



INFORMATION SERVICES BOARD

Scott Came
Department of Information Services

Laura Parma
Department of Information Services
Enterprise Architecture Committee Steward

Web Services Service Interaction Profile

ISB Standards

Version 4.1

September 14, 2006

Information Services Board
Enterprise Architecture Committee

Sue Fleener, *Washington State Patrol*
Cathy Munson, *Legislative Service Center*
Co-Chairs

Scott Came, *Department of Information Services*
Chief Enterprise Architect

1110 Jefferson Street SE
P.O. Box 42445
Olympia, WA 98504-2445
Phone 360/902.3519
Fax 360/902.2982
ScottCa@dis.wa.gov

Table of Contents

1. Document History 3

2. Document Context 3

3. Introduction and Purpose 4

 3.1. Usage 4

 3.2. Scope 5

4. Conformance Requirements..... 5

 4.1. Conformance Targets 5

 4.2. General Conformance Requirements 5

5. Service Interaction Requirements 6

 5.1. Service Consumer Authentication 6

 5.2. Service Consumer Authorization 6

 5.3. Service Authentication 7

 5.4. Message Non-Repudiation 7

 5.5. Message Integrity..... 7

 5.6. Message Confidentiality..... 7

 5.6.1. Encryption Algorithm 7

 5.7. Message Addressing 8

 5.8. Reliability..... 8

 5.9. Transaction Support..... 8

 5.10. Service Metadata Availability 8

 5.11. Large Message Handling 8

 5.12. Service Availability 9

 5.13. Service Responsiveness..... 9

6. Interface Description Requirements 9

7. Message Exchange Patterns..... 9

 7.1. Fire-and-Forget Pattern 9

 7.2. Request-Response Pattern..... 10

8. Message Definition Mechanisms 10

9. Execution Context Requirements 10

 9.1. Security Requirements..... 10

 9.2. Reliability Requirements 10

 9.3. Transaction Support Requirements 11

 9.4. General Interaction Requirements..... 11

10. Glossary..... 11

11. References 12

Appendix A: Documenter Team 14

Appendix B: Review Log 15

1. Document History

Date	Version	Editor	Change
March 17, 2006	1.0	Scott Came	Initial sketch / rough draft
April 14, 2006	1.1	Scott Came	Initial complete draft for Documenter Team review
May 26, 2006	1.2	Scott Came	Added scope section at EAC request
June 9, 2006	1.3	Scott Came	Change standards to guidelines
June 14, 2006	2.0	Scott Came	Endorsed by EAC
September 14, 2006	4.0	Scott Came	Adopted by ISB
October 23, 2006	4.1	Trina Regan	Change guidelines to standards

2. Document Context

This document currently has ISB Standard status. This status signifies that the document has been adopted as standards by a vote of the Information Services Board. For more information about the ISB Enterprise Architecture Committee and its initiative, please visit the EA Committee website at: <http://isb.wa.gov/committees/enterprise/Default.aspx>.

3. Introduction and Purpose

The purpose of this standard is to establish a **SERVICE INTERACTION PROFILE**[†] based on the web services family of technology standards.

A service interaction profile is an element identified in the Conceptual Integration Technical Reference Architecture (**[TRA]**). This element defines an approach to meeting the basic requirements necessary for interaction between **SERVICE CONSUMERS** and **SERVICES**. The approach utilizes a cohesive or natural grouping of technologies, standards, or techniques in meeting those basic interaction requirements. A profile establishes a basis for interoperability between service consumer systems and services that agree to utilize that profile for interaction.

A service interaction profile defines a guideline for **SERVICE INTERFACES**. Every service interface shared between two or more agencies in the state enterprise should conform to exactly one service interaction profile. Service consumers that interact with an interface should likewise conform to that interface's profile.

This profile is based on the web services family of technology standards, which is defined as follows:

- The Web Services Interoperability Organization (WS-I) Basic Profile, version 1.1 (noted in this document as **[WS-I BP]**[‡]) and all standards that it references
- The WS-I Attachments Profile (**[WS-I AP]**), version 1.0 and all standards that it references
- The WS-I Basic Security Profile current Working Group Draft (dated January 20, 2006, noted in this document as **[WS-I BSP]**), all current Token Profiles adopted as Working Group Drafts (dated January 20, 2006), and all standards that it references
- Other standards developed by the World Wide Web Consortium (W3C) or the Organization for the Advancement of Structured Information Standards (OASIS) explicitly identified in this document
- If no standard is available from WS-I, W3C, or OASIS to meet an identified requirement, then specifications developed by (and issued under the copyright of) a group of two or more companies

3.1. Usage

This standard is intended to serve as a guideline for how to exchange information between information systems, by meeting the common interaction requirements identified in **[TRA]**. It assumes that the reader is familiar with the conceptual architecture established in **[TRA]**, and that the reader interprets this document as a service interaction profile defined in the context of that architecture.

This standard is intended to be used as part of the technical requirements associated with the integration of information systems. The architecture defined in **[TRA]** identifies other important technical requirements associated with integration that the reader should consider. In addition, other service interaction profiles may exist within the architecture; these also should be considered as viable approaches to the exchange of information between systems.

[†] Words or phrases formatted in this **STYLE** are defined in the Glossary.

[‡] Abbreviations formatted in this **[style]** represent citations defined in the References section below.

40 System technical requirements specifications, including procurement documents such as
41 Requests for Proposals, could incorporate this standard as a required approach to system
42 integration.

43 **3.2. Scope**

44 These standards apply to executive and judicial branch agencies and educational institutions.
45 Academic and research applications at institutions of higher education are exempted.

46 In this document, the terms “state agency” and “agency” mean any agency or institution within the
47 scope of the previous paragraph, and the term “state enterprise” means all agencies and
48 institutions (collectively) within the scope of the previous paragraph.

49 **4. Conformance Requirements**

50 This section describes what it means to “conform to” this service interaction profile.

51 **4.1. Conformance Targets**

52 A conformance target is a component involved in the integration of the functionality of two or
53 more information systems, where the component must adhere to one or more rules established in
54 this service interaction profile. All of these components are concepts defined in [TRA].

55 This profile identifies the following conformance targets:

- 56 • **SERVICE INTERFACE**
- 57 • **SERVICE CONSUMER**
- 58 • **MESSAGE**

59 To conform to this service interaction profile, an approach to the integration of two or more
60 information systems must:

- 61 • Identify and implement all of the conformance targets listed above, in a way consistent
62 with their definitions in [TRA]
- 63 • Meet all of the requirements for each of these targets established in this service
64 interaction profile

65 **4.2. General Conformance Requirements**

66 A **SERVICE INTERFACE** conforms to this service interaction profile if:

- 67 • The interface’s description meets all requirements of the DESCRIPTION conformance
68 target in [WS-I BP].
- 69 • The interface meets all requirements of the INSTANCE and RECEIVER conformance
70 targets in [WS-I BP].

71 A **SERVICE CONSUMER** conforms to this service interaction profile if:

- 72 • The consumer meets all requirements of the CONSUMER and SENDER conformance
73 targets in [WS-I BP].

74 A **MESSAGE** conforms to this service interaction profile if:

- 75 • The message meets all requirements of the MESSAGE and ENVELOPE conformance
76 targets in [WS-I BP]

5. Service Interaction Requirements

This section demonstrates how this standard meets the Service Interaction Requirements defined in the [TRA]. This standard does not repeat the definition of each requirement.

Note that the following Service Interaction Requirements will not be requirements of every service interaction in the state enterprise. However, if a service has one or more of these interaction requirements, then an interface to that service must meet those requirements as indicated below in order for the interface to conform to this profile.

5.1. Service Consumer Authentication

This service interaction profile continues the state's practice of authenticating participants in the integration of information systems primarily by verifying the identity, location, and organizational ownership and control of the hardware node sending each message. Integration of systems within the state's security perimeter—that is, within the State Government Network—will continue to rely on the security features of that network, as documented in the State Government Network Solution Set and Information Services Board security policies and standards. Agencies will also continue to set firewall rules and policies to enforce specific authentication requirements. Integration of systems across the state's security perimeter—that is, between the State Government Network and the Intergovernmental Network, K20 Network, or public Internet—will continue to use security gateways designed to secure access across the perimeter.

If a **SERVICE** requires consumer authentication stronger or more specific than the access controls provided by the state's security perimeter or security gateways combined with agency-enforced firewall policies or rules, then conformance with this service interaction profile requires that the **MESSAGE(S)** sent to the **SERVICE INTERFACE** by a **SERVICE CONSUMER** meet these consumer authentication requirements as follows.

- Each **MESSAGE** must meet the requirements of section 5 of [WS-I BSP], "SOAP Message Security".
- Each **MESSAGE** must contain one or more security tokens that meet the requirements of Section 7 of [WS-I BSP], "X.509 Certificate Token Profile".
- Each **MESSAGE** must not contain security tokens of any other type, even if such type is permitted by [WS-I BSP].

Note that these mechanisms still rely on the identification of the hardware node that sends messages as or on behalf of the service consumer. However, instead of relying solely on transport-layer mechanisms such as IP addresses or MPLS labels to verify the source of each message, they rely on a digital certificate for additional verification of the sending node's identity.

This profile's satisfaction of Service Consumer Authentication requirements relies on mechanisms in **EXECUTION CONTEXT**. See section 9.1.

5.2. Service Consumer Authorization

This version of this service interaction profile does not support the transmission of authorization assertions from a **SERVICE CONSUMER** to a **SERVICE**.

Section 5.1 above describes how service consumers supply proof of identity if required by a service. Once in possession of consumer identity, a service can query data sources internal to its implementation or available through other services to determine what actions, if any, the consumer is authorized to invoke on the service.

119 5.3. Service Authentication

120 This version of this service interaction profile relies on transport-level mechanisms to allow
121 **SERVICE CONSUMERS** to authenticate **SERVICE INTERFACES**. In particular, if a **SERVICE INTERFACE**
122 provides a method for consumers to authenticate it, the method must be for the consumer to
123 access the interface over HTTP/S.

124 When a **SERVICE INTERFACE** is available over HTTP/S, the interface must meet the requirements
125 of an **INSTANCE** in **[WS-I BP]**, section 6.1.

126 5.4. Message Non-Repudiation

127 If interaction between a **SERVICE CONSUMER** and **SERVICE** requires non-repudiation of a **MESSAGE**,
128 the sender of the **MESSAGE** must:

- 129 • Include a creation timestamp in the manner prescribed in Section 10 of **[WS-Security]**.
- 130 • Create a digital signature of the creation timestamp and the part of the message requiring
131 non-repudiation, which may be the entire message. This signature must conform to the
132 requirements of **[WS-I BSP]** Section 8.

133 By itself, this method does not provide for absolute non-repudiation.[†] The business parties (e.g.,
134 agencies) involved in the service interaction should supplement the technical approach here with
135 a written agreement that establishes whether, and under what circumstances, they permit
136 repudiation.

137 Note that **[WS-Security]** provides an example of this technical approach in Section 11.

138 5.5. Message Integrity

139 This service interaction profile meets the requirement of message integrity by signing all or part of
140 a **MESSAGE** using **[XML Signature]**. The **MESSAGE** must meet all requirements of **[WS-I BSP]**
141 Section 8.

142 This profile's satisfaction of Message Integrity requirements relies on mechanisms in **EXECUTION**
143 **CONTEXT**. See section 9.1.

144 5.6. Message Confidentiality

145 This service interaction profile meets the requirement of message confidentiality by encrypting all
146 or part of a **MESSAGE** using **[XML Encryption]** as further specified and constrained in **[WS-I BSP]**.

147 Confidential elements or sections of a **MESSAGE** must meet the requirements associated with
148 **ENCRYPTED_DATA** in **[WS-I BSP]**, Section 9.

149 This profile's satisfaction of Message Confidentiality requirements relies on mechanisms in
150 **EXECUTION CONTEXT**. See section 9.1.

151 5.6.1. Encryption Algorithm

152 Conformance with this service interaction profile requires that, if encryption of data is required,
153 the Triple-DES encryption algorithm, as described in chapter 12 of **[Schneier]**, must be used,
154 and that the **ED_ENCRYPTION_METHOD** Algorithm attribute must have the value
155 "http://www.w3.org/2001/04/xmlenc#tripleledes-cbc," as required by Section 9.4 of **[WS-I BSP]**.

[†] A detailed explanation of the difficulty in using digital signatures with timestamps to implement non-repudiation is available in **[Schneier]**, pages 40-41.

156 5.7. Message Addressing

157 Conformance with this profile requires that every message conform to the WS-Addressing 1.0
158 Core ([**WS-Addressing Core**]) and SOAP Binding ([**WS-Addressing SOAP Binding**])
159 specifications, as described in Section 8 of [**WS-Addressing SOAP Binding**]. Conformance of
160 messages with the WS-Addressing 1.0 WSDL Binding ([**WS-Addressing WSDL Binding**]) is
161 recommended but not required at this time.

162 5.8. Reliability

163 If interaction between a **SERVICE CONSUMER** and **SERVICE** requires reliable delivery of a **MESSAGE**,
164 then the **MESSAGE** must contain SOAP headers that conform to the requirements of the OASIS
165 WS-Reliable Messaging standard ([**WS-RM**]).

166 This profile's satisfaction of Reliability requirements relies on mechanisms in **EXECUTION CONTEXT**.
167 See section 9.2.

168 5.9. Transaction Support

169 If interaction between a group of **SERVICE CONSUMERS** and **SERVICES** requires transaction support,
170 then the following must be true of the **CONSUMERS**, **SERVICES**, and **MESSAGES** involved in the
171 interaction:

- 172 • The consumers and services must meet the behavioral requirements of “applications”
173 and “participants” as defined in [**WS-Coordination**], [**WS-Atomic Transaction**], and
174 [**WS-Business Activity**], as appropriate depending on the nature of the transaction
175 requirements.
- 176 • Messages must include the appropriate Coordination Context SOAP header to identify
177 the transactional activity, as defined in [**WS-Coordination**], and as further specified in
178 [**WS-Atomic Transaction**] or [**WS-Business Activity**], as appropriate depending on the
179 nature of the transaction requirements.

180 The description of the service interface for each service involved in the interaction must conform
181 to the policy assertion requirements identified in Section 5 of [**WS-Atomic Transaction**] and
182 Section 4 of [**WS-Business Activity**], as appropriate, depending on the nature of the transaction
183 requirements.

184 This profile's satisfaction of Transaction Support requirements relies on mechanisms in
185 **EXECUTION CONTEXT**. See section 9.3.

186 5.10. Service Metadata Availability

187 If a **SERVICE INTERFACE** responds to requests for metadata about the interface and underlying
188 service, it must do so by responding to a service consumer's Get Metadata Request **MESSAGE** or
189 Get Request **MESSAGE** with a Get Metadata Response **MESSAGE** or Get Response **MESSAGE**,
190 respectively, where these messages conform to the requirements of the WS-Metadata Exchange
191 specification ([**WS-Metadata Exchange**]).

192 5.11. Large Message Handling

193 There is no fixed limit to the size of an **HTTP** request or response, nor is there a limit to the size of
194 a **SOAP MESSAGE**, which means there is no limit to the size of a message transmitted according
195 to this service interaction profile. The state's choice of **EXECUTION CONTEXT** should ensure that
196 underlying transport technologies are capable of transmitting large messages within this profile.

197 If in a particular situation it is not feasible to represent a large message as a SOAP message, it
198 may be advisable to transmit the large message as an attachment to a smaller SOAP body.

199 Emerging web services specifications, such as [XOP] and [MTOM] may prove viable for
200 improving the transmission of large messages via web services. However, support for these
201 specifications is not strong enough yet to warrant adoption of these specifications as standards
202 within this profile.

203 5.12. Service Availability

204 This service interaction profile relies on the EXECUTION CONTEXT to meet availability requirements.

205 5.13. Service Responsiveness

206 This service interaction profile relies on the EXECUTION CONTEXT to meet responsiveness
207 requirements.

208 6. Interface Description Requirements

209 This section demonstrates how this profile meets the Service Description Requirements identified
210 in the Integration Technical Reference Architecture.

211 Section 4.2 above indicates that a SERVICE INTERFACE conforms to this service interaction profile if
212 its description meets all requirements of the DESCRIPTION conformance target in [WS-I BP].
213 [WS-I BP] requires an interface's description to consist of a Web Services Description Language
214 (WSDL) document that conforms to [WSDL 1.1].

215 The WSDL document must include the following child elements of the `wsdl:definitions`
216 element:

- 217 • at least one `wsdl:message` element for each MESSAGE involved in the interaction with
218 the SERVICE
- 219 • within the `wsdl:portType` and `wsdl:binding` elements, a `wsdl:operation`
220 element corresponding to each action in the service's behavior model (as defined in
221 [TRA])

222 Note that many of the standards referenced by this profile require use of particular SOAP
223 headers. The WSDL document that describes a service interface must describe these headers in
224 conformance with the guidance of these standards.

225 7. Message Exchange Patterns

226 This section documents how this profile supports the Message Exchange Patterns identified in
227 the Integration Technical Reference Architecture.

228 7.1. Fire-and-Forget Pattern

229 The fire-and-forget message exchange pattern corresponds to a one-way operation as defined in
230 [WSDL 1.1]. This service interaction profile supports this pattern by requiring that SERVICE
231 CONSUMERS and SERVICE INTERFACES conform to [WS-I BP]. In particular, section 4.7.9 of [WS-I
232 BP] requires that a service interface respond to a one-way operation by returning an HTTP
233 response with an empty entity-body.

234 7.2. Request-Response Pattern

235 The request-response message exchange pattern corresponds to a request-response operation
236 as defined in **[WSDL 1.1]**. This service interaction profile supports this pattern by requiring that
237 **SERVICE CONSUMERS** and **SERVICE INTERFACES** conform to **[WS-I BP]**.

238 8. Message Definition Mechanisms

239 This section demonstrates how this profile supports the Message Definition Mechanisms
240 identified in the Integration Technical Reference Architecture.

241 This service interaction profile requires that each **MESSAGE** consist of one, but not both, of the
242 following:

- 243 • A single SOAP message (defined as the MESSAGE conformance target in **[WS-I BP]**)
244 that meets all requirements of this profile
- 245 • A SOAP message package (as defined in **[SwA]** and as constrained by **[WS-I AP]**)

246 Note that **[WS-I BP]** and **[WS-I AP]** require that the single SOAP message, in the first case
247 above, or the “root part” of the SOAP message package, in the second case, be well-formed
248 XML. This XML must be valid against an XML Schema (as defined in **[XML Schema]**) that
249 defines the message structure.

250 The names of all elements in this XML Schema must conform to the guidelines documented in
251 **[SMG]**.

252 9. Execution Context Requirements

253 This section describes what this profile requires of **EXECUTION CONTEXT**. Consult **[TRA]** for a
254 complete definition of **EXECUTION CONTEXT**.

255 9.1. Security Requirements

256 Implementation of the Service Consumer Authentication, Message Integrity, and Message
257 Confidentiality service interaction requirements, as described by this profile, requires the following
258 of **EXECUTION CONTEXT**:

- 259 • Public Key Infrastructure (PKI) to manage digital certificates for hardware nodes that
260 need to create or process digital signatures and encrypted messages
- 261 • Digital certificates managed by the PKI must support the following attributes as defined in
262 **[RFC 3280]**: keyEncipherment, dataEncipherment, digitalSignature, and nonRepudiation

263 If practical, the interface to the PKI mentioned above should conform to the requirements of the
264 WS-Trust specification (**[WS-Trust]**).

265 9.2. Reliability Requirements

266 Implementation of the Reliability service interaction requirement, as described by this profile,
267 requires **EXECUTION CONTEXT** elements that implement the RM Source and RM Destination
268 components identified in **[WS-RM]**. Any **EXECUTION CONTEXT** that fully implements these
269 requirements conforms to this Service interaction profile.

270 9.3. Transaction Support Requirements

271 Implementation of the Transaction Support service interaction requirement, as described by this
272 profile, requires **EXECUTION CONTEXT** elements that implement the Activation and Registration
273 services identified in **[WS-Coordination]**. The implementation of these services must conform to
274 the behavioral requirements identified in **[WS-Atomic Transaction]** and **[WS-Business Activity]**.

275 9.4. General Interaction Requirements

276 The state's choice of execution context must support the following:

- 277 • Transmission of messages, including messages up to 1 gigabyte in size, from service
278 consumer to service interface via HTTP, as required by the **[WS-I BP]**
- 279 • Satisfaction of minimum availability and responsiveness requirements, as identified
280 above and in the Conceptual Integration Technical Reference Architecture

281 10. Glossary

282	EXECUTION CONTEXT	The set of technical and business elements that form a path between those with needs and those with capabilities and that permit service providers and consumers to interact.
283		
284		
285		
286	HTTP	HyperText Transport Protocol is the protocol used to transport requests and replies over the World Wide Web
287		
288	MESSAGE	The entire “package” of information sent between service consumer and service (or vice versa), including any logical partitioning of the message into segments or sections.
289		
290		
291		
292	MPLS	MultiProtocol Label Switching is a technology for speeding up network traffic flow and making it easier to manage. It consists of a family of Internet Engineering Task Force (IETF) standards in which Internet Protocol networks can make packet forwarding decisions based on a pre-allocated label between the layer 2 and layer 3 headers of a packet.
293		
294		
295		
296		
297		
298		
299	SERVICE	The means by which the needs of a consumer are brought together with the capabilities of a provider. A service is the way in which one partner gains access to a capability offered by another partner.
300		
301		
302		
303	SERVICE CONSUMER	An entity which seeks to satisfy a particular need through the use capabilities offered by means of a service
304		
305		
306	SERVICE INTERACTION PROFILE	A family of standards or other technologies or techniques that together demonstrate implementation or satisfaction of all the requirements of interaction with a service. See section 5.2.5.1 of [TRA] for details.
307		
308		
309		
310	SERVICE INTERFACE	The means by which the underlying capabilities of a service are accessed. A service interface is the means for interacting with a service. It includes the specific protocols, commands, and information exchange by which actions are initiated on the service. A service
311		
312		
313		
314		

315 interface is what a system designer or implementer
316 (programmer) uses to design or build executable
317 software that interacts with the service.

318 11. References

319 These references use the following acronyms to represent standards organizations.

- 320 • IETF: Internet Engineering Task Force
- 321 • OASIS: Organization for the Advancement of Structured Information Standards
- 322 • W3C: World Wide Web Consortium
- 323 • WS-I: Web Services Interoperability Organization

324

325 **MTOM** W3C (2004). *SOAP Message Transmission Optimization*
326 *Mechanism*, W3C Candidate Recommendation.
327 Retrieved April 14, 2006 from
328 <http://www.w3.org/TR/soap12-mtom/>

329 **RFC 3280** IETF (2002). *Internet X.509 Public Key Infrastructure*
330 *Certificate and Certificate Revocation List (CRL) Profile*.
331 Retrieved April 14, 2006 from
332 <http://www.ietf.org/rfc/rfc3280.txt?number=3280>.

333 **Schneier** Bruce Schneier, *Applied Cryptography*, 2nd Ed, John
334 Wiley & Sons, Inc., 1996

335 **SMG** Washington State Department of Information Services,
336 Enterprise Architecture Program (2006). *Service*
337 *Modeling Guidelines*, Documenter Team Draft.

338 **SwA** W3C (2004). *SOAP Messages with Attachments*, W3C
339 Note. Retrieved April 14, 2006 from
340 <http://www.w3.org/TR/SOAP-attachments>

341 **TRA** Washington State Information Services Board,
342 Enterprise Architecture Committee (2006). *Conceptual*
343 *Integration Technical Reference Architecture*, Enterprise
344 Architecture Committee Document

345 **WS-I BP** WS-I (2004). *Basic Profile Version 1.1*. Retrieved April
346 14, 2006 from [http://www.ws-i.org/Profiles/BasicProfile-](http://www.ws-i.org/Profiles/BasicProfile-1.1.html)
347 [1.1.html](http://www.ws-i.org/Profiles/BasicProfile-1.1.html)

348 **WS-I AP** WS-I (2004). *Attachment Profile Version 1.0*. Retrieved
349 April 14, 2006 from [http://www.ws-](http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html)
350 [i.org/Profiles/AttachmentsProfile-1.0.html](http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html)

351 **WS-I BSP** WS-I (2004). *Basic Security Profile*, Working Group
352 Draft. Retrieved April 14, 2006 from [http://www.ws-](http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html)
353 [i.org/Profiles/BasicSecurityProfile-1.0.html](http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html)

354 **WS-Security** OASIS (2004). *Web Services Security: SOAP Message*
355 *Security 1.1*, OASIS Standard. Retrieved April 14, 2006
356 from <http://docs.oasis-open.org/wss/v1.1/>

357 **WS-Addressing Core** W3C (2004). *Web Services Addressing 1.0*, W3C
358 Member Submission. Retrieved April 14, 2006 from
359 <http://www.w3.org/Submission/ws-addressing/>

360	WS-Addressing SOAP Binding	W3C (2006). <i>Web Services Addressing 1.0 - SOAP Binding</i> , W3C Proposed Recommendation. Retrieved April 14, 2006 from http://www.w3.org/TR/ws-addr-soap
361		
362		
363	WS-Addressing WSDL Binding	W3C (2006). <i>Web Services Addressing 1.0 – WSDL Binding</i> , W3C Working Draft. Retrieved April 14, 2006 from http://www.w3.org/TR/ws-addr-wsdl
364		
365		
366	WS-RM	OASIS (2006). <i>Web Services Reliable Messaging</i> , Committee Draft. Retrieved April 14, 2006 from http://docs.oasis-open.org/ws-rx/wsrml/200602/wsrml-1.1-spec-cd-03.pdf
367		
368		
369		
370	WS-Coordination	OASIS (2006). <i>Web Services Coordination 1.1</i> , Committee Draft. Retrieved April 14, 2006 from http://docs.oasis-open.org/ws-tx/wstx-wscoor-1.1-spec-cd-01.pdf
371		
372		
373		
374	WS-Atomic Transaction	OASIS (2006). <i>Web Services Atomic Transaction 1.1</i> , Committee Draft. Retrieved April 14, 2006 from http://docs.oasis-open.org/ws-tx/wstx-wsat-1.1-spec-cd-01.pdf
375		
376		
377		
378	WS-Business Activity	OASIS (2006). <i>Web Services Business Activity 1.1</i> , Committee Draft. Retrieved April 14, 2006 from http://docs.oasis-open.org/ws-tx/wstx-wsba-1.1-spec-cd-01.pdf
379		
380		
381		
382	WS-Metadata Exchange	BEA Systems Inc., Computer Associates International, Inc., International Business Machines Corporation, Microsoft Corporation, Inc., SAP AG, Sun Microsystems, and webMethods (2004). <i>Web Services Metadata Exchange</i> . Retrieved April 14, 2006 from http://msdn.microsoft.com/ws/2004/09/ws-metadataexchange/
383		
384		
385		
386		
387		
388		
389	WSDL 1.1	W3C (2004). <i>Web Services Description Language version 1.1</i> , W3C Note. Retrieved April 14, 2006 from http://www.w3.org/TR/wsdl
390		
391		
392	WS-Trust	Actional Corporation, BEA Systems, Inc., Computer Associates International, Inc., International Business Machines Corporation, Layer 7 Technologies, Microsoft Corporation, Oblix Inc., OpenNetwork Technologies Inc., Ping Identity Corporation, Reactivity Inc., RSA Security Inc., and VeriSign Inc. (2005). <i>Web Services Trust Language</i> . Retrieved April 14, 2006 from http://msdn.microsoft.com/library/en-us/dnglobspec/html/WS-trust.pdf
393		
394		
395		
396		
397		
398		
399		
400		
401	XML Signature	W3C (2002). <i>XML Signature Syntax and Processing</i> , W3C Recommendation. Retrieved April 14, 2006 from http://www.w3.org/TR/xmlsig-core/
402		
403		
404	XML Encryption	W3C (2002). <i>XML Encryption Syntax and Processing</i> , W3C Recommendation. Retrieved April 14, 2006 from http://www.w3.org/TR/xmlenc-core/
405		
406		
407	XOP	W3C (2004). <i>XML-binary Optimized Packaging</i> , W3C Candidate Recommendation. Retrieved April 14, 2006 from http://www.w3.org/TR/xop10/
408		
409		

410 **Appendix A: Documenter Team**

411 This standard was developed through the Integration Architecture enterprise architecture
412 initiative, chartered December 14, 2005. The following individuals were members of the
413 Documenter Team for this initiative, and participated in review of this document.

- 414 • Kent Andrus, Office of Financial Management
- 415 • Lori Bame, LEAP Committee
- 416 • Jerry Britcher, Department of Social and Health Services
- 417 • Scott Came, Department of Information Services
- 418 • Gary Dubuque, Department of Revenue
- 419 • Jim Eby, Department of Fish and Wildlife
- 420 • Brian Everson, Washington State Patrol
- 421 • Laura Graham, Legislative Service Center
- 422 • Robin Griggs, Department of Licensing
- 423 • John Hanson, Commission on Trade and Economic Development
- 424 • Tom Henderson, Department of Labor & Industries
- 425 • Paul Hubert, Department of Information Services
- 426 • Debbie Johnson, The Higher Education Coordinating Board
- 427 • Lorraine Louderback, Department of Corrections
- 428 • Dan Mercer, Department of Labor & Industries
- 429 • Miles Neale, Department of Ecology
- 430 • Bill Norris, Department of Health
- 431 • Laura Parma, Department of Information Services
- 432 • Mike Rohrbach, Administrative Office of the Courts
- 433 • Jeff Sharp, Office of the State Treasurer
- 434 • Matt Stevens, Department of Information Services
- 435 • Lyle Tillett, Department of Retirement Systems

436

Appendix B: Review Log

437

The following feedback on this document was received by the Enterprise Architecture Program;

438

the response to each contribution is noted below.

Review by whom and when	Contribution	Response
EA Committee May 17, 2006	<ul style="list-style-type: none">• Add scope section to all service interaction profiles	Incorporated into document
EA Committee June 9, 2006	<ul style="list-style-type: none">• Change standards to guidelines	Incorporated into document
ISB September 14, 2006	<ul style="list-style-type: none">• Adopted profile as guidelines	Adopted and posted as Guidelines

439