Global Justice Information Sharing Initiative

United States
Department of Justice

U.S. Department of Justice's Global

Global Reference Architecture (GRA)

Reliable Secure Web Services Service Interaction Profile

Version 1.1

May 2011

Global Infrastructure/Standards
Working Group

This project was supported by Grant No. 2008-DD-BX-K520 awarded by the Bureau of Justice Assistance, Office of Justice Programs, 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 publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.

Table of Contents

As a part of Global's effort to support information sharing activities that span jurisdictional boundaries within and outside of criminal justice, the Justice Reference Architecture (JRA) has been rebranded to the Global Reference Architecture (GRA). This change will not introduce any significant technical modifications to the architecture but is rather intended to provide a more inclusive service-oriented model that will meet the broader needs of justice, public safety, homeland security, health and human services, and additional stakeholders. The GRA, therefore, is designed to be an information sharing architecture that will meet the needs of government at all levels and fulfill the need for improved collaboration across communities.

Acknowledgements

The Global Reference Architecture (GRA) Framework 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 two committees, Management and Policy and Service Implementation.

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. Sincere appreciation is expressed to Mr. Scott Came, state of Washington, and SEARCH, The National Consortium for Justice Information and Statistics, for their 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 recognition include the OASIS Court Filing Technical Committee, OASIS SOA Reference Model Technical Committee, Messaging Focus Group, and GISWG Service Implementation Committee, especially Mr. Patrice Yuh, Federal Bureau of Investigation, and Mr. Bob Slaski, Open Networks, Inc.

For more information about the Global efforts, including the Global Reference Architecture initiative and corresponding deliverables, please refer to the Global Web site, http://it.ojp.gov/, 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 **RELIABLE SECURE WEB SERVICES SERVICE INTERACTION PROFILE (RS WS-SIP)** based on the Web services (WS) family of technology standards and, in particular, the Web Services Interoperability Organization (WS-I) Reliable Secure Profile **[WS-I RSP]** to the extent practical.

A **SERVICE INTERACTION PROFILE** (SIP) is a concept identified in the Global Reference Architecture **([GRA]).** 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.

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:**
Reliable Secure Web Services SIP	SOAP, WS-I, WS-*, SAML 2.0, GFIPM, WS-I Basic Profile 1.2, and (to the extent practical) the WS-I Reliable Secure Profile 1.0
Web Services SIP	SOAP, WS-I, WS-* and WS-I Basic Profile 1.1
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 GRA Specification document[1] ([GRA]). 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 RS WS-SIPs. However, to remain valid and consistent with the GRA, 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 GRA Specification and that the reader interprets this document as a service interaction profile defined in the context of that architecture.

1.3. Profiles, Standards, and Recommendations

The term "profile" refers to a collection of standards and associated constraints. A profile may itself become a standard, and a profile may be composed of other profiles in addition to standards. In addition to specifying the related standards, a profile defines constraints on the use of specific elements and the behavior of the profiled standards. It is possible for a profile to be composed entirely of approved standards, but the profile itself may not be fully approved. This is currently the case with the WS-I Reliable Secure Profile. All World Wide Web Consortium (W3C) and OASIS standards that are referenced in the WS-I Reliable Secure Profile are approved, but the WS-I Reliable Secure Profile itself is still a working profile.

The terminology for standards approval varies with the different standards development organizations (SDO). For most standards organizations, a specification has the term "draft" in the document title until it is an approved standard. W3C uses the term "recommendation" to indicate an approved standard and identifies a draft with the term "candidate."

1.4. Web Services Interoperability (WS-I) Reliable Secure Profile

The WS-I Reliable Secure Profile 1.0 is designed to be composed with the WS-I Basic Profile 1.2, WS-I Basic Profile 2.0, WS-I Basic Security Profile 1.0, and WS-I Basic Security Profile 1.1. Because of the limited support at present for WS-I Basic Profile 2.0, only the use of WS-I Basic Profile 1.2 will be required for compliance with this SIP.

Basic Profile 1.2 builds on Basic Profile 1.1 by incorporating Basic Profile 1.1 errata and requirements from Simple SOAP Binding Profile 1.0 and by adding support for WS-

[1] Global Reference Architecture Specification, Version 1.8, http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015

Addressing and Message Transmission Optimization Method (MTOM). Because WS-Addressing and MTOM are key building blocks for more advanced services, Basic Profile 1.2-compliance is required. In general, Basic Profile 1.2 preserves forwards and backwards compatibility with the Basic Profile 1.1. Minor potential issues have been identified, but these are addressed by adding constraints that do not allow the circumstances associated with the potential issues.

The Reliable Secure Web Services Service Interaction Profile introduced in this document is based on the Web services family of technology standards, defined as follows:

- WS-I Reliable Secure Profile **[WS-I RSP]**, Version 1.0, dated November 9, 2010, and all standards that it references.
- WS-I Basic Profile **[WS-I BP 1.2]**, Version 1.2, dated November 9, 2010, and all standards that it references.
- WS-I Basic Profile **[WS-I BP 1.1]**, Version 1.1, Second Edition, dated October 25, 2007, also identified as ISO/IEC 29361:2008, and all standards that it references.
- WS-I Basic Security Profile (**[WS-I BSP 1.0]**), Version 1.0, dated July 5, 2010, and all Token Profiles and related standards adopted by reference.
- WS-I Basic Security Profile **[WS-I BSP 1.1]**, Version 1.1 dated January 24, 2010, 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 profile or 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.

1.5. Reliable Secure Profile Usage Scenarios

Usage scenarios for the **[WS-I RSP]** are defined in the Reliable Secure Profile Usage Scenarios Version 1.0 **[RSP USE]**. This service interaction profile supports these usage scenarios by requiring that service consumers and service interfaces conform to **[WS-I RSP]** and support the usage scenarios defined in **[RSP USE]**.

1.6. Transport Independent Messaging Protocol

Web services use SOAP [SOAP] as a messaging framework. SOAP is not tied to any specific transport protocol, although most SOAP web service exchanges are implemented using HTTP [HTTP]. SOAP message exchange using the Simple Mail Transfer Protocol (SMTP) has also been standardized as well as the exchange of SOAP messages using the Advanced Message Queuing Protocol (AMQP).

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 to ensure interoperable implementations of those concepts.

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

- **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 conformance targets listed above in a way consistent with their definitions in the **[GRA].**
- 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 implement every Service Interaction Requirement identified in this profile. If an interface needs one or more of the listed service interaction requirements, conformance to this profile requires that each requirement be met pursuant to 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 1.2].**

- The interface meets all requirements of the **INSTANCE** and **RECEIVER** conformance targets in **[WS-I BP 1.2]**.

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 1.2]**.

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 1.2]**.
- The message conforms to the National Information Exchange Model (**[NIEM]**) or other published standard **DOMAIN VOCABULARIES** in which the semantics of the service's information model match components in those vocabularies.

Note: LEXS offers great potential to simplify and standardize the content of the information model of services; as such, designers of MESSAGEs should consider using LEXS as a framework for structuring the information model.

2.3. Implementation Notes and Implications (Non-Normative)

Global intends to monitor progress on the WS-I Basic Profile 1.2 as it reaches final approval.

Global intends to monitor progress on the the WS-I Reliable Secure Profile 1.0 and WS-I Basic Profile 2.0 as they reach final approval and broader implementation.

3. Service Interaction Requirements

This service interaction profile assumes that implementers will utilize Network and Transport Layer Security features of their data networks to provide confidentiality and message integrity between two communicating end points (including but not limited to HTTPS, firewalls, and virtual private networks **[VPNs]**).

Web Services Message Layer Security Standards and WS* standards are implemented by embedding XML metadata specific to each WS* standards in the SOAP Message Header blocks. The Service Interaction Requirements listed in this profile are specific to SOAP messaging and the Application/Service level specific requirements for reliability, authentication, non-repudiation, authorization, metadata discovery, etc.

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 GRA

The GRA 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 context token that conforms to [WS-I BSP 1.1].

Implementers are strongly encouraged to use the Global Federated Identity and Privilege Management ([GFIPM]) security initiative for consumer authentication. GFIPM is capable of providing authentication, authorization, and single sign-on for both user-to-system and system-to-system applications. For the specific normative requirements for federated authentication using GFIPM, please refer to the ([GFIPM]) Web Services System-to-System Profile. Service consumer authentication may be performed using a secure conversation, which is performed in two steps. A secure conversation must be established in accordance with [RSP USE]. The secure conversation must be compliant with WS-SecureConversation [WS-SECURECONVERSATION]. Service consumer authentication will be performed as part of the process of establishing the secure conversation, and a security context token will be created. Subsequent exchanges will require the use of the security context token to authenticate the consumer as part of the ongoing secure conversation.

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)

3.2. Service Consumer Authorization

None.

3.2.1. Statement of Requirement From GRA

The GRA 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 security token(s).

3.2.3. Implementation Notes and Implications (Non-Normative)

Implementers are strongly encouraged to use the Global Federated Identity and Privilege Management ([GFIPM]) security initiative for consumer authorization. GFIPM is capable of providing authentication, authorization, and single sign-on for both user-to-system and system-to-system applications. For the specific normative requirements and consumer authorization using GFIPM, please refer to the ([GFIPM]) Web Services System-to-System Profile.

3.3. Identity and Attribute Assertion Transmission

None.

3.3.1. Statement of Requirement From GRA

The GRA 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 provide the consumer's authorization security token(s) to perform the requested action.

Implementers are strongly encouraged to use the Global Federated Identity and Privilege Management ([GFIPM]) security initiative for identity and authorization attributes. GFIPM is capable of providing authentication, authorization, and single sign-on for both user-to-system and system-to-system applications. For the specific normative requirements and attribute assertion requirements using GFIPM, please refer to the ([GFIPM]) Web Services System-to-System Profile and and GFIPM metadata attributes ([GFPIM-MS]).

3.3.3. Implementation Notes and Implications (Non-Normative)

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.

3.4. Service Authentication

3.4.1. Statement of Requirement From GRA

The GRA 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 1.1].**

Implementers are strongly encouraged to use the Global Federated Identity and Privilege Management (**[GFIPM]**) security initiative for service authentication. GFIPM is capable of providing authentication, authorization, and single sign-on for both user-to-system and system-to-system applications. For the specific normative requirements and service authentication using GFIPM, please refer to the (**[GFIPM]**) Web Services System-to-System Profile.

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)

GFIPM utilizes X.509 Certificates from the GFIPM Federation Trust file to perform Service Authentication and digital signature validation.

3.5. Message Non-Repudiation

3.5.1. Statement of Requirement From GRA

The GRA 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 1.1].**

- 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 1.1]** 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 1.1]** provides an example of this technical approach in Section 11, “Extended Example.”

3.6. Message Integrity

3.6.1. Statement of Requirement From GRA

The GRA 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 1.1]** Section 9, “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)

None.

3.7. Message Confidentiality

3.7.1. Statement of Requirement From GRA

The GRA 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 1.1]. 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 1.1] Section 10, "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 GRA

The GRA 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 includes 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.

2. The endpoint reference includes 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)

Implementations with Web services intermediaries are considered best practices and are encouraged to use the actor or role concepts to identify intermediate processes and/or routing in accordance with [WS-I BP 1.2].

The W3C has created the Web Services Resource Access Working Group to provide standards for accessing resource-oriented services. Global intends to monitor the progress of the Web Services Resource Access Working Group and consider the completed standards for later inclusion.

3.9. Reliability

3.9.1. Statement of Requirement From GRA

The GRA 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-RELIABLEMESSAGING]).

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-RELIABLEMESSAGING] standard.

3.9.3. Implementation Notes and Implications (Non-Normative)

The implementation of reliable messaging services is particularly important for one-way message exchange patterns since no "response" is expected and, consequently, a successful response cannot be used to assume a successful exchange.

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 GRA

The GRA 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-ATOMICTRANSACTION], and [WS-BUSINESSACTIVITY], 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-ATOMICTRANSACTION] to support synchronous short-duration transactions or [WS-BUSINESSACTIVITY] 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-ATOMICTRANSACTION] and Section 4 of [WS-BUSINESSACTIVITY], 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 GRA

The GRA 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-MetadataExchange specification ([WS-METADATAEXCHANGE]).

3.11.3. Implementation Notes and Implications (Non-Normative)

WS-MetadataExchange is part of a group of W3C member submission standards, including WS-Transfer, that are being advanced as W3C standards by the W3C Web Services Resource Access Working Group. Global intends to monitor the progress of the Web Services Resource Access Working Group and consider the completed standards for later inclusion.

3.12. Interface Description Requirements

3.12.1. Statement of Requirement From GRA

This section demonstrates how this profile meets the Service Interaction Requirements identified in the [GRA].

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 1.2]. [WS-I BP 1.2] 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 [GRA]).

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.

Message exchange patterns [MEPs] as defined in the usage scenarios [RSP USE] are required by the service interaction profile.

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 Definition Mechanisms

This section discusses how the message exchange patterns identified in the [GRA] are supported by this profile.

4.1. 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 [RSP USE].

This MEP is synchronous and can be combined with One-Way 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 MEPs.

4.2. One-Way Pattern

The One-Way 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 **[RSP USE]**. Many composite asynchronous message exchange patterns can be derived from this primitive pattern.

4.3. Faults

Faults should be specified in accordance with WS-BaseFaults [WS-BaseFaults].

4.4. 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 one-way primitive MEP.
2. A publisher sends an event message to the intermediary using the one-way 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 one-way primitive MEP.
   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 **[GRA]**.

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 1.2]**) that meets all requirements of this profile.

- An XML information set as defined in **[XML INFOSET]**.

Note that **[WS-I BP 1.2]** requires 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.

An **[XML INFOSET]** may utilize XML binary Optimized Packaging **[XOP]** and streamline the information exchange using the Message Transmission Optimization Method **[MTOM]**.

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

6. Requirements Conformance Targets Summary

This section provides a summary of the conformance targets for each requirement in tabular form.

Requirement	Specification
Service Consumer Authentication	✓ WS-I Security Profile 1.1 ✓ WS-SecureConversation 1.3 ✓ GFIPM
Service Consumer Authorization	✓ WS-I Security Profile 1.1 ✓ SAML 2.0 ✓ GFIPM
Identity Attribute Assertion Transmission	✓ SAML 2.0 ✓ GFIPM
Service Authentication	✓ WS-I Security Profile 1.1 ✓ GFIPM
Non-Repudiation	✓ WS-I Security Profile 1.1 ✓ Timestamp w/XML Signature
Reliability	✓ WS-ReliableMessaging 1.1
Message Integrity	✓ WS-I Security Profile 1.1

Requirement	Specification
	✓ XML Signature
Message Confidentiality	✓ WS-I Security Profile 1.1 ✓ XML Encryption ✓ FIPS 140-2Transport Layer Security
Message Addressing	✓ WS-Addressing 1.0
Transaction Support	✓ WS-AtomicTransaction 1.2 ✓ WS-BusinessActivity 1.2 ✓ WS-Coordination 1.2
Service Metadata Availability	✓ WS-MetadataExchange 1.1 ✓ WS-Transfer
Interface Description	✓ WSDL 1.1
Message Exchange Patterns	✓ Request-Response, One-Way ✓ WS-BaseFaults 1.2 ✓ WS-Notification 1.3
Simple Message	✓ XML ✓ SOAP
Composite Message	✓ XML Infoset
Binary Data	✓ XML-Binary Optimized Packaging ✓ Message Transmission Optimization Package

7. 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 that seeks to satisfy a particular need through the use of 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 **[GRA]** 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.

8. 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)

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) Web Services Concept of Operations

GFIPM-MS Global Security Working Group (GSWG) Global Federated Identity and Privilege Management (GFIPM) Metadata Specification, Version 2.0, September 15, 2010, http://it.ojp.gov/gfipm

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

HTTP Hypertext Transfer Protocol RFC 2616, June 1999, http://www.w3.org/Protocols/rfc2616/rfc2616.html

GRA Global Infrastructure/Standards Working Group (GISWG) Global Reference Architecture (GRA) Specification, Version 1.8, April 2011, 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

RSP USE WS-I Reliable Secure Profile Usage Scenarios, Final, Version 1.0, December 15, 2008, http://www.ws-i.org/profiles/rsp-scenarios-1.0.pdf

SAML OASIS Security Assertion Markup Language, Version 2.0 specification set, OASIS standard—Errata composite, February 12, 2007, http://saml.xml.org/saml-specifications

SDG GISWG GRA Service Description Guidelines, http://it.ojp.gov/globaljra

SOAP W3C SOAP Note, May 8, 2000, http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

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-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/

WS-AtomicTransaction OASIS Web Services Atomic Transaction 1.2, OASIS standard, February 2, 2009, http://docs.oasis-open.org/ws-tx/wsat/2006/06

WS-BaseFaults OASIS Web Services Base Faults 1.2, OASIS standard, April 1, 2006, http://docs.oasis-open.org/wsrf/wsrf-ws_base_faults-1.2-spec-os.pdf

WS-BusinessActivity OASIS Web Services Business Activity 1.2, February 2, 2009, http://docs.oasis-open.org/ws-tx/wsba/2006/06

WS-Coordination OASIS Web Services Coordination 1.2, February 2, 2009, http://docs.oasis-open.org/ws-tx/wscoor/2006/06

WS-SecureConversation OASIS Web Services Secure Conversation 1.3, March 1, 2007, http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.3/ws-secureconversation.html

WSDL 1.1 W3C Web Services Description Language, Version 1.1, W3C Note, March 15, 2001, http://www.w3.org/TR/wsdl

WS-I BP 1.2 WS-I Basic Profile Version 1.2, Final Material, November 9, 2010, http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html

WS-I BSP 1.1 WS-I Basic Security Profile Version 1.1, January 24, 2010, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html

WS-I RSP WS-I Reliable Secure Profile Version 1.0, Final Material, November 9, 2010, http://www.ws-i.org/profiles/ReliableSecureProfile-1.0-2010-11-09.html

WS-MetadataExchange WS-Metadata Exchange 1.1 W3C Member Submission, August 13, 2008, http://www.w3.org/Submission/WS-MetadataExchange/

WS-ReliableMessaging OASIS Web Services Reliable Messaging 1.1, January 7, 2008, http://docs.oasis-open.org/ws-rx/wsrm/v1.1/wsrm.html

WS-Transfer Web Services Transfer, W3C Member Submission, January 7, 2008, http://www.w3.org/Submission/2006/SUBM-WS-Transfer-20060927/

WS-Security 1.1 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 Infoset W3C XML Information Set (second edition), W3C Recommendation, February 4, 2004, http://www.w3.org/TR/xml-infoset/

XML Schema W3C XML Schema, W3C Recommendation, August 12, 2004, http://www.w3. org/XML/Schema

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

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

This document associates the following namespace abbreviations and namespace identifiers:

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

9. Document History

Date	Version	Editor	Change
June 1, 2009	0.9	Patrice Yuh Bob Slaski	The initial document is based on the Global Web Services Service Interaction Profile (WS SIP) and the WS-I Reliable Secure Profile.
July 10, 2009	1.0		Final formatting and editing and document published.
October 2010	1.1	Bob Slaski, Scott Came	Specified WS-I BP 1.2 along with WS-SecureConversation V1.3 and WS-ReliableMessaging 1.1 instead of WS-I RSP; updated standard references; added WS-BaseFaults 1.2.
April 2011	1.1	Bob Slaski, James Dyche, Matt Moyer, John Ruegg	Consolidated the discussion on Transport Level Security into the lead-in paragraph under the section Service Interaction Requirements. Also clarified that all SIP guidelines are specific to SOAP WS* standards.
		James Douglas	Updated 2.2, message conformance paragraph.
April 2011	1.1		Changed JRA to GRA.

Editors

Scott Came	James Dyche	David Gillespie

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). The following individuals were members of the Development Team for this document and participated in its review:

- Mr. Scott Came, SEARCH, The National Consortium for Justice Information and Statistics
- Mr. Patrice Yuh, Federal Bureau of Investigation
- Mr. Bob Slaski, Open Networks Inc.

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
U.S. Department of Justice