BJA

Bureau of Justice Assistance
U.S. Department of Justice

Federated Identity and Privilege Management

Web Services System-to-System Profile

Version 1.0

June 2012

Global
Information
Sharing Standard

Global Standards

Global's collection of normative standards has been versioned independently and assembled into a package of composable, interoperable solutions specifically supporting an information exchange. The package is known as the Global Standards Package (GSP). GSP solutions are generally technically focused but also may include associated guidelines and operating documents. GSP deliverables include artifacts associated with many of the Global product areas, including but not limited to:

- **Global Reference Architecture (GRA):** Offers guidance on the design, specification, and implementation of services (and related infrastructure) as part of a justice Service-Oriented Architecture (SOA).
- **Global Service Specification Packages (SSPs):** Reference services that serve as the means by which the information needs of a consumer are connected with the information capabilities of an information provider.
- **Global Federated Identity and Privilege Management (GFIPM):** Guidelines and standards for establishing, implementing, and governing federated identity management approaches.
- **Global Privacy Technology Framework:** A framework for automating access control (in particular, privacy) policy as part of information exchange.

For More Information

For more information on the GSP and the Global Standards Council (GSC)—the Global group responsible for developing, maintaining, and sustaining the same—please visit http://www.it.ojp.gov/gsc.

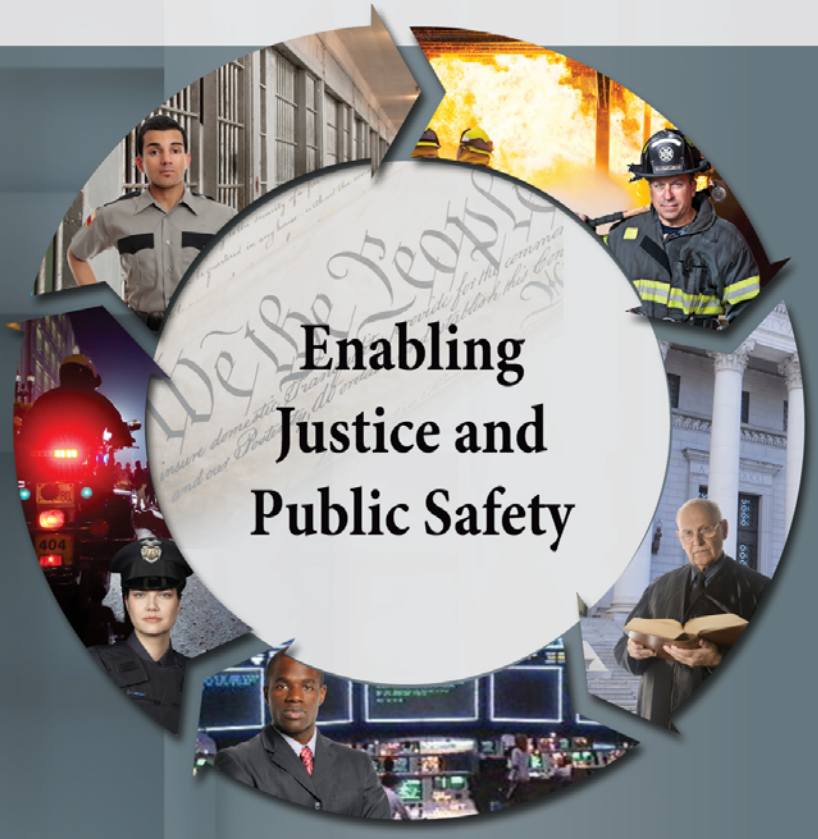

Table of Contents

Acknowledgements

The Global Federated Identity and Privilege Management (GFIPM) initiative was developed through a collaborative effort of the Global Justice Information Sharing Initiative (Global) membership; the U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA); and the U.S. Department of Homeland Security (DHS). The Global Standards Council (GSC) would like to express its appreciation to BJA and DHS for their continued guidance and support of this key initiative for secure and trusted information sharing among state, regional, local, tribal, and federal organizations. The GSC would also like to thank the GFIPM Delivery Team (DT), under the direction of Mr. John Ruegg, Los Angeles County Information Systems Advisory Body, for its dedication and commitment to developing this artifact and all other companion GFIPM artifacts. The creation of this document was guided by a volunteer effort of numerous contributors who participated by leveraging GFIPM standards within their state, regional, and federal organizations. Without their subject-matter expertise, ongoing experience, and feedback from lessons learned, the development of these guidelines would not have been possible.

1. Introduction

The objective of the Global Federated Identity and Privilege Management (GFIPM) standards and specifications is to provide a security framework for securely connecting justice and public safety personnel to interagency applications and data over the Internet. *Federation* is a fundamental concept within the GFIPM framework. The goal of a federation is to provide justice and public safety organizations with the following benefits:

- Provide single sign-on capabilities to end users for accessing online services.
- Eliminate the requirement to register user identity information in multiple external systems.
- Retain identity management and user authentication responsibility at the local organization level.
- Provide an interoperable standard vocabulary of identity access attributes.
- Support informed access and authorization decisions based on a trusted set of user identity attributes, thereby improving the security controls and scalability for justice and public safety electronic information sharing.

The federated approach to identity and privilege management provides a standards-based means for local, state, tribal, and federal entities to locally authenticate their organizations' users and provide accurate and current user identity attributes to external justice and public safety information systems which, in turn, utilize the trusted attributes to make authorization and system access decisions.

Formation of a federation represents a trust model that enables local, state, tribal, federal and other justice and public safety-related entities to access online services based on the federation **ATTRIBUTES** issued by trusted **IDENTITY PROVIDERS** (IDPs).

2. Background

Since 2005, the Global Federated Identity and Privilege Management (GFIPM) program has been developing information sharing solutions based on the concept of federated identity and privilege management. The Global Standards Council (GSC) has identified two primary uses cases that GFIPM must support: *user-to-system* and *system-to-system*. In the user-to-system use case, a user interacts with a Web application (system) via the Web browser across a GFIPM federation. In the *system-to-system* use case, Web service consumers and providers interact across a GFIPM federation. Note that even in the system-to-system use case, a user will typically interact with an application (system) that initiates a request for a Web service across the federation to another system on behalf of the user.

Initial work on the GFIPM project focused primarily on development of technical standards and prototype implementations for the Web browser-based, user-to-system use case. But since the start of the program, it has been clear that to be successful, GFIPM would also need to develop information sharing standards for a system-to-system, or "Web services," use case. Further, it is critical that the GFIPM system-to-system solution be compatible and interoperable with the GFIPM user-to-system solution.

To facilitate the development of the GFIPM system-to-system technical standards in a manner that included a wide variety of Global stakeholders, the GFIPM Delivery Team[1] created a GFIPM Web Services Tiger Team in early 2009. The purpose of the GFIPM-WS Tiger Team was to develop use cases and requirements to guide the development of technical standards for GFIPM Web services (GFIPM-WS). In June 2009, the GFIPM-WS Tiger Team completed a Concept of Operations (CONOPS) document [GFIPM-WS CONOPS] containing the results of its initial research into use cases and requirements for GFIPM Web services.

3. Target Audience and Purpose

This document specifies technical interoperability requirements for connection to an operational GFIPM federation in accordance with the Web Services System-to-System use case.[2] For the purpose of this document, all references to the concept of "joining" the federation are meant to imply connection to an operational GFIPM federation. The target audience includes technical representatives of prospective federation participants who intend to join a GFIPM federation as Identity Provider Organizations (IDPOs), Service Provider Organizations (SPOs), or both.[3] It also includes vendors, contractors, and consultants who, as part of their project or product implementation, have a requirement to establish technical interoperability with a GFIPM federation.

The GFIPM project plans to provide a free, open source federation middleware solution that conforms to this document, for both Web Service Consumers (WSCs) and Web Service Providers (WSPs). Participants may choose to use other commercial products in a GFIPM federation as long as they can be configured to conform to the interoperability requirements provided in this document.

This document focuses only on issues of technical interoperability. It does not cover governance, policy, or other nontechnical interoperability requirements. For more information about those topics, see [GFIPM Gov] and [GFIPM OPP].

[1] The GFIPM Delivery Team acts as the steering committee for the GFIPM project. It is under the direction of the Global Standards Council (GSC).

[2] The Web Services System-to-System use case, covered in this document, is one of two basic GFIPM use cases. The other is the Web Browser User-to-System use case, which is covered in [GFIPM U2S Profile].

[3] See [GFIPM Terms] for terminology related to various organizational and technical roles in GFIPM.

In addition, this document focuses only on SOAP Web services. It does not currently address REST[4] Web services.

4. Terminology

This document contains language that uses technical terms related to federations, identity management, Web services, and other related technologies. To minimize confusion for readers, it is important that each technical term have a precise definition. Accordingly, all technical terms in this document are to be interpreted as described in [GFIPM Terms].

5. References

Table 1 and Table 2 contain a list of documents that pertain to the specifications and requirements described in this document (including GFIPM domain-specific standards and industry standards).

Document References for GFIPM Domain-Specific Standards	
Document ID	**Document Name and URL**
GFIPM Terms	GFIPM Terminology Matrix 1.0 http://it.ojp.gov/docdownloader.aspx?ddid=1333
GFIPM Gov	GFIPM Governance Guideline 1.0 http://it.ojp.gov/docdownloader.aspx?ddid=1341
GFIPM OPP	GFIPM Operational Policies and Procedures Guideline 1.1 http://it.ojp.gov/docdownloader.aspx?ddid=1340
GFIPM Meta	GFIPM Metadata Specification 2.0 http://gfipm.net/standards/metadata/2.0/index.html
GFIPM Trust	GFIPM Cryptographic Trust Model 1.2 [URL TBD]
GFIPM CPS	GFIPM Certification Practice Statement Template 1.0 http://it.ojp.gov/docdownloader.aspx?ddid=1337
GFIPM Member CP	GFIPM Member Certificate Policy Template 1.0 [URL TBD]
GFIPM U2S Profile	GFIPM Web Browser User-to-System Profile 1.1 http://it.ojp.gov/docdownloader.aspx?ddid=1336
GFIPM S2S Profile	GFIPM Web Services System-to-System Profile 1.0 (This Doc) [URL TBD]
GFIPM-WS CONOPS	GFIPM Web Services Concept of Operations (CONOPS) 1.0 http://it.ojp.gov/docdownloader.aspx?ddid=1332

Table 1: Document References for GFIPM Domain-Specific Standards

[4] See http://en.wikipedia.org/wiki/Representational_State_Transfer for more information about REST Web services.

Document References for Industry Standards	
Document ID	**Document Name and URL**
FIPS 140-2	Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules* December 3, 2002 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
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 Reference Architecture Specification 1.9 April 2011 http://it.ojp.gov/globalgra
GRA RS WS-SIP	Global Reference Architecture Reliable Secure Web Services Service Interaction Profile 1.1 May 2011 http://it.ojp.gov/docdownloader.aspx?ddid=1134
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/
NIST SP 800-63	*NIST Special Publication 800-63,* Electronic Authentication Guideline, Version 1.0.2, April 2006 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
RFC 2119	Internet Engineering Task Force (IETF) Request for Comments (RFC) 2119, March 1997 http://www.ietf.org/rfc/rfc2119.txt
SAML2	Security Assertion Markup Language, Version 2.0 http://wiki.oasis-open.org/security
SAML2 Core	Assertions and Protocols for the OASIS Security Markup Language (SAML) Version 2.0. OASIS Standard, March 15, 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
SAML2 Delegation	SAML 2.0 Condition for Delegation Restriction, Version 1.0 OASIS Committee Specification 01, November 15, 2009 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-delegation-cs-01.html
SOAP	W3C SOAP Note, May 8, 2000 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, May 9, 2006 http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/

WS-Addr SOAP	Web Services Addressing SOAP Binding W3C Recommendation, May 9, 2006 http://www.w3.org/TR/2006/REC-ws-addr-soap-20060509/
WS-Addr WSDL	Web Services Addressing WSDL Binding W3C Candidate Recommendation, May 29, 2006 http://www.w3.org/TR/2006/CR-ws-addr-wsdl-20060529/
WS-AT	Web Services Atomic Transaction 1.2 OASIS Standard, February 2, 2009 http://docs.oasis-open.org/ws-tx/wsat/2006/06
WS-BA	OASIS Web Services Business Activity 1.2 February 2, 2009 http://docs.oasis-open.org/ws-tx/wsba/2006/06
WS-BF	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
WSDL	W3C Web Services Description Language 1.1 W3C Note, March 15, 2001 http://www.w3.org/TR/wsdl
WS-I BP	Web Services Interoperability Basic Profile 1.2 WS-I Working Group Standard, November 9, 2010 http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html
WS-I BSP	Web Services Interoperability Basic Security Profile 1.1 January 24, 2010 http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html
WS-Coordination	OASIS Web Services Coordination 1.2 February 2, 2009 http://docs.oasis-open.org/ws-tx/wscoor/2006/06
WS-MX	Web Services Metadata Exchange 1.1 W3C Member Submission, August 13, 2008 http://www.w3.org/Submission/WS-MetadataExchange/
WS-Notification	OASIS Web Services Notification http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn
WS-Policy	Web Services Policy Framework http://www.w3.org/2002/ws/policy/
WS-RM	OASIS Web Services Reliable Messaging 1.1 January 7, 2008 http://docs.oasis-open.org/ws-rx/wsrm/v1.1/wsrm.html
WS-SC	OASIS Web Services Secure Conversation 1.3 March 1, 2007 http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.3/ws-secureconversation.html
WS-Sec	OASIS Web Services Security: SOAP Message Security 1.1 OASIS Standard, February 1, 2006 http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

WS-Sec SAML	Web Services Security SAML Token Profile http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf
WS-SP	Web Services Security Policy Language http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/ws-securitypolicy.html
WS-Transfer	Web Services Transfer W3C Member Submission, January 7, 2008 http://www.w3.org/Submission/2006/SUBM-WS-Transfer-20060927/
WS-Trust	Web Services Trust Language http://www.ibm.com/developerworks/library/specification/ws-trust/
XML-Encryption	*XML Encryption Syntax and Processing* W3C Recommendation December 10, 2002 http://www.w3.org/TR/xmlenc-core/
XML Schema	XML Schema W3C Recommendation, August 12, 2004 http://www.w3.org/XML/Schema
XOP	W3C XML-Binary Optimized Packaging W3C Recommendation, January 25, 2005 http://www.w3.org/TR/xop10/
XML-Signature	*XML Signature Syntax and Processing (Second Edition)* W3C Recommendation February 12, 2002 http://www.w3.org/TR/xmldsig-core/

Table 2: Document References for Industry Standards

6. Notation for Normative Content

This document contains both normative and non-normative content. Sections containing normative content are marked appropriately. In those sections, the key words "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" are to be interpreted as described in [RFC 2119].

7. GFIPM Web Services Functional Requirements

The GFIPM-WS Tiger Team identified the following functional requirements for GFIPM Web services.[5,6] When interpreting these requirements, please note that an Authorization Service (AS) is treated as a special case of a Web Service Provider (WSP), and as such must conform to all the requirements of a WSP unless otherwise stated.

[5] These functional requirements originally appeared in [GFIPM-WS CONOPS] and have been reproduced in this document for the benefit of the reader.

[6] Functional requirement Number 5 in [GFIPM-WS CONOPS] ("Web Service User Consent and Logging of Attribute Release Events") has been removed from the list of functional requirements in this document because several reviewers of this document indicated that it introduced unnecessary ambiguity for implementers.

Although this section contains language written in a normative style, *the contents of this section do not constitute normative conformance targets for the purpose of this specification*. Sections 8 and 9 contain the actual normative language for the GFIPM Web Services SIPs.

1. ***GFIPM System Entity Metadata***—Every system entity that appears in the GFIPM Cryptographic Trust Fabric document MUST have a GFIPM Entity Assertion within that document. This includes every Identity Provider (IDP), Service Provider (SP), Web Service Consumer (WSC), Web Service Provider (WSP), Authorization Service (AS), and Trusted Identity Broker (TIB), or their respective Web services interfaces and/or endpoints.[7]

2. ***Message Sender Authentication***—For every message received, the receiving system MUST verify the identity of the sender of the message. Specifically, upon receipt of any message, the receiving system MUST attempt to verify that the sender is a member of the GFIPM Cryptographic Trust Fabric and MUST reject the message if it cannot verify that the sender is a member of the GFIPM Cryptographic Trust Fabric.

3. ***Web Service Consumer Authorization***—For every request message received by a WSP, the WSP MUST verify the authorization of the sender (WSC) to perform the requested action. If necessary, the WSP MAY refer to its local copy of the GFIPM Entity Assertion for the WSC to obtain necessary attributes about the WSC for the purpose of making an access control decision about the WSC's permission to perform the requested action. The WSP MAY also use information from the WSC's GFIPM Entity Assertion for other business purposes, including audit logging.

4. ***Web Service User Authorization***—For every request message sent by a WSC on behalf of a user, the WSC MUST provide a GFIPM User Assertion containing attribute information about that user. The GFIPM User Assertion MUST be signed by the user's IDP in a manner that allows the receiving system (WSP) to verify that the GFIPM User Assertion was generated by the user's IDP. Also, the GFIPM User Assertion MUST be encrypted by the sender using [XML-Encryption], so that only the receiving system can decrypt it.[8] If necessary, the WSP that receives the message MAY refer to the information within the user's GFIPM User Assertion for the purpose of making an access control decision about the user's permission to perform the requested action. The WSP MAY also

[7] Please refer to [GFIPM Terms] for detailed definitions of the system entities listed in this requirement.

[8] This requirement serves to ensure that all personally identifiable information (PII) about GFIPM users is protected while in transit within a GFIPM-WS message. Note that this requirement does NOT pertain to PII within a GFIPM-WS message payload. Protection of PII within GFIPM-WS message payloads is outside the scope of the GFIPM-WS specification.

use information from the user's GFIPM User Assertion for other business purposes, including audit logging.

5. ***Message Nonrepudiation and Integrity***—For every message received, it MUST be possible for the receiving system to prove (1) that the sender which claimed to have sent the message did actually send it, and (2) that the message was not altered since it left control of the sender. In addition, upon receipt of any message, the receiving system MUST attempt to verify that these two properties are true for the message and MUST reject the message if it cannot verify that these properties are true for the message.

6. ***Message Confidentiality***—Every message sent MUST be cryptographically protected from being read by any person or entity other than its intended receiving system, in a manner that conforms to the guidelines described in [FIPS 140-2].[9]

7. ***Message Addressing***—It MUST be possible for the sender of a message to provide message addressing information within the message to indicate: (1) where the message originated, (2) the ultimate destination of the message beyond physical endpoint, (3) a specific recipient to whom the message should be delivered (this includes sophisticated metadata designed specifically to support routing), and (4) a specific address or entity to which reply messages (if any) should be sent. Also, message recipients MUST honor any message addressing directives or instructions specified within messages.

8. ***Message Reliability***—It MUST be possible for a message sender to receive notification of the success or failure of a message transmission, and it MUST also be possible for a message sender and receiver to engage in an arrangement in which the sender requires that a group of messages sent with specific sequence-related rules either arrive as intended or fail as a group.

9. ***Transaction Support***—It MUST be possible for a message sender and receiver to engage in an arrangement in which a sequence of messages is to be treated as an atomic transaction by the receiving system.

10. ***Service Metadata Availability***—It MUST be possible for a WSP to provide an interface through which it makes available to WSCs metadata about the services that it offers.

[9] To meet this requirement, the GFIPM-WS specification will state that all messages MUST be encrypted at either the Web services layer (e.g., via [XML-Encryption]) or the link layer (e.g., via TLS).

11. ***Interface Description***—Each Web service (WSP) MUST meet all requirements of the *description* conformance target in [WS-I BP].

12. ***Session Support***—To accommodate efficiency concerns and other system architectural/design considerations, it MUST be possible to bind a WSC, a WSP, and, if necessary, a user to a session to avoid redundant processing over repeated transactions.

13. ***Security Token Service Support***—To accommodate efficiency concerns and other system architectural/design considerations, it MUST be possible for a participating organization to deploy systems in an architecture based on Security Token Services (STSes),[10] provided that all STSes act in roles that are permitted within GFIPM. STS roles that are permitted within GFIPM are Identity Provider, Attribute Service, and Authorization Service. See Appendix F of [GFIPM-WS CONOPS] for more detailed information about GFIPM requirements and rules related to the use of Security Token Services.[11]

8. Baseline Requirements for GRA Conformance

Each GFIPM Web Services Service Interaction Profile MUST conform to the Global Reference Architecture (GRA) Reliable Secure Web Services Service Interaction Profile [GRA RS WS-SIP]. This section provides normative baseline requirements to ensure conformance.

1. When using standards and profiles in Table 3, systems MUST use the version of the standard or profile as specified in the table.

Standard/Profile	Version/Date
WS-I Basic Profile ([WS-I BP])	1.2
WS-I Basic Security Profile ([WS-I BSP])	1.1
SOAP	1.1
Web Services Description Language (WSDL)	1.1
WS-Security ([WS-Sec])	1.1
WS-SecureConversation	1.3
XML Signature	2002-02-12
XML Encryption	2002-12-10
WS-Trust ([WS-Trust])	1.3
WS-Policy	1.2
WS-PolicyAttachment	1.2
WS-SecurityPolicy	1.2

[10] In an STS-based architecture, an organization's WSPs typically rely on one or more Security Token Services (STSes) to perform some amount of security-related processing on their behalf. Please refer to [WS-Trust] for more information about this type of architecture.

[11] [GFIPM-WS CONOPS] also permits an STS to act in the role of a Validation Service. However, this document does not address any Validation Service use cases.

WS-ReliableMessaging ([WS-RM])	1.1
WS-ReliableMessaging Policy	1.1
WS-MetadataExchange ([WS-MX])	1.1
WS-Notification ([WS-Notification])	1.3
WS-Coordination ([WS-Coordination])	1.2
WS-AtomicTransaction ([WS-AT])	1.2
WS-BusinessActivity ([WS-BA])	1.2
WS-BaseFaults ([WS-BF])	1.2
Security Assertion Markup Language ([SAML])	2.0
Web Services Security SAML Token Profile ([WS-Sec SAML])	1.1

Table 3: Required Version Numbers for GRA Reliable Secure Web Services SIP

2. The WSP MUST meet all of its functional requirements in a manner pursuant to the normative language stipulated for the *SERVICE INTERFACE* conformance target in [GRA RS WS-SIP].

3. The WSC MUST meet all of its functional requirements in a manner pursuant to the normative language stipulated for the *SERVICE CONSUMER* conformance target in [GRA RS WS-SIP].

4. Every message sent by the WSC or the WSP MUST meet all of its functional requirements in a manner pursuant to the normative language stipulated for the *MESSAGE* conformance target in [GRA RS WS-SIP].

9. GFIPM Web Services Service Interaction Profiles

Each GFIPM Web Services Service Interaction Profile (SIP) is derived from a GFIPM Federated Service Interaction Model (FSIM).[12,13] Table 4 summarizes the GFIPM Web Services SIPs based on the components and basic requirements supported by each one.[14] The remainder of this section describes each GFIPM Web Services SIP in detail, including its motivating use case (FSIM), normative conformance targets, and implementation notes.

[12] Seven (7) GFIPM FSIMs were originally defined in [GFIPM-WS CONOPS]. Two (2) additional FSIMs were identified after [GFIPM-WS CONOPS] was published; therefore, they are not included in it.

[13] One GFIPM FSIM that was defined in [GFIPM-WS CONOPS]—specifically, FSIM Number 6, which addresses Web services interaction with a Validation Service—is not covered in this document because the use case that it covers was deemed to be redundant by several reviewers of early drafts of this document.

[14] As Table 4 implies, it is possible to construct use cases for which no GFIPM Web Services SIP can support all the requirements. For example, there is no SIP that can support a use case that includes both an Authorization Service and a Trusted Identity Broker. Official GFIPM standards support for such use cases does not currently exist, but support could be provided via either or both of the following: (1) explicitly define new GFIPM Web Services SIPs to support new use cases as they are identified, and (2) define a set of guidelines about how to combine and/or compose multiple GFIPM Web Services SIPs to handle unsupported use cases.

Requirement (Support for…)	Consumer-Provider SIP	User-Consumer-Provider SIP	Consumer-Provider Session SIP	User-Consumer-Provider Session SIP	Authorization Service SIP	Trusted Identity Broker SIP	Consumer-Provider Multiuser Session SIP	SAML Assertion Delegate Service SIP
[GRA RS WS-SIP]	✔	✔	✔	✔	✔	✔	✔	✔
Web Service Consumers	✔	✔	✔	✔	✔	✔	✔	✔
Web Service Providers	✔	✔	✔	✔	✔	✔	✔	✔
Identity Providers/Users	✖	✔	✖	✔	✖	✔	✔	✔
Sessions	✖	✖	✔	✔	✖	✖	✔	✖
Authorization Services	✖	✖	✖	✖	✔	✖	✖	✖
Trusted Identity Brokers	✖	✖	✖	✖	✖	✔	✖	✔

Table 4: Summary of GFIPM Web Services SIPs

9.1 GFIPM-WS Consumer-Provider SIP

The GFIPM Web Services Consumer-Provider SIP provides a normative specification for implementing GFIPM FSIM Number 1. It is appropriate for use in a scenario in which a WSC connects to a WSP one time to access an application service, without acting directly on behalf of a user, without setting up a session for subsequent connections, and without using a Security Token Service (STS).

9.1.1 Motivating Use Case (Non-Normative)

This SIP derives its motivation from GFIPM FSIM Number 1, which represents the simplest Web service transaction. In this FSIM, a WSC initiates a one-time transaction with a WSP. It consists of the following steps:

1. The WSC sends an Application Service Request to the WSP.

2. The WSP processes the Application Service Request. In this step, the WSP authenticates the WSC via the WSC's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric. The WSP also may make an access control decision about the WSC based on information in the WSC's GFIPM Entity Assertion.

3. The WSP sends an Application Service Response to the WSC, if necessary.

4. If the WSP sent an Application Service Response, then the WSC processes the response. In this step, the WSC authenticates the WSP via the WSP's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric.

For any transaction that conforms to this use case, Steps 3 and 4 are optional. Figure 1 depicts FSIM Number 1.

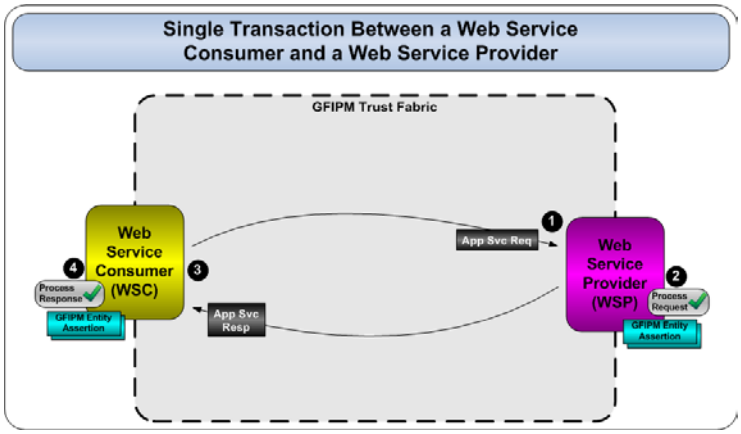

Figure 1: Diagram of Federation Service Interaction Model Number 1

9.1.2 Normative Conformance Requirements

This section contains the normative conformance requirements for this SIP.

1. The WSC and the WSP MUST each have an entry in the GFIPM Cryptographic Trust Fabric document.[15]

2. The entry in the GFIPM Cryptographic Trust Fabric document for the WSC MAY contain GFIPM Metadata entity attributes pertaining to that entity.[16]

3. The entry in the GFIPM Cryptographic Trust Fabric document for the WSP MAY contain GFIPM Metadata entity attributes pertaining to that entity.

4. The WSP MUST make its service interface(s) available via HTTPS (HTTP over TLS 1.x).[17]

[15] See [GFIPM Trust] for details about the format of the GFIPM Cryptographic Trust Fabric document.
[16] See [GFIPM Meta] for details on how to encode GFIPM Metadata entity attributes in the GFIPM Cryptographic Trust Fabric document.
[17] FIPS Publication 140-2 [FIPS 140-2] is a standards document that provides criteria used to accredit cryptographic modules for secure electronic communications. To facilitate the growth and success of a GFIPM federation, and to attract new members and new resources into the federation, it is in the best interests of all GFIPM federation members to understand [FIPS 140-2] and to know how it affects the policy decisions that are made within the federation. One such policy decision related to [FIPS 140-2] involves a GFIPM

5. The WSP MUST use one of its signing certificates from the GFIPM Cryptographic Trust Fabric document as the basis for establishment of encrypted TLS channels.

6. The WSP MAY require that connecting WSCs use TLS client certificate authentication (CCA) when connecting to it via TLS. If the WSP requires TLS CCA, then it MUST accept any of the WSC's signing certificates from the GFIPM Cryptographic Trust Fabric as the client certificate.[18]

7. The WSP MUST publish the following information about its service interface(s) in a WSDL document at a URL that is accessible to WSCs.

   a. Details about the application service interface(s) that are available.

   b. WS-Policy and WS-SecurityPolicy details about the security policy for the service interface(s).[19] Cryptographic aspects of the WSP's security policy MUST conform to [FIPS 140-2] where applicable.

   In addition, if the WSP's WSDL file specifies external import of any other documents, those documents MUST be at URLs that are accessible to WSCs.

8. When sending a request message to the WSP, the WSC MUST connect to the WSP via an encrypted TLS channel.

9. The WSC MUST verify that the certificate presented by the WSP during the TLS handshake process belongs to an entity in the federation's Cryptographic Trust Fabric document. The WSC MUST immediately terminate the TLS session and MUST NOT send its request message if this verification process fails.[20]

10. When sending a request message to the WSP, the WSC MUST include a creation timestamp in the manner prescribed in Section 10, "Security

---

federation's use of the TLS protocol for securing transactions within the federation. NIST has issued a document titled "Implementation Guidance for [FIPS 140-2] and the Cryptographic Module Validation Program," which provides supplementary information about FIPS PUB 140-2. Page 44 of this document states that for the purposes of FIPS 140-2 compliance, TLS version 1.0 or higher is an acceptable key establishment protocol, while SSL (all versions up to and including 3.0) is not acceptable. Therefore, in order to be FIPS 140-2 compliant, a GFIPM federation must use TLS.

[18] In practice, a WSP can accomplish this by preloading its TLS certificate store with all of the certificates from the federation's Cryptographic Trust Fabric document.

[19] Appendix C of this document provides sample WS-Policy and WS-SecurityPolicy language templates that WSPs can adopt for this SIP.

[20] In practice, a WSC can accomplish this by preloading its TLS certificate store with all of the certificates from the federation's Cryptographic Trust Fabric document.

Timestamps," of [WS-Sec]. In addition, the WSC MUST sign the following parts of the message with one of its signing certificates from the GFIPM Cryptographic Trust Fabric document, using [XML-Signature]. The message must meet all requirements of [WS-I BSP] Section 9, "XML-Signature."

a. SOAP Body and SOAP Attachments[21]

b. Timestamp

c. WS-Addressing Headers

11. When receiving a request message from the WSC, the WSP MUST perform the following verification tasks to authenticate the identity of the WSC.

    a. Verify that the following parts of the request message are properly signed by the WSC.

        i. SOAP Body and SOAP Attachments[22]

        ii. Timestamp

        iii. WS-Addressing Headers

    b. Verify that the certificate used to sign the request message belongs to an entity in the federation's GFIPM Cryptographic Trust Fabric document.

    If any of the verification tasks fails, the WSP MUST reject the request message.[23]

12. The WSP MAY enforce an access control policy for the purpose of protecting access to its application-level services. In its enforcement of the access control policy, the WSP MAY use the GFIPM Cryptographic Trust Fabric document to obtain entity attributes about the WSC sending the request, and the WSP MAY choose to deny access for any reason, including a scenario in which one or more of the entity attributes it attempted to obtain were not present.

[21] SOAP attachments need not be separately signed when using [MTOM].
[22] SOAP attachments need not be separately signed when using [MTOM].
[23] It may be advantageous for this spec to stipulate a particular protocol and/or a set of standard security error codes through which the WSP can communicate security failure events (e.g., authentication failure or access denial) to the WSC. Future versions of this spec may address this topic.

13. The WSP MAY send a response message to the WSC, but a response is not required.

14. When sending a response message to the WSC, the WSP MUST send via the same TLS channel that was established when the WSC originally sent the corresponding request message to the WSP[24].

15. When sending a response message to the WSC, the WSP MUST include a creation timestamp in the manner prescribed in Section 10, "Security Timestamps," of [WS-Sec]. In addition, the WSP MUST sign the following parts of the message with one of its signing certificates from the GFIPM Cryptographic Trust Fabric document, using [XML-Signature]. The message must meet all requirements of [WS-I BSP] Section 9, "XML-Signature."

    a. SOAP Body and SOAP Attachments[25]

    b. Timestamp

    c. WS-Addressing Headers

16. When receiving a response message from the WSP, the WSC MUST perform the following verification tasks:

    a. Verify that the following parts of the request message are properly signed by the WSP.

        i. SOAP Body and SOAP Attachments[26]

        ii. Timestamp

        iii. WS-Addressing Headers

    b. Verify that the certificate used to sign the request message belongs to the WSP to which the corresponding request message was sent.

If any of the verification tasks fails, the WSC MUST reject the response message.

17. For all messages sent as part of this conformance target, the message sender MAY use XML encryption on any or all parts of a message;

[24] This requirement implies that the WSP's TLS channel MUST be kept open throughout the duration of the WSP's processing of the request message.
[25] SOAP attachments need not be separately signed when using [MTOM].
[26] SOAP attachments need not be separately signed when using [MTOM].

however, XML encryption is NOT REQUIRED, since message confidentiality in transit is provided via a TLS channel. If XML encryption is used, both the encryption algorithm and its implementation MUST conform to Security Level 1 or higher as specified in [FIPS 140-2].[27] In addition, all encrypted parts of the message must meet the requirements associated with ENCRYPTED_DATA in [WS-I BSP] Section 10, "XML Encryption." Finally, if XML encryption is used on any part of a message, then the sender MUST encrypt using the ultimate message recipient's encryption certificate, and the ultimate message recipient MUST reject the message unless the message can be successfully decrypted using the private key associated with its encryption certificate.

9.1.3 Implementation Notes and Implications (Non-Normative)

Systems that conform to this SIP also conform to [GRA RS WS-SIP].

9.2 GFIPM-WS User-Consumer-Provider SIP

The GFIPM Web Services User-Consumer-Provider SIP provides a normative specification for implementing GFIPM FSIM Number 2. It is appropriate for use in a scenario in which a WSC connects to a WSP one time to access an application service, acting directly on behalf of a user, but without setting up a session for subsequent connections.

9.2.1 Motivating Use Case (Non-Normative)

This SIP derives its motivation from GFIPM FSIM Number 2, which introduces a user authentication event and GFIPM User Assertion into the Web services transaction. In this FSIM, the WSC is also a Web portal, and it performs a Web service transaction with a WSP on behalf of the user. FSIM Number 2 consists of the following steps.

1. The user authenticates with the IDP and sends a signed GFIPM User Assertion to the Web Portal / WSC.[28]

2. The Web Portal / WSC sends an Application Service Request to the WSP, passing the user's GFIPM User Assertion in the request header.

3. The WSP processes the Application Service Request. In this step, the WSP authenticates the WSC via the WSC's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric, and also authenticates the user via the

[27] FIPS PUB 140-2 states, "Security Level 1 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system."

[28] The details by which the user authenticates to the IDP and transmits a signed GFIPM User Assertion to the Web Portal are outside the scope of this service interaction model. In practice, this step may be performed using the GFIPM Web User-to-System Profile [GFIPM U2S Profile], but this is not required.

GFIPM User Assertion sent with the request. The WSP also may make an access control decision about the WSC and/or the user based on information in the WSC's GFIPM Entity Assertion and in the user's GFIPM User Assertion.

4. The WSP sends an Application Service Response to the Web Portal/WSC, if necessary.

5. If the WSP sent an Application Service Response, then the Web Portal/WSC processes the response. In this step, the WSC authenticates the WSP via the WSP's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric.

For any transaction that conforms to this use case, Steps 4 and 5 are optional. Figure 2 depicts FSIM Number 2.

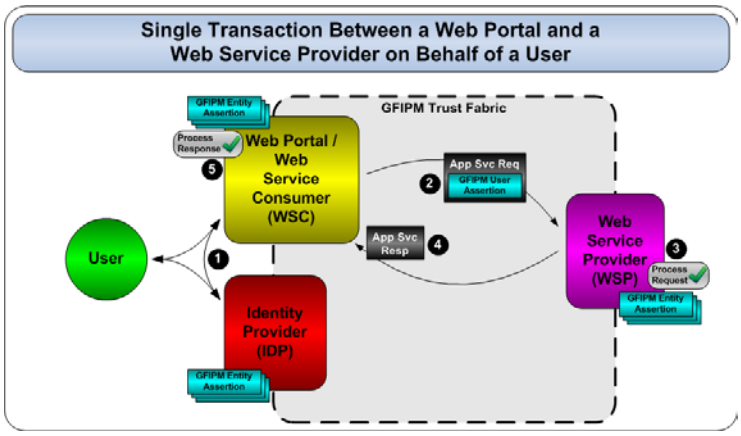

Figure 2: Diagram of Federation Service Interaction Model Number 2

9.2.2 Normative Conformance Requirements

This section contains the normative conformance requirements for this SIP.

1. The IDP, WSC, and WSP MUST each have an entry in the GFIPM Cryptographic Trust Fabric document.[29]

2. The entry in the GFIPM Cryptographic Trust Fabric document for the IDP MAY contain GFIPM Metadata entity attributes pertaining to that entity.[30]

[29] See [GFIPM Trust] for details about the format of the GFIPM Cryptographic Trust Fabric document.
[30] See [GFIPM Meta] for details on how to encode GFIPM Metadata entity attributes in the GFIPM Cryptographic Trust Fabric document.

3. The entry in the GFIPM Cryptographic Trust Fabric document for the WSC MAY contain GFIPM Metadata entity attributes pertaining to that entity.

4. The entry in the GFIPM Cryptographic Trust Fabric document for the WSP MAY contain GFIPM Metadata entity attributes pertaining to that entity.

5. The WSP MUST make its service interface(s) available via HTTPS (HTTP over TLS 1.x).

6. The WSP MUST use one of its signing certificates from the GFIPM Cryptographic Trust Fabric document as the basis for establishment of encrypted TLS channels.

7. The WSP MAY require that connecting WSCs use TLS client certificate authentication (CCA) when connecting to it via TLS. If the WSP requires TLS CCA, then it MUST accept any of the WSC's signing certificates from the GFIPM Cryptographic Trust Fabric as the client certificate.[31]

8. The WSP MUST publish the following information about its service interface(s) in a WSDL document at a URL that is accessible to WSCs.

   a. Details about the application service interface(s) that are available.

   b. WS-Policy and WS-SecurityPolicy details about the security policy for the service interface(s).[32] Cryptographic aspects of the WSP's security policy MUST conform to [FIPS 140-2] where applicable.

   In addition, if the WSP's WSDL file specifies external import of any other documents, those documents MUST be at URLs that are accessible to WSCs.

9. When sending a request message to the WSP, the WSC MUST connect to the WSP via an encrypted TLS channel.

10. The WSC MUST verify that the certificate presented by the WSP during the TLS handshake process belongs to an entity in the federation's Cryptographic Trust Fabric document. The WSC MUST immediately

[31] In practice, a WSP can accomplish this by preloading its TLS certificate store with all of the certificates from the federation's Cryptographic Trust Fabric document.

[32] Appendix C of this document provides sample WS-Policy and WS-SecurityPolicy language templates that WSPs can adopt for this SIP.

terminate the TLS session and MUST NOT send its request message if this verification process fails.[33]

11. Prior to sending a request message to the WSP on behalf of a user, the WSC MUST acquire a SAML assertion for the user from the user's IDP.[34] The format of the SAML assertion MUST conform to the rules described in [SAML2 Core], and MUST also conform to the GFIPM-specific SAML assertion format rules described in Appendix A.[35]

12. When sending a request message to the WSP, the WSC MUST include a creation timestamp in the manner prescribed in Section 10, "Security Timestamps," of [WS-Sec]. In addition, the WSC MUST encode the user's SAML assertion in the message's SOAP header using the rules described in the WS-Security SAML Token Profile [WS-Sec SAML]. In addition, the WSC MUST sign the following parts of the message with one of its signing certificates from the GFIPM Cryptographic Trust Fabric document, using [XML-Signature]. The message must meet all requirements of [WS-I BSP] Section 9, "XML-Signature."

    a. SOAP Body and SOAP Attachments[36]

    b. Timestamp

    c. WS-Addressing Headers

    d. WS-Security Token for User's SAML Assertion

13. When receiving a request message from the WSC, the WSP MUST perform the following verification tasks to authenticate the identity of the WSC.

    a. Verify that the following parts of the request message are properly signed by the WSC.

[33] In practice, a WSC can accomplish this by preloading its TLS certificate store with all of the certificates from the federation's Cryptographic Trust Fabric document.

[34] Details about how to acquire the SAML assertion from the IDP are beyond the scope of this SIP; however, in many implementations, the WSC may acquire an assertion from the IDP via the GFIPM SAML Assertion Delegate Service SIP. See Section 9.8 for more information.

[35] The GFIPM-specific format rules for SAML assertions are already described normatively in Section 6.3 of [GFIPM U2S Profile], but are repeated in Appendix A of this document for convenience.

[36] SOAP attachments need not be separately signed when using [MTOM].

i. SOAP Body and SOAP Attachments[37]

ii. Timestamp

iii. WS-Addressing Headers

iv. WS-Security Token for User's SAML Assertion

b. Verify that the certificate used to sign the request message belongs to an entity in the federation's GFIPM Cryptographic Trust Fabric document.

If any of the verification tasks fails, the WSP MUST reject the request message.

14. When receiving a request message from a WSC, the WSP MUST perform the following verification tasks to authenticate the user as a legitimate user within the federation.

    a. Verify that the SAML assertion in the request message is properly signed.

    b. Verify that the certificate used to sign the SAML assertion in the request message belongs to an IDP in the federation's GFIPM Cryptographic Trust Fabric document.

    c. Verify that the SAML assertion is valid according to the SAML processing rules, as defined in [SAML2 Core] and [WS-Sec SAML].

    If any of the verification tasks fails, the WSP MUST reject the request message.

15. The WSP MAY enforce an access control policy for the purpose of protecting access to its application-level services. In its enforcement of the access control policy, the WSP MAY use the GFIPM Cryptographic Trust Fabric document to obtain entity attributes about the WSC sending the request and MAY use the SAML assertion received in the request message to obtain user attributes about the user on whose behalf the request was made. The WSP MAY choose to deny access for any reason, including a scenario in which one or more of the entity attributes or user attributes it attempted to obtain were not present.

[37] SOAP attachments need not be separately signed when using [MTOM].

16. The WSP MAY send a response message to the WSC, but a response is not required.

17. When sending a response message to the WSC, the WSP MUST send the response via the same TLS channel that was established when the WSC originally sent the corresponding request message to the WSP[38].

18. When sending a response message to the WSC, the WSP MUST include a creation timestamp in the manner prescribed in Section 10, "Security Timestamps," of [WS-Sec]. In addition, the WSP MUST sign the following parts of the message with one of its signing certificates from the GFIPM Cryptographic Trust Fabric document, using [XML-Signature]. The message must meet all requirements of [WS-I BSP] Section 9, "XML-Signature."

    a. SOAP Body and SOAP Attachments[39]

    b. Timestamp

    c. WS-Addressing Headers

19. When receiving a response message from the WSP, the WSC MUST perform the following verification tasks.

    a. Verify that the following parts of the request message are properly signed by the WSP.

        i. SOAP Body and SOAP Attachments[40]

        ii. Timestamp

        iii. WS-Addressing Headers

    b. Verify that the certificate used to sign the request message belongs to the WSP to which the corresponding request message was sent.

    If any of the verification tasks fails, the WSC MUST reject the response message.

[38] This requirement implies that the WSP's TLS channel MUST be kept open throughout the duration of the WSP's processing of the request message.
[39] SOAP attachments need not be separately signed when using [MTOM].
[40] SOAP attachments need not be separately signed when using [MTOM].

20. For all messages sent as part of this conformance target, the message sender MAY use XML encryption on any or all parts of a message; however, XML encryption is NOT REQUIRED, since message confidentiality in transit is provided via a TLS channel. If XML encryption is used, both the encryption algorithm and its implementation MUST conform to Security Level 1 or higher as specified in [FIPS 140-2]. In addition, all encrypted parts of the message must meet the requirements associated with ENCRYPTED_DATA in [WS-I BSP] Section 10, "XML Encryption." Finally, if XML encryption is used on any part of a message, then the sender MUST encrypt using the ultimate message recipient's encryption certificate, and the ultimate message recipient MUST reject the message unless the message can be successfully decrypted using the private key associated with its encryption certificate.

9.2.3 Implementation Notes and Implications (Non-Normative)

Systems that conform to this SIP also conform to [GRA RS WS-SIP].

9.3 GFIPM-WS Consumer-Provider Session SIP

The GFIPM Web Services Consumer-Provider Session SIP provides a normative specification for implementing GFIPM FSIM Number 3. It is appropriate for use in a scenario in which a WSC connects to a WSP to set up a session and then uses that session during subsequent connections to access the WSP's application service. In this scenario, the WSC does not act directly on behalf of a user, and no Security Token Services (STSes) are used during the transaction.

9.3.1 Motivating Use Case (Non-Normative)

This SIP derives its motivation from GFIPM FSIM Number 3, which introduces the concept of a session into a series of Web services transactions. In this FSIM, rather than engaging in one transaction, the WSC and WSP establish a session between them and then use the session to perform multiple transactions. This FSIM would be used in a scenario in which the WSC and WSP need to engage in many transactions within a relatively short time span and wish to minimize the amount of overhead per transaction required for security processing. FSIM Number 3 consists of the following steps:

1. The WSC sends a Session Token Request to the WSP.

2. The WSP processes the Session Token Request. In this step, the WSP authenticates the WSC via the WSC's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric. The WSP also may make an access control decision about the WSC based on information in the WSC's GFIPM Entity Assertion.

3. The WSP sends a Session Response to the WSC. The Session Response contains a Session Token.

4. The WSC processes the Session Response. In this step, the WSC authenticates the WSP via the WSP's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric.

5. The WSC sends an Application Service Request to the WSP, passing the Session Token in the request header.

6. The WSP processes the Application Service Request. In this step, the WSP may take advantage of the Session Token included in the request to bypass the authentication and/or access control decision processes.

7. The WSP sends an Application Service Response to the WSC, if necessary.

8. If the WSP sent an Application Service Response, then the WSC processes the response. In this step, the WSC may take advantage of the Session Token included in the response to bypass the authentication process.

Steps 5–8 can be repeated as necessary using the same Session Token as long as it remains valid. Also, for any transaction that occurs within the session, Steps 7 and 8 are optional. Figure 3 depicts FSIM Number 3.

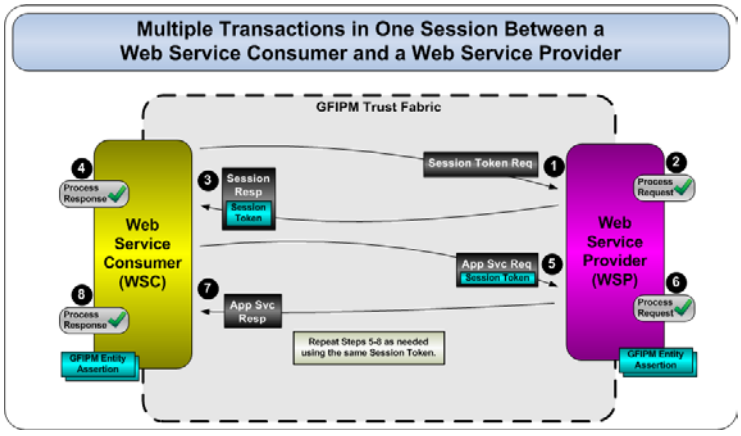

Figure 3: Diagram of Federation Service Interaction Model Number 3

9.3.2 Normative Conformance Requirements

Normative language for this SIP is planned for a future version of this document.

9.3.3 Implementation Notes and Implications (Non-Normative)

Systems that conform to this SIP also conform to [GRA RS WS-SIP].

9.4 GFIPM-WS User-Consumer-Provider Session SIP

The GFIPM Web Services User-Consumer-Provider Session SIP provides a normative specification for implementing GFIPM FSIM Number 4. It is appropriate for use in a scenario in which a WSC connects to a WSP to set up a session on behalf of a user and then uses that session during subsequent connections to access the WSP's application service on behalf of that same user. No Security Token Services (STSes) are used during the transaction.

9.4.1 Motivating Use Case (Non-Normative)

This SIP derives its motivation from GFIPM FSIM Number 4, which introduces a session into a series of Web services transactions. But unlike FSIM Number 3, in this FSIM the session is established on behalf of a WSC and a user. In this FSIM, the WSC is also a Web portal. As in FSIM Number 3, the WSC establishes a session with a WSP and performs multiple transactions using that session. But in this FSIM, the session between WSC and WSP is also bound to the user, thereby allowing the user to execute multiple transactions with the WSP via the Web Portal. FSIM Number 4 consists of the following steps:

1. The user authenticates with the IDP and sends a signed GFIPM User Assertion to the Web Portal / WSC.[41]

2. The WSC sends a Session Token Request to the WSP, passing the user's GFIPM User Assertion in the request header.

3. The WSP processes the Session Token Request. In this step, the WSP authenticates the WSC via the WSC's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric and also authenticates the user via the GFIPM User Assertion sent with the request. The WSP may also make an access control decision about the WSC and/or the user based on information in the WSC's GFIPM Entity Assertion and the in user's GFIPM User Assertion.

4. The WSP sends a Session Response to the Web Portal/WSC. The Session Response contains a Session Token that binds both the WSC and the user to the session.

[41] As in Federation Service Interaction Model Number 2, the details of this step are outside the scope of this model.

5. The WSC processes the Session Response. In this step, the WSC authenticates the WSP via the WSP's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric.
6. The WSC sends an Application Service Request to the WSP, passing the Session Token in the request header.

7. The WSP processes the Application Service Request. In this step, the WSP may take advantage of the Session Token included in the request to bypass the authentication and/or access control decision processes.

8. The WSP sends an Application Service Response to the WSC, if necessary.

9. If the WSP sent an Application Service Response, then the WSC processes the response. In this step, the WSC authenticates the WSP via the WSP's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric.

Steps 6–9 can be repeated as necessary using the same Session Token as long as it remains valid. Also, for any transaction that occurs within the session, Steps 8 and 9 are optional. Figure 4 depicts FSIM Number 4.

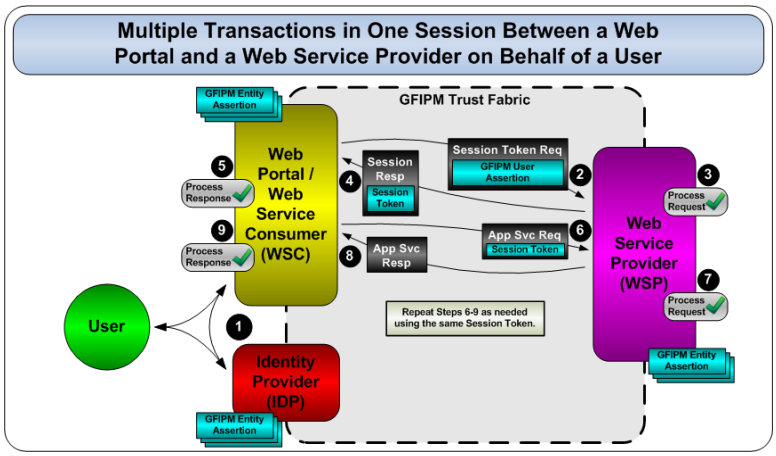

Figure 4: Diagram of Federation Service Interaction Model Number 4

9.4.2 Normative Conformance Requirements

Normative language for this SIP is planned for a future version of this document.

9.4.3 Implementation Notes and Implications (Non-Normative)

Systems that conform to this SIP also conform to [GRA RS WS-SIP].

9.5 GFIPM-WS Authorization Service SIP

The GFIPM Web Services Authorization Service SIP provides a normative specification for implementing GFIPM FSIM Number 5. It is appropriate for use in a scenario in which a WSC connects to a WSP that does not make its own access control decisions, but rather offloads that responsibility to a Security Token Service (STS) acting in the role of an Authorization Service (AS).

9.5.1 Motivating Use Case (Non-Normative)

This SIP derives its motivation from GFIPM FSIM Number 5, which addresses a scenario in which the WSP does not make its own access control decisions, and must be accessed via an Authorization Service (AS). FSIM Number 5 consists of the following steps:

1. The WSC sends an Authorization Token Request to the AS.

2. The AS processes the Authorization Token Request. In this step, the AS authenticates the WSC via the WSC's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric. The AS may also make an access control decision about the WSC based on information in the WSC's GFIPM Entity Assertion.

3. The AS sends an Authorization Token Response to the WSC. The Authorization Token Response contains an Authorization Token.

4. The WSC processes the Authorization Token Response. In this step, the WSC authenticates the AS via the AS's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric.

5. The WSC sends an Application Service Request to the WSP, passing the Authorization Token in the request header.

6. The WSP processes the Application Service Request. In this step, the WSP may take advantage of the Authorization Token included in the request to bypass the authentication and/or access control decision processes.

7. The WSP sends an Application Service Response to the WSC, if necessary.

8. If the WSP sent an Application Service Response, then the WSC processes the response. In this step, the WSC authenticates the WSP via the WSP's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric.

For any transaction that conforms to this use case, Steps 7 and 8 are optional. Figure 5 depicts FSIM Number 5.

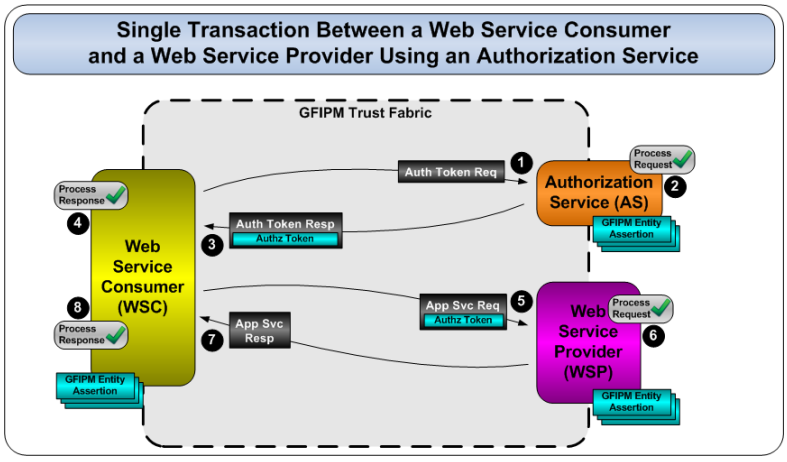

Figure 5: Diagram of Federation Service Interaction Model Number 5

9.5.2 Normative Conformance Requirements

Normative language for this SIP is planned for a future version of this document.

9.5.3 Implementation Notes and Implications (Non-Normative)

Systems that conform to this SIP also conform to [GRA RS WS-SIP].

9.6 GFIPM-WS Trusted Identity Broker SIP

The GFIPM Web Services Secure Trusted Identity Broker SIP provides a normative specification for implementing GFIPM FSIM Number 7. It is appropriate for use in a scenario in which a WSC connects to a WSP one time to access an application service, acting directly on behalf of a user, but without setting up a session for subsequent connections. This SIP is very similar to the GFIPM Web Services Secure User-Consumer-Provider SIP (see Section 9.2), with one difference: this SIP includes a Trusted Identity Broker (TIB) rather than an IDP.

9.6.1 Motivating Use Case (Non-Normative)

This SIP derives its motivation from GFIPM FSIM Number 7, which addresses a scenario in which trust must be brokered for an IDP that is outside the GFIPM Cryptographic Trust Fabric. The only type of entity that can broker trust for an IDP is a Trusted Identity Broker (TIB). The practical purpose of this FSIM is to address use cases in which a non-GFIPM user (i.e., a user from an IDP that is not in the GFIPM Cryptographic Trust Fabric) wants to gain access to GFIPM resources. FSIM Number 7 consists of the following steps:

1. The user authenticates with the IDP and/or the TIB, has a GFIPM User Assertion signed by the TIB, and sends the GFIPM User Assertion to the Web Portal / WSC.[42]

2. The Web Portal / WSC sends an Application Service Request to the WSP, passing the user's GFIPM User Assertion in the request header.

3. The WSP processes the Application Service Request. In this step, the WSP authenticates the WSC via the WSC's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric and also authenticates the user via the GFIPM User Assertion sent with the request. The WSP also may make an access control decision about the WSC and/or the user based on information in the WSC's GFIPM Entity Assertion and in the user's GFIPM User Assertion.

4. The WSP sends an Application Service Response to the Web Portal/WSC, if necessary.

5. If the WSP sent an Application Service Response, then the Web Portal/WSC processes the response. In this step, the WSC authenticates the WSP via the WSP's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric.

For any transaction that conforms to this use case, Steps 4 and 5 are optional. Figure 6 depicts FSIM Number 7.

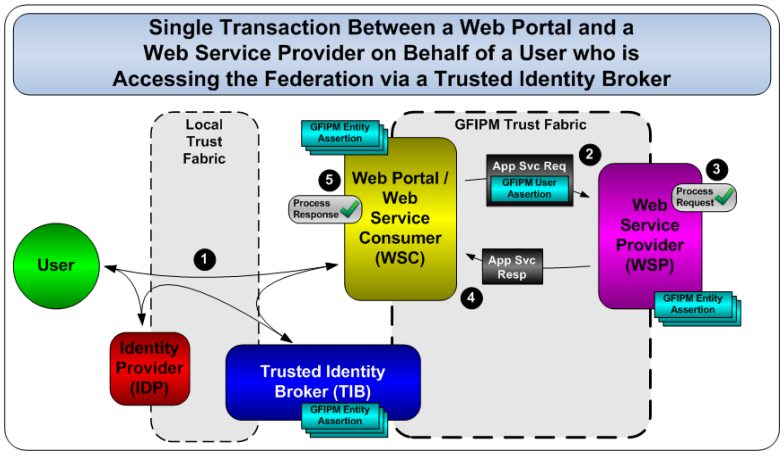

Figure 6: Diagram of Federation Service Interaction Model Number 7

[42] The details of this step are outside the scope of GFIPM Web services. Also, note that while the set of connected arrows in Figure 6 may seem confusing, they are merely intended to indicate that in Step 1, the user somehow communicates with the IDP, TIB, and Web Portal / WSC for the purpose of (1) authenticating with the TIB and/or the IDP, (2) acquiring a signed GFIPM User Assertion, and (3) transmitting the GFIPM User Assertion to the Web Portal / WSC.

9.6.2 Normative Conformance Requirements

This section contains the normative conformance requirements for this SIP.

1. The TIB, WSC, and WSP MUST each have an entry in the GFIPM Cryptographic Trust Fabric document.[43]

2. The entry in the GFIPM Cryptographic Trust Fabric document for the TIB MAY contain GFIPM Metadata entity attributes pertaining to that entity.[44]

3. The entry in the GFIPM Cryptographic Trust Fabric document for the WSC MAY contain GFIPM Metadata entity attributes pertaining to that entity.

4. The entry in the GFIPM Cryptographic Trust Fabric document for the WSP MAY contain GFIPM Metadata entity attributes pertaining to that entity.

5. The WSP MUST make its service interface(s) available via HTTPS (HTTP over TLS 1.x).

6. The WSP MUST use one of its signing certificates from the GFIPM Cryptographic Trust Fabric document as the basis for establishment of encrypted TLS channels.

7. The WSP MAY require that connecting WSCs use TLS client certificate authentication (CCA) when connecting to it via TLS. If the WSP requires TLS CCA, then it MUST accept any of the WSC's signing certificates from the GFIPM Cryptographic Trust Fabric as the client certificate.[45]

8. The WSP MUST publish the following information about its service interface(s) in a WSDL document at a URL that is accessible to WSCs.

    a. Details about the application service interface(s) that are available.

    b. WS-Policy and WS-SecurityPolicy details about the security policy for the service interface(s).[46] Cryptographic aspects of the WSP's security policy MUST conform to [FIPS 140-2] where applicable.

[43] See [GFIPM Trust] for details about the format of the GFIPM Cryptographic Trust Fabric document.
[44] See [GFIPM Meta] for details on how to encode GFIPM Metadata entity attributes in the GFIPM Cryptographic Trust Fabric document.
[45] In practice, a WSP can accomplish this by preloading its TLS certificate store with all of the certificates from the federation's Cryptographic Trust Fabric document.
[46] Appendix C of this document provides sample WS-Policy and WS-SecurityPolicy language templates that WSPs can adopt for this SIP.

In addition, if the WSP's WSDL file specifies external import of any other documents, those documents MUST be at URLs that are accessible to WSCs.

9. When sending a request message to the WSP, the WSC MUST connect to the WSP via an encrypted TLS channel.

10. The WSC MUST verify that the certificate presented by the WSP during the TLS handshake process belongs to an entity in the federation's Cryptographic Trust Fabric document. The WSC MUST immediately terminate the TLS session and MUST NOT send its request message if this verification process fails.[47]

11. Prior to sending a request message to the WSP on behalf of a user, the WSC MUST acquire a SAML assertion for the user from the user's TIB.[48] The format of the SAML assertion MUST conform to the rules described in [SAML2 Core] and MUST also conform to the GFIPM-specific SAML assertion format rules described in Appendix A.

12. When sending a request message to the WSP, the WSC MUST include a creation timestamp in the manner prescribed in Section 10, "Security Timestamps," of [WS-Sec]. In addition, the WSC MUST encode the user's SAML assertion in the message's SOAP header using the rules described in the WS-Security SAML Token Profile [WS-Sec SAML]. In addition, the WSC MUST sign the following parts of the message with one of its signing certificates from the GFIPM Cryptographic Trust Fabric document, using [XML-Signature]. The message must meet all requirements of [WS-I BSP] Section 9, "XML-Signature."

    a. SOAP Body and SOAP Attachments[49]

    b. Timestamp

    c. WS-Addressing Headers

    d. WS-Security Token for User's SAML Assertion

[47] In practice, a WSC can accomplish this by preloading its TLS certificate store with all of the certificates from the federation's Cryptographic Trust Fabric document.

[48] Details about how to acquire the SAML assertion from the TIB are outside the scope of this SIP; however, in many implementations, the WSC may acquire an assertion from the TIB via the GFIPM SAML Assertion Delegate Service SIP. See Section 9.8 for more information.

[49] SOAP attachments need not be separately signed when using [MTOM].

13. When receiving a request message from the WSC, the WSP MUST perform the following verification tasks to authenticate the identity of the WSC.

    a. Verify that the following parts of the request message are properly signed by the WSC.

        i. SOAP Body and SOAP Attachments[50]

        ii. Timestamp

        iii. WS-Addressing Headers

        iv. WS-Security Token for User's SAML Assertion

    b. Verify that the certificate used to sign the request message belongs to an entity in the federation's GFIPM Cryptographic Trust Fabric document.

    If any of the verification tasks fails, the WSP MUST reject the request message.

14. When receiving a request message from a WSC, the WSP MUST perform the following verification tasks to authenticate the user as a legitimate user within the federation.

    a. Verify that the SAML assertion in the request message is properly signed.

    b. Verify that the certificate used to sign the SAML assertion in the request message belongs to a TIB in the federation's GFIPM Cryptographic Trust Fabric document.

    c. Verify that the SAML assertion is valid according to the SAML processing rules, as defined in [SAML2 Core] and [WS-Sec SAML].

    If any of the verification tasks fails, the WSP MUST reject the request message.

15. The WSP MAY enforce an access control policy for the purpose of protecting access to its application-level services. In its enforcement of the access control policy, the WSP MAY use the GFIPM Cryptographic Trust Fabric document to obtain entity attributes about the WSC sending the

[50] SOAP attachments need not be separately signed when using [MTOM].

request and MAY use the SAML assertion received in the request message to obtain user attributes about the user on whose behalf the request was made. The WSP MAY choose to deny access for any reason, including a scenario in which one or more of the entity attributes or user attributes it attempted to obtain were not present.

16. The WSP MAY send a response message to the WSC, but a response is not required.

17. When sending a response message to the WSC, the WSP MUST send the response via the same TLS channel that was established when the WSC originally sent the corresponding request message to the WSP[51].

18. When sending a response message to the WSC, the WSP MUST include a creation timestamp in the manner prescribed in Section 10, "Security Timestamps," of [WS-Sec]. In addition, the WSP MUST sign the following parts of the message with one of its signing certificates from the GFIPM Cryptographic Trust Fabric document, using [XML-Signature]. The message must meet all requirements of [WS-I BSP] Section 9, "XML-Signature."

    a. SOAP Body and SOAP Attachments[52]

    b. Timestamp

    c. WS-Addressing Headers

19. When receiving a response message from the WSP, the WSC MUST perform the following verification tasks:

    a. Verify that the following parts of the request message are properly signed by the WSP.

        i. SOAP Body and SOAP Attachments[53]

        ii. Timestamp

        iii. WS-Addressing Headers

[51] This requirement implies that the WSP's TLS channel MUST be kept open throughout the duration of the WSP's processing of the request message.
[52] SOAP attachments need not be separately signed when using [MTOM].
[53] SOAP attachments need not be separately signed when using [MTOM].

b. Verify that the certificate used to sign the request message belongs to the WSP to which the corresponding request message was sent.

If any of the verification tasks fails, the WSC MUST reject the response message.

20. For all messages sent as part of this conformance target, the message sender MAY use XML encryption on any or all parts of a message; however, XML encryption is NOT REQUIRED, since message confidentiality in transit is provided via a TLS channel. If XML encryption is used, both the encryption algorithm and its implementation MUST conform to Security Level 1 or higher as specified in [FIPS 140-2]. In addition, all encrypted parts of the message must meet the requirements associated with ENCRYPTED_DATA in [WS-I BSP] Section 10, "XML Encryption." Finally, if XML encryption is used on any part of a message, then the sender MUST encrypt using the ultimate message recipient's encryption certificate, and the ultimate message recipient MUST reject the message unless the message can be successfully decrypted using the private key associated with its encryption certificate.

9.6.3 Implementation Notes and Implications (Non-Normative)

Systems that conform to this SIP also conform to [GRA RS WS-SIP].

9.7 GFIPM-WS Consumer-Provider Multiuser Session SIP

The GFIPM Web Services Consumer-Provider Multiuser Session SIP provides a normative specification for implementing GFIPM FSIM Number 8. It is appropriate for use in a scenario in which a WSC connects to a WSP to set up a session and then uses that session during subsequent connections to access the WSP's application service on behalf of multiple users. No Security Token Services (STSes) are used during the transaction.

9.7.1 Motivating Use Case (Non-Normative)

This SIP derives its motivation from GFIPM FSIM Number 8, which introduces a session into a series of Web services transactions and uses that session to execute transactions on behalf of multiple users within the same session. In this FSIM, the WSC is also a Web portal. FSIM Number 8 consists of the following steps.

1. The Web Portal/WSC sends a Session Token Request to the WSP.

2. The WSP processes the Session Token Request. In this step, the WSP authenticates the Web Portal/WSC via the Web Portal's/WSC's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric. The WSP may

also make an access control decision about the Web Portal/WSC based on information in the Web Portal's/WSC's GFIPM Entity Assertion.

3. The WSP sends a Session Response to the Web Portal/WSC. The Session Response contains a Session Token.

4. The Web Portal/WSC processes the Session Response. In this step, the Web Portal/WSC authenticates the WSP via the WSP's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric.

5. A user authenticates with the IDP and sends a signed GFIPM User Assertion to the Web Portal/WSC.[54]

6. The WSC sends an Application Service Request to the WSP, passing the Session Token and the user's GFIPM User Assertion in the request header.

7. The WSP processes the Application Service Request. In this step, the WSP authenticates the user via the GFIPM User Assertion sent with the request. The WSP may make an access control decision about the WSC and/or the user based on information in the WSC's GFIPM Entity Assertion and in the user's GFIPM User Assertion. The WSP may take advantage of the Session Token included in the request to bypass the authentication and/or access control decision processes for the WSC/Web Portal.

8. The WSP sends an Application Service Response to the WSC, if necessary.

9. If the WSP sent an Application Service Response, then the WSC processes the response. In this step, the WSC authenticates the WSP via the WSP's GFIPM Entity Assertion in the GFIPM Cryptographic Trust Fabric.

Steps 5–9 can be repeated as necessary for any number of users using the same Session Token as long as it remains valid. Also, for any transaction that occurs within the session, Steps 8 and 9 are optional. Figure 7 depicts FSIM Number 8.

[54] The details of this step are outside the scope of this model.

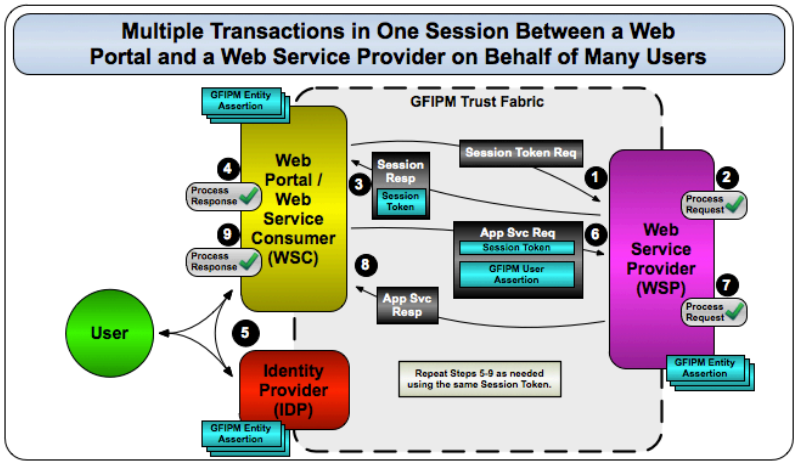

Figure 7: Diagram of Federation Service Interaction Model Number 8

9.7.2 Normative Conformance Requirements

Normative language for this SIP is planned for a future version of this document.

9.7.3 Implementation Notes and Implications (Non-Normative)

Systems that conform to this SIP also conform to [GRA RS WS-SIP].

9.8 GFIPM-WS SAML Assertion Delegate Service SIP

The GFIPM Web Services SAML Assertion Delegate Service SIP provides a normative specification for implementing an exchange between a WSC and an Assertion Delegate Service (ADS). The purpose of this exchange is for the WSC to acquire a delegated SAML assertion that is appropriate for use in a subsequent Web services transaction that it will perform on behalf of a user. This SIP is intended for use in conjunction with either the GFIPM Web Services User-Consumer-Provider SIP (see Section 9.2) or the GFIPM Web Services Trusted Identity Broker SIP (see Section 9.6).

9.8.1 Motivating Use Case (Non-Normative)

This SIP does not derive its motivation from any service interaction models defined in [GFIPM-WS CONOPS]. It is motivated by the need for a WSC to acquire a SAML assertion that will allow it to perform a transaction on behalf of a user. The SAML spec ([SAML2 Core]) rigorously defines a set of rules that the recipient of a SAML assertion must obey when processing the assertion and deciding whether to trust the information it conveys. These rules prohibit the practice of reusing, or "forwarding," a SAML assertion through multiple hops from one Web service to another as part of a transaction performed on behalf of a user. Performing Web services transactions in a GFIPM federation therefore requires the use of an auxiliary STS that operates as part of an IDP. This STS, which is called an Assertion Delegate Service (ADS), enables a WSC to exchange one SAML assertion for

another, such that the new "delegated" assertion allows the WSC to act on behalf of a user when communicating with a specified WSP.

This SIP assumes that a WSC already possesses a SAML assertion for a user and needs to exchange the assertion for a new SAML assertion for the same user. The WSC could have received the original SAML assertion in one of two ways.

1. The WSC is also a SAML service provider (SP) and received the original SAML assertion as part of a SAML single sign-on (SSO) transaction.[55]

2. The WSC is also a WSP and received the original assertion as part of a previous Web services request from another WSC.[56]

In either case, the WSC needs to make a request on behalf of the user but cannot do so using the SAML assertion it currently possesses because the assertion it possesses may have any or all of the following problems:

1. The assertion may not contain the correct target audience.

2. The assertion may not contain the correct SAML subject confirmation data.

3. The assertion may have expired.

4. The assertion does not contain information about the chain of delegates through which it has passed since the IDP originally generated it.

This SIP effectively allows the WSC to contact the IDP that generated the assertion and request a new assertion that is suited to the WSC's needs. In this SIP, the ADS is effectively an STS acting in the role of an Identity Provider, which is one of the STS roles allowed per [GFIPM Terms].

9.8.2 Normative Conformance Requirements

This section contains the normative conformance requirements for this SIP.

1. The IDP MUST expose an Assertion Delegate Service (ADS) as a Web service endpoint in the federation.

[55] A normative specification for performing SAML SSO transactions in GFIPM is in [GFIPM U2S Profile].
[56] In this case, the WSC that sent the original assertion to this WSC would have used this SIP to acquire it from an ADS prior to sending it.

2. During all transactions with the ADS, the WSC and ADS MUST conform to the GFIPM Web Services Consumer-Provider SIP (see Section 9.1), with the ADS acting as a WSP.

3. The ADS MUST conform to [WS-Trust] and MUST publish a WS-Trust-conformant WSDL document describing its interface.

4. When sending a single-token request to the ADS, the WSC MUST send a message that conforms to [WS-Trust]. The request message body MUST be formatted as follows:

    a. The message body MUST contain a **<wst:RequestSecurityToken>** element.

    b. The **<wst:RequestSecurityToken>** element MUST contain a **<wst:RequestType>** element with a value of **http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue**.

    c. The **<wst:RequestSecurityToken>** element MUST contain a **<wst:TokenType>** element with a value of **http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0**.

    d. The **<wst:RequestSecurityToken>** element MUST contain a **<wst:OnBehalfOf>** element, which MUST contain the SAML assertion that the WSC wishes to present to the ADS.

    e. The **<wst:RequestSecurityToken>** element MUST contain a **<wsp:AppliesTo>** element, which MUST contain a WS-Addressing **<wsa:EndpointReference>** element that identifies the WSP to which the WSC wishes to send the delegated assertion after receiving it from the ADS.

Figure 8 depicts the request message structure described above.

```
<wst:RequestSecurityToken>
  <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
  <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
  <wst:OnBehalfOf>
    <saml:Assertion>
      ... Orignal Assertion Content ...
    </saml:Assertion>
  </wst:OnBehalfOf>
  <wsp:AppliesTo>
    <wsa:EndpointReference>
      <wsa:Address>NIEF:WSP:XYZ123</wsa:Address>
    </wsa:EndpointReference>
  </wsp:AppliesTo>
</wst:RequestSecurityToken>
```

Figure 8: Structure of a Single-Token Request from WSC to ADS

5. When receiving a single-token request from a WSC, the ADS MUST perform the following verification tasks:

    a. Verify that the following properties are true for the SAML assertion presented by the WSC within the **<wst:OnBehalfOf>** element.

        i. The WSC is a member of the assertion's audience, as indicated by its **<AudienceRestriction>** and **<Audience>** elements.

        ii. The **<Issuer>** element identifies the IDP associated with this ADS.

        iii. The digital signature is valid.

        iv. The IDP associated with this ADS was the signer of the assertion.

        v. The timestamp indicated by the **"AuthnInstant"** attribute of the **<AuthnStatement>** element does not represent a time that is more than N seconds in the past, where N represents the maximum assertion age allowed by the ADS.[57]

    b. Verify that the intended recipient of the requested (delegated) SAML assertion, as indicated by the **<wsp:AppliesTo>** element within the

[57] An ADS MAY define any maximum assertion age, but it SHOULD use a value that limits the assertion reissuance window to a reasonable amont of time after the assertion was originally issued. It is RECOMMENDED that an ADS choose a value of no more than 10,800 seconds, or 3 hours.

request message, has an entry in the GFIPM Cryptographic Trust Fabric document.

If any of these verification tasks fails, the ADS MUST reject the request.

6. If all the verification tasks in the preceding step are successful, the ADS MUST construct a new SAML assertion by applying the following transformations to the SAML assertion presented by the WSC:

   a. Modify the **<AudienceRestriction>** element to contain exactly one **<Audience>** element, which contains the SAML 2.0 Metadata Entity ID that appears in the GFIPM Cryptographic Trust Fabric document for the intended recipient for the new assertion.

   b. Remove the **<SubjectConfirmationData>** element, if it is present.

   c. Modify the "Method" attribute of the **<SubjectConfirmation>** element so that **"urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"** is its value.

   d. Within the **<Conditions>** element of the assertion, add a new **<Delegate>** element. Within the new **<Delegate>** element, add a **<NameID>** element with a value equal to the SAML 2.0 Metadata Entity ID that appears in the GFIPM Cryptographic Trust Fabric document for the WSC that requested the assertion.[58,59] Also, on the new **<Delegate>** element, add a **"DelegationInstant"** attribute containing a timestamp representing the current moment in time.

   e. Modify the **"NotBefore"** attribute of the **<Conditions>** element to contain a timestamp representing the current moment in time.

   f. Modify the **"NotOnOrAfter"** attribute of the **<Conditions>** element to contain a timestamp representing a moment in time that is N seconds in the future, where N represents length of time, in seconds, for which the new assertion will be valid.[60]

[58] The insertion of **<Delegate>** elements into a delegated SAML assertion makes the ADS conformant with [SAML2 Delegation].

[59] It is possible, through a chain of SAML assertion delegations, for multiple <Delegate> elements to appear inside a <Conditions> element. When adding a new <Delegate> element, the ADS MUST NOT delete or modify any previously existing <Delegate> elements that already appear in the assertion.

[60] The ADS MAY use any value for the assertion validity period; however, it is RECOMMENDED that the ADS use a value that is reasonably small, so as to limit the validity period to no more than would be required for a relying party to receive and process the assertion. A value of 300 seconds (5 minutes) is reasonable under most circumstances.

g. Remove the old digital signature from the assertion, and replace it with a new digital signature. When generating this new signature, the ADS MUST use the private key that corresponds to the signing certificate for the ADS's IDP, as indicated in the GFIPM Cryptographic Trust Fabric document.

7. If the ADS was unable to construct a new SAML assertion because of a processing error, it MAY respond to the WSC using an appropriate WS-Trust error code.

8. If the ADS was able to construct a new SAML assertion, then it MUST send the new assertion to the WSC in a response message that conforms to [WS-Trust]. When responding to a single-token request, the response message body MUST be formatted as follows:

   a. The message body MUST contain a **<wst:RequestSecurityTokenResponse>** element.

   b. The **<wst:RequestSecurityTokenResponse>** element MUST contain a **<wst:RequestType>** element with a value of **http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue**.

   c. The **<wst:RequestSecurityTokenResponse>** element MUST contain a **<wst:TokenType>** element with a value of **http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0**.

   d. The **<wst:RequestSecurityTokenResponse>** element MUST contain a **<wsp:AppliesTo>** element, which MUST contain a WS-Addressing **<wsa:EndpointReference>** element that identifies the WSP to which the WSC wishes to send the delegated assertion after receiving it from the ADS.

   e. The **<wst:RequestSecurityTokenResponse>** element MUST contain a **<wst:RequestedSecurityToken>** element, which MUST contain the new SAML assertion constructed by the ADS.

Figure 9 depicts the response message structure described above.

```
<wst:RequestSecurityTokenResponse>
  <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
  <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
<wsp:AppliesTo>
   <wsa:EndpointReference>
     <wsa:Address>NIEF:WSP:XYZ123</wsa:Address>
   </wsa:EndpointReference>
  </wsp:AppliesTo>
  <wst:RequestedSecurityToken>
   <saml:Assertion>
     ... New Assertion Content ...
   </saml:Assertion>
  </wst:RequestedSecurityToken>
</wst:RequestSecurityTokenResponse>
```

Figure 9: Structure of a Single-Token Request Response from ADS to WSC

9. In addition to supporting single-token requests and processing them as described above, the ADS also MAY provide support for processing multitoken requests, which are defined in [WS-Trust] and allow a token requestor (WSC) to request multiple tokens (delegated SAML assertions) using a single request message. When processing a multitoken request, the ADS MUST obey the request processing rules defined in this section for each request in the message. Sample multitoken request and response messages are depicted in Figure 10 and Figure 11, respectively.

```
<wst:RequestSecurityTokenCollection>
  <wst:RequestSecurityToken>
   <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/BatchIssue</wst:RequestType>
   <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
   <wst:OnBehalfOf>
     <saml:Assertion>
       ... Orignal Assertion Content ...
     </saml:Assertion>
   </wst:OnBehalfOf>
   <wsp:AppliesTo>
     <wsa:EndpointReference>
       <wsa:Address>NIEF:WSP:XYZ123</wsa:Address>
     </wsa:EndpointReference>
   </wsp:AppliesTo>
  </wst:RequestSecurityToken>
  <wst:RequestSecurityToken>
   <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/BatchIssue</wst:RequestType>
```

```
   <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
   <wst:OnBehalfOf>
    <saml:Assertion>
     ... Orignal Assertion Content ...
    </saml:Assertion>
   </wst:OnBehalfOf>
   <wsp:AppliesTo>
    <wsa:EndpointReference>
     <wsa:Address>NIEF:WSP:ABC789</wsa:Address>
    </wsa:EndpointReference>
   </wsp:AppliesTo>
  </wst:RequestSecurityToken>
  ... Additional RequestSecurityToken elements as needed ...
</wst:RequestSecurityTokenCollection>
```

Figure 10: Structure of a Multi-Token Request from WSC to ADS

```
<wst:RequestSecurityTokenResponseCollection>
  <wst:RequestSecurityTokenResponse>
   <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/BatchIssue</wst:RequestType>
   <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>    <wsp:AppliesTo>
    <wsa:EndpointReference>
     <wsa:Address>NIEF:WSP:XYZ123</wsa:Address>
    </wsa:EndpointReference>
   </wsp:AppliesTo>
   <wst:RequestedSecurityToken>
    <saml:Assertion>
     ... New Assertion Content ...
    </saml:Assertion>
   </wst:RequestedSecurityToken>
  </wst:RequestSecurityTokenResponse>
  <wst:RequestSecurityTokenResponse>
   <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/BatchIssue</wst:RequestType>
   <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
   <wsp:AppliesTo>
    <wsa:EndpointReference>
     <wsa:Address>NIEF:WSP:ABC789</wsa:Address>
    </wsa:EndpointReference>
   </wsp:AppliesTo>
   <wst:RequestedSecurityToken>
    <saml:Assertion>
     ... New Assertion Content ...
    </saml:Assertion>
   </wst:RequestedSecurityToken>
  </wst:RequestSecurityTokenResponse>
  ... Additional RequestSecurityTokenResponse elements as needed ...
</wst:RequestSecurityTokenResponseCollection>
```

Figure 11: Structure of a Multitoken Request Response From ADS to WSC

9.8.3 Implementation Notes and Implications (Non-Normative)

Systems that conform to this SIP also conform to [GRA RS WS-SIP].

10. Additional Considerations

This section describes additional considerations for implementers.

10.1 Conformance Testing and Onboarding Process

Prior to joining a GFIPM federation, each WSC, WSP, IDP, TIB, AS, and VS MUST undergo a conformance testing and onboarding process as described in [GFIPM OPP].

10.2 Web Service Provider Health Monitoring

A GFIPM federation MAY require each WSP system in the federation to support a basic health monitoring protocol. This section describes the general concept of GFIPM WSP Health Monitoring and also provides normative requirements to which federation WSPs must conform if the federation chooses to implement a monitoring system.

10.2.1 Health Monitoring Objectives and Overview

A GFIPM federation health monitoring system generally seeks to test each federation WSP on a regular basis for its network connectivity, SOAP protocol behavior, and ability to behave appropriately with standards-conformant GFIPM Metadata assertions. The primary objective of a health monitoring system is to regularly test for these criteria at each federation WSP. Additional details about this topic are TBD pending additional GFIPM Web services implementation experience and standards development.

10.2.2 Health Status URL

Details about this topic are TBD pending additional GFIPM Web services implementation experience and standards development.

10.2.3 Health Status Request–Response Protocol

Details about this topic are TBD pending additional GFIPM Web services implementation experience and standards development.

10.3 Conformance With GFIPM Reference Documents

This document does not represent the complete set of GFIPM federation requirements. Other documents may apply, including business and policy documents (e.g., [GFIPM Gov] and [GFIPM OPP]), additional GFIPM technical standards (e.g., [GFIPM Meta], [GFIPM

CPS], [GFIPM Member CP], and [GFIPM Trust]), laws and regulations (*e.g.*, [NIST SP 800-63]), and applicable technology standards (*e.g.*, [FIPS 140-2]).

Appendix A—GFIPM-Specific SAML Assertion Format Rules

This appendix contains normative language that describes GFIPM-specific requirements that apply to any SAML assertion generated by an IDP or ADS for use in a GFIPM Web services transaction. These requirements augment the SAML assertion format requirements that appear in the SAML 2.0 specification ([SAML2 Core]) and the SAML 2.0 Condition for Delegation Restriction ([SAML2 Delegation]).

1. An **<Assertion>** element MUST be signed.

2. The **Version** attribute within **<Assertion>** MUST have "**2.0**" as its value.

3. The **<Issuer>** element within **<Assertion>** MUST be present, and its value MUST be the identifier of the IDP.

4. The **<Issuer>** element within **<Assertion>** MUST be agreed upon between the IDP and the federation and must match the **EntityID** specified for this IDP in the GFIPM Cryptographic Trust Fabric document (see [GFIPM Trust]).

5. An **<Assertion>** MUST contain exactly one **<Subject>** element.

6. A **<Subject>** element MUST uniquely identify the user to which the **<Assertion>** pertains.

7. The **<NameID>** element within **<Subject>** MUST contain a **Format** attribute set to one of the following values:

   a. **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**

   b. **urn:oasis:names:tc:SAML:2.0:nameid-format:transient**

8. An **<Assertion>** element MUST contain exactly one **<AuthnStatement>** element and exactly one **<AttributeStatement>** element.

9. An **<Assertion>** element MUST NOT contain an **<AuthzDecisionStatement>** element.

10. The **<AuthnStatement>** in an **<Assertion>** SHOULD include the **SessionIndex** of the user so that the IDP can properly perform a single logout (SLO) for that IDP session without unnecessarily affecting any other IDP sessions for that user.

11. The **SessionIndex** attribute within an **<AuthnStatement>** element SHOULD NOT be used to track a user from SP to SP. Instead, federation members SHOULD use the measures suggested in [SAML2 Core].

12. The contents of the **<AuthnContext>** element within the **<AuthnStatement>** element MUST accurately represent the authentication method used by the IDP to authenticate the user.

13. If the user was authenticated to the IDP via an authentication method for which a standard SAML authentication context class exists in [SAML2 Context], then the **<AuthnContext>** element within the **<AuthnStatement>** element MUST contain an **<AuthnContextClassRef>** element that specifies the appropriate authentication context class.

14. The **<AttributeStatement>** element in an **<Assertion>** MAY contain one or more **<Attribute>** elements and MUST NOT contain any **<EncryptedAttribute>** elements.[61]

15. Each **<Attribute>** element MAY contain application-level user attribute data corresponding to a GFIPM user attribute defined in [GFIPM Meta].[62]

16. If the **<Attribute>** element corresponds to a GFIPM user attribute defined in [GFIPM Meta], then the **Name** attribute within the **<Attribute>** element MUST contain the fully qualified formal name of the attribute as defined in [GFIPM Meta]. In addition, the **NameFormat** attribute within the **<Attribute>** element MUST be present, and "**urn:oasis:names:tc:SAML:2.0:attrname-format:uri**" MUST be the value of the **NameFormat** attribute.

17. Each **<Attribute>** element MUST contain one or more **<AttributeValue>** elements.

18. Each **<AttributeValue>** element MUST contain the following attribute name/value pairs:

    a. **xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"**

    b. **xsi:type="xs:string"**

[61] It is customary for a GFIPM federation to define a set of user attributes that are designated as mandatory and therefore must appear in every SAML assertion; however, such federation-specific constraints are beyond the scope of this specification. Therefore, this specification does not require any specific number of **<Attribute>** elements.

[62] This statement implies that it is permissible for an **<Attribute>** element to contain any type of user attribute, including GFIPM Metadata user attributes defined in [GFIPM Meta] as well as other (non-GFIPM) attributes.

19. Each **<AttributeValue>** element MUST contain data corresponding to the value of the GFIPM user attribute represented by its enclosing **<Attribute>** element.

Please see Appendix B for a sample SAML <**Assertion**> XML element that is conformant with these requirements.

Appendix B—Sample SAML Assertion

Figure 12 contains a sample SAML assertion that is intended to provide an example of conformance with the requirements specified in Appendix A.

```
<saml:Assertion ID="_c0594b43e28a2f94311d395d57d4ae5a"
 IssueInstant="2011-10-16T15:16:19.938Z" Version="2.0"
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
 <saml:Issuer
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
  https://rhelidp.ref.gfipm.net/shibboleth
 </saml:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:CanonicalizationMethod
    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
   <ds:SignatureMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
   <ds:Reference URI="_c0594b43e28a2f94311d395d57d4ae5a"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transforms
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transform
      Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
     <ds:Transform
      Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#WithComments"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ec:InclusiveNamespaces PrefixList="ds saml xs"
       xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
     </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod
     Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
    <ds:DigestValue
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     O/LiVrYP7MG5/bNCSQARk7tBAuI=
    </ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   [base64 signature snipped for brevity]
  </ds:SignatureValue>
 </ds:Signature>
 <saml:Subject>
  <saml:NameID
   Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
   NameQualifier="http://rhelidp.ref.gfipm.net/shib-idp/">
   _84b810c771472f309d0bbdf6a517813a
  </saml:NameID>
  <saml:SubjectConfirmation
   Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">
  </saml:SubjectConfirmation>
 </saml:Subject>
 <saml:Conditions NotBefore="2011-10-16T15:16:19.938Z"
  NotOnOrAfter="2011-10-16T15:21:19.938Z">
  <saml:AudienceRestriction>
   <saml:Audience>https://rhelsp.ref.gfipm.net/shibboleth</saml:Audience>
  </saml:AudienceRestriction>
```

```
    <saml:Condition xmlns:del="urn:oasis:names:tc:SAML:2.0:conditions:delegation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="del:DelegationRestrictionType">
      <del:Delegate DelegationInstant="2011-10-16T15:16:19.938Z">
        <NameID>E=gfipm-support@lists.gatech.edu, CN=HA50WSC, O=Hawaii Five0, L=Honolulu, S=Hawaii,
C=US</NameID>
      </del:Delegate>
    </saml:Condition>
  </saml:Conditions>
  <saml:AuthnStatement AuthnInstant="2011-10-16T15:16:19.878Z"
    SessionNotOnOrAfter="2011-10-16T15:46:19.878Z">
    <saml:SubjectLocality Address="130.207.204.222"
      DNSName="130.207.204.222" />
    <saml:AuthnContext>
      <saml:AuthnContextDeclRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
      </saml:AuthnContextDeclRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute Name="gfipm:2.0:user:FederationId"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xsi:type="xs:string">
        GFIPM:IDP:JNET:USER:johndoe@jnet.net
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="gfipm:2.0:user:GivenName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xsi:type="xs:string">
        John
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="gfipm:2.0:user:SurName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xsi:type="xs:string">
        Doe
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Figure 12: Sample SAML Assertion

Appendix C—Sample WSDL Policy Language

This appendix contains sample WS-Policy and WS-SecurityPolicy policy language that WSPs can use in their WSDL documents for various security requirements specified by this document.

Figure 13 and Figure 14 contain sample policy language to indicate that a WSP requires XML digital signatures on messages. Figure 13 uses the WS-SecurityPolicy <AsymmetricBinding> element to indicate the type of signature required, including certificate type (X.509 Version 3), digest algorithm (SHA-256), and various other details. Figure 14 uses the WS-Policy <SignedParts> element to indicate which parts of a message must be signed.

```
<wsp:Policy>
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:AsymmetricBinding xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <wsp:Policy>
          <sp:InitiatorToken>
            <wsp:Policy>
              <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                <wsp:Policy>
                  <sp:WssX509V3Token10/>
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:InitiatorToken>
          <sp:RecipientToken>
            <wsp:Policy>
              <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                <wsp:Policy>
                  <sp:WssX509V3Token10/>
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:RecipientToken>
          <sp:AlgorithmSuite>
            <wsp:Policy>
              <sp:Basic256Sha256/>
            </wsp:Policy>
          </sp:AlgorithmSuite>
          <sp:Layout>
            <wsp:Policy>
              <sp:Lax/>
            </wsp:Policy>
          </sp:Layout>
          <sp:IncludeTimestamp/>
          <sp:OnlySignEntireHeadersAndBody/>
        </wsp:Policy>
      </sp:AsymmetricBinding>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
```

Figure 13: Sample WSDL Policy Language for Digital Signature Key Binding

```
<wsp:Policy>
 <wsp:ExactlyOne>
  <wsp:All>
   <sp:SignedParts xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
    <sp:Body />
    <sp:Header Name="To" Namespace="http://www.w3.org/2005/08/addressing" />
    <sp:Header Name="From" Namespace="http://www.w3.org/2005/08/addressing" />
    <sp:Header Name="FaultTo" Namespace="http://www.w3.org/2005/08/addressing" />
    <sp:Header Name="ReplyTo" Namespace="http://www.w3.org/2005/08/addressing" />
    <sp:Header Name="MessageID" Namespace="http://www.w3.org/2005/08/addressing" />
    <sp:Header Name="RelatesTo" Namespace="http://www.w3.org/2005/08/addressing" />
    <sp:Header Name="Action" Namespace="http://www.w3.org/2005/08/addressing" />
   </sp:SignedParts>
  </wsp:All>
 </wsp:ExactlyOne>
</wsp:Policy>
```

Figure 14: Sample WSDL Policy Language for Message Part Digital Signature Requirements

Figure 15 contains sample policy language to indicate that a WSP requires the use of TLS as the transport medium for messages.

```
<sp:TransportBinding>
 <wsp:Policy>
  <sp:TransportToken>
   <wsp:Policy>
    <sp:HttpsToken />
   </wsp:Policy>
  </sp:TransportToken>
  <sp:AlgorithmSuite>
   <wsp:Policy>
    <sp:Basic256 />
   </wsp:Policy>
  </sp:AlgorithmSuite>
  <sp:Layout>
   <wsp:Policy>
    <sp:Strict />
   </wsp:Policy>
  </sp:Layout>
  <sp:IncludeTimestamp />
 </wsp:Policy>
</sp:TransportBinding>
```

Figure 15: Sample WSDL Policy Language for Use of a TLS Transport Binding

Figure 16 contains sample policy language to indicate that a WSP requires the use of XML encryption on the body of messages. Note that the use of XML encryption is optional for GFIPM Web services.

```
<wsp:Policy>
 <wsp:ExactlyOne>
  <wsp:All>
   <sp:EncryptedParts>
    <sp:Body/>
   </sp:EncryptedParts>
  </wsp:All>
 </wsp:ExactlyOne>
</wsp:Policy>
```

Figure 16: Sample WSDL Policy Language for Use of XML Encryption

Figure 17 contains alternate sample policy language to indicate that a WSP requires the inclusion of a SAML 2.0 assertion issued by an Assertion Delegate Service within a request message from a WSC. This example requires the use of a WS-SecurityPolicy SamlToken Assertion rather than an IssuedToken Assertion, as is required by the policy language in Figure 17. We have included examples with both IssuedToken and SamlToken because either is acceptable for conformance to the GFIPM-WS User-Consumer-Provider SIP.

```
<wsp:Policy>
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:SignedSupportingTokens xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <wsp:Policy>
          <sp:IssuedToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
            <sp:RequestSecurityTokenTemplate>
              <trust:TokenType xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512">http://docs.oasis-
open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</trust:TokenType>
            </sp:RequestSecurityTokenTemplate>
            <wsp:Policy>
              <sp:RequireInternalReference/>
            </wsp:Policy>
          </sp:IssuedToken>
        </wsp:Policy>
      </sp:SignedSupportingTokens>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
```

Figure 17: Sample WSDL Policy Language for SAML Assertion Requirements

Figure 18 contains sample policy language to indicate that a WSP requires the inclusion of a SAML 2.0 assertion issued by an Assertion Delegate Service within a request message from a WSC. The GFIPM-WS User-Consumer-Provider SIP (see Section 9.2) requires this. Note that this example specifies the use of a WS-SecurityPolicy IssuedToken Assertion.

```
<wsp:Policy wsu:Id="CommercialVehicleCollisionBindingPolicy">
   <wsp:ExactlyOne>
         <wsoma:OptimizedMimeSerialization/>
         <wsaw:UsingAddressing wsp:Optional="false"/>
         <sp:AsymmetricBinding>
            <wsp:Policy>
               <sp:InitiatorToken>
                  <wsp:Policy>
                     <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                        <wsp:Policy>
                           <sp:RequireThumbprintReference/>
                           <sp:WssX509V3Token10/>
                        </wsp:Policy>
                     </sp:X509Token>
                  </wsp:Policy>
               </sp:InitiatorToken>
               <sp:RecipientToken>
                  <wsp:Policy>
                     <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                        <wsp:Policy>
                           <sp:RequireThumbprintReference/>
                           <sp:WssX509V3Token10/>
                        </wsp:Policy>
```

```
                    </sp:X509Token>
                 </wsp:Policy>
              </sp:RecipientToken>
              <sp:Layout>
                 <wsp:Policy>
                    <sp:Lax/>
                 </wsp:Policy>
              </sp:Layout>
              <sp:IncludeTimestamp/>
              <sp:OnlySignEntireHeadersAndBody/>
              <sp:AlgorithmSuite signatureAlgorithm="SHA256withRSA">
                 <wsp:Policy>
                    <sp:Basic256Sha256/>
                 </wsp:Policy>
              </sp:AlgorithmSuite>
           </wsp:Policy>
        </sp:AsymmetricBinding>
        <sp:Wss11>
           <wsp:Policy>
              <sp:MustSupportRefKeyIdentifier/>
              <sp:MustSupportRefIssuerSerial/>
              <sp:MustSupportRefThumbprint/>
              <sp:MustSupportRefEncryptedKey/>
              <sp:RequireSignatureConfirmation/>
           </wsp:Policy>
        </sp:Wss11>
        <sp:Trust13>
           <wsp:Policy>
              <sp:MustSupportIssuedTokens/>
              <sp:RequireClientEntropy/>
              <sp:RequireServerEntropy/>
           </wsp:Policy>
        </sp:Trust13>
        <sp:SignedEncryptedSupportingTokens>
           <wsp:Policy>
              <sp:SamlToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                 <wsp:Policy>
                    <sp:WssSamlV20Token11/>
                 </wsp:Policy>
              </sp:SamlToken>
           </wsp:Policy>
        </sp:SignedEncryptedSupportingTokens>
     </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
```

Figure 18: Alternate Sample WSDL Policy Language for SAML Assertion Requirements

Appendix D—Document History

Date	Version	Editor	Change
04/12/2012	1.0	Global Standards Council (GSC), Global Federated Identity and Privilege Management Delivery Team (GFIPM DT)	Approved

About Global

www.it.ojp.gov/global

The 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 Global and its products, including those referenced in this document, call (850) 385-0600 or visit http://www.it.ojp.gov/GIST.

About GSC

www.it.ojp.gov/gsc

In accordance with the founding principle of Global, the Global Standards Council (GSC) directly supports the broadscale exchange of pertinent justice and public safety information by promoting standards-based electronic information exchanges for the justice community as a whole. Specifically, the GSC develops, maintains, and sustains the standards—including this particular standard—associated with these aforementioned information exchanges. To further foster community participation and reuse, the GSC also receives, evaluates, and recommends to Global for adoption proposed standards submitted by Global consumers and stakeholders. In turn, the GSC employs an enterprise architecture approach for developing and maintaining the cohesive body of Global standards as one Global Standards Package (GSP), which can be accessed at http://www.it.ojp.gov/gsp.

http://www.it.ojp.gov/gsp

This project was supported by Grant No. 2009-DB-BX-K105 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.