National Identity Exchange Federation

Trustmark Signing Certificate Policy

Version 1.0

Published October 3, 2014
Revised March 30, 2016

Table of Contents

1 Introduction and Purpose of This Document

This ***National Identity Exchange Federation (NIEF) Trustmark Signing Certificate Policy*** governs the digital certificates used to digitally sign all trustmarks that are issued by the National Identity Exchange Federation Center ("NIEF Center"). Its purpose is to explicitly specify and document the lifecycle management process for the X.509 certificates and corresponding private keys used by the NIEF Center to sign all trustmarks that it issues. This document is a companion to the ***National Identity Exchange Federation Trustmark Policy ("NIEF Trustmark Policy")***, which governs the overall lifecycle management process for all trustmarks issued and signed by the NIEF Center.

Background and Basic Concepts

A **trustmark** is a machine-readable, cryptographically signed artifact, issued by a **Trustmark Provider** (TP) to a **Trustmark Recipient** (TR), for the benefit of one or more **Trustmark Relying Parties** (TRPs). A Trustmark represents an official attestation by the TP of conformance by the TR to a well-defined set of requirements pertaining to trust and/or interoperability for the purpose of interaction with and use of digital information resources and services. A TRP may rely upon a trustmark as the basis for third-party trust in the TR with respect to the set of requirements represented by the trustmark. A **Trustmark Definition** (TD) expresses the specific set of requirements represented by a Trustmark.

In its role as a TP, the National Identity Exchange Federation (NIEF) Center issues, cryptographically signs, and publishes various trustmarks for agencies (TRs) that wish to obtain and use those trustmarks as a mechanism for establishing trust with other entities (TRPs), including partner agencies and individuals. The NIEF Center, along with the TRs for and about which the NIEF Center issues trustmarks, and the TRPs that rely on those trustmarks, do not rely upon a traditional Public Key Infrastructure (PKI) security model for the cryptographic integrity of trustmarks; however, all of these parties rely on the cryptographic integrity of the trustmarks issued by the NIEF Center, 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 trustmarks that it issues. For these reasons, the NIEF Center has adopted this NIEF Trustmark Signing Certificate Policy.

Due to the specific details of the trustmark 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 trustmark security model, and explains the differences between a traditional PKI security model and the NIEF trustmark security model where necessary.

Definitions and Perspective of This Document

The following paragraphs delineate the fundamental differences between the NIEF trustmark security 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 RPs. This NIEF CP uses the concepts of CA, subscriber, and RP, but defines them differently, as follows.

1. The only subscriber to this CP is the NIEF Center.

2. 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 trustmarks and thereby ensure their integrity.

3. Each TR and TRP 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 certificate that is generated and managed by the NIEF Center, and which is used to cryptographically sign trustmarks issued by the NIEF Center.

Note that in this CP, the NIEF Center has multiple roles (CA and subscriber), and therefore many of the sections of this document must be read from multiple perspectives to fully understand the NIEF Center's responsibilities. Note also that this CP pertains only to the certificate that is used by NIEF to sign trustmarks that it issues.

This CP does not pertain to, and has no direct relation to, certificates that appear in the NIEF Cryptographic Trust Fabric or are used by NIEF to sign the NIEF Cryptographic Trust Fabric. Similarly, 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 is the only subscriber to this CP and this CP's security model does not require registration of subscribers with a CA in the traditional sense.

1.1   Certificate Policy Concept and Applicability

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, in its role as a TP, along with the TRs for and about which the NIEF Center issues trustmarks, and the TRPs that rely on those trustmarks. A trustmark is a cryptographically signed digital artifact that represents an official attestation by a TP of conformance by a TR to a well-defined set of requirements pertaining to trust and/or interoperability for the purpose of interaction with and use of digital information resources and services. The purpose of this CP is to set forth a list of rules that the NIEF Center must obey to help ensure that trustmarks issued by the NIEF Center maintain their legitimacy and trustworthiness at all times.

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**
TFTS	Trustmark Framework Technical Specification, version 1.0 https://trustmark.gtri.gatech.edu/specifications/trustmark-framework/1.0/tfts-1.0.pdf
FIPS 140-2	Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules,* 3 December 2002. http://csrc.nist.gov/groups/STM/cmvp/standards.html
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 https://www.ietf.org/rfc/rfc3647.txt

Table 1: References for Related Documents

1.3   Document Name and Identification

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

1.4   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.

1.4.1   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
> Information and Communications Laboratory
> 75 5th Street, NW
> Suite 900
> Atlanta, GA 30308

1.4.2   Contact Person

The contact person for the NIEF Center is:

> John Wandelt, National Identity Exchange Federation Center Director
> Georgia Tech Research Institute
> Information and Communications Laboratory
> 75 5th Street, NW
> Suite 900
> Atlanta, GA 30308
> Phone: 404-407-8956
> Email: John.Wandelt@gtri.gatech.edu

1.4.3   Entity Determining CP Suitability

The NIEF Center determines the suitability of this CP.

1.4.4   CP Approval Procedures

This CP requires approval by the NIEF Center Director.

1.5   PKI Participants

This CP does not pertain directly to the operation of a PKI; however, this CP does impact the NIEF Center, along with the TRs for and about which the NIEF Center issues trustmarks, and the TRPs that rely on those trustmarks, as called out in the following subsections.

1.5.1   Certification Authorities

The NIEF Center acts as a CA for the X.509 certificate that it generates and manages, and which is used to cryptographically sign all trustmarks that the NIEF Center issues. But the NIEF Center does not generate certificates for any TRs or TRPs.

1.5.2   Subscribers

The NIEF Center is the sole subscriber to this CP. As noted in Section 1.5.1, the NIEF Center acts as its own CA for the certificates that it generates, manages, and uses.

1.5.3   Relying Parties

A Relying Party (RP) 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. RPs to this CP include all TRs for and about which the NIEF Center issues trustmarks, as well as all TRPs that rely on those trustmarks. Both the TRs and TRPs rely upon the certificate used by the NIEF Center to cryptographically sign the trustmarks it issues.

1.6   Definitions and Acronyms

The following acronyms are used in this CP and related documents.

Acronym	Meaning
TP	Trustmark Provider
TR	Trustmark Recipient
TRP	Trustmark Relying Party
TFTS	Trustmark Framework Technical Specification
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
NIEF	National Identity Exchange Federation
PKI	Public Key Infrastructure
RA	Registration Authority
URL	Uniform Resource Locator

2   Publication of This Document and Trustmark Signing Certificates

The NIEF Center shall maintain this CP at an official, publicly accessible Publication URL. The Publication URL for this document is:

https://nief.org/policies/nief-trustmark-signing-cp-1.0.pdf

In addition, the NIEF Center shall maintain a list of its Trustmark Signing Certificates at an official, publicly accessible URL. The URL at which NIEF Trustmark Signing Certificates are published is:

https://nief.org/certificates/

3   Certificate Issuance

The NIEF Center does not operate a traditional CA, and therefore does not issue certificates in the traditional way. As previously noted, the only subscriber to this CP is the NIEF Center itself.

4   Certificate Content

This section and its subsections pertain to the content and use of certificates that are covered by this CP. All rules described in this section are oriented towards the goal of ensuring the integrity of trustmarks issued by the NIEF Center.

4.1   Naming

This section pertains to naming and name management issues that can arise for names within X.509 certificates. As the NIEF Center does not employ a traditional PKI trust model, many naming issues that pertain to a PKI are either not applicable to the NIEF Center 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 must contain the Subject Name stipulated in Section 4.1.2.

4.1.2   Need for Names to Be Meaningful

Any certificate covered by this CP must clearly identify the NIEF Center as the organization that owns the certificate. In addition, any certificate covered by this CP must clearly indicate that it is to be used only for digital signing of trustmarks issued by the NIEF Center. Accordingly, the NIEF Center has established by convention that any certificate covered by this CP must contain the following Subject information.

Organization Name = National Identity Exchange Federation
Organizational Unit = GTRI NSTIC Trustmark Pilot
Common Name = trustmark.gtri.gatech.edu

> *Email Address = TrustmarkFeedback@gtri.gatech.edu*
> *Country = US*
> *State/Province = GA*
> *Locality = Atlanta*

4.1.3   Anonymity or Pseudonymity of Subscribers

This CP does not permit anonymity or pseudonymity of subscribers. The only subscriber to this CP is the NIEF Center, and its identity is well known to all RPs.

4.1.4   Uniqueness of Names

As the NIEF Center is both the CA for this CP and the only subscriber under this CP, and the NIEF Center has established the certificate naming convention indicated in Section 4.1.2, name collisions between certificates are not possible except in the circumstance where the NIEF Center issues multiple trustmark signing certificates to itself. In this case, RPs for these certificates will be able to clearly recognize and understand each certificate's name and purpose.

4.2   Criteria for Interoperation

Any certificate that is covered by this CP must meet the following interoperation 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   NIEF Center Private Key and Certificate Usage

The NIEF Center may use certificates to which this CP applies only for the purpose of digitally signing trustmarks issued by the NIEF Center. All other uses are prohibited.

5.2   NIEF Center Public Key and Certificate Usage

RPs may use certificates to which this CP applies, as well as their corresponding public keys, only for the purpose of validating digital signatures on trustmarks issued by the NIEF Center. 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 trustmarks issued by the NIEF Center, the NIEF Center must obey the rules outlined in this section.

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 NIEF Center using the RSA key generation algorithm[1], 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.

---

[1] 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.

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).

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

See Section 5. Private key usage is limited to generating digital signatures for trustmarks issued by the NIEF Center.

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].[2]

6.1.3   Private Key Backup

Copies of private keys governed by this CP may be made to provide a backup in the event of destruction or failure of the original. If undertaking a private key backup procedure, the NIEF Center shall 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

---

[2] 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.

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

The private key used by the NIEF Center to sign the trustmarks that it issues 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

The cryptographic module containing the private key used by the NIEF Center to sign the NIEF Trust Fabric 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 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 operations on the corresponding private key is no longer authorized to do so.

6.1.8.1   Public Key Archival

Public keys corresponding to the private keys used by the NIEF Center to sign trustmarks issued by the NIEF Center are archived by the NIEF Center by virtue of being included in each trustmark signed with the corresponding private key.

6.1.8.2   Certificate Operational Periods and Key Pair Usage Periods

Certificates corresponding to private keys used by the NIEF Center to sign trustmarks issued by the NIEF Center shall be limited to a maximum lifetime of five (5) years.

6.1.9   Activation Data

For certificates corresponding to private keys used by the NIEF Center to sign trustmarks issued by the NIEF Center, 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 trustmarks issued by the NIEF Center, 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 trustmarks issued by the NIEF Center, 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

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. Enforce process isolation.

NIEF Center equipment containing one or more private keys governed by this CP shall be configured and operated to activate these controls.

Note also, as indicated in Section 6.1.7, that the private key used by the NIEF Center to sign the trustmarks that it issues is 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.

6.1.11 Life Cycle Technical Controls

The following life cycle technical controls pertain to all NIEF Center 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.

3. Proper care 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 NIEF Center's physical location, (b) creation, storage, transport, or manipulation of NIEF Center key material, and (c) physical or logical access to NIEF Center systems.

6. Controls pertaining to configuration, modifications, and upgrades shall be provided.

6.1.12 Network Security Controls

The NIEF Center 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.

Note, as indicated in Section 6.1.7, that the private key used by the NIEF Center to sign the trustmarks that it issues is maintained on an offline machine, thereby satisfying the stipulation in this section regarding 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 the NIEF Center, as well as the NIEF Center's operational controls relating to personnel.

6.2.1 Physical Controls

The NIEF Center's servers, workstations, and other sensitive components must be located in an environment that prevents unauthorized access to equipment and records. The NIEF Center must use facilities that are actively monitored for protection against intrusion.

6.2.1.1 Site Location and Construction

The location and construction of the NIEF Center facility housing its trustmark signing equipment and operations shall be locked at all times and require restricted access.

6.2.1.2 Physical Access

NIEF Center equipment associated with the signing of trustmarks shall always be protected from unauthorized access and subversion as stipulated in Sections 6.1.10 and 6.2.1.1.

6.2.1.3 Re-use and Repurposing of Physical Equipment

NIEF Center 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

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

A trusted person is one who performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. These persons must be responsible for their designated actions or the integrity of all trustmarks issued by the NIEF Center is weakened. Functions performed by these persons form the basis of trust for all uses of trustmarks issued by the NIEF Center. The NIEF Center shall maintain a list of appropriate trusted persons, per the local procedural controls that it implements.

6.2.2.2   Personnel Redundancy

The NIEF Center shall arrange for a suitable level of redundancy among its personnel to address operational issues that may arise due to 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 NIEF Center.

6.2.3   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

The NIEF Center shall positively identify and maintain an up-to-date list of the individuals that are responsible and accountable for the management of the NIEF Center's operational environment. In addition, persons trusted to perform sensitive operations shall be chosen on the basis of loyalty, trustworthiness, and integrity.

6.2.3.2   Background Check Procedures

As a unit of the Georgia Tech Research Institute (GTRI), the NIEF Center shall rely on GTRI's standard background check procedure to demonstrate that requirements set forth in Section 6.2.3.1 are met.

6.2.3.3   Training Requirements

The NIEF Center 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

The NIEF Center shall implement a policy whereby all trusted persons shall be aware of changes in the NIEF Center's operations that may occur as a result of changes to this CP.

6.2.3.5   Sanctions for Unauthorized Actions

The NIEF Center 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 NIEF Center. This may include revocation of digital credentials.

6.2.3.6   Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the NIEF Center's operational environment shall meet applicable requirements set forth in this CP.

6.2.3.7   Documentation Supplied To Personnel

The NIEF Center 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

The NIEF Center shall generate audit log files for all events relating to the security of NIEF Center systems that are governed by this CP. Where possible, the security audit logs shall be automatically collected. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

6.2.5   Incident Response

As part of its incident and compromise handling procedures, the NIEF Center shall implement a procedure whereby it publishes a public notice promptly upon discovery of any incident in which private key material governed by this CP was compromised, or might have been compromised.

In addition, if the NIEF Center discovers an incident in which private key material governed by this CP was compromised, or might have been compromised, it shall immediately revoke all trustmarks that were signed by that private key.