National Identity Exchange Federation

Certificate Policy

Version 1.3

July 31, 2018

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 Center 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 Security Assertion Markup Language (SAML) Cryptographic Trust Fabric* document. This "Trust Fabric" concept comes from the 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. The NIEF Cryptographic Trust Model also defines a JavaScript Object Notation (JSON) based structure for the NIEF Representational State Transfer (REST) Cryptographic Trust Fabric document, which captures this type of metadata for NIEF REST service endpoints. In the NIEF security paradigm, a "Trust Fabric", which is a SAML Trust Fabric document and a REST Trust Fabric document that are published in tandem, 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 NIEF Cryptographic Trust Fabric documents requires implicit reliance on the proper lifecycle management process for the X.509 certificates that appear in those Trust Fabric documents, 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 NIEF Cryptographic Trust Fabric documents, 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 documents. For these reasons, the NIEF Center has adopted the NIEF Cryptographic Trust Fabric Management Guide [NIEF CTFMP] and this NIEF Center Certificate Policy [NIEF CP].

Due to the specific details of the NIEF Center security model described above, this certificate policy (CP) does not address all the standard CP topics in the same manner that a traditional PKI CP would cover them in a format such as that defined in [RFC 3647]. Instead, it addresses the topics that are relevant to the NIEF security model, and explains the differences between a traditional PKI security model and the NIEF security model where necessary.

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

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.

A traditional PKI CP typically describes 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). A traditional PKI CP typically also describes the responsibilities of subscribers and relying parties. This NIEF CP uses the concepts of CA, subscriber, and RP, but defines them differently, as follows.

1. Subscribers to this CP include the NIEF Center as well as all NIEF Center members; however, subscribers to this CP are not subscribers in the traditional PKI sense wherein a CA has generated an X.509 certificate for them. (See the following item about certificate self-generation by subscribers.)
2. Each NIEF Center member acts as a CA in this CP for the X.509 certificates that it generates and manages, and which appear in the NIEF Cryptographic Trust Fabric. No NIEF Center member generates certificates for another member, i.e. each subscriber to this NIEF CP generates and manages its own certificates and corresponding public/private key pairs.
3. The NIEF Center acts as a CA in this CP for the X.509 certificate that it generates and manages, and which is used to cryptographically sign the NIEF Cryptographic Trust Fabric and thereby ensure the integrity of the Trust Fabric documents.
4. Each NIEF Center member acts as a relying party (RP) in this CP, 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 NIEF Cryptographic Trust Fabric.
5. Each NIEF Center member acts as a relying party (RP) in this CP, in that it also 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 NIEF Cryptographic Trust Fabric documents.

Note that in this NIEF CP, organizational entities often have multiple roles (CA, subscriber, and RP), and therefore many of the sections of this document must be read from multiple perspectives to fully understand the responsibilities of each party. Note also that this CP pertains only to certificates that appear in the NIEF Cryptographic Trust Fabric or are used by NIEF to sign the NIEF Cryptographic Trust Fabric. This CP does not pertain to, and has no direct relation to, certificates that may be generated, managed, or purchased by the NIEF Center or NIEF Center member agencies for other purposes, such as authenticating users or establishing secure SSL/TLS sessions between HTTP user agents (web browsers) and secure web applications. Finally, note that the traditional PKI concept of a registration authority (RA) has no meaning in this CP, since the NIEF Center's security model does not require registration of subscribers with a CA in the traditional sense.

Applicability of This Document

This CP 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 the subscribers to this CP.)

The NIEF Center is also a subscriber to this CP, but it does not participate in operational information-sharing transactions with other members. This CP applies to the certificate(s) and private key(s) used for signing the NIEF Cryptographic Trust Fabric.

All requirements in this document that are not targeted specifically towards one of the categories of subscribers above are applicable to all subscribers.

1.1 Overview

1.1.1 Certificate Policy

The term "certificate policy" (CP) is defined by the X.509 standard as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements".

This CP is geared towards the NIEF Center and its members (subscribers) that operate trusted software system endpoints within the federation. (A trusted software system endpoint can be an identity provider, service provider, or other service.) The NIEF Cryptographic Trust Fabric includes an entry for each trusted software system endpoint in the federation. The Trust Fabric entry for a trusted endpoint includes basic information about the endpoint (e.g. its URL, points of contact for the organization that manages the endpoint, etc.) as well as one or more X.509 certificates used by the endpoint for cryptographic operations. The purpose of the Trust Fabric is to attest, on behalf of the NIEF Center, that the X.509 certificate(s) assigned to an endpoint are legitimate and trustworthy. The purpose of this CP is to set forth a list of rules that each subscriber must obey to help ensure that the X.509 certificates assigned to their trusted software service endpoints are in fact legitimate and trustworthy, and that the NIEF Cryptographic Trust Fabric documents maintain their legitimacy and trustworthiness at all times.

1.1.2 References

Table 1 provides a list of references for documents that are related to this CP.

References for Related Documents	
Document ID	**Document Name and URL**

NIEF Terms	NIEF Terminology Reference
NIEF Audit	NIEF Audit Policy
NIEF CTFMP	NIEF Cryptographic Trust Fabric Management Policy
NIEF Trust	NIEF Cryptographic Trust Model
NIEF U2S	NIEF Web Browser User-to-System Profile
NIEF S2S	NIEF Web Services System-to-System Profile
NIEF REST	NIEF REST Services Profile
NIEF Bylaws	NIEF Center Bylaws
NIEF OPP	NIEF Center Operational Policies and Procedures
NIEF CP	NIEF Center Certificate Policy (This Document)
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 for Related Documents

1.2 Document Name and Identification

The name of this document is: "National Identity Exchange Federation Center Certificate Policy".

1.3 Policy Administration

This section includes the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of this CP. It also includes the name, electronic mail address, and telephone number of a contact person.

1.3.1 Organization Administering the Document

The NIEF Center is the administering organization for this CP. 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

1.3.2 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

1.3.3 Entity Determining CP Suitability

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

1.3.4 CP Approval Procedures

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

1.4 PKI Participants

This CP does not pertain directly to the operation of a PKI; however, this CP does impact the NIEF Center, and all NIEF Center member agencies, in various ways as called out in the following subsections.

1.4.1 Certification Authorities

Each NIEF Center member acts as a CA for the X.509 certificates that it generates and manages, and which appear in the NIEF Cryptographic Trust Fabric; however, no NIEF Center member generates certificates for another member.

In addition, 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 NIEF Cryptographic Trust Fabric and thereby ensure the integrity of the Trust Fabric documents. But the NIEF Center does not generate certificates for any member agencies.

1.4.2 Subscribers

Subscribers to this CP include the NIEF Center as well as all NIEF Center member agencies; however, subscribers to this CP are not subscribers in the traditional PKI sense wherein a CA has generated an X.509 certificate for them. As noted in Section 1.4.1, each subscriber to this CP acts as its own CA for the certificates that it uses.

1.4.3 Relying Parties

A relying party is a recipient of a certificate that acts in reliance on that certificate and/or any digital signatures verified using that certificate and/or any messages encrypted using that certificate.

Organizations that are NIEF Center members are relying parties of the X.509 certificates covered by this CP, and the NIEF Trust Fabric in which the certificates are published, in that they rely on digital signatures and message encryption operations made using certificates covered by this CP and published in the NIEF Trust Fabric. Specifically, Service Provider Organizations (SPOs), Service Consumer Organizations (SCOs), Identity Provider Organizations (IDPOs), and Attribute Provider Organizations (APOs) rely upon these certificates to authenticate digitally signed messages and to decrypt digitally encrypted messages within the scope of communications protocols and profiles defined in [NIEF U2S], [NIEF S2S], and [NIEF REST].

In addition to these "member-to-member" trust relationships, whenever NIEF Center members process a new version of one of the NIEF Trust Fabric documents, they rely on the X.509 certificate that is used by the NIEF Center to cryptographically sign the document.

1.5 Definitions and Acronyms

The following acronyms are used in this CP 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

Acronym	Meaning
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
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
SP	Service Provider
SCO	Service Consumer Organization
SPO	Service Provider Organization
WSC	Web Service Consumer
WSP	Web Service Provider
URL	Uniform Resource Locator

2 Publication and Repository Responsibilities

The NIEF Center maintains two document repositories.

All policy documents, forms, and signed agreements submitted by NIEF Center 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]

Also, the current NIEF Cryptographic Trust Fabric documents are posted at the following URL and are publicly available for download.

https://nief.org/trust-fabric/

Subscriber certificates are not published in any other certificate repository.[3]

All NIEF policy documents, including this CP and related NIEF Center policies (e.g. [NIEF Bylaws], etc.), are available to current and prospective NIEF members upon written request to the NIEF Center.

3 Certificate Issuance

The NIEF Center does not operate a traditional CA, and therefore does not issue certificates in the traditional way. In lieu of a certificate application process, NIEF stipulates a formal application and onboarding process, which is described in [NIEF OPP].

After undergoing the formal application and onboarding process, a subscriber 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 NIEF Trust Fabric. See [NIEF CTFMP] more information about this process.

4 Certificate Content

This section and its subsections pertain to the content and use of certificates that are covered by this CP. The NIEF Center does not issue private keys or certificates to NIEF Center members; however, it does perform certain security functions and stipulate certain subscriber identification and authentication rules that parallel the subscriber identification and authentication rules

[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.

[3] In a traditional PKI model, subscriber certificates are typically published in a directory, e.g. X.500 or LDAP. The Trust Fabric model used by NIEF does not require separate publication of certificates in any location other than the NIEF Trust Fabric.

stipulated for a traditional PKI. All rules described in this section are oriented towards the goal of ensuring the integrity of the NIEF Cryptographic Trust Fabric and the certificates that it contains.

4.1 Naming

This section pertains to naming and name management issues that can arise for names within X.509 certificates. As NIEF does not employ a traditional PKI trust model, many naming issues that pertain to a PKI are either not applicable to NIEF or are applicable in a slightly different context than what is typically expected in a PKI. Each subsection provides appropriate details as needed.

4.1.1 Types of Names

A certificate that is covered by this CP MAY contain any type of name, as long as the name represented is meaningful according to the requirements stipulated in Section 4.1.2.

4.1.2 Need for Names to Be Meaningful

A certificate that is covered by this CP MUST contain a name that clearly and uniquely identifies the organization that owns the certificate. In the case where multiple certificates pertain to the same organization, it is RECOMMENDED that the certificate name also identify the system or service endpoint of the subscriber and/or the purpose for which the certificate is to be used (e.g. signing only, encryption only, or both).

4.1.3 Anonymity or Pseudonymity of Subscribers

This CP does not permit anonymity or pseudonymity of subscribers. Subscribers to this CP include the NIEF Center and NIEF Center members, and the identity of each subscriber is well known to all other subscribers.

4.1.4 Uniqueness of Names

Due to the naming rules stipulated in Section 4.1.2, name collisions between certificates are possible only for certificates that pertain to the same organization. In the case where multiple certificates pertain to the same organization, it is RECOMMENDED that the certificate name also identify the system or service endpoint of the subscriber and/or the purpose for which the certificate is to be used (e.g. signing only, encryption only, or both).

4.2 Criteria for Interoperation

For proper interoperation with other subscribers and inclusion in the NIEF Cryptographic Trust Fabric, a certificate MUST meet the following criteria.

1. It MUST be a valid X.509 certificate.
2. It MUST contain the following attributes.
    a. **Subject** (See Section 4.1 and its subsections for subject naming rules.)

   b. **Version** (The X.509 version number to which this certificate conforms.)
   c. **Validity** (The "Not Before" and "Not After" dates of validity.)
   d. **Algorithm ID** (The public-key algorithm used to generate the certificate.)
   e. **Signature Algorithm** (The algorithm used to sign the certificate.)
   f. **Public Key**
3. It MAY contain additional attributes.

5 Key Pair and Certificate Usage

This section describes acceptable and prohibited usage of certificates to which this CP applies, as well as the public/private key pairs corresponding to those certificates.

5.1 Subscriber Private Key and Certificate Usage

NIEF Center members MAY use certificates to which this CP applies, as well as their corresponding private keys, for the following purposes.

1. Cryptographic signing of messages that are to be sent between trusted software service endpoints within NIEF as part of transactions that conform to NIEF Communication Profiles ([NIEF U2S], [NIEF S2S], or [NIEF REST]).
2. Decryption of encrypted messages or encrypted parts of messages sent between trusted software service endpoints within NIEF as part of transactions that conform to NIEF Communication Profiles ([NIEF U2S], [NIEF S2S], or [NIEF REST]).

All other uses are prohibited.

5.2 Relying Party Public Key and Certificate Usage

Relying parties MAY use certificates to which this CP applies, as well as their corresponding public keys, for the following purposes.

1. Verification of digital cryptographic signatures on messages sent between trusted software service endpoints within NIEF as part of transactions that conform to NIEF Communication Profiles ([NIEF U2S], [NIEF S2S], or [NIEF REST]).
2. Encryption of messages or parts of messages that are to be sent between trusted software service endpoints within NIEF as part of transactions that conform to NIEF Communication Profiles ([NIEF U2S], [NIEF S2S], or [NIEF REST]).

All other uses are prohibited.

5.3 NIEF Center Private Key and Certificate Usage

The NIEF Center MAY use its certificate to which this CP applies, as well as its corresponding private key, for the purpose of cryptographically signing individual entries within and/or the NIEF Trust Fabric documents.

All other uses are prohibited.

5.4 NIEF Center Public Key and Certificate Usage

Relying parties MAY use the NIEF Center's certificate to which this CP applies, as well as its corresponding public key to verify the NIEF Center's digital cryptographic signatures on the NIEF Trust Fabric documents and individual entries within the documents.

All other uses are prohibited.

6 Protection of Certificate Private Key

6.1 Technical Security Controls

This section contains rules representing the minimal acceptable level of technical protection that MUST be applied to sensitive private key material corresponding to certificates covered by this CP and the systems on which the private key material is used. To help ensure the trustworthiness of the NIEF Cryptographic Trust Fabric, all subscribers MUST obey the rules outlined in this section.

In some circumstances, a subscriber may already have policies and procedures in place that preclude their ability to obey these rules. In this circumstance, the subscriber MUST notify the NIEF Center in writing of its inability to meet these requirements, and MUST also provide an explanation of why it is unable to meet the requirements.

6.1.1 Key Pair Generation and Installation

This section and its subsections stipulate public/private key pair generation and installation rules for key pairs that correspond to certificates covered by this CP.

6.1.1.1 Key Pair Generation

The key pair MUST be generated by the subscriber using the RSA key generation algorithm[4], and MUST be generated on the physical machine or module within which it will be used. In addition, private key material MUST NOT appear outside of the module from which it was generated unless it is encrypted for local transmission or for processing or storage by a key recovery mechanism.

6.1.1.2 Key Sizes

All certificates governed by this CP SHALL use at least 2048-bit RSA and Secure Hash Algorithm 256 (SHA-256).

If the NIEF Center determines that the security of a particular algorithm may be compromised, it SHALL immediately remove all certificates that use the algorithm from the NIEF Trust Fabric.

6.1.1.3 Public Key Parameters Generation and Quality Checking

Public key parameters SHALL be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used.

6.1.1.4 Key Usage Purposes (As Per X.50vkey Usage Field)

See Section 5. In general, keys MAY be used for signing, encryption, or both. For keys that appear in the NIEF Trust Fabric, key usage is indicated by other attributes in the NIEF Trust Fabric documents. For the key that the NIEF Center uses to sign the NIEF Trust Fabric, key usage is limited to generating digital signatures for the NIEF Trust Fabric.

6.1.2 Cryptographic Module Standards and Controls

Cryptographic modules employed for the generation and operational use of public/private key pairs corresponding to certificates governed by this CP MUST conform to Security Level 1 or higher as specified in [FIPS 140-2].[5]

[4] For more information about how to generate a public/private key pair using the RSA algorithm, please see http://en.wikibooks.org/wiki/Transwiki:Generate_a_keypair_using_OpenSSL. For more information about the mathematics of the RSA algorithm, please see http://en.wikipedia.org/wiki/RSA.

[5] FIPS PUB 140-2 states that: "Security Level 1 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system." Note that security levels defined in [FIPS 140-2] are unrelated to levels of assurance for electronic identities as defined in NIST PUB 800-63.

6.1.3 Private Key Backup

Copies of private keys governed by this CP are strongly discouraged, but MAY be made to provide a backup in the event of destruction or failure of the original. If undertaking a private key backup procedure, a subscriber MUST do so in a fashion that ensures proper accountability for all actions performed.

6.1.4 Private Key Archival

Private keys governed by this CP SHALL NOT be archived.

6.1.5 Private Key Transfer Into or From a Cryptographic Module

Private keys governed by this CP SHALL be generated by and remain in a cryptographic module. Private keys MAY be backed up in accordance with the rules stipulated in Section 6.1.3.

In the event a private key, generated by and in a cryptographic module, MUST be transported into another cryptographic module, the second or recipient module MUST have equal or greater security controls, the private key MUST be encrypted during transport, and private key material MUST NOT exist in plaintext outside the boundaries of the source or destination cryptographic modules.

6.1.6 Private Key Storage on Cryptographic Module

No stipulation beyond what is specified in [FIPS 140-2].

6.1.7 Method of Activating Private Key

Private keys corresponding to certificates in the NIEF Trust Fabric are used for digital signature and encryption operations on information-sharing transactions between NIEF Center members. According to previously articulated rules in this CP, these private keys MUST reside on secure servers, within cryptographic modules, at all times, except for certain exceptional conditions such as private key backup and transfer from one cryptographic module to another. Due to the location of these keys, it is generally infeasible for them to be activated (for example, via a passphrase) on a per-crypto-operation basis, or even on a short-term cache basis for use in crypto operations. It is therefore assumed that these keys require no method of activation, other than knowledge of the private key material.

The private key used by the NIEF Center to sign the NIEF Trust Fabric MUST be maintained on an offline machine in a location that is locked at all times and requires 2-factor access control (e.g. key card + PIN) for physical access. This private key SHALL require a pass-phrase or PIN for activation, and the pass-phrase or PIN SHALL be protected from disclosure to unauthorized personnel.

6.1.7.1 Method of Deactivating Private Key

Per the preceding section, private keys corresponding to certificates in the NIEF Trust Fabric do not require activation, so this section is not applicable to those keys.

For the private key used by the NIEF Center to sign the NIEF Trust Fabric, the cryptographic module SHALL be deactivated after use, e.g. via a manual logout procedure, or automatically after a period of inactivity.

6.1.7.2 Method of Destroying Private Key

Private signature keys SHALL be destroyed in accordance with [FIPS 140-2] when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

6.1.8 Other Aspects of Key Pair Management

All certificates governed by this CP SHALL be subject to revocation and/or re-key in the event of a personnel change in which a person previously authorized to perform trusted role operations on the corresponding private key is no longer authorized to do so.

6.1.8.1 Public Key Archival

Public keys that appear in the NIEF Trust Fabric are archived as part of their publication in the NIEF Trust Fabric. Public keys corresponding to the private keys used by the NIEF Center to sign the NIEF Trust Fabric are also archived by virtue of being included in the NIEF Trust Fabric.

6.1.8.2 Certificate Operational Periods and Key Pair Usage Periods

Certificates that are governed by this CP and also appear in the NIEF Trust Fabric SHALL be limited to a maximum lifetime of two (2) years. Certificates corresponding to private keys used by the NIEF Center to sign the NIEF Trust Fabric SHALL be limited to a maximum lifetime of five (5) years.

Refer to [NIEF CTFMP] for more information about the certificate re-key process.

6.1.9 Activation Data

For certificates that are governed by this CP and also appear in the NIEF Trust Fabric, this section and its subsections do not apply. (See Section 6.1.7 for more details.)

For certificates corresponding to private keys used by the NIEF Center to sign the NIEF Trust Fabric, the following subsections apply.

6.1.9.1 Activation Data Generation and Installation

For certificates corresponding to private keys used by the NIEF Center to sign the NIEF Trust Fabric, the activation data used to unlock the private keys SHALL have an appropriate level of strength. If the activation data must be transmitted, it SHALL be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module. If the NIEF Center uses passwords as activation data for the private key, the activation data SHALL be changed upon re-key, if not more frequently.

6.1.9.2 Activation Data Protection

For certificates corresponding to private keys used by the NIEF Center to sign the NIEF Trust Fabric, the data used to unlock the keys SHALL be protected from disclosure. If the activation data is recorded, it SHALL be secured at the level of assurance associated with the activation of the cryptographic module, and SHALL NOT be stored with the cryptographic module.

6.1.10 Computer Security Controls

As part of the NIEF application and onboarding processes (see [NIEF OPP]), subscribers fully disclose their local security policies and practices, including those related to computer security controls.

The following computer security functions SHALL be provided by the operating system, or through a combination of operating system, software, and physical safeguards for all computer systems on which one or more private keys governed by this CP reside.

1. Require authenticated logins.
2. Provide discretionary access control.
3. Provide non-discretionary access controls for policy-enforced operations.
4. Provide a security audit capability.
5. Enforce separation of duties for locally defined trusted identities and/or roles. (See Section 6.2.2.1.)
6. Require identification and authentication of trusted identities and trusted roles if applicable.
7. Require use of cryptography for session communication, if and when appropriate. Refer to [NIEF Trust], Section 5.4.3.
8. Require a trusted path for identification of trusted identities and/or roles.
9. Enforce process isolation.

Subscriber equipment SHALL be configured and operated to activate these controls.

6.1.11 Life Cycle Technical Controls

The following life cycle technical controls pertain to all subscriber systems on which private keys governed by this CP reside.

1. The hardware and software SHALL be procured in a fashion that reduces the likelihood of tampering for any particular component.
2. The hardware and software SHALL be limited to performing NIEF-related functions. This MAY include providing specific service endpoints at which the keys and certificates governed by this CP are used.
3. Proper care (e.g. anti-virus, intrusion detection software) SHALL be taken to prevent malicious software from being loaded onto the equipment.
4. Hardware and software updates SHALL be obtained and installed by trusted and trained personnel in a defined manner.
5. Chain of custody mechanisms SHALL be provided throughout the lifecycle of the system, to include (a) shipment and delivery of hardware and software from the purchase location to the subscriber's physical location, (b) creation, storage, transport, or manipulation of subscriber key material, and (c) physical or logical access to subscriber systems.
6. Controls pertaining to configuration, modifications, and upgrades SHALL be provided. In addition, there SHALL be a mechanism on these systems for detecting unauthorized modification to the local software or configuration.

6.1.12 Network Security Controls

Subscribers SHALL employ appropriate security measures to ensure systems housing private key material subject to this CP are guarded against subversion and intrusion attacks. Such measures MAY include, but are not limited to, firewalls, intrusion detection devices, and filtering routers. Unused network ports and services SHALL be turned off, and any network software and user accounts present SHALL be restricted to the functioning of the subscriber systems.

In addition, as part of the NIEF application and onboarding processes (see [NIEF OPP]), subscribers fully disclose their local security policies and practices, including those related to network security controls.

6.2 Facility, Management, and Operational Controls

This section and its subsections address issues relating to the physical facility in which sensitive key material is housed by subscribers, as well as subscribers' operational controls relating to personnel.

6.2.1 Physical Controls

As part of the NIEF application and onboarding processes (see [NIEF OPP]), subscribers fully disclose their local security policies and practices, including those related to physical controls.

Subscriber servers, workstations, and other sensitive components MUST be located in an environment that prevents unauthorized access to equipment and records. Subscribers MUST use

facilities that are protected with intrusion alarms or actively monitored for protection against intrusion, regardless of assurance level.

6.2.1.1 Site Location and Construction

The location and construction of the facility housing subscriber equipment and operations SHALL be locked at all times and require restricted access. The subscriber approves the authorized list of personnel into this facility.

6.2.1.2 Physical Access

Subscriber equipment housing or storing private key material subject to this CP SHALL always be protected from unauthorized access and subversion as stipulated in Sections 6.1.10 and 6.2.1.1. Additionally, these security mechanisms SHALL be commensurate with the level of threat in the equipment environment.

6.2.1.3 Re-use and Repurposing of Physical Equipment

Subscriber equipment housing private key material that is subject to this CP SHALL be properly sanitized prior to re-use or repurposing.

6.2.1.4 Waste Disposal

Sensitive equipment that is no longer in operation and considered to be waste SHALL be destroyed in a particular manner rendering the equipment impossible to reuse. In cases where data is involved (hard drives, tokens etc.), the data SHALL be destroyed in a manner that prevents data recovery.

6.2.2 Procedural Controls

As part of the NIEF application and onboarding processes (see [NIEF OPP]), subscribers fully disclose their local security policies and practices, including those related to procedural controls.

The following sections address procedural controls that MUST be in place with respect to sensitive private key material corresponding to certificates covered by this CP and the systems on which the private key material is used.

6.2.2.1 Trusted Persons and Trusted Roles

A trusted person is one who performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. Trusted persons and persons selected to fill trusted roles MUST be responsible for their designated actions or the integrity of the NIEF Trust Fabric is weakened. Functions performed by trusted persons or persons in trusted roles form the basis of trust for all uses of the NIEF Trust Fabric. The NIEF Center shall maintain a list of appropriate trusted persons, per the local procedural controls that it implements.

Subscribers to this CP SHALL maintain a list of appropriate trusted persons and (if applicable) trusted roles, per the local procedural controls that they implement.

6.2.2.2 Number of Persons Required Per Task

To ensure the integrity of subscriber operations, it is RECOMMENDED that wherever possible and as applicable per local procedural controls, a separate individual be identified for each trusted role. Additionally, redundancy of personnel SHOULD also be observed in support of subscriber operations in the event of personnel absence.

6.2.2.3 Identification and Authentication of Trusted Persons

An individual SHALL be REQUIRED to identify and authenticate himself/herself as a trusted person before being permitted to perform any actions set forth by the subscriber for that role or identity.

6.2.3 Personnel Controls

As part of the NIEF application and onboarding processes (see [NIEF OPP]), subscribers fully disclose their local security policies and practices, including those related to personnel controls.

The following sections address personnel controls that MUST be in place with respect to sensitive private key material corresponding to certificates covered by this CP and the systems on which the private key material is used.

6.2.3.1 Qualifications, Experience, and Clearance Requirements

Each subscriber SHALL positively identify and maintain an up-to-date list of the individuals that are responsible and accountable for the management of the subscriber's operational environment. In addition, persons selected to perform sensitive operations or fill trusted roles SHALL be chosen on the basis of loyalty, trustworthiness, and integrity.

6.2.3.2 Background Check Procedures

Each subscriber SHALL implement a background check procedure to demonstrate that requirements set forth in Section 6.2.3.1 are met. Such procedures SHALL be performed solely to determine the suitability of a person to fill a trusted role as defined by a subscriber.

6.2.3.3 Training Requirements

Each subscriber SHALL implement a policy whereby all persons trusted with respect to the operation of any equipment containing certificates or private keys governed by this CP SHALL receive comprehensive training. Training SHALL be conducted in the following areas.

1. All certificate management duties they are expected to perform
2. Operation of certificate management software and hardware in use on the system

3. Incident response and business continuity procedures

6.2.3.4 Retraining frequency and requirements

Each subscriber SHALL implement a policy whereby all trusted persons SHALL be aware of changes in the subscriber's operation that may occur as a result of changes in the subscriber's local security policy or changes to this CP.

6.2.3.5 Sanctions for Unauthorized Actions

Each subscriber SHALL take appropriate administrative and disciplinary actions against personnel who have performed actions that are not authorized in this CP and could result in security vulnerabilities for the subscriber or other NIEF Center members. This MAY include revocation of digital credentials.

6.2.3.6 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to each subscriber's operational environment SHALL meet applicable requirements set forth in this CP.

6.2.3.7 Documentation Supplied To Personnel

Each subscriber SHALL make available to appropriate personnel the certificate policies it supports, as well as any relevant statutes, policies, or contracts that apply to the person's duties.

6.2.4 Audit Logging Procedures

All subscribers to this CP SHALL generate audit log files for all events relating to the security of the subscriber's systems. Where possible, the security audit logs SHALL be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism SHALL be used. All security audit logs, both electronic and non-electronic, SHALL be retained and made available during compliance audits.

In addition, as part of the NIEF application and onboarding processes (see [NIEF OPP]), subscribers fully disclose their local audit logging policies and procedures.

6.2.5 Incident Response

As part of the NIEF application and onboarding processes (see [NIEF OPP]), subscribers fully disclose their local security policies and practices, including those related to incident response and data compromise.

As part of its incident and compromise handling procedures, each subscriber SHALL implement a procedure whereby it contacts the NIEF Center promptly upon discovery of any incident in which private key material governed by this CP was, or might have been, compromised. See also [NIEF CTFMP].

7 Compliance Audit and Other Assessments

The NIEF Center and NIEF members MUST comply with the audit and assessment requirements defined in the NIEF Audit Policy [NIEF Audit].

8 Other Business and Legal Matters

This section and its subsections pertain to the topic of business and legal matters that may affect this CP. Generally, these topics are beyond the scope of this CP and addressed in [NIEF Bylaws].

8.1 Amendments

Amendments to this CP are covered under Section 6 of [NIEF OPP], "Change Management for Normative Standards". In addition, amendments to this CP require approval by the NIEF Center Director and NIEF Executive Committee.

8.2 Dispute Resolution Provisions

All disputes SHALL be resolved as per the rules stipulated in [NIEF Bylaws] and [NIEF OPP].