National Identity Exchange Federation

Cryptographic Trust Fabric Management Policy

Version 1.0

August 18, 2014

Table of Contents

1 Introduction

In order to allow for the connection of multiple parties in a trusted environment known as the National Identity Exchange Federation (NIEF), the National Identity Exchange Federation Center ("NIEF Center") has adopted a suite of technical specifications and profiles that provide for the establishment and operation of secure, interoperable communication profiles between NIEF members for the purpose of exchanging information subject to appropriate access control policies. One of the specifications adopted by the NIEF Center is the NIEF Cryptographic Trust Model [NIEF Trust], which is a normative specification that describes the structure of a NIEF Cryptographic Trust Fabric (Trust Fabric). This "Trust Fabric" concept comes from the Security Assertion Markup Language (SAML) 2.0 suite of standards – specifically from the normative SAML 2.0 Metadata specification[1] – and refers to a cryptographically signed XML document containing names, service endpoints, X.509 certificates, and other ancillary information about the members of a federation. In the NIEF security paradigm, the Trust Fabric defines the membership of a federation at a specific point in time.

While the NIEF Center and its members do not rely on a traditional Public Key Infrastructure (PKI) security model, their reliance on the Trust Fabric requires implicit reliance on the proper lifecycle management process for the X.509 certificates that appear in that Trust Fabric, as well as the private keys corresponding to those X.509 certificates. In addition, the NIEF Center and its members rely on the cryptographic integrity of the Trust Fabric, which requires implicit reliance on the lifecycle management process for the X.509 certificate and corresponding private key used by the NIEF Center to sign the Trust Fabric (NIEF Master Key). For these reasons, the NIEF Center has adopted the NIEF Center Certificate Policy [NIEF CP] and this NIEF Cryptographic Trust Fabric Management Policy [NIEF CTFMP].

While [NIEF Trust] prescribes the format and required content in the Trust Fabric, this guide provides the procedures to be used by the NIEF Center and its members for the management of its assembly, maintenance, and distribution.

Note that NIEF members often have multiple roles - Identity Provider Organizations (IDPOs), Attribute Provider Organizations (APOs), Service Provider Organizations (SPOs), and/or Service Consumer Organizations (SCOs). Therefore many of the sections of this document must be read from multiple perspectives to fully understand the responsibilities of each party.

[1] See http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

1.1 Definitions and Acronyms

The following acronyms are used in this guide and related GFIPM and NIEF documents. Some of the terms listed below are defined or described in more detail in [GFIPM Terms].

Acronym	Meaning
AC	Attribute Consumer
AP	Attribute Provider
APO	Attribute Provider Organization
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DS	Discovery Service
GFIPM	Global Federated Identity and Privilege Management
IDP	Identity Provider
IDPO	Identity Provider Organization
NIEF	National Identity Exchange Federation
NIEF Master Key	The private key used by the NIEF Center to sign the NIEF Cryptographic Trust Fabric
Public NIEF Master Key	The public key used by the NIEF members to validate signatures applied by the NIEF Master Key
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
SP	Service Provider
SCO	Service Consumer Organization
SPO	Service Provider Organization
Trust Fabric	The NIEF Cryptographic Trust Fabric
WSC	Web Service Consumer
WSP	Web Service Provider

1.2 Applicability of This Document

This guide applies to the NIEF Center and all its members: Identity Provider Organizations (IDPOs), Attribute Provider Organizations (APOs), Service Provider Organizations (SPOs), and

Service Consumer Organizations (SCOs). (All of these organizations are collectively referred to as "members".)

1.3 NIEF Identity Trust Framework

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

1.4 References

Table 1 provides a list of references used within this document.

References	
Document ID	Document Name and URL
NEIF Terms	NIEF Terminology Reference
NIEF CTFMP	NIEF Cryptographic Trust Fabric Management Policy (This document)
NIEF Trust	NIEF Cryptographic Trust Model
NIEF Bylaws	NIEF Center Bylaws
NIEF OPP	NIEF Center Operational Policies and Procedures
NIEF CP	NIEF Center Certificate Policy
FIPS 140-2	Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules,* 3 December 2002.
RFC 3647	Internet Engineering Task Force (IETF) Request for Comments 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", November 2003

Table 1: References

1.5 Definitions and Perspective of This Document

The following paragraphs delineate the fundamental differences between the [NIEF Trust] model and a traditional PKI trust model, to provide the appropriate context for the remainder of this document.

Traditional PKI certificate policies typically describe the responsibilities of a single *certificate authority* (CA): an entity that issues certificates for use by one or more *subscribers*, for the benefit of one or more *relying parties* (RPs). They also typically describe the responsibilities of subscribers and relying parties. The concepts of CA, subscriber, and RP are related to the [NIEF Trust] model as follows.

1. The NIEF Center as well as all NIEF Center member agencies are analogous to subscribers in the PKI trust model, however they are not subscribers in the traditional sense. Rather than receiving X.509 certificates that a CA has generated for them, and relying on traceability to a common root CA, NIEF members are responsible for generating their own certificates, and rely on the NIEF Center's signing of the Trust Fabric to vouch for the certificates it contains.

2. Each NIEF Center member acts as a CA for the X.509 certificates that it generates and manages, and which appear in the Trust Fabric. No NIEF Center member generates certificates for another member, i.e. each subscriber generates and manages its own certificates and corresponding public/private key pairs.

3. The NIEF Center acts as a CA for the X.509 certificate that it generates and manages, and which is used to cryptographically sign the Trust Fabric and thereby ensure the integrity of the Trust Fabric.

4. Each NIEF Center member acts as a relying party (RP), in that it relies on the integrity of the lifecycle management process for the X.509 certificates that are generated and managed by other NIEF Center member agencies, and which appear in the Trust Fabric.

5. Each NIEF Center member also acts as a relying party (RP) in that it relies on the integrity of the lifecycle management process for the X.509 certificate that is generated and managed by the NIEF Center, and which is used to cryptographically sign the Trust Fabric.

6. Finally, note that the traditional PKI concept of a registration authority (RA) has no meaning in this guide, since the NIEF Center's security model does not require registration of subscribers with a CA in the traditional sense.

1.6 Document Administration

1.6.1 Document Name and Identification

The name of this document is: "National Identity Exchange Federation Center Cryptographic Trust Fabric Management Guide".

1.6.2 Organization Administering the Document

The NIEF Center is the administering organization for this guide. The NIEF Center's full name and mailing address is:

Georgia Tech Applied Research Corporation
National Identity Exchange Federation Center
Georgia Tech Research Institute
ITTL/IEAD 0832
250 14th Street NW
Atlanta, GA 30332-0832

1.6.3 Contact Person

The contact person for the NIEF Center is:

John Wandelt, National Identity Exchange Federation Center Director
Georgia Tech Research Institute
ITTL/IEAD 0832
250 14th Street NW
Atlanta, GA 30332-0832

Phone: 404-407-8956

Email: John.Wandelt@gtri.gatech.edu

1.6.4 Entity Determining Guide Suitability

The NIEF Center and NIEF Advisory Board (AB) determine the suitability of this guide.

1.6.5 Guide Approval Procedures

This guide requires approval by the NIEF Center Director and NIEF Executive Committee.

1.6.6 Publication

All NIEF policy documents, including this guide, related NIEF Center policies, and policy documents submitted by NIEF members, are published in the NIEF Portal, which is a non-public repository. They are available to NIEF Portal account holders, subject to appropriate access controls.[2]

[2] NIEF Portal account holders with the "Organization Administrator" or "Federation Administrator" role are eligible to download and view NIEF policy documents via the portal. Other users are denied access.

2 Trust Fabric Management

2.1 NIEF Master Key Management

2.1.1 NIEF Master Key Generation

The (private) NIEF Master Key and Public NIEF Master Key SHALL be generated as an RSA 4096-bit RSA public/private key pair. The command line version of OpenSSL is currently used to perform this task.

The Public NIEF Master Key is published as a self-signed X.509 certificate with the following issuer and attributes:

- Issuer and Subject equaling C=US, ST=GA, L=Atlanta, O=National Identity Exchange Federation, OU=NIEF Trust Operations, CN=NIEF Certificate Authority
- emailAddress set to help@gfipm.net
- Validity window to not exceed five years.

2.1.2 NIEF Master Key Changeover

Anytime during the final two years of validity of the NIEF Master Key, a new key pair and certificate may be generated to replace the current certificate and key pair. When this occurs, all members will be notified of the new certificate and from where this new certificate may be downloaded. After a period to not exceed 30 days, the new key and certificate will be used to sign the Trust Fabric.

2.1.3 NIEF Master Key Protection

The NIEF Master Key SHALL be kept on a removal flash drive that is kept in a locked container when not in use, and SHALL only be used with an offline computer designated for Trust Fabric operations.

2.1.4 NIEF Master Key Validation

When initially retrieving the Public NIEF Master Key X.509 certificate, and upon retrieving any subsequently issued certificates, the NIEF members MUST confirm the validity of the certificate through verbal communication with the NIEF Center verifying the certificate's SHA-1 fingerprint.

2.2 Vetting of Trust Fabric Entries

2.2.1 Authentication of Organization Identity

This section pertains to the validation of identities to which X.509 certificates are bound, for the purpose of installing a new entry and corresponding certificate in the Trust Fabric on behalf of a new member. Note that in the NIEF trust model, identities are bound to certificates not through the names in those certificates, but through the Trust Fabric.

During the application and onboarding process, and prior to including a member in the Trust Fabric, the NIEF Center MUST perform the following tasks.

1. Vet the legitimacy of the member as a legal entity.
2. Vet the legitimacy of the points of contact (POCs) that have been listed on the member's application form as representatives of the member.

The processes used to accomplish these tasks are outside the scope of this guide. Please refer to [NIEF Bylaws] and/or [NIEF OPP] for details about these processes.

2.2.2 Transmittal of Entry Metadata to NIEF

Members providing their initial metadata for including in the Trust Fabric, or requesting updates to that information MUST use the following procedure for transmitting their information to the NIEF Center:

1. The NIEF Member contacts the NIEF Center via email or phone at one of its documented points of contact (POC). The purpose of this communication is to coordinate the transmission of the member's information, e.g. the E-mail address of the NIEF Center technical representative to send the file to, etc.

2. After acquiring the email address of the NIEF's Center's technical representative, the NIEF member's representative E-mails their Trust Fabric entry. It is RECOMMENDED that the member digitally sign this entry prior to transmission using the private key for the signing certificate contained within the entry, as this ensures the integrity of the transmitted data.

3. If signed, the NIEF Center representative validates the signature on the overall entry using the public key from the certificate it contains. If the signature is found to be invalid, the entry MUST NOT be accepted for inclusion in the Trust Fabric.

4. Upon verification of the entry's digital signature (or if none was provided), the process continues in order to verify the member's possession of the private key for the certificate contained within the entry.

5. If the entry was not signed, the member and NIEF representative MUST conduct a verbal exchange to verify the entry's contents.

2.2.3 Method to Prove Possession of Private Key

Before the NIEF Center will bind a certificate to a member, the member MUST prove possession of the private key corresponding to that certificate through a simple cryptographic challenge-response protocol. The process of proving private key possession SHALL proceed as follows.

NOTE: If the provided trust fabric entry was signed and the signature verified, the following steps are NOT necessary:

1. A NIEF Center representative contacts the member via email or phone at one of its documented points of contact (POC).[3] The purpose of this communication is to identify the technical representative of the member who will be designated to participate in the challenge-response protocol on behalf of the member.

2. After acquiring the email address of the member's technical representative, a NIEF Center representative generates a sufficiently long random value (at least 160 bits), encrypts it using the public key of the certificate that the member wishes to bind to its identity, and sends the encrypted value to the member's designated technical representative via email, along with a set of instructions for decrypting the value.

3. The member's designated technical representative decrypts the encrypted value using the private key corresponding to the certificate that the member wishes to bind to its identity, and sends the decrypted value to the NIEF Center representative via email.

4. The NIEF Center representative compares the original random value with the value sent by the member's designated technical representative. If the two values match, then the member has proven possession of the private key.

In all cases, the member and NIEF Center SHALL confirm that both parties are referencing the same X.509 certificate through verbal confirmation of the certificate's SHA-1 fingerprint.

[3] At this point, the member will have already submitted an application form containing one or more POCs as part of the application process. See [NIEF Center OPP] for more information about the NIEF application process.

2.3 Trust Fabric Production and Signing

The Trust Fabric must be digitally signed to ensure its integrity, and the NIEF Master Key is used for this function.

The following procedure MUST be followed when producing the Trust Fabric for publication:

1. Before the signature may be applied, and subsequent to all updates, edits, and other changes, the unsigned Trust Fabric MUST pass schema validation.

2. XML digital signature SHALL be applied with the NIEF master key in accordance with [NIEF Trust]. Additionally, Validuntil SHALL be set to no greater than 42 days after the date the signature is applied.

3. The signed Trust Fabric MUST pass schema validation.

4. The signature applied to the Trust Fabric must be validated using the Public NIEF Master Key as contained in the NIEF Center signing certificate included in the Trust Fabric

2.4 Trust Fabric Publication

2.4.1 Published Location

The NIEF Center publishes members' certificates in the NIEF Trust Fabric, which is publicly available at the URL specified below. Member certificates are not published in any other certificate repository. [4]

The current NIEF Cryptographic Trust Fabric document SHALL be posted at the following URL.

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

In addition, for redundancy, the current Trust Fabric document MAY be posted at an alternative URL, to be chosen by the NIEF Center. This secondary location SHOULD be chosen so as to minimize the likelihood that both copies of the Trust Fabric document are unavailable simultaneously.

[4] The trust model used by NIEF does not rely on the secrecy of the Trust Fabric.

2.4.2 Time or Frequency of Publication

The NIEF Center SHALL publish a revised version of the Trust Fabric every 30 days, and whenever changes to the federation membership or other circumstances such as the updates described in Section 2.6 necessitate it. Upon publication of a new Trust Fabric, the NIEF Center SHALL notify all NIEF members about the revision via the technical contact points they have provided, as per the instructions in [NIEF Trust].

Members MUST implement the new revision of the Trust Fabric within their local systems within one business day after receiving notification of its publication.

2.5 Trust Fabric Use

NIEF members MAY use Trust Fabric entries to establish trust and trusted communications with other members. NIEF members are NOT REQUIRED to trust any entries in the Trust Fabric.

Per [NIEF Trust], NIEF members MUST perform XML signature verification at the root level of the Trust Fabric, and MUST NOT rely on the contents of the document unless the document was signed by the NIEF Master Key.

2.6 Trust Fabric Updates

Per [NIEF Trust], the Trust Fabric MUST be regenerated and redistributed upon the occurrence of any of the following events.

1. A new system entity (e.g., IDP, SP, AP, AC, WSC, or WSP) joins the federation.
2. An existing system entity leaves the federation.
3. An existing system entity undergoes a configuration change that affects its entry in the Trust Fabric (e.g., certificate expiration, migration to a new server, key compromise on a server, etc.).
4. The NIEF Master Key expires.
5. It is suspected that the NIEF Master Key has been compromised.
6. The current Trust Fabric has expired or is due to expire in the very near future.

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

The sections that follow address the handling of these situations.

2.6.1 Addition of a New Trust Fabric Entry

The action of installing the new entry in the Trust Fabric indicates that the member has met all the requirements of the NIEF application and onboarding processes as defined in [NIEF OPP]. It also indicates that the subscriber has proven possession of the private key corresponding to the signing certificate in that entry.

After undergoing the formal application and onboarding process, a member MUST generate its own certificate and prove possession of the private key corresponding to that certificate before the NIEF Center will allow that certificate to be installed in the Trust Fabric. See Section 2.2.3.

The NIEF Center SHALL NOT install an entry in the Trust Fabric until after the member has completed these steps.

2.6.2 Updates to Certificates in a Trust Fabric Entry

A member MAY request a certificate update upon any of the following circumstances.

1. A certificate in the Trust Fabric, belonging to the member, is within 120 days of expiration.
2. The private key corresponding to a certificate in the Trust Fabric has been compromised, or is suspected of having been compromised.
3. A change to the NIEF technical specifications necessitates a certificate update.
4. A certificate in the Trust Fabric belonging to the member needed to be reissued for other technical or policy reasons.

Prior to updating the Trust Fabric entry with a new/updated certificate, its possession by the member MUST be verified via the procedure outlined in Section 2.2.3.

Note, however, that for circumstances in which a member updates a certificate but does not change the private key on which the certificate is based, the proof-of-possession process described in Section 2.2.3 is unnecessary.

The NIEF Center SHALL honor any request for a certificate update that comes from a representative of the member for which the request is made, provided that the request contains a new certificate with an effective date that is no later than the present date and an expiration date that is later than the expiration date of the certificate that this new certificate is intended to replace.

In addition, the NIEF Center itself MAY initiate the update process for any certificate in the Trust Fabric when appropriate, as per the circumstances outlined above.

For routine certificate update requests, the NIEF Center SHALL process the request within 15 days of receiving the request, and SHALL ensure that the process is complete no less than 15 days before the expiration date of the public/private key pair corresponding to the certificate that the request is intended to replace.

2.6.3 Updates to Non-Certificate Data of a Trust Fabric Entry

The NIEF Center SHALL honor any request for updates to a Trust Fabric entry that DOES NOT pertain to certificate data provided the request comes from a representative of the member organization for which the update is to be made.

In addition, the NIEF Center itself MAY initiate the update process for any entry in the Trust Fabric when appropriate, as per the circumstances outlined above.

For routine Trust Fabric entry update requests, the NIEF Center SHALL process the request within 15 days of receiving the request.

2.6.4 Removal of a Trust Fabric Entry

At any time, any NIEF Center member representative MAY request that a specific entry be removed from the Trust Fabric by contacting the NIEF Center at the point of contact specified in Section 1.6.3.

Before honoring the request, the NIEF Center SHALL verify the legitimacy of the request by contacting one or more of the official points of contact (POCs) for the member that issued the request as well as the member to which the request pertains.

Any member MAY request removal for any entry in the Trust Fabric upon any of the following circumstances.

1. A certificate in the Trust Fabric entry has expired.

2. The private key corresponding to a certificate in the Trust Fabric entry has been compromised, or is suspected of having been compromised.

3. Suspension of NIEF membership

4. The requesting member wishes to no longer participate as a member of NIEF. (See Section 2.6.9 for more information.)

In addition, the NIEF Center itself MAY initiate the removal process for any entry in the Trust Fabric when appropriate, as per the circumstances outlined above.

2.6.4.1 Procedure for Removal Request

The NIEF Center SHALL respond to a removal request as follows.

If the member to which the entry in question belongs ("affected member") is the same as the requesting member, or the affected member concedes to the removal of the entry in question, the NIEF Center SHALL immediately remove the entry from the Trust Fabric, republish the Trust Fabric without the entry, and notify all members, as per the instructions in Section 2.6.6.

Should the affected member disputes the requesting member's claim, then the NIEF Center SHALL treat the matter as a dispute between the members and resolve it as per [NIEF Bylaws and NIEF OPP].

2.6.4.2 Removal Request Grace Period

In general, the NIEF Center SHALL NOT implement any removal request grace period. In the case of a dispute between members that arises over a removal request, the NIEF Bylaws [NIEF Bylaws and NIEF OPP] SHALL govern the resolution process.

2.6.4.3 Time within Which Removal Requests MUST Be Processed

The NIEF Center SHALL process a removal request as soon as reasonably possible, and the NIEF Center SHALL NOT under any circumstances wait longer than one business day after receiving the request, before processing it.

For requests that affect a member other than the requesting member, the affected member MUST provide an initial acknowledgment of the removal request as soon as reasonably possible, and the affected member SHALL NOT under any circumstances wait longer than one business day after receiving the request, before providing an initial acknowledgment of it.

Due to the time-sensitive and security-critical nature of removal requests due to compromised certificates, it is important that the NIEF Center and all members treat such requests with utmost urgency, so that requests can be resolved as quickly as possible.

2.6.5 Review of Trust Fabric Changes

The NIEF Center SHALL allow members to review any change to the Trust Fabric that affects one or more of that member's Trust Fabric entries.[5] This allows the member to confirm whether

[5] Acceptance of a change to the NIEF Trust Fabric is NOT REQUIRED for revocation (removal from the Trust Fabric).

the change is correct, and helps to prevent incorrect information from being formally published in the Trust Fabric.

2.6.6 Notice of Trust Fabric Updates

The NIEF Center SHALL notify the members via email to the member's designated point(s) of contact when requesting acceptance of a change to the Trust Fabric. The email SHALL either contain the proposed revision to the Trust Fabric as either an attachment or a pointer (URL) to a location where the revision can be downloaded and inspected.

The member SHALL notify the NIEF Center via an email reply as soon as possible to indicate whether it formally accepts the Trust Fabric change.

After receiving notice of the member's formal acceptance of the revised Trust Fabric, the NIEF Center SHALL publish the updated Trust Fabric as described in Section 2.4.

If the member does not reply to the NIEF Center within three (3) business days after receiving the request for acceptance, the NIEF Center MAY proceed with the publication of the revised Trust Fabric as if the member had formally accepted it.

2.6.7 Urgent Requests - Key Compromise or Suspected Compromise

NIEF does not employ a traditional PKI trust model, and the NIEF Center does not issue certificates to its members, so the concept of certificate revocation as it applies to a traditional PKI is not directly applicable. The NIEF trust model does prescribe appropriate actions to prevent relying parties from trusting a certificate that is known or suspected to have been compromised; however, rather than using certificate revocation to accomplish this goal, NIEF accomplishes it via removal of entries from the Trust Fabric.

When requesting a certificate update, the member SHALL indicate whether the request is being made as the result of a private key compromise or suspected private key compromise. If key compromise has occurred or is suspected, all parties involved SHALL treat the request as urgent and cooperate to complete the process as quickly as possible.

For urgent requests, the NIEF Center SHALL process the request in two separate parts:

1. Immediate removal of the affected entry from the Trust Fabric to effect revocation of the compromised certificate, performed in accordance with the rules specified in Section 2.6.4; and
2. Acceptance of a new certificate, with a new public/private key pair, to replace the compromised certificate, performed in accordance with the rules specified in Sections 2.2.3, 2.6.5, and 2.6.6.

2.6.8 Suspension

Any NIEF member representative, Advisory Board (AB) member, or Executive Committee member MAY request suspension of a member.

To request suspension of a member, the requestor MUST contact the NIEF Center Director in writing at the address or email address specified in Section 1.6.3. The suspension request MUST include a justification for requesting the suspension. See [NIEF Bylaws] and [NIEF OPP] for more information.

The NIEF Center handles suspension from the federation via removal of its entries from the Trust Fabric.

A member MAY be suspended by the NIEF Center at any time, and for any reason, at the discretion of the NIEF Center Director.

At any time after a suspension has occurred, the member MAY be reinstated via reinsertion into the Trust Fabric, also at the discretion of the NIEF Center Director. Reinstatement MAY require new certificate(s) to be generated by the member, and depending on the specific circumstances the member MAY be required to perform additional actions to demonstrate that it has sufficiently mitigated the security vulnerability, risk, or other situation that precipitated its suspension and removal from the Trust Fabric.

For more information about the policies and procedures that the NIEF Center follows in making decisions about federation membership changes, please see [NIEF OPP].

All disputes arising out of the suspension of a member SHALL be handled via the procedure described in [NIEF Bylaws] and [NIEF OPP].

2.6.9 Withdrawal From NIEF

In the event that a member notifies the NIEF Center of its desire to end its relationship with NIEF[6], the NIEF Center SHALL remove all entries belonging to the member from the Trust Fabric.

[6] See [NIEF Bylaws]