentifier> child element specified in section 7.3 of [WSS].
- A <Nonce> element that MUST conform to section 8 of [WSSC].

3.6.4.1.2.8 Signature

The <Signature> element is specified in section 4.0 of [XMLDSig/2002]. Each <Signature> element MUST contain the following child elements:

- A <SignedInfo> element that MUST conform to section SignedInfo Element.
- A <SignatureValue> element as specified in section 4.2 of [XMLDSig/2002].
- A <KeyInfo> element as specified in section 4.4 of [XMLDSig/2002].

3.6.4.1.2.9 SecurityContextToken

The <SecurityContextToken> element is specified in section 3 of the [WSSC]; for further details on how the presence of this element is determined, see section 3.3.4.1.

3.6.4.1.2.10 BinarySecurityToken

The <BinarySecurityToken> element is specified in section 6.3 of [WSS]; for further details on how the presence of this element is determined, see section 3.3.4.1.

3.6.4.1.2.11 UsernameToken

The <UsernameToken> element is specified in section 6.2 of [WSS]; for further details on how the presence of this element is determined, see section 3.3.4.1.

3.6.4.1.2.12 EncryptionMethod

The <EncryptionMethod> element is specified in section 3.2 of [XMLEnc]. For further details on how the value of the element's **Algorithm** attribute is determined, see section 3.3.4.1. The <EncryptionMethod> element SHOULD contain a <DigestMethod> element. For further details on how the value of the <DigestMethod> element's **Algorithm** attribute is determined, see section 3.3.4.1. If the <DigestMethod> element is not present, its value is assumed to be "http://www.w3.org/2000/09/xmldsig#sha1".

3.6.4.1.2.13 KeyIdentifier

The <KeyIdentifier> element is specified in section 7.3 of [WSS]. This element SHOULD contain following attributes:

- A **ValueType** attribute that MUST equal a URI that conforms to [RFC3986]. This value MUST be equal to "http://docs.oasisopen.org/wss/oasiswss-soap-messagesecurity-1.1#ThumbPrintSHA1".
- An **EncodingType** attribute that MUST equal a URI that conforms to [RFC3986]. This value MUST be equal to "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary".

If the **EncodingType** attribute is not present, its value is assumed to be "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary".

3.6.4.1.2.14 SignedInfo

The <SignedInfo> element is specified in section 4.3 of [XMLDSig/2002]. For further details on how the value of the Algorithm attribute of the <SignatureMethod>, which is a child element of the <SignedInfo>element, is determined, see section 3.3.4.1. Each <Reference> child element MUST conform to section 3.6.4.1.2.15.

3.6.4.1.2.15 Reference

The <Reference> element is specified in section 4.3.3 of [XMLDSig/2002]; for further details on how the cardinality of this element is determined, see section 3.3.4.2. The **Algorithm** attribute of the <Transforms> element MUST equal "http://www.w3.org/2001/10/xml-exc-c14n#".

The <Reference> element MUST contain the <Transforms> element specified in section 4.3.3.4 of [XMLDSig/2002]. For further details on how the presence of the <Transforms> element is determined, see section 3.3.4.1.

3.6.4.1.2.16 Assertion

The <Assertion> element is specified in [SAMLCore] section 2.3.2. The <Assertion> element's attributes MajorVersion and MinorVersion MUST equal 1.

The <Assertion> element MUST contain the <Conditions> element that MUST conform to section 3.6.4.1.2.17. The <Assertion> element MUST contain the <Signature> element. The Signature child element MUST conform to section 3.6.4.1.2.8. The <Assertion> element MAY contain an <AttributeStatement> element that MUST conform to section 3.6.4.1.2.18.

3.6.4.1.2.17 Conditions

The <Conditions> element is specified in section 2.3.2.1.1 of [SAMLCore].

The <Conditions> element MUST contain the NotBefore and NotOnOrAfter attributes; these attributes MUST conform to [SAMLCore] section 2.3.2.1.1.

The <Conditions> element MUST contain an <AudienceRestrictionCondition> element specified in section 2.3.2.1.3 of [SAMLCore]. The <AudienceRestrictionCondition> element MUST contain only one <Audience> element specified in section 2.3.2.1.3 [SAMLCore].

3.6.4.1.2.18 AttributeStatement

The <AttributeStatement> element is specified in section 2.4.4 of [SAMLCore].

The <AttributeStatement> element MUST contain the following child elements:

- The <Subject> element that MUST conform to section 3.6.4.1.2.19.
- The <Attribute> element as specified in section 2.4.4.1 of [SAMLCore]; for further details on how the cardinality and format of this element is determined, see section 3. The <Attribute> element MUST contain an <AttributeValue> element.

3.6.4.1.2.19 Subject

The <Subject> element is specified in section 2.4.2.1 of [SAMLCore]. This element MUST contain the <SubjectConfirmation> element specified in section 2.4.2.3 of [SAMLCore]. The <SubjectConfirmation> element MUST contain the following child elements:

- A <ConfirmationMethod> element that MUST equal a URI that conforms to [RFC3986]. The value of the element MUST be either urn:oasis:names:tc:SAML:1.0:cm:bearer or urn:oasis:names:tc:SAML:1.0:cm:holder-of-key.
- The <SubjectConfirmation> element MAY contain a <KeyInfo> element specified in section 4.4 of [XMLDSig/2002]; for further details on how the format of this element is determined, see section 3.

3.6.4.1.2.20 RequestDisplayToken

The <RequestDisplayToken> element MUST belong to the http://schemas.xmlsoap.org/ws/2005/05/identity namespace; this element MUST contain a lang attribute that MUST conform to [XMLSCHEMA2]; for further details on how the value of the lang attribute is determined, see section 3.7.4.1.2.1.4.

3.6.4.1.2.21 InformationCardReference

The <InformationCardReference> element and its child elements MUST belong to the http://schemas.xmlsoap.org/ws/2005/05/identity namespace and MUST contain the following child element:

- The <CardId> element. This element MUST equal a URI that conforms to [RFC3986]; for further details on how the value of this element is determined, see section 3.7.4.1.2.1.3.

The <InformationCardReference> element MAY contain the following child element:

- The <CardVersion> element. This element MUST equal an unsigned integer; for further details on how the presence and value of this element is determined, see section 3.7.4.1.2.1.3.

3.6.4.1.2.22 Claims

The <Claims> element is specified in section 3 of [WSTrust1.3] and MAY contain one or more <ClaimType> child elements; for further details on how the cardinality of the <ClaimType> element is determined, see section 3.7.4.1.2.1.6. The <ClaimType> element MUST conform to section 3.6.4.1.2.23. A Dialect attribute MAY be present. If present, the Dialect attribute MUST NOT equal http://schemas.xmlsoap.org/ws/2006/12/authorization/authclaims.<49>

3.6.4.1.2.23 ClaimType

The <ClaimType> element MUST belong to the http://schemas.xmlsoap.org/ws/2005/05/identity namespace. This element MUST contain the Uri attribute that MUST equal a URI as conforming to

[RFC3986]; for further details on how the value of the Uri attribute is determined, see section 3.7.4.1.2.1.6.

3.6.4.1.2.24 EndpointReference

The <EndpointReference> element is specified in [WSA] section 2 and MAY contain an <Identity> element specified in [WSAIdentity] section 2. The <Identity> element MUST contain a <KeyInfo> element specified in [XMLDSig/2002] section 4.4, or a <Dns> element specified in [WSAIdentity] section 3.1, or a <Spn> element specified in [WSAIdentity] section 3.2, or a Upn element specified in [WSAIdentity] section 3.3.

3.6.4.1.2.25 ClientPseudonym

The <ClientPseudonym> element and its child element MUST belong to the http://schemas.xmlsoap.org/ws/2005/05/identity namespace and this element MUST contain the child element <PPID>. The <PPID> element MUST equal a **base64** binary value.

3.6.4.1.2.26 RequestSecurityTokenResponse

The <RequestSecurityTokenResponse> element is specified in section 3 and 4 of WS-Trust [WSTrust1.3]. The XML namespace of the WS-Trust elements used by this protocol MUST be either "http://schemas.xmlsoap.org/ws/2005/02/trust" or "http://docs.oasis-open.org/ws-sx/ws-trust/200512". For further details on protocol behavior for namespaces, see sections 3.3.4.1 and 3.2.4.1.1.2.1. The <RequestSecurityTokenResponse> element MAY contain the following child elements:

- A <RequestType> element as specified in section 4.4 of [WSTrust1.3]. This element MUST have a value equal to http://schemas.xmlsoap.org/ws/2005/02/trust/Issue or http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue.
- A <RequestedSecurityToken> element element that MUST conform to section 3.6.4.1.2.28.
- A <KeyType> element as specified in section 9.2 of [WSTrust1.3]. For further details on how the value of this element is determined, see section 3.6.4.1.1.2.2.7. The <KeyType> element MUST equal one of the following values:
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey
  - http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey
  - http://schemas.xmlsoap.org/ws/2005/02/trust/Bearer
  - http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey
- A <Lifetime> element that MUST conform to the section 3.6.4.1.2.27.
- A <RequestedAttachedReference> element as specified in section 4.4.2 of the WS-Trust [WSTrust1.3].
- A <RequestedUnattachedReference> element as specified in section 4.4.2 of the WS-Trust [WSTrust1.3].
- A <TokenType> element as specified in section 4.4 of [WSTrust1.3].

- A <RequestedProofToken> element that MUST conform to section 3.6.4.1.2.29; for further details on how the presence of this element is determined, see section 3.6.4.1.1.2.2.8.
- A <RequestedDisplayToken> element that MUST conform to section 3.6.4.1.2.30; for further details on how the presence and value of this element is determined, see section 3.6.4.1.1.2.2.3.
- A <KeySize> element as specified in section 9.2 of [WSTrust1.3]; for further details on how the value of this element is determined, see section 3.6.4.1.1.2.2.9.
- A <Entropy> element as specified in section 4.4.3 of [WSTrust1.3]; for further details on how the presence and value of this element is determined, see section 3.6.4.1.1.2.2.9.

3.6.4.1.2.27 Lifetime

The <Lifetime> element is specified in sections 3.2 and 4.4 of [WSTrust1.3]. This element MUST contain the following child elements:

- The <Created> element
- The <Expires> element

3.6.4.1.2.28 RequestedSecurityToken

The <RequestedSecurityToken> element is specified in sections 3.2 and 4.4 of [WSTrust1.3]. For further details on how the format of this element is determined, see sections 3.7.4.2.2.1 and 3.6.4.1.1.2.2.1. The content of this element is not required to be understood by the client.

3.6.4.1.2.29 RequestedProofToken

The <RequestedProofToken> element is specified in section 4.4 of [WSTrust1.3]; either this element or the <RequestedSecurityToken> element MUST be present. For further details on how the format of this element is determined, see section 3.6.4.1.1.2.2.8.

3.6.4.1.2.30 RequestedDisplayToken

The <RequestedDisplayToken> element MUST belong to http://schemas.xmlsoap.org/ws/2005/05/identity. This element MUST contain the <DisplayToken> element that MUST conform to 3.6.4.1.2.31.

3.6.4.1.2.31 DisplayToken

The <DisplayToken> element MUST belong to http://schemas.xmlsoap.org/ws/2005/05/identity. This element MUST contain at least one <DisplayClaim> element; for further details on the cardinality of the <DisplayClaim> element, see section 3.6.4.1.1.2.2.3. The <DisplayClaim> element MUST conform to section 3.6.4.1.2.32.

3.6.4.1.2.32 DisplayClaim

The <DisplayClaim> element and its child elements MUST belong to http://schemas.xmlsoap.org/ws/2005/05/identity namespace. The <DisplayClaim> element MUST contain the Uri attribute that MUST equal a URI that conforms to [RFC3986]; for further details on how the value of this attribute is determined, see section 3.6.4.1.1.2.2.3:

The <DisplayClaim> element SHOULD contain the following child elements; for further details on how the format of the <DisplayClaim> element is formatted, see section 3.6.4.1.1.2.2.3:

- The <DisplayTag> element MUST equal string conforming to [XMLSCHEMA2] section 3.2.1.
- The <Description> element MUST equal string conforming to [XMLSCHEMA2] section 3.2.1.
- The <DisplayValue> element MUST equal string conforming to [XMLSCHEMA2] section 3.2.1.

3.6.4.1.3 Complex Types

There is no XML Schema defined to specify the schema types that govern the XML elements of the protocol beyond the XML schemas that are defined by existing normative documents. Those normative documents are referenced in the Elements section above.

3.6.4.1.4 Simple Types

There is no XML Schema defined to specify the schema types that govern the XML elements of the protocol beyond the XML schemas that are defined by existing normative documents. Those normative documents are referenced in the Elements section above.

3.6.4.1.5 Attributes

The following table summarizes the XML Schema attribute definitions that are specific to this operation. Attributes are included below if they are not specified in normative references.

Attribute	Description
Uri	Used on ClaimType elements to specify the identifier of the claim type.

3.6.4.1.5.1 Uri

The Uri attribute MUST belong to the http://schemas.xmlsoap.org/ws/2005/05/identity namespace. The Uri attribute that MUST equal a URI as conforming to [RFC3986]; for further details on how the value of the Uri attribute is determined, see section 3.7.4.1.2.1.6.

3.6.5 Timer Events

There are no protocol-specific timer events that are serviced by an implementation. This protocol does not require timers except those that may be used by the underlying transport to transmit and receive messages over HTTP. The protocol does not include provisions for time-based retry for sending protocol messages.

The security tokens that are transported in protocol messages have a specific time interval during which they are considered to be valid. The STS that issues the Security Tokens MUST set the time interval by using the **NotBefore** and **NotOnOrAfter** attributes of the <Conditions> (section 3.6.4.1.2.17) element. For more details, see [SAMLCore] section 2.3.2.1.1.

Implementations can use a timer to indicate when the validity interval of a security token or an Authentication Context expires; however, the protocol does not require the use of a timer. Timers are not used to determine when validity intervals expire. The **NotBefore** and **NotOnOrAfter** values that are obtained from security tokens MUST be explicitly checked.

3.6.6 Other Local Events

This protocol does not have dependencies on any transport protocols other than HTTP 1.1. This protocol relies on this transport mechanism for the correct and timely delivery of protocol messages.

The protocol does not take action in response to any changes or failure in machine state or network communications.

3.7 Token Acquisition Client Details

This port type uses the protocol defined in [WSTrust1.3] to send/receive a security token. The protocol uses port types IWSTrustFeb2005Async and IWSTrust13Async for Token Acquisition. The port types implement substantially the same protocol, and so are documented in a single section. Differences are called out inline.

3.7.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

Client Language: For displaying human readable text to its users, the client role implementation may maintain the preferred language of the user. This language may be obtained from the operating system on which the client is deployed.

STS Token Acquisition Endpoint: See definition in section 3.3.1 above.

Requested Claim Types: The client may request particular claim types using the message syntax for Claims Element (section 3.6.4.1.2.22). This data is a set of URIs and is often supplied by the RP.

Requested Key Type: The client may request a particular key type using the message syntax for <KeyType> described in section 3.6.4.1.2.4. This data is a URI and is often supplied by the RP.

Relying Party URI: The client may request that the token be targeted for an RP identified by a URI using the message syntax for <AppliesTo> described in section 3.6.4.1.2.4.

Relying Party X509 Certificate: The client may request that the token be targeted for an RP identified by an X.509 certificate using the message syntax for <AppliesTo> described in section 3.6.4.1.2.4.

ClientPA: This element is an array of Boolean values to track whether the client received particular policy assertions in the Service Metadata Exchange response from the STS. The index to the array represents the assertion number, and the array is initialized to false.

X.509 Session Key: When clients authenticate with an X.509 certificate, a symmetric session key is used in the Token Acquisition request, as described in section 3.7.4.1.1.1.3. This value is used in processing the response as well, so it must be preserved. This value is a 256-bit binary value used as a symmetric key.

Information Card Identifier: Clients may have an information card as described in [IMI] that corresponds to the STS. The identifier of the information card may be used in token acquisition requests as described by section 3.6.4.1.2.21 and 3.7.4.1.2.1.3.

Information Card Version: Clients may have an information card as described in [IMI] that corresponds to the STS. The version of the information card may be used in token acquisition requests as described by section 3.6.4.1.2.21 and 3.7.4.1.2.1.3.

3.7.2 Timers

Clients SHOULD fault if a Token Acquisition Response Message (section 3.6.4.1.2.1.2) is not received within 1 minute after a Token Acquisition Request Message (section 3.6.4.1.2.1.1) is issued to the server role.

There are no other protocol-specific timer events that are serviced by an implementation. The protocol does not include provisions for time-based retry for sending protocol messages.

3.7.3 Initialization

The client MUST maintain a language selection for use when requesting display tokens from the STS that will be displayed to users, as described in section 3.7.4.1.2.1.4.

Before sending any protocol messages, the client MUST have the following information to be used when requesting the security token from the Security Token Service (STS). How this information is obtained is outside the scope of the protocol.

- The URI of the relying party to whom the security token will be given.
- The X.509 certificate of the relying party to whom the security token will be given.
- The URIs of all of the claim types requested by the relying party.
- The key type requested by the relying party.

Section 3.1.1.2 describes the abstract interface for how these values may be provided to the client role implementation.

3.7.4 Message Processing Events and Sequencing Rules

The Token Acquisition messages conform to the protocol behavior for the "issue" request type that is specified in [WSTrust1.3] section 4.1.

3.7.4.1 Processing Request Messages

The following sections describe the processing rules for the SOAP header and body of the outgoing Token Acquisition request message.

3.7.4.1.1 SOAP Header Processing

The Token Acquisition request MUST be formatted as described by the requirements of the policy assertions obtained from the WSDL Metadata of a Service Metadata Exchange response message that are applicable to the chosen endpoint. The formatting and message processing requirements of those policy assertions are described above in section 3.3.4.1.

3.7.4.1.1.1 Protecting the Message

As described in the policy assertions above, one of the following mechanisms MUST be used to protect the message. The mechanism chosen will influence the content of the SOAP <Header> element.

3.7.4.1.1.1.1 Protection Using Transport Layer Security

If the policy assertion PA01 is present and applies to the endpoint being used for the Token Acquisition request message, then the client MUST use TLS as described in [RFC2246] to protect the request message.

3.7.4.1.1.1.2 Protection Using Message Level Windows Authentication

If the policy assertion PA16 is present and applies to the endpoint being used for the Token Acquisition request message, then the client MUST use Microsoft Windows® authentication to protect the message to the Security Token Service (STS). In this case, the SecurityContextToken MUST be obtained by the mechanism described in section 3.5.4 and used in the Token Acquisition message as indicated in section 3.5.4. The message protection signature and the message encryption must be performed with the key obtained from mechanism described in section 3.5.4.

3.7.4.1.1.1.3 Protection Using Message Level X.509 Certificate

If the policy assertion PA12 is present and applies to the endpoint being used for the Token Acquisition request message, then the client MUST generate a symmetric key, use that symmetric key for encrypting and signing the message parts required by PA24, PA58, and PA61, and encrypt that symmetric key using the X.509 certificate of the Security Token Service (STS). The ADM element for the symmetric key is described in section 3.7.1. The X.509 certificate of the STS is obtained from the Service Metadata Exchange response in the <Identity> element described in section 3.2.4.1.2.3. If PA13 is present and applies to the endpoint, derived key tokens generated from the generated symmetric key must be used for the encryption and signing.

3.7.4.1.1.2 Proving the User Identity

As described in the policy assertions above, one of the following mechanisms MUST be used to prove the user's identity to the Security Token Service (STS).

3.7.4.1.1.2.1 Proving the User Identity Using Windows Authentication

If the policy assertions PA16 or PA30 are present and apply to the endpoint being used for the Token Acquisition request message, then the client MUST use Microsoft Windows® authentication to prove the identity of the user to the Security Token Service (STS). In this case the SecurityContextToken MUST be obtained by the mechanism described in section 3.5.4 and used in the Token Acquisition message as indicated in section 3.5.4.

3.7.4.1.1.2.2 Proving the User Identity Using Kerberos

If the policy assertion PA33 is present and applies to the endpoint being used for the Token Acquisition request message, then the client MUST use Kerberos to prove the identity of the user to the Security Token Service (STS). The client MUST sign the message with the symmetric key from a Kerberos ticket, as described in [WSSKerb] section 3.4.

3.7.4.1.1.2.3 Proving the User Identity Using X.509 Certificates

If the policy assertion PA27 is present and applies to the endpoint being used for the Token Acquisition request message, then the client MUST use X.509 certificate authentication to prove the identity of the user to the Security Token Service (STS). The client MUST sign the existing message signature with the private key of the X.509 certificate in order to prove the identity of the user to the STS.

3.7.4.1.1.2.4 Proving the User Identity Using Username and Password

If the policy assertion PA40 is present and applies to the endpoint being used for the Token Acquisition Request Message (section 3.6.4.1.2.1.1), then the client MUST use username and password authentication to prove the identity of the user to the Security Token Service (STS). The client MUST include both the username and the password in the message in order to prove the identity of the user to the STS.

3.7.4.1.1.2.5 Proving the User Identity Using an Issued Token

If the policy assertion PA5 is present and applies to the endpoint being used for the Token Acquisition request message, then the client MUST use issued token authentication to prove the identity of the user to the Security Token Service (STS) If a symmetric key issued token is requested by policy assertion PA33, then the client MUST sign the message with the symmetric key to prove the identity of the user to the STS. If an asymmetric key issued token is requested by policy assertion PA35, then the client MUST sign the message with the private key to prove the identity of the user to the STS.

3.7.4.1.1.3 Number of <Signature> Elements Generated

There are three possible Signature elements that may be generated:

- A Signature element for message protection.
- A <Signature> element to prove the user's identity.
- A <Signature> element to prove private key possession when requesting an asymmetric key token.

If PA01 is in effect, no <Signature> element for message protection is generated. If PA58 is in effect, a <Signature> element for message protection MUST be present.

If PA27 or PA33 are in effect, there MUST be a <Signature> element for the client to prove possession of the private key corresponding to the provided Security Token (**SAML** or X.509) and thus prove the user's identity.

Finally, if the client is requesting an asymmetric key and using the UseKey element, there MUST be one more <Signature> element for the client to prove possession of the private key corresponding to the public key in the UseKey element.

If PA24 applies to the endpoint being used, each <Signature> element MUST be encrypted in an <EncryptedData> element.

3.7.4.1.2 SOAP Body Processing

The following sections describe the processing rules for the SOAP body of the outgoing Token Acquisition request message, arranged by the elements that are present in the body.

3.7.4.1.2.1 Elements Included Regardless of Requested Key Type

The inclusion of the following elements in the request is not determined by the key type being requested.

3.7.4.1.2.1.1 <AppliesTo> Element

As described in section 3.6.4.1.2.4, the <AppliesTo> element SHOULD be present in the RequestSecurityToken element. The EndpointReference (section 3.6.4.1.2.24) element contained within the <AppliesTo> element MUST contain the prerequisite items 1 and 2 described in section 3.7.3. The **Relying Party URI** MUST be contained within the <Address> element. The **Relying Party X509 Certificate** MUST be contained within the <Identity> element specified in 3.6.4.1.2.24.<50>

3.7.4.1.2.1.2 <EncryptionAlgorithm> Element

The <EncryptionAlgorithm> element SHOULD be included to indicate the symmetric key algorithm to use when encrypting the Security Token to the relying party.<51>

3.7.4.1.2.1.3 <InformationCardReference> Element

The <InformationCardReference> element SHOULD be included to indicate the identifier and version of the information about the Security Token Service (STS) stored in an information card as described above in section 3.3.3.<52>

3.7.4.1.2.1.4 <RequestDisplayToken> Element

The <RequestDisplayToken> element SHOULD be included to indicate that a display token is requested by the client.<53>

3.7.4.1.2.1.5 <CanonicalizationAlgorithm> Element

The <CanonicalizationAlgorithm> element SHOULD be included to indicate the canonicalization algorithm to use when signing the Security Token to be issued.<54>

3.7.4.1.2.1.6 <Claims> Element

The <Claims> element SHOULD be included to indicate the claims requested by the client from the Security Token Service (STS). Each requested claim type MUST be identified by a URI.<55>

3.7.4.1.2.1.7 <ClientPseudonym> Element

The client SHOULD include a <ClientPseudonym> element that conforms to section 3.6.4.1.2.25.<56>

3.7.4.1.2.1.8 <OnBehalfOf> Element

The client SHOULD include an <OnBehalfOf> element that conforms to [WSTrust1.3] section 9.1.<57>

3.7.4.1.2.2 Elements Included for Public Key Type

When requesting a SAML token with a public key, the value of the <KeyType> element MUST equal http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey or http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey

3.7.4.1.2.2.1 <EncryptWith> Element

The <EncryptWith> element SHOULD be included to indicate the key wrap algorithm supported by the key to be included in the Security Token by the Security Token Service (STS).<58>

3.7.4.1.2.2.2 <SignWith> Element

The <SignWith> element SHOULD be included to indicate the signature algorithm supported by the key to be included in the Security Token by the Security Token Service (STS).<59>

3.7.4.1.2.2.3 <UseKey> Element

The <UseKey> element SHOULD be included to specify the key to be used in the Security Token.<60>

3.7.4.1.2.2.4 <KeySize> Element

The <KeySize> element SHOULD be included to specify the size of the asymmetric key included in the <UseKey> element.<61>

3.7.4.1.2.3 Elements Included for Symmetric Key Type

When requesting a SAML token with a symmetric key, the value of the <KeyType> element MUST equal one of the following values:

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey
- http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey

3.7.4.1.2.3.1 <EncryptWith> Element

The <EncryptWith> element MUST be included to indicate the encryption algorithm supported by the key to be included in the Security Token by the Security Token Service (STS).

The following URI is used to indicate the encryption algorithm that is supported by the symmetric key: http://www.w3.org/2001/04/xmlenc#aes256-cbc (as specified in [XMLEnc] section 5.2.2).

3.7.4.1.2.3.2 <SignWith> Element

The <SignWith> element MUST be included to indicate the signature algorithm supported by the key to be included in the Security Token by the Security Token Service (STS).

When requesting a Security Token with a symmetric key, the following URI is used to indicate the signature algorithm that is supported by the symmetric key:
http://www.w3.org/2000/09/xmldsig#hmac-sha1 (as specified in [XMLDSig/2002] section 6.3.1).

3.7.4.1.2.3.3 <Entropy> Element

The <Entropy> element MUST be included to assist in calculating a symmetric key at the Security Token Service (STS).

The <Entropy> element contains only a <BinarySecret> element conforming to [WSTrust1.3] section 2.2 that contains a 256-bit cryptographically random number.

3.7.4.1.2.3.4 <KeySize> Element

The <KeySize> element MUST be included to specify the desired symmetric key size. If no pre-existing configuration for <KeySize> is available, the <KeySize> element is emitted with a default value of 256.

3.7.4.1.2.4 Elements Included for Bearer Token Request

If a SAML token with no key material is being requested, the possible values for the <KeyType> element are as follows:

- http://schemas.xmlsoap.org/ws/2005/05/identity/NoProofKey. This value MUST be used if the policy assertion PA48 is present and applies to the **endpoint** being used for the Token Acquisition request message.
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer. This value MUST be used if the policy assertion PA52 is present and applies to the endpoint being used for the Token Acquisition request message.

3.7.4.2 Processing Response Messages

The following sections describe the processing rules for the SOAP header and body of the incoming Token Acquisition response message.

3.7.4.2.1 SOAP Header Processing

The first processing step on receipt of a response message MUST be to verify the protection of the response message. To verify the protection of the message, the following actions MUST be taken:

- If PA61 is in effect, the client MUST successfully decrypt the message to remove any confidentiality protections.
- If PA58 is in effect, the client MUST successfully check the integrity of the message protection mechanisms to ensure the message has not been altered in transit.
- If PA01 is not in effect, the client MUST verify that the identity of the STS that sent the message is the expected identity. To verify that the identity of the STS is the expected identity, the client MUST use the symmetric key generated for the request or the SPNego context token and evaluate the proof of possession that the STS provided in the SOAP header <Signature> element described in 3.6.4.1.2.8. If PA01 is in effect, the identity of the STS is verified by the underlying TLS channel as described in [RFC2246].

The client MUST also verify that the value of the <RelatesTo> element is equal to the value of the <MessageID> element used in the Token Acquisition request.

3.7.4.2.2 SOAP Body Processing

The following sections describe the processing rules for the SOAP body of the incoming Token Acquisition response message sectioned by the elements that are present in the body.

3.7.4.2.2.1 <RequestedSecurityToken> Element

The <RequestedSecurityToken> element described in section 3.6.4.1.2.28 contains the Security Token that was requested by the Token Acquisition request message. The Security Token MUST be considered opaque to the client, and the client MUST NOT perform any action specific to the contents of the <RequestedSecurityToken> element.

3.7.4.2.2.2 <RequestedProofToken> Element

The <RequestedProofToken> element described in section 3.6.4.1.2.29 MUST be present in the response message if the <KeyType> element included in the request was equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey or http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey.

When the Token Acquisition request included a <KeyType> element equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey or http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey and included client entropy as described in section 3.6.4.1.2.6 and section 3.7.4.1.2.3.3, the <RequestedProofToken> element MUST only contain a <ComputedKey> element conforming to [WSTrust1.3] section 2.2 with a value of http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1 or http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1. In addition to the <ComputedKey> element, an <Entropy> element conforming to [WSTrust1.3] section 2.2 should be present in the <RequestSecurityTokenResponse> element. The <Entropy> element MUST contain a <BinarySecret> element conforming to [WSTrust1.3] section 3.3. The value of the <BinarySecret> element is used along with the value of the submitted entropy and the PSHA1 algorithm to construct the symmetric key proof token.

When the Token Acquisition request included a <KeyType> element equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey or http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey and no client entropy was included in the request, a <BinarySecret> child element as specified in [WSTrust1.3] section 3.3 MUST be present containing the symmetric key.

3.7.4.2.2.3 <RequestedDisplayToken> Element

If present, the <RequestedDisplayToken> element described in section 3.6.4.1.2.30 SHOULD be used to inform the user of the claim types and values issued by the STS. If the <RequestDisplayToken> (section 3.6.4.1.2.20) element was included in the WS-Trust request, the response MUST contain the <RequestedDisplayToken> element.<62>

3.7.5 Timer Events

There are no protocol-specific timer events that are serviced by an implementation. This protocol does not require timers except those that may be used by the underlying transport to transmit and receive messages over HTTP. The protocol does not include provisions for time-based retry for sending protocol messages.

The security tokens that are transported in protocol messages have a specific time interval during which they are considered to be valid. The STS that issues the Security Tokens MUST set the time interval by using the **NotBefore** and **NotOnOrAfter** attributes of the <Conditions> (section 3.6.4.1.2.17) element. For more details, see [SAMLCore] section 2.3.2.1.1.

Implementations can use a timer to indicate when the validity interval of a security token or an Authentication Context expires; however, the protocol does not require the use of a timer. Timers are not used to determine when validity intervals expire. The **NotBefore** and **NotOnOrAfter** values that are obtained from security tokens MUST be explicitly checked.

3.7.6 Other Local Events

This protocol does not have dependencies on any transport protocols other than HTTP 1.1. This protocol relies on this transport mechanism for the correct and timely delivery of protocol messages. The protocol does not take action in response to any changes or failure in machine state or network communications.

4 Protocol Examples

This section describes an example flow of messages between a client and a Security Token Service for each type of authentication that may be supported by the Security Token Service.

4.1 WS-MetadataExchange Request

The following is an example of a WS-MetadataExchange request.

```
<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://schemas.xmlsoap.org/ws/2004/09/transfer/Get</a:Action>
<a:MessageID>urn:uuid:fe768037-0fb1-4dd5-9c75-0d4b68d631de</a:MessageID>
<a:ReplyTo>
<a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
</a:ReplyTo>
<a:To s:mustUnderstand="1">https://identity.redmond.corp.microsoft.com/Trust/Mex</a:To>
</s:Header>
<s:Body></s:Body>
</s:Envelope>
```

4.2 WS-MetadataExchange Response

The following is an example of a WS-MetadataExchange response. It describes a single endpoint that uses Integrated Windows Authentication (SPNego). The namespace http://schemas.microsoft.com/ws/2005/12/wsdl/contract is defined in [MS-WSPOL].

```
<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://schemas.xmlsoap.org/ws/2004/09/transfer/GetResponse</a:Action>
<a:RelatesTo>urn:uuid:fe768037-0fb1-4dd5-9c75-0d4b68d631de</a:RelatesTo>
</s:Header>
<s:Body>
<Metadata xmlns="http://schemas.xmlsoap.org/ws/2004/09/mex"
xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex">
<wsx:<MetadataSection> Dialect="http://schemas.xmlsoap.org/wsdl/"
Identifier="http://tempuri.org/" xmlns="">
<wsdl:definitions name="WSTrustFeb2005ContractAsync" targetNamespace="http://tempuri.org/"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:tns="http://tempuri.org/"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsap="http://schemas.xmlsoap.org/ws/2004/08/addressing/policy"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:msc="http://schemas.microsoft.com/ws/2005/12/wsdl/contract"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:wsa10="http://www.w3.org/2005/08/addressing">
<wsp:Policy wsu:Id="WSHttpBinding_IWSTrustFeb2005ContractAsync_policy">
<wsp:ExactlyOne>
<wsp:All>
<sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
<wsp:Policy>
```

```
<sp:ProtectionToken>
<wsp:Policy>
<sp:SpnegoContextToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
<wsp:Policy>
<sp:RequireDerivedKeys></sp:RequireDerivedKeys>
</wsp:Policy>
</sp:SpnegoContextToken>
</wsp:Policy>
</sp:ProtectionToken>
<sp:AlgorithmSuite>
<wsp:Policy>
<sp:Basic256></sp:Basic256>
</wsp:Policy>
</sp:AlgorithmSuite>
<sp:Layout>
<wsp:Policy>
<sp:Strict></sp:Strict>
</wsp:Policy>
</sp:Layout>
<sp:IncludeTimestamp></sp:IncludeTimestamp>
<sp:EncryptSignature></sp:EncryptSignature>
<sp:OnlySignEntireHeadersAndBody></sp:OnlySignEntireHeadersAndBody>
</wsp:Policy>
</sp:SymmetricBinding>
<sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
<wsp:Policy>
<sp:MustSupportRefKeyIdentifier></sp:MustSupportRefKeyIdentifier>
<sp:MustSupportRefIssuerSerial></sp:MustSupportRefIssuerSerial>
<sp:MustSupportRefThumbprint></sp:MustSupportRefThumbprint>
<sp:MustSupportRefEncryptedKey></sp:MustSupportRefEncryptedKey>
</wsp:Policy>
</sp:Wss11>
<sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
<wsp:Policy>
<sp:MustSupportIssuedTokens></sp:MustSupportIssuedTokens>
<sp:RequireClient<Entropy>></sp:RequireClient<Entropy>>
<sp:RequireServer<Entropy>></sp:RequireServer<Entropy>>
</wsp:Policy>
</sp:Trust10>
<wsaw:UsingAddressing></wsaw:UsingAddressing>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
<wsp:Policy wsu:Id="WSHttpBinding_IWSTrustFeb2005ContractAsync_IssueAsync_policy">
<wsp:ExactlyOne>
<wsp:All>
<sp:EndorsingSupportingTokens
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
<wsp:Policy>
<mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true"
xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"></mssp:RsaToken>
</wsp:Policy>
</sp:EndorsingSupportingTokens>
</wsp:All>
</wsp:ExactlyOne>
```

```
</wsp:Policy>
<wsp:Policy wsu:Id="WSHttpBinding_IWSTrustFeb2005ContractAsync_IssueAsync_Input_policy">
<wsp:ExactlyOne>
<wsp:All>
<sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
<sp:Body></sp:Body>
<sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="FaultTo" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="ReplyTo" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="MessageID" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="RelatesTo" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="Action" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
</sp:SignedParts>
<sp:EncryptedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
<sp:Body></sp:Body>
</sp:EncryptedParts>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
<wsp:Policy wsu:Id="WSHttpBinding_IWSTrustFeb2005ContractAsync_IssueAsync_output_policy">
<wsp:ExactlyOne>
<wsp:All>
<sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
<sp:Body></sp:Body>
<sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="FaultTo" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="ReplyTo" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="MessageID" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="RelatesTo" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
<sp:Header Name="Action" Namespace="http://www.w3.org/2005/08/addressing"></sp:Header>
</sp:SignedParts>
<sp:EncryptedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
<sp:Body></sp:Body>
</sp:EncryptedParts>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
<wsdl:types>
<xsd:schema targetNamespace="http://tempuri.org/Imports">
<xsd:import namespace="http://schemas.microsoft.com/Message"></xsd:import>
</xsd:schema>
</wsdl:types>
<wsdl:message name="IWSTrustFeb2005ContractAsync_IssueAsync_InputMessage">
<wsdl:part name="request" type="q3:MessageBody"
xmlns:q3="http://schemas.microsoft.com/Message"></wsdl:part>
</wsdl:message>
<wsdl:message name="IWSTrustFeb2005ContractAsync_IssueAsync_OutputMessage">
<wsdl:part name="IssueAsyncResult" type="q4:MessageBody"
xmlns:q4="http://schemas.microsoft.com/Message"></wsdl:part>
</wsdl:message>
<wsdl:portType name="IWSTrustFeb2005ContractAsync">
<wsdl:operation name="CancelAsync">
<wsdl:input wsaw:Action="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Cancel"
message="tns:IWSTrustFeb2005ContractAsync_CancelAsync_InputMessage"></wsdl:input>
<wsdl:output wsaw:Action="http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Cancel"
message="tns:IWSTrustFeb2005ContractAsync_CancelAsync_OutputMessage"></wsdl:output>
</wsdl:operation>
```

```
<wsdl:operation name="IssueAsync">
<wsdl:input wsaw:Action="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
message="tns:IWSTrustFeb2005ContractAsync_IssueAsync_InputMessage"></wsdl:input>
<wsdl:output wsaw:Action="http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue"
message="tns:IWSTrustFeb2005ContractAsync_IssueAsync_OutputMessage"></wsdl:output>
</wsdl:operation>
<wsdl:operation name="RenewAsync">
<wsdl:input wsaw:Action="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Renew"
message="tns:IWSTrustFeb2005ContractAsync_RenewAsync_InputMessage"></wsdl:input>
<wsdl:output wsaw:Action="http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Renew"
message="tns:IWSTrustFeb2005ContractAsync_RenewAsync_OutputMessage"></wsdl:output>
</wsdl:operation>
<wsdl:operation name="ValidateAsync">
<wsdl:input wsaw:Action="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Validate"
message="tns:IWSTrustFeb2005ContractAsync_ValidateAsync_InputMessage"></wsdl:input>
<wsdl:output wsaw:Action="http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Validate"
message="tns:IWSTrustFeb2005ContractAsync_ValidateAsync_OutputMessage"></wsdl:output>
</wsdl:operation>
</wsdl:portType>
<wsdl:binding name="WSHttpBinding_IWSTrustFeb2005ContractAsync"
type="tns:IWSTrustFeb2005ContractAsync">
<wsp:PolicyReference
URI="#WSHttpBinding_IWSTrustFeb2005ContractAsync_policy"></wsp:PolicyReference>
<soap12:binding transport="http://schemas.xmlsoap.org/soap/http"></soap12:binding>
<wsdl:operation name="CancelAsync">
<soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Cancel"
style="document"></soap12:operation>
<wsdl:input>
<wsp:PolicyReference
URI="#WSHttpBinding_IWSTrustFeb2005ContractAsync_CancelAsync_Input_policy"></wsp:PolicyRefere
nce>
<soap12:body use="literal"></soap12:body>
</wsdl:input>
<wsdl:output>
<wsp:PolicyReference
URI="#WSHttpBinding_IWSTrustFeb2005ContractAsync_CancelAsync_output_policy"></wsp:PolicyRefer
ence>
<soap12:body use="literal"></soap12:body>
</wsdl:output>
</wsdl:operation>
<wsdl:operation name="IssueAsync">
<wsp:PolicyReference
URI="#WSHttpBinding_IWSTrustFeb2005ContractAsync_IssueAsync_policy"></wsp:PolicyReference>
<soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"></soap12:operation>
<wsdl:input>
<wsp:PolicyReference
URI="#WSHttpBinding_IWSTrustFeb2005ContractAsync_IssueAsync_Input_policy"></wsp:PolicyReferen
ce>
<soap12:body use="literal"></soap12:body>
</wsdl:input>
<wsdl:output>
<wsp:PolicyReference
URI="#WSHttpBinding_IWSTrustFeb2005ContractAsync_IssueAsync_output_policy"></wsp:PolicyRefere
nce>
<soap12:body use="literal"></soap12:body>
</wsdl:output>
</wsdl:operation>
<wsdl:operation name="RenewAsync">
<soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Renew"
style="document"></soap12:operation>
```

```
<wsdl:input>
<wsp:PolicyReference
URI="#WSHttpBinding_IWSTrustFeb2005ContractAsync_RenewAsync_Input_policy"></wsp:PolicyReferen
ce>
<soap12:body use="literal"></soap12:body>
</wsdl:input>
<wsdl:output>
<wsp:PolicyReference
URI="#WSHttpBinding_IWSTrustFeb2005ContractAsync_RenewAsync_output_policy"></wsp:PolicyRefere
nce>
<soap12:body use="literal"></soap12:body>
</wsdl:output>
</wsdl:operation>
<wsdl:operation name="ValidateAsync">
<soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Validate"
style="document"></soap12:operation>
<wsdl:input>
<wsp:PolicyReference
URI="#WSHttpBinding_IWSTrustFeb2005ContractAsync_ValidateAsync_Input_policy"></wsp:PolicyRefe
rence>
<soap12:body use="literal"></soap12:body>
</wsdl:input>
<wsdl:output>
<wsp:PolicyReference
URI="#WSHttpBinding_IWSTrustFeb2005ContractAsync_ValidateAsync_output_policy"></wsp:PolicyRef
erence>
<soap12:body use="literal"></soap12:body>
</wsdl:output>
</wsdl:operation>
</wsdl:binding>
<wsdl:service name="WSTrustFeb2005ContractAsync">
<wsdl:port name="WSHttpBinding_IWSTrustFeb2005ContractAsync"
binding="tns:WSHttpBinding_IWSTrustFeb2005ContractAsync">
<soap12:address
location="http://identity.redmond.corp.microsoft.com/Trust/Windows"></soap12:address>
<wsa10:EndpointReference>
<wsa10:Address>http://identity.redmond.corp.microsoft.com/Trust/Windows</wsa10:Address>
<Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
<Spn>host/identity.redmond.corp.microsoft.com</Spn>
</Identity>
</wsa10:EndpointReference>
</wsdl:port>
</wsdl:service>
</wsdl:definitions>
</wsx:<MetadataSection>>
<wsx:<MetadataSection> Dialect="http://www.w3.org/2001/XMLSchema"
Identifier="http://schemas.microsoft.com/Message" xmlns="">
<xs:schema elementFormDefault="qualified"
targetNamespace="http://schemas.microsoft.com/Message"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://schemas.microsoft.com/Message">
<xs:complexType name="MessageBody">
<xs:sequence>
<xs:any minOccurs="0" maxOccurs="unbounded" namespace="##any"></xs:any>
</xs:sequence>
</xs:complexType>
</xs:schema>
</wsx:<MetadataSection>>
</Metadata>
</s:Body>
```

```
</s:Envelope>
```

4.3 WS-Trust for SPNego Request

The following is a WS-Trust for SPNego request.

```
<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://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue</a:Action>
<a:MessageID>urn:uuid:e30466e0-9f37-42b4-80e5-8d2f8cabedf6</a:MessageID>
<a:ReplyTo>
<a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
</a:ReplyTo>
<a:To s:mustUnderstand="1">http://identity.redmond.corp.microsoft.com/Trust/Windows</a:To>
</s:Header>
<s:Body>
<t:<RequestSecurityToken> Context="uuid-2a4ff557-9cbe-4da6-a268-740b551ad6fe-1"
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust">
<t:TokenType>http://schemas.xmlsoap.org/ws/2005/02/sc/sct</t:TokenType>
<t:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Issue</t:RequestType>
<t:<KeySize>>256</t:<KeySize>>
<t:BinaryExchange ValueType="http://schemas.xmlsoap.org/ws/2005/02/trust/spnego"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">YIIR7gYGKw... ==</t:BinaryExchange>
</t:<RequestSecurityToken>>
</s:Body>
</s:Envelope>
```

4.4 WS-Trust for SPNego Response

The following is a response to the WS-Trust for SPNego request.

```
<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://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue</a:Action>
<a:RelatesTo>urn:uuid:e30466e0-9f37-42b4-80e5-8d2f8cabedf6</a:RelatesTo>
</s:Header>
<s:Body>
<t:<RequestSecurityToken>ResponseCollection
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust">
<t:<RequestSecurityToken>Response Context="uuid-2a4ff557-9cbe-4da6-a268-740b551ad6fe-1"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<t:TokenType>http://schemas.xmlsoap.org/ws/2005/02/sc/sct</t:TokenType>
<t:RequestedSecurityToken>
<c:<SecurityContextToken> u:Id="uuid-3303141f-94fd-4111-ab9f-c5cbadba9a8e-67"
xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
<c:Identifier>urn:uuid:46fd761b-dfed-45fc-a6b5-9821c7905e8f</c:Identifier>
</c:<SecurityContextToken>>
</t:RequestedSecurityToken>
<t:RequestedAttachedReference>
<o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
```

```
<o:Reference ValueType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct" URI="#uuid-3303141f-
94fd-4111-ab9f-c5cbadba9a8e-67"></o:Reference>
</o:SecurityTokenReference>
</t:RequestedAttachedReference>
<t:RequestedUnattachedReference>
<o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
<o:Reference URI="urn:uuid:46fd761b-dfed-45fc-a6b5-9821c7905e8f"
ValueType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct"></o:Reference>
</o:SecurityTokenReference>
</t:RequestedUnattachedReference>
<t:RequestedProofToken>
<e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:EncryptionMethod
Algorithm="http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap"></e:EncryptionMethod>
<e:CipherData>
<e:CipherValue>YEwGCSqGSIb3EgECAgIBEQAQAP//cYXPst0AvWgasCzatwJYuYz88h+QNbyMKXGdhZn5wyP7fyY/PU
nyaikbdlbYnSgDf8CTxh+5ZyTg</e:CipherValue>
</e:CipherData>
</e:EncryptedKey>
</t:RequestedProofToken>
<t:Lifetime>
<u:Created>2007-10-21T20:13:11.461Z</u:Created>
<u:Expires>2007-10-22T06:13:11.461Z</u:Expires>
</t:Lifetime>
<t:<KeySize>>256</t:<KeySize>>
<t:BinaryExchange ValueType="http://schemas.xmlsoap.org/ws/2005/02/trust/spnego"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">oYGgMIG...==</t:BinaryExchange>
</t:<RequestSecurityToken>Response>
<t:<RequestSecurityToken>Response Context="uuid-2a4ff557-9cbe-4da6-a268-740b551ad6fe-1"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<t:Authenticator>
<t:CombinedHash>iMWJNDfEgGJH/UWDGE2EQBH2scPf5x+hS4wKpyy0V7Q=</t:CombinedHash>
</t:Authenticator>
</t:<RequestSecurityToken>Response>
</t:<RequestSecurityToken>ResponseCollection>
</s:Body>
</s:Envelope>
```

4.5 Token Acquisition Request Messages

The following sections contain examples of WS-Trust request messages for acquiring tokens. The sections are separated based on the type of authentication used to prove the user's identity to the STS. Each message was sent using full message security, so examples of encrypted content and decrypted content are included. All of these messages request a security token containing a symmetric key. Content encoded using base64 encoding (such as encrypted content, digests or certificates) is redacted with an ellipsis.

4.5.1 Windows Integrated Authentication

These examples are from a token acquisition request that uses negotiated windows authentication.

4.5.1.1 Encrypted Content

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<s:Header>
<a:Action s:mustUnderstand="1"
u:Id="_4">http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue</a:Action>
<a:MessageID u:Id="_5">urn:uuid:02889445-7db4-427c-8ea5-1d5176c888d6</a:MessageID>
<a:ReplyTo u:Id="_6">
<a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
</a:ReplyTo>
<a:To s:mustUnderstand="1" u:Id="_7">http://shiung-
vista.redmond.corp.microsoft.com:8000/Sts/zwqPpXayMK_Cb1_4_2/ISyncContract</a:To>
<o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
<u:Timestamp u:Id="uuid-c3af77c0-cd89-4597-ac52-0531074f5d82-34">
<u:Created>2007-11-14T19:46:24.927Z</u:Created>
<u:Expires>2007-11-14T19:51:24.927Z</u:Expires>
</u:Timestamp>
<c:SecurityContextToken u:Id="uuid-1ccdb2d6-1519-4585-a309-72382220b5f2-1"
xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
<c:Identifier>urn:uuid:a60bf9e6-71ed-436b-9525-1227a0f472e6</c:Identifier>
</c:SecurityContextToken>
<c:DerivedKeyToken u:Id="_0" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
<o:SecurityTokenReference>
<o:Reference ValueType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct" URI="#uuid-1ccdb2d6-
1519-4585-a309-72382220b5f2-1"></o:Reference>
</o:SecurityTokenReference>
<c:Offset>0</c:Offset>
<c:Length>24</c:Length>
<c:Nonce>Y5CtHxARBUQPCWsM6cG7WQ==</c:Nonce>
</c:DerivedKeyToken>
<c:DerivedKeyToken u:Id="_1" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
<o:SecurityTokenReference>
<o:Reference ValueType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct" URI="#uuid-1ccdb2d6-
1519-4585-a309-72382220b5f2-1"></o:Reference>
</o:SecurityTokenReference>
<c:Nonce>o7GyJVjjZ0FCBeT5GFy55w==</c:Nonce>
</c:DerivedKeyToken>
<e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:DataReference URI="#_3"></e:DataReference>
<e:DataReference URI="#_8"></e:DataReference>
</e:ReferenceList>
<e:EncryptedData Id="_8" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<o:SecurityTokenReference>
<o:Reference URI="#_1"></o:Reference>
</o:SecurityTokenReference>
</KeyInfo>
<e:CipherData>
<e:CipherValue>...Fhb2x</e:CipherValue>
</e:CipherData>
</e:EncryptedData>
</o:Security>
</s:Header>
<s:Body u:Id="_2">
```

```
<e:EncryptedData Id="_3" Type="http://www.w3.org/2001/04/xmlenc#Content"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
<o:Reference URI="#_1"></o:Reference>
</o:SecurityTokenReference>
</KeyInfo>
<e:CipherData>
<e:CipherValue>...zIW7</e:CipherValue>
</e:CipherData>
</e:EncryptedData>
</s:Body>
</s:Envelope>
```

4.5.1.2 Decrypted Content

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope">
    <s:Header>
      <a:Action s:mustUnderstand="1" u:Id="_4" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:a="http://www.w3.org/2005/08/addressing">http://schemas.xmlsoap.org/ws/2005/02/trust/RS
T/Issue</a:Action>
      <a:MessageID u:Id="_5" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd"
xmlns:a="http://www.w3.org/2005/08/addressing">urn:uuid:02889445-7db4-427c-8ea5-
1d5176c888d6</a:MessageID>
      <a:ReplyTo u:Id="_6" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:a="http://www.w3.org/2005/08/addressing">
        <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
      </a:ReplyTo>
      <a:To s:mustUnderstand="1" u:Id="_7" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:a="http://www.w3.org/2005/08/addressing">http://shiung-
vista.redmond.corp.microsoft.com:8000/Sts/zwqPpXayMK_Cb1_4_2/ISyncContract</a:To>
      <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
        <u:Timestamp u:Id="uuid-c3af77c0-cd89-4597-ac52-0531074f5d82-34"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
          <u:Created>2007-11-14T19:46:24.927Z</u:Created>
          <u:Expires>2007-11-14T19:51:24.927Z</u:Expires>
        </u:Timestamp>
        <c:SecurityContextToken u:Id="uuid-1ccdb2d6-1519-4585-a309-72382220b5f2-1"
xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
          <c:Identifier>urn:uuid:a60bf9e6-71ed-436b-9525-1227a0f472e6</c:Identifier>
        </c:SecurityContextToken>
        <c:DerivedKeyToken u:Id="_0" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
          <o:SecurityTokenReference>
            <o:Reference ValueType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct" URI="#uuid-
1ccdb2d6-1519-4585-a309-72382220b5f2-1"></o:Reference>
          </o:SecurityTokenReference>
          <c:Offset>0</c:Offset>
          <c:Length>24</c:Length>
          <c:Nonce>Y5CtHxARBUQPCWsM6cG7WQ==</c:Nonce>
        </c:DerivedKeyToken>
```

```
        <c:DerivedKeyToken u:Id="_1" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
          <o:SecurityTokenReference>
            <o:Reference ValueType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct" URI="#uuid-
1ccdb2d6-1519-4585-a309-72382220b5f2-1"></o:Reference>
          </o:SecurityTokenReference>
          <c:Nonce>o7GyJVjjZ0FCBeT5GFy55w==</c:Nonce>
        </c:DerivedKeyToken>
        <e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
          <e:DataReference URI="#_3"></e:DataReference>
          <e:DataReference URI="#_8"></e:DataReference>
        </e:ReferenceList>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
          <SignedInfo>
            <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
            <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
sha1"></SignatureMethod>
            <Reference URI="#_2">
              <Transforms>
                <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
              </Transforms>
              <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
              <DigestValue>54lIv2loPVGpZduCTRZnSZQLIW0=</DigestValue>
            </Reference>
            <Reference URI="#_4">
              <Transforms>
                <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
              </Transforms>
              <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
              <DigestValue>N0f3pfg6K2iKWqtltYnmZZimqPE=</DigestValue>
            </Reference>
            <Reference URI="#_5">
              <Transforms>
                <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
              </Transforms>
              <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
              <DigestValue>yO9Bqr5W7xrAtvAAtmqIxG/lN6I=</DigestValue>
            </Reference>
            <Reference URI="#_6">
              <Transforms>
                <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
              </Transforms>
              <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
              <DigestValue>CuNmjfm/U6y2+ZScFHyVRRpkyKQ=</DigestValue>
            </Reference>
            <Reference URI="#_7">
              <Transforms>
                <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
              </Transforms>
              <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
              <DigestValue>5iCXjJoM4yD7xBqE4eCYNNxwDM0=</DigestValue>
            </Reference>
            <Reference URI="#uuid-c3af77c0-cd89-4597-ac52-0531074f5d82-34">
              <Transforms>
```

```
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>TnjkwumT7CdI/E+jXFvYv2c4FXs=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>yeyGPiNDDWDSBhKpx7xJWYvc0BM=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
            <o:Reference URI="#_0"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_2" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
    <wst:RequestSecurityToken Context="ProcessRequestSecurityToken"
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust">
      <wst:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Issue</wst:RequestType>
      <wsid:InformationCardReference
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity">
        <wsid:CardId>urn:uuid:6e5d96e5-98c5-4af3-b4bd-12a5a28c045e</wsid:CardId>
        <wsid:CardVersion>1</wsid:CardVersion>
      </wsid:InformationCardReference>
      <wst:Claims>
        <wsid:ClaimType
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:ClaimType>
        <wsid:ClaimType
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:ClaimType>
      </wst:Claims>
      <wst:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</wst:KeyType>
      <wst:KeySize>256</wst:KeySize>
      <wst:Entropy>
        <t:BinarySecret u:Id="uuid-c3af77c0-cd89-4597-ac52-0531074f5d82-35"
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">GdIEm8ii8NzMZIC/mJLuBdm2vVXb2HmR3xwFJfaLcJ8=</t:BinarySecret>
      </wst:Entropy>
      <wst:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-cbc</wst:EncryptWith>
      <wst:SignWith>http://www.w3.org/2000/09/xmldsig#hmac-sha1</wst:SignWith>
      <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
          <Address>http://shiung-
vista.redmond.corp.microsoft.com:8000/ServiceLocation/zwqPpXayMK_Cb1_4_1/ISecureService</Addr
ess>
          <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
              <X509Data>
                <X509Certificate>...jIBPs=</X509Certificate>
              </X509Data>
            </KeyInfo>
          </Identity>
        </EndpointReference>
      </wsp:AppliesTo>
      <ClientPseudonym xmlns="http://schemas.xmlsoap.org/ws/2005/05/identity">
```

```
          <PPID>V5biGjGiN82W+A43OYUX55/oKgw3csd1Cb+V7k34xis=</PPID>
        </ClientPseudonym>
        <wst:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</wst:EncryptionAlgorithm>
        <wst:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</wst:CanonicalizationAlgorithm>
        <wsid:RequestDisplayToken xml:lang="en"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:RequestDisplayToken>
      </wst:RequestSecurityToken>
    </s:Body>
  </s:Envelope>
```

4.5.2 Certificate Authentication

These examples are from a token acquisition request that uses X.509 certificate authentication.

4.5.2.1 Encrypted Content

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <s:Header>
    <a:Action s:mustUnderstand="1"
u:Id="_5">http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue</a:Action>
    <a:MessageID u:Id="_6">urn:uuid:e9e91908-3a6e-4305-bc67-98269e6db0f4</a:MessageID>
    <a:ReplyTo u:Id="_7">
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1" u:Id="_8">http://shiung-
vista.redmond.corp.microsoft.com:8000/Qm3Gl7QsMK_gO_3_1/Qm3Gl7QsMK_gO_3_4/IWSTrustFeb2005Cont
ract</a:To>
    <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
      <u:Timestamp u:Id="uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-10">
        <u:Created>2007-10-24T01:46:44.235Z</u:Created>
        <u:Expires>2007-10-24T01:51:44.235Z</u:Expires>
      </u:Timestamp>
      <e:EncryptedKey Id="uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-9"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns="http://www.w3.org/2000/09/xmldsig#"></DigestMethod>
        </e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-
message-security-1.1#ThumbprintSHA1" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">hGrIpsPp8P3b1IGg+LlhD1WZ3cY=</o:KeyIdentifier>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>...MjkM=</e:CipherValue>
        </e:CipherData>
      </e:EncryptedKey>
      <c:DerivedKeyToken u:Id="_0" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
        <o:SecurityTokenReference>
          <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-
security-1.1#EncryptedKey" URI="#uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-9"></o:Reference>
```

```
        </o:SecurityTokenReference>
        <c:Offset>0</c:Offset>
        <c:Length>24</c:Length>
        <c:Nonce>5TsnZWTHZLDkTX9RtDgHMg==</c:Nonce>
      </c:DerivedKeyToken>
      <c:DerivedKeyToken u:Id="_2" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
        <o:SecurityTokenReference>
          <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-
security-1.1#EncryptedKey" URI="#uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-9"></o:Reference>
        </o:SecurityTokenReference>
        <c:Nonce>KCEXvyuDL0rUAodmuYa9aQ==</c:Nonce>
      </c:DerivedKeyToken>
      <e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:DataReference URI="#_4"></e:DataReference>
        <e:DataReference URI="#_9"></e:DataReference>
        <e:DataReference URI="#_10"></e:DataReference>
      </e:ReferenceList>
      <o:BinarySecurityToken u:Id="uuid-ff5ca108-aa93-4dc8-93f4-d5719165d15a-8"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary">...KLQ9I</o:BinarySecurityToken>
      <e:EncryptedData Id="_9" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:Reference URI="#_2"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>...DahJJ</e:CipherValue>
        </e:CipherData>
      </e:EncryptedData>
      <e:EncryptedData Id="_10" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:Reference URI="#_2"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>...wq7lA=</e:CipherValue>
        </e:CipherData>
      </e:EncryptedData>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_3">
    <e:EncryptedData Id="_4" Type="http://www.w3.org/2001/04/xmlenc#Content"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
          <o:Reference URI="#_2"></o:Reference>
        </o:SecurityTokenReference>
      </KeyInfo>
```

```
      <e:CipherData>
        <e:CipherValue>...yja</e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

4.5.2.2 Decrypted Content

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope">
  <s:Header>
    <a:Action s:mustUnderstand="1" u:Id="_5" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:a="http://www.w3.org/2005/08/addressing">http://schemas.xmlsoap.org/ws/2005/02/trust/RS
T/Issue</a:Action>
    <a:MessageID u:Id="_6" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:a="http://www.w3.org/2005/08/addressing">urn:uuid:e9e91908-
3a6e-4305-bc67-98269e6db0f4</a:MessageID>
    <a:ReplyTo u:Id="_7" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:a="http://www.w3.org/2005/08/addressing">
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1" u:Id="_8" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:a="http://www.w3.org/2005/08/addressing">http://shiung-
vista.redmond.corp.microsoft.com:8000/Qm3Gl7QsMK_gO_3_1/Qm3Gl7QsMK_gO_3_4/IWSTrustFeb2005Cont
ract</a:To>
    <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
      <u:Timestamp u:Id="uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-10"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <u:Created>2007-10-24T01:46:44.235Z</u:Created>
        <u:Expires>2007-10-24T01:51:44.235Z</u:Expires>
      </u:Timestamp>
      <e:EncryptedKey Id="uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-9"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns="http://www.w3.org/2000/09/xmldsig#"></DigestMethod>
        </e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-
message-security-1.1#ThumbprintSHA1" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">hGrIpsPp8P3b1IGg+LlhD1WZ3cY=</o:KeyIdentifier>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>

<e:CipherValue>h1swM6E/13Ea1x4msjH23SrChEMI+PNZ9Q7lstJQzp+szYV4TUA/q39C4KeyHmUMgkuaYmJoRBLtFF
YYf5A5yP/4k3s1I/sLodYPqQMG/deAoJhGzhJl5a1M7xYDPl5h+1owerD43yfP+ZtZeDImQQAih21+yZ9F6N6kCpIMjkM
=</e:CipherValue>
        </e:CipherData>
      </e:EncryptedKey>
      <c:DerivedKeyToken u:Id="_0" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <o:SecurityTokenReference>
          <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-
security-1.1#EncryptedKey" URI="#uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-9"></o:Reference>
```

```
        </o:SecurityTokenReference>
        <c:Offset>0</c:Offset>
        <c:Length>24</c:Length>
        <c:Nonce>5TsnZWTHZLDkTX9RtDgHMg==</c:Nonce>
      </c:DerivedKeyToken>
      <c:DerivedKeyToken u:Id="_2" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <o:SecurityTokenReference>
          <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-
security-1.1#EncryptedKey" URI="#uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-9"></o:Reference>
        </o:SecurityTokenReference>
        <c:Nonce>KCEXvyuDL0rUAodmuYa9aQ==</c:Nonce>
      </c:DerivedKeyToken>
      <e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:DataReference URI="#_4"></e:DataReference>
        <e:DataReference URI="#_9"></e:DataReference>
        <e:DataReference URI="#_10"></e:DataReference>
      </e:ReferenceList>
      <o:BinarySecurityToken u:Id="uuid-ff5ca108-aa93-4dc8-93f4-d5719165d15a-8"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd">...UN8KLQ9I</o:BinarySecurityToken>
      <Signature Id="_1" xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
sha1"></SignatureMethod>
          <Reference URI="#_3">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>UXK1D7d7MIwJOSt+LsLlsM9OYv0=</DigestValue>
          </Reference>
          <Reference URI="#_5">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>wwJgraeIxm8410jSBWUmlsIuldg=</DigestValue>
          </Reference>
          <Reference URI="#_6">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>2t637DM4LiXqQrao3+IvDpssdLg=</DigestValue>
          </Reference>
          <Reference URI="#_7">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>/VQp7dyoeHil2eDAcX4gSMW41Mo=</DigestValue>
          </Reference>
          <Reference URI="#_8">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
```

```
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>BMLlgXQ/nNqOpUTgfipF4cMT1e8=</DigestValue>
          </Reference>
          <Reference URI="#uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-10">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>nk4CB/5aT5pGPWCEMBMLgq5Gf5A=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>BGi4f742OKEKoMcPqffO+ApDd9g=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
            <o:Reference URI="#_0"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"></SignatureMethod>
          <Reference URI="#_1">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>TByNjWWng8Y0k/gt8yDALG0WaiI=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>...YB8U=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
            <o:Reference ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3" URI="#uuid-ff5ca108-aa93-4dc8-93f4-d5719165d15a-
8"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_3" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
    <wst:RequestSecurityToken Context="ProcessRequestSecurityToken"
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust">
      <wst:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Issue</wst:RequestType>
      <wsid:InformationCardReference
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity">
        <wsid:CardId>urn:uuid:6a6bf4f3-2fc8-40ec-82c5-f958fe5717d7</wsid:CardId>
        <wsid:CardVersion>1</wsid:CardVersion>
      </wsid:InformationCardReference>
      <wst:Claims>
        <wsid:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:ClaimType>
```

```
        <wsid:ClaimType
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:ClaimType>
      </wst:Claims>
      <wst:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</wst:KeyType>
      <wst:KeySize>256</wst:KeySize>
      <wst:Entropy>
        <t:BinarySecret u:Id="uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-11"
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">MK7ZE2h0irOvb/i74N2zA8QU/17Gc20rt5Rt4Lh3nt4=</t:BinarySecret>
      </wst:Entropy>
      <wst:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-cbc</wst:EncryptWith>
      <wst:SignWith>http://www.w3.org/2000/09/xmldsig#hmac-sha1</wst:SignWith>
      <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
          <Address>http://shiung-
vista.redmond.corp.microsoft.com:8000/Qm3Gl7QsMK_gO_3_2/Qm3Gl7QsMK_gO_3_3/ISecureService</Add
ress>
          <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
              <X509Data>
                <X509Certificate>...jIBPs=</X509Certificate>
              </X509Data>
            </KeyInfo>
          </Identity>
        </EndpointReference>
      </wsp:AppliesTo>
      <ClientPseudonym xmlns="http://schemas.xmlsoap.org/ws/2005/05/identity">
        <PPID>0jOzJ8JdrQyLGREfdvOSYLHhHUiclpNujjt4MfbYcbU=</PPID>
      </ClientPseudonym>
      <wst:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</wst:EncryptionAlgorithm>
      <wst:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</wst:CanonicalizationAlgorithm>
      <wsid:RequestDisplayToken xml:lang="en"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:RequestDisplayToken>
    </wst:RequestSecurityToken>
  </s:Body>
</s:Envelope>
```

4.5.3 Username Password Authentication

These examples are from a token acquisition request that uses username and password authentication.

4.5.3.1 Encrypted Content

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <s:Header>
    <a:Action s:mustUnderstand="1"
u:Id="_4">http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue</a:Action>
    <a:MessageID u:Id="_5">urn:uuid:e3024ffb-6bbf-415e-aff6-f680fbc4626e</a:MessageID>
    <a:ReplyTo u:Id="_6">
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
```

```
    <a:To s:mustUnderstand="1" u:Id="_7">http://shiung-
vista.redmond.corp.microsoft.com:8000/Cp2hU8QsMK_gK_4_1/Cp2hU8QsMK_gK_4_2/IWSTrustFeb2005Cont
ract</a:To>
    <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
      <u:Timestamp u:Id="uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-14">
        <u:Created>2007-10-24T01:49:10.214Z</u:Created>
        <u:Expires>2007-10-24T01:54:10.214Z</u:Expires>
      </u:Timestamp>
      <e:EncryptedKey Id="uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-13"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns="http://www.w3.org/2000/09/xmldsig#"></DigestMethod>
        </e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-
message-security-1.1#ThumbprintSHA1" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">hGrIpsPp8P3b1IGg+LlhD1WZ3cY=</o:KeyIdentifier>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>...ooUM=</e:CipherValue>
        </e:CipherData>
      </e:EncryptedKey>
      <c:DerivedKeyToken u:Id="_0" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
        <o:SecurityTokenReference>
          <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-
security-1.1#EncryptedKey" URI="#uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-13"></o:Reference>
        </o:SecurityTokenReference>
        <c:Offset>0</c:Offset>
        <c:Length>24</c:Length>
        <c:Nonce>WRAf6xm7IncAEf5hPh/XmA==</c:Nonce>
      </c:DerivedKeyToken>
      <c:DerivedKeyToken u:Id="_1" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
        <o:SecurityTokenReference>
          <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-
security-1.1#EncryptedKey" URI="#uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-13"></o:Reference>
        </o:SecurityTokenReference>
        <c:Nonce>hznKEjwo8JUvZC8STjd+cg==</c:Nonce>
      </c:DerivedKeyToken>
      <e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:DataReference URI="#_3"></e:DataReference>
        <e:DataReference URI="#_8"></e:DataReference>
        <e:DataReference URI="#_9"></e:DataReference>
      </e:ReferenceList>
      <e:EncryptedData Id="_9" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:Reference URI="#_1"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>...VFGQ=</e:CipherValue>
        </e:CipherData>
```

```
      </e:EncryptedData>
      <e:EncryptedData Id="_8" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:Reference URI="#_1"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>...R4Scx</e:CipherValue>
        </e:CipherData>
      </e:EncryptedData>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_2">
    <e:EncryptedData Id="_3" Type="http://www.w3.org/2001/04/xmlenc#Content"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
          <o:Reference URI="#_1"></o:Reference>
        </o:SecurityTokenReference>
      </KeyInfo>
      <e:CipherData>
        <e:CipherValue>...LYb6AF</e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

4.5.3.2 Decrypted Content

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope">
  <s:Header>
    <a:Action s:mustUnderstand="1" u:Id="_4" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:a="http://www.w3.org/2005/08/addressing">http://schemas.xmlsoap.org/ws/2005/02/trust/RS
T/Issue</a:Action>
    <a:MessageID u:Id="_5" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:a="http://www.w3.org/2005/08/addressing">urn:uuid:e3024ffb-
6bbf-415e-aff6-f680fbc4626e</a:MessageID>
    <a:ReplyTo u:Id="_6" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:a="http://www.w3.org/2005/08/addressing">
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1" u:Id="_7" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:a="http://www.w3.org/2005/08/addressing">http://shiung-
vista.redmond.corp.microsoft.com:8000/Cp2hU8QsMK_gK_4_1/Cp2hU8QsMK_gK_4_2/IWSTrustFeb2005Cont
ract</a:To>
    <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
      <u:Timestamp u:Id="uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-14"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <u:Created>2007-10-24T01:49:10.214Z</u:Created>
```

```
        <u:Expires>2007-10-24T01:54:10.214Z</u:Expires>
      </u:Timestamp>
      <e:EncryptedKey Id="uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-13"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns="http://www.w3.org/2000/09/xmldsig#"></DigestMethod>
        </e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-
message-security-1.1#ThumbprintSHA1" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">hGrIpsPp8P3b1IGg+LlhD1WZ3cY=</o:KeyIdentifier>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>...ooUM=</e:CipherValue>
        </e:CipherData>
      </e:EncryptedKey>
      <c:DerivedKeyToken u:Id="_0" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <o:SecurityTokenReference>
          <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-
security-1.1#EncryptedKey" URI="#uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-13"></o:Reference>
        </o:SecurityTokenReference>
        <c:Offset>0</c:Offset>
        <c:Length>24</c:Length>
        <c:Nonce>WRAf6xm7IncAEf5hPh/XmA==</c:Nonce>
      </c:DerivedKeyToken>
      <c:DerivedKeyToken u:Id="_1" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <o:SecurityTokenReference>
          <o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-
security-1.1#EncryptedKey" URI="#uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-13"></o:Reference>
        </o:SecurityTokenReference>
        <c:Nonce>hznKEjwo8JUvZC8STjd+cg==</c:Nonce>
      </c:DerivedKeyToken>
      <e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:DataReference URI="#_3"></e:DataReference>
        <e:DataReference URI="#_8"></e:DataReference>
        <e:DataReference URI="#_9"></e:DataReference>
      </e:ReferenceList>
      <o:UsernameToken u:Id="uuid-ff5ca108-aa93-4dc8-93f4-d5719165d15a-11"
xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <o:Username>lameUser</o:Username>
        <o:Password o:Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-
token-profile-1.0#PasswordText">lamePassword</o:Password>
      </o:UsernameToken>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
sha1"></SignatureMethod>
          <Reference URI="#_2">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
```

```
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>ufnBhvDEnla3RbfmZlJXr1uAAfw=</DigestValue>
          </Reference>
          <Reference URI="#_4">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>N0f3pfg6K2iKWqtltYnmZZimqPE=</DigestValue>
          </Reference>
          <Reference URI="#_5">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>cv2zB9Jfpwuc3TDnApdv15uYRQw=</DigestValue>
          </Reference>
          <Reference URI="#_6">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>CuNmjfm/U6y2+ZScFHyVRRpkyKQ=</DigestValue>
          </Reference>
          <Reference URI="#_7">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>Mp5euR5o/nOxa4Ot4qU8gfZLUC4=</DigestValue>
          </Reference>
          <Reference URI="#uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-14">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>s05/c4S8AiekbZrGmp17vTGrnA4=</DigestValue>
          </Reference>
          <Reference URI="#uuid-ff5ca108-aa93-4dc8-93f4-d5719165d15a-11">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>Ucl233xTVUuOPhGabglOl3H58hA=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>qepZKdUXx6dzLnt5kIHBGFvsOLU=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
            <o:Reference URI="#_0"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_2" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
```

```
    <wst:RequestSecurityToken Context="ProcessRequestSecurityToken"
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust">
      <wst:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Issue</wst:RequestType>
      <wsid:InformationCardReference
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity">
        <wsid:CardId>urn:uuid:795e414a-7efd-4ccc-b8f4-7bf794d3214b</wsid:CardId>
        <wsid:CardVersion>1</wsid:CardVersion>
      </wsid:InformationCardReference>
      <wst:Claims>
        <wsid:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:ClaimType>
        <wsid:ClaimType
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:ClaimType>
      </wst:Claims>
      <wst:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</wst:KeyType>
      <wst:KeySize>256</wst:KeySize>
      <wst:Entropy>
        <t:BinarySecret u:Id="uuid-a72aeb31-c89c-4b92-bc98-2268f057ccd5-15"
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">cVUxQTCIb5eF0EiHZLz+ns04W4NrLrmSiUDUGluV7u8=</t:BinarySecret>
      </wst:Entropy>
      <wst:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-cbc</wst:EncryptWith>
      <wst:SignWith>http://www.w3.org/2000/09/xmldsig#hmac-sha1</wst:SignWith>
      <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
          <Address>http://shiung-
vista.redmond.corp.microsoft.com:8000/Cp2hU8QsMK_gK_4_3/Cp2hU8QsMK_gK_4_4/ISecureService</Add
ress>
          <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
              <X509Data>
                <X509Certificate>...jIBPs=</X509Certificate>
              </X509Data>
            </KeyInfo>
          </Identity>
        </EndpointReference>
      </wsp:AppliesTo>
      <ClientPseudonym xmlns="http://schemas.xmlsoap.org/ws/2005/05/identity">
        <PPID>FduL05AD9JX4zqWTgLe9gTvZ+jDnv9nfCNLS80KmeZo=</PPID>
      </ClientPseudonym>
      <wst:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</wst:EncryptionAlgorithm>
      <wst:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</wst:CanonicalizationAlgorithm>
      <wsid:RequestDisplayToken xml:lang="en"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:RequestDisplayToken>
    </wst:RequestSecurityToken>
  </s:Body>
</s:Envelope>
```

4.5.4 SAML Token Authentication

These examples are from a token acquisition request that uses a SAML token with a symmetric key for authentication.

4.5.4.1 Encrypted Content

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<s:Header>
<a:Action s:mustUnderstand="1"
u:Id="_5">http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue</a:Action>
<a:MessageID u:Id="_6">urn:uuid:78f81c86-2ed2-466b-b405-1fb24cd2ffdb</a:MessageID>
<a:ReplyTo u:Id="_7">
<a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
</a:ReplyTo>
<a:To s:mustUnderstand="1" u:Id="_8">http://shiung-
vista.redmond.corp.microsoft.com:8000/Sts/JqVggtcyMK_861_4_2/ISyncContract</a:To>
<o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
<u:Timestamp u:Id="uuid-f539a6de-c99c-4929-8ba6-ad13ba6d5669-37">
<u:Created>2007-11-14T22:09:52.128Z</u:Created>
<u:Expires>2007-11-14T22:14:52.128Z</u:Expires>
</u:Timestamp>
<e:EncryptedKey Id="uuid-f539a6de-c99c-4929-8ba6-ad13ba6d5669-36"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns="http://www.w3.org/2000/09/xmldsig#"></DigestMethod>
</e:EncryptionMethod>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<o:SecurityTokenReference>
<o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-
1.1#ThumbprintSHA1" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary">hGrIpsPp8P3b1IGg+LlhD1WZ3cY=</o:KeyIdentifier>
</o:SecurityTokenReference>
</KeyInfo>
<e:CipherData>
<e:CipherValue>...iIhM=</e:CipherValue>
</e:CipherData>
</e:EncryptedKey>
<c:DerivedKeyToken u:Id="_0" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
<o:SecurityTokenReference>
<o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-
1.1#EncryptedKey" URI="#uuid-f539a6de-c99c-4929-8ba6-ad13ba6d5669-36"></o:Reference>
</o:SecurityTokenReference>
<c:Offset>0</c:Offset>
<c:Length>24</c:Length>
<c:Nonce>k3ffkwBqOtu1ZGEtN6mTqA==</c:Nonce>
</c:DerivedKeyToken>
<c:DerivedKeyToken u:Id="_2" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
<o:SecurityTokenReference>
<o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-
1.1#EncryptedKey" URI="#uuid-f539a6de-c99c-4929-8ba6-ad13ba6d5669-36"></o:Reference>
</o:SecurityTokenReference>
<c:Nonce>CssygF9nEuCZkRRLE5NZOw==</c:Nonce>
</c:DerivedKeyToken>
<e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:DataReference URI="#_4"></e:DataReference>
<e:DataReference URI="#_10"></e:DataReference>
<e:DataReference URI="#_11"></e:DataReference>
</e:ReferenceList>
<enc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:enc="http://www.w3.org/2001/04/xmlenc#">
```

```
<enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></enc:EncryptionMethod>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
</e:EncryptionMethod>
<KeyInfo>
<o:SecurityTokenReference>
<o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-
1.1#ThumbprintSHA1" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary">hGrIpsPp8P3b1IGg+LlhD1WZ3cY=</o:KeyIdentifier>
</o:SecurityTokenReference>
</KeyInfo>
<e:CipherData>
<e:CipherValue>B74fFF9A21JVWnur5yERrXfYzsDZbySmzoe4ubpVkX7EhFuPRdqiQau/Bm1Egy5UqAKxw7Jxjkb3u0
M5jSaZy1stDbuXCtNLEYtwtMa3LAqwATBPdLCyR0iO/edS8+pmJbdFjnqEUgDAtVV62AAy8bmDVeG0MpJ4ZauEMW86Uns
=</e:CipherValue>
</e:CipherData>
</e:EncryptedKey>
</KeyInfo>
<enc:CipherData>
<enc:CipherValue>...nY7w==</enc:CipherValue>
</enc:CipherData>
</enc:EncryptedData>
<c:DerivedKeyToken u:Id="_9" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
<o:SecurityTokenReference>
<o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.0#SAMLAssertionID">uuid:1d7b9f6d-49a0-486b-b72c-ed3fba2e7115</o:KeyIdentifier>
</o:SecurityTokenReference>
<c:Offset>0</c:Offset>
<c:Length>24</c:Length>
<c:Nonce>cbdDqMYOGEjuQ+owGegY7w==</c:Nonce>
</c:DerivedKeyToken>
<e:EncryptedData Id="_10" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<o:SecurityTokenReference>
<o:Reference URI="#_2"></o:Reference>
</o:SecurityTokenReference>
</KeyInfo>
<e:CipherData>
<e:CipherValue>...irllP02</e:CipherValue>
</e:CipherData>
</e:EncryptedData>
<e:EncryptedData Id="_11" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<o:SecurityTokenReference>
<o:Reference URI="#_2"></o:Reference>
</o:SecurityTokenReference>
</KeyInfo>
<e:CipherData>
<e:CipherValue>...qFo=</e:CipherValue>
</e:CipherData>
</e:EncryptedData>
```

```
</o:Security>
</s:Header>
<s:Body u:Id="_3">
<e:EncryptedData Id="_4" Type="http://www.w3.org/2001/04/xmlenc#Content"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
<o:Reference URI="#_2"></o:Reference>
</o:SecurityTokenReference>
</KeyInfo>
<e:CipherData>
<e:CipherValue>...kHIrQ</e:CipherValue>
</e:CipherData>
</e:EncryptedData>
</s:Body>
</s:Envelope>
```

4.5.4.2 Decrypted Content

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope">
<s:Header>
<a:Action s:mustUnderstand="1" u:Id="_5" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:a="http://www.w3.org/2005/08/addressing">http://schemas.xmlsoap.org/ws/2005/02/trust/RS
T/Issue</a:Action>
<a:MessageID u:Id="_6" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:a="http://www.w3.org/2005/08/addressing">urn:uuid:78f81c86-
2ed2-466b-b405-1fb24cd2ffdb</a:MessageID>
<a:ReplyTo u:Id="_7" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:a="http://www.w3.org/2005/08/addressing">
<a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
</a:ReplyTo>
<a:To s:mustUnderstand="1" u:Id="_8" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
xmlns:a="http://www.w3.org/2005/08/addressing">http://shiung-
vista.redmond.corp.microsoft.com:8000/Sts/JqVggtcyMK_861_4_2/ISyncContract</a:To>
<o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
<u:Timestamp u:Id="uuid-f539a6de-c99c-4929-8ba6-ad13ba6d5669-37" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<u:Created>2007-11-14T22:09:52.128Z</u:Created>
<u:Expires>2007-11-14T22:14:52.128Z</u:Expires>
</u:Timestamp>
<e:EncryptedKey Id="uuid-f539a6de-c99c-4929-8ba6-ad13ba6d5669-36"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns="http://www.w3.org/2000/09/xmldsig#"></DigestMethod>
</e:EncryptionMethod>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<o:SecurityTokenReference>
<o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-
1.1#ThumbprintSHA1" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary">hGrIpsPp8P3b1IGg+LlhD1WZ3cY=</o:KeyIdentifier>
</o:SecurityTokenReference>
</KeyInfo>
```

```
<e:CipherData>
<e:CipherValue>...iIhM=</e:CipherValue>
</e:CipherData>
</e:EncryptedKey>
<c:DerivedKeyToken u:Id="_0" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<o:SecurityTokenReference>
<o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-
1.1#EncryptedKey" URI="#uuid-f539a6de-c99c-4929-8ba6-ad13ba6d5669-36"></o:Reference>
</o:SecurityTokenReference>
<c:Offset>0</c:Offset>
<c:Length>24</c:Length>
<c:Nonce>k3ffkwBqOtu1ZGEtN6mTqA==</c:Nonce>
</c:DerivedKeyToken>
<c:DerivedKeyToken u:Id="_2" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<o:SecurityTokenReference>
<o:Reference ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-
1.1#EncryptedKey" URI="#uuid-f539a6de-c99c-4929-8ba6-ad13ba6d5669-36"></o:Reference>
</o:SecurityTokenReference>
<c:Nonce>CssygF9nEuCZkRRLE5NZOw==</c:Nonce>
</c:DerivedKeyToken>
<e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:DataReference URI="#_4"></e:DataReference>
<e:DataReference URI="#_10"></e:DataReference>
<e:DataReference URI="#_11"></e:DataReference>
</e:ReferenceList>
<saml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="uuid:1d7b9f6d-49a0-486b-b72c-
ed3fba2e7115" Issuer="http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self"
IssueInstant="2007-11-14T22:09:52.104Z" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
<saml:Conditions NotBefore="2007-11-14T22:09:52.104Z" NotOnOrAfter="2007-11-
14T23:09:52.104Z">
<saml:AudienceRestrictionCondition>
<saml:Audience>http://shiung-
vista.redmond.corp.microsoft.com:8000/Sts/JqVggtcyMK_861_4_2/ISyncContract</saml:Audience>
</saml:AudienceRestrictionCondition>
</saml:Conditions>
<saml:AttributeStatement>
<saml:Subject>
<saml:SubjectConfirmation>
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-
key</saml:ConfirmationMethod>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
</e:EncryptionMethod>
<KeyInfo>
<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-soap-message-security-
1.1#ThumbprintSHA1" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary">hGrIpsPp8P3b1IGg+LlhD1WZ3cY=</o:KeyIdentifier>
</o:SecurityTokenReference>
</KeyInfo>
<e:CipherData>
<e:CipherValue>...is=</e:CipherValue>
</e:CipherData>
</e:EncryptedKey>
</KeyInfo>
```

```
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Attribute AttributeName="privatepersonalidentifier"
AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">
<saml:AttributeValue>RneShyYgwZig8UnJ+Vr2ds6bU86B+PQ27XnL0qD4Ydc=</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></SignatureMethod>
<Reference URI="#uuid:1d7b9f6d-49a0-486b-b72c-ed3fba2e7115">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></Transform>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
<DigestValue>j3arUXY9/mXbup6JKCuMRmXbn+c=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>...V79fg==</SignatureValue>
<KeyInfo>
<KeyValue>
<RSAKeyValue>
<Modulus>...+zw==</Modulus>
<Exponent>AQAB</Exponent>
</RSAKeyValue>
</KeyValue>
</KeyInfo>
</Signature>
</saml:Assertion>
<c:DerivedKeyToken u:Id="_9" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<o:SecurityTokenReference>
<o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.0#SAMLAssertionID">uuid:1d7b9f6d-49a0-486b-b72c-ed3fba2e7115</o:KeyIdentifier>
</o:SecurityTokenReference>
<c:Offset>0</c:Offset>
<c:Length>24</c:Length>
<c:Nonce>cbdDqMYOGEjuQ+owGegY7w==</c:Nonce>
</c:DerivedKeyToken>
<Signature Id="_1" xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"></SignatureMethod>
<Reference URI="#_3">
<Transforms>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
<DigestValue>BQHf92DhP5j7SEkX8m8ACcmfBqo=</DigestValue>
</Reference>
<Reference URI="#_5">
<Transforms>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
```

```
<DigestValue>wwJgraeIxm8410jSBWUmlsIuldg=</DigestValue>
</Reference>
<Reference URI="#_6">
<Transforms>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
<DigestValue>6nR5Euz59JDYQy3yACaeEsKIUo0=</DigestValue>
</Reference>
<Reference URI="#_7">
<Transforms>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
<DigestValue>/VQp7dyoeHil2eDAcX4gSMW41Mo=</DigestValue>
</Reference>
<Reference URI="#_8">
<Transforms>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
<DigestValue>SzTkHUhPSpVwTpdXN6e2E5X+jIY=</DigestValue>
</Reference>
<Reference URI="#uuid-f539a6de-c99c-4929-8ba6-ad13ba6d5669-37">
<Transforms>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
<DigestValue>hyEZIxUPIW8AvhcHwE+bYFx05a0=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>YhYnwuW0uJXqkDKQNe1FaqFgwZM=</SignatureValue>
<KeyInfo>
<o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
<o:Reference URI="#_0"></o:Reference>
</o:SecurityTokenReference>
</KeyInfo>
</Signature>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"></SignatureMethod>
<Reference URI="#_1">
<Transforms>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
<DigestValue>iBe31InV9sVpSFgz1nwjakuUX0c=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>uh52c8j5ILF9B5draT/pBzDlfFQ=</SignatureValue>
<KeyInfo>
<o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
<o:Reference URI="#_9"></o:Reference>
</o:SecurityTokenReference>
</KeyInfo>
```

```
</Signature>
</o:Security>
</s:Header>
<s:Body u:Id="_3" xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
<wst:RequestSecurityToken Context="ProcessRequestSecurityToken"
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust">
<wst:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Issue</wst:RequestType>
<wsid:InformationCardReference xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity">
<wsid:CardId>urn:uuid:35197d6f-2fdf-4ee9-8af7-a046247efd5d</wsid:CardId>
<wsid:CardVersion>1</wsid:CardVersion>
</wsid:InformationCardReference>
<wst:Claims>
<wsid:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:ClaimType>
<wsid:ClaimType
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:ClaimType>
</wst:Claims>
<wst:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</wst:KeyType>
<wst:KeySize>256</wst:KeySize>
<wst:Entropy>
<t:BinarySecret u:Id="uuid-f539a6de-c99c-4929-8ba6-ad13ba6d5669-38"
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">QXdei4L/LnyQ/3pncTxosMFc2plGpmw/Bq54IVz37sQ=</t:BinarySecret>
</wst:Entropy>
<wst:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-cbc</wst:EncryptWith>
<wst:SignWith>http://www.w3.org/2000/09/xmldsig#hmac-sha1</wst:SignWith>
<wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
<EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
<Address>http://shiung-
vista.redmond.corp.microsoft.com:8000/ServiceLocation/JqVggtcyMK_861_4_1/ISecureService</Addr
ess>
<Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate>...jIBPs=</X509Certificate>
</X509Data>
</KeyInfo>
</Identity>
</EndpointReference>
</wsp:AppliesTo>
<ClientPseudonym xmlns="http://schemas.xmlsoap.org/ws/2005/05/identity">
<PPID>38PJiFDWTVxgV6ULxoO3ecujBUK0mUVj02GLwXNeDDY=</PPID>
</ClientPseudonym>
<wst:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</wst:EncryptionAlgorithm>
<wst:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</wst:CanonicalizationAlgorithm>
<wsid:RequestDisplayToken xml:lang="en"
xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity"></wsid:RequestDisplayToken>
</wst:RequestSecurityToken>
</s:Body>
</s:Envelope>
```

4.6 Token Acquisition Response Messages

The following sections contain examples of a WS-Trust response message for acquiring a Security Token. The response to a certificate binding is included since the responses don't vary widely based on the type of authentication used. The message was sent using full message security, so an example of the encrypted content and decrypted body are included. This message is a response to a request for a Security Token containing a symmetric key. Content encoded using base 64 encoding (such as encrypted content, digests or certificates) is redacted with an ellipsis.

4.6.1 Encrypted Content

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <s:Header>
    <a:Action s:mustUnderstand="1"
u:Id="_7">http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue</a:Action>
    <ActivityId CorrelationId="81422a37-9163-45fc-a393-babad4197888"
xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">610bd55c-0b27-4f1d-
ae38-5ce4d7098f13</ActivityId>
    <a:RelatesTo u:Id="_8">urn:uuid:6ee25b79-4c25-439c-8595-8351bf5b776f</a:RelatesTo>
    <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
      <u:Timestamp u:Id="uuid-c6faaf82-2318-4e0c-8e40-5bd1a188f3a7-6">
        <u:Created>2007-10-24T02:23:12.663Z</u:Created>
        <u:Expires>2007-10-24T02:28:12.663Z</u:Expires>
      </u:Timestamp>
      <c:DerivedKeyToken u:Id="_0" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
        <o:SecurityTokenReference k:TokenType="http://docs.oasis-open.org/wss/oasis-wss-soap-
message-security-1.1#EncryptedKey" xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-
wssecurity-secext-1.1.xsd">
          <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-
security-1.1#EncryptedKeySHA1" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-
1.0#Base64Binary">PjtWs6Qy28v7lLDPjDy0Q1H8pMg=</o:KeyIdentifier>
        </o:SecurityTokenReference>
        <c:Offset>0</c:Offset>
        <c:Length>24</c:Length>
        <c:Nonce>E/FnTId81s1yla31j1MjEA==</c:Nonce>
      </c:DerivedKeyToken>
      <c:DerivedKeyToken u:Id="_4" xmlns:c="http://schemas.xmlsoap.org/ws/2005/02/sc">
        <o:SecurityTokenReference k:TokenType="http://docs.oasis-open.org/wss/oasis-wss-soap-
message-security-1.1#EncryptedKey" xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-
wssecurity-secext-1.1.xsd">
          <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-
security-1.1#EncryptedKeySHA1" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-
1.0#Base64Binary">PjtWs6Qy28v7lLDPjDy0Q1H8pMg=</o:KeyIdentifier>
        </o:SecurityTokenReference>
        <c:Nonce>wPo+6LDobZWQjdnsMtM9kQ==</c:Nonce>
      </c:DerivedKeyToken>
      <e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:DataReference URI="#_6"></e:DataReference>
        <e:DataReference URI="#_9"></e:DataReference>
        <e:DataReference URI="#_10"></e:DataReference>
        <e:DataReference URI="#_11"></e:DataReference>
        <e:DataReference URI="#_12"></e:DataReference>
      </e:ReferenceList>
      <e:EncryptedData Id="_10" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
```

```
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:Reference URI="#_4"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>...qwwWg=</e:CipherValue>
        </e:CipherData>
      </e:EncryptedData>
      <e:EncryptedData Id="_11" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:Reference URI="#_4"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue...6KuM=</e:CipherValue>
        </e:CipherData>
      </e:EncryptedData>
      <e:EncryptedData Id="_12" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:Reference URI="#_4"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>...jnWd</e:CipherValue>
        </e:CipherData>
      </e:EncryptedData>
      <e:EncryptedData Id="_9" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:Reference URI="#_4"></o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>...NaE0</e:CipherValue>
        </e:CipherData>
      </e:EncryptedData>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_5">
    <e:EncryptedData Id="_6" Type="http://www.w3.org/2001/04/xmlenc#Content"
xmlns:e="http://www.w3.org/2001/04/xmlenc#">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></e:EncryptionMethod>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
```

```
          <o:Reference URI="#_4"></o:Reference>
        </o:SecurityTokenReference>
      </KeyInfo>
      <e:CipherData>
        <e:CipherValue>...K9Ow==</e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
```

4.6.2 Decrypted Body

```
<t:RequestSecurityTokenResponse Context="ProcessRequestSecurityToken"
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust">
  <t:Entropy>
    <t:BinarySecret>xLlswgvdA0KPhnTrkMfoC6vSG/tVASRu1jNb3iM+Fig=</t:BinarySecret>
  </t:Entropy>
  <t:KeySize>256</t:KeySize>
  <t:Lifetime>
    <wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2007-10-24T18:27:21.543Z</wsu:Created>
    <wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2007-10-25T02:27:21.543Z</wsu:Expires>
  </t:Lifetime>
  <t:RequestedSecurityToken>
    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
      <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#">
          <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            </e:EncryptionMethod>
            <KeyInfo>
              <o:SecurityTokenReference xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
                <X509Data>
                  <X509IssuerSerial>
                    <X509IssuerName>CN=Indigo Trusted Root</X509IssuerName>
                    <X509SerialNumber>-
452401585098136606784167449060769659 69</X509SerialNumber>
                  </X509IssuerSerial>
                </X509Data>
              </o:SecurityTokenReference>
            </KeyInfo>
            <e:CipherData>
              <e:CipherValue>...VaEQ=</e:CipherValue>
            </e:CipherData>
          </e:EncryptedKey>
      </KeyInfo>
      <xenc:CipherData>
        <xenc:CipherValue>
          ...hezQ==
        </xenc:CipherValue>
      </xenc:CipherData>
    </xenc:EncryptedData>
  </t:RequestedSecurityToken>
  <i:RequestedDisplayToken xmlns:i="http://schemas.xmlsoap.org/ws/2005/05/identity">
    <i:DisplayToken xml:lang="en-US">
      <i:DisplayClaim Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
```

```
        <i:DisplayTag>First Name</i:DisplayTag>
        <i:Description>A person's name which is not their surname nor middle
name</i:Description>
        <i:DisplayValue>Indigo</i:DisplayValue>
      </i:DisplayClaim>
      <i:DisplayClaim Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">
        <i:DisplayTag>Last Name</i:DisplayTag>
        <i:Description>The family name of a person</i:Description>
        <i:DisplayValue>Gauntlet</i:DisplayValue>
      </i:DisplayClaim>
      <i:DisplayClaim
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
        <i:DisplayTag>Email Address</i:DisplayTag>
        <i:Description>an electronic mailbox address of a person</i:Description>
        <i:DisplayValue>indgaunt@microsoft.com</i:DisplayValue>
      </i:DisplayClaim>
      <i:DisplayClaim
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier">
        <i:DisplayTag>PPID</i:DisplayTag>
        <i:Description>A private personal identifier</i:Description>
        <i:DisplayValue>l12onowarf2nfjsldfph+1-0332</i:DisplayValue>
      </i:DisplayClaim>
      <i:DisplayClaim
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authenticationtype">
        <i:DisplayValue>X509</i:DisplayValue>
      </i:DisplayClaim>
    </i:DisplayToken>
    </i:RequestedDisplayToken>
    <t:RequestedProofToken>
      <t:ComputedKey>http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1</t:ComputedKey>
    </t:RequestedProofToken>
    <t: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">_87b14d59-3459-4186-85e9-9b9fbb633e0b</o:KeyIdentifier>
      </o:SecurityTokenReference>
    </t:RequestedAttachedReference>
    <t: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">_87b14d59-3459-4186-85e9-9b9fbb633e0b</o:KeyIdentifier>
      </o:SecurityTokenReference>
    </t:RequestedUnattachedReference>
    <t:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV1.1</t:TokenType>
    <t:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Issue</t:RequestType>
    <t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</t:KeyType>
</t:RequestSecurityTokenResponse>
```

5 Security

5.1 Security Considerations for Implementers

The security considerations specified in [WSTrust1.3] section 12, [WSS] section 13, [WSSC] section 11, [WSSP] section 12, [WSSX509TP] section 4, [WSSUTP] section 4, and [WSTSPNego] section 5 apply to the CardSpace Security Token Acquisition Protocol. No further security considerations are necessary.

5.2 Index of Security Parameters

Security Parameter	Section
Security header element	3.6.4.1.2.2.1 and 3.6.4.1.2.2.2
Timestamp element	3.6.4.1.2.5 and 3.6.4.1.2.2.2
EncryptedKey element	3.6.4.1.2.6
DerivedKeyToken element	3.6.4.1.2.7 and 3.6.4.1.2.2.2
Signature element	3.6.4.1.2.8 and 3.6.4.1.2.2.2
SignatureConfirmation element	3.6.4.1.2.2.2
SecurityContextToken element	3.6.4.1.2.9
BinarySecurityToken element	3.6.4.1.2.10
UsernameToken element	3.6.4.1.2.11
Assertion element	3.6.4.1.2.16
EncryptedData element	3.6.4.1.2.1.1, 3.6.4.1.2.2.1 and 3.6.4.1.2.1.2

6 Appendix A: Full WSDL

For ease of implementation, the full WSDL and schema are provided in this appendix:

WSDL or schema name	Prefix	Section
Service Metadata Exchange WSDL and Schema	n/a	6.1
Message Protection Negotiation WSDL and Schema	n/a	6.2
Token Acquisition WSDL and Schema	n/a	6.3

For ease of implementation, the full WSDLs and schemas are provided in the following sections.

6.1 Service Metadata Exchange WSDL and Schema

6.1.1 WS-MetadataExchange WSDL

```
<wsdl:definitions
    targetNamespace='http://schemas.xmlsoap.org/ws/2004/09/mex'
    xmlns:tns='http://schemas.xmlsoap.org/ws/2004/09/mex'
    xmlns:wsa10='http://www.w3.org/2006/05/addressing/wsdl'
    xmlns:wsa04='http://schemas.xmlsoap.org/ws/2004/08/addressing'
    xmlns:wsdl='http://schemas.xmlsoap.org/wsdl/'
    xmlns:xs='http://www.w3.org/2001/XMLSchema' >
  <wsdl:types>
    <xs:schema
        targetNamespace='http://schemas.xmlsoap.org/ws/2004/09/mex' >
      <xs:include schemaLocation='MetadataExchange.xsd' />
    </xs:schema>
  </wsdl:types>
  <wsdl:message name='GetMetadataMsg' >
    <wsdl:part name='body' element='tns:GetMetadata' />
  </wsdl:message>
  <wsdl:message name='GetMetadataResponseMsg' >
    <wsdl:part name='body' element='tns:Metadata' />
  </wsdl:message>
  <wsdl:portType name='MetadataExchange' >
    <wsdl:operation name='GetMetadata' >
      <wsdl:input
       message='tns:GetMetadataMsg'
       wsa10:Action=
        'http://schemas.xmlsoap.org/ws/2004/09/mex/GetMetadata/Request'
       wsa04:Action=
        'http://schemas.xmlsoap.org/ws/2004/09/mex/GetMetadata/Request' />
      <wsdl:output
       message='tns:GetMetadataResponseMsg'
       wsa10:Action=
        'http://schemas.xmlsoap.org/ws/2004/09/mex/GetMetadata/Response'
       wsa04:Action=
        'http://schemas.xmlsoap.org/ws/2004/09/mex/GetMetadata/Response'/>
    </wsdl:operation>
  </wsdl:portType>
</wsdl:definitions>
```

6.1.2 WS-MetadataExchange Schema

```
<xs:schema
    targetNamespace='http://schemas.xmlsoap.org/ws/2004/09/mex'
    xmlns:tns='http://schemas.xmlsoap.org/ws/2004/09/mex'
    xmlns:wsa10='http://www.w3.org/2005/08/addressing'
    xmlns:wsa04='http://schemas.xmlsoap.org/ws/2004/08/addressing'
    xmlns:xs='http://www.w3.org/2001/XMLSchema'
    elementFormDefault='qualified'
    blockDefault='#all' >

  <!-- Get Metadata request -->
  <xs:element name='GetMetadata' >
    <xs:complexType>
      <xs:sequence>
        <xs:element ref='tns:Dialect' minOccurs='0' />
        <xs:element ref='tns:Identifier' minOccurs='0' />
      </xs:sequence>
      <xs:anyAttribute namespace='##other' processContents='lax' />
    </xs:complexType>
  </xs:element>

  <xs:element name='Dialect' type='xs:anyURI' />
  <xs:element name='Identifier' type='xs:anyURI' />

  <!-- Get Metadata response -->
  <xs:element name='Metadata' >
    <xs:complexType>
      <xs:sequence>
        <xs:element ref='tns:MetadataSection'
                    minOccurs='0'
                    maxOccurs='unbounded' />
        <xs:any namespace='##other' processContents='lax'
                minOccurs='0'
                maxOccurs='unbounded' />
      </xs:sequence>
      <xs:anyAttribute namespace='##other' processContents='lax' />
    </xs:complexType>
  </xs:element>
  <xs:element name='MetadataSection' >
    <xs:complexType>
      <xs:choice>
        <xs:any namespace='##other' processContents='lax' />
        <xs:element ref='tns:MetadataReference' />
        <xs:element ref='tns:Location' />
      </xs:choice>
      <xs:attribute name='Dialect' type='xs:anyURI' use='required' />
      <xs:attribute name='Identifier' type='xs:anyURI' />
      <xs:anyAttribute namespace='##other' processContents='lax' />
    </xs:complexType>
  </xs:element>
  <xs:element name='MetadataReference'>
    <xs:complexType>
      <xs:sequence>
        <xs:any minOccurs='1' maxOccurs='unbounded'
                processContents='lax' namespace='##other' />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
```

```
  <xs:element name='Location'
              type='xs:anyURI' />
</xs:schema>
```

6.2 Message Protection Negotiation WSDL and Schema

As specified in [WSTSPNego], this port type uses the WS-Trust WSDL and schema that may be found in [WSTrust1.3].

6.3 Token Acquisition WSDL and Schema

6.3.1 Token Acquisition WSDL

```
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions name="SecurityTokenService"
targetNamespace="http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:tns="http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice"
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: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="WindowsWSTrustBinding_IWSTrustFeb2005Async_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:SpnegoContextToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                  </wsp:Policy>
                </sp:SpnegoContextToken>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="WindowsWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_Input_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="WindowsWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_output_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="CustomBinding_IWSTrustFeb2005Async_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:SpnegoContextToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <wsp:Policy/>
            </sp:SpnegoContextToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
            <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
```

```
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="CustomBinding_IWSTrustFeb2005Async1_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <http:NegotiateAuthentication
xmlns:http="http://schemas.microsoft.com/ws/06/2004/policy/http"/>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict/>
              </wsp:Policy>
            </sp:Layout>
          </wsp:Policy>
        </sp:TransportBinding>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="CertificateWSTrustBinding_IWSTrustFeb2005Async_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
```

```
                <sp:Basic256/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <wsp:Policy>
                <sp:RequireThumbprintReference/>
                <sp:WssX509V3Token10/>
              </wsp:Policy>
            </sp:X509Token>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="CertificateWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_Input_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="CertificateWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_output_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="CertificateWSTrustBinding_IWSTrustFeb2005Async1_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
```

```
              <wsp:Policy>
                <sp:RequireThumbprintReference/>
                <sp:WssX509V3Token10/>
              </wsp:Policy>
            </sp:X509Token>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
            <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="CertificateWSTrustBinding_IWSTrustFeb2005Async2_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="true"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict/>
              </wsp:Policy>
            </sp:Layout>
          </wsp:Policy>
        </sp:TransportBinding>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="UserNameWSTrustBinding_IWSTrustFeb2005Async_policy">
```

```
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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:SignedSupportingTokens
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:UsernameToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <wsp:Policy>
                <sp:WssUsernameToken10/>
              </wsp:Policy>
            </sp:UsernameToken>
          </wsp:Policy>
        </sp:SignedSupportingTokens>
        <sp:EndorsingSupportingTokens
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
```

```
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="UserNameWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_Input_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="UserNameWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_output_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="UserNameWSTrustBinding_IWSTrustFeb2005Async1_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <http:BasicAuthentication
xmlns:http="http://schemas.microsoft.com/ws/06/2004/policy/http"/>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
```

```
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict/>
              </wsp:Policy>
            </sp:Layout>
          </wsp:Policy>
        </sp:TransportBinding>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="UserNameWSTrustBinding_IWSTrustFeb2005Async2_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict/>
              </wsp:Policy>
            </sp:Layout>
            <sp:IncludeTimestamp/>
          </wsp:Policy>
        </sp:TransportBinding>
        <sp:SignedSupportingTokens
  xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:UsernameToken
  sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
  cipient">
              <wsp:Policy>
                <sp:WssUsernameToken10/>
              </wsp:Policy>
            </sp:UsernameToken>
          </wsp:Policy>
        </sp:SignedSupportingTokens>
        <sp:EndorsingSupportingTokens
  xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
```

```
            <mssp:RsaToken
  sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
  wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
            <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="CustomBinding_IWSTrustFeb2005Async2_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic128/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:KerberosToken
  sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Once">
              <wsp:Policy>
                <sp:WssGssKerberosV5ApReqToken11/>
              </wsp:Policy>
            </sp:KerberosToken>
```

```
            <mssp:RsaToken
  sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
  wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
            <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token
  sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>
                <t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey</t:KeyType>
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#rsa-
sha1</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_Input_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_output_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async1_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>
                <t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey</t:KeyType>
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async1_TrustFeb2005IssueAsync_Input_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async1_TrustFeb2005IssueAsync_output_policy"
>
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async2_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>
                <t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey</t:KeyType>
```

```
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#rsa-
sha1</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
            <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async3_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>
                <t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey</t:KeyType>
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
            <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async4_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
```

```
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>

<t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</t:KeyType>
                <t:KeySize>256</t:KeySize>
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-cbc</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#hmac-
sha1</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
            <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
```

```
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async5_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>

<t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</t:KeyType>
                <t:KeySize>256</t:KeySize>
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-cbc</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#hmac-
sha256</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
            <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
```

```
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async6_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>

<t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</t:KeyType>
                <t:KeySize>256</t:KeySize>
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-cbc</t:EncryptWith>
```

```
                <t:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#hmac-
sha1</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async6_TrustFeb2005IssueAsync_Input_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async6_TrustFeb2005IssueAsync_output_policy"
>
```

```
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async7_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>

<t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</t:KeyType>
```

```
                <t:KeySize>256</t:KeySize>
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-cbc</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#hmac-
sha256</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async7_TrustFeb2005IssueAsync_Input_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
```

```
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async7_TrustFeb2005IssueAsync_output_policy"
>
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async8_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:TripleDes/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
```

```
              <sp:RequestSecurityTokenTemplate>

  <t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</t:KeyType>
                <t:KeySize>192</t:KeySize>
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#tripledes-cbc</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#hmac-
  sha1</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
  c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-
  cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
  sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
  wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
  wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async8_TrustFeb2005IssueAsync_Input_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
```

```
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async8_TrustFeb2005IssueAsync_output_policy"
>
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async9_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SymmetricBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:TripleDesSha256/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
```

```
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>

<t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</t:KeyType>
                <t:KeySize>192</t:KeySize>
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#tripledes-cbc</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#hmac-
sha256</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sp:Wss11 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async9_TrustFeb2005IssueAsync_Input_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
```

```
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async9_TrustFeb2005IssueAsync_output_policy"
>
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async10_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:TripleDes/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>

<t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</t:KeyType>
                <t:KeySize>192</t:KeySize>
```

```
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#tripledes-cbc</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#hmac-
sha1</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
            <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async11_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:TripleDesSha256/>
              </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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRe
cipient">
              <sp:RequestSecurityTokenTemplate>

<t:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</t:KeyType>
                <t:KeySize>192</t:KeySize>
                <t:EncryptWith>http://www.w3.org/2001/04/xmlenc#tripledes-cbc</t:EncryptWith>
                <t:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#hmac-
sha256</t:SignatureAlgorithm>
                <t:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</t:CanonicalizationAlgorithm>
                <t:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</t:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <mssp:RsaToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never"
wsp:Optional="true" xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy"/>
            <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://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:Trust10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:MustSupportIssuedTokens/>
            <sp:RequireClientEntropy/>
            <sp:RequireServerEntropy/>
          </wsp:Policy>
        </sp:Trust10>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="CustomBinding_IWSTrust13Async_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <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:Basic128/>
            </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:KerberosToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Once">
            <wsp:Policy>
              <sp:WssGssKerberosV5ApReqToken11/>
            </wsp:Policy>
          </sp:KerberosToken>
          <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never" wsp:Optional="true"/>
          <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>
<wsp:Policy wsu:Id="CertificateWSTrustBinding_IWSTrust13Async_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:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <wsp:Policy>
                <sp:RequireThumbprintReference/>
                <sp:WssX509V3Token10/>
              </wsp:Policy>
            </sp:X509Token>
            <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:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </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>
```

```
  <wsp:Policy
wsu:Id="CertificateWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_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="CertificateWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_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="CertificateWSTrustBinding_IWSTrust13Async1_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <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:Basic256/>
              </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:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <wsp:Policy>
                <sp:RequireThumbprintReference/>
                <sp:WssX509V3Token10/>
              </wsp:Policy>
            </sp:X509Token>
            <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never" wsp:Optional="true"/>
            <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>
  <wsp:Policy wsu:Id="CertificateWSTrustBinding_IWSTrust13Async2_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="true"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
```

```
              <wsp:Policy>
                <sp:Strict/>
              </wsp:Policy>
            </sp:Layout>
          </wsp:Policy>
        </sp:TransportBinding>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="UserNameWSTrustBinding_IWSTrust13Async_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:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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:SignedEncryptedSupportingTokens xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
          <wsp:Policy>
            <sp:UsernameToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <wsp:Policy>
                <sp:WssUsernameToken10/>
              </wsp:Policy>
            </sp:UsernameToken>
          </wsp:Policy>
        </sp:SignedEncryptedSupportingTokens>
        <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: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>
  <wsp:Policy wsu:Id="UserNameWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_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="UserNameWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_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="UserNameWSTrustBinding_IWSTrust13Async1_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <http:BasicAuthentication
xmlns:http="http://schemas.microsoft.com/ws/06/2004/policy/http"/>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict/>
              </wsp:Policy>
            </sp:Layout>
          </wsp:Policy>
        </sp:TransportBinding>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="UserNameWSTrustBinding_IWSTrust13Async2_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <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:Basic256/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict/>
              </wsp:Policy>
            </sp:Layout>
            <sp:IncludeTimestamp/>
          </wsp:Policy>
        </sp:TransportBinding>
        <sp:SignedEncryptedSupportingTokens xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
          <wsp:Policy>
```

```
            <sp:UsernameToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <wsp:Policy>
                <sp:WssUsernameToken10/>
              </wsp:Policy>
            </sp:UsernameToken>
          </wsp:Policy>
        </sp:SignedEncryptedSupportingTokens>
        <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"/>
            <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>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async_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:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/PublicKey</trust:KeyType>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#rsa-
sha1</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <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:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </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>
```

```
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async1_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:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/PublicKey</trust:KeyType>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <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:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </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>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async1_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async1_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async2_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <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:Basic256/>
              </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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/PublicKey</trust:KeyType>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#rsa-
sha1</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never" wsp:Optional="true"/>
            <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>
```

```
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async3_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/PublicKey</trust:KeyType>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never" wsp:Optional="true"/>
            <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>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async4_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <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:Basic256/>
              </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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/SymmetricKey</trust:KeyType>
                <trust:KeySize>256</trust:KeySize>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#hmac-
sha1</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
```

```
            </sp:IssuedToken>
            <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never" wsp:Optional="true"/>
            <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>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async5_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/SymmetricKey</trust:KeyType>
```

```
                <trust:KeySize>256</trust:KeySize>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#hmac-
sha256</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never" wsp:Optional="true"/>
            <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>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async6_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:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
```

```
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/SymmetricKey</trust:KeyType>
                <trust:KeySize>256</trust:KeySize>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#hmac-
sha1</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <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:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </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>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async6_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async6_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async7_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:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
```

```
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/SymmetricKey</trust:KeyType>
                <trust:KeySize>256</trust:KeySize>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#hmac-
sha256</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <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:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </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>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async7_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async7_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async8_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:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:TripleDes/>
              </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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/SymmetricKey</trust:KeyType>
                <trust:KeySize>192</trust:KeySize>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#hmac-
sha1</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <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:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
```

```
            <sp:RequireSignatureConfirmation/>
          </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>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async8_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async8_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async9_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:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:RequireDerivedKeys/>
                    <sp:RequireThumbprintReference/>
                    <sp:WssX509V3Token10/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:TripleDesSha256/>
              </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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/SymmetricKey</trust:KeyType>
                <trust:KeySize>192</trust:KeySize>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#hmac-
sha256</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireDerivedKeys/>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <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:MustSupportRefKeyIdentifier/>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
            <sp:RequireSignatureConfirmation/>
          </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>
  <wsp:Policy
wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async9_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async9_Trust13IssueAsync_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="IssuedTokenWSTrustBinding_IWSTrust13Async10_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <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:TripleDes/>
              </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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/SymmetricKey</trust:KeyType>
                <trust:KeySize>192</trust:KeySize>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#hmac-
sha1</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never" wsp:Optional="true"/>
            <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>
  <wsp:Policy wsu:Id="IssuedTokenWSTrustBinding_IWSTrust13Async11_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <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:TripleDesSha256/>
              </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:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <sp:RequestSecurityTokenTemplate>
                <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/SymmetricKey</trust:KeyType>
                <trust:KeySize>192</trust:KeySize>
                <trust:KeyWrapAlgorithm>http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p</trust:KeyWrapAlgorithm>
                <trust:EncryptWith>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</trust:EncryptWith>
                <trust:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#hmac-
sha256</trust:SignatureAlgorithm>
                <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-
cbc</trust:EncryptionAlgorithm>
              </sp:RequestSecurityTokenTemplate>
```

```
              <wsp:Policy>
                <sp:RequireInternalReference/>
              </wsp:Policy>
            </sp:IssuedToken>
            <sp:KeyValueToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never" wsp:Optional="true"/>
            <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>
  <wsp:Policy wsu:Id="WindowsWSTrustBinding_IWSTrust13Async_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:Basic256/>
              </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: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>
  <wsp:Policy wsu:Id="WindowsWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_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="WindowsWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_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="CustomBinding_IWSTrust13Async1_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <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:Basic256/>
              </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"/>
            <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>
  <wsp:Policy wsu:Id="CustomBinding_IWSTrust13Async2_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <http:NegotiateAuthentication
xmlns:http="http://schemas.microsoft.com/ws/06/2004/policy/http"/>
        <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken RequireClientCertificate="false"/>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic256/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict/>
              </wsp:Policy>
            </sp:Layout>
          </wsp:Policy>
        </sp:TransportBinding>
        <wsaw:UsingAddressing/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsdl:types>
    <xsd:schema
targetNamespace="http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice/Import
s">
      <xsd:import schemaLocation="https://adfsdemo.com/adfs/services/trust/mex?xsd=xsd0"
namespace="http://schemas.microsoft.com/Message"/>
      <xsd:import schemaLocation="https://adfsdemo.com/adfs/services/trust/mex?xsd=xsd1"
namespace="http://schemas.xmlsoap.org/ws/2005/02/trust"/>
      <xsd:import schemaLocation="https://adfsdemo.com/adfs/services/trust/mex?xsd=xsd2"
namespace="http://docs.oasis-open.org/ws-sx/ws-trust/200512"/>
    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="IWSTrustFeb2005Async_TrustFeb2005IssueAsync_InputMessage">
    <wsdl:part name="request" element="t:RequestSecurityToken"/>
  </wsdl:message>
  <wsdl:message name="IWSTrustFeb2005Async_TrustFeb2005IssueAsync_OutputMessage">
    <wsdl:part name="TrustFeb2005IssueAsyncResult" element="t:RequestSecurityTokenResponse"/>
```

```
  </wsdl:message>
  <wsdl:message name="IWSTrust13Async_Trust13IssueAsync_InputMessage">
    <wsdl:part name="request" element="trust:RequestSecurityToken"/>
  </wsdl:message>
  <wsdl:message name="IWSTrust13Async_Trust13IssueAsync_OutputMessage">
    <wsdl:part name="Trust13IssueAsyncResult"
element="trust:RequestSecurityTokenResponseCollection"/>
  </wsdl:message>
  <wsdl:portType name="IWSTrustFeb2005Async">
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <wsdl:input wsaw:Action="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
message="tns:IWSTrustFeb2005Async_TrustFeb2005IssueAsync_InputMessage"/>
      <wsdl:output wsaw:Action="http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue"
message="tns:IWSTrustFeb2005Async_TrustFeb2005IssueAsync_OutputMessage"/>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:portType name="IWSTrust13Async">
    <wsdl:operation name="Trust13IssueAsync">
      <wsdl:input wsaw:Action="http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue"
message="tns:IWSTrust13Async_Trust13IssueAsync_InputMessage"/>
      <wsdl:output wsaw:Action="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RSTRC/IssueFinal"
message="tns:IWSTrust13Async_Trust13IssueAsync_OutputMessage"/>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="WindowsWSTrustBinding_IWSTrustFeb2005Async"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#WindowsWSTrustBinding_IWSTrustFeb2005Async_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#WindowsWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#WindowsWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="CustomBinding_IWSTrustFeb2005Async" type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#CustomBinding_IWSTrustFeb2005Async_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="CustomBinding_IWSTrustFeb2005Async1" type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#CustomBinding_IWSTrustFeb2005Async1_policy"/>
```

```
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="CertificateWSTrustBinding_IWSTrustFeb2005Async"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#CertificateWSTrustBinding_IWSTrustFeb2005Async_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#CertificateWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#CertificateWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="CertificateWSTrustBinding_IWSTrustFeb2005Async1"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#CertificateWSTrustBinding_IWSTrustFeb2005Async1_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="CertificateWSTrustBinding_IWSTrustFeb2005Async2"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#CertificateWSTrustBinding_IWSTrustFeb2005Async2_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
```

```
  </wsdl:binding>
  <wsdl:binding name="UserNameWSTrustBinding_IWSTrustFeb2005Async"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#UserNameWSTrustBinding_IWSTrustFeb2005Async_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#UserNameWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#UserNameWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="UserNameWSTrustBinding_IWSTrustFeb2005Async1"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#UserNameWSTrustBinding_IWSTrustFeb2005Async1_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="UserNameWSTrustBinding_IWSTrustFeb2005Async2"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#UserNameWSTrustBinding_IWSTrustFeb2005Async2_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="CustomBinding_IWSTrustFeb2005Async2" type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#CustomBinding_IWSTrustFeb2005Async2_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
```

```
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async_TrustFeb2005IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async1"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async1_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async1_TrustFeb2005IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async1_TrustFeb2005IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async2"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async2_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async3"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async3_policy"/>
```

```
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async4"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async4_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async5"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async5_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async6"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async6_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async6_TrustFeb2005IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async6_TrustFeb2005IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
```

```
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async7"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async7_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async7_TrustFeb2005IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async7_TrustFeb2005IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async8"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async8_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async8_TrustFeb2005IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async8_TrustFeb2005IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async9"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async9_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async9_TrustFeb2005IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async9_TrustFeb2005IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async10"
type="tns:IWSTrustFeb2005Async">
```

```
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async10_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async11"
type="tns:IWSTrustFeb2005Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrustFeb2005Async11_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="TrustFeb2005IssueAsync">
      <soap12:operation soapAction="http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="CustomBinding_IWSTrust13Async" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#CustomBinding_IWSTrust13Async_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="CertificateWSTrustBinding_IWSTrust13Async" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#CertificateWSTrustBinding_IWSTrust13Async_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue" style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#CertificateWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#CertificateWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
```

```
  </wsdl:binding>
  <wsdl:binding name="CertificateWSTrustBinding_IWSTrust13Async1" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#CertificateWSTrustBinding_IWSTrust13Async1_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="CertificateWSTrustBinding_IWSTrust13Async2" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#CertificateWSTrustBinding_IWSTrust13Async2_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="UserNameWSTrustBinding_IWSTrust13Async" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#UserNameWSTrustBinding_IWSTrust13Async_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue" style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#UserNameWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#UserNameWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="UserNameWSTrustBinding_IWSTrust13Async1" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#UserNameWSTrustBinding_IWSTrust13Async1_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="UserNameWSTrustBinding_IWSTrust13Async2" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#UserNameWSTrustBinding_IWSTrust13Async2_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue" style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async1" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async1_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue" style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async1_Trust13IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async1_Trust13IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async2" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async2_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async3" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async3_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async4" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async4_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async5" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async5_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async6" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async6_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue" style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async6_Trust13IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
```

```
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async6_Trust13IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async7" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async7_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue" style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async7_Trust13IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async7_Trust13IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async8" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async8_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue" style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async8_Trust13IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async8_Trust13IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async9" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async9_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue" style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async9_Trust13IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#IssuedTokenWSTrustBinding_IWSTrust13Async9_Trust13IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
```

```
  </wsdl:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async10"
type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async10_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="IssuedTokenWSTrustBinding_IWSTrust13Async11"
type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#IssuedTokenWSTrustBinding_IWSTrust13Async11_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="WindowsWSTrustBinding_IWSTrust13Async" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#WindowsWSTrustBinding_IWSTrust13Async_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue" style="document"/>
      <wsdl:input>
        <wsp:PolicyReference
URI="#WindowsWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_Input_policy"/>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <wsp:PolicyReference
URI="#WindowsWSTrustBinding_IWSTrust13Async_Trust13IssueAsync_output_policy"/>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="CustomBinding_IWSTrust13Async1" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#CustomBinding_IWSTrust13Async1_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:binding name="CustomBinding_IWSTrust13Async2" type="tns:IWSTrust13Async">
    <wsp:PolicyReference URI="#CustomBinding_IWSTrust13Async2_policy"/>
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Trust13IssueAsync">
      <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:binding>
  <wsdl:service name="SecurityTokenService">
    <wsdl:port name="WindowsWSTrustBinding_IWSTrustFeb2005Async"
binding="tns:WindowsWSTrustBinding_IWSTrustFeb2005Async">
      <soap12:address location="http://adfsdemo.com/adfs/services/trust/2005/windows"/>
      <wsa10:EndpointReference>
        <wsa10:Address>http://adfsdemo.com/adfs/services/trust/2005/windows</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <Upn>adfsaccount@adac.com</Upn>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CustomBinding_IWSTrustFeb2005Async"
binding="tns:CustomBinding_IWSTrustFeb2005Async">
      <soap12:address location="https://adfsdemo.com/adfs/services/trust/2005/windowsmixed"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/windowsmixed</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CustomBinding_IWSTrustFeb2005Async1"
binding="tns:CustomBinding_IWSTrustFeb2005Async1">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/windowstransport"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/windowstransport</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <Upn>adfsaccount@adac.com</Upn>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CertificateWSTrustBinding_IWSTrustFeb2005Async"
binding="tns:CertificateWSTrustBinding_IWSTrustFeb2005Async">
      <soap12:address location="http://adfsdemo.com/adfs/services/trust/2005/certificate"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/2005/certificate</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
```

```
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CertificateWSTrustBinding_IWSTrustFeb2005Async1"
binding="tns:CertificateWSTrustBinding_IWSTrustFeb2005Async1">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/certificatemixed"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/certificatemixed</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CertificateWSTrustBinding_IWSTrustFeb2005Async2"
binding="tns:CertificateWSTrustBinding_IWSTrustFeb2005Async2">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/certificatetransport"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/certificatetransport</wsa10:Addr
ess>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="UserNameWSTrustBinding_IWSTrustFeb2005Async"
binding="tns:UserNameWSTrustBinding_IWSTrustFeb2005Async">
      <soap12:address location="http://adfsdemo.com/adfs/services/trust/2005/username"/>
      <wsa10:EndpointReference>
        <wsa10:Address>http://adfsdemo.com/adfs/services/trust/2005/username</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="UserNameWSTrustBinding_IWSTrustFeb2005Async1"
binding="tns:UserNameWSTrustBinding_IWSTrustFeb2005Async1">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/usernamebasictransport"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/usernamebasictransport</wsa10:Ad
dress>
      </wsa10:EndpointReference>
    </wsdl:port>
```

```
    <wsdl:port name="UserNameWSTrustBinding_IWSTrustFeb2005Async2"
binding="tns:UserNameWSTrustBinding_IWSTrustFeb2005Async2">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/usernamemixed"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/usernamemixed</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CustomBinding_IWSTrustFeb2005Async2"
binding="tns:CustomBinding_IWSTrustFeb2005Async2">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/kerberosmixed"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/kerberosmixed</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/2005/issuedtokenasymmetricbasic256"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/2005/issuedtokenasymmetricbasic256</ws
a10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async1"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async1">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/2005/issuedtokenasymmetricbasic256sha256"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/2005/issuedtokenasymmetricbasic256sha2
56</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
```

```
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async2"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async2">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedasymmetricbasic256"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedasymmetricbasic2
56</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async3"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async3">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedasymmetricbasic256sha
256"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedasymmetricbasic2
56sha256</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async4"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async4">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedsymmetricbasic256"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedsymmetricbasic25
6</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async5"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async5">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedsymmetricbasic256sha2
56"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedsymmetricbasic25
6sha256</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async6"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async6">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/2005/issuedtokensymmetricbasic256"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/2005/issuedtokensymmetricbasic256</wsa
10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
```

```
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async7"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async7">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/2005/issuedtokensymmetricbasic256sha256"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/2005/issuedtokensymmetricbasic256sha25
6</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async8"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async8">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/2005/issuedtokensymmetrictripledes"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/2005/issuedtokensymmetrictripledes</ws
a10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
```

```
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async9"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async9">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/2005/issuedtokensymmetrictripledessha256"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/2005/issuedtokensymmetrictripledessha2
56</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async10"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async10">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedsymmetrictripledes"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedsymmetrictripled
es</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrustFeb2005Async11"
binding="tns:IssuedTokenWSTrustBinding_IWSTrustFeb2005Async11">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedsymmetrictripledessha
256"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/2005/issuedtokenmixedsymmetrictripled
essha256</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CustomBinding_IWSTrust13Async"
binding="tns:CustomBinding_IWSTrust13Async">
      <soap12:address location="https://adfsdemo.com/adfs/services/trust/13/kerberosmixed"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/kerberosmixed</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CertificateWSTrustBinding_IWSTrust13Async"
binding="tns:CertificateWSTrustBinding_IWSTrust13Async">
      <soap12:address location="http://adfsdemo.com/adfs/services/trust/13/certificate"/>
      <wsa10:EndpointReference>
        <wsa10:Address>http://adfsdemo.com/adfs/services/trust/13/certificate</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
```

```
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CertificateWSTrustBinding_IWSTrust13Async1"
binding="tns:CertificateWSTrustBinding_IWSTrust13Async1">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/13/certificatemixed"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/certificatemixed</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CertificateWSTrustBinding_IWSTrust13Async2"
binding="tns:CertificateWSTrustBinding_IWSTrust13Async2">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/13/certificatetransport"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/certificatetransport</wsa10:Addres
s>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="UserNameWSTrustBinding_IWSTrust13Async"
binding="tns:UserNameWSTrustBinding_IWSTrust13Async">
      <soap12:address location="http://adfsdemo.com/adfs/services/trust/13/username"/>
      <wsa10:EndpointReference>
        <wsa10:Address>http://adfsdemo.com/adfs/services/trust/13/username</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="UserNameWSTrustBinding_IWSTrust13Async1"
binding="tns:UserNameWSTrustBinding_IWSTrust13Async1">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/13/usernamebasictransport"/>
      <wsa10:EndpointReference>
```

```
<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/usernamebasictransport</wsa10:Addr
ess>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="UserNameWSTrustBinding_IWSTrust13Async2"
binding="tns:UserNameWSTrustBinding_IWSTrust13Async2">
      <soap12:address location="https://adfsdemo.com/adfs/services/trust/13/usernamemixed"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/usernamemixed</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/13/issuedtokenasymmetricbasic256"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/13/issuedtokenasymmetricbasic256</wsa1
0:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async1"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async1">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/13/issuedtokenasymmetricbasic256sha256"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/13/issuedtokenasymmetricbasic256sha256
</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
```

```
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async2"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async2">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedasymmetricbasic256"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedasymmetricbasic256
</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async3"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async3">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedasymmetricbasic256sha25
6"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedasymmetricbasic256
sha256</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async4"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async4">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256<
/wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async5"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async5">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256sha256
"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256s
ha256</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async6"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async6">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/13/issuedtokensymmetricbasic256"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/13/issuedtokensymmetricbasic256</wsa10
:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
```

```
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async7"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async7">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/13/issuedtokensymmetricbasic256sha256"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/13/issuedtokensymmetricbasic256sha256<
/wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async8"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async8">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/13/issuedtokensymmetrictripledes"/>
      <wsa10:EndpointReference>

<wsa10:Address>http://adfsdemo.com/adfs/services/trust/13/issuedtokensymmetrictripledes</wsa1
0:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async9"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async9">
      <soap12:address
location="http://adfsdemo.com/adfs/services/trust/13/issuedtokensymmetrictripledessha256"/>
      <wsa10:EndpointReference>
```

```
<wsa10:Address>http://adfsdemo.com/adfs/services/trust/13/issuedtokensymmetrictripledessha256
</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Data>

<X509Certificate>MIIB4TCCAUqgAwIBAgIQaMhYkGS9hrtJWrQzgG7OEjANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQD
EwxhZGZzZGVtby5jb20wHhcNMTAwNzI5MDAyNzI5WhcNMTEwNzI5MDYyNzI5WjAXMRUwEwYDVQQDEwxhZGZzZGVtby5jb
20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALtG7RzWvLEo09ulSMYxkXUw+nkCm4cTZ1NjhdZc23qmSRLhgPrDEZ
EjwfBapyUxyd1idKqWbAuAU8V+xtmM72ZzptYSQq7E36tfmChW3yThxPTM2/LO6eeOovhBTIaN/YnEa9KvrQdkfy+uR1h
3rd+8s3AHe8squ/3dCMF51Pk1AgMBAAGjLjAsMAsGA1UdDwQEAwIE8DAdBgNVHQ4EFgQUG8Esvlu55YffghMb6aQ05k/g
vBYwDQYJKoZIhvcNAQEFBQADgYEAOSTveJrM6NZkccqnlh4cXxQdKGmPfRP56BqnSNl1jGgNVCezgk/XHrjItt8Tfnyb9
bB4JTHye3BqVuXAC0sF9G8ggPEkbG84OHp7CFUhkY/InSJ0SuriRUbb5IWIsm684DwpJxKXbz3du+AixAa9S07oQtymMo
kGqKjYWRd0Fg8=</X509Certificate>
            </X509Data>
          </KeyInfo>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async10"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async10">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes
</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="IssuedTokenWSTrustBinding_IWSTrust13Async11"
binding="tns:IssuedTokenWSTrustBinding_IWSTrust13Async11">
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedsymmetrictripledessha25
6"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes
sha256</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="WindowsWSTrustBinding_IWSTrust13Async"
binding="tns:WindowsWSTrustBinding_IWSTrust13Async">
      <soap12:address location="http://adfsdemo.com/adfs/services/trust/13/windows"/>
      <wsa10:EndpointReference>
        <wsa10:Address>http://adfsdemo.com/adfs/services/trust/13/windows</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <Upn>adfsaccount@adac.com</Upn>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CustomBinding_IWSTrust13Async1"
binding="tns:CustomBinding_IWSTrust13Async1">
      <soap12:address location="https://adfsdemo.com/adfs/services/trust/13/windowsmixed"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/windowsmixed</wsa10:Address>
      </wsa10:EndpointReference>
    </wsdl:port>
    <wsdl:port name="CustomBinding_IWSTrust13Async2"
binding="tns:CustomBinding_IWSTrust13Async2">
```

```
      <soap12:address
location="https://adfsdemo.com/adfs/services/trust/13/windowstransport"/>
      <wsa10:EndpointReference>

<wsa10:Address>https://adfsdemo.com/adfs/services/trust/13/windowstransport</wsa10:Address>
        <Identity xmlns="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity">
          <Upn>adfsaccount@adac.com</Upn>
        </Identity>
      </wsa10:EndpointReference>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

6.3.2 Schema for http://schemas.microsoft.com/Message

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified"
targetNamespace="http://schemas.microsoft.com/Message"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://schemas.microsoft.com/Message">
  <xs:complexType name="MessageBody">
    <xs:sequence>
      <xs:any minOccurs="0" maxOccurs="unbounded" namespace="##any"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

6.3.3 Schema for http://schemas.xmlsoap.org/ws/2005/02/trust

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified"
targetNamespace="http://schemas.xmlsoap.org/ws/2005/02/trust"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust">
  <xs:element name="RequestSecurityToken" type="wst:RequestSecurityTokenType"/>
  <xs:complexType name="RequestSecurityTokenType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:any minOccurs="0" maxOccurs="unbounded" namespace="##any" processContents="lax"/>
    </xs:choice>
    <xs:attribute name="Context" type="xs:anyURI" use="optional"/>
    <xs:anyAttribute namespace="##other" processContents="lax"/>
  </xs:complexType>
  <xs:element name="RequestSecurityTokenResponse"
type="wst:RequestSecurityTokenResponseType"/>
  <xs:complexType name="RequestSecurityTokenResponseType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:any minOccurs="0" maxOccurs="unbounded" namespace="##any" processContents="lax"/>
    </xs:choice>
    <xs:attribute name="Context" type="xs:anyURI" use="optional"/>
    <xs:anyAttribute namespace="##other" processContents="lax"/>
  </xs:complexType>
</xs:schema>
```

6.3.4 Schema for http://docs.oasis-open.org/ws-sx/ws-trust/200512

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<xs:schema elementFormDefault="qualified" targetNamespace="http://docs.oasis-open.org/ws-
sx/ws-trust/200512" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
  <xs:element name="RequestSecurityToken" type="trust:RequestSecurityTokenType"/>
  <xs:complexType name="RequestSecurityTokenType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:any minOccurs="0" maxOccurs="unbounded" namespace="##any" processContents="lax"/>
    </xs:choice>
    <xs:attribute name="Context" type="xs:anyURI" use="optional"/>
    <xs:anyAttribute namespace="##other" processContents="lax"/>
  </xs:complexType>
  <xs:element name="RequestSecurityTokenResponse"
type="trust:RequestSecurityTokenResponseType"/>
  <xs:complexType name="RequestSecurityTokenResponseType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:any minOccurs="0" maxOccurs="unbounded" namespace="##any" processContents="lax"/>
    </xs:choice>
    <xs:attribute name="Context" type="xs:anyURI" use="optional"/>
    <xs:anyAttribute namespace="##other" processContents="lax"/>
  </xs:complexType>
  <xs:element name="RequestSecurityTokenResponseCollection"
type="trust:RequestSecurityTokenResponseCollectionType"/>
  <xs:complexType name="RequestSecurityTokenResponseCollectionType">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="unbounded"
ref="trust:RequestSecurityTokenResponse"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##other" processContents="lax"/>
  </xs:complexType>
</xs:schema>
```

7 Appendix B: Product Behavior

This document specifies version-specific details in the Microsoft® .NET Framework. For information about which versions of .NET Framework are available in each released Microsoft Windows® product or as supplemental software, see **.NET Framework**.

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Active Directory Federation Services (ADFS) 2.0
- Microsoft® .NET Framework 3.0
- Microsoft® .NET Framework 3.5
- Windows CardSpace™ 1.0
- Windows CardSpace™ 2.0
- Windows Vista® operating system
- Windows® 7 operating system
- Windows Server® 2008 operating system
- Windows Server® 2008 R2 operating system

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.

<1> Section 3.2.4.1: The Active Directory Federation Services (ADFS) 2.0 STS implements endpoints for both types of Service Metadata Exchange messages.

<2> Section 3.2.4.1.1.2.1: Windows Behavior for CardSpace to Active Directory Federation Services (ADFS) 2.0 Exchanges:

Active Directory Federation Services (ADFS) 2.0 supports only the TripleDes and Basic256 algorithm sets.

<3> Section 3.2.4.1.1.2.1: Active Directory Federation Services (ADFS) 2.0 returns a SOAP fault message if the current time is greater than the time in the <Expires> element.

<4> Section 3.2.4.1.1.2.1: Active Directory Federation Services (ADFS) 2.0 chooses a time of current time plus 5 minutes for the <Expires> element.

<5> Section 3.2.4.1.1.2.1: PA16 and PA17 are always produced together on Active Directory Federation Services (ADFS) 2.0.

<6> Section 3.2.4.1.1.2.1: Active Directory Federation Services (ADFS) 2.0 uses two <DerivedKeyToken> elements.

<7> Section 3.2.4.1.1.2.1: For CardSpace exchanges, Active Directory Federation Services (ADFS) 2.0 only supports the TripleDes and Basic256 algorithm sets specified in section 7.1 of [WSSP]. No other algorithm sets are supported.

<8> Section 3.2.4.1.1.2.1: For CardSpace exchanges, Active Directory Federation Services (ADFS) 2.0 only supports the TripleDes and Basic256 algorithm sets specified in section 7.1 of [WSSP]. No other algorithm sets are supported.

<9> Section 3.2.4.1.1.2.1: Active Directory Federation Services (ADFS) 2.0 returns a SOAP fault message if the current time is greater than the time in the <Expires> element.

<10> Section 3.2.4.1.1.2.1: Active Directory Federation Services (ADFS) 2.0 chooses a time of current time plus 5 minutes for the <Expires> element.

<11> Section 3.2.4.1.1.2.1: Active Directory Federation Services (ADFS) 2.0 will fault if a message is received that does not include the full X.509 certificate used by the client, even if that certificate is referenced using a thumbprint. Therefore, PA28 does not have an effect on the message exchanges between a Windows client and Active Directory Federation Services (ADFS) 2.0.

<12> Section 3.2.4.1.1.2.1: Active Directory Federation Services (ADFS) 2.0 only emits key specific identifiers when PA27 or PA40 is also present.

<13> Section 3.2.4.1.1.2.1: Active Directory Federation Services (ADFS) 2.0 does not emit issuer and serial number references.

<14> Section 3.2.4.1.1.2.1: Active Directory Federation Services (ADFS) 2.0 emits X509 thumbprint references.

<15> Section 3.2.4.1.1.2.1: When an endpoint with assertion PA03 is used, Active Directory Federation Services (ADFS) 2.0 will use an <EncryptedKey> element reference in the response message to refer to the <EncryptedKey> element included in the request message.

<16> Section 3.2.4.1.1.2.1: Windows CardSpace 1.0 uses "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal" while Windows CardSpace 2.0 uses "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Issue".

<17> Section 3.2.4.1.2.3: The Windows CardSpace 1.0 client software shipped with .NET Framework 3.0 and .NET Framework 3.5.

Windows CardSpace 1.0 and Windows CardSpace 2.0 client software communicates with ADFS 2.0.

Windows Server 2008 and Windows Server 2008 R2 implement ADFS 2.0.

Windows CardSpace 1.0 requires that an endpoint with assertions PA03 and PA33 MUST have no <Identity>, or MUST have an <Identity> of a <Dns> element specified in [WSAIdentity] section 3.1 or an <Spn> element specified in [WSAIdentity] section 3.2 in the metadata.

ADFS 2.0 never includes an <Identity> for an endpoint with assertions PA03 and PA33.

Windows CardSpace 1.0 requires that an endpoint with assertions PA03 and PA30 MUST have no <Identity>, or MUST have an <Identity> of a <Dns> element specified in [WSAIdentity] section 3.1 or an <Spn> element specified in [WSAIdentity] section 3.2 in the metadata.

ADFS 2.0 never includes an <Identity> for an endpoint with assertions PA03 and PA30.

Windows CardSpace 1.0 requires that an endpoint with assertion PA16 MUST have no <Identity>, or MUST have an <Identity> of a <Dns> element specified in [WSAIdentity] section 3.1 or an <Spn> element specified in [WSAIdentity] section 3.2 in the metadata.

ADFS 2.0 includes an <Identity> of an <Spn> element specified in [WSAIdentity] section 3.2 for an endpoint with assertion PA16.

Windows CardSpace 1.0 requires that an endpoint with assertions PA03 and PA40 MUST have an <Identity> of a <KeyInfo> element specified in [XMLDSig/2002] section 4.4.

ADFS 2.0 never includes an <Identity> for an endpoint with assertions PA03 and PA40.

Windows CardSpace 1.0 requires that an endpoint with assertions PA12 and PA40 MUST have an <Identity> of a <KeyInfo> element specified in [XMLDSig/2002] section 4.4.

ADFS 2.0 includes an <Identity> of a <KeyInfo> element specified in [XMLDSig/2002] section 4.4 for an endpoint with assertions PA12 and PA40.

Windows CardSpace 1.0 requires that an endpoint with assertions PA03 and PA27 MUST have an <Identity> of a <KeyInfo> element specified in [XMLDSig/2002] section 4.4.

ADFS 2.0 never includes an <Identity> for an endpoint with assertions PA03 and PA27.

Windows CardSpace 1.0 requires that an endpoint with assertions PA12 and PA27 MUST have an <Identity> of a <KeyInfo> element specified in [XMLDSig/2002] section 4.4.

ADFS 2.0 includes an <Identity> of a <KeyInfo> element specified in [XMLDSig/2002] section 4.4 for an endpoint with assertions PA12 and PA27.

Windows CardSpace 1.0 requires that an endpoint with assertions PA03 and PA35 MUST have an <Identity> of a <KeyInfo> element specified in [XMLDSig/2002] section 4.4.

ADFS 2.0 never includes an <Identity> for an endpoint with assertions PA03 and PA35.

Windows CardSpace 1.0 requires that an endpoint with assertions PA12 and PA35 MUST have an <Identity> of a <KeyInfo> element specified in [XMLDSig/2002] section 4.4.

ADFS 2.0 includes an <Identity> of a <KeyInfo> element specified in [XMLDSig/2002] section 4.4 for an endpoint with assertions PA12 and PA35.

<18> Section 3.3.3: Windows CardSpace 1.0 uses WS-MetadataExchange requests. Windows CardSpace 2.0 uses HTTPS GET requests.

<19> Section 3.3.4.1: Windows chooses a time of current time plus 5 minutes for the <Expires> element. See section 3.2.4.1.1.2.1 for how Active Directory Federation Services (ADFS) 2.0 handles request messages received after this time.

<20> Section 3.3.4.1: See section 3.2.4.1.1.2.1 for how Active Directory Federation Services (ADFS) 2.0 chooses the time for the <Expires> element. Windows does not accept messages received after the time specified in the <Expires> element and displays an error.

<21> Section 3.3.4.1: Windows uses two DerivedKeyToken elements.

<22> Section 3.3.4.1: Active Directory Federation Services (ADFS) 2.0 uses two <DerivedKeyToken> elements.

<23> Section 3.3.4.1: PA16 and PA17 are always produced together on Active Directory Federation Services (ADFS) 2.0.

<24> Section 3.3.4.1: Windows uses two <DerivedKeyToken> elements.

<25> Section 3.3.4.1: Windows chooses a time of current time plus 5 minutes for the <Expires> element. See section 3.2.4.1.1.2.1 for how Active Directory Federation Services (ADFS) 2.0 handles request messages received after this time.

<26> Section 3.3.4.1: See section 3.2.4.1.1.2.1 for how Active Directory Federation Services (ADFS) 2.0 chooses the time for the <Expires> element. Windows does not accept messages received after the time specified in the <Expires> element and displays an error.

<27> Section 3.3.4.1: Windows uses one <DerivedKeyToken> element.

<28> Section 3.3.4.1: Windows only emits key specific identifiers when PA27 or PA40 is also present.

<29> Section 3.3.4.1: Windows does not emit an <X509IssuerSerial> element to identify an X.509 certificate.

<30> Section 3.3.4.1: Windows uses a thumbprint reference to identify an X.509 certificate.

<31> Section 3.3.4.1: Windows does not reference <EncryptedKey> elements that are not in the request message.

<32> Section 3.4.3: Active Directory Federation Services (ADFS) 2.0 will fault if an attribute store is unavailable.

<33> Section 3.6.3: By default, Active Directory Federation Services (ADFS) 2.0 STS is configured with the URL of the relying party, an applicable claims policy, as well as the X509 certificates to sign Security Tokens issued for the relying party service.

<34> Section 3.6.3: Active Directory Federation Services (ADFS) 2.0 STS does not support CRL checking via a Certificate Revocation List (CRL) Distribution Point.

<35> Section 3.6.3: Active Directory Federation Services (ADFS) 2.0 will fault if an attribute store is unavailable.

<36> Section 3.6.4.1.1.1.2.2: Active Directory Federation Services (ADFS) 2.0 returns a SOAP fault if it cannot generate all of the **Requested Claim Types**.

<37> Section 3.6.4.1.1.1.2.4: Active Directory Federation Services (ADFS) 2.0 defaults to a 256 bit AES key for symmetric key requests. Active Directory Federation Services (ADFS) 2.0 uses the size of the key included in the <UseKey> element for asymmetric key requests. Active Directory Federation Services (ADFS) 2.0 does not have a default asymmetric key size.

<38> Section 3.6.4.1.1.1.2.5: Active Directory Federation Services (ADFS) 2.0 will generate symmetric keys but will not generate asymmetric keys.

<39> Section 3.6.4.1.1.1.2.6: Active Directory Federation Services (ADFS) 2.0 ignores the <EncryptWith> element. Active Directory Federation Services (ADFS) 2.0 uses http://www.w3.org/2001/04/xmlenc#aes256-cbc by default for symmetric keys, and http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p for key wrap.

<40> Section 3.6.4.1.1.1.2.7: Active Directory Federation Services (ADFS) 2.0 ignores the <SignWith> element. Active Directory Federation Services (ADFS) 2.0 uses http://www.w3.org/2000/09/xmldsig#hmac-sha1 by default for symmetric keys, and http://www.w3.org/2000/09/xmldsig#rsa-sha1 for asymmetric key signing.

<41> Section 3.6.4.1.1.1.2.8: Active Directory Federation Services (ADFS) 2.0 ignores the <EncryptionAlgorithm> element. Active Directory Federation Services (ADFS) 2.0 uses only

http://www.w3.org/2001/04/xmlenc#aes256-cbc for encrypting the Security Token using symmetric keys.

<42> Section 3.6.4.1.1.1.2.9: Active Directory Federation Services (ADFS) 2.0 ignores the <CanonicalizationAlgorithm> element and only uses http://www.w3.org/2001/10/xml-exc-c14n# for canonicalization.

<43> Section 3.6.4.1.1.1.2.10: Active Directory Federation Services (ADFS) 2.0 uses the **lang** attribute to attempt to provide language-specific display tokens.

<44> Section 3.6.4.1.1.1.2.11: Active Directory Federation Services (ADFS) 2.0 ignores the <InformationCardReference> element and its child elements.

<45> Section 3.6.4.1.1.1.2.12: Active Directory Federation Services (ADFS) 2.0 ignores the <ClientPseudonym> element.

<46> Section 3.6.4.1.1.1.2.13: Active Directory Federation Services (ADFS) 2.0 will use the value of the <OnBehalfOf> element to generate claims for the user if it is configured to do so for the caller.

<47> Section 3.6.4.1.1.1.2.14: Active Directory Federation Services (ADFS) 2.0 has per relying party policy for the claims it will issue to each relying party to ensure correct claim naming and avoid unnecessary information disclosure. Active Directory Federation Services (ADFS) 2.0 does not use the Security Token that may be found in the <Identity> element. Active Directory Federation Services (ADFS) 2.0 will return a SOAP fault if the <AppliesTo> element is not present in the request message.

<48> Section 3.6.4.1.1.2.2.1: Active Directory Federation Services (ADFS) 2.0 can be configured to encrypt Security Tokens or emit them without encryption.

<49> Section 3.6.4.1.2.22: Windows does not include the Dialect attribute.

<50> Section 3.7.4.1.2.1.1: Windows always includes the <AppliesTo> element to Active Directory Federation Services (ADFS) 2.0.

<51> Section 3.7.4.1.2.1.2: Windows always includes the <EncryptionAlgorithm> element with a value of http://www.w3.org/2001/04/xmlenc#aes256-cbc (as specified in [XMLEnc] section 5.2.2).

<52> Section 3.7.4.1.2.1.3: Windows includes the identifier of the information card in the <CardId> element, as well as the information card version integer as the value of the <CardVersion> element described above in 3.6.4.1.2.21.

<53> Section 3.7.4.1.2.1.4: Windows always includes a <RequestDisplayToken> element with an attribute indicating the language to use in the display token returned as described in section 3.3.3.

<54> Section 3.7.4.1.2.1.5: Windows always includes this element with a value of http://www.w3.org/2001/10/xml-exc-c14n# ([Excl-C14N]).

<55> Section 3.7.4.1.2.1.6: Windows includes the <Claims> element populated by the claim type URIs that are required by the relying party, as described in section 3.7.3.

<56> Section 3.7.4.1.2.1.7: Windows always includes this element, and the value of the <PPID> child element is a base64-encoded SHA256 hash value.

<57> Section 3.7.4.1.2.1.8: Windows CardSpace 1.0 never includes this element.

When acting as a proxy, Active Directory Federation Services (ADFS) 2.0 includes this element when forwarding a request for a client.

<58> Section 3.7.4.1.2.2.1: When requesting a Security Token Service (STS) with an asymmetric key, the following URI is used by Windows to indicate the key wrap algorithm that must be supported by the asymmetric key: http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p (as specified in [XMLEnc] section 5.4.2).

<59> Section 3.7.4.1.2.2.2: When requesting a Security Token with an asymmetric key, the following URI is used by Windows to indicate the signature algorithm that must be supported by the asymmetric key: http://www.w3.org/2000/09/xmldsig#rsa-sha1 (as specified in [XMLDSig/2002] section 6.4.2).

<60> Section 3.7.4.1.2.2.3: When requesting a Security Token with an asymmetric key, Windows generates an RSA public/private key pair and places the public key in the <KeyInfo> child element of the <UseKey> element, conforming to [XMLDSig/2002].

<61> Section 3.7.4.1.2.2.4: Windows includes this element and sets the value to 2048.

<62> Section 3.7.4.2.2.3: Windows uses the information in the <RequestedDisplayToken> element to display the emitted claims to the user.

8 Change Tracking

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

9 Index

M

N

O

P

R

S

T

V

W