



United States
Department of Justice

The Global Justice Reference Architecture (JRA) ebXML Messaging Service Interaction Profile

Version 1.0

**by
The Global Infrastructure/Standards
Working Group**

October 1, 2007



This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Table of Contents

Acknowledgements	5
1. Introduction and Purpose.....	6
1.1. Profile Selection Guidance.....	8
1.2. Usage.....	8
1.3. Namespace References.....	9
2. Conformance Requirements.....	9
2.1. Conformance Targets	9
2.2. General Conformance Requirements (Normative)	10
2.3. Implementation Notes and Implications (Non-Normative).....	11
3. Service Interaction Requirements	11
3.1. Service Consumer Authentication	11
3.1.1. Statement of Requirement from JRA.....	11
3.1.2. Conformance Targets (Normative)	11
3.1.3. Implementation Notes and Implications (Non-Normative)	11
3.2. Service Consumer Authorization.....	12
3.2.1. Statement of Requirement from JRA.....	12
3.2.2. Conformance Targets (Normative)	12
3.2.3. Implementation Notes and Implications (Non-Normative)	12
3.3. Identity and Attribute Assertion Transmission.....	12
3.3.1. Statement of Requirement from JRA.....	12
3.3.2. Conformance Targets (Normative)	13
3.3.3. Implementation Notes and Implications (Non-Normative)	13
3.4. Service Authentication.....	13
3.4.1. Statement of Requirement from JRA.....	13
3.4.2. Conformance Targets (Normative)	13
3.4.3. Implementation Notes and Implications (Non-Normative)	14
3.5. Message Non-Repudiation.....	14
3.5.1. Statement of Requirement from JRA.....	14
3.5.2. Conformance Targets (Normative)	14
3.5.3. Implementation Notes and Implications (Non-Normative)	14
3.6. Message Integrity.....	15
3.6.1. Statement of Requirement from JRA.....	15
3.6.2. Conformance Targets (Normative)	15

3.6.3. Implementation Notes and Implications (Non-Normative)	15
3.7. Message Confidentiality	15
3.7.1. Statement of Requirement from JRA	15
3.7.2. Conformance Targets (Normative)	15
3.7.3. Implementation Notes and Implications (Non-Normative)	16
3.8. Message Addressing.....	16
3.8.1. Statement of Requirement from JRA	16
3.8.2. Conformance Targets (Normative)	16
3.8.3. Implementation Notes and Implications (Non-Normative)	17
3.9. Reliability	17
3.9.1. Statement of Requirement from JRA	17
3.9.2. Conformance Targets (Normative)	17
3.9.3. Implementation Notes and Implications (Non-Normative)	17
3.10. Transaction Support	17
3.10.1. Statement of Requirement from JRA	17
3.10.2. Conformance Targets (Normative)	18
3.10.3. Implementation Notes and Implications (Non-Normative)	18
3.11. Service Metadata Availability	18
3.11.1. Statement of Requirement from JRA	18
3.11.2. Conformance Targets (Normative)	19
3.11.3. Implementation Notes and Implications (Non-Normative)	19
3.12. Interface Description Requirements.....	19
3.12.1. Statement of Requirement from JRA	19
3.12.2. Conformance Targets (Normative)	19
3.12.3. Implementation Notes and Implications (Non-Normative)	19
4. Message Exchange Patterns	19
4.1. Fire-and-Forget Pattern	19
4.2. Request-Response Pattern	20
4.3. Publish-Subscribe Pattern	20
5. Message Definition Mechanisms	20
6. Glossary.....	21
7. References	23
8. Document History	27
Appendix A: Documenter Team.....	28

Acknowledgements

The Global Justice Reference Architecture (JRA) was developed through a collaborative effort of the Global Justice Information Sharing Initiative (Global), Office of Justice Programs (OJP), United States Department of Justice (DOJ).

Global aids its member organizations and the people they serve through a series of important initiatives. These include the facilitation of Global Working Groups. The Global Infrastructure/Standards Working Group (GISWG) is one of four Global Working Groups covering critical topics such as intelligence, privacy, security, and standards. The GISWG is under the direction of Tom Clarke, Ph.D., National Center for State Courts. The GISWG consists of three committees: the Management and Policy Committee, Service Interaction Committee, and Services Committee.

Although this document is the product of Global and its GISWG membership, it was primarily adapted from the technical reference architecture developed by the state of Washington, and sincere appreciation is expressed to Mr. Scott Came, state of Washington and SEARCH, The National Consortium for Justice Information and Statistics, for his guidance and leadership. In addition, parts of the architecture were derived from the Organization for the Advancement of Structured Information Standards (OASIS) Reference Model for Service-Oriented Architecture 1.0 (SOA-RM). Other major contributors deserving recognition include the OASIS Court Filing Technical Committee, OASIS SOA Reference Model Technical Committee, Messaging Focus Group, and GISWG Service Interaction Committee.

Mr. Jim Cabral—IJIS Institute, Global Security Working Group

Mr. Scott Came—SEARCH, The National Consortium for Justice Information and Statistics, GISWG Service Interaction Committee

Dr. Tom Clarke—National Center for State Courts, Chair, GISWG

Mr. Kael Goodman—IJIS Institute, Chair, GISWG Service Interaction Committee

Mr. Zemin Luo—IJIS Institute, GISWG Service Interaction Committee

Mr. Tom Merkle—National Institute of Justice, GISWG Service Interaction Committee

Mr. John Ruegg—Los Angeles County Information Systems Advisory Body, GISWG Service Interaction Committee

For more information about Global efforts, including the Global Justice Reference Architecture initiative and corresponding deliverables, please refer to the Global Web site, <http://it.ojp.gov/globaljra>, for official announcements.

1. Introduction and Purpose

The purpose of this document is to establish a **SERVICE INTERACTION PROFILE**¹ (SIP) based on the ebXML family of technology standards.

A Service Interaction Profile is a concept identified in the Global Justice Reference Architecture ([**JRA**²]). This concept 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 guides the definition of **SERVICE INTERFACES**. In an SOA environment, every service interface shared between two or more information systems should conform to exactly one Service Interaction Profile. Service consumers who interact with an interface should likewise conform to that interface's profile.

The profile discussed in this document is based on the ebXML family of technology standards, defined as follows:

- OASIS ebXML Messaging Services, Version 3.0: Part 1, Core Features, 2007 [**ebMS3**]
- OASIS ebXML “Conformance Profiles Gateway RX V3 or RX V2/3 for e-Business and e-Government applications [**ebMS3-PROFILES**]
Profile summary: < “Sending+Receiving” / “ gateway-rxv3” / Level 1 /HTTP1.1 + SOAP 1.2 + WSS1.1 + WS-ReliableMessaging1.1 >
- OASIS ebXML Business Process Specification Schema v2.0.4 [**ebBP**]
- OASIS ebXML Collaboration-Protocol Profile and Agreement Specification Version 2.0 [**ebCPPA v2**]
- The Web Services Interoperability Organization (WS-I) Basic Profile, Version 1.1, dated April 10, 2006 (noted in this document as [**WS-I BP**]), ebXML Messaging Services v3 is conformant with Section 3 MESSAGES and Section 6 SECURITY and all standards that those sections reference. Section 4 of WS-I Basic Profile does NOT APPLY

¹ Words or phrases formatted in this **STYLE** are defined in the Glossary.

² Abbreviations formatted in this [**style**] represent citations defined in the References section below.

33 to ebXML. ebXML does not specify WSDL for service descriptions
34 and service bindings.

- 35 • The WS-I Attachments Profile (**[WS-I AP]**), Version 1.0, and all
36 standards that it references
- 37 • The WS-I Basic Security Profile Version 1.0 (dated March 30, 2007,
38 noted in this document as **[WS-I BSP]**), all current Token Profiles, and
39 all standards that they reference.

40 The following notes apply to this SIP:

- 41
- 42 • Compliance with **[WS-I AP]** Version 1.0 would normally require
43 compliance with **[WS-I BP]** Version 1.1, which in turn requires the
44 absence of SOAP Envelope in the HTTP response of a One-Way
45 (R2714). However, recent **[WS-I BP]** versions such as Basic Profile
46 Version 1.2 **[WS-I BP12]** override this requirement. Consequently,
47 the Gateway conformance profile does not require conformance to
48 these deprecated requirements inherited from **[WS-I BP]** Version 1.1
49 (R2714, R1143) regarding the use of HTTP.
- 50
- 51 • There must be compliance with the above WS-I profiles within the
52 scope of features exhibited by the Gateway RX V3 ebMS conformance
53 profile. For example, since only SOAP 1.2 is required by Gateway RX
54 V3, the requirements from **[WS-I BSP 1.1]** that depend on SOAP
55 1.1 would not apply. Similarly, none of the requirements for
56 DESCRIPTION (WSDL) or REGDATA (UDDI) apply here, as these
57 are not used.
- 58

59 This ebXML conformance profile may be refined in a future version to require
60 conformance with the following WS-I profiles, once approved and published by
61 WS-I:

- 62
- 63 • Basic Profile 2.0
- 64 • Reliable and Secure Profile 1.1
- 65 • Other standards explicitly identified in this document developed by the
66 World Wide Web Consortium (W3C) or the Organization for the
67 Advancement of Structured Information Standards (OASIS)
- 68 • If no standard is available from WS-I, W3C, or OASIS to meet an
69 identified requirement, then specifications developed by and issued
70 under the copyright of a group of two or more companies will be
71 referenced.
- 72

1.1. Profile Selection Guidance

The following table provides guidance on the selection of Service Interaction Profiles (SIPs).

Select this profile...	if your technology stack for information sharing includes:
Web Services SIP	SOAP, WS-I, WS-*
ebXML SIP	ebXML technologies [ebXML]

1.2. Usage

This document is intended to serve as a guideline for exchanging information among consumer systems and provider systems by satisfying the service interaction requirements identified in the JRA Specification Document (JRA) on pages 35–36. This profile does not guide interaction between humans and services, even though such interaction is within the scope of the OASIS Reference Model for Service-Oriented Architecture (SOA-RM), Version 1.0. However, in demonstrating satisfaction of the “Identity and Attribute Assertion Transmission” service interaction requirement, this profile defines how a consumer system should send identity and other information about a human to a service.

This document may serve as a reference or starting point for implementers defining their own Service Interaction Profile. However, to ensure that a profile remains valid and consistent with the JRA, an implementer may only further specify or constrain this profile and may not introduce techniques or mechanisms that conflict with this profile’s guidance.

This document assumes that the reader is familiar with the JRA Specification document³ and that the reader interprets this document as a Service Interaction Profile defined in the context of that architecture.

³ Global Justice Reference Architecture Specification Working Draft V.,1.4, <http://it.ojp.gov/globaljra>.

1.3. Namespace References

This document associates the following namespace abbreviations and namespace identifiers:

eb: <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/>.

2. Conformance Requirements

This section describes what it means to conform to this ebXML Messaging Service Interaction Profile.

2.1. Conformance Targets

A conformance target is any element or aspect of an information sharing architecture whose implementation or behavior is constrained by this Service Interaction Profile. This profile places such constraints on concepts to ensure interoperable implementations of those concepts.

This profile identifies the following conformance targets, which are concepts from the **[JRA]**:

- Service interface
- Service consumer
- Message

That is, this Service Interaction Profile only addresses, specifies, or constrains these three conformance targets. Other elements of an information sharing architecture are not addressed, specified, or constrained by this profile.

To conform to this Service Interaction Profile, an approach to integrating two or more information systems must:

- Identify and implement all of the conformance targets listed above in a way consistent with their definitions in the **[JRA]**
- Meet all the requirements for each of the targets established in this Service Interaction Profile

Conformance to this Service Interaction Profile does not require a service interface to enforce every service interaction requirement identified in the JRA. Conformance with this profile requires that if an interface enforces a particular service interaction requirement, it do so as directed by the guidance specified here.

2.2. General Conformance Requirements (Normative)

A **SERVICE INTERFACE** conforms to this Service Interaction Profile if:

- The service interface's description (e.g., server-mode Message Service Handler) meets all requirements of the RX V3 or RX V2/3 [**ebMS3-PROFILES**], [**ebMS3**] and if included [**ebBP**].
- A Collaboration Protocol Profile & Collaboration Profile Agreement (CPP/CPA) [**ebCPPA v2**] is not required for [**ebMS3**]; but if used, conformance must be to the forthcoming Version 3 of the CPP/CPA specification. Refer to [**ebCPPA v3**] to monitor the progress of this specification.

A **SERVICE CONSUMER** conforms to this Service Interaction Profile if:

- The consumer meets the requirements defined within the service interface RX V3 or RX V2/3 [**ebMS3-PROFILES**] for consumer and sender (e.g., client-mode Message Service Handler) conformance targets, [**ebMS3**] and if included [**ebBP**].
- A Collaboration Protocol Profile & Collaboration Profile Agreement (CPP/CPA) [**ebCPPA v2**] is not required for [**ebMS3**]; but if used, conformance must be to the forthcoming Version 3 of the CPP/CPA specification. Refer to [**ebCPPA v3**] to monitor the progress of this specification.

A **MESSAGE** conforms to this Service Interaction Profile if:

- The message meets all requirements of the message and envelope conformance targets in [**WS-I BP**].
- The message meets all requirements of ebXML Messaging Service v3.0 [**ebMS3**], specified requirements of the RX V3 or RX V2/3 [**ebMS3-PROFILES**], and if included, [**ebBP**].
- A Collaboration Protocol Profile & Collaboration Profile Agreement (CPP/CPA) [**ebCPPA v2**] is not required for [**ebMS3**]; but if used, conformance must be to the forthcoming Version 3 of the CPP/CPA specification. Refer to [**ebCPPA v3**] to monitor the progress of this specification.
- The message conforms to the National Information Exchange Model (NIEM), Version 1.0: Global Justice XML Data Model (GJXDM), Version 3.0.3; or other published standard **DOMAIN VOCABULARIES** where the semantics of the service's information model match components in those vocabularies.

163 **2.3. Implementation Notes and Implications (Non-Normative)**

164 Global intends to monitor progress on the World Wide Web Consortium (W3C)
165 Message Transmission Optimization Mechanism [**MTOM**] and XML-Binary
166 Optimized Packaging [**XOP**] standards, as well as emerging WS-I Basic Profile
167 versions that reference these standards, to assess these standards' appropriateness
168 for inclusion in this ebXML Messaging Service Interaction Profile. Implementers
169 should be aware that not all product and infrastructure vendors are supporting the
170 WS-I Attachments Profile because of its reliance on the Multipurpose Internet Mail
171 Extensions (MIME) standard for encoding attachments.

172 **3. Service Interaction Requirements**

173 Conformance to this ebXML Messaging Service Interaction Profile requires that, if an
174 approach to integrating two systems has any of the following requirements, each
175 such requirement be implemented as indicated in each section below.

176 **3.1. Service Consumer Authentication**

177 **3.1.1. Statement of Requirement from JRA**

178 The JRA requires that each Service Interaction Profile define how information is
179 provided with messages transmitted from service consumer to service to verify the
180 identity of the consumer.

181 **3.1.2. Conformance Targets (Normative)**

182 Conformance with this Service Interaction Profile requires that message(s) sent to the
183 service interface by a service consumer must assert the consumer's identity by
184 including a security token that conforms to [**WS-I BSP**].

185 If the chosen security token relies on a digital signature, then conformance with this
186 Service Interaction Profile requires that the **EXECUTION CONTEXT** supporting the
187 service interaction include appropriate public key infrastructure (PKI).

188 **3.1.3. Implementation Notes and Implications (Non-Normative)**

189 This Service Interaction Profile assumes that implementers will utilize features of their
190 data networks (including but not limited to HTTPS, firewalls, and virtual private
191 networks (VPNs)) to satisfy consumer authentication requirements. Conformance to
192 the guidance above is necessary only when network features are inadequate to
193 authenticate the consumer (for instance, when the message must transit an
194 intermediary service or when persistent message-level authentication is required by
195 the service.)

196 **3.2. Service Consumer Authorization**

197 **3.2.1. Statement of Requirement from JRA**

198 The JRA requires that each Service Interaction Profile define how information is
199 provided with messages transmitted from service consumer to service to document or
200 assert the consumer's authorization to perform certain actions on and/or to access
201 certain information via the service.

202 **3.2.2. Conformance Targets (Normative)**

203 Conformance with this Service Interaction Profile requires that message(s) sent to the
204 service interface by a service consumer must assert the consumer's authorization to
205 perform the requested action by including a security assertion containing an attribute
206 statement, such that the assertion and attribute statement conform to the Security
207 Assertion Markup Language [**SAML**] Version 2.0 specification.

208 **3.2.3. Implementation Notes and Implications (Non-Normative)**

209 Implementers are encouraged to monitor the development of the Global Federated
210 Identity and Privilege Management (**GFIPM**) metadata initiative and reflect the
211 guidance of that initiative and its message definitions. Future versions of this
212 Service Interaction Profile may require conformance with GFIPM metadata structures
213 and encoding once they have been finalized and endorsed by the appropriate Global
214 committees and working groups.

215 Additionally, future conformance with this Service Interaction Profile may require
216 that the execution context supporting the service interaction include a valid GFIPM
217 identity provider that shall have generated the SAML assertion.

218 Global will continue to monitor the SAML standard to assess the appropriateness of
219 SAML updates for inclusion in this Service Interaction Profile.

220 The current GFIPM metadata and SAML encoding specifications referenced are an
221 early version and will undergo substantive changes. Specifically, the current GFIPM
222 specification will be reconciled with NIEM 2.0 and incorporate feedback resulting
223 from the ongoing GFIPM pilot project.

224 **3.3. Identity and Attribute Assertion Transmission**

225 **3.3.1. Statement of Requirement from JRA**

226 The JRA requires that each Service Interaction Profile define how information is
227 provided with messages transmitted from service consumer to service to must assert
228 the validity of information about a human or machine, including its identity.

229 **3.3.2. Conformance Targets (Normative)**

230 Conformance with this ebXML Messaging Service Interaction Profile requires that
231 message(s) sent to the service interface by a service consumer must assert the
232 consumer's authorization to perform the requested action by including an assertion
233 containing an attribute statement, such that the assertion and attribute statement
234 conform to the Security Assertion Markup Language (SAML) Version 2.0.

235 **3.3.3. Implementation Notes and Implications (Non-Normative)**

236 Implementers are encouraged to monitor the development of the Global Federated
237 Identity and Privilege Management ([**GFIPM**]) metadata initiative and to reflect the
238 guidance of that initiative and its message definitions. Future versions of this Service
239 Interaction Profile may require conformance with GFIPM metadata structures and
240 encoding, once they have been finalized and endorsed by the appropriate Global
241 committees and working groups.

242 Additionally, future conformance with this Service Interaction Profile may require
243 that the execution context supporting the service interaction include a valid GFIPM
244 identity provider that shall have generated the SAML assertion.

245 The current GFIPM metadata and SAML encoding specifications referenced are an
246 early version and will undergo substantive changes. Specifically, the current GFIPM
247 specification will be reconciled with NIEM 2.0 and incorporate feedback resulting
248 from the ongoing GFIPM initiative.

249 **3.4. Service Authentication**

250 **3.4.1. Statement of Requirement from JRA**

251 The JRA requires that each Service Interaction Profile define how a service provides
252 information to a consumer that demonstrates the service's identity to the consumer's
253 satisfaction.

254 **3.4.2. Conformance Targets (Normative)**

255 Conformance with this Service Interaction Profile requires that message(s) sent to the
256 service interface by a **SERVICE PROVIDER** must assert the provider's identity by
257 including a security token that conforms to [**WS-I BSP**].

258 If the chosen security token relies on a digital signature, then conformance with this
259 Service Interaction Profile requires that the execution context supporting the service
260 interaction include appropriate public key infrastructure (PKI).

261 **3.4.3. Implementation Notes and Implications (Non-Normative)**

262 This Service Interaction Profile assumes that implementers will utilize features of their
263 data networks (including but not limited to HTTPS, firewalls, and virtual private
264 networks (VPNs)) to satisfy consumer authentication requirements. Conformance to
265 the guidance above is necessary only when network features are inadequate to
266 authenticate the provider (for instance, when the message must transit an
267 intermediary service or when persistent message-level authentication is required by
268 the service.)

269 **3.5. Message Non-Repudiation**

270 **3.5.1. Statement of Requirement from JRA**

271 The JRA requires that each Service Interaction Profile define how information is
272 provided in a message to allow the recipient to prove that a particular authorized
273 sender in fact sent the message.

274 **3.5.2. Conformance Targets (Normative)**

275 Conformance with this ebXML Messaging Service Interaction Profile requires that the
276 sender of the message must:

- 277 • Include a creation timestamp in the manner prescribed in Section 10
278 “Security Timestamps” of **[WS-Security]**.
- 279 • Create a digital signature of the creation timestamp and the part of the
280 message requiring non-repudiation (which may be the entire
281 message). This signature must conform to the requirements of **[WS-I**
282 **BSP]** Section 8 “XML-Signature.”

283 Conformance with this ebXML Messaging Service Interaction Profile requires that the
284 execution context supporting the service interaction include appropriate public key
285 infrastructure (PKI).

286 **3.5.3. Implementation Notes and Implications (Non-Normative)**

287 By itself, this method does not provide for absolute non-repudiation. The business
288 parties (e.g., agencies) involved in the service interaction should supplement the
289 technical approach with a written agreement that establishes whether—and under
290 what circumstances—they permit repudiation.

291 Note that **[WS-Security]** provides an example of this technical approach in Section
292 11 “Extend Example.”

293 **3.6. Message Integrity**

294 **3.6.1. Statement of Requirement from JRA**

295 The JRA requires that each Service Interaction Profile define how information is
296 provided in a message to allow the recipient to verify that the message has not
297 changed since it left control of the sender.

298 **3.6.2. Conformance Targets (Normative)**

299 Conformance with this ebXML Service Interaction Profile requires that the sender of
300 the message must sign all or part of a message using **[XML Signature]**. The
301 message must meet all requirements of **[WS-I BSP]** Section 8 “XML-Signature.”

302 Conformance with this Service Interaction Profile requires that the execution context
303 supporting the service interaction include appropriate public key infrastructure (PKI).

304 **3.6.3. Implementation Notes and Implications (Non-Normative)**

305 This ebXML Messaging Service Interaction Profile assumes that implementers will
306 utilize features of their data networks (including but not limited to HTTPS, firewalls,
307 and virtual private networks to satisfy integrity requirements. Conformance to the
308 guidance above is necessary only when network features are inadequate to provide
309 integrity (for instance, when the message must transit an intermediary service or
310 when persistent message-level integrity is required by the service.)

311 **3.7. Message Confidentiality**

312 **3.7.1. Statement of Requirement from JRA**

313 The JRA requires that each Service Interaction Profile define how information is
314 provided in a message to protect anyone except an authorized recipient from reading
315 the message or parts of the message.

316 **3.7.2. Conformance Targets (Normative)**

317 Conformance with this ebXML Messaging Service Interaction Profile requires that the
318 sender of the message must encrypt all or part of a message using **[XML**
319 **Encryption]** as further specified and constrained in **[WS-I BSP]**. The encryption
320 must result from application of an encryption algorithm approved by **[FIPS 140-2]**.

321 Confidential elements or sections of a message must meet the requirements
322 associated with ENCRYPTED_DATA in **[WS-I BSP]**, Section 9 “XML Encryption.”

323 Conformance with this Service Interaction Profile requires that the execution context
324 supporting the service interaction include appropriate public key infrastructure (PKI).

3.7.3. Implementation Notes and Implications (Non-Normative)

None.

3.8. Message Addressing

3.8.1. Statement of Requirement from JRA

The JRA requires that each Service Interaction Profile define how information is provided in a message to indicate:

- Where a message originated,
- The ultimate destination of the message (beyond physical endpoint),
- A specific recipient to whom the message should be delivered (this includes sophisticated metadata designed specifically to support routing), and
- A specific address or entity to which reply messages (if any) should be sent.

3.8.2. Conformance Targets (Normative)

Conformance with this ebXML Messaging Service Interaction Profile requires that every message conform to the ebXML SOAP header requirements for eb:Messaging of **[ebMS3]**. Specifically, the PartyID value and type in the From and To elements are used for Message Addressing.

If the addressing requirements of a specific interaction are satisfied by the components within the XML namespace defined by the OASIS Emergency Management Technical Committee and whose identifier is

`urn:oasis:names:tc:emergency:EDXL:DE:1.0`

(or later version), then conformance with this Service Interaction Profile requires that:

1. The message include a SOAP header that conforms to the ebXML SOAP header addressing requirements for **[ebMS3]** and provide operation mapping to intermediary service responsible for implementing the EDXL addressing requirements. Interfaces to non-ebXML services are specified in the CPP/CPA per Section 3.4.9.8 of the ebXML Business Process specification **[ebBP]**; and
2. The endpoint reference include, as a reference property, an XML structure conformant to and valid against the components in the namespace whose identifier is

`urn:oasis:names:tc:emergency:EDXL:DE:1.0`.

358 In this section, the terms “endpoint reference” and “reference property” are to be
359 interpreted as they are defined in **[WS-Addressing Core]**.

360 **3.8.3. Implementation Notes and Implications (Non-Normative)**

361 Note that the EDXL Distribution Element is included in the current production
362 release of NIEM (Version 1.0) as an external standard. The EDXL “Distribution
363 Element” defines an enveloping mechanism that duplicates the capabilities of the
364 ebMS3 header and MIME structure. EbMS3 can process EDXL as is, or the EDXL
365 message can be mapped to an ebMS3 message with PayloadInfo elements and
366 attachment metadata expressing the EDXL information.

367 **3.9. Reliability**

368 **3.9.1. Statement of Requirement from JRA**

369 The JRA requires that each Service Interaction Profile define how information is
370 provided with messages to permit message senders to receive notification of the
371 success or failure of message transmissions, and to permit messages sent with specific
372 sequence-related rules either to arrive as intended or fail as a group.

373 **3.9.2. Conformance Targets (Normative)**

374 Conformance with this ebXML Service Interaction Profile requires that message(s)
375 contain SOAP headers that conform to the requirements of the OASIS WS-Reliable
376 Messaging standard (**[WS-RM]**).

377 Conformance with this Service Interaction Profile requires that the execution context
378 supporting the interaction include components that implement the RM-Source and
379 RM-Destination components defined in the (**[WS-RM]**) standard.

380 **3.9.3. Implementation Notes and Implications (Non-Normative)**

381 Global will continue monitoring the emerging WS-I Reliable Secure Profile
382 (**[WS-I RSP]**) as to appropriateness for inclusion in this Service Interaction Profile.

383 **3.10. Transaction Support**

384 **3.10.1. Statement of Requirement from JRA**

385 The JRA requires that each Service Interaction Profile define how information is
386 provided with messages to permit a sequence of messages to be treated as an atomic
387 transaction by the recipient.

388 **3.10.2. Conformance Targets (Normative)**

389 Conformance with this ebXML Messaging Service Interaction Profile requires that the
390 following must be true of the consumers, services, and messages involved in the
391 interaction:

- 392 • The consumers and services must meet the behavioral requirements as
393 defined in ebXML Business Process Specification Schema [**ebBP**]
394 specifications for one of the six defined Business Transaction patterns
395 (Commercial Transaction, Notification, Information Distribution,
396 Request-Response, Request-Confirm, and Query Response).
- 397 • The description of the Business Service Interface (BSI) for each service
398 involved in the interaction must conform to the collaboration
399 requirements identified in the ebBP schema definition and ebBP
400 Business Signal Definitions (schema). The ebBP definition(s) and
401 ebBP Signal definitions are incorporated into trading partner
402 Collaboration Protocol Profile(s) per the ebXML Collaboration
403 Protocol Profile and Agreements [**ebCPPA v2**] specifications and
404 ebMS processing mode parameters. The ebMS must conform to the
405 RX V3 or RX V2/3 [**ebMS3-PROFILES**].

406 **3.10.3. Implementation Notes and Implications (Non-Normative)**

407 A Business Service Interface (BSI) may logically represent middleware, applications,
408 back-end systems, software, or services. A mapping between ebBP Business
409 Transaction Activities (BTAs) and operations of one or multiple Web Services is
410 supported within the ebBP specification. The support of WSDL operations is
411 intended for the design of Business Collaborations in which one or more of the
412 business partners are not capable of supporting ebXML interchanges. Reference to
413 WSDL files would be specified in the ebXML Collaboration Profile Agreement
414 (CPA).

415 **3.11. Service Metadata Availability**

416 **3.11.1. Statement of Requirement from JRA**

417 The JRA requires that each Service Interaction Profile define how the service
418 captures and makes available (via query) metadata about the service. (Metadata is
419 information that describes or categorizes the service and often assists consumers in
420 interacting with the service in some way.)

421

422 **3.11.2. Conformance Targets (Normative)**

423 Conformance to this ebXML Messaging Service Interaction Profile requires that
424 service interfaces responding to requests for metadata about the interface and
425 underlying ebXML business process must be available from a Registry/Repository
426 service.

427 **3.11.3. Implementation Notes and Implications (Non-Normative)**

428 The ebBP specification states that the required artifacts for ebXML Service metadata
429 may be stored in any Registry/Repository including the ebXML Registry/Repository
430 **[ebRS3]**.

431 **3.12. Interface Description Requirements**

432 **3.12.1. Statement of Requirement from JRA**

433 This section demonstrates how this profile meets the service interaction requirements
434 identified in the **[JRA]**.

435 **3.12.2. Conformance Targets (Normative)**

436 Section 2.2 above indicates that a service interface conforms to this Service
437 Interaction Profile if its description meets all requirements of Collaboration Protocol
438 Profile (CPP) conformance target in **[ebCPPA v2]** and, if included, **[ebBP]** and
439 **[ebMS3]**. The CPP and CPA provide the details of transport, messaging, security
440 constraints, and bindings to a Business-Process-Specification document that contains
441 the definition of the interactions between the two parties while engaging in a
442 specified electronic Business Collaboration.

443 **3.12.3. Implementation Notes and Implications (Non-Normative)**

444 None.

445 **4. Message Exchange Patterns**

446 This section discusses how the Message Exchange Patterns (MEP) identified in the
447 **[JRA]** are supported by this profile.

448 **4.1. Fire-and-Forget Pattern**

449 The fire-and-forget message exchange pattern corresponds to a one-way ebMS MEP
450 in **[ebMS3]**. ebXML Messaging Services defines both a one-way push mode and a
451 one-way pull mode asynchronous MEP. This Service Interaction Profile supports this
452 pattern by requiring that service consumers and service interfaces conform to **[WS-I**

453 **BP]**. In particular, Section 4.7.9 “One-Way Operations” of **[WS-I BP]** requires that
454 a service interface respond to a one-way operation by returning an HTTP response
455 with an empty entity-body. Many composite asynchronous message exchange
456 patterns can be derived from this primitive pattern.

457 **4.2. Request-Response Pattern**

458 The request-response message exchange pattern corresponds to the ebXML two-
459 way/synch request-response operation as defined in **[ebMS3]**. This Service
460 Interaction Profile supports this pattern by requiring that service consumers and
461 service interfaces conform to **[WS-I BP]**.

462 This MEP is synchronous and can be combined with a fire-and-forget MEP to form
463 more sophisticated composite MEPs.

464 Asynchronous request-response patterns may also be supported, as defined by the
465 **[ebMS3]** Two-Way/Push-and-Pull and Two-Way/Pull-and-Push MEPs.

466 **4.3. Publish-Subscribe Pattern**

467 The publish-subscribe message exchange pattern is an asynchronous MEP.
468 Normally, the publisher and the subscriber are decoupled by an intermediary.

469 The publish-subscribe MEP could be constructed as a composite MEP by using
470 primitive MEPs as defined in this document:

- 471 1. A subscriber sends a subscription message to the intermediary using the fire-
472 and-forget primitive MEP
- 473 2. A publisher sends an event message to the intermediary using the fire-and-
474 forget primitive MEP
- 475 3. There are two ways to deliver the event to the subscriber:
 - 476 a. The intermediary sends the event notification to the subscriber using
477 the fire-and-forget primitive MEP, or
 - 478 b. The subscriber pulls from the intermediary periodically until the event
479 notification message is retrieved using the request-response primitive
480 MEP.

481 The publish-subscribe MEP is increasingly being used in a Web Services context. An
482 emerging standard, **[WS-Notification]**, defines a standard-based Web Services
483 approach to notification using a publish-subscribe message pattern.

484 **5. Message Definition Mechanisms**

485 This section demonstrates how this profile supports the **MESSAGE DEFINITION**
486 **MECHANISMS** identified in the Justice Reference Architecture.

487 This Service Interaction Profile requires that each message consist of one, but not
488 both, of the following:

- 489 • A single SOAP message (defined as the message conformance target
490 in ([**WS-I BP**]) that meets all requirements of this profile
- 491 • A SOAP message package (as defined in [**SwA**] and as constrained by
492 [**WS-I AP**] and [**WSS SwA**])

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

497 The names of all elements in this XML Schema must conform to the guidelines
498 documented in Service Description Guidelines [**SDG**].

499 **6. Glossary**

500 **DOMAIN VOCABULARIES**

501
502
503
504
505
506
507
508
509
510
511
512
513

Includes canonical data models, data dictionaries, and markup languages that standardize the meaning and structure of information for a domain. Domain vocabularies can improve the interoperability between consumer and provider systems by providing a neutral, common basis for structuring and assigning semantic meaning to information exchanged as part of service interaction. Domain vocabularies can usually be extended to address information needs specific to the service interaction or to the business partners integrating their systems.

514 **EXECUTION CONTEXT**

515
516
517

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.

518 **MESSAGE**

519
520
521
522
523

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.

524	MESSAGE DEFINITION MECHANISM	Establishes a standard way of defining the structure and contents of a message; for example, GJXDM- or NIEM-conformant schema sets. Note that since a message includes the concept of an attachment, the message definition mechanism must identify how different sections of a message (for example, the main section and any attachment sections) are separated and identified and how attachment sections are structured and formatted.
525		
526		
527		
528		
529		
530		
531		
532		
533		
534		
535	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.
536		
537		
538		
539		
540	SERVICE CONSUMER	An entity which seeks to satisfy a particular need through the use capabilities offered by means of a service.
541		
542		
543	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 “Service Interaction Profile” section of [JRA] for details.
544		
545		
546		
547		
548		
549	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 interface is what a system designer or implementer (programmer) uses to design or build executable software that interacts with the service.
550		
551		
552		
553		
554		
555		
556		
557		
558		
559		
560	SERVICE PROVIDER	An entity (person or organization) that offers the use of capabilities by means of a service.
561		
562		

7. References

563

564 These references use the following acronyms to represent standards organizations:

- 565 • FIPS: Federal Information Processing Standards IETF: Internet
566 Engineering Task Force
- 567 • NIST: National Institute of Standards and Technology
- 568 • OASIS: Organization for the Advancement of Structured Information
569 Standards
- 570 • W3C: World Wide Web Consortium
- 571 • WS-I: Web Services Interoperability Organization

572

ebBP

573 OASIS ebXML Business Process Specification
574 Schema v2.0.4, [http://docs.oasis-](http://docs.oasis-open.org/ebxml-bp/2.0.4/OS/spec/ebxmlbp-v2.0.4-Spec-os-en.pdf)
575 [open.org/ebxml-bp/2.0.4/OS/spec/ebxmlbp-](http://docs.oasis-open.org/ebxml-bp/2.0.4/OS/spec/ebxmlbp-v2.0.4-Spec-os-en.pdf)
576 [v2.0.4-Spec-os-en.pdf](http://docs.oasis-open.org/ebxml-bp/2.0.4/OS/spec/ebxmlbp-v2.0.4-Spec-os-en.pdf)

ebCPPA v2

577 OASIS ebXML Collaboration-Protocol Profile
578 and Agreement Specification, Version 2.0,
579 [http://www.oasis-open.org/committees/ebxml-](http://www.oasis-open.org/committees/ebxml-cppa/documents/ebcpp-2.0.pdf)
580 [cppa/documents/ebcpp-2.0.pdf](http://www.oasis-open.org/committees/ebxml-cppa/documents/ebcpp-2.0.pdf)

ebCPPA v3

581 OASIS ebXML Collaboration-Protocol Profile
582 and Agreement Specification, Version 3.0
583 DRAFT, refer to home page for latest v3
584 specification, [http://www.oasis-](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-cppa)
585 [open.org/committees/tc_home.php?wg_abbrev=](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-cppa)
586 [ebxml-cppa](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-cppa)

ebMS3

587 OASIS ebXML Messaging Services, Version 3.0:
588 Part 1, Core Features, 2007,
589 [http://docs.oasis-open.org/ebxml-](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.pdf)
590 [msg/ebms/v3.0/core/ebms_core-3.0-spec.pdf](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.pdf)

ebMS3-PROFILES

591 OASIS ebXML Messaging Services 3.0
592 Conformance Profiles, Committee Draft 02,
593 July 25, 2007, [http://docs.oasis-open.org/ebxml-](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/cd02/ebms-3.0-confprofiles-cd-02.pdf)
594 [msg/ebms/v3.0/prof/cd02/ebms-3.0-confprofiles-](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/cd02/ebms-3.0-confprofiles-cd-02.pdf)
595 [cd-02.pdf](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/cd02/ebms-3.0-confprofiles-cd-02.pdf)

ebRS3

596 OASIS ebXML Registry Services Specification
597 (RS) v3.0, [http://docs.oasis-](http://docs.oasis-open.org/regrep/v3.0/regrep-3.0-os.zip)
598 [open.org/regrep/v3.0/regrep-3.0-os.zip](http://docs.oasis-open.org/regrep/v3.0/regrep-3.0-os.zip)

599	ebXML	ebXML FAQs for overview of ebXML
600		Technologies, http://www.oasis-
601		open.org/committees/download.php/21792/ebxm
602		lbp-v2.0.4-faq-os-en.htm
603	FIPS 140-2	NIST May 2001, Security Requirements for
604		Cryptographic Modules,
605		http://csrc.nist.gov/publications/fips/
606	GFIPM	Global Security Working Group (GSWG) Global
607		Federated Identity and Privilege Management
608		(GFIPM) Metadata Package, Version 0.3,
609		Working Draft, September 23, 2006,
610		http://it.ojp.gov/gfipm
611	GJXDM	Global Justice XML Data Model,
612		http://it.ojp.gov/jxdm/
613	JRA	Global Infrastructure/Standards Working Group
614		(GISWG) Justice Reference Architecture (JRA)
615		Specification, Working Draft, Version 1.4,
616		February 14, 2007, http://it.ojp.gov/globaljra
617	MTOM	SOAP Message Transmission Optimization
618		Mechanism (MTOM), W3C Recommendation,
619		January 25, 2005,
620		http://www.w3.org/TR/2005/REC-soap12-mtom-
621		20050125/
622	NIEM	National Information Exchange Model,
623		http://www.niem.gov/library.php
624	SAML	OASIS Security Assertion Markup Language,
625		Version 2.0 specification set, March 15, 2005,
626		http://www.oasis-open.org/committees/tc_home.
627		php?wg_abbrev=security#samlv2.0
628	SDG	GISWG JRA Service Description Guidelines,
629		http://it.ojp.gov/globaljra
630	SwA	W3C (2004), SOAP Messages with Attachments,
631		W3C Note, Retrieved April 14, 2006, from
632		http://www.w3.org/TR/SOAP-attachments

633	WS Notification	OASIS Web Services Notification, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn
634		
635		
636	WS-Addressing Core	W3C Web Services Addressing 1.0—Core, W3C Recommendation, May 9, 2006, http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/
637		
638		
639		
640	WS-I AP	WS-I Attachments Profile, Version 1.0, Second Edition, April 20, 2006, http://www.ws- i.org/Profiles/AttachmentsProfile-1.0.html
641		
642		
643	WS-I BP	WS-I Basic Profile, Version 1.1, April 10, 2006, http://www.ws-i.org/Profiles/BasicProfile-1.1.html
644		
645	WS-I BP12	WS-I (2007), Basic Profile Version 1.2 (draft), http://www.ws- i.org/deliverables/workinggroup.aspx?wg=basicp rofile
646		
647		
648		
649	WS-I BSP	WS-I Basic Security Profile, Working Group Draft, March 30, 2007, http://www.ws- i.org/Profiles/BasicSecurityProfile-1.0.html
650		
651		
652	WS-I RSP	WS-I Reliable Secure Profile Usage Scenarios Document, Working Group Draft, Version 1.0, November 6, 2006, http://www.ws- i.org/profiles/rsp-scenarios-1.0.pdf
653		
654		
655		
656	WSS SwA	OASIS WS-Security SOAP Messages with Attachments Profile 1.1 2006-02-01, http://www.oasis- open.org/committees/download.php/16672/wss- v1.1-spec-os-SwAProfile.pdf
657		
658		
659		
660		
661	WS-RM	OASIS (2007), Web Services ReliableMessaging, Version 1.1, http://docs.oasis-open.org/ws- rx/wrm/v1.1/wrm.pdf
662		
663		
664	WS-Security	OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard, February 1, 2006, http://www.oasis- open.org/committees/download.php/16790/wss- v1.1-spec-os-SOAPMessageSecurity.pdf
665		
666		
667		
668		

669	XML Encryption	W3C (2002), XML Encryption Syntax and
670		Processing, W3C Recommendation, April 14,
671		2006, http://www.w3.org/TR/xmlenc-core/
672	XML Signature	W3C (2002), XML Signature Syntax and
673		Processing, W3C Recommendation, April 14,
674		2006, http://www.w3.org/TR/xmldsig-core/
675	XOP	W3C Recommendation XML-binary Optimized
676		Packaging, 2005-01-25,
677		http://www.w3.org/TR/xop10/
678		
679		

680

8. Document History

Date	Version	Editor	Change
April 12, 2007	0.1	John Ruegg	The initial document is based on the Web Services Service Interaction Profile v1.0 (WS SIP) from the Global Infrastructure & Standards Working Group (GISWG)
July 25, 2007	0.8	John Ruegg	Updated ebMS Profile to the later Gateway RX V3 or RX V2/V3 supporting WS-Reliable Messaging, dropped the WebSphere and File Drop SIPs from list of Global SIPs. Updated the WS-I requirements consistent with ebXML PROFILES specifications. Updated ebXML registry reference from V2.0 to V3.0
September 10, 2007	0.9	John Ruegg	Incorporated OASIS ebXML TC comments and minor editing for consistency with the Web Services SIP format
October 1, 2007	1.0 Release Candidate	Monique La Bare	Minor edits and formatting for publication

681

682

683

Appendix A: Documenter Team

684

This document was developed by the U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) Infrastructure/Standards Working Group (GISWG) Service Interaction Committee. The following individuals were members

685

686

687

of the Development Team for this document and participated in its review:

688

- Mr. Jim Cabral, IJIS Institute

689

- Mr. Scott Came, SEARCH, The National Consortium for Justice Information and Statistics

690

691

- Mr. Scott Fairholm, National Center for State Courts

692

- Mr. Kael Goodman, IJIS Institute, Service Interaction Committee Chair

693

- Mr. Alan Harbitter, IJIS Institute

694

- Mr. Zemin Luo, IJIS Institute

695

- Mr. Tom Merkle, National Institute of Justice

696

- Mr. John Ruegg, Los Angeles County Information Systems Advisory Body

697

698

699