OASIS WEB SERVICES SECURE EXCHANGE TC

Frederick Hirsch 12/6/05 2:17 PM
Formatted: Numbering: Continuous

a. Name of the TC

OASIS Web Services Secure Exchange (WS-SX) Technical Committee

b. Statement of Purpose

The purpose of the Web Services Secure Exchange (WS-SX) Technical Committee (TC) is to define extensions to OASIS Web Services Security [1] to enable trusted SOAP message exchanges involving multiple message exchanges and to define security policies that govern the formats and tokens of such messages. This work will be carried out through continued refinement of the Web Services SecureConversation, SecurityPolicy and Trust specifications [2-4] submitted to the TC as referenced in this charter.

c. Scope of Work

The TC will accept as input the February 2005 Version 1.2 of the WS-SecureConversation [2] and the February 2005 Version 1.2 of the WS-Trust [3] as published by Actional Corporation, BEA Systems, Inc., Computer Associates International, Inc., IBM, Layer 7 Technologies, Microsoft Corporation, Oblix Inc., OpenNetwork Technologies Inc., Ping Identity Corporation, Reactivity Inc., RSA Security Inc., and VeriSign Inc and the July 2005 Version 1.1 WS-SecurityPolicy [4] specifications (the Input Documents) as published by IBM, Microsoft, RSA Security and VeriSign.

Other contributions and changes to the input documents will be accepted for consideration without any prejudice or restrictions and evaluated based on technical merit in so far as they conform to this charter. OASIS members with extensive experience and knowledge in these areas are particularly invited to participate.

In order to support general secure Web Service messaging, additional facilities are needed beyond what is provided in OASIS Web Services Security [1]. The OASIS Web Services Security specification describes a base mechanism for securing SOAP messages but does not deal with trust brokering, multi-message exchanges, and policies describing how to secure message exchanges with a Web service. The following sub-sections describe the charter of the WS-SX TC with respect to these areas.

The scope of the TC’s work is to continue further refinement and finalization of the Input Documents to produce as output modular specifications that standardize the concepts, WSDL documents and XML Schema renderings of the areas described below.

Frederick Hirsch 12/7/05 4:52 PM
Deleted: ’

Trusted Brokering of SOAP message exchanges

OASIS Web Services Security [1] defines the basic mechanism for providing secure SOAP messaging. It describes how to use security tokens to obtain message integrity, confidentiality and authentication of the message sender. In order to establish the authenticity of any message sender, the recipient needs to “trust” the asserted credentials of the sender. The WS-SX TC will add additional primitives to enable the establishing and brokering of these trust relationships between parties in a SOAP message exchange as defined by the policy expressions associated with the SOAP endpoints.

The scope of this work is to develop extensions to OASIS Web Services Security [1] that facilitate “trusted” SOAP message exchanges. This will be done by enabling the web services to participate in the establishment and brokering of trust relationships by means of an exchange and issuance of the relevant security tokens. In addition, some token and message validation may require the definition of specialized SOAP messages and header blocks.

This work will focus on:

1. Describing a protocol for brokering trust on behalf of a requestor by obtaining designated security tokens containing required claims from the trusted authorities.
2. Describing a framework for interactions with trusted authorities known as security token services. This includes describing the request/response elements for interactions with a security token service. This base framework for requesting and returning of security tokens should be usable for a variety of purposes related to security token services. Web service trust bindings define how this

framework is used for specific usage patterns. This specification defines Web service trust bindings for issuance, renewal, cancellation and validation of security tokens.

3. Declaring specific Web service bindings to a security token service for security token issuance including, but not limited to the following cases:

a. Actions and elements for requesting a security token (or tokens).

b. Actions and elements for responding with a security token (or tokens).

c. Specifying the scope of each requested and returned security token using WS-Policy [5] <wsp:AppliesTo> (eg. wsa:endpointReference).

d. Specifying mechanisms for issuing, computing or utilizing existing keys as proof keys associated with the issued token.

e. Support for requesting and returning bearer tokens

f. Requesting or returning multiple security tokens.

g. Transferring security tokens as part of application messages as well as part of the SOAP body of a separate response message

h. Requesting a security token (or tokens) on behalf of another entity (or entities).

i. Requesting a security token (or tokens) that may be forwardable or delegatable.

j. Specifying characteristics of the requested type of keys.

k. Enabling additional negotiation and challenge protocol mechanisms to be used (e.g. SASL mechanisms, SPNEGO) initiated by either client or server.

4. Declaring specific Web service bindings of the security token service framework for security token renewal. Renewal is the process by which a previously issued token with expiration is presented at a security token service and the same token is returned with new expiration characteristics. Such a renewal binding should be defined for (but not be limited to) the following:

a. Actions and elements for requesting the renewal of a single token.

b. Actions and elements for responding with a renewed token (or tokens).

c. Allowing for direct or indirect references to the security tokens

Frederick Hirsch 12/6/05 2:12 PM
Formatted: Font:Times New Roman, 16 pt

Frederick Hirsch 12/6/05 2:12 PM
Formatted: Font:Times New Roman, 16 pt

Frederick Hirsch 12/6/05 2:12 PM
Formatted: Font:Times New Roman

Frederick Hirsch 12/6/05 2:12 PM
Formatted: Font:Times New Roman, 16 pt

Frederick Hirsch 12/7/05 4:41 PM
Formatted: Indent: Left: 0.24"

Frederick Hirsch 12/6/05 2:12 PM
Formatted: Font:Times New Roman, 16 pt

Frederick Hirsch 12/6/05 2:12 PM
Formatted: Font:Times New Roman, 16 pt

Frederick Hirsch 12/6/05 2:12 PM
Formatted: Font:Times New Roman, 16 pt

Frederick Hirsch 12/6/05 2:12 PM
Formatted: Font:Times New Roman, 16 pt

Frederick Hirsch 12/6/05 2:13 PM
Formatted: Font:Times New Roman, 16 pt

Frederick Hirsch 12/6/05 2:13 PM
Formatted: Font:Times New Roman

being renewed.

5. Declaring specific Web service trust bindings of the security token service framework for cancellation. When a previously issued token is no longer needed, the cancel binding can be used to cancel the token, terminating its use. Such cancel binding should define (but not be limited to) the following cases:

   a. Actions and elements for requesting the cancellation of a single token.

   b. Actions and elements for responding with the cancellation result.

   c. Allowing for direct or indirect references to the security tokens being cancelled.

6. Declaring specific Web service trust bindings of the security token service framework for token validation. Validation binding is used to evaluate a security token (or OASIS Web Services Security [1] compliant message) and the result is returned as a status, token or both. Such a validation binding should be defined for (but not be limited to) the following:

   a. Actions and elements for requesting the validation of a token (or message).

   b. Actions and elements for responding about the validity of a token (or tokens).

   c. Allowing for direct or indirect references to the security tokens being validated.

7. Generalizing the mechanism for a security token service to allow for multi-leg exchanges. Such exchange should allow for, but not be limited to "challenges", tunnelling of legacy binary protocols, and tunnelling of hardware-based legacy protocols. Specifically, the following models of challenge and exchanges should be defined by this specification:

   a. Signature challenge that requires the other party to sign specified information.

   b. Binary exchanges involving the usage of binary data from existing non-Web Services protocols.

   c. Exchanges involving request and passing of a key exchange token

Shared security contexts

OASIS Web Services Security [1] describes using security credentials to implement message integrity, confidentiality and authentication. In cases where multiple messages need to be exchanged securely, typically a shared security context is established between the communicating parties and used for the life time of the message exchange. This TC will also address adding extensions to Web Services Security [1] and define the appropriate secure SOAP message exchanges (see above) to permit the definition of shared security contexts.

This work will encompass:

1. Defining mechanisms for establishing a shared security context in the following cases:
    a. When one of the communicating parties creates the context and propagates it to other parties.
    b. When the shared context is achieved through a sequence of negotiations.
    c. When the shared context is brokered through a third party security token service.
2. Defining specific Web service bindings for security context establishment by utilizing the Web service trust binding elements for requesting and responding with security context tokens.
3. Defining specific Web service bindings for renewal of the security context token.
4. Defining specific Web service bindings for cancellation of the security context token.
5. Defining specific Web service bindings for amendment of the claims associated with a security context.
6. Since a shared security context may contain or imply a shared key, this specification must contain descriptions of common elements for key derivation models, where such a scheme is desirable for improving the security characteristics of the keys being used.
7. Defining a token profile for use of security context tokens with OASIS Web Services Security [1].
8. Defining a token profile for use of derived key tokens with OASIS Web Services Security [1].

Security policies

OASIS Web Services Security [1], WS-SecureConversation [2] and

WS-Trust [3] define open-ended wire formats. WS-Policy [5] defines a framework for allowing web services to express their constraints and requirements as policy assertions. WS-SecurityPolicy [4] uses the facilities of WS-Policy [5] to express the conditions and restrictions on the wire formats defined by OASIS Web Services Security [1], WS-SecureConversation [2] and WS-Trust [3] to a specific set of typed message interchanges. That is to say WS-SecurityPolicy "strongly types" the supported security messages. This type of policy enablement allows the supported message exchanges to be analyzed from a security perspective to indicate which security protocols an end point supports.

This work will specifically define the following:

1. Mechanism for specifying what parts of the message must be secured, called protection assertions
    a. Such protection assertions must be able to specify integrity requirements at both the element and header/body level in a security policy binding (defined below) neutral manner.
    b. Such protection assertions must be able to specify confidentiality requirements at both the element and header/body level in a security policy binding (defined below) neutral manner.
    c. Such mechanisms must not require the use of XPath [21] but may provide it as an option.

Frederick Hirsch 12/7/05 4:40 PM
Deleted: 1.0

2. Mechanism for specifying pre-conditions of security, called conditional assertions
    a. Such conditional assertions must be able to specify the required elements in the message
3. General mechanism for specifying tokens to use in protecting the message or binding claims to the message, called token assertions
    a. Such token assertions should facilitate the specification of at least the following token types defined by OASIS SOAP Message Security, WS-Trust and WS-SecureConversation: Username token, X509 token, Kerberos token, SPNego Context Token, Security Context Token, Secure Conversation Token, SAML token, REL token, HTTPS token as well as any opaque token issued by a security token service.
    b. Such token assertions should specify conditions for inclusion in the message such as whether the token should be included in every message explicitly, whether the token should be always excluded from the message and a reference included in the message, whether

the token should be included once in a message exchange and external reference should be used subsequently.

c. Such token assertions should support specification of derived keys.

4. An abstraction for describing some of the common security usage patterns called security policy bindings.

a. Such an abstraction should contain a description of the required and optional elements of such a security policy binding, including minimal token requirements, necessary key transfer mechanism, structure and contents of elements in wsse:security header, and correlation mechanisms.

b. Such a binding framework should also include properties for describing algorithm suite to be used, whether a timestamp should be included, signature/encryption ordering in the message, whether signatures are encrypted, and whether the signing token should also be covered by the signature.

c. Specific security policy binding assertions for the patterns where transport is used, where a symmetric key token is used for message security or where an asymmetric key token pair is used for message security.

5. A mechanism for specifying additional token types that provide additional claims, called supporting token assertions. Such a mechanism should support the following cases:

a. When additional tokens are used to sign additional parts of the message

b. When additional tokens are signed by the primary signature token

c. When additional tokens sign the primary signature

d. When additional tokens sign the primary signature and are signed by the primary signature token

6. A mechanism for specifying token referencing and token issuance called WSS assertions and Trust assertions that meet the referencing mechanisms and properties defined in OASIS Web Services Security 1.0 (and associated token profiles) [1], OASIS Web Services Security 1.1 (and associated token profiles) [6], in WS-Trust [3] and WS-SecureConversation [2]. Such a mechanism should include:

a. Properties for indicating the Web Services Security 1.0 [1] defined reference mechanism to use

b. Properties for indicating the Web Services Security 1.1 [6] defined reference mechanism to use including thumbprint reference and encryptedkey reference

c. Signature confirmation requirement

d. Properties for indicating the type of challenges required (as defined in WS-Trust [3])

e. Properties for indicating the type of entropy mechanism required in a negotiation sequence (as defined in WS-Trust [3])

Frederick Hirsch 12/7/05 4:53 PM
Deleted: on

General Notes on Scope

The output specifications will uphold the basic principles of other Web services specifications of independence and composition and be composable with the other specifications in the Web services architecture, such as the specifications listed in the References section, numbers 1, 5-12 and 18-20. The TC will also take into consideration the following specifications/works listed in the References section, numbers 13, 14, 15 and 16.

If any of the above specifications is outside of a standardization process at the time this TC moves to ratify its deliverables, or is not far enough along in the standardization process, any normative references to it in the TC output will be expressed in an abstract manner, and the incarnation will be left at that time as an exercise in interoperability.

While composition with other specifications is a goal of the TC, it is also a goal to leave the specifics of how that composition is achieved outside the scope of this TC.

Each of the protocol elements will use implementation and language neutral XML formats defined in XML Schema [17].

Out of Scope

The following is a non-exhaustive list. It is provided only for the sake of clarity. If some function, mechanism or feature is not mentioned here, and it is not mentioned in the Scope of Work section either, then it will be deemed to be out of scope.

The TC will not define a mapping of the functions and elements described in the specifications to any programming language, to any particular messaging middleware, nor to specific network transports.

The following items are specifically out of scope of the work of the

TC:

1. Definition and management of trust policy expressions (that is, statements about who is trusted to make what claims about an entity); these are different from the in-scope "trust assertions" referred to in the Scope of Work section above
2. Token revocation notifications and revocation management (e.g. via CRLs)
3. Schemas for specific tokens issued, renewed, cancelled or validated as part of the trust process.
4. The establishment of trust between two or more business parties
5. Definition of new key derivation algorithms
6. Providing a general purpose boxcaring model
7. Definition of APIs
8. Definition of additional negotiation and challenge protocol mechanisms.
9. Developing the roadmaps [15], [16] or other specifications mentioned in those roadmaps, beyond the material listed explicitly as within the scope of this charter.

Frederick Hirsch 12/6/05 2:15 PM
Formatted: Font:Times New Roman, 16 pt

Frederick Hirsch 12/6/05 2:15 PM
Formatted: Font:Times New Roman

The TC will not attempt to define concepts or renderings for functions that are of wider applicability including but not limited to:

-- Addressing
-- Policy language frameworks
-- Routing
-- Reliable message exchange
-- Transactions and compensation

Where required these functions are achieved by composition with other Web services specifications.

The TC will not attempt to define functionality duplicating that of any normatively referenced specification in the input WS-SecureConversation [2], WS-Trust [3] or WS-SecurityPolicy [4] specifications.If the referenced specification is outside of a standardization process at the time this TC moves to ratify its deliverables, or is not far along enough in the standardization process, any normative references to it in the TC output will be expressed in an abstract manner, and the incarnation will be left at that time as an exercise in interoperability.

d. Deliverables

The TC has the following set of deliverables:

* A revised Web Services SecureConversation specification and associated Schema. A Committee Specification is scheduled for completion within 18 months of the first TC meeting.
* A revised Web Services Trust specification with associated Schema and WSDL. A Committee Specification is scheduled for completion within 18 months of the first TC meeting.
* A revised Web Services SecurityPolicy specification and associated Schema. A Committee Specification is scheduled for completion within 18 months of the first TC meeting.

These specifications will reflect refinements, corrections or material technological improvements with respect to the input documents and in accordance with this charter.
Ratification of the above specifications as OASIS standards, including a brief period to address any errata will mark the end of the TC’s lifecycle.

Frederick Hirsch 12/7/05 4:55 PM
Deleted: ’

e. Anticipated Audience

The anticipated audience for this work includes:

* Vendors offering web services products
* Other specification authors that need security for Web services
* Software architects and programmers, who design, write or integrate applications for Web services
* End users implementing Web services-based solutions that require an interoperable, composable solution for trusted SOAP message exchanges, security policies and shared security contexts.
* Vendors making gateway and router class products (both hardware and software)

f. Language

TC business will be conducted in English.

g. IPR Policy

This TC will operate under the "RF (Royalty Free) on RAND Terms" IPR mode as defined in the OASIS Intellectual Property Rights (IPR) Policy, effective 15 April 2005.