Global Justice Information Sharing Initiative

United States
Department of Justice

U.S. Department of Justice's Global

# Justice Reference Architecture (JRA)

# ebXML Messaging Service Interaction Profile

Version 1.0

March 2009

Global Infrastructure/Standards
Working Group

# Table of Contents

# Acknowledgements

The Global Justice Reference Architecture (JRA) was developed through a collaborative effort of the U.S. Department of Justice (DOJ) Global Justice Information Sharing Initiative (Global) membership and DOJ's Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA). The Global Infrastructure/Standards Working Group (GISWG) would like to express their appreciation to BJA for their continued support and guidance. GISWG is under the direction of Tom Clarke, Ph.D., National Center for State Courts. The creation of this document was a volunteer effort by numerous contributors, and sincere thanks is extended to them for the development of this resource.

Global aids its member organizations and the people they serve through a series of important initiatives. These include the facilitation of Global Working Groups. GISWG is one of five Global Working Groups covering critical topics such as intelligence, privacy, security, outreach, and standards.

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.

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.

# Document Conventions

In this document, use of a bold small-caps typeface, as in this **EXAMPLE**, indicates an important concept or a term defined either in the glossary or in the body of the text at the point where the term or concept is first used.

In this document, use of a bold caps typeface, as in this **[EXAMPLE]**, indicates an important resource document noted in the Reference Section of this document.

# 1. Introduction and Purpose

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

A Service Interaction Profile is a concept identified in the Global Justice Reference Architecture (**[JRA]**). 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 to ebXML. ebXML does not specify WSDL for service descriptions and service bindings.
- The WS-I Attachments Profile (**[WS-I AP]**), Version 1.0, and all standards that it references

- The WS-I Basic Security Profile Version 1.0 (dated March 30, 2007, noted in this document as **[WS-I BSP]**), all current Token Profiles, and all standards that they reference.

The following notes apply to this SIP:

- Compliance with **[WS-I AP]** Version 1.0 would normally require compliance with **[WS-I BP]** Version 1.1, which in turn requires the absence of SOAP Envelope in the HTTP response of a One-Way (R2714). However, recent **[WS-I BP]** versions such as Basic Profile Version 1.2 **[WS-I BP12]** override this requirement. Consequently, the Gateway conformance profile does not require conformance to these deprecated requirements inherited from **[WS-I BP]** Version 1.1 (R2714, R1143) regarding the use of HTTP.

- There must be compliance with the above WS-I profiles within the scope of features exhibited by the Gateway RX V3 ebMS conformance profile. For example, since only SOAP 1.2 is required by Gateway RX V3, the requirements from **[WS-I BSP 1.1]** that depend on SOAP 1.1 would not apply. Similarly, none of the requirements for DESCRIPTION (WSDL) or REGDATA (UDDI) apply here, as these are not used.

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

- Basic Profile 2.0
- Reliable and Secure Profile 1.1
- Other standards explicitly identified in this document developed by the World Wide Web Consortium (W3C) or the Organization for the Advancement of Structured Information Standards (OASIS)
- 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 will be referenced.

## 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, page 29]**. 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 document and that the reader interprets this document as a Service Interaction Profile defined in the context of that architecture.

## 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.

### 2.3. Implementation Notes and Implications (Non-Normative)

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

## 3. Service Interaction Requirements

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

### 3.1.1. Service Consumer Authentication

### 3.1.2. Statement of Requirement from JRA

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

### 3.1.3. Conformance Targets (Normative)

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

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

### 3.1.4. Implementation Notes and Implications (Non-Normative)

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

## 3.2. Service Consumer Authorization

### 3.2.1. Statement of Requirement from JRA

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

### 3.2.2. Conformance Targets (Normative)

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

### 3.2.3. Implementation Notes and Implications (Non-Normative)

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

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

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

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

## 3.3. Identity and Attribute Assertion Transmission

### 3.3.1. Statement of Requirement from JRA

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

### 3.3.2. Conformance Targets (Normative)

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

### 3.3.3. Implementation Notes and Implications (Non-Normative)

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

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

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

## 3.4. Service Authentication

### 3.4.1. Statement of Requirement from JRA

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

### 3.4.2. Conformance Targets (Normative)

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

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

### 3.4.3. Implementation Notes and Implications (Non-Normative)

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

## 3.5. Message Non-Repudiation

### 3.5.1. Statement of Requirement from JRA

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

### 3.5.2. Conformance Targets (Normative)

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

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

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

### 3.5.3. Implementation Notes and Implications (Non-Normative)

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

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

## 3.6. Message Integrity

### 3.6.1. Statement of Requirement from JRA

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

### 3.6.2. Conformance Targets (Normative)

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

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

### 3.6.3. Implementation Notes and Implications (Non-Normative)

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

## 3.7. Message Confidentiality

### 3.7.1. Statement of Requirement from JRA

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

### 3.7.2. Conformance Targets (Normative)

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

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

Conformance with this Service Interaction Profile requires that the execution context 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.

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

### 3.8.3. Implementation Notes and Implications (Non-Normative)

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

## 3.9. Reliability

### 3.9.1. Statement of Requirement from JRA

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

### 3.9.2. Conformance Targets (Normative)

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

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

### 3.9.3. Implementation Notes and Implications (Non-Normative)

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

## 3.10. Transaction Support

### 3.10.1. Statement of Requirement from JRA

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

### 3.10.2. Conformance Targets (Normative)

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

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

### 3.10.3. Implementation Notes and Implications (Non-Normative)

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

## 3.11. Service Metadata Availability

### 3.11.1. Statement of Requirement from JRA

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

### 3.11.2. Conformance Targets (Normative)

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

### 3.11.3. Implementation Notes and Implications (Non-Normative)

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

## 3.12. Interface Description Requirements

### 3.12.1. Statement of Requirement from JRA

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

### 3.12.2. Conformance Targets (Normative)

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

### 3.12.3. Implementation Notes and Implications (Non-Normative)

None.

# 4. Message Exchange Patterns

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

## 4.1. Fire-and-Forget Pattern

The fire-and-forget message exchange pattern corresponds to a one-way ebMS MEP in **[ebMS3]**. ebXML Messaging Services defines both a one-way push mode and a one-way pull mode asynchronous MEP. This Service Interaction Profile supports this pattern by requiring that service consumers and service interfaces conform to **[WS-I BP].** In particular, Section 4.7.9 “One-Way Operations” of **[WS-I BP]** requires that a service interface respond to a one-way operation by returning an HTTP response with an empty entity-body. Many composite asynchronous message exchange patterns can be derived from this primitive pattern.

## 4.2. Request-Response Pattern

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

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

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

## 4.3. Publish-Subscribe Pattern

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

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

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

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

# 5. Message Definition Mechanisms

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

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

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

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

# 6. Glossary

**DOMAIN VOCABULARIES**
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.

**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.

**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.

**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.

**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.

**SERVICE CONSUMER** An entity which seeks to satisfy a particular need through the use capabilities offered by means of a service.

**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.

**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.

**SERVICE PROVIDER** An entity (person or organization) that offers the use of capabilities by means of a service.

# 7. References

These references use the following acronyms to represent standards organizations:

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

| | |
|---|---|
| **ebBP** | OASIS ebXML Business Process Specification Schema v2.0.4, http://docs.oasis-open.org/ebxml-bp/2.0.4/OS/spec/ebxmlbp-v2.0.4-Spec-os-en.pdf |
| **ebCPPA v2** | OASIS ebXML Collaboration-Protocol Profile and Agreement Specification, Version 2.0, http://www.oasis-open.org/committees/ebxml-cppa/documents/ebcpp-2.0.pdf |
| **ebCPPA v3** | OASIS ebXML Collaboration-Protocol Profile and Agreement Specification, Version 3.0 DRAFT, refer to home page for latest v3 specification, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-cppa |
| **ebMS3** | OASIS ebXML Messaging Services, Version 3.0: Part 1, Core Features, 2007, http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.pdf |
| **ebMS3-PROFILES** | OASIS ebXML Messaging Services 3.0 Conformance Profiles, Committee Draft 02, July 25, 2007, http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/cd02/ebms-3.0-confprofiles-cd-02.pdf |
| **ebRS3** | OASIS ebXML Registry Services Specification (RS) v3.0, http://docs.oasis-open.org/regrep/v3.0/regrep-3.0-os.zip |

**ebXML** ebXML FAQs for overview of ebXML Technologies, http://www.oasis-open.org/committees/download.php/21792/ebxmlbp-v2.0.4-faq-os-en.htm

**FIPS 140-2** NIST May 2001, Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/fips/

**GFIPM** Global Security Working Group (GSWG) Global Federated Identity and Privilege Management (GFIPM) Metadata Package, Version 0.3, Working Draft, September 23, 2006, http://it.ojp.gov/gfipm

**GJXDM** Global Justice XML Data Model, http://it.ojp.gov/jxdm/

**JRA** Global Infrastructure/Standards Working Group (GISWG) Justice Reference Architecture (JRA) Specification, Version 1.7, March 2009, http://it.ojp.gov/globaljra

**MTOM** SOAP Message Transmission Optimization Mechanism (MTOM), W3C Recommendation, January 25, 2005, http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/

**NIEM** National Information Exchange Model, http://www.niem.gov/library.php

**SAML** OASIS Security Assertion Markup Language, Version 2.0 specification set, March 15, 2005, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv2.0

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

**WS Notification** OASIS Web Services Notification, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn

**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/

**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

**WS-I BP** WS-I Basic Profile, Version 1.1, April 10, 2006, http://www.ws-i.org/Profiles/BasicProfile-1.1.html

**WS-I BP12** WS-I (2007), Basic Profile Version 1.2 (draft), http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile

**WS-I BSP** WS-I Basic Security Profile, Working Group Draft, March 30, 2007, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html

**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

**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

**WS-RM** OASIS (2007), Web Services ReliableMessaging, Version 1.1, http://docs.oasis-open.org/ws-rx/wsrm/v1.1/wsrm.pdf

**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

**XML Encryption** W3C (2002), XML Encryption Syntax and Processing, W3C Recommendation, April 14, 2006, http://www.w3.org/TR/xmlenc-core/

**XML Signature** W3C (2002), XML Signature Syntax and Processing, W3C Recommendation, April 14, 2006, http://www.w3.org/TR/xmldsig-core/

**XOP** W3C Recommendation  XML-binary Optimized Packaging, 2005-01-25, http://www.w3.org/TR/xop10/

# 8. Document History

| Date | Version | Editor | Change |
|---|---|---|---|
| April 12, 2007 | 1.0 | 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) |

# Appendix A: Documenter Team

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

- Mr. Jim Cabral, IJIS Institute
- Mr. Scott Came, SEARCH, The National Consortium for Justice Information and Statistics
- Mr. Scott Fairholm, National Center for State Courts
- Mr. Kael Goodman, IJIS Institute, Service Interaction Committee Chair
- Mr. Alan Harbitter, IJIS Institute
- Mr. Zemin Luo, IJIS Institute
- Mr. Tom Merkle, National Institute of Justice
- Mr. John Ruegg, Los Angeles County Information Systems Advisory Body

## *About Global*

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

For more information on DOJ's Global and its products, including those referenced in this document, call

(850) 385-0600

or visit

**www.it.ojp.gov/globaljra**

BJA Bureau of Justice Assistance

This project was supported by Grant No. 2007-NC-BX-K001 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.