BJA

Bureau of Justice Assistance
U.S. Department of Justice

Federated Identity and Privilege Management

Cryptographic Trust Model

Version 2.0

April 2012

Global
Information
Sharing Standard

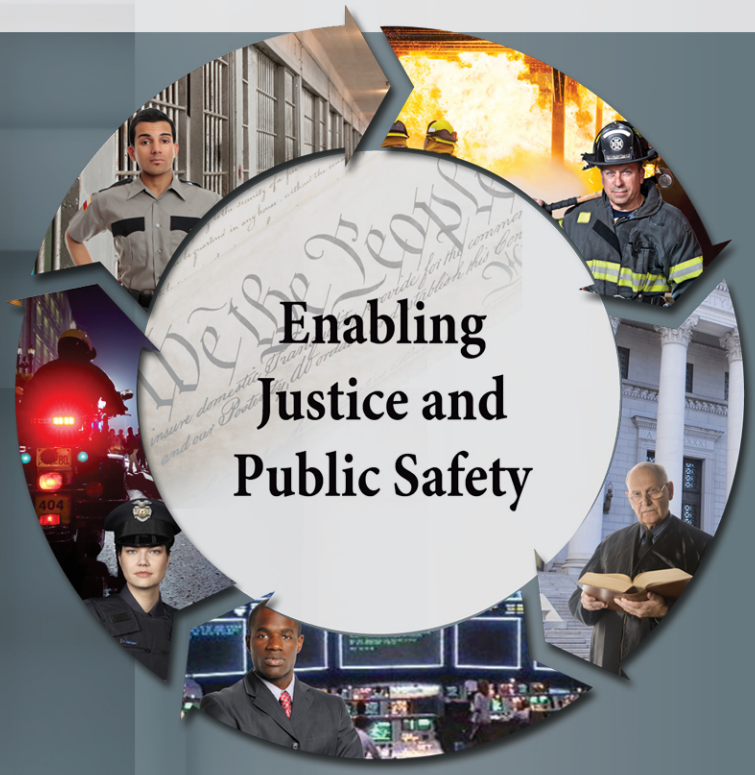
Global Standards

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 Cryptographic Trust Model defines a normative schema for a *GFIPM Cryptographic Trust Fabric*, a document shared among all members of a GFIPM federation. A GFIPM Cryptographic Trust Fabric document contains public key material and system entity metadata for each trusted endpoint in the federation. The spec also defines a set of processes by which the GFIPM Cryptographic Trust Fabric document is

created, distributed, and updated based on changes in federation membership. In addition, it defines a normative set of rules that all federation members must follow during interorganizational transactions to ensure that all transactions properly utilize the Cryptographic Trust Fabric. The standard incorporates normative standards from SAML 2.0 and the GFIPM Metadata 2.0 spec.

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. 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 use 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. The GSC has established a GFIPM Delivery Team to provide oversight and guidance to evolve the initial GFIPM products, specifications, and operational federation into a fully vetted and production-quality capability which can be leveraged across the federal, state, local, and tribal justice and public safety community. Additional information on Global and GFIPM can be found at http://it.ojp.gov/GFIPM.

2. Target Audience and Purpose

This document specifies technical security and interoperability requirements for a GFIPM Cryptographic Trust Model. The purpose of this trust model is to provide a cryptographic foundation for secure communications and information sharing transactions within a GFIPM federation. All GFIPM communication profiles, including the GFIPM Web Browser User-to-System Profile [GFIPM U2S Profile] and the GFIPM Web Services System-to-System Profile [GFIPM S2S Profile], rely on this trust model to provide a cryptographically secure basis for trusted communications between federation participants.

This document's 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.[1] 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.

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

Note that the requirements expressed in this section pertain only to the GFIPM User-to-System use case and do not yet address the GFIPM System-to-System ("Web Services") use case. This document will undergo revision to accommodate the GFIPM System-to-System use case when the necessary requirements have been identified.

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

3. Terminology

This document contains language that uses technical terms related to federations, identity management, 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].

4. References

Table 1, Table 2, and Table 3 contain a list of documents that pertain to the specifications and requirements described in this document (including GFIPM domain-specific standards and industry standards), and a list of reference URLs.

Document References for GFIPM Domain-Specific Standards	
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 IDP AG	GFIPM Federation Identity Provider Agreement
GFIPM SP AG	GFIPM Federation Service Provider Agreement
NIEM 2.1	National Information Exchange Model (NIEM) 2.1 http://www.niem.gov/niem/
GFIPM Meta	GFIPM Metadata 2.0 Specification http://gfipm.net/standards/metadata/2.0/
GFIPM Trust	GFIPM Cryptographic Trust Model (this document)
GFIPM Cert	GFIPM Certification Practice Statement Template
GFIPM U2S Profile	GFIPM Web Browser User-to-System Profile
GFIPM Status	GFIPM System Status Document Schema http://ref.gfipm.net/monitor/schemas/status/GFIPMSystemStatus.xsd
GFIPM S2S Profile	GFIPM Web Services System-to-System Profile

Table 1: Document References for GFIPM Domain-Specific Standards

Document References for Industry Standards	
Document ID	**Document Name and URL**
SAML2 Core	"Assertions and Protocol for the OASIS Security Markup Language (SAML) V2.0" OASIS Standard, 15 March 2005 Document Identifier: saml-core-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
SAML2 Bindings	"Bindings for the OASIS Security Markup Language (SAML) V2.0" OASIS Standard, 15 March 2005 Document Identifier: saml-bindings-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
SAML2 Profiles	"Profiles for the OASIS Security Markup Language (SAML) V2.0" OASIS Standard, 15 March 2005 Document Identifier: saml-profiles-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

Document References for Industry Standards	
SAML2 Metadata	"Metadata for the OASIS Security Markup Language (SAML) V2.0" OASIS Standard, 15 March 2005 Document Identifier: saml-metadata-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
SAML2 Context	"Authentication Context for the OASIS Security Markup Language (SAML) V2.0" OASIS Standard, 15 March 2005 Document Identifier: saml-authn-context-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf
SAML2 Conform	"Conformance Requirements for the OASIS Security Markup Language (SAML) V2.0" OASIS Standard, 15 March 2005 Document Identifier: saml-conformance-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf
SAML2 Security	"Security and Privacy Considerations for the OASIS Security Markup Language (SAML) V2.0" OASIS Standard, 15 March 2005 Document Identifier: saml-sec-consider-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf
SAML2 Glossary	"Glossary for the OASIS Security Markup Language (SAML) V2.0" OASIS Standard, 15 March 2005 Document Identifier: saml-glossary-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf
IDP Disc Profile	Identity Provider Discovery Service Protocol and Profile OASIS Committee Specification 01, 27 March 2008 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery-cs-01.pdf
FISMA	Federal Information Security Management Act http://csrc.nist.gov/sec-cert/
NIST SP 800-52	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations National Institute of Science and Technology (NIST) Special Publication 800-52 http://csrc.nist.gov/publications/nistpubs/
NIST SP 800-63	Electronic Authentication Guideline National Institute of Science and Technology (NIST) Special Publication 800-63 http://csrc.nist.gov/publications/nistpubs/
OMB M-03-22	OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 Office of Management and Budget (OMB) Memorandum M-03-22 http://www.whitehouse.gov/omb/memoranda/m03-22.html
RFC 2459	"RFC 2459— Internet X.509 Public Key Infrastructure Certificate and CRL Profile" Internet RFC/STD/FYI/BCP Archives http://www.ietf.org/rfc/rfc2459.txt
RFC 2119	"RFC 2119—Key Words for Use in RFCs to Indicate Requirement Levels" Internet RFC/STD/FYI/BCP Archives http://www.ietf.org/rfc/rfc2119.txt
FIPS 140-2	Federal Information Processing Standard (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules" http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Table 2: Document References for Industry Standards

Reference URLs	
Topic	**Links**
SAML	http://www.oasis-open.org/home/index.php http://www.oasis-open.org/specs/index.php#samlv2.0 http://www.oasis-open.org/committees/security/ http://www.oasis-open.org/committees/security/docs
XML	http://www.w3.org/ http://www.w3.org/XML/ http://www.w3.org/1999/XMLSchema-instance http://www.w3.org/1999/XMLSchema

Table 3: Reference URLs

5. Notation

This document contains both normative and nonnormative 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].

6. GFIPM Cryptographic Trust Model

All subsections that follow are normative, unless otherwise noted.

6.1 GFIPM Federation Certificate Authority (Nonnormative)

The Federation Management Organization (FMO) of a GFIPM federation typically operates a federation certificate authority (CA) to provide trust and security to the federation. The sole purpose of this CA is to sign the federation's GFIPM Cryptographic Trust Fabric (see Section 6.2). The CA does NOT issue certificates to federation members, and although it is possible for the CA to sign federation members' certificates, it is not required. Trust between federation members is anchored by the federation's GFIPM Cryptographic Trust Fabric document and the CA's signature of the document.

6.2 GFIPM Cryptographic Trust Fabric

At a technical level, trust between all communications endpoints in a GFIPM federation is implemented using the SAML 2.0 standard for federated system entity metadata. This information is delivered to participants via the *GFIPM Cryptographic Trust Fabric* document, which defines the most current cryptographic security context of the federation. The document contains an entry for each communications endpoint in the federation, including identity providers (IDPs), service providers (SPs), Web Service consumers (WSCs), Web Service providers (WSPs), and others. The FMO maintains the document and makes a new version of it available to federation members whenever the membership of the federation changes because of the addition or removal of a communications

endpoint. To ensure compliance with the current federation Trust Fabric, each communications endpoint in a GFIPM federation MUST incorporate the most current version of the GFIPM Cryptographic Trust Fabric document into its security policy decisions in a timely fashion. The FMO shall provide guidance to federation members as to the urgency with which a new Trust Fabric document must be incorporated, at the time the new document is made available. In cases in which the new Trust Fabric document has been published because of a security or trust violation, or because of the removal of a member from the federation for disciplinary reasons, it is imperative that members incorporate the new Trust Fabric document as soon as is reasonably possible, and in any case, not more than 24 hours after its release.

The GFIPM Cryptographic Trust Fabric document conforms to the specification defined in [SAML2 Metadata]. It also uses two extension schemas: one extension defined for the **<idpdisc:DiscoveryResponse>** element, as specified in [IDP Disc Profile], and another extension defined for the <**md:RoleDescriptor**> element, to accommodate the use of GFIPM Cryptographic Trust Fabric with various GFIPM Web Services endpoints.[2] Additional constraints specified in this section also apply to the document within the federation. Appendices A and B contain these two extension schemas.

SAML <EntitiesDescriptor> Element Requirements

The following additional requirements apply to the **<EntitiesDescriptor>** element, which is the top-level XML element within the GFIPM Cryptographic Trust Fabric document. These requirements supplement the requirements described in [SAML2 Metadata].

1. The **Name** attribute within **<EntitiesDescriptor>** MUST be present.

2. The **ID** attribute within **<EntitiesDescriptor>** MUST be present.

3. The **validUntil** attribute within **<EntitiesDescriptor>** MUST be present.

4. The **<ds:Signature>** element within **<EntitiesDescriptor>** MUST be present.

5. The **<Extensions>** element within <**EntitiesDescriptor>** MUST NOT be present.

6. Nested **<EntitiesDescriptor>** elements within the top-level **<EntitiesDescriptor>** MUST NOT be present.

[2] See http://gfipm.net/standards/trust/2.0/gfipm-webservices-trustfabric-2.0.xsd.

7. One or more **<EntityDescriptor>** elements within **<EntitiesDescriptor>** MUST be present.

SAML <EntityDescriptor> Element Requirements

The following requirements apply to **<EntityDescriptor>** elements that appear in the GFIPM Cryptographic Trust Fabric document. Each **<EntityDescriptor>** element provides entity metadata for a specific federation IDP or SP. These requirements supplement the requirements described in [SAML2 Metadata].

1. The **entityID** attribute within **<EntityDescriptor>** MUST be present, and MUST be set to the value that was agreed upon for this entity between the entity and the FMO. (The entity (IDP or SP) chooses its **entityID** value, but the choice MUST be approved by the FMO.)

2. The **<ds:Signature>** element within **<EntityDescriptor>** MUST NOT be present.

3. Each **<EntityDescriptor>** element MUST contain at least one **<IDPSSODescriptor>** element, OR at least one **<SPSSODescriptor>** element, OR at least one **<RoleDescriptor>** element, and MAY contain additional **<IDPSSODescriptor>**, **<SPSSODescriptor>**, or **<RoleDescriptor>** elements.

4. Each **<EntityDescriptor>** element MUST contain at least one **<ContactPerson>** element with each technical **contactType**. An **<EntityDescriptor>** element MAY contain additional **<ContactPerson>** elements.

5. The following requirements apply to each **<ContactPerson>** element within an **<EntityDescriptor>** element.

    a. The **<Extensions>** element MUST NOT be present.

    b. The **<Company>** element MUST be present.

    c. The **<GivenName>** element MUST be present.

    d. The **<SurName>** element MUST be present.

    e. At least one **<EmailAddress>** element is MUST be present.

    f. At least one **<TelephoneNumber>** element MUST be present.

6. The **<AdditionalMetadataLocation>** element within **<EntityDescriptor>** MUST NOT be present.

7. Each **<EntityDescriptor>** element MAY contain one **<Extensions>** element, and the **<Extensions>** element MAY contain one or more **<gfipm:EntityAttribute>** elements as defined by the GFIPM Entity Attribute Extension Schema.[3]

8. Each **<EntityDescriptor>** element MAY contain one **<Organization>** element. If it is present, the **<Organization>** element MAY contain an **<Extensions>** element, and the **<Extensions>** element MAY contain one or more **<gfipm:EntityAttribute>** elements as defined by the GFIPM Entity Attribute Extension Schema.

SAML <IDPSSODescriptor> Element Requirements

The following requirements apply to **<IDPSSODescriptor>** elements that appear in the GFIPM Cryptographic Trust Fabric document. Each **<IDPSSODescriptor>** element provides metadata for the SAML services provided by a specific federation IDP. These requirements supplement the requirements described in [SAML2 Metadata].

1. The **protocolSupportEnumeration** attribute within **<IDPSSODescriptor>** MUST be present, and MUST have "**urn:oasis:names:tc:SAML:2.0:protocol**" as its value.

2. The **WantAuthnRequestsSigned** attribute within **<IDPSSODescriptor>** MUST be present, and "**true**" MUST be its value.

3. The **<ds:Signature>** element within **<IDPSSODescriptor>** MUST NOT be present.

4. Each **<IDPSSODescriptor>** element MAY contain one **<Extensions>** element, and the **<Extensions>** element MAY contain one or more **<gfipm:EntityAttribute>** elements as defined by the GFIPM Entity Attribute Extension Schema.

[3] The GFIPM Entity Attribute Extension Schema is located at [URL]. It defines an XML extension schema to the SAML 2.0 Metadata schema, and is to be used for encoding entity attributes defined in the GFIPM Metadata Specification (versions 2.0 and higher).

5. One or more **<KeyDescriptor>** elements containing a **use** attribute with a value of "**signing**" MUST be present within **<IDPSSODescriptor>**.

6. One **<KeyDescriptor>** element containing a **use** attribute with a value of "**encryption**" MUST be present within **<IDPSSODescriptor>**.

7. The **<ArtifactResolutionService>** element within **<IDPSSODescriptor>** MUST NOT be present.

8. The **<ManageNameIDService>** element within **<IDPSSODescriptor>** MUST NOT be present.

9. Two **<NameIDFormat>** elements MUST be present within **<IDPSSODescriptor>**. One MUST have a value of "**urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**" and "**urn:oasis:names:tc:SAML:2.0:nameid-format:transient**" MUST be the value of the other.

10. One **<SingleSignOnService>** element MUST be present within **<IDPSSODescriptor>**; its **Binding** attribute MUST be present, and "**urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST**" MUST be the value of the **Binding** attribute. Also, its **Location** attribute MUST be present, with a value specifying the live service endpoint (URL) of this IDP's SAML HTTP POST Single Sign-On (SSO) service.

11. A second **<SingleSignOnService>** element MAY be present within **<IDPSSODescriptor>**. If the element is present, "**urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect**" MUST be the value of its **Binding** attribute. Also, its **Location** attribute MUST be present, with a value specifying the live service endpoint (URL) of this IDP's SAML HTTP Redirect Single Sign-On (SSO) service.

12. The **<NameIDMappingService>** element within **<IDPSSODescriptor>** MUST NOT be present.

13. The <**AssertionIDRequestService>** element within **<IDPSSODescriptor>** MUST NOT be present.

14. The **<AttributeProfile>** element within **<IDPSSODescriptor>** MUST NOT be present.

SAML <SPSSODescriptor> Element Requirements

The following requirements apply to **<SPSSODescriptor>** elements that appear in the GFIPM Cryptographic Trust Fabric document. Each **<SPSSODescriptor>** element provides metadata for the SAML services provided by a specific federation SP. These requirements supplement the requirements described in [SAML2 Metadata].

1. The **protocolSupportEnumeration** attribute within **<SPSSODescriptor>** MUST be present, and "**urn:oasis:names:tc:SAML:2.0:protocol**" MUST be its value.

2. The **WantAssertionsSigned** attribute MUST be present within **<SPSSODescriptor>**, and "**true**" MUST be its value.

3. The **<ds:Signature>** element within **<SPSSODescriptor>** MUST NOT be present.

4. The **<Extensions>** element within **<SPSSODescriptor>** MAY be present. If present, it MUST contain exactly one **<idpdisc:DiscoveryResponse>** element. The **Binding** attribute of the **<idpdisc:DiscoveryResponse>** element MUST be present, and "**urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol**" MUST be its value. The **Location** attribute of the **<idpdisc:DiscoveryResponse>** element MUST also be present, and its value MUST contain the URL at which the federation's IDP Discovery Service is expected to respond to this SP during IDP discovery transactions.

5. If the **<Extensions>** element within an **<SPSSODescriptor>** element is present, it MAY contain one or more **<gfipm:EntityAttribute>** elements as defined by the GFIPM Entity Attribute Extension Schema.

6. One or more **<KeyDescriptor>** elements containing a **use** attribute with a value of "**signing**" MUST be present within **<SPSSODescriptor>**.

7. One **<KeyDescriptor>** element containing a **use** attribute with a value of "**encryption**" MUST be present within **<SPSSODescriptor>**.

8. The **<ArtifactResolutionService>** element within **<SPSSODescriptor>** MUST NOT be present.

9. The **<ManageNameIDService>** element within **<SPSSODescriptor>** MUST NOT be present.

10. At least one **<NameIDFormat>** element MUST be present within **<SPSSODescriptor>**. Either "**urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**" or "**urn:oasis:names:tc:SAML:2.0:nameid-format:transient**" MUST be its value.

11. A second **<NameIDFormat>** element MAY be present within **<SPSSODescriptor>**. Either "**urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**" or "**urn:oasis:names:tc:SAML:2.0:nameid-format:transient**" MUST be its value, and it MUST NOT have the same value as the first **<NameIDFormat>** element. The maximum number of **<NameIDFormat>** elements allowed is two.

12. Exactly one **<AssertionConsumerService>** element MUST be present within **<SPSSODescriptor>**. Its **Binding** attribute MUST be present, and "**urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST**" MUST be its value. Also, its **Location** attribute MUST be present, with a value specifying the live service endpoint (URL) of this SP's SAML HTTP POST Assertion Consumer Service.

13. The **<AttributeConsumingService>** element within **<SPSSODescriptor>** MUST NOT be present.

<md:RoleDescriptor> Element Requirements

The following requirements apply to **<RoleDescriptor>** elements that appear in the GFIPM Cryptographic Trust Fabric document. Each **<RoleDescriptor>** element provides metadata for a specific federation Web Services component. These requirements supplement the requirements described in the trust fabric extension schema for GFIPM Web Services.[4]

[4] See http://gfipm.net/standards/trust/2.0/gfipm-webservices-trustfabric-2.0.xsd.

1. The **xsi:type** attribute within **<md:RoleDescriptor>** MUST be present, and its value MUST be one of the following values defined within the trust fabric extension schema for GFIPM Web Services:

   - gfipmws:GFIPMWebServiceConsumerType
   - gfipmws:GFIPMWebServiceProviderType
   - gfipmws:GFIPMAssertionDelegateServiceType

2. The **protocolSupportEnumeration** attribute within **<md:RoleDescriptor>** MUST be present, and its value MUST consist of a list of one or more supported GFIPM Web Services service interaction profiles (SIPs), delimited by spaces (" ") specified using the following URIs.[5,6]

   - http://gfipm.net/standards/webservices/1.0/consumer-provider-sip.html
   - http://gfipm.net/standards/webservices/1.0/user-consumer-provider-sip.html
   - http://gfipm.net/standards/webservices/1.0/trusted-identity-broker-sip.html
   - http://gfipm.net/standards/webservices/1.0/saml-assertion-delegate-service-sip.html

3. The **<Extensions>** element within **<RoleDescriptor>** MAY be present. If the **<Extensions>** element within an **<RoleDescriptor>** element is present, it MAY contain one or more **<gfipm:EntityAttribute>** elements as defined by the GFIPM Entity Attribute Extension Schema.

4. One or more **<KeyDescriptor>** elements containing a **use** attribute with a value of "**signing**" MUST be present within **<RoleDescriptor>**.

5. One **<KeyDescriptor>** element containing a **use** attribute with a value of "**encryption**" MUST be present within **<RoleDescriptor>**.

[5] See [GFIPM S2S Profile] for information about each GFIPM Web Services service interaction profile (SIP), including motivating use cases and normative language.

[6] The list of SIPs below includes only those SIPs for which normative language has been defined as of version 1.0 of [GFIPM S2S Profile]. Subsequent versions of [GFIPM S2S Profile] will contain normative language for additional SIPs, and when those SIPs are available for operational use, this document will be updated to indicate the appropriate URIs to use for them.

6.3 Trust Fabric Lifecycle Management Procedures

This section describes policies and procedures used to manage the GFIPM Cryptographic Trust Fabric ("Trust Fabric"). It includes details about how the Trust Fabric is created and distributed, as well as the conditions under which the Trust Fabric is updated.

6.3.1 Trust Fabric Creation Procedure

Upon the occurrence of a triggering condition for a Trust Fabric update (see Section 6.3.3), the Trust Fabric must be regenerated. The process of generating a new Trust Fabric document consists of two basic operations: editing the document to reflect the desired policy change (e.g., new IDP added to the federation) and digitally signing the new document with the federation CA private key. The following steps describe the process in more detail.

1. Starting with the most recent Trust Fabric document, edit the document as needed to incorporate the necessary changes.

2. Copy the edited Trust Fabric document to a USB flash token.

3. Connect the flash token containing the unsigned Trust Fabric document to the physical machine on which the signing operation will be performed. Also connect the USB flash token containing the CA private key to the machine.[7]

4. Perform the cryptographic signing operation on the Trust Fabric document using the CA private key. At no point during this operation shall the CA private key be copied from the flash token onto any other storage device. Also, at no point during this operation shall the physical machine be connected to a network.

5. Copy the signed Trust Fabric document onto the USB flash token that contains the unsigned Trust Fabric document.

6.3.2 Trust Fabric Distribution Procedure

Upon the occurrence of a triggering condition for a Trust Fabric update (see Section 6.3.3), and after the generation and signing of a new Trust Fabric document (see Section 6.3.1), the new Trust Fabric document must be distributed to all federation members. The following steps describe the process in more detail.

[7] See [GFIPM Cert] for more detail about how the federation's CA private key is managed.

1. Publish the new Trust Fabric document at a well-known URL.[8]

2. Notify all federation members of the new Trust Fabric document via the technical contact points they have provided.

Note that while the integrity of the Trust Fabric document is paramount to the security of the federation, the Trust Fabric need not necessarily be kept confidential. Therefore, it is permissible for the Trust Fabric URL to be publicly accessible, and encryption of the Trust Fabric document is not necessary.

6.3.3 Triggering Conditions for Trust Fabric Updates

The following events shall constitute cause for a Trust Fabric regeneration and redistribution.

1. A new system entity (e.g., IDP, SP, WSC, or WSP) joins the federation.

2. An existing system entity leaves the federation.

3. An existing system entity undergoes a configuration change that affects its entry in the trust fabric (e.g., certificate expiration, migration to a new server, key compromise on a server, etc.).

4. The federation CA public key certificate expires.

5. It is suspected that the federation CA private key has been compromised.

Note that (1) and (2) are usually (but not always) caused when a federation member organization joins or leaves the federation.

6.4 Standard GFIPM Trust and Security Considerations

This section provides basic normative rules regarding the use of cryptography for messages sent within all GFIPM communication profiles. Message senders and recipients MUST obey these rules at all times, unless directed otherwise by a specific communication profile.

6.4.1 Digital Signature Creation and Processing

A message sender must sign all messages, or the appropriate parts thereof according to the rules of the applicable GFIPM communication profile, using the sender's digital signature certificate that appears in the federation's GFIPM Cryptographic Trust Fabric document.

[8] This URL is federation-specific and is beyond the scope of this document.

The digital signature allows the recipient of the message to authenticate the sender and confirm that the message has not been altered since the time of signature.

1. The recipient MUST authenticate the sender and verify the signature upon receipt of the message.

2. The recipient MUST verify that the sender of the message is a current member of the federation (i.e., that the sender is represented in the federation's GFIPM Cryptographic Trust Fabric document).

3. If membership in the federation cannot be determined for the message sender, then the message recipient MUST reject the message.

6.4.2 Message Encryption

Encryption ensures that only the intended recipient can decipher the message and gain access to confidential information in it.

1. For all GFIPM communication profiles, all confidential information in a message MUST be encrypted according to the rules of the applicable communication profile.

2. Unless otherwise stipulated by the applicable GFIPM communication profile, encryption MUST use the public key of the intended recipient's encryption certificate as it appears in the federation's GFIPM Cryptographic Trust Fabric document.

6.4.3 Minimum Required Cryptographic Algorithms

The following are the minimum algorithms required for all communications in GFIPM:

1. Communications MUST use AES with 128 bit keys, or better.

2. Communications MUST use SHA-256 with RSA, or better.

3. A federation member MAY use stronger algorithms than those specified herein, provided that the algorithms are compliant with [FIPS 140-2] and prior arrangements are made with the FMO and partners.

6.5 Conformance With GFIPM Reference Documents (Nonnormative)

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

[GFIPM OPP]), laws and regulations (e.g., [NIST SP 800-63]), and applicable technology standards (e.g., XML standards).

Appendix A—Extension Schema for <idpdisc:DiscoveryResponse>

The diagram below contains the SAML Metadata extension schema for the **<idpdisc:DiscoveryResponse>** element, as specified in [IDP Disc Profile].

```
<schema
targetNamespace="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery- protocol"
xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery- protocol"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns="http://www.w3.org/2001/XMLSchema"
elementFormDefault="unqualified"
attributeFormDefault="unqualified"
blockDefault="substitution"
version="1.0">
<annotation>
<documentation>
Document identifier: sstc-saml-idp-discovery
Location: http://www.oasis-open.org/committees/documents.php? wg_abbrev=security
Revision history:
V1.0 (January 2007):
Initial version.
</documentation>
</annotation>
<import namespace="urn:oasis:names:tc:SAML:2.0:metadata"
schemaLocation="saml-schema-metadata-2.0.xsd"/>
<element name="DiscoveryResponse" type="md:IndexedEndpointType"/>
</schema>
```

Figure 1: Extension Schema for <idpdisc:DiscoveryResponse>

Appendix B—Extension Schema for <md:RoleDescriptor>

The diagram below contains the SAML Metadata extension schema for the **<md:RoleDescriptor>** element, which accommodates the inclusion of GFIPM Web Services endpoints within a GFIPM Cryptographic Trust Fabric document.

```
<?xml version="1.0" encoding="US-ASCII"?>
<xs:schema targetNamespace="http://gfipm.net/standards/trust/2.0/webservices"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:gfipmws="http://gfipm.net/standards/trust/2.0/webservices"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:wsa="http://www.w3.org/2005/08/addressing"
  elementFormDefault="unqualified"
  attributeFormDefault="unqualified"
  version="1.0">

  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:metadata"
                        schemaLocation="saml-schema-metadata-2.0.xsd" />
  <xs:import namespace="http://www.w3.org/2005/08/addressing"
                        schemaLocation="ws-addr.xsd" />

  <!-- Based on WS-Federation Section 3.1.2.1 -->
  <xs:complexType name="WebServiceDescriptorType" abstract="true">
    <xs:complexContent>
      <xs:extension base="md:RoleDescriptorType">
        <xs:attribute name="ServiceDisplayName" type="xs:string" use="optional"/>
        <xs:attribute name="ServiceDescription" type="xs:string" use="optional"/>
    </xs:extension>
    </xs:complexContent>
  </xs:complexType>

  <!-- GFIPM Web Service Provider -->
  <xs:complexType name="GFIPMWebServiceProviderType">
    <xs:complexContent>
      <xs:extension base="gfipmws:WebServiceDescriptorType">
        <xs:sequence>
          <xs:element ref="gfipmws:WebServiceEndpoint"       minOccurs="1"
maxOccurs="unbounded"/>
          <xs:element ref="gfipmws:WSDLURL"                  minOccurs="0"
maxOccurs="unbounded"/>
          <xs:element ref="gfipmws:MetadataExchangeEndpoint" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>

  <xs:element name="WSDLURL"                 type="gfipmws:EndpointType"/>
  <xs:element name="WebServiceEndpoint"      type="gfipmws:EndpointType"/>
  <xs:element name="MetadataExchangeEndpoint" type="gfipmws:EndpointType"/>

  <!-- GFIPM Assertion Delegate Service -->
  <xs:complexType name="GFIPMAssertionDelegateServiceType">
    <xs:complexContent>
      <xs:extension base="gfipmws:WebServiceDescriptorType">
        <xs:sequence>
          <xs:element ref="gfipmws:DelegatedTokenServiceEndpoint" minOccurs="1"
maxOccurs="unbounded"/>
          <xs:element ref="gfipmws:WSDLURL"                       minOccurs="0"
maxOccurs="unbounded"/>
          <xs:element ref="gfipmws:MetadataExchangeEndpoint"      minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
```

```
  <xs:element name="DelegatedTokenServiceEndpoint" type="gfipmws:EndpointType" />

  <!-- GFIPM Web Service Consumer -->
  <xs:complexType name="GFIPMWebServiceConsumerType">
    <xs:complexContent>
      <xs:extension base="gfipmws:WebServiceDescriptorType">
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>

  <!-- Based on Section 3.1.4 from the WS-Federation Schmeas -->
  <xs:complexType name="EndpointType">
    <xs:sequence>
      <xs:element ref="wsa:EndpointReference" minOccurs="1" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>
```

Figure 2: Extension Schema for <md:RoleDescriptor>

Appendix C—Sample Trust Fabric Document Contents

The figure below contains content that conforms to the normative rules specified in Section 6.2 regarding the structure of a GFIPM Trust Fabric Document.

```
<?xml                    version="1.0"                    encoding="UTF-8"?><md:EntitiesDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity"
xmlns:gfipmws="http://gfipm.net/standards/trust/2.0/webservices"
xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"       xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  Name="global:gfipm:ref"  validUntil="2011-
08-01T00:00:00Z"  xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata  saml-schema-metadata-
2.0.xsd              urn:mace:shibboleth:metadata:1.0              shibboleth-metadata-1.0.xsd
http://www.w3.org/2000/09/xmldsig#                          xmldsig-core-schema.xsd"><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI="">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha384"/>
<ds:DigestValue>ZCMByWzEfjIpcyZ34wMR0o6tdbzb82MMdyCjal8ZYH1b0AstGrmo4gBT1LxmhVFj</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
 <!—snipped for brevity -->
</ds:SignatureValue>
<ds:KeyInfo>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:Modulus>
<!—snipped for brevity -->
</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
<ds:X509Data>
<ds:X509Certificate>
<!—snipped for brevity -->
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>

  <md:EntityDescriptor entityID="https://rhelidp.ref.gfipm.net/shibboleth">
      <md:Extensions>
        <gfipmentity:EntityAttribute
Name="gfipm:2.0:entity:OwnerAgencyOrganizationGeneralCategoryCode"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
          <gfipmentity:EntityAttributeValue  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
            Private Industry
          </gfipmentity:EntityAttributeValue>
        </gfipmentity:EntityAttribute>
        <gfipmentity:EntityAttribute               Name="gfipm:2.0:entity:OwnerAgencySubUnitName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
          <gfipmentity:EntityAttributeValue  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
            GTRI Reference Federation
          </gfipmentity:EntityAttributeValue>
        </gfipmentity:EntityAttribute>
```

```
        <gfipmentity:EntityAttribute                        Name="gfipm:2.0:entity:OwnerAgencyORI"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
          <gfipmentity:EntityAttributeValue  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
            GA012345
          </gfipmentity:EntityAttributeValue>
        </gfipmentity:EntityAttribute>
      </md:Extensions>
    <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:Extensions>
        <gfipmentity:EntityAttribute                              Name="gfipm:2.0:entity:EntityId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
          <gfipmentity:EntityAttributeValue  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
            GFIPM:IDP:Reference
          </gfipmentity:EntityAttributeValue>
        </gfipmentity:EntityAttribute>
      </md:Extensions>
      <md:KeyDescriptor use="signing">
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:X509Data>
            <ds:X509Certificate>
              <!-- Certificate Removed for Brevity -->
            </ds:X509Certificate>
          </ds:X509Data>
       </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:SingleLogoutService        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://rhelidp.ref.gfipm.net/idp/profile/SAML2/Redirect/SLO"/>
      <md:SingleLogoutService            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://rhelidp.ref.gfipm.net/idp/profile/SAML2/POST/SLO"/>
      <md:SingleSignOnService            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://rhelidp.ref.gfipm.net/idp/profile/SAML2/POST/SSO"/>
      <md:SingleSignOnService        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://rhelidp.ref.gfipm.net/idp/profile/SAML2/Redirect/SSO"/>
    </md:IDPSSODescriptor>

    <md:RoleDescriptor  ServiceDescription="The  Assertion  Delegate  Service  for  the  RHEL  IDP"
ServiceDisplayName="ADS                                  for                                  RHELIDP"
protocolSupportEnumeration="http://gfipm.net/standards/webservices/1.0/saml-assertion-delegate-
service-sip.html" xsi:type="gfipmws:GFIPMAssertionDelegateServiceType">
      <md:KeyDescriptor use="signing">
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:X509Data>
            <ds:X509Certificate>
              <!-- Certificate Removed for Brevity -->
            </ds:X509Certificate>
          </ds:X509Data>
       </ds:KeyInfo>
      </md:KeyDescriptor>

      <gfipmws:DelegatedTokenServiceEndpoint xmlns:wsa="http://www.w3.org/2005/08/addressing">

<wsa:EndpointReference><wsa:Address>https://url/service</wsa:Address></wsa:EndpointReference>
      </gfipmws:DelegatedTokenServiceEndpoint>
    </md:RoleDescriptor>

    <md:Organization>
      <md:OrganizationName xml:lang="en-US">Georgia Tech Research Institute</md:OrganizationName>
      <md:OrganizationDisplayName xml:lang="en-US">GTRI</md:OrganizationDisplayName>
      <md:OrganizationURL xml:lang="en-US">http://www.gtri.gatech.edu/</md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="administrative">
      <md:Company>Georgia Tech Research Institute</md:Company>
      <md:GivenName>Jeffrey</md:GivenName>
      <md:SurName>Krug</md:SurName>
      <md:EmailAddress>jeff.krug@gtri.gatech.edu</md:EmailAddress>
      <md:TelephoneNumber>4044077903</md:TelephoneNumber>
    </md:ContactPerson>
```

```
  </md:EntityDescriptor>

  <md:EntityDescriptor entityID="GFIPM:SP:ReferenceSP">
    <md:Extensions>
      <gfipmentity:EntityAttribute
Name="gfipm:2.0:entity:OwnerAgencyOrganizationGeneralCategoryCode"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
        <gfipmentity:EntityAttributeValue    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
          Local Government
        </gfipmentity:EntityAttributeValue>
      </gfipmentity:EntityAttribute>
      <gfipmentity:EntityAttribute                                    Name="gfipm:2.0:entity:EntityId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
        <gfipmentity:EntityAttributeValue    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
          GFIPM:SP:ReferenceSP
        </gfipmentity:EntityAttributeValue>
      </gfipmentity:EntityAttribute>
      <gfipmentity:EntityAttribute                 Name="gfipm:2.0:entity:OwnerAgencySubUnitName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
        <gfipmentity:EntityAttributeValue    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
          GTRI Reference Federation
        </gfipmentity:EntityAttributeValue>
      </gfipmentity:EntityAttribute>
    </md:Extensions>
    <md:SPSSODescriptor          protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol">
              <md:Extensions>
                <gfipmentity:EntityAttribute                    Name="gfipm:2.0:entity:EntityId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
                      <gfipmentity:EntityAttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
                        GFIPM:SP:ReferenceSP
                      </gfipmentity:EntityAttributeValue>
                </gfipmentity:EntityAttribute>
              </md:Extensions>
      <md:KeyDescriptor use="signing">
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>
              <!-- Certificate Removed for Brevity -->
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>

      <md:KeyDescriptor use="encryption">
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>
              <!-- Certificate Removed for Brevity -->
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>

      <md:SingleLogoutService                 Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SLO/SOAP"/>
      <md:SingleLogoutService        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SLO/Redirect"/>
      <md:SingleLogoutService            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SLO/POST"/>
      <md:SingleLogoutService        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SLO/Artifact"/>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
```

```
      <md:AssertionConsumerService       Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SAML2/POST" index="1" isDefault="true"/>
    </md:SPSSODescriptor>

    <md:RoleDescriptor  ServiceDescription="Sample  Metadata  for  a  GFIPM  Web  Service  Consumer"
ServiceDisplayName="Web                                Service                                Consumer"
protocolSupportEnumeration="http://gfipm.net/standards/webservices/1.0/consumer-provider-sip.html
http://gfipm.net/standards/webservices/1.0/user-consumer-provider-sip.html"
xsi:type="gfipmws:GFIPMWebServiceConsumerType">
      <md:KeyDescriptor use="signing">
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:X509Data>
            <ds:X509Certificate>
              <!-- Certificate Removed for Brevity -->
            </ds:X509Certificate>
          </ds:X509Data>
       </ds:KeyInfo>
      </md:KeyDescriptor>

    </md:RoleDescriptor>

    <md:ContactPerson contactType="technical">
      <md:SurName>GFIPM Tech Support</md:SurName>
      <md:EmailAddress>gfipm-support@lists.gatech.edu</md:EmailAddress>
    </md:ContactPerson>
  </md:EntityDescriptor>

   <md:EntityDescriptor entityID="net:id:entityid:saml:organization">
      <md:Extensions>
        <gfipmentity:EntityAttribute
Name="gfipm:2.0:entity:OwnerAgencyOrganizationGeneralCategoryCode"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
          <gfipmentity:EntityAttributeValue  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
            Local Government
          </gfipmentity:EntityAttributeValue>
        </gfipmentity:EntityAttribute>
        <gfipmentity:EntityAttribute               Name="gfipm:2.0:entity:OwnerAgencySubUnitName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
          <gfipmentity:EntityAttributeValue  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
            GTRI Reference Federation
          </gfipmentity:EntityAttributeValue>
        </gfipmentity:EntityAttribute>
      </md:Extensions>
    <md:SPSSODescriptor          protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol">
      <md:Extensions>
        <gfipmentity:EntityAttribute                                Name="gfipm:2.0:entity:EntityId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
          <gfipmentity:EntityAttributeValue  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
            GFIPM:SP:ExampleOrg
          </gfipmentity:EntityAttributeValue>
        </gfipmentity:EntityAttribute>
      </md:Extensions>

      <md:KeyDescriptor use="signing">
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>
              <!-- Certificate Removed for Brevity -->
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>

      <md:KeyDescriptor use="encryption">
```

```
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>
              <!-- Certificate Removed for Brevity -->
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>

      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
      <md:AssertionConsumerService       Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SAML2/POST" index="1" isDefault="true"/>
    </md:SPSSODescriptor>

    <md:RoleDescriptor  ServiceDescription="Sample  Metadata  for  a  GFIPM  Web  Service  Provider"
ServiceDisplayName="WebServiceProvider"
protocolSupportEnumeration="http://gfipm.net/standards/webservices/1.0/user-consumer-provider-
sip.html" xsi:type="gfipmws:GFIPMWebServiceProviderType">
      <md:KeyDescriptor use="signing">
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:X509Data>
            <ds:X509Certificate>
              <!-- Certificate Removed for Brevity -->
            </ds:X509Certificate>
          </ds:X509Data>
       </ds:KeyInfo>
      </md:KeyDescriptor>

      <gfipmws:WebServiceEndpoint xmlns:wsa="http://www.w3.org/2005/08/addressing">

<wsa:EndpointReference><wsa:Address>https://url/service</wsa:Address></wsa:EndpointReference>
      </gfipmws:WebServiceEndpoint>

      <gfipmws:WSDLURL xmlns:wsa="http://www.w3.org/2005/08/addressing">

<wsa:EndpointReference><wsa:Address>https://url/service/service.wsdl</wsa:Address></wsa:EndpointR
eference>
      </gfipmws:WSDLURL>

      <gfipmws:MetadataExchangeEndpoint xmlns:wsa="http://www.w3.org/2005/08/addressing">

<wsa:EndpointReference><wsa:Address>https://url/service</wsa:Address></wsa:EndpointReference>
      </gfipmws:MetadataExchangeEndpoint>

    </md:RoleDescriptor>

    <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:Extensions>
        <gfipmentity:EntityAttribute                              Name="gfipm:2.0:entity:EntityId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
xmlns:gfipmentity="http://gfipm.net/standards/metadata/2.0/entity">
          <gfipmentity:EntityAttributeValue  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
            GFIPM:IDP:ExampleOrg
          </gfipmentity:EntityAttributeValue>
        </gfipmentity:EntityAttribute>
      </md:Extensions>
      <md:KeyDescriptor use="signing">
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:X509Data>
            <ds:X509Certificate>
              <!-- Certificate Removed for Brevity -->
            </ds:X509Certificate>
          </ds:X509Data>
       </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:SingleLogoutService        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://rhelidp.ref.gfipm.net/idp/profile/SAML2/Redirect/SLO"/>
      <md:SingleLogoutService            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://rhelidp.ref.gfipm.net/idp/profile/SAML2/POST/SLO"/>
```

```
      <md:SingleSignOnService            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://rhelidp.ref.gfipm.net/idp/profile/SAML2/POST/SSO"/>
      <md:SingleSignOnService        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://rhelidp.ref.gfipm.net/idp/profile/SAML2/Redirect/SSO"/>
    </md:IDPSSODescriptor>

    <md:ContactPerson contactType="technical">
      <md:GivenName>First Name</md:GivenName>
      <md:SurName>Last Name</md:SurName>
      <md:EmailAddress>e-mail address</md:EmailAddress>
    </md:ContactPerson>
  </md:EntityDescriptor>

</md:EntitiesDescriptor>
```

Figure 3: Example of GFIPM Trust Fabric Document Contents

Appendix D—Document History

Date	Version	Editor	Change
04/12/2012	2.0	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.