BJA
Bureau of Justice Assistance
U.S. Department of Justice

Federated Identity and Privilege Management

Trusted Identity Broker Onboarding Guide

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.

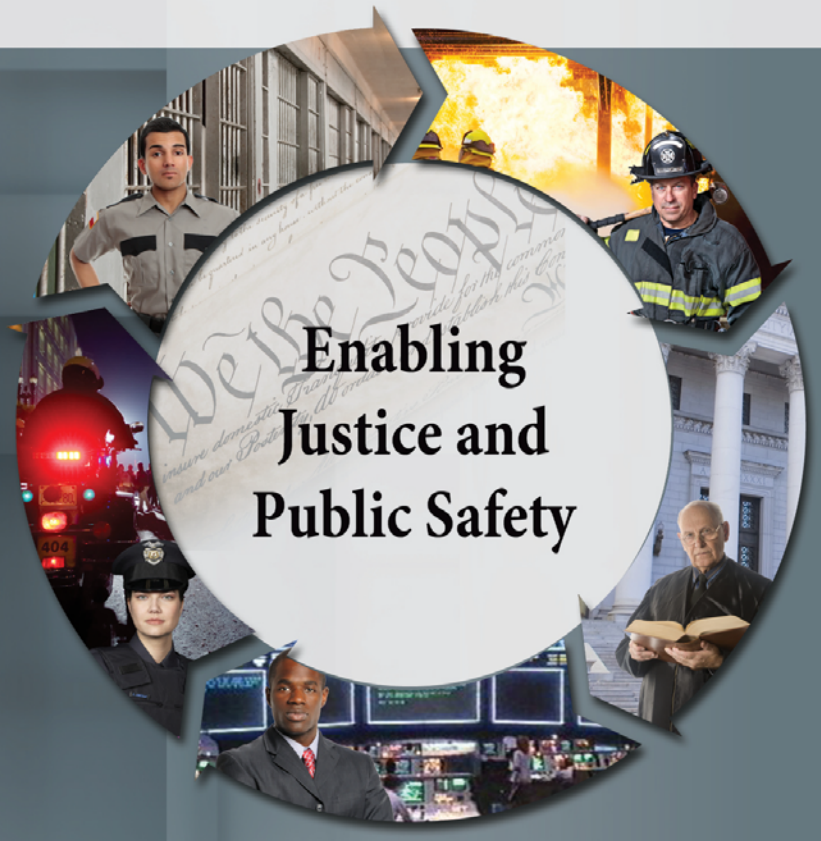

Table of Contents

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. Purpose of This Document

This document serves three main purposes.

1. It provides background information about interfederation information sharing within the Global Federated Identity and Privilege Management (GFIPM) paradigm.
2. It supplements the GFIPM Federation Membership Processes, documented in Section 5 of [GFIPM OPP], to address federation membership for trusted identity brokers (TIBs).

3. It provides supplementary technical requirements and guidance for TIBs.

Its target audience includes representatives from agencies that want to perform interfederation information sharing and also conform to the GFIPM paradigm, as well as implementers working on behalf of those agencies.

3. Background: Interfederation Information Sharing in GFIPM

GFIPM relies on the concept of a *federation*: a group of agencies that establish a mutual trust relationship for the purpose of sharing information to accomplish their business objectives. Agencies in a GFIPM federation participate in a well-defined federation governance process and follow a well-defined set of operational policies and procedures.[1] In addition, agencies agree to disclose certain internal policy documents with each other, including local security policies, local user agreements, etc. These steps ensure a solid base of mutual trust among federation member agencies, and this trust is a fundamental part of a GFIPM federation. Without it, cryptographic trust between federation members would be meaningless. Figure 1 shows all the interoperability layers in the GFIPM paradigm, and it illustrates how mutual organizational trust underpins all other layers of the model.

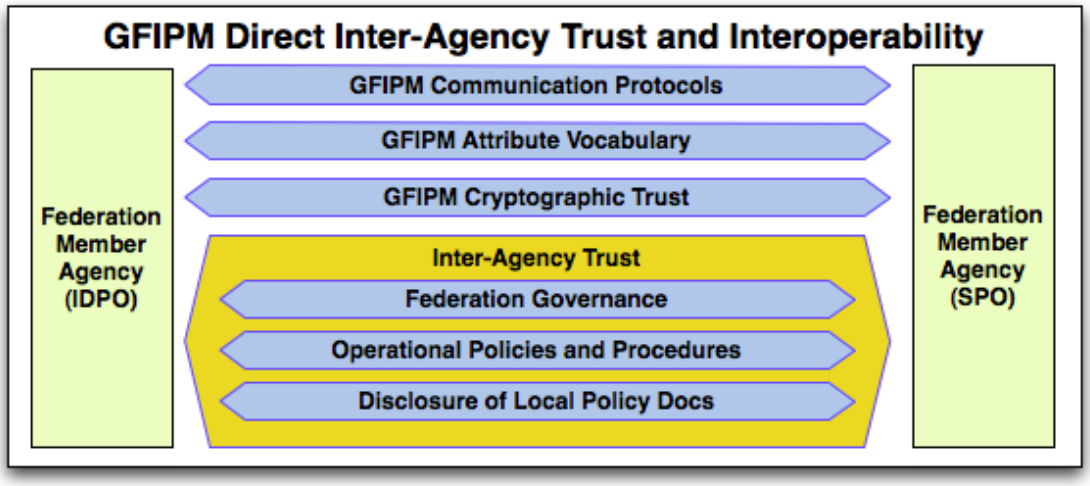

Figure 1: GFIPM Direct Inter-Agency Trust and Interoperability

The GFIPM federation concept provides a convenient mechanism for establishing interagency trust; however, it does not provide an adequate solution for all interagency information sharing scenarios. It is sometimes necessary to establish information sharing arrangements that cross federation boundaries or span multiple federations. These *interfederation* information sharing scenarios still rely on the establishment of mutual trust between the participating agencies, but they require a different approach for establishing that trust. The GFIPM solution to interfederation information sharing is to use a *trusted*

[1] The GFIPM federation governance structure is defined in [GFIPM Gov]. Operational policies and procedures for GFIPM federations are defined in [GFIPM OPP].

identity broker organization (TIBO) and a *trusted identity broker* (TIB). The remainder of this section describes these concepts in detail.

3.1 Trusted Identity Broker Organization

The GFIPM Terminology Matrix [GFIPM Terms] identifies three organizational roles in a GFIPM federation: identity provider organization (IDPO), service provider organization (SPO), and trusted identity broker organization (TIBO).[2] Table 1 summarizes the responsibilities that accompany each role.

Role	*Responsibilities*
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 identity providers (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

As indicated by Table 1, a TIBO acts as a conduit through which users from an IDPO can access resources across federations. From the standpoint of inter-agency trust, a TIBO agency must act on behalf of an IDPO agency and ensure that all other federation member agencies can trust the brokered IDPO as if it were a federation member. Figure 2 shows all the interoperability layers in the GFIPM paradigm as in Figure 1, but it also illustrates how the organizational trust relationship works when a TIBO is used.

[2] [GFIPM Terms] identifies a fourth organizational role—federation manager organization (FMO)—but this role pertains to operational management of a federation and is not critical to this discussion of trusted identity brokers.

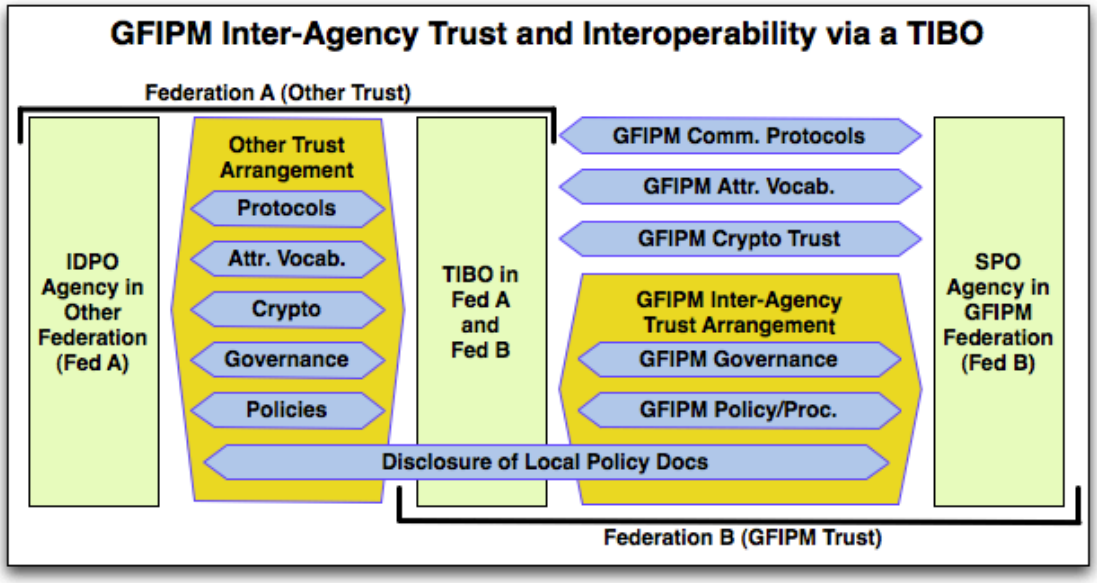

Figure 2: GFIPM Inter-Agency Trust and Interoperability via a TIBO

3.2 Trusted Identity Broker

As defined in [GFIPM Terms], a trusted identity broker (TIB) is a software endpoint that generates SAML assertions containing GFIPM metadata about users from an IDP.[3] A TIB must conform to the GFIPM Web Browser User-to-System Profile [GFIPM U2S Profile], and a TIB can be operated only by a TIBO.

At a technical level within a GFIPM federation, a TIB is nearly indistinguishable from an IDP. It conforms to the same normative communication profile and makes assertions about users with the same set of metadata attributes. But there are three ways in which a TIB differs from an IDP at a technical level.

1. When asserting a user's Federation ID and Identity Provider ID attributes in a SAML assertion, a TIB must assert them using a syntax that indicates the brokered relationship between the user's IDP and the federation.

2. When appearing in a GFIPM Cryptographic Trust Fabric document,[4] a TIB's Entity ID attribute must use a syntax that identifies it as a TIB rather than an IDP.

[3] For simplicity, the remainder of this section is written to assume that a TIB provides a brokering arrangement for only one IDP; however, in practice, a TIB can broker one or more IDPs. Obvious practical engineering constraints exist, but in theory there is no limit on the number of IDPs that a TIB can broker.

[4] The GFIPM Cryptographic Trust Fabric concept is defined in [GFIPM Terms], and the syntax and semantics of a GFIPM Cryptographic Trust Fabric document are defined in [GFIPM Trust].

3. A TIB must bridge the gap between the user authentication and attribute assertion technologies used by a brokered IDP and the technologies used within a GFIPM federation.

The first two differences are minor, and are described in more detail in Section 4.4. But the third difference can be significant. It is not possible to state definitively how a TIB must broker an IDP at a technical level, since the implementation details for a TIB depend on the technologies used by the brokered IDP. But in general, a TIB must be implemented so as to provide the following assurances to relying parties in its GFIPM federation.

1. Each SAML assertion generated by a TIB within a GFIPM federation must contain accurate information about the authentication event that was used as the basis for generating the assertion. In other words, before generating a SAML assertion, a TIB must have reliable evidence that an authentication event occurred and that the user who authenticated is the user for whom the assertion will be generated.

2. Each SAML assertion generated by a TIB within a GFIPM federation must contain accurate attribute data about the user for whom the assertion was generated.

A GFIPM IDP must also make these assurances, i.e., they are not unique to a TIB. But they are highlighted here because of the nature a TIB and the interfederation relationships that it brokers. A TIB is a trust conduit on which the other federation members rely.

4. Requirements for Trusted Identity Brokers

Based on the interfederation concepts described in the previous section, this section highlights all of the requirements that pertain to TIBOs and TIBs throughout the entire suite of GFIPM normative technical standards and supporting guidelines. Where necessary, it also supplements those documents with additional TIBO-specific and TIB-specific requirements. To fully conform to GFIPM standards, a TIBO or TIB must meet all requirements in this section, as well as all applicable requirements in all GFIPM documents listed in this section.

4.1 GFIPM Governance Guideline

The GFIPM Governance Guideline [GFIPM Gov] document identifies the role of a Trusted Identity Broker Organization in a GFIPM federation. A TIBO must participate in the federation's governance process as defined in this guideline, or as defined in its federation's alternative governance document if the federation does not adopt this guideline.[5]

[5] Documents that are named using "guideline" or "template" represent a recommended solution to a specific aspect of the information sharing problem that GFIPM solves. Use of these documents is not strictly required, and some federations will opt to develop their own solutions in lieu of these documents.

4.2 GFIPM Operational Policies and Procedures Guideline

Section 5 of the GFIPM Operational Policies and Procedures Guideline [GFIPM OPP] describes the GFIPM Federation Membership Processes, which defines a series of processes leading to membership in a GFIPM federation. The current version of [GFIPM OPP] defines these processes for IDPOs (and their IDPs) and SPOs (and their SPs), and TIBOs (and their TIBs). This section reproduces the guidance found in [GFIPM OPP] for TIBOs and their TIBs. A TIBO must follow these processes and procedures if its federation has adopted [GFIPM OPP] as its federation's operational policies and procedures. If its federation has not adopted [GFIPM OPP], then this section does not apply; however, other federation-specific policies may apply to the TIBO in this case.

[GFIPM OPP] defines a sequence of four membership phases.

1. Request-to-Join Process
2. Application Process
3. Onboarding Process
4. Ongoing Membership

The following sections define each phase along with its associated TIBO-specific and TIB-specific requirements and processes.

4.2.1 Request-to-Join Process

The Request-to-Join Process serves as a preliminary qualifications assessment for the application process. The Request-to-Join Process works as follows:

1. The prospective TIBO member organization completes and submits a Request-to-Join Form as a TIBO. Request-to-Join Form templates are available in the Appendix Section of [GFIPM OPP].

2. The federation management organization (FMO) evaluates the Request-to-Join Form and decides if the perspective TIBO member has the required qualifications to submit a formal application for admission to the federation. The FMO may communicate with current federation members, at its discretion, as part of the decision-making process.

3. The FMO notifies the prospective TIBO member of the decision and invites the prospective TIBO member to submit a formal application for admission to the federation if the request to join has been approved. At

this time, the FMO may assign or solicit an existing member to shepherd the prospective TIBO member through the application process.

4.2.2 Application Process

The Application Process is the formal process through which a prospective TIBO member must be admitted to the federation as a TIBO. A prospective member must be approved to submit an application via the Request-to-Join Process before submitting an application for admission.

The Application Process works as follows:

1. The prospective TIBO member completes and submits to the FMO a TIBO application package. The TIBO application package consists of the following contents.

    a. ***Completed Application Form***—a standard form on which an organization provides basic organization information about itself, e.g., name, address, names and titles of its organizational officers.

    b. ***Signed TIBO Agreement***—an agreement signed by a TIBO to indicate its intent and willingness to abide by the governance and rules of the federation.

    c. ***Completed Brokered IDPO Registry Form***—a document that provides the name, description, and identifier of each IDPO that the TIBO will broker.[6]

    d. ***Authority-to-Operate Document(s)***—a document or set of documents attesting to the TIBO's authority to operate as a TIB for the users whose identities it will broker. One document is required for each IDPO (or the IDPO's corresponding legal jurisdiction) that the TIBO will broker.

    e. ***TIBO Local Security Policy Document***—a document describing the security policy currently in place within the TIBO.

    f. ***Brokered IDP Local Security Policy Document(s)***—a document or set of documents describing the security policy or policies currently in place within the IDPOs that the TIBO will broker. One document is required for each brokered IDPO.

[6] The TIB will use the IDP identifiers called out in this form to identify the IDP of a brokered user within a SAML assertion. See Section 4.4 for more information.

g. ***Local User Agreement Document(s)***—a document or set of documents describing the terms and conditions to which users must agree as a prerequisite for using a digital identity issued by each brokered IDPO. One document is required for each IDPO that the TIBO will broker.

h. ***Local User Vetting Policies and Procedures Document(s)***—a document or set of documents describing the user vetting policies and procedures currently in place within each brokered IDPO. One document is required for each IDPO that a TIBO will broker.

i. ***Completed Brokered Attribute Map***—a document describing how the TIBO will map the local policies and local user attributes of its brokered IDPOs into attributes conforming to [GFIPM Meta].

j. ***Completed TIBO Security Practices Checklist***—a checklist that summarizes the TIBO's local security policy. The checklist is "For Information Only." Applicants are not required to check "yes" for all items on the checklist as a prerequisite for membership approval.

k. ***Completed Brokered IDPO Security Practices Checklist(s)***—a checklist that summarizes the local security policy or policies of all IDPOs that the TIBO will broker. One document is required for each brokered IDPO. The checklists are "For Information Only." Applicants are not required to check "yes" for all items on the checklist as a prerequisite for membership approval.

Template forms are located in the Appendix Section of [GFIPM OPP]. In addition, a TIBO Application Package Checklist is available to help track the collection of required documents.

2. The FMO reviews the application package for completeness and requests additional information and documents from the prospective TIBO member as needed. At this time, the FMO provides a copy of the prospective TIBO member's Brokered Attribute Mapping Form to all existing members for review and comment.

3. The FMO performs due diligence on the application package.

4. The FMO generates a recommendation to approve or deny the application and disseminates the recommendation to current federation members and the Board of Directors.[7] To ensure that all federation

[7] If the Federation Management's recommendation is to deny membership to the prospective member, the Federation Management may engage in a dialogue with the prospective member about what actions are

members have been given adequate time to review the prospective TIBO member's Brokered Attribute Mapping Form, the FMO shall refrain from disseminating its recommendation for at least three weeks after distributing those forms to the members.

5. If the FMO recommends approval of the prospective member's application, then the Board of Directors and federation members must be given a three-week period to raise an objection to the approval. If no objections are raised during this period, the FMO shall grant membership to the prospective TIBO member.

    a. If an objection is raised, and the FMO agrees with the objection, the FMO may engage in a dialogue with the prospective TIBO member about what actions are necessary on the part of the prospective member to rectify the problem(s) that prevent approval of its application.

    b. If an objection is raised, and the FMO does not agree with the objection, the matter shall be handled as a dispute between a federation member and the FMO and handled via a Board of Directors vote.

6. The FMO notifies the prospective member of the federation's decision and delivers a letter of membership approval to the prospective TIBO member if the application was approved. If membership is denied, the FMO shall provide the prospective member with a set of recommendations that, if followed, would lead to subsequent approval for membership.

4.2.3 Onboarding Process

After successfully completing the application process, the prospective member is officially a member of the federation. At that time, the new member may begin the Onboarding Process. The Onboarding Process is a sequence of steps and tests that leads to a live, operational connection between the new member's local information systems and the information systems of other federation members.

The onboarding process consists of a set of technical interoperability tests. For a TIB, the process is the same as the process for IDP and, therefore, does not warrant additional explanation beyond the current description in Section 5.3 of [GFIPM OPP].

necessary on the part of the prospective member to rectify the problem(s) that prevent approval of its application.

4.2.4 Ongoing Membership

After becoming a member of the federation, the TIBO is required to notify the FMO of any changes to its local policies and procedures or the local policies and procedures of any of the IDPOs that it brokers, as these may affect the TIBO's standing in the federation as well as the trust relationships between the brokered IDPOs and the relying parties (SPOs) in the federation. Notification of local policy or procedural changes is subject to a submission and approval process that is defined in Section 5.4 of [GFIPM OPP].

4.3 GFIPM Cryptographic Trust Model

The GFIPM Cryptographic Trust Model [GFIPM Trust] document does not currently identify the role of a TIBO or a TIB or call out any TIBO-specific or TIB-specific requirements.[8] To conform to this specification, a TIBO must meet the requirements identified for an IDPO, and a TIB must meet the requirements identified for an IDP.

4.4 GFIPM Metadata Specification, Version 2.0

The GFIPM Metadata Specification, Version 2.0 [GFIPM Meta], provides a dictionary of metadata attributes, including a set of user attributes that IDPs and TIBs may assert on behalf of users. The spec also provides syntactical rules for asserting the values of these attributes. When asserting user attributes on behalf of a user, a TIB may assert any attribute, as long as the information conveyed by the attribute's value is accurate with regard to the user about whom the attribute is asserted.[9] In addition, when asserting the "Federation ID" attribute or the "Identity Provider ID" attribute for a user, a TIB must encode the attribute's value according to the TIB-specific requirements described in the spec. See the definitional content for these attributes at http://gfipm.net/standards/metadata/2.0/user/FederationId.html and http://gfipm.net/standards/metadata/2.0/user/IdentityProviderId.html for more information. Note also that when asserting these values, a TIB must assert IDP identifiers that are consistent with the identifiers it has assigned to each of its brokered IDPs in the Brokered IDP Registry Form that the TIBO submitted during the federation application process. (See Section 4.2.2 for details.)

In addition to user attributes, [GFIPM Meta] also provides a set of entity attributes that a federation manager organization (FMO) may assert on behalf of entities (trusted software endpoints) in a federation within that federation's GFIPM Cryptographic Trust Fabric document. When asserting entity attributes on behalf of a TIB, an FMO must meet the following requirements.

[8] Future versions of [GFIPM Trust] may call out TIBO-specific and/or TIB-specific requirements. If any such changes occur, this document will updated to reflect them.
[9] This requirement also applies to IDPs.

1. When asserting the "Entity ID" attribute for a TIB, the FMO must encode the attribute's value according to the TIB-specific requirements described in the spec. For more information, see the definitional content for this attribute at http://gfipm.net/standards/metadata/2.0/entity/EntityId.html.

2. When asserting the "Technical Role" attribute for a TIB, the FMO must use an attribute value of "TIB" in accordance with the attribute's definition. For more information, see the definitional content for this attribute at http://gfipm.net/standards/metadata/2.0/entity/TechnicalRole.html.

[GFIPM Meta] also provides other types of attributes, including resource attributes, action attributes, and environment attributes. But none of these attributes pertain to IDPs or TIBs.

4.5 GFIPM Federation Certification Practice Statement Template

The GFIPM Federation Certification Practice Statement (CPS) Template [GFIPM CPS] document pertains to the operations of the federation manager organization (FMO) and does not contain any language that constrains the behavior of other organizations in the federation or the systems operated by them. Accordingly, there are no TIBO-specific or TIB-specific requirements in this document.

4.6 GFIPM Federation Member Certificate Policy Template

The GFIPM Federation Member Certificate Policy (CP) Template [GFIPM Member CP] is still under development.

4.7 GFIPM Web Browser User-to-System Profile

The GFIPM Web Browser User-to-System Profile [GFIPM U2S Profile] document does not currently identify the role of a TIBO or a TIB or call out any TIBO-specific or TIB-specific requirements.[10] To conform to this specification, a TIBO must meet the requirements identified for an IDPO, and a TIB must meet the requirements identified for an IDP.

4.8 GFIPM Web Services System-to-System Profile

The GFIPM Web Services System-to-System Profile [GFIPM S2S Profile] is still under development.

[10] Future versions of [GFIPM U2S Profile] may call out TIBO-specific and/or TIB-specific requirements. If any such changes occur, this document will updated to reflect them.

5. References

Document ID	Document Name and URL
GFIPM Gov	GFIPM Governance Guideline http://it.ojp.gov/docdownloader.aspx?ddid=1341
GFIPM OPP	GFIPM Operational Policies and Procedures Guideline http://it.ojp.gov/docdownloader.aspx?ddid=1340
GFIPM Terms	GFIPM Terminology Matrix http://it.ojp.gov/docdownloader.aspx?ddid=1333
GFIPM Meta	GFIPM Metadata Specification, Version 2.0 http://gfipm.net/standards/metadata/2.0/
GFIPM Trust	GFIPM Cryptographic Trust Model http://it.ojp.gov/docdownloader.aspx?ddid=1338
GFIPM CPS	GFIPM Federation Certification Practice Statement Template http://it.ojp.gov/docdownloader.aspx?ddid=1337
GFIPM Member CP	GFIPM Federation Member Certificate Policy Template [To Be Published – URL TBD]
GFIPM U2S Profile	GFIPM Web Browser User-to-System Profile http://it.ojp.gov/docdownloader.aspx?ddid=1336
GFIPM S2S Profile	GFIPM Web Services System-to-System Profile [To Be Published – URL TBD]

Appendix A—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
06/2012	1.0	GSC	Global Advisory Committee 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.