Web Services Reliable Messaging Policy Assertion (WS-RM Policy) Version 1.2

Committee Draft 02

20 November 2008

Specification URIs:

This Version:

http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-cd-02.pdf
http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-cd-02.html
http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-cd-02.doc (Authoritative)

Previous Version:

http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-cs-01.pdf
http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-cs-01.html
http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-cs-01.doc

Latest Version:

http://docs.oasis-open.org/ws-rx/wsrmp/v1.2/wsrmp.pdf
http://docs.oasis-open.org/ws-rx/wsrmp/v1.2/wsrmp.html
http://docs.oasis-open.org/ws-rx/wsrmp/v1.2/wsrmp.doc

Technical Committee:

OASIS Web Services Reliable Exchange (WS-RX) TC

Chairs:

Paul Fremantle <paul@wso2.com>
Sanjay Patil <sanjay.patil@sap.com>

Editors:

Doug Davis, IBM <dug@us.ibm.com>
Anish Karmarkar, Oracle <Anish.Karmarkar@oracle.com>
Gilbert Pilz, BEA <gpilz@bea.com>
Ümit Yalçinalp, SAP <umit.yalcinalp@sap.com>

Related Work:

This specification replaces or supercedes:

- WS-ReliableMessaging Policy v1.1

Declared XML Namespaces:

http://docs.oasis-open.org/ws-rx/wsrmp/200702

Abstract:

This specification describes a domain-specific policy assertion for WS-ReliableMessaging [WS-RM] that that can be specified within a policy alternative as defined in WS-Policy Framework [WS-Policy].

By using the XML [XML], SOAP [SOAP 1.1], [SOAP 1.2] and WSDL [WSDL 1.1] extensibility models, the WS* specifications are designed to be composed with each other to provide a rich Web services environment. This by itself does not provide a negotiation solution for Web services. This is a building block that is used in conjunction with other Web service and application-specific protocols to accommodate a wide variety of policy exchange models.

Status:

This document was last revised or approved by the WS-RX Technical Committee on the above date. The level of approval is also listed above. Check the "Latest Version" or "Latest Approved Version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at http://www.oasis-open.org/committees/ws-rx/.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (http://www.oasis-open.org/committees/ws-rx/ipr.php).

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/ws-rx/.

Notices

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS", WS-ReliableMessaging Policy, WS-ReliableMessaging, WSRMP, WSRM, WS-RX are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction ... 5
1.1 Terminology ... 5
1.2 Normative ... 5
1.3 Non Normative ... 6
1.4 Namespace ... 7
1.5 Conformance ... 7
2 RM Policy Assertions ... 8
2.1 Assertion Model ... 8
2.2 Normative Outline ... 8
2.3 Assertion Attachment ... 9
2.4 Assertion Example ... 11
2.5 Sequence Security Policy ... 11
3 Security Considerations ... 13
Appendix A. Schema ... 14
Appendix B. Acknowledgments ... 16

1 Introduction

This specification defines a domain-specific policy assertion for reliable messaging for use with WS-Policy and WS-ReliableMessaging.

1.1 Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [KEYWORDS].

This specification uses the following syntax to define normative outlines for messages:

- The syntax appears as an XML instance, but values in italics indicate data types instead of values.
- Characters are appended to elements and attributes to indicate cardinality:
    - "?" (0 or 1)
    - "*" (0 or more)
    - "+" (1 or more)
- The character "|" is used to indicate a choice between alternatives.
- The characters "[" and "]" are used to indicate that contained items are to be treated as a group with respect to cardinality or choice.
- An ellipsis (i.e. "...") indicates a point of extensibility that allows other child, or attribute, content. Additional children and/or attributes MAY be added at the indicated extension points but MUST NOT contradict the semantics of the parent and/or owner, respectively. If an extension is not recognized it SHOULD be ignored.
- XML namespace prefixes (see section 1.4) are used to indicate the namespace of the element being defined.

Elements and Attributes defined by this specification are referred to in the text of this document using XPath 1.0 [XPATH 1.0] expressions. Extensibility points are referred to using an extended version of this syntax:

- An element extensibility point is referred to using {any} in place of the element name. This indicates that any element name can be used, from any namespace other than the wsrm: namespace.
- An attribute extensibility point is referred to using @{any} in place of the attribute name. This indicates that any attribute name can be used, from any namespace other than the wsrm: namespace.

1.2 Normative

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

[SOAP 1.1] W3C Note, "SOAP: Simple Object Access Protocol 1.1" 08 May 2000.
http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

[SOAP 1.2] W3C Recommendation, "SOAP Version 1.2 Part 1: Messaging Framework" June 2003.
http://www.w3.org/TR/2003/REC-soap12-part1-20030624/

[URI] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax," RFC 3986, MIT/LCS, U.C. Irvine, Xerox Corporation, January 2005.
http://ietf.org/rfc/rfc3986

[WS-RM] OASIS WS-RX Technical Committee Draft, "Web Services Reliable Messaging (WS-ReliableMessaging)," November 2008.
http://docs.oasis-open.org/ws-rx/wsrm/v1.2/wsrm.pdf

[WSDL 1.1] W3C Note, "Web Services Description Language (WSDL 1.1)," 15 March 2001.
http://www.w3.org/TR/2001/NOTE-wsdl-20010315

[XML] W3C Recommendation, "Extensible Markup Language (XML) 1.0 (Fourth Edition)", September 2006.
http://www.w3.org/TR/REC-xml/

[XML-ns] W3C Recommendation, "Namespaces in XML," 14 January 1999.
http://www.w3.org/TR/1999/REC-xml-names-19990114/

[XML-Schema Part1] W3C Recommendation, "XML Schema Part 1: Structures," October 2004.
http://www.w3.org/TR/xmlschema-1/

[XML-Schema Part2] W3C Recommendation, "XML Schema Part 2: Datatypes," October 2004.
http://www.w3.org/TR/xmlschema-2/

[XPATH 1.0] W3C Recommendation, "XML Path Language (XPath) Version 1.0," 16 November 1999.
http://www.w3.org/TR/xpath

1.3 Non Normative

[RDDL 2.0] Jonathan Borden, Tim Bray, eds. “Resource Directory Description Language (RDDL) 2.0,” January 2004
http://www.openhealth.org/RDDL/20040118/rddl-20040118.html

[SecurityPolicy] OASIS WS-SX Technical Committee Editor Draft, "WS-SecurityPolicy 1.3"
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200802

[WS-Policy] W3C Recommendation, "Web Services Policy 1.5 - Framework," September 2007.
http://www.w3.org/TR/2007/REC-ws-policy-20070904

[WS-PolicyAttachment] W3C Recommendation, "Web Services Policy 1.5 - Attachment," September 2007.
http://www.w3.org/TR/2007/REC-ws-policy-attach-20070904

[WS-Security] Anthony Nadalin, Chris Kaler, Phillip Hallam-Baker, Ronald Monzillo, eds. "OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", OASIS Standard 200401, March 2004.
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

Anthony Nadalin, Chris Kaler, Phillip Hallam-Baker, Ronald Monzillo, eds. "OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", OASIS Standard 200602, February 2006.
http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

1.4 Namespace

The XML namespace [XML-ns] URI that MUST be used by implementations of this specification is:

```
http://docs.oasis-open.org/ws-rx/wsrmp/200702
```

Dereferencing the above URI will produce the Resource Directory Description Language [RDDL 2.0] document that describes this namespace.

Table 1 lists the XML namespaces that are used in this specification. The choice of any namespace prefix is arbitrary and not semantically significant.

Table 1

Prefix	Namespace	Specification
wsdl	http://schemas.xmlsoap.org/wsdl/	[WSDL 1.1]
wsp	http://www.w3.org/ns/ws-policy	WS-Policy 1.5
wsrmp	http://docs.oasis-open.org/ws-rx/wsrmp/200702	This specification.
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	WS-Security-Utility Schema

The normative schema for WS-ReliableMessaging can be found linked from the namespace document that is located at the namespace URI specified above.

All sections explicitly noted as examples are informational and are not to be considered normative.

1.5 Conformance

An implementation is not compliant with this specification if it fails to satisfy one or more of the MUST or REQUIRED level requirements defined herein. A SOAP Node MUST NOT use the XML namespace identifier for this specification (listed in section 1.4) within SOAP Envelopes unless it is compliant with this specification.

Normative text within this specification takes precedence over normative outlines, which in turn take precedence over the XML Schema [XML-Schema Part1, XML-Schema Part2] descriptions.

2 RM Policy Assertions

WS-Policy Framework and WS-Policy Attachment [WS-PolicyAttachment] collectively define a framework, model and grammar for expressing the requirements, and general characteristics of entities in an XML Web services-based system. To enable an RM Destination and an RM Source to describe their requirements for a given Sequence, this specification defines a single RM policy assertion that leverages the WS-Policy framework.

2.1 Assertion Model

The RM policy assertion indicates that the RM Source and RM Destination MUST use WS-ReliableMessaging to ensure reliable delivery of messages. Specifically, the WS-ReliableMessaging protocol determines invariants maintained by the reliable messaging endpoints and the directives used to track and manage the delivery of a Sequence of messages.

2.2 Normative Outline

The normative outline for the RM assertion is:

```
<wsrmp:RMAssertion [wsp:Optional="true"]? ... >
  <wsp:Policy>
    [ <wsrmp:SequenceSTR/> |
      <wsrmp:SequenceTransportSecurity/> ] ?
    <wsrmp:DeliveryAssurance>
      <wsp:Policy>
        [ <wsrmp:ExactlyOnce/> |
          <wsrmp:AtLeastOnce/> |
          <wsrmp:AtMostOnce/> ]
        <wsrmp:InOrder/> ?
      </wsp:Policy>
    </wsrmp:DeliveryAssurance> ?
  </wsp:Policy>
  ...
</wsrmp:RMAssertion>
```

The following describes the content model of the `RMAssertion` element.

`/wsrmp:RMAssertion`

A policy assertion that specifies that WS-ReliableMessaging protocol MUST be used when sending messages.

`/wsrmp:RMAssertion/@wsp:Optional="true"`

Per WS-Policy, this is compact notation for two policy alternatives, one with and one without the assertion. The intuition is that the behavior indicated by the assertion is optional, or in this case, that WS-ReliableMessaging MAY be used.

`/wsrmp:RMAssertion/wsp:Policy`

This required element allows for the inclusion of nested policy assertions.

`/wsrmp:RMAssertion/wsp:Policy/wsrmp:SequenceSTR`

When present, this assertion defines the requirement that an RM Sequence MUST be bound to an explicit token that is referenced from a `wsse:SecurityTokenReference` in the `CreateSequence` message. See section 2.5.1.

/wsrmp:RMAssertion/wsp:Policy/wsrmp:SequenceTransportSecurity

When present, this assertion defines the requirement that an RM Sequence MUST be bound to the session(s) of the underlying transport-level protocol used to carry the `CreateSequence` and `CreateSequenceResponse` message. When present, this assertion MUST be used in conjunction with the `sp:TransportBinding` assertion, see section 2.5.2.

/wsrmp:RMAssertion/wsp:Policy/wsrmp:DeliveryAssurance

This expression, which may be omitted, describes the message delivery quality of service between the RM and application layer. When used by an RM Destination it expresses the delivery assurance in effect between the RM Destination and its corresponding application destination, and it also indicates requirements on any RM Source that transmits messages to this RM destination. Conversely when used by an RM Source it expresses the delivery assurance in effect between the RM Source and its corresponding application source, as well as indicating requirements on any RM Destination that receives messages from this RM Source. In either case the delivery assurance does not affect the messages transmitted on the wire. Absence of this expression from a `wsrmp:RMAssertion` policy assertion simply means that the endpoint has chosen not to advertise its delivery assurance characteristics.
Note that when there are multiple policy alternatives of the RM Assertion, the Delivery Assurance on each MUST NOT conflict.

/wsrmp:RMAssertion/wsp:Policy/wsrmp:DeliveryAssurance/wsp:Policy

This required element identifies additional requirements for the use of the `wsrmp:DeliveryAssurance`.

/wsrmp:RMAssertion/wsp:Policy/wsrmp:DeliveryAssurance/wsp:Policy/wsrmp:ExactlyOnce

This expresses the ExactlyOnce Delivery Assurance defined in [WS-RM].

/wsrmp:RMAssertion/wsp:Policy/wsrmp:DeliveryAssurance/wsp:Policy/wsrmp:AtLeastOnce

This expresses the AtLeastOnce Delivery Assurance defined in [WS-RM].

/wsrmp:RMAssertion/wsp:Policy/wsrmp:DeliveryAssurance/wsp:Policy/wsrmp:AtMostOnce

This expresses the AtMostOnce Delivery Assurance defined in [WS-RM].

/wsrmp:RMAssertion/wsp:Policy/wsrmp:DeliveryAssurance/wsp:Policy/wsrmp:InOrder

This expresses the InOrder Delivery Assurance defined in [WS-RM].

/wsrmp:RMAssertion/{any}

This is an extensibility mechanism to allow different (extensible) types of information, based on a schema, to be passed.

/wsrmp:RMAssertion/@{any}

This is an extensibility mechanism to allow different (extensible) types of information, based on a schema, to be passed.

2.3 Assertion Attachment

The RM policy assertion is allowed to have the following Policy Subjects [WS-PolicyAttachment]:

- Endpoint Policy Subject
- Message Policy Subject

WS-PolicyAttachment defines a set of WSDL/1.1 policy attachment points for each of the above Policy Subjects. Since an RM policy assertion specifies a concrete behavior, it MUST NOT be attached to the abstract WSDL policy attachment points.

The following is the list of WSDL/1.1 elements whose scope contains the Policy Subjects allowed for an RM policy assertion but which MUST NOT have RM policy assertions attached:

- wsdl:message
- wsdl:portType/wsdl:operation/wsdl:input
- wsdl:portType/wsdl:operation/wsdl:output
- wsdl:portType/wsdl:operation/wsdl:fault
- wsdl:portType

The following is the list of WSDL/1.1 elements whose scope contains the Policy Subjects allowed for an RM policy assertion and which MAY have RM policy assertions attached:

- wsdl:port
- wsdl:binding
- wsdl:binding/wsdl:operation/wsdl:input
- wsdl:binding/wsdl:operation/wsdl:output
- wsdl:binding/wsdl:operation/wsdl:fault

If an RM policy assertion is attached to any of:

- wsdl:binding/wsdl:operation/wsdl:input
- wsdl:binding/wsdl:operation/wsdl:output
- wsdl:binding/wsdl:operation/wsdl:fault

then an RM policy assertion, specifying `wsp:Optional=”true”` MUST be attached to the corresponding `wsdl:binding` or `wsdl:port`, indicating that the endpoint supports WS-RM. Any messages, regardless of whether they have an attached Message Policy Subject RM policy assertion, MAY be sent to that endpoint using WS-RM. Additionally, the receiving endpoint MUST NOT reject any message belonging to a Sequence, simply because there was no Message Policy Subject RM policy assertion attached to that message. There might be certain RM implementations that are incapable of applying RM Quality of Service (QoS) semantics on a per-message basis. In order to ensure the broadest interoperability, when an endpoint decorates its WSDL with RM policy assertions using Message Policy Subject, it MUST also be prepared to accept that all messages sent to that endpoint might be sent within the context of an RM Sequence, regardless of whether the corresponding wsdl:input, wsdl:output or wsdl:fault had an attached RM policy assertion.

Rather than turn away messages that were unnecessarily sent with RM semantics, the receiving endpoint described by the WSDL MUST accept these messages.

By attaching an RM policy assertion that specifies `wsp:Optional="true"` to the corresponding endpoint that has attached RM policy assertions at the Message Policy Subject level, the endpoint is describing the above constraint in policy.

In the case where an optional RM Assertion applies to an output message, there is no requirement on the client to support an RM Destination implementation

2.4 Assertion Example

Table 2 lists an example use of the RM policy assertion.

Table 2: Example policy with RM policy assertion

```
(01)<wsdl:definitions
(02)    targetNamespace="example.com"
(03)    xmlns:tns="example.com"
(04)    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
(05)    xmlns:wsp="http://www.w3.org/ns/ws-policy"
(06)    xmlns:wsrmp="http://docs.oasis-open.org/ws-rx/wsrmp/200702"
(07)    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
(08)
(09) <wsp:UsingPolicy wsdl:required="true" />
(10)
(11) <wsp:Policy wsu:Id="MyPolicy" >
(12)   <wsrmp:RMAssertion>
(13)     <wsp:Policy/>
(14)   </wsrmp:RMAssertion>
(15)   <!-- omitted assertions -->
(16) </wsp:Policy>
(17)
(18) <!-- omitted elements -->
(19)
(20) <wsdl:binding name="MyBinding" type="tns:MyPortType" >
(21)   <wsp:PolicyReference URI="#MyPolicy" />
(22)   <!-- omitted elements -->
(23) </wsdl:binding>
(24)
(25)</wsdl:definitions>
```

Line (09) in Table 2 indicates that WS-Policy is in use as a required extension.

Lines (11-16) are a policy expression that includes a RM policy assertion (lines 12-14) to indicate that WS-ReliableMessaging must be used.

Lines (20-23) are a WSDL binding. Line (21) indicates that the policy in lines (11-16) applies to this binding, specifically indicating that WS-ReliableMessaging must be used over all the messages in the binding.

2.5 Sequence Security Policy

WS-SecurityPolicy [SecurityPolicy] provides a framework and grammar for expressing the security requirements and characteristics of entities in a XML web services based system. The following assertions MAY be used in conjunction with WS-SecurityPolicy to express additional security requirements particular to RM Sequences.

2.5.1 RM Assertion with Sequence STR Assertion

This version of the RM assertion includes the requirement that an RM Sequence MUST be bound to an explicit token that is referenced from a `wsse:SecurityTokenReference` in the `CreateSequence` message.

This assertion MUST apply to [Endpoint Policy Subject]. The normative outline for this form of the Sequence STR Assertion is:

```
<wsrmp:RMAssertion [wsp:Optional="true"]? ...>
```

```
  <wsp:Policy>
    <wsrmp:SequenceSTR/>
  <wsp:Policy>
</wsrmp:RMAssertion>
```

The following describes the content model of the `SequenceSTR` element.

`/wsrmp:SequenceSTR`

> A policy assertion that specifies security requirements which MUST be used with an RM Sequence that are particular to WS-RM and beyond what can be expressed in WS-SecurityPolicy.

2.5.2 RM Assertion with Sequence Transport Security Assertion

This version of the RM assertion includes the requirement that an RM Sequence MUST be bound to the session(s) of the underlying transport-level security protocol (e.g. SSL/TLS) used to carry the `CreateSequence` and `CreateSequenceResponse` messages.

This assertion MUST apply to [Endpoint Policy Subject]. This assertion MUST be used in conjunction with the `sp:TransportBinding` assertion that requires the use of some transport-level security mechanism (e.g. `sp:HttpsToken`).

The normative outline for this form of the RM Assertion with the Sequence Transport Security Assertion is:

```
<wsp:Policy>
  <wsp:ExactlyOne>
    <wsp:All>
      <wsrm:RMAssertion [wsp:Optional="true"]> ...>
        <wsp:Policy>
          <wsrmp:SequenceTransportSecurity/>
        </wsp:Policy>
      </wsrm:RMAssertion>
      <sp:TransportBinding ...>
        ...
      </sp:TransportBinding>
    <wsp:All>
  <wsp:ExactlyOne>
</wsp:Policy>
```

The following describes the content model of the `SequenceTransportSecurity` element.

`/wsrmp:SequenceTransportSecurity`

> A policy assertion that specifies that any Sequences targeted to the indicated endpoint MUST be bound to the underlying session(s) of the transport-level security used to carry messages related to the Sequence.

This form of the RM Assertion says that an endpoint MAY have RM as an option but always requires HTTPS to be used. All the `SequenceTransportSecurity` assertion indicates is that RM's rules for protecting the Sequence over TLS are followed.

3 Security Considerations

It is strongly RECOMMENDED that policies and assertions be signed to prevent tampering.

It is RECOMMENED that policies SHOULD NOT be accepted unless they are signed and have an associated security token to specify the signer has proper claims for the given policy. That is, a relying party shouldn't rely on a policy unless the policy is signed and presented with sufficient claims to pass the relying parties acceptance criteria.

It should be noted that the mechanisms described in this document could be secured as part of a SOAP message using WS-Security [WS-Security] or embedded within other objects using object-specific security mechanisms.

Appendix A. Schema

A normative copy of the XML Schema [XML-Schema Part1, XML-Schema Part2] description for this specification may be retrieved from the following address:

```
http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.1-schema-200702.xsd
```

The following copy is provided for reference.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright(C) OASIS(R) 1993-2007. All Rights Reserved.
     OASIS trademark, IPR and other policies apply.  -->
<xs:schema xmlns:tns="http://docs.oasis-open.org/ws-rx/wsrmp/200702"
xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="http://docs.oasis-
open.org/ws-rx/wsrmp/200702" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <xs:element name="RMAssertion">
    <xs:complexType>
      <xs:sequence>
        <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="SequenceSTR">
    <xs:complexType>
      <xs:sequence/>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="SequenceTransportSecurity">
    <xs:complexType>
      <xs:sequence/>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="DeliveryAssurance">
    <xs:complexType>
      <xs:sequence>
        <xs:any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="ExactlyOnce">
    <xs:complexType>
      <xs:sequence/>
    </xs:complexType>
  </xs:element>
  <xs:element name="AtLeastOnce">
    <xs:complexType>
      <xs:sequence/>
    </xs:complexType>
  </xs:element>
  <xs:element name="AtMostOnce">
    <xs:complexType>
      <xs:sequence/>
    </xs:complexType>
  </xs:element>
  <xs:element name="InOrder">
    <xs:complexType>
      <xs:sequence/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Appendix B. Acknowledgments

This document is based on initial contribution to OASIS WS-RX Technical Committee by the following authors:

Stefan Batres-Editor, Microsoft
Ruslan Bilorusets, BEA
Don Box, Microsoft
Luis Felipe Cabrera, Microsoft
Derek Collison, TIBCO Software
Donald Ferguson, IBM
Christopher Ferris, IBM
Tom Freund, IBM
Mary Ann Hondo, IBM
John Ibbotson, IBM
Lei Jin, BEA
Chris Kaler, Microsoft
David Langworthy, Microsoft
Amelia Lewis, TIBCO Software
Rodney Limprecht, Microsoft
Steve Lucco, Microsoft
Don Mullen, TIBCO Software
Anthony Nadalin, IBM
Mark Nottingham, BEA
David Orchard, BEA
Shivajee Samdarshi, TIBCO Software
John Shewchuk, Microsoft
Tony Storey, IBM

The following individuals have provided invaluable input into the initial contribution:

Keith Ballinger, Microsoft
Allen Brown, Microsoft
Michael Conner, IBM
Francisco Curbera, IBM
Steve Graham, IBM
Pat Helland, Microsoft
Rick Hill, Microsoft
Scott Hinkelman, IBM
Tim Holloway, IBM
Efim Hudis, Microsoft
Johannes Klein, Microsoft
Frank Leymann, IBM
Martin Nally, IBM
Peter Niblett, IBM
Jeffrey Schlimmer, Microsoft
Chris Sharp, IBM
James Snell, IBM
Keith Stobie, Microsoft
Satish Thatte, Microsoft
Stephen Todd, IBM
Sanjiva Weerawarana, IBM
Roger Wolter, Microsoft

The following individuals were members of the committee during the development of this specification:

Abbie Barbir, Nortel
Charlton Barreto, Adobe
Stefan Batres, Microsoft
Hamid Ben Malek, Fujitsu
Andreas Bjarlestam, Ericsson
Toufic Boubez, Layer 7
Doug Bunting, Sun
Lloyd Burch, Novell
Steve Carter, Novell
Martin Chapman, Oracle
Dave Chappell, Sonic
Paul Cotton, Microsoft
Glen Daniels, Sonic
Doug Davis, IBM
Blake Dournaee, Intel
Jacques Durand, Fujitsu
Colleen Evans, Microsoft
Christopher Ferris, IBM
Paul Fremantle, WSO2
Robert Freund, Hitachi
Peter Furniss, Erebor
Marc Goodner, Microsoft
Alastair Green, Choreology
Mike Grogan, Sun
Ondrej Hrebicek, Microsoft
Kazunori Iwasa, Fujitsu
Chamikara Jayalath, WSO2
Lei Jin, BEA
Ian Jones, BTplc
Anish Karmarkar, Oracle
Paul Knight, Nortel
Dan Leshchiner, Tibco
Mark Little, JBoss
Lily Liu, webMethods
Matt Lovett, IBM
Ashok Malhotra, Oracle
Jonathan Marsh, Microsoft
Daniel Millwood, IBM
Jeff Mischkinsky, Oracle
Nilo Mitra, Ericsson
Peter Niblett, IBM
Duane Nickull, Adobe
Eisaku Nishiyama, Hitachi
Dave Orchard, BEA

Chouthri Palanisamy, NEC
Sanjay Patil, SAP
Gilbert Pilz, BEA
Martin Raepple, SAP
Eric Rajkovic, Oracle
Stefan Rossmanith, SAP
Tom Rutt, Fujitsu
Rich Salz, IBM
Shivajee Samdarshi, Tibco
Vladimir Videlov, SAP
Claus von Riegen, SAP
Pete Wenzel, Sun
Steve Winkler, SAP
Ümit Yalçinalp, SAP
Nobuyuki Yamamoto, Hitachi