OASIS

Web Services Reliable Messaging Policy Assertion (WS-RM Policy) Version 1.1

OASIS Standard

14 June 2007

Specification URIs:
This Version:
> http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.1-spec-os-01.pdf
> http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.1-spec-os-01.html
> http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.1-spec-os-01.doc

Previous Version:
> http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.1-spec-cs-01.pdf
> http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.1-spec-cs-01.html
> http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.1-spec-cs-01.doc

Latest Version:
> http://docs.oasis-open.org/ws-rx/wsrmp/v1.1/wsrmp.pdf
> http://docs.oasis-open.org/ws-rx/wsrmp/v1.1/wsrmp.html
> http://docs.oasis-open.org/ws-rx/wsrmp/v1.1/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 v1.0

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

Copyright © OASIS® 1993–2007. All Rights Reserved. OASIS trademark, IPR and other policies apply.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

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

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/

156 157 158	**[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/
159 160 161 162	**[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
163 164 165	**[WS-RM]**	OASIS WS-RX Technical OASIS Standard, "Web Services Reliable Messaging (WS-ReliableMessaging)," June 2007. http://docs.oasis-open.org/ws-rx/wsrm/v1.1/wsrm.pdf
166 167	**[WSDL 1.1]**	W3C Note, "Web Services Description Language (WSDL 1.1)," 15 March 2001. http://www.w3.org/TR/2001/NOTE-wsdl-20010315
168 169 170	**[XML]**	W3C Recommendation, "Extensible Markup Language (XML) 1.0 (Fourth Edition)", September 2006. http://www.w3.org/TR/REC-xml/
171 172	**[XML-ns]**	W3C Recommendation, "Namespaces in XML," 14 January 1999. http://www.w3.org/TR/1999/REC-xml-names-19990114/
173 174	**[XML-Schema Part1]**	W3C Recommendation, "XML Schema Part 1: Structures," October 2004. http://www.w3.org/TR/xmlschema-1/
175 176	**[XML-Schema Part2]**	W3C Recommendation, "XML Schema Part 2: Datatypes," October 2004. http://www.w3.org/TR/xmlschema-2/
177 178 179	**[XPATH 1.0]**	W3C Recommendation, "XML Path Language (XPath) Version 1.0," 16 November 1999. http://www.w3.org/TR/xpath

180 1.3 Non Normative

181 182 183	**[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
184 185 186	**[SecurityPolicy]**	G. Della-Libra, et. al. "Web Services Security Policy Language (WS-SecurityPolicy)", July 2005 http://specs.xmlsoap.org/ws/2005/07/securitypolicy/ws-securitypolicy.pdf
187 188 189 190 191 192	**[WS-Policy]**	W3C Member Submission "Web Services Policy 1.2 - Framework", April 2006 http://www.w3.org/Submission/2006/SUBM-WS-Policy-20060425/ W3C ~~Candidate~~ Recommendation, "Web Services Policy 1.5 - Framework," ~~September~~February 2007. http://www.w3.org/TR/2007/REC~~CR~~-ws-policy-20070~~904~~228
193 194 195 196 197 198 199	**[WS-PolicyAttachment]**	W3C Member Submission "Web Services Policy 1.2 - Attachment", April 2006 http://www.w3.org/Submission/2006/SUBM-WS-PolicyAttachment-20060425/ W3C ~~Candidate~~ Recommendation, "Web Services Policy 1.5 - Attachment," ~~February~~ September 2007. http://www.w3.org/TR/2007/REC~~CR~~-ws-policy-attach-20070~~904~~228
200 201 202 203 204	**[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

Field Code Changed

Field Code Changed

205	
206	Anthony Nadalin, Chris Kaler, Phillip Hallam-Baker, Ronald Monzillo, eds. "OASIS
207	Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", OASIS
208	Standard 200602, February 2006.
209	http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

1.4 Namespace

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

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

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

215 Table 1 lists the XML namespaces that are used in this specification. The choice of any namespace prefix
216 is arbitrary and not semantically significant. The assertions defined within this specification have been
217 designed to work independently of a specific version of WS-Policy. At the time of the publication of this
218 specification the versions of WS-Policy known to correctly compose with this specification are WS-Policy
219 1.2 and 1.5. Within this specification the use of the namespace prefix wsp refers generically to the WS-
220 Policy namespace, not a specific version.

221 Table 1

Prefix	Namespace	Specification
wsdl	http://schemas.xmlsoap.org/wsdl/	[WSDL 1.1]
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

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

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

1.5 Conformance

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

230 Normative text within this specification takes precedence over normative outlines, which in turn take
231 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

303 /wsrmp:RMAssertion/{any}

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

306 /wsrmp:RMAssertion/@{any}

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

2.3 Assertion Attachment

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

311 • Endpoint Policy Subject

312 • Message Policy Subject

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

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

318 • wsdl:message

319 • wsdl:portType/wsdl:operation/wsdl:input

320 • wsdl:portType/wsdl:operation/wsdl:output

321 • wsdl:portType/wsdl:operation/wsdl:fault

322 • wsdl:portType

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

325 • wsdl:port

326 • wsdl:binding

327 • wsdl:binding/wsdl:operation/wsdl:input

328 • wsdl:binding/wsdl:operation/wsdl:output

329 • wsdl:binding/wsdl:operation/wsdl:fault

330 If an RM policy assertion is attached to any of:

331 • wsdl:binding/wsdl:operation/wsdl:input

332 • wsdl:binding/wsdl:operation/wsdl:output

333 • wsdl:binding/wsdl:operation/wsdl:fault

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

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

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

350 In the case where an optional RM Assertion applies to an output message, there is no requirement on the
351 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://schemas.xmlsoap.org/ws/2004/09/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>
```

```
400        <wsrmp:SequenceSTR/>
401      <wsp:Policy>
402    </wsrmp:RMAssertion>
```

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

404 /wsrmp:SequenceSTR

405   A policy assertion that specifies security requirements which MUST be used with an RM Sequence

406   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

408 This version of the RM assertion includes the requirement that an RM Sequence MUST be bound to the

409 session(s) of the underlying transport-level security protocol (e.g. SSL/TLS) used to carry the

410 `CreateSequence` and `CreateSequenceResponse` messages.

411 This assertion MUST apply to [Endpoint Policy Subject]. This assertion MUST be used in conjunction with

412 the `sp:TransportBinding` assertion that requires the use of some transport-level security mechanism

413 (e.g. `sp:HttpsToken`).

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

```
415    <wsp:Policy>
416      <wsp:ExactlyOne>
417        <wsp:All>
418          <wsrm:RMAssertion [wsp:Optional="true"]> ...>
419            <wsp:Policy>
420              <wsrmp:SequenceTransportSecurity/>
421            </wsp:Policy>
422          </wsrm:RMAssertion>
423          <sp:TransportBinding ...>
424            ...
425          </sp:TransportBinding>
426        <wsp:All>
427      <wsp:ExactlyOne>
428    </wsp:Policy>
```

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

430 /wsrmp:SequenceTransportSecurity

431   A policy assertion that specifies that any Sequences targeted to the indicated endpoint MUST be

432   bound to the underlying session(s) of the transport-level security used to carry messages related to the

433   Sequence.

434 This form of the RM Assertion says that an endpoint MAY have RM as an option but always requires

435 HTTPS to be used. All the `SequenceTransportSecurity` assertion indicates is that RM's rules for

436 protecting the Sequence over TLS are followed.

| Formatted: Font: (Default) Courier New |

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>
```

```
501        </xs:element>
502        <xs:element name="InOrder">
503          <xs:complexType>
504            <xs:sequence/>
505          </xs:complexType>
506        </xs:element>
507    </xs:schema>
```
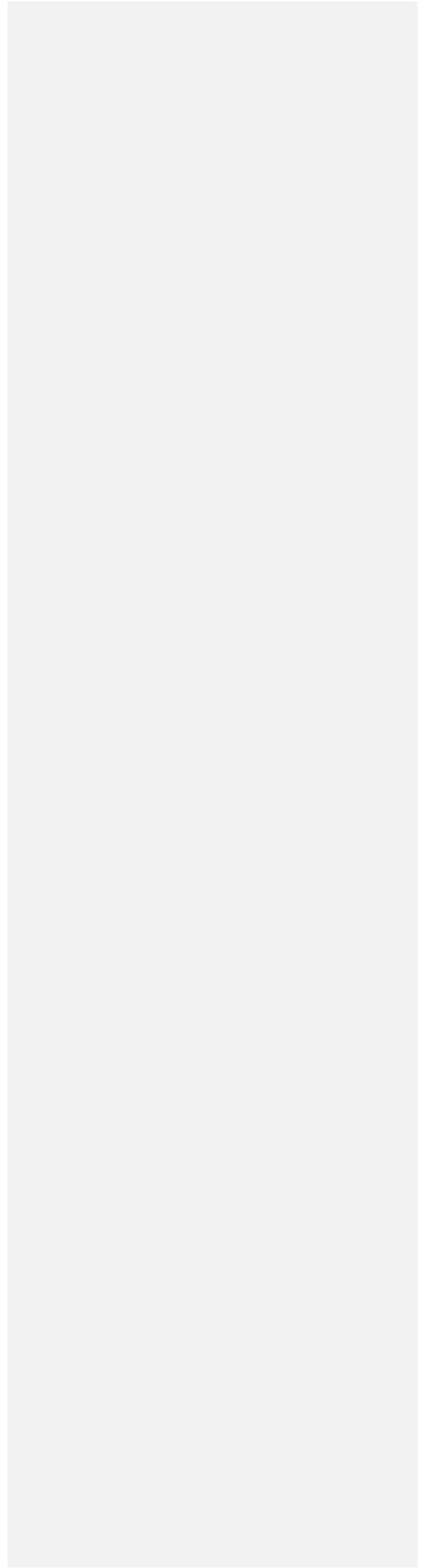
Appendix B. Acknowledgments

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

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

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

602   Chouthri Palanisamy, NEC   610   Shivajee Samdarshi, Tibco
603   Sanjay Patil, SAP   611   Vladimir Videlov, SAP
604   Gilbert Pilz, BEA   612   Claus von Riegen, SAP
605   Martin Raepple, SAP   613   Pete Wenzel, Sun
606   Eric Rajkovic, Oracle   614   Steve Winkler, SAP
607   Stefan Rossmanith, SAP   615   Ümit Yalçinalp, SAP
608   Tom Rutt, Fujitsu   616   Nobuyuki Yamamoto, Hitachi
609   Rich Salz, IBM

617