National Identity Exchange Federation

Cryptographic Trust Model

Version 1.0

August 18, 2014

Table of Contents

1. Target Audience and Purpose

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

This document's target audience includes technical representatives of organizations who intend to participate in NIEF as Identity Provider Organizations (IDPOs), Service Provider Organizations (SPOs), Service Consumer Organizations (SCOs), Attribute Provider Organizations (APOs), or any allowable combination of these.[1] It also includes vendors, contractors, and consultants who, as part of their project or product implementation, have a requirement to establish technical interoperability with NIEF endpoints.

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

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

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 CP	NIEF Certificate Policy
NIEF U2S Profile	NIEF Web Browser User-to-System Profile
NIEF S2S Profile	NIEF Web Services System-to-System Profile

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
SAML2 Assurance	"SAML V2.0 Identity Assurance Profiles, Version 1.0" OASIS Committee Specification 01, 5 November 2010 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cs-01.pdf
SAML2 Entity Attr	"SAML V2.0 Metadata Extension for Entity Attributes, Version 1.0" OASIS Committee Specification 01, 4 August 2009 http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html

Document References for Industry Standards	
SAML2 Meta AR Ext	"SAML Metadata Extension for a Standalone Attribute Requester" Working Draft 01, 11 March 2005 Document Identifier: draft-saml-metadata-ext-01 https://www.oasis-open.org/committees/download.php/11805/draft-saml-metadata-ext-01.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 800-63-2	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
FIPS 140-2	Federal Information Processing Standard (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules" http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Table 2: Document References for Industry Standards

Reference URLs 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/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 Cryptographic Trust Model

All subsections that follow are normative, unless otherwise noted.

5.1 NIEF Trust Anchor (Nonnormative)

The NIEF Center cryptographically signs the NIEF Cryptographic Trust Fabric (see Section 5.2). The NIEF Center does NOT issue certificates to NIEF participants, and although it is possible for the NIEF Center to sign NIEF participants' certificates, it is not required. Trust between NIEF participants is anchored by the NIEF Cryptographic Trust Fabric document and the NIEF Center's cryptographic signature of the document.

5.2 NIEF Cryptographic Trust Fabric

At a technical level, trust between all communications endpoints in NIEF is implemented using the SAML 2.0 standard for federated system entity metadata. This information is delivered to participants via the *NIEF Cryptographic Trust Fabric* document, which defines the most current NIEF cryptographic security context. The document contains an entry for each communications endpoint in NIEF, including identity providers (IDPs), service providers (SPs), Web Service consumers (WSCs), Web Service providers (WSPs), Attribute Consumers (ACs), Attribute Providers (APs), and others. The NIEF Center maintains the document and makes a new version of it available to NIEF participants periodically as needed due to the addition or removal of communications endpoints. To ensure compliance with the current NIEF Cryptographic Trust Fabric, each communications endpoint in NIEF MUST incorporate the most current version of the NIEF Cryptographic Trust Fabric document into its security policy decisions in a timely fashion. The NIEF Center shall provide guidance to NIEF participants as to the urgency with which a new Trust Fabric document must be incorporated, at the time the new document is made available. In cases in which the new Trust Fabric document has been published because of a security or trust violation, or because of the removal of a member from NIEF for disciplinary reasons, it is recommended that members incorporate the new Trust Fabric document as soon as is reasonably possible, and in any case, not more than 24 hours after its release.

The NIEF Cryptographic Trust Fabric document conforms to the specification defined in [SAML2 Metadata]. It also uses several extension schemas,

1. A custom extension schema for the **<md:RoleDescriptor>** element serves to accommodate the use of NIEF Cryptographic Trust Fabric with various NIEF Web Services endpoints, by defining the types of NIEF Web Services endpoint elements that **<md:RoleDescriptor>** can contain. Appendix A contains this schema. It is also available at the following URL.

   http://gfipm.net/standards/trust/2.0/gfipm-webservices-trustfabric-2.0.xsd

2. A SAML standard extension schema for the **<mdattr:EntityAttributes>** element serves to accommodate the use of entity attributes, which are facts or

properties asserted by the NIEF Center about a NIEF Cryptographic Trust Fabric entity and its endpoints. This schema is defined by [SAML2 Entity Attr].

3. Another SAML standard extension schema for the <**md:RoleDescriptor**> element defines a new element type, **AttributeRequesterDescriptorType**, that serves to enable a NIEF Cryptographic Trust Fabric to contain information about an endpoint that belongs to a SAML "Attribute Requester", i.e., a consumer of attributes from an Attribute Provider. This schema is defined by [SAML2 Meta AR Ext].

Additional constraints specified in this section also apply to the NIEF Cryptographic Trust Fabric document.

5.2.1 SAML <EntitiesDescriptor> Element Requirements

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

1. The **Name** attribute within the top-level **<EntitiesDescriptor>** MUST be present.

2. The **ID** attribute within the top-level **<EntitiesDescriptor>** MUST be present.

3. The **validUntil** and **cacheDuration** attributes within **<EntitiesDescriptor>** MUST be present. It is RECOMMENDED that **cacheDuration** not exceed 18 hours.

4. The **<ds:Signature>** element within the top-level **<EntitiesDescriptor>** MUST be present, and it MUST contain a valid signature for the document, signed by the NIEF Center.

5. The **<Extensions>** element within the top-level <**EntitiesDescriptor>** MUST NOT be present.

6. Nested **<EntitiesDescriptor>** elements within the top-level **<EntitiesDescriptor>** MAY be present. Nested **<EntitiesDescriptor>** elements SHOULD include **Name** and **ID** attributes.

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

5.2.2 SAML <EntityDescriptor> Element Requirements

The following requirements apply to **<EntityDescriptor>** elements that appear in the NIEF Cryptographic Trust Fabric document. Each **<EntityDescriptor>** element provides entity metadata for a specific entity that fulfills a NIEF Technical Role (see [NIEF Terms]). These requirements supplement the requirements described in [SAML2 Metadata].

1. The **entityID** attribute within **<EntityDescriptor>** MUST be present, MUST be unique within NIEF, and MUST be set to the value that was agreed upon for this entity between the entity and the NIEF Center. (The entity chooses its **entityID** value, but the choice MUST be approved by the NIEF Center.) Also, the requirements in the following subsections apply.

    a. For an SP, the **entityID** attribute MUST be a URL that is under the SP's control.

    b. For an AC, the **entityID** attribute MUST be a URN of the format "**urn:idmanagement.gov:icam:bae:v2:[LI]**" where "**[LI]**" is to be replaced with a value that was agreed upon between the AC and the NIEF Center.[2]

    c. For an AP, the **entityID** attribute MUST be a URN of the format "**urn:idmanagement.gov:icam:bae:v2:[LI]**" where "**[LI]**" is to be replaced with a value that was agreed upon between the AP and the NIEF Center.[2]

2. If the **<EntityDescriptor>** appears within a signed **<EntitiesDescriptor>**, then the **<ds:Signature>** element within **<EntityDescriptor>** MUST NOT be present. If the **<EntityDescriptor>** is standalone, then the **<ds:Signature>** element MUST be present, and must contain a digital signature from the NIEF Center.

3. The **validUntil** and **cacheDuration** attributes within **<EntityDescriptor>** MUST be present, with their values set using risk-based methods. It is RECOMMENDED that **cacheDuration** not exceed 18 hours.

[2] The purpose of this requirement is to support the NIEF-WS Attribute Provider SIP which adopts the requirements of the SAML 2.0 Identifier and Protocol Profiles for Backend Attribute Exchange (BAE) v2.0 which is published at http://idmanagement.gov/sites/default/files/documents/BAE_v2_SAML2_Profile_Final_v1.0.0.pdf

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

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

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

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

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

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

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

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

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

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

8. Each **<EntityDescriptor>** element MAY contain one **<Extensions>** element, and the **<Extensions>** element MAY contain one **<mdattr:EntityAttributes>** element as defined by [SAML2 Entity Attr]. The **<mdattr:EntityAttributes>** element MAY contain zero or more SAML **<Attribute>** elements, in accordance with [SAML2 Entity Attr].

9. If the **<EntityDescriptor>** element pertains to an IDP that has been certified at one or more NIST Levels of Assurance under the Federal Identity, Credentialing, and Access Management (FICAM) trust framework or an equivalent trust framework, then it MUST contain one **<Extensions>** element, and the **<Extensions>** element MUST contain one **<mdattr:EntityAttributes>** element as

defined by [SAML2 Entity Attr]. The **<mdattr:EntityAttributes>** element MUST contain a SAML **<Attribute>** element containing the list of NIST Levels of Assurance (LOAs) that the IDP is certified to assert. These LOAs MUST be expressed in accordance with the SAML Identity Assurance Certification Attribute Profile, which can be found in Section 3 of [SAML2 Assurance]. Specific **<AttributeValue>** elements MUST contain values that pertain to valid FICAM LOAs, as per the following list of values.

- **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**

In this case, the **<mdattr:EntityAttributes>** element MAY also contain zero or more additional SAML **<Attribute>** elements, in accordance with [SAML2 Entity Attr].

10. Each **<EntityDescriptor>** element SHOULD contain one **<Organization>** element. If it is present, the **<Organization>** element SHOULD contain at least one of each of these elements: **<OrganizationName>**, **<OrganizationDisplayName>**, and **<OrganizationURL>**.

5.2.3 SAML <IDPSSODescriptor> Element Requirements

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

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

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

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

4. Each **<IDPSSODescriptor>** element MAY contain one **<Extensions>** element, and the **<Extensions>** element MAY contain one **<mdattr:EntityAttributes>** element as defined by

[SAML2 Entity Attr]. The **<mdattr:EntityAttributes>** element MAY contain zero or more SAML **<Attribute>** elements, in accordance with [SAML2 Entity Attr].

5. At least one **<KeyDescriptor>** element containing a **use** attribute with a value of "**signing**" MUST be present within **<IDPSSODescriptor>**.

6. Each **<KeyDescriptor>** 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. Other sub-elements of the **<KeyDescriptor>** element are permitted, but they MUST represent the same key.

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

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

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

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

11. The **<IDPSSODescriptor>** element MUST contain a series of SAML **<Attribute>** elements, with one **<Attribute>** element for each attribute supported by the IDP.

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

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

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

5.2.4 SAML <SPSSODescriptor> Element Requirements

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

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

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

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

4. Each **<SPSSODescriptor>** element MAY contain one **<Extensions>** element, and the **<Extensions>** element MAY contain one **<mdattr:EntityAttributes>** element as defined by [SAML2 Entity Attr]. The **<mdattr:EntityAttributes>** element MAY contain zero or more SAML **<Attribute>** elements, in accordance with [SAML2 Entity Attr].

5. At least one **<KeyDescriptor>** element containing a **use** attribute with a value of "**signing**" MUST be present within **<SPSSODescriptor>**.

6. At least one **<KeyDescriptor>** element containing a **use** attribute with a value of "**encryption**" MUST be present within **<SPSSODescriptor>**.

7. Each **<KeyDescriptor>** 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. Other sub-elements of the **<KeyDescriptor>** element are permitted, but they MUST represent the same key.

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

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

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

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

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

13. If the SP requires specific user attributes (e.g. from [NIEF Attrs]) as a condition of access to any of its services, then one or more **<AttributeConsumingService>** elements within **<SPSSODescriptor>** MUST be present, and each **<AttributeConsumingService>** element MUST contain the list of required user attributes for access to that service. Required attributes MUST be indicated using the **<RequestedAttribute>** element. The SP MAY either publish one **<AttributeConsumingService>** element containing the user attribute requirements for all of its available services (resources), or a series of **<AttributeConsumingService>** elements, with one element per service (resource) that it offers.

5.2.5 SAML <AttributeAuthorityDescriptor> Element Requirements

The following requirements apply to **<AttributeAuthorityDescriptor>** elements that appear in the NIEF Cryptographic Trust Fabric document. Each

<AttributeAuthorityDescriptor> element provides metadata for the SAML services provided by a specific NIEF AP. These requirements supplement the requirements described in [SAML2 Metadata].

1. The **protocolSupportEnumeration** attribute within **<AttributeAuthorityDescriptor>** MUST be present, and MUST include both of the following values:

    - "**urn:oasis:names:tc:SAML:2.0:protocol**"
    - "**http://gfipm.net/standards/webservices/1.1/attribute-provider-sip.html**".

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

3. Each **<AttributeAuthorityDescriptor>** element MAY contain one **<Extensions>** element, and the **<Extensions>** element MAY contain one **<mdattr:EntityAttributes>** element as defined by [SAML2 Entity Attr]. The **<mdattr:EntityAttributes>** element MAY contain zero or more SAML **<Attribute>** elements, in accordance with [SAML2 Entity Attr].

4. At least one **<KeyDescriptor>** element containing a **use** attribute with a value of "**signing**" MUST be present within **<AttributeAuthorityDescriptor>**.

5. If the AP endpoint supports XML encryption, then at least one **<KeyDescriptor>** element containing a **use** attribute with a value of "**encryption**" MUST be present within **<AttributeAuthorityDescriptor>**.

6. Each **<KeyDescriptor>** 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. Other sub-elements of the **<KeyDescriptor>** element are permitted, but they MUST represent the same key.

7. At least one **<NameIDFormat>** element MUST be present within **<AttributeAuthorityDescriptor>**. The following additional requirements also apply.

    a. If the AP supports the use of the GFIPM Federation Id User Attribute for subject identification, then one of the **<NameIDFormat>** elements MUST have a value of

"**urn:idmanagement.gov:icam:bae:v2:SAML:2.0:nameid-format:gfipm:2.0:user:FederationId**".

b. If the AP supports the use of the GFIPM Email Address Text User Attribute for subject identification, then one of the **<NameIDFormat>** elements MUST have a value of "**urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**".

c. If the AP supports the use of the FASC-N identifier of a PIV credential for subject identification, then one of the **<NameIDFormat>** elements MUST have a value of "**urn:idmanagement.gov:icam:bae:v2:SAML:2.0:nameid-format:fasc-n**".

d. If the AP supports the use of the UUID of a PIV-I credential for subject identification, then one of the **<NameIDFormat>** elements MUST have a value of "**urn:idmanagement.gov:icam:bae:v2:SAML:2.0:nameid-format:uuid**".

e. If the AP supports the use of the X.509 Subject Distinguished Name for subject identification, then one of the **<NameIDFormat>** elements MUST have a value of "**urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName**".

8. At least one **<AttributeService>** element MUST be present within **<AttributeAuthorityDescriptor>**. The requirements in the following subsections apply to each **<AttributeService>** element.

   a. The **Binding** attribute MUST be present, and its value MUST be "**urn:oasis:names:tc:SAML:2.0:bindings:SOAP**".

   b. The **Location** attribute MUST be present and its value MUST specify a live service endpoint (URL) of the AP.

9. The **<AttributeAuthorityDescriptor>** element MUST contain a series of SAML **<Attribute>** elements, with one **<Attribute>** element for each attribute supported by the AP.

10. The <**AssertionIDRequestService>** element within **<AttributeAuthorityDescriptor>** MUST NOT be present.

11. One or two **<AttributeProfile>** elements MUST be present within **<AttributeAuthorityDescriptor>** to indicate that the AP supports encrypted or clear-text subject identifiers, or both, as follows:

    a. If the AP supports clear-text subject identifiers, then one of the **<AttributeProfile>** elements MUST have a value of "**urn:idmanagement.gov:icam:bae:v2:SAML:2.0:profiles:query:attribute:nameid-cleartext**".

    b. If the AP supports encrypted subject identifiers, then one of the **<AttributeProfile>** elements MUST have a value of "**urn:idmanagement.gov:icam:bae:v2:SAML:2.0:profiles:query:attribute:nameid-encrypted**".

5.2.6 <md:RoleDescriptor> Element Requirements

The following requirements apply to **<RoleDescriptor>** elements that appear in the NIEF Cryptographic Trust Fabric document. Each **<RoleDescriptor>** element provides metadata for a specific NIEF Web Services endpoint. These requirements supplement the requirements described in the trust fabric extension schema for NIEF Web Services[3] and in [SAML2 Meta AR Ext].

1. The **xsi:type** attribute within **<md:RoleDescriptor>** MUST be present, and its value MUST be specified in accordance with the following subsections.

    a. If the <RoleDescriptor> element describes a Web Service Consumer (WSC), then the **xsi:type** value MUST be "**gfipmws:GFIPMWebServiceConsumerType".**

    b. If the <RoleDescriptor> element describes a Web Service Provider (WSP), then the **xsi:type** value MUST be "**gfipmws:GFIPMWebServiceProviderType".**

    c. If the <RoleDescriptor> element describes an Assertion Delegate Service (ADS), then the **xsi:type** value MUST be "**gfipmws:GFIPMAssertionDelegateServiceType".**

    d. If the <RoleDescriptor> element describes an Attribute Consumer (AC), then the **xsi:type** value MUST be "**mdext:AttributeRequesterDescriptorType".**

2. The **protocolSupportEnumeration** attribute within **<md:RoleDescriptor>** MUST be present, and its value MUST

[3] See http://gfipm.net/standards/metadata/2.1/webservices.

consist of a list of one or more supported NIEF Web Services service interaction profiles (SIPs), delimited by spaces (" ") specified using the following URIs.[4,5]

- **`http://gfipm.net/standards/webservices/1.0/consumer-provider-sip.html`**
- **`http://gfipm.net/standards/webservices/1.0/user-consumer-provider-sip.html`**
- **`http://gfipm.net/standards/webservices/1.0/trusted-identity-broker-sip.html`**
- **`http://gfipm.net/standards/webservices/1.0/saml-assertion-delegate-service-sip.html`**
- **`http://gfipm.net/standards/webservices/1.1/attribute-provider-sip.html`**

3. Each **`<RoleDescriptor>`** element MAY contain one **`<Extensions>`** element, and the **`<Extensions>`** element MAY contain one **`<mdattr:EntityAttributes>`** element as defined by [SAML2 Entity Attr]. The **`<mdattr:EntityAttributes>`** element MAY contain zero or more SAML **`<Attribute>`** elements, in accordance with [SAML2 Entity Attr].

4. At least one **`<KeyDescriptor>`** element containing a **`use`** attribute with a value of "**`signing`**" MUST be present within **`<RoleDescriptor>`**.

5. If the endpoint supports XML encryption, then at least one **`<KeyDescriptor>`** element containing a **`use`** attribute with a value of "**`encryption`**" MUST be present within **`<RoleDescriptor>`**.

6. Each **`<KeyDescriptor>`** 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. Other sub-elements of the **`<KeyDescriptor>`** element are permitted, but they MUST represent the same key.

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

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

7. If the **<RoleDescriptor>** element has a type of **mdext:AttributeRequesterDescriptorType**, then the additional requirements in the following subsections apply.

    a. The **WantAssertionsSigned** attribute MUST be present and its value MUST be "true".

    b. The **<RoleDescriptor>** element SHOULD, for descriptive and discovery purposes, contain at least one **<AttributeConsumingService>** element that contains a series of **<RequestedAttribute>** elements that denotes the set of attributes that the AC may request from an AP.

5.3 Trust Fabric Lifecycle Management Procedures

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

5.3.1 Providing Federated System Entity Metadata to the NIEF Center

The NIEF Cryptographic Trust Fabric document is produced by the NIEF Center and comprises metadata about each system endpoint within NIEF. It is the responsibility of the NIEF Center to keep the NIEF Cryptographic Trust Fabric document up-to-date with the correct information for all NIEF system endpoints.

To enable the NIEF Center to keep the NIEF Cryptographic Trust Fabric document up-to-date, each IDPO, APO, SPO, and SCO in NIEF MUST provide the necessary metadata to the NIEF Center prior to its initial participation in NIEF, and on an ongoing basis thereafter any time that the metadata changes.

The NIEF Center SHALL notify each NIEF participating organization about the specific metadata that the member must keep up-to-date. This metadata typically differs based on the type of member organization (IDPO, APO, SPO, or SCO) and the specific systems and system endpoints implemented by the member organization.

5.3.2 NIEF Trust Fabric Creation Procedure (Nonnormative)

Upon the occurrence of a triggering condition for a Trust Fabric update (see Section 5.3.4), the NIEF Center regenerates the NIEF Cryptographic Trust Fabric. The process of generating a new Trust Fabric document consists of two basic operations: editing the document to reflect the desired policy change (e.g., new IDP added to NIEF) and digitally signing the new document with the NIEF Center's Trust Fabric signing key. The following steps describe how the basic NIEF Cryptographic Trust Fabric creation process works.

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

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

3. Connect the flash token containing the unsigned NIEF Cryptographic Trust Fabric document to the physical machine on which the signing operation will be performed. Also connect the USB flash token containing the NIEF Center's Trust Fabric signing key to the machine.[6]

4. Perform the cryptographic signing operation on the NIEF Cryptographic Trust Fabric document using the NIEF Center's Trust Fabric signing key. At no point during this operation is the NIEF Center's Trust Fabric signing key copied from the flash token onto any other storage device. Also, at no point during this operation is the physical machine connected to a network.

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

5.3.3 NIEF Trust Fabric Distribution Procedure (Nonnormative)

Upon the occurrence of a triggering condition for a Trust Fabric update (see Section 5.3.4), and after the generation and signing of a new Trust Fabric document (see Section 5.3.2), the NIEF Center distributes an updated version of the NIEF Cryptographic Trust Fabric document to all NIEF participants. The following steps describe how the basic NIEF Cryptogrphic Trust Fabric distribution process works.

1. Publish the new NIEF Cryptographic Trust Fabric document at a well-known URL.[7]

2. Notify all NIEF participants of the new NIEF Cryptographic Trust Fabric document via the technical contact points they have provided.

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

5.3.4 Triggering Conditions for NIEF Trust Fabric Updates

[6] See [NIEF CP] for a more detail about how NIEF's Trust Fabric signing key is managed.
[7] See Appendix B for the current URL at which the NIEF Cryptographic Trust Fabric document is published.

The NIEF Center MUST regenerate and redistribute the NIEF Cryptographic Trust Fabric upon the occurrence of any of the following events.

1. A new system entity (e.g., IDP, SP, AP, AC, WSC, or WSP) begins participating in NIEF.

2. An existing system entity withdraws from participation in NIEF.

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

4. The NIEF Center's Trust Fabric signing key certificate expires.

5. It is suspected that the NIEF Center's Trust Fabric signing key has been compromised.

6. The current Trust Fabric document has expired or is due to expire in the very near future.

Note that (1) and (2) are usually (but not always) caused when an organization begins participating in NIEF or withdraws from NIEF.

5.3.5 Import and Consumption of Trust Fabric by NIEF Members

A NIEF Metadata-Consuming System is any system that implements one or more NIEF-facing endpoints and relies on the NIEF Cryptographic Trust Fabric as a basis for its cryptographic trust decisions.

1. A NIEF Metadata-Consuming System MUST support at least one of the following mechanisms for automated import of NIEF Cryptographic Trust Fabric documents:

    a. Automated import from a remote resource at a fixed location accessible via HTTP 1.1 over TLS 1.1 or higher; or
    b. Automated import from a local file obtained out-of-band.

2. At trust fabric consumption time, a NIEF Metadata-Consuming System MUST perform XML signature verification at the root level of the NIEF Cryptographic Trust Fabric document, and MUST NOT import the contents of the document unless the document was signed by the NIEF Center's trust fabric signing key.

3. A NIEF Metadata-Consuming System MUST honor the **`validUntil`** and **`cacheDuration`** attributes of all **`<EntitiesDescriptor>`** and **`<EntityDescriptor>`** elements in the NIEF Cryptographic Trust Fabric document, and attempt to refresh the document before it expires. If the document cannot be refreshed before its **`cacheDuration`** expires, the system

MUST make a risk-based determination about whether to continue transacting with the affected entities. If the **`validUntil`** timestamp has passed for an **`<EntitiesDescriptor>`** or **`<EntityDescriptor>`** element, the system MUST discontinue trusting the affected entities until it obtains a new document with updated **`validUntil`** timestamps.

4. A NIEF Metadata-Consuming System SHOULD be capable of processing a NIEF Cryptographic Trust Fabric document that contains one or more **`<EntitiesDescriptor>`** elements nested within another **`<EntitiesDescriptor>`** element.

5.4 Standard NIEF Trust and Security Considerations

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

5.4.1 Digital Signature Creation and Processing

A message sender MUST sign all messages, or the appropriate parts thereof according to the rules of the applicable NIEF communication profile, using the sender's digital signature certificate that appears in the NIEF Cryptographic Trust Fabric document. The digital signature allows the recipient of the message to authenticate the sender and confirm that the message has not been altered since the time at which the signature was applied.

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

2. The recipient MUST verify that the sender of the message is included in the NIEF Cryptographic Trust Fabric document.

3. If inclusion in the NIEF Cryptographic Trust Fabric document cannot be determined for the message sender, then the message recipient MUST reject the message.

5.4.2 Message Encryption

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

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

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

5.4.3 Minimum Requirements for Cryptographic Algorithms and Modules

For all NIEF communications, the following cryptographic algorithm and module requirements are in force.

1. For symmetric key encryption functions, all communications MUST use AES with keys of 128 bits keys or longer, or a stronger [FIPS 140-2] approved algorithm.

2. For hashing functions, all communications MUST use SHA-256, SHA-384, or SHA-512, or a stronger [FIPS 140-2] approved algorithm.

3. For public-key encryption and signing functions, all communications MUST use RSA or a stronger [FIPS 140-2] approved algorithm.

4. All NIEF-facing systems MUST use [FIPS 140-2] validated cryptographic modules for all encryption and digital signature functions.

5.5 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]), laws and regulations (e.g., [NIST SP 800-63-2]), and applicable technology standards (e.g., XML standards).

Appendix A: Extension Schema for <md:RoleDescriptor>

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

```
<?xml version="1.0" encoding="US-ASCII"?>
<xs:schema targetNamespace="http://gfipm.net/standards/metadata/2.1/webservices"
           xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:gfipmws="http://gfipm.net/standards/metadata/2.1/webservices"
           xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
           xmlns:wsa="http://www.w3.org/2005/08/addressing"
           elementFormDefault="unqualified"
           attributeFormDefault="unqualified"
           version="1.0">

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

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

    <!-- GFIPM Security Token Service which currently works as an Assertion Delegate Service -->
    <xs:complexType name="GFIPMSecurityTokenServiceType">
        <xs:complexContent>
            <xs:extension base="gfipmws:WebServiceDescriptorType">
                <xs:sequence>
                    <xs:element ref="gfipmws:SecurityTokenService" minOccurs="1"
maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>

    <!-- GFIPM Web Service Consumer -->
    <xs:complexType name="GFIPMWebServiceConsumerType">
        <xs:complexContent>
            <xs:extension base="gfipmws:WebServiceDescriptorType">
                <xs:sequence>
                    <xs:element ref="gfipmws:WebService" minOccurs="0" maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>

    <!-- Based on Section 3.1.2.1 from the WS-Federation Schemas -->
    <xs:complexType name="WebServiceDescriptorType" abstract="true">
        <xs:complexContent>
            <xs:extension base="md:RoleDescriptorType"/>
        </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="WebServiceType">
        <xs:sequence>
            <xs:element ref="gfipmws:ServiceDisplayName" minOccurs="0" maxOccurs="1"/>
```

```
            <xs:element ref="gfipmws:ServiceDescription" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="gfipmws:WebServiceEndpoint" minOccurs="1" maxOccurs="1"/>
            <xs:element ref="gfipmws:MetadataExchangeEndpoint" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="gfipmws:WSDLEndpoint" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
        <xs:attribute name="endpointID" type="md:entityIDType" use="required"/>
    </xs:complexType>

    <xs:element name="WebService"  type="gfipmws:WebServiceType" />
    <xs:element name="SecurityTokenService" type="gfipmws:WebServiceType" />

    <xs:element name="WebServiceEndpoint" type="wsa:EndpointReferenceType"/>
    <xs:element name="MetadataExchangeEndpoint" type="wsa:EndpointReferenceType"/>
    <xs:element name="WSDLEndpoint" type="wsa:EndpointReferenceType"/>

    <xs:element name="ServiceDisplayName" type="xs:string"/>
    <xs:element name="ServiceDescription" type="xs:string"/>

</xs:schema>
```

Figure 2: Extension Schema for `<md:RoleDescriptor>`

Appendix B: NIEF Cryptographic Trust Fabric

The most recent version of the NIEF Cryptographic Trust Fabric document is always available at the following URL.

https://nief.gfipm.net/trust-fabric/nief-trust-fabric.xml

This document is signed by the NIEF Center, and it conforms to all normative rules specified in Section 5.2 of this document.