BJA

Bureau of Justice Assistance
U.S. Department of Justice

Federated Identity and Privilege Management

Terminology Matrix

Version 1.0.1

April 2012

Global
Information
Sharing Standard

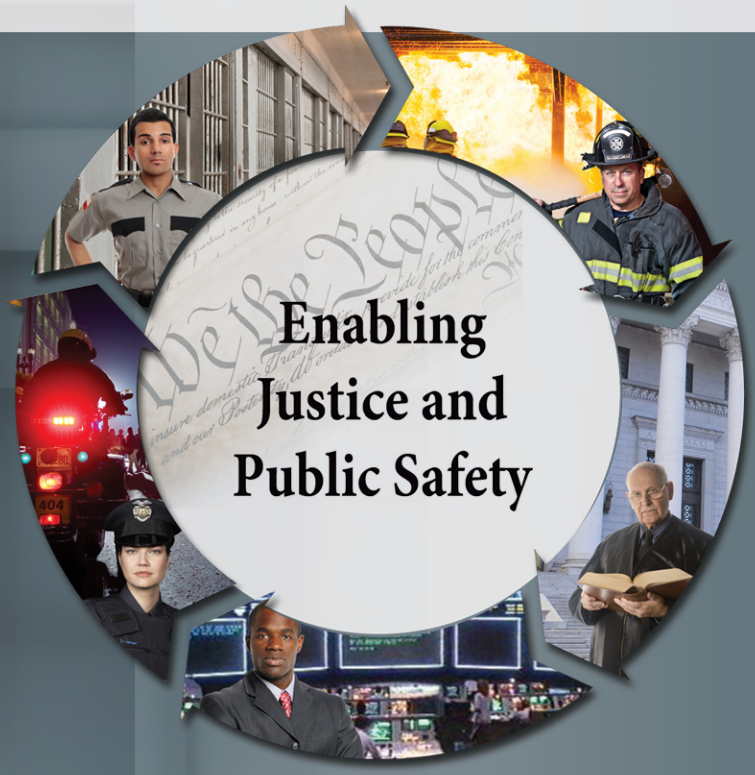
Global Standards

The collection of Global-recommended normative standards has been developed and assembled into a unified package of composable, interoperable solutions that enable effective information exchange. This collection is known as the Global Standards Package (GSP). GSP solutions are generally focused on resolving technical interoperability challenges but also include associated guidelines and operating documents to assist implementers. The GSP includes 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 are reusable nationwide in order to save time and money and reduce complexity when implementing particular information exchanges with external partners.
- **Global Federated Identity and Privilege Management (GFIPM):** Guidelines and standards for establishing, implementing, and governing security, identity management, and access control solutions to ensure that information can be accessed only securely and appropriately.
- **Global Privacy Technology Framework:** A framework for automating information access controls based on privacy and related policies restricting the use or dissemination of such information.

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.



About the Document

Justice organizations are looking for ways to provide secured access to multiple agency information systems with a single logon. The Global Federated Identity and Privilege Management (GFIPM) initiative, developed by the U.S. Department of Justice's Global Justice Information Sharing Initiative, provides the justice community with a security and information sharing architecture that is based on an electronic justice credential. This standards-based justice credential can be used to securely connect law enforcement and public safety personnel to interagency applications and data over the Internet.

Background: The GFIPM framework provides the justice community and partner organizations with a standards-based approach for implementing federated identity. Common use of these standards across federation systems is essential to their interoperability. Leveraging the Global Justice XML and National Information Exchange Model (NIEM), a standard set of XML-based elements and attributes (referred to collectively as GFIPM metadata) about a federation user's identities, privileges, and authentication can be universally communicated.

Value to the Justice Community:

1. **User Convenience:** Users can access multiple services using a common set of standardized security credentials, making it easier to sign on and access applications and to manage account information.
2. **Interoperability:** By specifying common security standards and framework, applications can adopt interoperable security specifications for authentication and authorization.
3. **Cost-Effectiveness:** GFIPM facilitates information sharing by using a standardized XML-based credential that includes information about each user's identity and privileges. This reduces the cost and complexity of identity administration required to access applications and vet users.
4. **Privacy:** GFIPM can reduce the propagation of personally identifiable information, reduce the redundant capture and storage of personal identity information, and depersonalize data exchanges across domains using privacy metadata.
5. **Security:** A federation model can improve the security of local identity information and data in applications by providing a standardized approach to online identities between agencies or applications.

Contents: The GFIPM Terminology Matrix provides a terminology and concept map between GFIPM and other prominent paradigms in the areas of identity management, privilege management, and service-oriented architecture. Its purpose is to help GFIPM stakeholders better understand the various technical terms used in GFIPM by mapping each GFIPM term to the corresponding terms from other technologies.

Target Audience: The target audience for this document includes managers and technical representatives of prospective GFIPM participant organizations who are planning to implement an identity provider (IDP) and/or a service provider (SP) within a GFIPM federation. It also includes vendors, contractors, and consultants who are required to establish technical interoperability with GFIPM standards as part of their project or product implementation.

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 and Purpose

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. By its nature, the GFIPM program involves collaboration among many disparate groups and individuals, and each collaborator brings a unique set of experiences in terms of problems encountered and terminology used to describe those problems and the solutions to those problems. In particular, the GFIPM program makes use of federated identity management standards and other related technical standards, many of which contain terminology that may cause confusion when used in the context of other standards and technologies.

The GFIPM Terminology Matrix has been developed to maximize the level of precision in other GFIPM documents and minimize the level of confusion that readers may face as they work through and try to interpret these documents within the context of their experiences and prior knowledge. This document attempts to define and reconcile common terms from the following technologies, technical standards, and related initiatives, as those terms relate to the GFIPM program.

1. Security Assertion Markup Language (SAML)
2. Web Services (WS-*)
3. Web Services Interoperability (WS-I)
4. Global Reference Architecture (GRA)

2. References

This section contains references to other documents that are related to this document. It includes documents that are relevant to the GFIPM program, as well as SAML, GRA, Web Services industry standards and profiles, and other topics that are closely related to GFIPM.

Document ID	Document Name and URL
GFIPM Map	GFIPM Document Map
GFIPM Terms	GFIPM Terminology Matrix
GFIPM Gov	GFIPM Governance Guidelines
GFIPM OPP	GFIPM Operational Policies and Procedures
GFIPM Meta	GFIPM Metadata Standard
GRA WS-SIP	Global Reference Architecture Web Services Service Interaction Profile
GRA RS WS-SIP	Global Reference Architecture Reliable Secure Web Services Service Interaction Profile

OpenID	OpenID is an open, decentralized standard for authenticating users. It replaces the common login process that uses a login name and a password by allowing a user to log in once and gain access to the resources of multiple software systems. http://openid.net/
SAML2	Security Assertion Markup Language (SAML) 2.0 is an XML-based standard for exchanging authentication and authorization data between identity providers and service providers. SAML is a product of the OASIS Security Services Technical Committee (SSTC). http://wiki.oasis-open.org/security
SOAP	SOAP is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. SOAP was originally an acronym for "Simple Object Access Protocol," but the name was subsequently changed to SOAP. SOAP is currently maintained by the XML Protocol Working Group of the World Wide Web Consortium (W3C). http://www.w3.org/2000/xp/Group/
WS-Sec	Web Services Security (WS-Security) is a communications protocol for applying security to Web Services. It describes how to attach signatures, encryption headers, and other security tokens to SOAP messages. WS-Security is under the control of OASIS. http://docs.oasis-open.org/wss/
WS-Sec SAML	Web Services Security (WS-Security) SAML Token Profile is an OASIS standard that specifies how to use SAML 1.1 and SAML 2.0 assertions with the WS-Security standard. http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf
WS-I BP	WS-I Basic Profile (WS-I BP) is a standard that promotes interoperability between Web Services in general. It is a product of the Web Services Interoperability Organization. http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile
WS-I BSP	Web Services Interoperability Basic Security Profile (WS-I BSP) is a standard that promotes interoperability for secure Web Services. It is based on SOAP and WS-Security and provides guidance on the use of various WS-Security token formats. It is based on the WS-I Basic Profile (WS-I BP) and is a product of the Web Services Interoperability Organization. http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicsecurity

WS-Addr	Web Services Addressing (WS-Addressing) is a transport-agnostic standard used to communicate message-addressing information in Web Services. It is under the control of the World Wide Web Consortium (W3C) WS-Addressing Working Group. http://www.w3.org/2002/ws/addr/
WS-Trust	Web Services Trust Language (WS-Trust) is a Web Services specification and OASIS standard that provides extensions to the WS-Security standard for the issuance, renewal, and validation of security tokens, as well as establishing and brokering trust relationships between participants in a secure Web Services message exchange. http://docs.oasis-open.org/ws-sx/ws-trust/
WS-Policy	Web Services Policy Framework (WS-Policy) is a specification that enables Web Services providers and consumers to exchange policy information and requirements related to security, quality of services, and various other aspects of Web Services. It is under the control of the World Wide Web Consortium (W3C) WS-Policy Working Group. http://www.w3.org/2002/ws/policy/
WS-SC	Web Services Secure Conversation Language (WS-SecureConversation) is a specification that enables sharing of security contexts for Web Services. It works in conjunction with WS-Security, WS-Trust, and WS-Policy. http://docs.oasis-open.org/ws-sx/ws-secureconversation/
WS-RM	Web Services Reliable Messaging (WS-ReliableMessaging) is a specification that allows SOAP messages to be delivered reliably between distributed applications in the presence of software component, system, or network failures. It is an OASIS standard, under the control of the OASIS Web Services Reliable Exchange (WS-RX) Technical Committee. http://docs.oasis-open.org/ws-rx/wsrm/
WS-Fed	WS-Federation is an identity federation specification that defines mechanisms for allowing disparate security realms to broker information on identities, identity attributes, and authentication. It was ratified as an OASIS standard in May 2009. http://docs.oasis-open.org/wsfed/

WS-I RSP	Web Services Interoperability Reliable Secure Profile (WS-I RSP) is a standard that promotes interoperability for secure, reliable messaging capabilities for Web Services. It is designed to be composed with the Web Services Interoperability Basic Profile (WS-I BP) and the Web Services Interoperability Basic Security Profile (WS-I BSP), and it profiles WS-Addressing, WS-SecureConversation, and WS-ReliableMessaging. It is a product of the Web Services Interoperability Organization. http://www.ws-i.org/deliverables/workinggroup.aspx?wg=reliablesecure
FIPS 140-2	Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, is a U.S. government computer security standard used to accredit cryptographic modules. It was initially published on May 25, 2001, and most recently updated on December 3, 2002. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
XML-Encryption	*XML Encryption Syntax and Processing*, W3C Recommendation December 10, 2002, specifies a process for encrypting data and representing the result in XML. The data may be arbitrary data (including an XML document), an XML element, or XML element content. http://www.w3.org/TR/xmlenc-core/
XML-Signature	*XML Signature Syntax and Processing (Second Edition)*, W3C Recommendation June 10, 2008, specifies XML digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere. http://www.w3.org/TR/xmldsig-core/
RFC 2119	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2119, "Key Words for Use in RFCs to Indicate Requirement Levels," is a document that specifies best current practices regarding the use of key words that relate to requirements in technical and policy standards. It is mainly intended for use as an interpretive guide for understanding language in other IETF RFCs and standards; however, its language is generally applicable to all normative technical standards. http://www.ietf.org/rfc/rfc2119.txt

3. GFIPM Roles and Responsibilities

This section contains a series of three tables that provide descriptions of the basic roles and responsibilities that exist within the GFIPM concept. Table 1 addresses roles and responsibilities from an organizational standpoint, and Table 2 approaches them from a technical standpoint. Table 3 illustrates how the set of GFIPM organizational roles maps onto the set of GFIPM technical roles.

GFIPM Organizational Roles and Responsibilities	
Role	***Responsibilities***
Federation Manager Organization (FMO)	1. Vet prospective federation member organizations for membership. 2. Provide authentication credentials to member organizations. 3. Provide mechanism for authenticating member organizations.
Identity Provider Organization (IDPO)	1. Vet end users for access to the federation. 2. Provide authentication credentials to end users. 3. Authenticate end users. 4. Generate user assertions containing GFIPM metadata.
Service Provider Organization (SPO)	1. Provide application-level services to federation end users. 2. Perform access control based on GFIPM metadata.
Trusted Identity Broker Organization (TIBO)	1. Vet brokered IDPOs and their IDPs. 2. Represent brokered IDPs to the federation. 3. Generate user assertions containing GFIPM metadata on behalf of users from brokered IDPs.

Table 1: GFIPM Organizational Roles and Responsibilities

GFIPM Technical Roles and Responsibilities	
Role	***Responsibilities***
Certificate Authority (CA)	1. Sign cryptographic certificates for member systems. 2. Sign the GFIPM Cryptographic Trust Fabric document. 3. Distribute the GFIPM Cryptographic Trust Fabric document to all member organizations.
Identity Provider (IDP)	1. Perform authentication for end users. 2. Generate SAML assertions containing GFIPM metadata about users. 3. Conform to the GFIPM Web Browser User-to-System Profile.
SAML Service Provider (SP)[1]	1. Provide Web-based access to application-level services for end users. 2. Enforce resource access control policies based on GFIPM metadata from IDPs. 3. Conform to the GFIPM Web Browser User-to-System Profile.
Web Service Consumer (WSC)	1. Provide a connecting point through which a member organization can connect to GFIPM Web Services providers (WSPs).[2] 2. Conform to the GFIPM Web Services System-to-System Profile.
Web Service Provider (WSP)	1. Provide Web Services-based access to application-level services for member organizations and their end users. 2. Conform to the GFIPM Web Services System-to-System Profile.
Authorization Service (AS)	1. Make authorization decisions on behalf of other GFIPM Web Services providers (WSPs) and issue tokens that can be used at those WSPs. 2. Conform to the GFIPM Web Services System-to-System Profile.

[1] In some GFIPM documents, a SAML Service Provider is also called a Service Provider.

[2] It is possible to configure a Web Service Consumer (WSC) such that it acts as a proxy into various Web Service Providers (WSPs) in the federation on behalf of entities on the WSC's local network that are not in the GFIPM Cryptographic Trust Fabric. There is a potential security risk associated with this configuration, particularly in the case where a Web Services request is not associated with a user. It may be necessary for the GFIPM Governance and/or GFIPM Operational Policies and Procedures documents to be modified to prohibit this type of "open proxy" configuration for a WSC.

Role	*Responsibilities*
Assertion Delegate Service (ADS)	1. Translate SAML assertions into delegated SAML assertions that can be used by GFIPM Web Service Consumers (WSCs) when communicating with GFIPM Web Service Providers (WSPs) on behalf of users. 2. Conform to the GFIPM Web Services System-to-System Profile.
Trusted Identity Broker (TIB)	1. Generate SAML assertions containing GFIPM metadata about users from brokered IDPs. 2. Conform to the GFIPM Web Browser User-to-System Profile.

Table 2: GFIPM Technical Roles and Responsibilities[3]

GFIPM Organizational Role Mapping to GFIPM Technical Roles	
Organizational Role	***Technical Roles***
Federation Manager Organization (FMO)	Certificate Authority (CA)
Identity Provider Organization (IDPO)	Identity Provider (IDP) Assertion Delegate Service (ADS)
Service Provider Organization (SPO)	SAML Service Provider (SP) Web Service Consumer (WSC) Web Service Provider (WSP) Authorization Service (AS)
Trusted Identity Broker Organization (TIBO)	Trusted Identity Broker (TIB)

Table 3: GFIPM Organizational Role Mapping to GFIPM Technical Roles

[3] Entities that act in these technical roles are required to appear in the GFIPM Cryptographic Trust Fabric document.

4. GFIPM Service-Oriented Architecture Terminology Map

Table 4 below contains a "Terminology Map" that provides a concise comparison between GFIPM and several other prominent identity management paradigms in terms of what terminology is used to express various aspects of each paradigm.

GFIPM Service-Oriented Architecture Terminology Map				
	GFIPM	***SAML***	***WS-*/WS-I***	***GRA[4]***
Organizational Roles				
	Federation Manager Organization (FMO)	N/A	N/A	N/A
	IDP Organization (IDPO)	N/A	N/A	N/A
	SP Organization (SPO)	N/A	N/A	N/A
	TIB Organization (TIBO)	N/A	N/A	N/A
Technical Roles				
	Certificate Authority (CA)	N/A	N/A	N/A
	Identity Provider (IDP)	Same as GFIPM	WS-Federation: Identity Provider or Security Token Service in the role of Identity Provider or Security Token Service in the role of Attribute Service[5] Abbreviated as IP/STS	N/A
	SAML Service Provider (SP)	Service Provider	WS-Federation: Resource or Relying Party	Service Provider
	Web Service Consumer (WSC)	N/A	WS-Federation: Requestor	Service Consumer
	Web Service Provider (WSP)	N/A	WS-Federation: Resource or Relying Party	Service Provider
	Authorization Service (AS)	N/A	WS-Federation: Security Token Service in the role of Authorization Service[6]	Service Provider
	Assertion Delegate Service (ADS)	N/A	N/A	N/A
	Trusted Identity Broker (TIB)	N/A	N/A	Service Provider

[4] The Global Reference Architecture (GRA) is based on principles of Service-Oriented Architecture (SOA), in which many types of entities can play the role of a Service Provider. The SOA concept of a Service Provider is more general than the GFIPM concept of a Service Provider, which is a service that provides an interface to application data for the benefit of end users.

[5] WS-Federation defines an attribute service to enable privacy protection for certain attributes.

[6] WS-Federation supports the concept of authorization via an STS but does not specifically define an Authorization Service.

	GFIPM	SAML	WS-*/WS-I	GRA[7]
Other				
	Assertion	Assertion	Security Token	N/A
	Assertion Attribute	Assertion Attribute	Claim	N/A

Table 4: GFIPM Terminology Mapping to Service-Oriented Architecture Paradigms

5. Additional GFIPM Terms and Definitions

This section contains definitions of additional GFIPM terms that are not covered in Section 3.

Federation: A group of agencies acting together in a peer relationship to share sensitive information with each other, subject to applicable access control policies.

Transaction: An event between two software entities in a federation in which an attempt is made to exchange sensitive information, subject to applicable access controls.

Session: An arrangement between two software entities in a federation, and also possibly including a user, for the purpose of establishing and maintaining a security context in which multiple transactions can be performed over a period of time.

GFIPM Cryptographic Trust Fabric: A document signed by the Federation Manager Organization, containing trusted information about each IDP, SP, WSC, WSP, AS, ADS, and TIB in the federation. It includes X.509 certificate data for each software entity, as well as a GFIPM Entity Assertion providing various informational attributes about each entity. The GFIPM Trust Fabric is the cryptographic trust anchor for all federation transactions.

[7] The Global Reference Architecture (GRA) is based on principles of Service-Oriented Architecture (SOA), in which many types of entities can play the role of a Service Provider. The SOA concept of a Service Provider is more general than the GFIPM concept of a Service Provider, which is a service that provides an interface to application data for the benefit of end users.

Appendix A—Document History

Date	Version	Editor	Change
04/12/2012	1.0.1	Global Standards Council (GSC), Global Federated Identity and Privilege Management Delivery Team (GFIPM DT)	Approved

About the Global Advisory Committee

www.it.ojp.gov/global

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

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 the Global Standards Council

www.it.ojp.gov/gsc

The Global Standards Council (GSC) serves as a Global Advisory Committee (GAC) subcommittee, supporting broadscale electronic sharing of pertinent justice- and public safety-related information by recommending to BJA (through the GAC) associated information sharing standards and guidelines. To foster community participation and reuse, the GSC reviews proposed information sharing standards submitted by Global consumers and stakeholders. Additionally, BJA emphasizes an open, participatory review-and-comment process for proposed standards; please see the Global Justice Tools Web site at www.globaljusticetools.net for more information on this opportunity. BJA-approved standards are developed, maintained, and sustained as one cohesive Global Standards Package (GSP) located at 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, U.S. Department of Justice, in collaboration with the 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.