LEXS 3.1.4 Web Services Service Interaction Profile Version 0.4

(Draft 2011-08-15)

Table of Contents

Table of Contents i
Acknowledgements iii
1. Introduction 1
2. Purpose 4
2.1. Usage 4
2.2. Profile Selection Guidance 4
2.3. References 4
3. Conformance Requirements 7
3.1. Conformance Targets 7
3.2. General Conformance Requirements 8
4. Service Interaction Requirements 10
4.1. Service Consumer Authentication 10
4.1.1. Statement of Requirement from GRA 10
4.1.2. Conformance Targets 10
4.1.3. Implementation Notes and Implications 10
4.2. Service Consumer Authorization 11
4.2.1. Statement of Requirement from GRA 11
4.2.2. Conformance Targets 11
4.2.3. Implementation Notes and Implications 11
4.3. Identity and Attribute Assertion Transmission 11
4.3.1. Statement of Requirement From GRA 12
4.3.2. Conformance Targets 11
4.3.3. Implementation Notes and Implications 12
4.4. Service Authentication 12
4.4.1. Statement of Requirement From GRA 12
4.4.2. Conformance Targets 12
4.4.3. Implementation Notes and Implications 12
4.5. Message Non-Repudiation 12
4.5.1. Statement of Requirement from GRA 12
4.5.2. Conformance Targets 12
4.5.3. Implementation Notes and Implications 13
4.6. Message Integrity 13

4.6.1. Statement of Requirement from GRA 13
4.6.2. Conformance Targets 13
4.6.3. Implementation Notes and Implications 13
4.7. Message Confidentiality 13
4.7.1. Statement of Requirement from GRA 13
4.7.2. Conformance Targets 14
4.7.3. Implementation Notes and Implications 14
4.8. Message Addressing 14
4.8.1. Statement of Requirement from GRA 14
4.8.2. Conformance Targets 14
4.8.3. Implementation Notes and Implications 14
4.9. Reliability 15
4.9.1. Statement of Requirement from GRA 15
4.9.2. Conformance Targets 15
4.9.3. Implementation Notes and Implications 15
4.10. Transaction Support 15
4.10.1. Statement of Requirement from GRA 15
4.10.2. Conformance Targets 15
4.11. Service Metadata Availability 15
4.11.1. Statement of Requirement from GRA 15
4.11.2. Conformance Targets 15
4.11.3. Implementation Notes and Implications 15
5. Interface Description Requirements 16
5.1. Statement of Requirement From GRA 16
5.2. Conformance Targets 16
5.3. Implementation Notes and Implications 17
5.4. Policy 17
6. Message Exchange Patterns 17
6.1. One-Way Pattern 17
6.2. Request-Response Pattern 18
6.3. Faults 18
7. Message Definition Mechanisms 18

Acknowledgements

The Global Reference Architecture Framework **[GRA]** 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.

National Information Exchange Model, NIEM, is an interagency initiative to provide the foundation and building blocks for national-level interoperable information sharing and data exchange. The NIEM project was initiated in 2005 as a joint venture between the U.S. Department of Homeland Security (DHS) and DOJ with outreach to other departments and agencies. Details can be obtained from http://www.niem.gov/ .

In 2003, The Office of the CIO at DOJ launched The Law Enforcement Information Sharing Program (LEISP) to transform the sharing of DOJ law enforcement information with its federal, state, local, and tribal law enforcement partners.

The Logical Entity Exchange Specification, version 3.1.4 **[LEXS]** (pronounced "lex"), is a product of the LEISP and leverages NIEM in defining formats for information exchange. Additional information about **[LEXS]** can be obtained from http://www.lexs.gov/ .

Although this document is also the product of the LEISP, it was primarily adapted from the technical reference entitled "The Global Reference Architecture (GRA) Reliable Secure Web Services Service Interaction Profile Version 1.1" (**[GRA RS WS-SIP]**) developed by Global and its GISWG membership. To obtain this reference please refer to the Global Web site.

The following individuals have attended our project meetings, assisted on this research effort, provided input, and reviewed this report:

Benjamin Shrom (Co-Author) - GTRI

Boris Shur, Chief Data Architect – DOJ / LEISP

Sudhi Umarji , (Co-Author) - DOJ / LEISP / Trusted Federal Systems Inc.

Jeremy Warren, CTO - DOJ / LEISP

Jack Wallace - GTRI

Brad Lee - GTRI

Priscilla Walmsley - DOJ / LEISP / Trusted Federal Systems Inc.

1. Introduction

This document uses a vocabulary from both **[GRA]** and **[LEXS]**, so it is helpful to review some terms used therein, that originated out of work in LEXS OASIS or GISWG.

"SERVICE ORIENTED ARCHITECTURE (SOA)" is a term that has been defined by OASIS in the Reference Model for Service-Oriented Architecture 1.0, OASIS Standard **[SOA-RM]** *as a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains* (e.g. HP, Microsoft, Intel, DOJ, DHS). **SOA** architectural patterns targeted to a particular domain or discipline (e.g. Justice, Health, Defense, Manufacturing, Retail) are called **REFERENCE ARCHITECTURES** and are developed to explain and underpin a generic design template supporting a specific **SOA**. A **REFERENCE MODEL** is intended to provide an even higher level of commonality, with definitions that should apply to all **SOA**. Specifically, a **REFERENCE MODEL** (see figure) is defined by **[SOA-RM]** as:

- A minimal set of unifying concepts, axioms and relationships common to **SOA**
- An abstract framework for understanding significant relationships among the entities in an **SOA**
- Independent of specific standards, technologies, implementations, or other concrete details

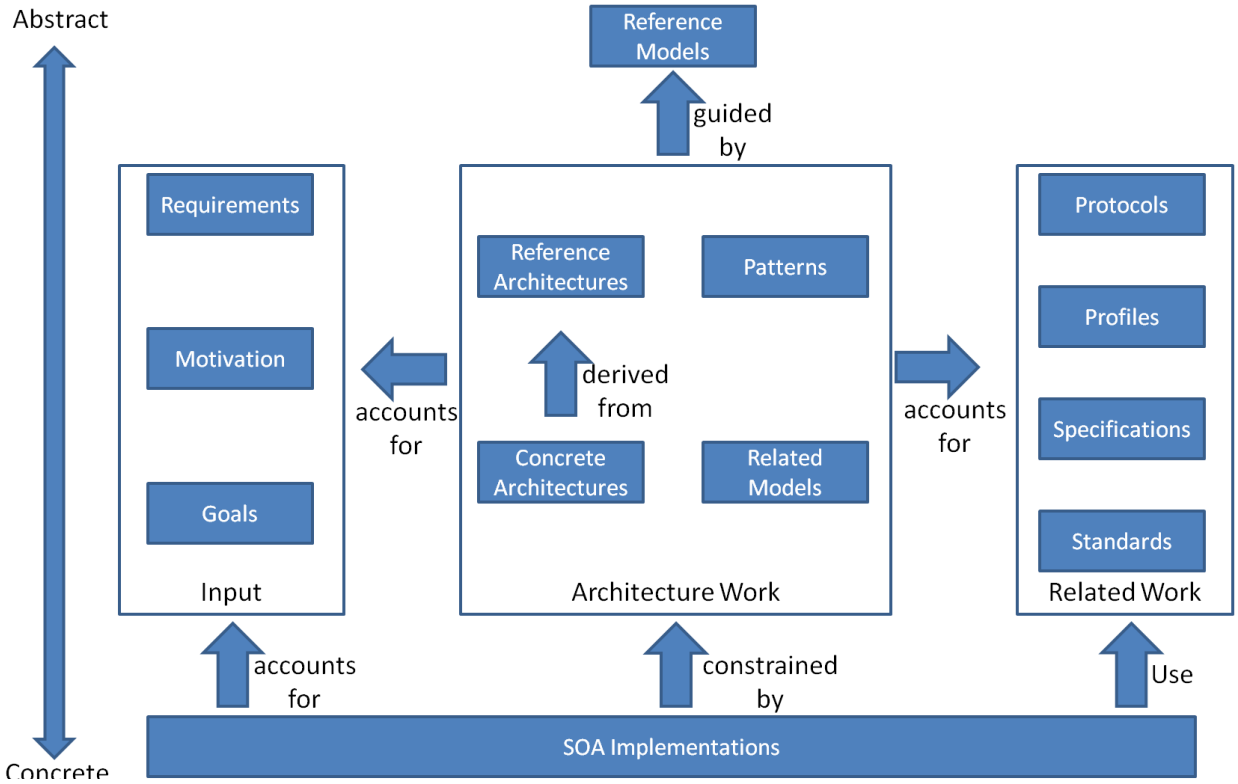

Figure 2: SOA-RM Conceptual Diagram

The Global Reference Architecture Framework version 1.9 **[GRA]**, defines a **REFERENCE ARCHITECTURE** guided by the **[SOA-RM]** that lays out common concepts and definitions as the

foundation for the development of consistent **SOA** implementations within the justice and public safety communities, creating a **REFERENCE MODEL** consistent with **[SOA-RM]**.

[LEXS] is a NIEM conformant family of IEPDs defining a **CONCRETE ARCHITECTURE** guided by the **[SOA-RM]** that was developed to enable information sharing among government organizations. The problems solved by **[LEXS]** are aggregation of and query on a common level of understanding (the digest). In **[LEXS]** there are two main divisions of data transfer, publish/discover **[LEXS-PD]** and search/retrieve **[LEXS-SR]**. **[LEXS-PD]** allows multiple remote services to transmit data to another remote service via a one-way publish operation. **[LEXS-SR]** allows users to search across multiple remote resources as shown below in Figure 3:

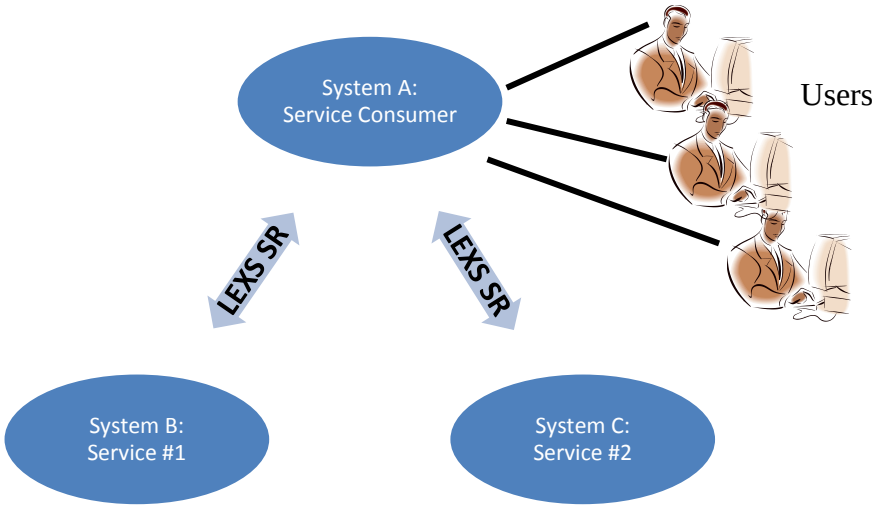

Figure 3: LEXS-SR Conceptual Usage Diagram

Although **[LEXS]** was not chronologically derived from **[GRA]**, it was developed with careful attention to **SOA** and **[SOAP]**-based web services standards, many of which are normative in **[GRA]**. As a result, an information sharing solution supporting a multitude of organizations that conforms to both **[LEXS]** and **[GRA]** can be implemented. It is also certainly possible for a solution to be implemented that conforms to **[LEXS]** and not to **[GRA]** (or vice versa).

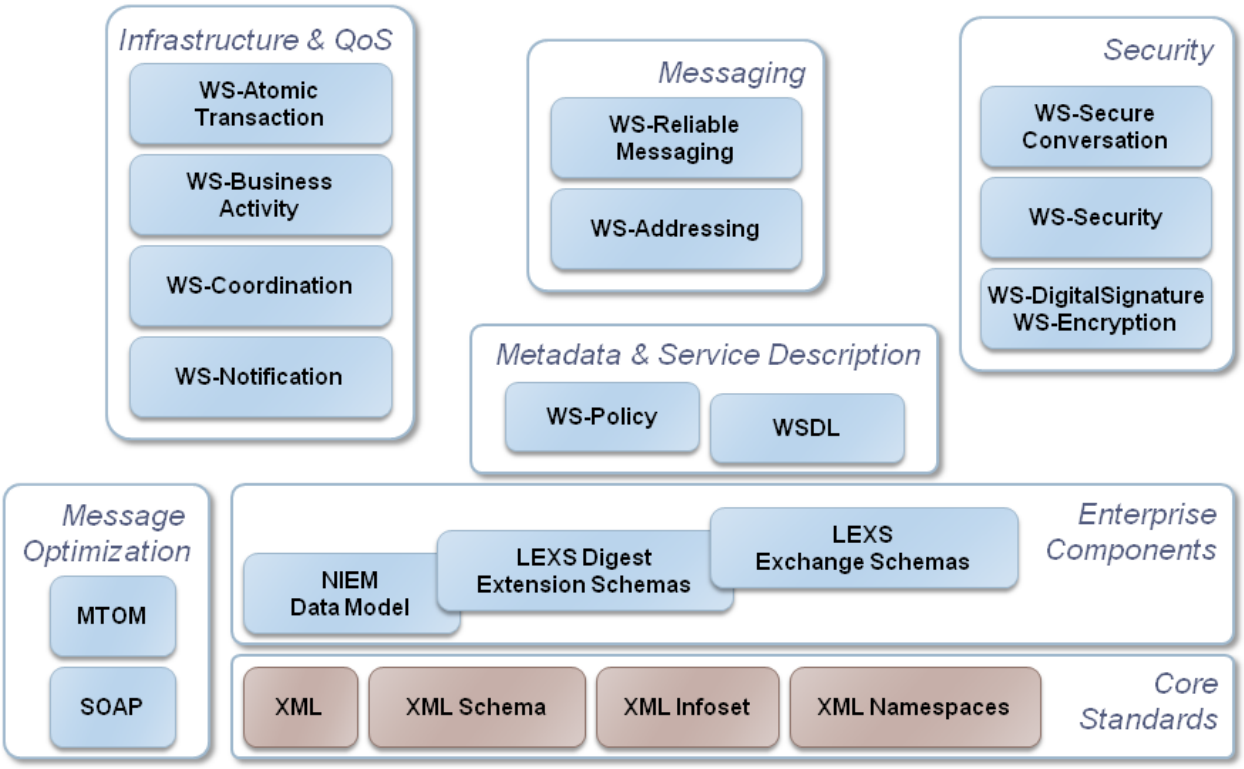

Figure 4: LEXS and GRA SOA Standards

While [SOAP]-based web services are a technical solution to enable SOA and [LEXS], they are not required to implement SOA or [LEXS]. For example, [LEXS] includes [LEXS-PD] and [LEXS-SR]; these specifications are based on SOA and existing [LEXS-PD] implementations today use XML over secure file transfer protocol (SFTP) instead of [SOAP] to implement SOA. [LEXS] does not mandate or require any specific SOA technology, and it was designed to be agnostic to the SOA implementation being used, often duplicating data found in many WS-I standards, such as Web Services Addressing [WS-ADDR]. Any possible combination of SOA implementations can be considered a valid [LEXS] exchange, provided the MESSAGE used is valid to [LEXS].

A Service Interaction Profile (SIP) is a concept identified in the [GRA]. This concept defines an approach to meeting the basic requirements necessary for interaction between SERVICE CONSUMERS and SERVICES. A SIP document specifies that requirements such as Message Integrity, Message Confidentiality and Message Addressing should be implemented using specifications such as WS-Security, XML-Encryption, XML-Signature and WS-Addressing. However, the profile also allows implementations to use alternative means to meet some requirements. For example, while requiring XML-Signature to support Message Integrity requirements, the profile also states "*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)*". To the extent possible, this SIP attempts to remove any alternative mechanism to aid in the interoperability of conformant web services.

2. Purpose

The purpose of this document is to provide a **SIP** for **[LEXS]** Web Services (LEXS WS-SIP) that further constrains conformance targets defined by **[GRA]** to increase interoperability. The increase of interoperability is achieved by defining normative constraints on possible **SOA** implementation technology and on the **MESSAGE** conformance target.

2.1. Usage

This document is intended to serve as a guideline for exchanging information among consumer systems (e.g. System A in Figure 3) and provider systems (e.g. System B or System C in Figure 3). This profile does not guide interaction between humans (e.g. users of System A in Figure 3) and services, even though such interaction is within the scope of **[SOA-RM]**.

This document may serve as a reference or starting point for implementers to use in defining their own **[LEXS]** based Web Services **SIP**. However, to remain valid and consistent with this **[LEXS WS-SIP]**, an implementer may only further specify or constrain this profile and may not introduce techniques or mechanisms that conflict with this profile's guidance.

2.2. Profile Selection Guidance

This profile is intended to define conformance between **[GRA]** and **[LEXS]**. For those who wish to use more sophisticated technologies, such as Reliable Secure Web Services, it is recommended to use the **[GRA WS RS-SIP]**, while maintaining the rules associated with the **MESSAGE** and **MESSAGE EXCHANGE PATTERN** conformance targets specified in this document. **[LEXS]** does not impose any additional requirements that would prohibit use of that profile with **[LEXS]**, and conformance to this profile does not guarantee any conformance to implementations of **[GRA WS RS-SIP]**.

2.3. References

To be in conformance with this document, extensions of this document MUST use the following standard/profile versions, where applicable:

Reference Name	Reference Information
MTOM	W3C Recommendation, 25 January, 2005 http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/
GFIPM	Global Security Working Group (GSWG) Global Federated Identity and Privilege Management (GFIPM) Web Services Concept of Operations http://it.ojp.gov/docdownloader.aspx?ddid=1332
GRA	Global Reference Architecture Framework 1.9, April, 2011

	http://it.ojp.gov/docdownloader.aspx?ddid=1223
GRA RS WS-SIP	GRA Reliable Secure Web Services Service Interaction Profile Version 1.1, May 2011 http://it.ojp.gov/docdownloader.aspx?ddid=1134
LEXS	LEXS IEPD 3.1.4, February 2009 http://www.lexs.gov/sites/all/lexs/docs/LEXS3.1.4_2009-02-06.zip
LEXS-PD	The Publish/Discover portion of the **[LEXS]** IEPD.
LEXS-SR	The Search/Retrieve portion of the **[LEXS]** IEPD.
NDR	Naming and Design Rules, version 1.3 http://www.niem.gov/pdf/NIEM-NDR-1-3.pdf
SOA-RA	Reference Architecture for Service-Oriented Architecture 1.0, Public Review Draft 1. OASIS, April 23, 2008. http://docs.open-oasis.org/soa-rm/soa-ra/v1.0/soa-ra-pr-1.0.pdf
SOA-REC	GISWG. A Framework for Justice Information Sharing: Service-Oriented Architecture. Global, December 9, 2004. http://it.ojp.gov/documents/20041209_SOA_Report.pdf
SOA-RM	Reference Model for Service-Oriented Architecture 1.0, OASIS Standard. OASIS, October 12, 2006. http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf
SOAP	Version 1.1 http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
WS-Addr	Web Services Addressing http://www.w3.org/2002/ws/addr/
WS-Addr Core	Web Services Addressing Core Specification W3C Recommendation, 9 May 2006 http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/

WS-Addr SOAP	Web Services Addressing SOAP Binding W3C Recommendation, 9 May 2006 http://www.w3.org/TR/2006/REC-ws-addr-soap-20060509/
WS-Addr WSDL	Web Services Addressing WSDL Binding W3C Candidate Recommendation, 29 May 2006 http://www.w3.org/TR/2006/CR-ws-addr-wsdl-20060529/
WS-I BP 1.2	Web Services Interoperability Basic Profile 1.2 WS-I Working Group Standard, 9 Nov 2010 http://ws-i.org/profiles/BasicProfile-1.2-2010-11-09.html
WSDL	W3C Web Services Description Language 1.1 W3C Note, 15 March 2001 http://www.w3.org/TR/wsdl
WS-I BSP 1.1	Web Services Interoperability Basic Security Profile 1.1 24, January 2010 http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html
WS-Policy	Web Services Policy Framework, v 1.5 http://www.w3.org/2002/ws/policy/
WS-Security	OASIS Web Services Security: SOAP Message Security 1.1 OASIS Standard, 1 February 2006 http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
XML-Encryption	*XML Encryption Syntax and Processing* W3C Recommendation 10 December 2002 http://www.w3.org/TR/xmlenc-core/
XML Schema	XML Schema W3C Recommendation, 12 August 2004 http://www.w3.org/XML/Schema

XOP	W3C XML-Binary Optimized Packaging W3C Recommendation, 25 January 2005 http://www.w3.org/TR/xop10/
XML-Signature	*XML Signature Syntax and Processing (Second Edition)* W3C Recommendation, 12 February 2002 http://www.w3.org/TR/xmldsig-core/
WS-ReliableMessaging	OASIS Web Services Reliable Messaging 1.1 7 January 2008 http://docs.oasis-open.org/ws-rx/wsrm/v1.1/wsrm.html
WS-BaseFaults	Web Services Base Faults 1.2 OASIS Standard, 1 April 2006 http://docs.oasis-open.org/wsrf/wsrf-ws_base_faults-1.2-spec-os.pdf

3. Conformance Requirements

This section describes what it means to "conform to" this service interaction profile.

3.1. 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 **SIP** does not require a **SERVICE INTERFACE** to enforce every service interaction requirement identified in the **[GRA]**. 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.

3.2. General Conformance Requirements

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 MUST validate to the NIEM-based XML Schema definitions defined by **[LEXS]**
- The message MUST conform to all rules defined in Section 8 of the NIEM Naming and Design Rules version 1.3 **[NDR]**.
- The message MUST use exchange elements defined in the following namespaces as the root element in the exchange. Other namespaces are NOT permitted.
  - http://usdoj.gov/leisp/lexs/publishdiscover/3.1
  - http://usdoj.gov/leisp/lexs/searchretrieve/3.1

3.3. Baseline Requirements for GRA Conformance

To maintain close compatibility with **[GRA]** and **[GRA WS RS-SIP]**, this **[LEXS WS-SIP]** mandates the use of the following version of standards/profiles were applicable, even if not directly referenced:

Standard/Profile	Version/Date
WS-I Basic Profile	1.2
WS-I Basic Security Profile	1.1
Simple Object Access Protocol (SOAP)	1.1
Web Services Description Language (WSDL)	1.1
WS-Security	1.1
WS-SecureConverstaion	1.3
XML Signature	2002-02-12
XML Encryption	2002-12-10
WS-Trust	1.3
WS-Policy	1.2
WS-PolicyAttachment	1.2
WS-SecurityPolicy	1.2
WS-ReliableMessaging	1.1
WS-ReliableMessaging Policy	1.1
WS-MetadataExchange	1.1
WS-Notification	1.3
WS-Coordination	1.2
WS-AtomicTransaction	1.2
WS-BusinessActivity	1.2

WS-BaseFaults	1.2
Security Assertion Markup Language (SAML)	2.0

4. 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.

This profile assumes that implementers will use features of their data networks to achieve improved message reliability, confidentiality, etc. However, implementers MUST NOT use only the additional features of their data networks to perform the functions listed from this **SIP**, but MAY use them to satisfy additional security requirements

Conformance to this **SIP** 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.

4.1. Service Consumer Authentication

4.1.1. 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.

4.1.2. Conformance Targets

Conformance with this **SIP** requires that **[LEXS]** 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]**.

The identity of the user or system provided in the security token(s) MUST match the identity given in the **[LEXS]** message(s) metadata, therefore services may use either for authentication purposes. For example, a user token must match lexs:UserAssertion or a system token must match ulex:MessageOriginMetadata.

4.1.3. Implementation Notes and Implications

Implementers are strongly encouraged to use the Global Federated Identity and Privilege Management **[GFIPM]** security initiative for consumer authentication.

X.509 certificate-based security tokens represent a situation in which the security token cannot map directly to the **[LEXS] MESSAGE**, so it is understood that implementing organizations MUST agree before the exchange how the certificates represent the systems or users present in the **MESSAGE**.

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

4.2. Service Consumer Authorization

4.2.1. Statement of Requirement from GRA

The [GRA] requires that each SIP 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.

4.2.2. Conformance Targets

Conformance with this SIP requires that the [LEXS] MESSAGE sent to the SERVICE INTERFACE by a SERVICE CONSUMER MUST assert the consumer's authorization security token(s). The security token(s) MUST conform to [WS-I BSP 1.1].

The identity of the user or system provided in the security token(s) MUST match the identity given in the [LEXS] message(s) metadata, therefore services may use either for authorization purposes. For example, a user token must match lexs:UserAssertion or a system token must match ulex:MessageOriginMetadata.

4.2.3. Implementation Notes and Implications

Implementers are strongly encouraged to use the Global Federated Identity and Privilege Management [GFIPM] security initiative for consumer authorization.

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

4.3. Identity and Attribute Assertion Transmission

4.3.1. Statement of Requirement from GRA

The [GRA] requires that each SIP 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.

4.3.2. Conformance Targets

Conformance to this SIP requires that message(s) sent to the service interface by a service consumer must provide the consumer's authorization security token(s) to identify the identity and attributes about the requesting entity. The security token(s) MUST conform to [WS-I BSP 1.1].

The identity of the user or system provided in the security token(s) MUST match the identity given in the [LEXS] message(s), therefore services may use either for identity and attribute

assertion purposes. For example, a user token must match lexs:UserAssertion or a system token must match ulex:MessageOriginMetadata.

4.3.3. Implementation Notes and Implications

Implementers are strongly encouraged to use the Global Federated Identity and Privilege Management **[GFIPM]** security initiative for identity and authorization attributes.

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

4.4. Service Authentication

4.4.1. Statement of Requirement From GRA

The **[GRA]** requires that each **SIP** define how a service provides information to a consumer that demonstrates the service's identity to the consumer's satisfaction.

4.4.2. Conformance Targets

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]**.

4.4.3. Implementation Notes and Implications

Implementers are strongly encouraged to use the Global Federated Identity and Privilege Management **[GFIPM]** security initiative for identity and authorization attributes. **[GFIPM]** utilizes X.509 certificates from the GFIPM Federation Trust File to perform Service Authentication and digital signature validation.

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

4.5. Message Non-Repudiation

4.5.1. Statement of Requirement from GRA

The **[GRA]** requires that each **SIP** define how information is provided in a message to allow the recipient to prove that a particular authorized sender in fact sent the message.

4.5.2. Conformance Targets

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 1.1]** Section 8, "XML-Signature."

4.5.3. Implementation Notes and Implications

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

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, "Extended Example."

4.6. Message Integrity

4.6.1. Statement of Requirement from GRA

The **[GRA]** requires that each **SIP** 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.

4.6.2. Conformance Targets

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 8, "XML-Signature."

4.6.3. Implementation Notes and Implications

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

4.7. Message Confidentiality

4.7.1. Statement of Requirement from GRA

The **[GRA]** requires that each **SIP** define how information is provided in a message to protect anyone except an authorized recipient from reading the message or parts of the message.

4.7.2. 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."

4.7.3. Implementation Notes and Implications

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

4.8. Message Addressing

4.8.1. Statement of Requirement from GRA

The **[GRA]** requires that each **SIP** 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.

4.8.2. Conformance Targets

Conformance with this Web Services SIP requires that every message SHOULD 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.

LEXS Messages can contain addressing information, and conformance to this **SIP** requires that these elements MUST duplicate the corresponding **[WS-ADDRESSING CORE]** information. Implementations may use either to determine origination/routing information, but are recommended to use **[WS-ADDRESSING CORE]**.

4.8.3. Implementation Notes and Implications

None.

4.9. Reliability

4.9.1. Statement of Requirement from GRA

The [GRA] requires that each SIP 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.

4.9.2. Conformance Targets

Conformance with this Web Services SIP recommends that [LEXS] message(s) SHOULD contain SOAP headers that conform to [WS-RELIABLEMESSAGING].

Conformance with this SIP recommends that the EXECUTION CONTEXT supporting the interaction include components that implement the RM-SOURCE and RM-DESTINATION components defined in the [WS-RELIABLEMESSAGING] standard.

4.9.3. Implementation Notes and Implications

[LEXS] support for Reliable Messaging requires support for Web Services Addressing.

The implementation of reliable messaging services is particularly important for LEXS doPublish operations, since no “response” is expected (one-way message exchange pattern).

4.10. Transaction Support

4.10.1. Statement of Requirement from GRA

The [GRA] requires that each SIP define how information is provided with messages to permit a sequence of messages to be treated as an atomic transaction by the recipient.

4.10.2. Conformance Targets

Each [LEXS] MESSAGE is independent; therefore LEXS does not require support for transactions.

4.11. Service Metadata Availability

4.11.1. Statement of Requirement from GRA

The [GRA] requires that each SIP 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.

4.11.2. Conformance Targets

[LEXS] supports metadata operations for obtaining service metadata in real time (e.g. getAvailability, getDataOwners). Implementations MUST use/implement these messages to transmit information about capabilities to relying parties. Implementations MAY also provide

information via **[WS-METADATAEXCHANGE]**, and if so, this information MUST match the information provided via the **[LEXS]** service metadata messages.

4.11.3. Implementation Notes and Implications

The **[LEXS]** program has talked about a tool (not written at the time of this document) to expose via **[WS-METADATAEXCHANGE]** **[LEXS]** service metadata operations. Please visit www.lexs.gov for more information.

5. Interface Description Requirements

5.1. Statement of Requirement From GRA

This section demonstrates how this profile meets the Service Interaction Requirements identified in the **[GRA]**. Interface description requirements establish common characteristics of service interface descriptions. These requirements address areas such as required interface contents, naming rules, documentation rules and specification of a standard structure and format for descriptions.

5.2. Conformance Targets

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 **[LEXS]** XML Schemas. Specifically:

- The referenced elements must come from the following namespaces as defined by **[LEXS]**:
  - http://usdoj.gov/leisp/lexs/publishdiscover/3.1
  - http://usdoj.gov/leisp/lexs/searchretrieve/3.1

5.3. Implementation Notes and Implications

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.

The **[LEXS]** specification includes template WSDL files as a convenience for developers in order to provide a starting point for **[LEXS]** WS implementations. **[LEXS]** does not mandate the use of these files, since some implementations do not use web services at all or do not use web services based on WS-* standards. The **[LEXS]** WS WSDL templates use an XML document-based information exchange, leaving the back-end implementation up to the developer.

The **[LEXS]** program also defines a "sample implementation" which provides a running sample application with pre-defined WSDL-first code samples. Copies can be found at www.lexs.gov.

Document/Literal wrapped style WSDL structure and **[LEXS]** schema constructs provide flexibility for platform choice.

The **[LEXS]** WS WSDL templates use the full **[LEXS]** message format schemas and provide a full set of core interfaces. Developers are allowed to modify the WSDL templates to address their specific functional requirements.

5.4. Policy

Implementers MUST implement **[WS-POLICY]** to be conformant with this **[LEXS]** **SIP**.

6. Message Exchange Patterns

This section discusses how the message exchange patterns (MEP) are supported by this profile.

6.1. One-Way Pattern

The one-way message exchange pattern corresponds to a one-way operation as defined in **[WSDL 1.1]**. This **SIP** supports this pattern by requiring that service consumers and service interfaces conform to **[WS-I BP 1.2]**. In particular section 4.7.8, "One-Way Operations" requires the HTTP response to a one-way operation indicates the success or failure of the transmission of the message. Many composite asynchronous message exchange patterns can be derived from this pattern.

[LEXS] uses one-way pattern for routing doPublish messages, which are "fire-and-forget" messages.

6.2. Request-Response Pattern

LEXS-SR is a request-response message exchange pattern and corresponds to a request-response operation as defined in [WSDL 1.1]. This SIP supports this pattern by requiring that service consumers and service interfaces conform to [WS-I BP 1.2].

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.

6.3. Faults

In [LEXS] application level faults will be found in the MESSAGE, the lexs:Advisory element in the lexs:ResponseMetadata. No other fault mechanism should be used, such as Base Faults.

7. 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 a single SOAP message (defined as the message conformance target in [WS-I BP 1.2]) that meets all requirements of this profile.

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 the [LEXS] XML Schema (as defined in [XML SCHEMA]) that defines the message structure. In addition, the root part must be an element as defined in the namespaces:

- http://usdoj.gov/leisp/lexs/publishdiscover/3.1
- http://usdoj.gov/leisp/lexs/searchretrieve/3.1

An [XML INFOSET] may utilize XML binary Optimized Packaging [XOP] and streamline the information exchange using the Message Transmission Optimization Method [MTOM]. Note that [LEXS] messages can support attachments by reference (xs:anyURI) via the lexs:AttachmentURI element, potentially eliminating the need for [XOP] or [MTOM] by providing richer message-level operations.

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