Bureau of Justice Assistance
U.S. Department of Justice

Federated Identity and Privilege Management

Web Browser User-To-System Profile

Version 1.2

April 2012

Global Justice Information Sharing Initiative

Global
Information
Sharing Standard

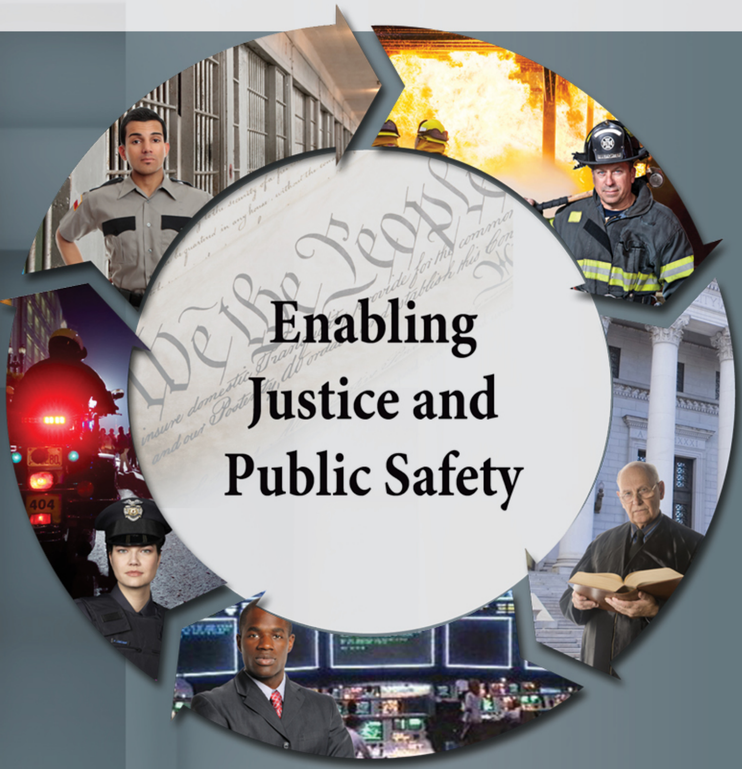
Global Standards

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 Web Browser User-to-System Profile is a normative specification that defines a set of protocols and bindings for Web browser-based interaction between users and resources across trust domains within a federation. It leverages parts of the SAML 2.0 specification, specifically Web Single Sign-On (SSO) and Single Log-Out (SLO). It also leverages the GFIPM Core Technical Standards and Guidelines.

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 that 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 interoperability requirements for connection to an operational GFIPM federation in the Web Browser User-to-System use case.[1] For the purpose of this document, all references to the concept of "joining" the federation are meant to imply connection to an operational GFIPM federation. The target audience includes technical representatives of prospective federation participants who intend to join a GFIPM federation as identity provider organizations (IDPOs), service provider organizations (SPOs), or both.[2] It also includes vendors, contractors, and consultants who, as part of their project or product implementation, have a requirement to establish technical interoperability with a GFIPM federation.

The GFIPM project provides a free, open-source federation middleware solution that conforms to this document, for both identity providers (IDPs) and service providers (SPs). Participants may choose to use other commercial products in a GFIPM federation as long as they can be configured to conform to the interoperability requirements provided in this document.

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

[1] The Web Browser User-to-System use case, covered in this document, is one of two basic GFIPM use cases. The other is the Web Services System-to-System use case, which is covered in [GFIPM S2S Profile].

[2] 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 http://it.ojp.gov/docdownloader.aspx?ddid=1334
GFIPM Terms	GFIPM Terminology Matrix http://it.ojp.gov/docdownloader.aspx?ddid=1333
GFIPM Gov	GFIPM Governance Guideline http://it.ojp.gov/docdownloader.aspx?ddid=1341
GFIPM OPP	GFIPM Operational Policies and Procedures Guidelines http://it.ojp.gov/docdownloader.aspx?ddid=1340
GFIPM IDPO AG	GFIPM Federation Identity Provider Organization Agreement [URL TBD]
GFIPM SPO AG	GFIPM Federation Service Provider Organization Agreement [URL TBD]
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 http://it.ojp.gov/docdownloader.aspx?ddid=1338
GFIPM Cert	GFIPM Certification Practice Statement Template http://it.ojp.gov/docdownloader.aspx?ddid=1337
GFIPM U2S Profile	GFIPM Web Browser User-to-System Profile (this document) http://it.ojp.gov/docdownloader.aspx?ddid=1336
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 [URL TBD]

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
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

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/tc_home.php?wg_abbrev=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 Web Browser User-to-System Profile

The GFIPM Web Browser User-to-System Profile builds upon the SAML 2.0 suite of specifications. This profile further specifies and constrains usage of particular SAML features, elements, attributes, URIs, or other values that are required within a GFIPM federation. Where this specification does not explicitly provide SAML guidance, one must implement in accordance with applicable OASIS SAML 2.0 requirements.

For purposes of this section and its subsections, Transport Layer Security (TLS) includes Secure Sockets Layer (SSL) version 3.01.

Also, throughout this section and its subsections, the following definitions apply:

1. *An **Identity Provider (IDP)** is a service that implements SAML 2.0 Identity Provider endpoint functionality.*

2. *A **Service Provider (SP)** is a service that implements SAML 2.0 Service Provider endpoint functionality.*

The above definitions serve to distinguish the concept of an identity provider (IDP) or a service provider (SP) as a SAML protocol endpoint from the concept of an identity provider organization (IDPO) or service provider organization (SPO) as a member agency within a GFIPM federation. ***All IDP and SP requirements listed in this section and its subsections pertain specifically to IDP and SP protocol endpoints.*** Additional cryptographic and policy-level requirements apply to GFIPM member agencies that wish to participate in a GFIPM federation as an IDP or SP. See Section 6.14 for additional information. Also, see [GFIPM Terms] for further information about GFIPM terminology used to distinguish technical roles (e.g., IDP and SP) from organizational roles (e.g., IDPO and SPO).

All subsections that follow are normative, unless otherwise noted.

6.1 Presentation and User Interface

IDP Requirements

1. An IDP MAY provide a Web interface that allows the user to initiate a single sign-on transaction directly with the IDP.[3]

2. If an IDP provides a Web interface to allow the user to initiate a single sign-on transaction directly with the IDP, then the following requirements apply.

   a. When a user arrives at an IDP without a SAML **<AuthnRequest>**,[4] the IDP MUST display a list of compatible SPs in the federation from which the user can select.[5] Upon user selection of an SP from this list,

[3] This requirement encompasses the "IDP-First" SAML 2.0 Web SSO use case. It is optional for two reasons. First, implementing it can potentially require a substantial amount of effort, both initially and on an ongoing basis. Second, for interoperability purposes, it is not necessary that all IDPs support this use case. It is, however, necessary for all SPs to support this use case by accepting both solicited and unsolicited SAML **<Response>** messages. This requirement is part of the SAML 2.0 standard and is also covered implicitly in Section 6.3 of this document.

[4] A user would arrive at an IDP without a SAML **<AuthnRequest>** if the user navigated directly to the IDP without navigating to an SP first.

[5] This requirement is necessary because it is of little value to allow a user to directly authenticate to an IDP without offering the user a choice of actions to take after authenticating. An IDP can populate this list of SPs using its latest version of the GFIPM Cryptographic Trust Fabric document. See [GFIPM Trust] for more information.

the IDP MUST send an unsolicited SAML **<Response>** that includes an **<Assertion>** to the selected SP.[6]

b. In addition to listing all compatible SPs in the federation, an IDP MAY also list specific SP resources for which it knows the URL.

SP Requirements

1. An SP MUST provide a link that the user can select to initiate a single sign-on transaction.

2. Upon user selection of an IDP, the SP MUST initiate a SAML **<AuthnRequest>** to the selected IDP. See Section 6.2 for more information about user selection of an IDP (also known as IDP Discovery). See Section 6.3 for more information about **<AuthnRequest>** requirements.

6.2 IDP Discovery

1. An SP MUST provide a mechanism through which it can discover the user's IDP. There are two implementation choices for this. One is to communicate with the federation's centralized IDP Discovery Service, if the federation provides such a service. The other is to implement a local IDP Discovery Service at the SP.

2. If an SP implements IDP discovery via the federation's centralized IDP Discovery Service, it MUST act in conformance with the Service Provider behavior as defined in the Identity Provider Discovery Protocol and Profile [IDP Disc Profile]. Also, if an SP chooses to use the federation's centralized IDP Discovery Service, then it must provide appropriate federated system entity metadata as needed for interoperability with that service. (See [GFIPM Trust] and Section 6.9 for more details about the federated system entity metadata required for this.)

3. If an SP implements IDP discovery via a local IDP Discovery Service, it MAY store a cookie in the user's browser reflecting the user's IDP choice. This cookie MUST be set to expire at the end of the user's browser session.

[6] Prior to sending a SAML **`<Response>`** with an **`<Assertion>`** to the SP, an IDP MUST ensure that the user has authenticated successfully to it. This requirement is implied here because it is part of the SAML 2.0 standard.

6.3 Use of SAML 2.0 Web SSO Profile

SAML <AuthnRequest> Element Requirements

1. An SP MUST form a **<AuthnRequest>** message in accordance with the SAML 2.0 Web Browser SSO Profile.

2. An IDP MUST accept **<AuthnRequest>** messages via the HTTP POST binding, using HTTPS (HTTP over TLS). In addition, an IDP MAY accept **<AuthnRequest>** messages via the HTTP Redirect binding, using HTTPS (HTTP over TLS).

3. An SP MUST send **<AuthnRequest>** messages to an IDP using a binding supported by that IDP.

4. All **<AuthnRequest>** messages MUST be signed by the SP to ensure message integrity and to authenticate the SP to the IDP.

5. All **<AuthnRequest>** messages MUST be communicated from SP to browser and from browser to IDP using Transport Layer Security (TLS).

6. All **<AuthnRequest>** messages MUST be delivered to the SSO Service of the IDP using TLS.

7. Certificates used to protect both TLS channels (from SP to browser and from browser to IDP) MUST be trusted by default in commonly used browsers.

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

9. The **Version** attribute within **<AuthnRequest>** MUST have "**2.0**" as its value.

10. If the **<AuthnRequest>** element contains a **<NameIDPolicy>** element, then **<NameIDPolicy>** MUST conform to the following requirements.

    a. If the **Format** attribute is present, then 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.

   b. The **SPNameQualifier** attribute MUST NOT be present.

11. When a user has an extended session with or has been inactive at the SP for some time, the SP may wish to refresh the authentication of the user. In that case, the SP MAY issue an **<AuthnRequest>** message with the **ForceAuthn** attribute set to true. If the **IsPassive** attribute is present, it MUST be set to false. **ForceAuthn** MAY be used to require the IDP to force the user to authenticate to the IDP regardless of the user's authentication session status at the IDP.

12. An **<AuthnRequest>** MUST NOT contain any of the following elements **<Subject>**, **<RequestedAuthnContext>**, **<Scoping>**, or **<Extensions>**.

13. An **<AuthnRequest>** MUST NOT contain an **AttributeConsumingServiceIndex** attribute.

14. If an **<AuthnRequest>** contains a **ProtocolBinding** attribute, then "**urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST**" MUST be the attribute's value.

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

SAML <Response> Element Requirements

1. The IDP MUST create a **<Response>** message in accordance with the SAML 2.0 Web Browser SSO Profile.

2. An IDP MUST send **<Response>** messages via the HTTP POST binding, using HTTPS (HTTP over TLS).

3. An SP MUST accept **<Response>** messages via the HTTP POST binding, using HTTPS (HTTP over TLS).

4. All **<Response>** messages MUST be signed by the IDP to ensure message integrity and to authenticate the IDP to the SP.

5. All **<Response>** messages MUST be communicated from IDP to browser and from browser to SP using Transport Layer Security (TLS).

6. All **<Response>** messages MUST be delivered to the Assertion Consumer Service of the SP using TLS.

7. Certificates used to protect both TLS channels (from IDP to browser and from browser to SP) MUST be trusted by default in commonly used browsers.

8. If sending an unsolicited **<Response>**, an IDP MAY include the URL of an SP resource selected by the user in the **RelayState** form field parameter.

9. The **Version** attribute within **<Response>** MUST have "**2.0**" as its value.

10. A **<Response>** MUST NOT contain an **<Extensions>** element or an **<Assertion>** element.

11. A **<Response>** MUST contain exactly one **<EncryptedAssertion>** element. When decrypted, its contents MUST conform to the requirements specified below regarding the SAML **<Assertion>** element.

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

SAML <Assertion> Element Requirements

After all processing rules have been completed in accordance with the SAML 2.0 specifications, and the IDP is satisfied that an **<Assertion>** can be made about the user, it MUST conform to the following requirements.

1. The IDP MUST create an **<Assertion>** element.

2. An **<Assertion>** element MUST be signed, encrypted, and included within a **<Response>** element in an **<EncryptedAssertion>** element.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15. The **<AttributeStatement>** element in an **<Assertion>** MAY contain one or more **<Attribute>** elements and MUST NOT contain any **<EncryptedAttribute>** elements.[7]

16. Each **<Attribute>** element MAY contain application-level user attribute data corresponding to a GFIPM user attribute defined in [GFIPM Meta].[8]

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

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

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

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

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

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

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

6.4 Use of SAML 2.0 Single Logout (SLO) Profile

The SAML 2.0 Single Logout (SLO) Profile provides a means by which all session participants (a user's IDP and all SPs at which the user has a local session associated with

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

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

his or her IDP authentication session) can terminate their sessions near-simultaneously for a specific user upon that user's request.

At the time of publication of this document, it is well known that not all SAML 2.0-conformant products fully support the SAML 2.0 SLO profile. In addition, it is well known that properly integrating the SAML 2.0 SLO feature into an IDP or SP requires more work than simply integrating the SAML Web SSO Profile. The requirements that follow are intended to foster a federation environment in which SLO is supported to the greatest extent possible in a GFIPM federation, while still allowing for the possibility that not all IDPs and SPs in the federation necessarily support it, in a manner that is user-friendly and supports appropriate and accepted best practices for user session security.

Single Logout User Interface Requirements

1. After a user has established a session at an IDP or SP, the IDP or SP MUST offer the user a clickable logout function. The type of logout may be either simple logout (logging out only from the local IDP or SP) or single logout (logging out of all SP sessions associated with a particular session at the user's IDP, and also logging out of the associated IDP authentication session). An IDP or SP MAY offer both types of logout but MUST offer at least one.

2. If the user selects an IDP's or SP's simple logout function, the IDP or SP MUST present the user with a warning message indicating that the user is being logged out only at the local IDP or SP, and not at all federation resources. This warning message MUST include text that instructs the user to close the browser for security reasons unless the user specifically wants to continue using other federation sessions.

3. If the user selects an IDP's or SP's single logout function, the IDP or SP MUST inform the user that he will be logged out of all active SP sessions and the associated IDP session. The user MUST confirm the request before the IDP or SP may proceed with a SAML Single Logout Protocol transaction. After the user has confirmed the request, the IDP or SP MUST initiate a SAML 2.0 Single Logout Protocol transaction with other session participants that are capable of participating in the protocol, as described in [SAML2 Core].

4. If a single logout transaction fails in any way (i.e., it does not successfully result in the appropriate termination of the user's sessions at all session participants, either because of an unsuccessful Single Logout Protocol transaction or because one or more session participants do not support the Single Logout Protocol), then the IDP or SP that first detects the failure MUST present the user with a warning message indicating that the

single logout transaction was not completely successful. This warning message MUST include text that instructs the user to close the browser for security reasons.

SAML <LogoutRequest> Element Requirements

1. All **<LogoutRequest>** messages MUST be communicated using the HTTP Redirect binding, using HTTPS (HTTP over TLS).

2. All **<LogoutRequest>** messages MUST be signed.

3. The **Version** attribute within **<LogoutRequest>** MUST have "**2.0**" as its value.

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

SAML <LogoutResponse> Element Requirements

1. All **<LogoutResponse>** messages MUST be communicated using the HTTP Redirect binding, using HTTPS (HTTP over TLS).

2. All **<LogoutResponse>** messages MUST be signed.

3. The Version attribute within **<LogoutResponse>** MUST have "**2.0**" as its value.

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

6.5 Use of Other SAML 2.0 Profiles (Nonnormative)

The only SAML 2.0 profiles used in the GFIPM Web Browser User-to-System Profile are the Web Single Sign-On (SSO) Profile and the Single Logout (SLO) Profile. Specifically, the following SAML 2.0 profiles (defined in [SAML2 Profiles]) are NOT used in the GFIPM Web Browser User-to-System Profile.[9]

[9] Use of any of the SAML profiles listed in this section is not prohibited within a GFIPM federation; however, any IDP or SP that makes use of profiles listed in this section MUST NOT require other IDPs or SPs in the federation to use them.

1. Enhanced Client or Proxy (ECP) Profile

2. Identity Provider Discovery Profile[10]

3. Name Identifier Management Profile

4. Artifact Resolution Profile

5. Assertion Query/Request Profile

6. Name Identifier Mapping Profile

7. SAML Attribute Profiles:
    a. Basic Attribute Profile
    b. X.500/LDAP Attribute Profile
    c. UUID Attribute Profile
    d. DCE PAC Attribute Profile
    e. XACML Attribute Profile

6.6 Use of GFIPM User Metadata

The GFIPM Metadata 2.0 Specification [GFIPM Meta] defines a standard syntax and semantics for a comprehensive set of metadata attributes about users. The purpose of the standard is to provide a means for IDPs to clearly and unambiguously communicate vital information about users to SPs. This user metadata MAY be used by SPs for various purposes, including identifying the user, evaluating access control logic, populating audit logs, establishing local user accounts, and anything else that does not violate the GFIPM Federation Service Provider Organization Agreement [GFIPM SPO AG].

6.7 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. Possession of a valid certificate issued by the federation CA is necessary but not sufficient to demonstrate membership in the federation. (It is also necessary to have an entry in the GFIPM Cryptographic Trust Fabric document. See [GFIPM Trust] and Section 6.9 for details.) The FMO issues one certificate to each SP and one certificate to each IDP. Certificates are to be used for both digital signing and encryption as required within SAML message exchanges. These certificates must be maintained in compliance with the policies stipulated in [GFIPM Cert].

[10] Note that the SAML 2.0 Identity Provider Discovery Profile is not the same as the OASIS Identity Provider Discovery Protocol and Profile, which is described normatively in [IDP Disc Profile].

6.8 Presence in GFIPM Trust Fabric

Every IDP and SP in the federation MUST have an entry in the GFIPM Cryptographic Trust Fabric document. See [GFIPM Trust] for details about the format of the GFIPM Cryptographic Trust Fabric document.

6.9 Providing Federated System Entity Metadata to the FMO

[GFIPM Trust] describes syntactical requirements for the GFIPM Cryptographic Trust Fabric document. As this document is produced by the FMO and comprises metadata about each IDP and SP within federation, it is the responsibility of each IDP and SP to provide specific metadata to the FMO upon first joining the federation and on an ongoing basis thereafter any time that the metadata changes.

This section captures specific requirements of IDPs and SPs related to the metadata that they must provide about themselves to the FMO.

1. Each IDP and SP must provide information about itself to the FMO, both upon first joining the federation and on an ongoing basis thereafter, whenever the information changes.

2. Each IDP MUST provide the FMO with the following information about itself, unless otherwise indicated via the word [**OPTIONAL**].

    a. Proposed **entityID** for this IDP. This is typically the URL of the host on which the IDP software resides; however, it need not be a resolvable URL.

    b. Contact information for at least one technical contact person, including first name, last name, company name, e-mail address, and phone number.

    c. X.509 certificate signing request (CSR) for the public key that will be used by this IDP to sign SAML messages.[11]

    d. Service endpoint (URL) for this IDP's SAML HTTP POST Single Sign-On (SSO) service.

    e. [**OPTIONAL**] Additional technical points of contact, as well as nontechnical points of contact. Each point of contact provided must

[11] [GFIPM Cert] contains a detailed description of the practices that must be followed by an IDP or SP when generating a certificate-signing request (CSR).

contain first name, last name, company name, e-mail address, and phone number.

f. [**OPTIONAL**] X.509 certificate signing request (CSR) for the public key that can be used by SPs to encrypt SAML messages sent to this IDP.

g. [**OPTIONAL**] Service endpoint (URL) for this IDP's SAML HTTP Redirect Single Sign-On (SSO) service.

3. Each SP MUST provide the FMO with the following information about itself, unless otherwise indicated via the word [**OPTIONAL**].

a. Proposed **entityID** for this SP. This is typically the URL of the host on which the SP software resides; however, it need not be a resolvable URL.

b. Contact information for at least one technical contact person, including first name, last name, company name, e-mail address, and phone number.

c. X.509 certificate signing request (CSR) for the public key that will be used by this SP to sign SAML messages.

d. X.509 certificate signing request (CSR) for the public key that can be used by IDPs to encrypt SAML messages sent to this SP.

e. Indicator specifying which type(s) of SAML Subject NameID formats this SP accepts: persistent, transient, or both.

f. Service endpoint (URL) of this SP's SAML HTTP POST Assertion Consumer Service.

g. [**OPTIONAL**] Additional technical points of contact, as well as nontechnical points of contact. Each point of contact provided must contain first name, last name, company name, e-mail address, and phone number.

h. [**OPTIONAL**] Service endpoint (URL) at which this SP expects to receive Discovery Response messages as part of the Identity Provider Discovery Service Protocol specified in [IDP Disc Profile]. (This is required only if the SP wants to use the federation's centralized IDP Discovery Service for IDP discovery.)

6.10 Trust and Security Considerations for Web Resources

The specification described in this document relies on the use of HTTP over TLS 1.0 (HTTPS) to transport messages. As previously stated in sections pertaining to specific messages within SAML transactions, all HTTPS transactions within the GFIPM Web Browser User-to-System Profile MUST use TLS 1.0 (SSL 3.1).[12] Also, it is RECOMMENDED that any HTTPS site managed by a federation SP be secured using a certificate trusted by default by commercially available browsers including Microsoft Internet Explorer and Mozilla Firefox.[13]

6.11 Error Handling

Table 4 lists errors that the federation member SAML service MUST handle gracefully. This is not a complete list of all possible errors. The table categorizes errors by SAML event. When these errors occur, the federation member's help desk SHOULD be able to tie the user session to the event that occurred given the approximate time of the error, the federation members involved, and the user.

[12] FIPS PUB 140-2, "Security Requirements for Cryptographic Modules," is a standards document that provides criteria used to accredit cryptographic modules for secure electronic communications. To facilitate the growth and success of the GFIPM program, it is in the best interest of all GFIPM federation members to understand FIPS PUB 140-2 and to know how it affects the policy decisions that are made within the federation. One such policy decision related to FIPS PUB 140-2 involves a GFIPM federation's use of the TLS protocol for securing transactions within the federation. NIST has issued a document titled "Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program," which provides supplementary information about FIPS PUB 140-2. Page 44 of this document states that for the purposes of FIPS 140-2 compliance, TLS is an acceptable key establishment protocol, while SSL (all versions up to and including 3.0) is not acceptable. Therefore, in order to be FIPS 140-2 compliant, a GFIPM federation must use TLS.

[13] Regarding the use of Web server TLS certificates, there is a tradeoff between user convenience and policy compliance. For user convenience, the optimal choice is for the SP to obtain a Web server TLS certificate from a commercial certificate authority that is trusted by default in popular Web browsers. For policy compliance, it may be best for an SP to install a Web server TLS certificate that was issued from a CA known to act in accordance with the SP's certificate policy needs; however, this choice leads to issues of certificate installation and management within users' Web browsers. More input from the GFIPM community may be required before a final decision can be made regarding the verbiage in this document on this topic. Note that this issue does not affect IDPs nearly as much as SPs, because for an IDP, the only users who will be connecting to it via TLS are local users who already have accounts with the IDP and relationships with the organization. In contrast, an SP must be concerned with users from many different organizations across the federation.

Error Processing <Response> • Incorrect/Unknown **<Issuer>** • Incorrect **Version** • Unrecognized **InResponseTo** • Unacceptable **IssueInstant** • Status not **Success**	**Error Processing <Assertion>** • Signature Invalid • Signature Certificate Revoked • Cannot Determine Revocation Status • **<Assertion>** Time Invalid • Cannot Decrypt **<Assertion>** • Incorrect Recipient • Incorrect **Version**
Error Processing <AuthnRequest> • Unknown **<Issuer>** • Signature Invalid • Signature Certificate Revoked • Cannot Determine Revocation Status	**Error Processing <LogoutRequest>** • Unknown **<Issuer>** • Signature Invalid • Signature Certificate Revoked • Cannot Determine Revocation Status
Error Processing <LogoutResponse> • Unknown **<Issuer>** • Signature Invalid • Unknown Status • Signature Certificate Revoked • Cannot Determine Revocation Status	

Table 4: Errors That Federation Services Must Handle Gracefully

6.12 Testing

Prior to joining a GFIPM federation, each IDP system and SP system MUST undergo an onboarding process as described in [GFIPM OPP].

6.13 Service Provider Health Monitoring

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

6.13.1 Health Monitoring Objectives and Overview (Nonnormative)

A GFIPM federation health monitoring system generally seeks to test each federation component on a regular basis for its network connectivity, SAML endpoint behavior, and ability to behave appropriately with standards-conformant GFIPM Metadata assertions. In practice, however, health monitoring for IDPs is not possible, since IDPs need not reside at a publicly accessible IP address. So the primary objective of a health monitoring system is to regularly test for the above criteria at each federation SP.

The technical approach used in GFIPM health monitoring involves the use of a well-defined "health status transaction" based on the SAML SSO profile. The Federation Management Organization (FMO) deploys and manages a special *Health Monitoring IDP* that is dedicated to health monitoring, as well as a *Health Monitoring Agent*, a software component that emulates a typical user agent (Web browser) and interacts with federation SPs to gather status information from them. The Health Monitoring Agent queries each federation SP, using credentials asserted by the Health Monitoring IDP, and makes an HTTP resource request that causes the SP to return specific status information about itself. In this approach, each GFIPM SP is required to implement support for a status transaction; however, in practice, SPs have a significant amount of latitude in their levels of support for the status transaction. Status responses can range from a simple "OK" to a complex list of diagnostic data about various SP resources and subsystems. The following sections contain normative language describing specific provisions that a GFIPM SP must make to accommodate a GFIPM federation's health monitoring system.

6.13.2 Health Status Monitoring URL

A GFIPM SP MUST provide the FMO with a *Health Status Monitoring URL* at which the SP's health status can be queried. The content at this URL MUST be protected by the SP's access control system and available only after successful sign-on via the SP's SAML SSO system. In addition, the URL MUST be accessible by any user from a GFIPM IDP upon successful sign-on. The following section describes the content and format of the document that resides at the Health Status Monitoring URL.

6.13.3 Monitoring Status Document

A GFIPM SP MUST provide a Health Monitoring Status Document at its Health Status Monitoring URL. The document MUST conform to the GFIPM System Status Document Schema [GFIPM Status]. The Health Monitoring Status Document MUST contain an overall status code for the SP. In addition, it MAY contain status codes for one or more SP subsystems.

6.14 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]), additional GFIPM technical standards (e.g., [GFIPM Meta], [GFIPM Cert], and [GFIPM Trust]), laws and regulations (e.g., [NIST SP 800-63]), and applicable technology standards (e.g., XML standards).

Appendix A—Sample GFIPM XML Artifacts

Sample SAML <AuthnRequest> Element

Figure A.1 contains a sample SAML <**AuthnRequest**> element that is intended to provide an example of conformance with the requirements specified in Section 6.3.

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 AssertionConsumerServiceIndex="1"
 Destination="https://rhelidp.ref.gfipm.net/idp/profile/SAML2/POST/SSO"
 ID="_3e2d82218bc92992574db6f214b5ebaa"
 IssueInstant="2008-07-08T20:34:36Z" Version="2.0">
 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  https://rhelsp.ref.gfipm.net/shibboleth
 </saml:Issuer>
 <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/2000/09/xmldsig#rsa-sha1" />
   <ds:Reference URI="#_3e2d82218bc92992574db6f214b5ebaa">
    <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#">
      <ec:InclusiveNamespaces
       xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
       PrefixList="ds saml samlp" />
     </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod
     Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>
     b5zmMVNT9E1w6mhL5DZd34jGQus=
    </ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
   V3/0J+47RV7oS/MrJ5fLaJopbQXlZdmK4KuPOgl8x0tLsHaJ4mrkn9ShyglnW7lU
   Sur4sLPPtxBJzhzsus8+LAKTdr3dBLT5rcAL6b8Yi8lF5jmaMRIorVAFnuEpUUVd
   zm1kNRl5aZJe2I5lpziHBlNLb4D2b0W8FBrk132pf/8=
  </ds:SignatureValue>
  <ds:KeyInfo>
   <ds:KeyName>rhelsp.ref.gfipm.net</ds:KeyName>
   <ds:X509Data>
    <ds:X509Certificate>
     MIIC3jCCAcagAwIBAgIBBTANBgkqhkiG9w0BAQQFADB3MSMwIQYDVQQDExpSZWZl
     --- X.509 Certificate Truncated for Brevity ---
     uN2B/38tg5nzeOTJ0x1YO1TbssLye2mfxjtq4sL3b+FirqhCBDL0r6B1PURbC9f3
     nHlDXHhlUSuN+F7HzXylBs7P
    </ds:X509Certificate>
   </ds:X509Data>
  </ds:KeyInfo>
 </ds:Signature>
 <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

Figure A.1: Sample SAML <AuthnRequest> Element

Sample SAML <Response> Element

Figure A.2 contains a sample SAML <**Response**> element that is intended to provide an example of conformance with the requirements specified in Section 6.3.

```
<samlp:Response Destination=https://rhelsp.ref.gfipm.net/Shibboleth.sso/SAML2/POST
  ID="_0cc75c87fb80c5ca01cc3a02f7a06a55"
  InResponseTo="_f3ce7afc452c3b58958d2997e11f170c"
  IssueInstant="2008-07-08T20:42:06.331Z" Version="2.0"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  https://rhelidp.ref.gfipm.net/shibboleth
 </saml:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:CanonicalizationMethod Algorithm=http://www.w3.org/2001/10/xml-exc-c14n#
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
   <ds:SignatureMethod Algorithm=http://www.w3.org/2000/09/xmldsig#rsa-sha1
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
   <ds:Reference URI="#_0cc75c87fb80c5ca01cc3a02f7a06a55"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transform
      Algorithm=http://www.w3.org/2000/09/xmldsig#enveloped-signature
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Transform
      Algorithm=http://www.w3.org/2001/10/xml-exc-c14n#
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ec:InclusiveNamespaces PrefixList="ds saml samlp xenc"
       xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm=http://www.w3.org/2000/09/xmldsig#sha1
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     rfAdrBSkDWDSzGLNNz/EvGNuUQ8=
    </ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   d/Z4dO/p84OBT0V3a2QJ1djv6mPwf4VubrTQWGRUV7/klhyRSEGB3hpTAwlXFMBRotVmeBLimMCl
   dOJF4wCMDMJq6DVSOaWah2dfl9NNdHvPBDOzm10aMc/me9BzPWpQG0nA21y/frgKQVL/2RRElRCB
   omaN0g2eu/t0mQ2z/eQ=
  </ds:SignatureValue>
  <ds:KeyInfo>
   <ds:X509Data>
    <ds:X509Certificate>
     MIIC3zCCAcegAwIBAgIBBzANBgkqhkiG9w0BAQQFADB3MSMwIQYDVQQDExpSZWZlcmVuY2UgR0ZJ
     --- X.509 Certificate Truncated for Brevity ---
     bmlaDMgHfrjHLjTQJ/+blpgQ5oBK+dGOypCxYowNDFBN2fK2GP/RHKOswhEFZqgYzIVOyxtqwQ==
    </ds:X509Certificate>
   </ds:X509Data>
  </ds:KeyInfo>
 </ds:Signature>
 <samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
 </samlp:Status>
 <saml:EncryptedAssertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <xenc:EncryptedData Id="_3bbffb5d0f18b09b6d3d459e1a0e4da8"
   Type=http://www.w3.org/2001/04/xmlenc#Element
   xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
   <xenc:EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc
```

```
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"/>
   <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <xenc:EncryptedKey Id="_1faa67deb1d10547d461b6aa7bc86b60"
     xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
     <xenc:EncryptionMethod
      Algorithm=http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p
      xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"><ds:DigestMethod
      Algorithm=http://www.w3.org/2000/09/xmldsig#sha1
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     </xenc:EncryptionMethod>
     <ds:KeyInfo>
      <ds:X509Data>
       <ds:X509Certificate>
        MIIC3jCCAcagAw...
        --- X.509 Certificate Truncated for Brevity ---
        0x1YO1TbssLye2mfxjtq4sL3b+FirqhCBDL0r6B1PURbC9f3nHlDXHhlUSuN+F7HzXylBs7P
       </ds:X509Certificate>
      </ds:X509Data>
     </ds:KeyInfo>
     <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
      <xenc:CipherValue xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
       Fp0ZcO+ImZNiyARrr0mwpa+W...
       --- Cipher Value Truncated for Brevity ---
       g5PK5ZtrkVHpsWH+nEY=
      </xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
   </ds:KeyInfo>
   <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
    <xenc:CipherValue xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
     R/UqZAkNaMOGssEuwJta7VyXvTFjJYls3cDWp1OJuF8PWWOcdV+0+6nbSG+AOObZ8C0g+1WV9V/6
     --- Cipher Data Truncated for Brevity ---
     kpsUXJucQqpGEjr9giKlNNPJchPg2EBTZmfvXqk28X4h+FhYwd+M5ILUG1FvEq1Xi+GnoRj7KxEL
     uw==
    </xenc:CipherValue>
   </xenc:CipherData>
  </xenc:EncryptedData>
 </saml:EncryptedAssertion>
</samlp:Response>
```

Figure A.2: Sample SAML <Response> Element

Sample SAML <Assertion> Element

Figure A.3 contains a sample SAML <**Assertion**> element that is intended to provide an example of conformance with the requirements specified in Section 6.3.

```
<saml:Assertion ID="_c0594b43e28a2f94311d395d57d4ae5a"
 IssueInstant="2007-10-16T15:16:19.938Z" Version="2.0"
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
 <saml:Issuer
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
  https://rhelidp.ref.gfipm.net/shibboleth
 </saml:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:CanonicalizationMethod
    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
   <ds:SignatureMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
   <ds:Reference URI="_c0594b43e28a2f94311d395d57d4ae5a"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:Transforms
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transform
     Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
    <ds:Transform
     Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#WithComments"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ec:InclusiveNamespaces PrefixList="ds saml xs"
      xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </ds:Transform>
   </ds:Transforms>
   <ds:DigestMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
   <ds:DigestValue
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    O/LiVrYP7MG5/bNCSQARk7tBAuI=
   </ds:DigestValue>
  </ds:Reference>
 </ds:SignedInfo>
 <ds:SignatureValue
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  [snip base64 signature]
 </ds:SignatureValue>
</ds:Signature>
<saml:Subject>
 <saml:NameID
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
  NameQualifier="http://rhelidp.ref.gfipm.net/shib-idp/">
  _84b810c771472f309d0bbdf6a517813a
 </saml:NameID>
 <saml:SubjectConfirmation
  Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
  <saml:SubjectConfirmationData Address="130.207.204.222"
   InResponseTo="_30ee6ed689da8f1d13518a052d217be6"
   NotOnOrAfter="2007-10-16T15:21:19.938Z"
   Recipient="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SAML2/POST" />
 </saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2007-10-16T15:16:19.938Z"
 NotOnOrAfter="2007-10-16T15:21:19.938Z">
 <saml:AudienceRestriction>
  <saml:Audience>https://rhelsp.ref.gfipm.net/shibboleth</saml:Audience>
 </saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2007-10-16T15:16:19.878Z"
 SessionNotOnOrAfter="2007-10-16T15:46:19.878Z">
 <saml:SubjectLocality Address="130.207.204.222"
  DNSName="130.207.204.222" />
 <saml:AuthnContext>
  <saml:AuthnContextDeclRef>
   urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
  </saml:AuthnContextDeclRef>
 </saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
 <saml:Attribute Name="gfipm:2.0:user:FederationId"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml:AttributeValue
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:type="xs:string">
   GFIPM:IDP:JNET:USER:johndoe@jnet.net
  </saml:AttributeValue>
 </saml:Attribute>
```

```
    <saml:Attribute Name="gfipm:2.0:user:GivenName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">
        John
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="gfipm:2.0:user:SurName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">
        Doe
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Figure A.3: Sample SAML <Assertion> Element

Sample SAML <LogoutRequest> Element

Figure A.4 contains a sample SAML <**LogoutRequest**> element that is intended to provide an example of conformance with the requirements specified in Section 6.4.

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_72424ea37e28763e351189529639b9c2b150ff37e5" Version="2.0"
  Destination="https://rhelidp.ref.gfipm.net/idp/profile/SAML2/POST/SLO"
  IssueInstant="2008-06-03T12:59:57Z">
  <saml:Issuer>
    https://rhelsp.ref.gfipm.net/shibboleth
  </saml:Issuer>
  <saml:NameID
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
    SPNameQualifier="https://rhelsp.ref.gfipm.net/shibboleth">
    6a171f538d4f733ae95eca74ce264cfb602808c850
  </saml:NameID>
  <samlp:SessionIndex>
    b976de57fcf0f707de297069f33a6b0248827d96a9
  </samlp:SessionIndex>
</samlp:LogoutRequest>
```

Figure A.4: Sample SAML <LogoutRequest> Element

Sample SAML <LogoutResponse> Element

Figure A.5 contains a sample SAML <**LogoutResponse**> element that is intended to provide an example of conformance with the requirements specified in Section 6.4.

```
<samlp:LogoutResponse xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_cbb63e9741259e3f1c98a1ae38ac5ac25889720b32" Version="2.0"
  IssueInstant="2008-06-03T12:59:57Z"
  Destination="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SLO/POST"
  InResponseTo="_72424ea37e28763e351189529639b9c2b150ff37e5">
  <saml:Issuer>https://rhelidp.ref.gfipm.net/shibboleth</saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode
      Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    <samlp:StatusMessage>
      Successfully logged out from service https://rhelidp.ref.gfipm.net/shibboleth
    </samlp:StatusMessage>
  </samlp:Status>
</samlp:LogoutResponse>
```

Figure A.5: Sample SAML <LogoutResponse> Element

Appendix B—Document History

Date	Version	Editor	Change
04/12/2012	1.2	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.