National Identity Exchange Federation

Web Browser User-to-System Profile

Version 1.0

August 18, 2014

Table of Contents

1. Target Audience and Purpose

This document specifies technical interoperability requirements for connection to operational endpoints in the National Identity Exchange Federation (NIEF) in the Web Browser User-to-System use case.[1] The target audience includes technical representatives of organizations that intend to participate in NIEF 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 NIEF endpoints.

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 [NIEF Bylaws] and [NIEF OPP].

2. NIEF Identity Trust Framework and Terminology

This document is one component of the NIEF Identity Trust Framework. See [NIEF OPP] for more information about the full NIEF Identity Trust Framework.

This document contains language that uses technical terms related to identity 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 [NIEF Terms].

3. 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 components from the NIEF Identity Assurance Framework and industry standards), and a list of reference URLs where applicable.

Document References for NIEF Identity Assurance Framework Components

Document ID	Document Name and URL if Applicable
NIEF Terms	NIEF Terminology Reference
NIEF Bylaws	NIEF Center Bylaws
NIEF OPP	NIEF Center Operational Policies and Procedures
NIEF Attrs	NIEF Attribute Registry
NIEF Trust	NIEF Cryptographic Trust Model

[1] The Web Browser User-to-System use case, covered in this document, is one of two basic NIEF use cases. The other is the Web Services System-to-System use case, which is covered in [NIEF S2S Profile].
[2] See [NIEF Terms] for terminology related to various organizational and technical roles in NIEF.

NIEF CP	NIEF Certificate Policy
NIEF S2S Profile	NIEF Web Services System-to-System Profile
NIEF Status	NIEF System Status Document Schema http://ref.gfipm.net/monitor/schemas/status/GFIPMSystemStatus.xsd

Table 1: Document References for NIEF Identity Assurance Framework Components

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 800-52-1	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations National Institute of Science and Technology (NIST) Special Publication 800-52-1 http://csrc.nist.gov/publications/nistpubs/

NIST SP 800-63-2	Electronic Authentication Guideline National Institute of Science and Technology (NIST) Special Publication 800-63-2 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
FBCA CP	"Federal Bridge Certification Authority Certificate Policy" http://www.idmanagement.gov/fpkipa/documents/fbca_cp_rfc3647.pdf
CPFCA CP	"Common Policy Framework Certification Authority Certificate Policy" http://www.idmanagement.gov/fpkipa/documents/commonpolicy.pdf

Table 2: Document References for Industry Standards

Reference URLs for SAML and XML	
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

4. 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].

5. NIEF Web Browser User-to-System Profile

The NIEF 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 NIEF. Where this specification does not explicitly provide SAML guidance, one must implement in accordance with applicable OASIS SAML 2.0 requirements.

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 participating agency within NIEF. ***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 agencies that wish to participate in NIEF as an IDP or SP. See Section 5.9 for additional information. Also, see [NIEF Terms] for further information about NIEF 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.

5.1 Presentation and User Interface

5.1.1 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 NIEF SPs from which the user can select.[5] Upon user selection of an SP from this list, the IDP

[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 in Section 5.3.2 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 NIEF Cryptographic Trust Fabric document. See [NIEF Trust] for more information.

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

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

5.1.2 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 5.2 for more information about user selection of an IDP (also known as IDP Discovery). See Section 5.3 for more information about **<AuthnRequest>** requirements.

5.2 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 NIEF's centralized IDP Discovery Service. The other is to implement a local IDP Discovery Service at the SP.

2. If an SP implements IDP discovery via NIEF 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].

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.

5.3 Use of SAML 2.0 Web SSO Profile

1. An IDP MUST implement the "Identity Provider" functionality described in the SAML Web Browser SSO Profile, as per Section 4.1 of [SAML2 Profiles], and as constrained by the normative language in the following subsections.

2. An SP MUST implement the "Service Provider" functionality described in the SAML Web Browser SSO Profile, as per Section 4.1 of [SAML2 Profiles] , and as constrained by the normative language in the following subsections.

5.3.1 SAML <AuthnRequest> Element Requirements

1. An IDP MUST accept **<AuthnRequest>** messages via the SAML HTTP Redirect binding.

2. An SP MUST send **<AuthnRequest>** messages to an IDP using the SAML HTTP Redirect binding.

3. All **<AuthnRequest>** messages SHOULD be signed by the SP to ensure message integrity and to authenticate the SP as the originator of the message.[7] In addition, upon receiving a signed **<AuthnRequest>** message, the IDP MUST attempt to verify the signature and MUST terminate the transaction if the signature cannot be verified a having originated from an SP trusted by the IDP.

4. An **<AuthnRequest>** MUST contain an **<Issuer>** element. It MUST be agreed upon between the SP and the NIEF Center, and it must match the **EntityID** specified for this SP in the IDP's NIEF Cryptographic Trust Fabric.

5. The **<NameIDPolicy>** MUST be present. Also, its **Format** attribute MUST be present, and the **Format** attribute's value MUST be "**urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**" or "**urn:oasis:names:tc:SAML:2.0:nameid-format:transient**".

6. 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. **ForceAuthn** can be used by the SP to require the IDP to force the user to authenticate to the IDP

[7] Because this spec requires the IDP to verify that the SP is trusted via an entry in the IDP's NIEF Cryptographic Trust Fabric document prior to responding to an **<AuthnRequest>**, omission of a digital signature on the **<AughnRequest>** does not introduce any attack vectors into the IDP.

regardless of the user's authentication session status at the IDP. The IDP MUST support the use of **`ForceAuthn`**.

7. The SP MAY issue an **`<AuthnRequest>`** message with the **`IsPassive`** attribute set to true. The IDP MUST support the use of **`IsPassive`**, and MUST NOT take control of the user agent's (e.g. the web browser's) interface if **`IsPassive`** is true.

8. An **`<AuthnRequest>`** MUST NOT contain any of the following elements: **`<Subject>`**, **`<Scoping>`**, **`<Extensions>`**, or **`<Conditions>`**.

9. If **`AssertionConsumerServiceURL`** is present in an **`<AuthnRequest>`**, the IDP SHOULD compare the **`AssertionConsumerServiceURL`** with the the **`Location`** attribute of the **`<AssertionConsumerService>`** element for that SP within the IDP's NIEF Cryptographic Trust Fabric. If the IDP does compare the **`AssertionConsumerServiceURL`** in the **`<AuthnRequest>`** with the the **`Location`** attribute of the **`<AssertionConsumerService>`** element for that SP within the IDP's NIEF Cryptographic Trust Fabric, and the two do not match, then the IDP MUST end the transaction.

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

11. If included in the **`<AuthnRequest>`**, the **`<RequestedAuthnContext>`** MUST contain one or more **`<AuthnContextClassRef>`** elements. Also, the **`<RequestedAuthnContext>`** MUST contain a **`Comparison`** attribute, and its value MUST be "**`exact`**". Also, the value of at least one **`<AuthnContextClassRef>`** element MUST be one of the following URLs, which are used to indicate the NIST Level(s) of Assurance (LOA(s)) required for access to the resources provided by the SP.[8]

    - **`http://idmanagement.gov/ns/assurance/loa/1`**
    - **`http://idmanagement.gov/ns/assurance/loa/2`**
    - **`http://idmanagement.gov/ns/assurance/loa/3`**
    - **`http://idmanagement.gov/ns/assurance/loa/4`**

[8] See [NIST 800-63-2] for more information about Levels of Assurance.

Please see Appendix A for a sample SAML <**AuthnRequest**> XML element that conforms to these requirements.

5.3.2 SAML <Response> Element Requirements

1. An IDP MUST send **<Response>** messages via the HTTP POST binding. An IDP MAY send unsolicited **<Response>** messages.

2. An SP MUST accept and process **<Response>** messages via the HTTP POST binding, including both solicited ("SP First") and unsolicited ("IDP First") **<Response>** messages.

3. The **<Issuer>** element MUST appear within a **<Response>**. It MUST be agreed upon between the IDP and the NIEF Center, and it must match the **EntityID** specified for this IDP in the SP's NIEF Cryptographic Trust Fabric.

4. When delivering a **<Response>** message to the Assertion Consumer Service of the SP, the IDP MUST use the location provided by the **Location** attribute of the **<AssertionConsumerService>** element for that SP within the IDP's NIEF Cryptographic Trust Fabric.

5. If the **<Response>** contains a digital signature, then the SP MUST verify that the digital signature on the **<Response>** element is valid and was created by the key associated with the **EntityID** in the SP's NIEF Cryptographic Trust Fabric that matches the contents of the **<Issuer>** element within the **<Response>**.

6. The **Version** attribute within a **<Response>** MUST have a value of "**2.0**".

7. A **<Response>** MUST NOT contain an **<Extensions>** element.

8. A **<Response>** SHOULD contain exactly one **<EncryptedAssertion>** element, and when decrypted, its contents MUST conform to the requirements specified below regarding the SAML <**Assertion**> element. If a **<Response>** does not contain an **<EncryptedAssertion>** element, then it MUST contain exactly one **<Assertion>** element.[9]

[9] We strongly encourage the use of an **<EncryptedAssertion>** element rather than the unencrypted **<Assertion>** element; however, in practice, some implementers may choose not to use encrypted assertions. If you choose not to use encrypted assertions, please be cognizant of the risk of sensitive data leakage via the user agent (web browser) cache.

Please see Appendix A for a sample SAML <**Response**> XML element that conforms to these requirements.

5.3.3 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 a SAML **<Assertion>** can be made about the user, the **<Assertion>** MUST conform to the following requirements.

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

2. An **<Assertion>** element SHOULD be encrypted. If encrypted, the **<Assertion>** element MUST be included within a **<Response>** element via an **<EncryptedAssertion>** element. If not encrypted, the **<Assertion>** element MUST be included directly within a **<Response>** element.

3. The **Version** attribute within **<Assertion>** MUST have a value of "**2.0**".

4. The **<Issuer>** element MUST appear within an **<Assertion>**. It MUST be agreed upon between the IDP and the NIEF Center, and it MUST match the **EntityID** specified for the IDP in the SP's NIEF Cryptographic Trust Fabric.

5. The SP MUST verify that the digital signature on the **<Assertion>** element is valid and was created by the key associated with the **EntityID** in the SP's NIEF Cryptographic Trust Fabric that matches the contents of the **<Issuer>** element within the **<Assertion>**.

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

7. A **<Subject>** element MUST contain a **<NameID>** element.

8. An **<Assertion>** MUST contain a **<Conditions>** element.

9. The **<NameID>** element within **<Subject>** MUST be present and 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**

In addition, if the **<Assertion>** was generated in response to an **<AuthnRequest>** message sent by an SP, then the Format attribute must correspond to the format specified by the **<NameIDPolicy>** in the **<AuthnRequest>**.

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

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

12. 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.

13. An **<AuthnStatement>** MUST contain an **<AuthnContext>** element, and the **<AuthnContext>** element MUST contain exactly one **<AuthnContextClassRef>** element.

    a. The value of the **<AuthnContextClassRef>** element MUST accurately represent the authentication method used by the IDP to authenticate the user, and MAY be one of the following URLs, which are used to indicate the NIST Level of Assurance (LOA) associated with the identity for which the **<Assertion>** was generated.[10]

       - **http://idmanagement.gov/ns/assurance/loa/1**
       - **http://idmanagement.gov/ns/assurance/loa/2**
       - **http://idmanagement.gov/ns/assurance/loa/3**
       - **http://idmanagement.gov/ns/assurance/loa/4**

    b. If the IDP specifies one of the NIST LOAs for the **<AuthnContextClassRef>**, the SP SHOULD compare the NIST LOA indicated by the **<AuthnContextClassRef>** element with the list of acceptable NIST LOAs for the asserting IDP, as per the SP's NIEF Cryptographic Trust Fabric. If the SP compares the asserted NIST LOA with the list of acceptable NIST LOAs for the asserting IDP, and the asserted NIST LOA is higher than the maximum acceptable NIST LOA for the asserting IDP, then the SP MUST either terminate the transaction or treat the **<Assertion>**

[10] See [NIST 800-63-2] for more information about Levels of Assurance.

as if its asserted NIST LOA is equal to the maximum acceptable NIST LOA for the asserting IDP.

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

15. The IDP MUST NOT send any attributes that are not specifically requested by the SP via its **<AttributeConsumerService>** entry or entries in the IDP's NIEF Cryptographic Trust Fabric.

16. Any **<Attribute>** element containing a user attribute about the user identity's LOA MUST be logically consistent with the LOA expressed by the **<AuthnContextClassRef>** element within the **<AuthnStatement>** for this **<Assertion>**.

Please see Appendix A for a sample SAML **<Assertion>** XML element that conforms to these requirements.

5.3.4 LOA 4 SAML Holder-of-Key Requirements

At NIST LOA 4, standard SAML assertions containing a Subject Confirmation Method of "**urn:oasis:names:tc:SAML:2.0:cm:bearer**" MUST NOT be used to authenticate the end-user to the SP; however, SAML assertions containing a Subject Confirmation Method of "**urn:oasis:names:tc:SAML:2.0:cm:holder-of-key**" MAY be used to bind keys or other attributes to an identity. Holder-of-Key assertions MAY be used at LOA 4 provided that the following requirements are met.[11]

1. The SP MAY require that the issuer of the user's certificate be cross-certified with the Federal Bridge Certification Authority, or that the user's certificate be issued under the Common Policy Framework Certification Authority. See [FBCA CP] or [CPFCA CP] for more information.[12]

2. When generating a Holder-of-Key SAML **<Assertion>**, the IDP MUST meet the following criteria.

   a. The IDP MUST authenticate the user via a LOA 4 certificate.

   b. The **<AuthnContextClassRef>** element MUST contain a value of "**http://idmanagement.gov/ns/assurance/loa/4** ".

[11] See information about Level of Assurance 4 in Section 10.3.2.4 of [NIST 800-63-2].
[12] The purpose of this statement is to ensure that this specification supports LOA 4 while not requiring the use of the Federal PKI Bridge unless it is specifically mandated by the SP.

c. The **Method** attribute of the **<SubjectConfirmation>** element MUST contain a value of "**urn:oasis:names:tc:SAML:2.0:cm:holder-of-key**".

d. The **<SubjectConfirmation>** element MUST include a **<ds:KeyInfo>** element containing exactly one **<ds:X509Data>** element, and the **<ds:X509Data>** element MUST contain exactly one **<ds:X509Certificate>** element. The **<ds:X509Certificate>** element MUST contain the certificate that the user used to authenticate to the IDP.

3. Upon receiving a Holder-of-Key SAML **<Assertion>**, the SP MUST verify that the end-user possesses the private key for the certificate that is referenced in the assertion. In performing this verification, the SP MUST use a LOA 4 protocol that is specified in [NIST 800-63-2], Section 9, "Authentication Process".

4. The SP MAY validate that the issuer of the user's certificate is cross-certified with the Federal Bridge Certification Authority, or that the user's certificate was issued under the Common Policy Framework Certification Authority. See [FBCA CP] or [CPFCA CP] for more information.

5.4 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 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 an environment in which SLO is supported to the greatest extent possible in NIEF, while still allowing for the possibility that not all NIEF IDPs and SPs necessarily support it, in a manner that is user-friendly and supports appropriate and accepted best practices for user session security.

5.4.1 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 NIEF 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 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.

5.4.2 SAML <LogoutRequest> Element Requirements

1. All **<LogoutRequest>** messages MUST be communicated using the SAML HTTP Redirect binding.

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

3. The **Version** attribute within **<LogoutRequest>** MUST have a value of "**2.0**".

Please see Appendix A for a sample SAML **<LogoutRequest>** XML element that conforms to these requirements.

5.4.3 SAML <LogoutResponse> Element Requirements

1. All **<LogoutResponse>** messages MUST be communicated using the SAML HTTP Redirect binding.

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

3. The **Version** attribute within **<LogoutResponse>** MUST have a value of "**2.0**".

Please see Appendix A for a sample SAML <**LogoutResponse**> XML element that conforms to these requirements.

5.5 Presence in NIEF Cryptographic Trust Fabric

Every NIEF IDP and NIEF SP in the MUST have an entry in each other's NIEF Cryptographic Trust Fabric, which provides signing and encryption certificates, and other configuration data, for system endpoints that are considered to be trusted. See [NIEF Trust] for details about the format of NIEF Cryptographic Trust Fabric.

5.6 Trust and Security Considerations for Web Resources

1. The specification described in this document relies on the use of HTTP over TLS (HTTPS) to transport messages. All transactions within the NIEF Web Browser User-to-System Profile MUST use HTTPS with TLS version 1.1 or higher.[13] TLS version 1.2 is RECOMMENDED.

2. It is RECOMMENDED that all TLS implementations conform to [NIST 800-52-1].

3. It is RECOMMENDED that any HTTPS site managed by a NIEF SP be secured using a certificate trusted by default by reasonably recent versions of Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, and Apple Safari.[14]

[13] 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 NIEF, it is in the best interest of all NIEF participants to understand FIPS PUB 140-2 and to know how it affects the policy decisions that are made within NIEF. One such policy decision related to FIPS PUB 140-2 involves NIEF's use of the TLS protocol for securing transactions within NIEF. 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, NIEF must use TLS.

[14] 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 NIEF community and the broader 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

4. All system endpoints implementing this profile MUST adhere to the requirements in [NIEF Trust] concerning minimum required cryptographic algorithms and modules.

5.7 Error Handling

This section lists errors that the SAML service MUST handle gracefully. Graceful handling of an error requires that a system present the user with an easy-to-understand explanation of the error, as well as suggested steps to take if the user wants to pursue resolution of the error.

1. When processing a SAML **<AuthnRequest>** message, an IDP MUST gracefully handle the following types of errors.

    - Unknown **<Issuer>**
    - Signature Invalid
    - Signing Certificate Untrusted

2. When processing a SAML **<Response>** message, an SP MUST gracefully handle the following types of errors.

    - Incorrect/Unknown **<Issuer>**
    - Incorrect **Version**
    - Unrecognized **InResponseTo**
    - Unacceptable **IssueInstant**
    - Status not **Success**

3. When processing a SAML **<Assertion>**, an SP MUST gracefully hanle the following types of errors.

    - Signature Invalid
    - Signing Certificate Untrusted
    - **<Assertion>** Time Invalid
    - Cannot Decrypt **<Assertion>**
    - Incorrect Recipient
    - Incorrect **Version**

4. When processing a SAML **<LogoutRequest>** message, an IDP or SP MUST gracefully handle the following types of errors.

    - Unknown <**Issuer**>

already have accounts with the IDP and relationships with the organization. In contrast, an SP must be concerned with users from many different NIEF participant organizations .

- Signature Invalid
- Signing Certificate Untrusted

5. When processing a SAML **<LogoutResponse>** message, an IDP or SP MUST gracefully handle the following types of errors.

    - Unknown **<Issuer>**
    - Signature Invalid
    - Signing Certificate Untrusted
    - Unknown Status

Please note that this section does not contain a complete list of all possible errors, and implementations SHOULD make every effort to gracefully handle other errors not covered by the language in this section. When these errors occur, NIEF help desk services SHALL make a best-effort attempt to to tie the user session to the event that occurred given the approximate time of the error, the NIEF participants involved, and the user.

5.8 Service Provider Health Monitoring

SP endpoints in NIEF MAY support a SAML-based SP health monitoring protocol. This section describes the general concept of NIEF SP Health Monitoring and also provides normative requirements to which NIEF SPs must conform if they choose to leverage NIEF's SP health monitoring capabilities.

5.8.1 Health Monitoring Objectives and Overview (Nonnormative)

A SAML 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 SAML 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 NIEF SP health monitoring involves the use of a well-defined "health status transaction" based on the SAML SSO profile. The NIEF Center 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 NIEF SPs to gather status information from them. The Health Monitoring Agent queries each NIEF 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 NIEF 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 NIEF SP must make to accommodate a SAML SP health monitoring system.

5.8.2 Health Status Monitoring URL

A NIEF SP MAY provide the NIEF Center 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. If provided, the URL MUST be accessible by any user from a NIEF IDP upon successful sign-on. The following section describes the content and format of the document that resides at the Health Status Monitoring URL.

5.8.3 Monitoring Status Document

A NIEF SP that provides a Health Status Monitoring URL MUST provide a Health Monitoring Status Document at that URL. The document MUST conform to the NIEF System Status Document Schema [NIEF 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.

5.9 Other NIEF Reference Documents (Nonnormative)

This document does not represent the complete set of requirements for participation in NIEF. Other documents may apply, including business and policy documents (e.g., [NIEF Bylaws] and [NIEF OPP]), additional NIEF technical standards (e.g., [NIEF Attrs], [NIEF CP], and [NIEF Trust]), laws and regulations (e.g., [NIST SP 800-63-2]), and applicable technology standards (e.g., XML standards).

Appendix A—Sample 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 5.3.1.

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    AssertionConsumerServiceURL="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SAML2/POST"
    Destination="https://idp.ref.gfipm.net/idp/profile/SAML2/Redirect/SSO"
    ID="_77938c8078293f9d59bcbc18afa31291"
    IssueInstant="2012-12-11T19:28:19Z"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Version="2.0">
    <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://rhelsp.ref.gfipm.net/shibboleth</saml:
Issuer>
    <samlp:NameIDPolicy AllowCreate="1" Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent" />
    <samlp:RequestedAuthnContext Comparison="exact">
        <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
http://idmanagement.gov/ns/assurance/loa/2</saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</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 5.3.2.

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 Destination="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SAML2/POST"
                 ID="_a2339c351b2f85caba95c6a9a062efeb"
                 InResponseTo="_e13cce5fe25af1d64a7137cfe146c319"
                 IssueInstant="2014-02-26T16:58:03.592Z"
                 Version="2.0">
 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
               Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
               https://idp.ref.gfipm.net/idp/shibboleth
  </saml2:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <!--Optional XML Digital Signature -->
 </ds:Signature>
 <saml2p:Status>
  <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
 </saml2p:Status>
 <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="_9aed640f53a988e1c2ffa975ebfe544a" Type="http://www.w3.org/2001/04/xmlenc#Element">
   <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" />
   <!-- Snipped for brevity -->
  </xenc:EncryptedData>
 </saml2:EncryptedAssertion>
</saml2p: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 5.3.3.

```
<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_1bef1bddb8e63eac8909b53e1772ac58"
    IssueInstant="2012-12-11T20:23:36.650Z" Version="2.0"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://idp.ref.gfipm.net/idp/shibboleth</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      [snipped for brevity]
    </ds:Signature>
    <saml2:Subject>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
            NameQualifier="https://idp.ref.gfipm.net/idp/shibboleth"

SPNameQualifier="https://rhelsp.ref.gfipm.net/shibboleth">Am1YovuI6Lq6rNXZVUQgGTbrwqE=</saml2:Nam
eID>
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData Address="10.50.76.247"
InResponseTo="_cfc1c870f326777713b3aba13049b12d"
               NotOnOrAfter="2012-12-11T20:28:36.650Z"
Recipient="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SAML2/POST" />
        </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2012-12-11T20:23:36.650Z" NotOnOrAfter="2012-12-
11T20:28:36.650Z">
        <saml2:AudienceRestriction>
            <saml2:Audience>https://rhelsp.ref.gfipm.net/shibboleth</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2012-12-11T20:23:35.544Z"
        SessionIndex="aecef47784a475cf0933a70556bdc04ba8fd0dac44272a0b4db52d8ba5aef3d5">
        <saml2:SubjectLocality Address="10.50.76.247" />
        <saml2:AuthnContext>
            <saml2:AuthnContextClassRef> http://idmanagement.gov/ns/assurance/loa/2
            </saml2:AuthnContextClassRef>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
        <saml2:Attribute FriendlyName="PublicData"
Name="gfipm:2.0:user:PublicDataSelfSearchHomePrivilegeIndicator"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">true
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="IDProofingLevel"
Name="gfipm:2.0:user:IdentityProofingAssuranceLevelCode"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">NISTLEVEL3
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="NISTAssuranceLevel"
Name="gfipm:2.0:user:ElectronicAuthenticationAssuranceLevelCode"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">NISTLEVEL2
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="FederationId" Name="gfipm:2.0:user:FederationId"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">GFIPM:IDP:ExampleIDP:USER:ms01
            </saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
```

```
</saml2: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 5.4.2.

```
<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 5.4.3.

```
<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