United States
Department of Justice

The Global Justice Reference Architecture (JRA) Web Services Service Interaction Profile

V 1.0

by
The Global Infrastructure/Standards Working Group

June 14, 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

The Global Justice Reference Architecture (JRA) was developed through a collaborative effort of the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global).

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, including Management and Policy, Service Interaction, and Services Committees.

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 (SOA-RM) 1.0. Other major contributors deserving of 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, Chair, 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—CapWIN, GISWG Service Interaction Committee

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

For more information about the 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 **WEB SERVICES SERVICE INTERACTION PROFILE (WS SIP)** based on the Web services (WS) family of technology standards.

A **SERVICE INTERACTION PROFILE** [†] (SIP) 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 that interact with an interface should likewise conform to that interface's profile.

The Web Services Service Interaction Profile (WS SIP) discussed in this document is based on the Web services family of technology standards, defined as follows:

- The Web Services Interoperability (WS-I) Organization Basic Profile **[WS-I BP]**,[‡] Version 1.2, and all standards that it references (dated March 28, 2007).
- The WS-I Attachments Profile (**[WS-I AP]**), Version 1.0, and all standards that it references.
- The WS-I Basic Security Profile **[WS-I BSP]** current Working Group Draft, Version 1.0 (dated March 30, 2007), and all Token Profiles and related standards adopted by reference.
- 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.

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

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

1.1. Profile Selection Guidance

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

Select this Profile…	**If your technology stack for information sharing includes:**
Web Services SIP	SOAP, WS-I, WS-*
Websphere MQ/MQ Series SIP	Websphere MQ technologies
ebXML SIP	ebXML technologies **[ebXML]**
File Drop SIP	FTP or S/FTP, flat files, traditional EDI

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[1] **[JRA]** on pages 35 and 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 to use in defining their own Web Services Service Interaction Profile (WS SIP). However, to remain 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 and that the reader interprets this document as a service interaction profile defined in the context of that architecture.

[1] Global Justice Reference Architecture Specification, Working Draft, Version 1.4, http://it.ojp.gov/globaljra.

1.3. Namespace References

This document associates the following namespace abbreviations and namespace identifiers:

- xsd: http://www.w3.org/2001/XMLSchema
- wsdl: http://schemas.xmlsoap.org/wsdl/

2. Conformance Requirements

This section describes what it means to "conform to" this 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 in order 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]**WS-SIP June 13 (comparison).doc
- 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. If an interface enforces a particular service interaction requirement, conformance to this profile requires that 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 interface's description meets all requirements of the **DESCRIPTION** conformance target in **[WS-I BP]**.
- The interface meets all requirements of the **INSTANCE** and **RECEIVER** conformance targets in **[WS-I BP]**.

A service consumer conforms to this service interaction profile if:

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

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 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** in which 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 Web Services Service Interaction Profile. Implementers should be aware that not all product and infrastructure vendors are supporting WS-I Attachments Profile, due to its reliance on the Multipurpose Internet Mail Extensions (MIME) standard for encoding attachments.

3. Service Interaction Requirements

Conformance to this Web Services 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. Service Consumer Authentication

3.1.1. 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 verify the identity of the consumer.

3.1.2. 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 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).

3.1.3. 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 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 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 set.

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 their 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 Web Services 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 assert the validity of information about a human or machine, including its identity.

3.3.2. Conformance Targets (Normative)

Conformance with this Web Services 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 reflect the guidance of that initiative and their 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 Web Services 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 service interaction profile requires that the execution context supporting the service interaction include appropriate 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 Web Services 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 PKI.

3.6.3. Implementation Notes and Implications (Non-Normative)

This Web Services 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 Web Services 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 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).
- A specific address or entity to which reply messages (if any) should be sent.

3.8.2. Conformance Targets (Normative)

Conformance with this Web Services Service Interaction Profile requires that every message must conform to the WS-Addressing 1.0 Core (**[WS-Addressing Core]**) and SOAP Binding (**[WS-Addressing SOAP Binding]**) specifications, as described in Section 8 of **[WS-Addressing SOAP Binding]**. Conformance of messages with the WS-Addressing 1.0 WSDL Binding (**[WS-Addressing WSDL Binding]**) is recommended but not required.

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 **[WS-Addressing Core]** and identifies, with an endpoint reference, the logical or physical address of an intermediary service responsible for implementing the addressing requirements; 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.

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 Web Services Service Interaction Profile requires that message(s) must contain SOAP headers that conform to the requirements of the OASIS WS-ReliableMessaging 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 Web Services 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 Web Services 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 of "applications" and "participants" as defined in **[WS-Coordination]**, **[WS-Atomic Transaction]**, and **[WS-Business Activity]**, as appropriate per nature of the transaction requirements.
- Messages must include the appropriate Coordination Context SOAP header to identify the transactional activity, as defined in **[WS-Coordination]** and as further specified in **[WS-Atomic Transaction]** to support synchronous short duration transactions or **[WS-Business Activity]** to support asynchronous long-running transactions, as appropriate per nature of the transaction requirements.

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

Conformance with this service interaction profile requires that the execution context supporting the interaction include components that implement the Activation and Registration services defined in **[WS-Coordination]**.

3.10.3. Implementation Notes and Implications (Non-Normative)

None.

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 Web Services Service Interaction Profile requires that service interfaces responding to requests for metadata about the interface and underlying service must respond to a service consumer's Get Metadata Request message or Get Request message with a Get Metadata Response message or Get Response message, respectively, where these messages conform to the requirements of the WS-Metadata Exchange specification (**[WS-Metadata Exchange]**).

3.11.3. Implementation Notes and Implications (Non-Normative)

None.

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 the description conformance target in **[WS-I BP]**. **[WS-I BP]** requires an interface's description to consist of a Web Services Description Language (WSDL) document that conforms to **[WSDL 1.1]**.

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

- At least one wsdl:message element for each message involved in the interaction with the service.
- Within the wsdl:portType and wsdl:binding elements, a wsdl:operation element corresponding to each action in the service's behavior model (as defined in the **[JRA]**).

The WSDL document should define types only through importing namespaces defined in external XML Schema. Specifically:

- The WSDL document's wsdl:types element should contain only a single child xsd:schema element.
- The single xsd:schema element should contain only xsd:import elements, each importing a namespace defined in an external schema.
- Each xsd:import element should contain exactly two attributes, namespace and schemaLocation, the value of which are non-null and non-empty.

3.12.3. Implementation Notes and Implications (Non-Normative)

These guidelines regarding definition of types outside a WSDL document are intended to improve reusability of message definitions across service interaction profiles and to separate the concerns of interface definition from message definition.

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

4. Message Exchange Patterns

4.1. Fire-and-Forget Pattern

This section discusses how the message exchange patterns (MEP) identified in the **[JRA]** are supported by this profile.

The fire-and-forget message exchange pattern corresponds to a one-way operation as defined in **[WSDL 1.1]**. 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 a request-response operation as defined in **[WSDL 1.1]**. 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 fire-and-forget MEPs to form more sophisticated composite MEPs.

An asynchronous request-response pattern is supported through a composite MEP. It is implemented using two one-way fire-and-forget 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 event notification messages periodically from the intermediary using the request-response primitive MEP.

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

5. Message Definition Mechanisms

This section demonstrates how this profile supports the **MESSAGE DEFINITION MECHANISMS** identified in the **[JRA]**.

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 SOAP messages with attachments **[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 well-formed XML. This XML must be valid against an XML Schema (as defined in **[XML Schema]**) that defines the message structure.

The names of all elements in this XML Schema must conform to the guidelines documented in Services Specification Guidelines (**[SSG]**).

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.

HTTP HyperText Transport Protocol is the protocol used to transport requests and replies over the World Wide Web.

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 that 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

ebXML ebXML Technical Committee FAQs (note: 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/

FIPS 199 NIST February 2004, Standards for Security Categorization of Federal Information and Information Systems, http://csrc.nist.gov/publications/fips/

FIPS 200 NIST March 2006, Minimum Security Requirements for Federal Information and Information Systems, 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, Working Draft, Version 1.4, February 14, 2007, 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

Schneier Bruce Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, Inc., 1996

SSG GISWG JRA Services Specifications Guidelines, http://it.ojp.gov/globaljra

SwA W3C SOAP Messages With Attachments, W3C Note, November 12, 2000, http://www.w3.org/TR/SOAP-attachments

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-Addressing SOAP Binding	W3C Web Services Addressing 1.0—SOAP Binding, W3C Recommendation, May 9, 2006, http://www.w3.org/TR/2006/REC-ws-addr-soap-20060509/
WS-Addressing WSDL Binding	W3C Web Services Addressing 1.0—WSDL Binding, W3C Candidate Recommendation, May 29, 2006, http://www.w3.org/TR/2006/CR-ws-addr-wsdl-20060529/
WSDL 1.1	W3C Web Services Description Language, Version 1.1, W3C Note, March 15, 2001, http://www.w3.org/TR/wsdl
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 1.2, March 28, 2007, http://www.ws-i.org/Profiles/BasicProfile-1.2.html
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
WS-I SSBP	WS-I Simple SOAP Binding Profile 1.0, August 24, 2004, http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html
WS Notification	OASIS Web Services Notification, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn

WSS SwA	OASIS WS-Security SOAP Messages With Attachments Profile 1.1, February 1, 2006, http://www.oasis-open.org/committees/download.php/16672/wss-v1.1-spec-os-SwAProfile.pdf
WS-Atomic Transaction	OASIS Web Services Atomic Transaction 1.1, Committee Draft, March 15, 2006, http://docs.oasis-open.org/ws-tx/wstx-wsat-1.1-spec-cd-01.pdf
WS-Business Activity	OASIS Web Services Business Activity 1.1, Committee Draft, March 15, 2006, http://docs.oasis-open.org/ws-tx/wstx-wsba-1.1-spec-cd-01.pdf
WS-Coordination	OASIS Web Services Coordination 1.1, Committee Draft, March 15, 2006, http://docs.oasis-open.org/ws-tx/wstx-wscoor-1.1-spec-cd-01.pdf
WS-Metadata Exchange	Industry vendor group specification Web Services Metadata Exchange, September 2004, http://specs.xmlsoap.org/ws/2004/09/mex/WS-MetadataExchange
WS-RM	OASIS Web Services Reliable Messaging, Committee Draft, March 14, 2006, http://docs.oasis-open.org/ws-rx/wsrm/200602/wsrm-1.1-spec-cd-03.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 XML Encryption Syntax and Processing, W3C Recommendation, December 10, 2002, http://www.w3.org/TR/xmlenc-core/
XML Schema	W3C XML Schema, W3C Recommendation, August 12, 2004, http://www.w3.org/XML/Schema

628 **XML Signature** W3C XML-Signature Syntax and Processing,
629 W3C Recommendation, February 12, 2002,
630 http://www.w3.org/TR/xmldsig-core/

631 **XOP** W3C XML-Binary Optimized Packaging, W3C
632 Recommendation, January 25, 2005,
633 http://www.w3.org/TR/xop10/

634

635

636

8. Document History

Date	Version	Editor	Change
August 4, 2006	0.5	Scott Came	The initial document is based on the Web Services Service Interaction Profile (WS SIP) from the state of Washington
August 25, 2006	0.6	Zemin Luo	Updated based on GISWG Service Interaction Committee team discussion
February 14, 2007	0.9	Scott Came	Revision
February 22, 2007	0.9.3	Service Interaction Committee	Review & revise
March 6, 2007	0.9.3	Security Working Group	Review & revise
March 16, 2007	1.0 Candidate	Monique LaBare	SIC Final review
March 23, 2007	1.0 Candidate	Monique La Bare	Formatting, Glossary, References, send to Scott Came for SWG edits.

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 review of this document.

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