National Identity Exchange Federation

Trustmark Signing Certificate Policy

Version 1.3

August 24, 2021

Table of Contents

1 Introduction and Purpose of This Document

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

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 trustmark provider of conformance by the trustmark recipient 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 trustmark relying party may rely upon a trustmark as the basis for third-party trust in the trustmark recipient 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.

A trustmark provider issues, cryptographically signs, and publishes various trustmarks for agencies (trustmark recipients) that wish to obtain and use those trustmarks as a mechanism for establishing trust with other entities (trustmark relying parties), including partner agencies and individuals. All of these parties rely on the cryptographic integrity of the trustmarks issued by the trustmark provider, which requires implicit reliance on the lifecycle management process for the X.509 certificate and corresponding private key used by the trustmark provider to sign the trustmarks that it issues. For these reasons, NIEF has adopted this *Trustmark Signing Certificate Policy*.

This certificate policy (CP) does not address all the standard CP topics in the same manner that a traditional Public Key Infrastructure (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 trustmark security model, and explains the differences between a traditional PKI security model and the trustmark security model where necessary.

Definitions and Perspective of This Document

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

1. The sole subscriber to this CP is NIEF.

2. NIEF acts as a CA in this CP for the X.509 certificates that it generates and manages, and which is used to cryptographically sign trustmarks and thereby ensure their integrity.

3. Each trustmark recipient and trustmark relying party 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 NIEF, and which is used to cryptographically sign trustmarks issued by NIEF.

Note that in this CP, the trustmark provider (NIEF) 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 trustmark provider's responsibilities. Note also that this CP pertains only to those certificates that are used by the trustmark provider to sign trustmarks that it issues. *This CP does not pertain to, and has no direct relation to, certificates that are used for purposes other than for digitally signing trustmarks.*

Finally, note that the traditional PKI concept of a registration authority (RA) has no meaning in this CP, since 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 trustmark provider, along with the trustmark recipients for and about which the trustmark provider issues trustmarks, and the trustmark relying parties that rely on those trustmarks. A trustmark is a cryptographically signed digital artifact that represents an official attestation by a trustmark provider of conformance by a trustmark recipient 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 trustmark provider must obey to help ensure that trustmarks issued by the trustmark provider 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.

Document ID	Document Name and URL if Applicable
TFTS	Trustmark Framework Technical Specification https://trustmarkinitiative.org/specifications/trustmark-framework/
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 maintaining and updating this document. It also includes the name, email address, and telephone number of a contact person.

1.4.1 Organization Administering the Document

NIEF is the administering organization for this policy. Its 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

For executive-level matters, NIEF's Executive Director is:

Mr. John Wandelt
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

For technical matters related to this policy, NIEF's contact person is:

Mr. Matthew Moyer
Georgia Tech Research Institute
Information and Communications Laboratory
75 5th Street, NW
Suite 900
Atlanta, GA 30308
Phone: 404-407-6679
Email: Matthew.Moyer@gtri.gatech.edu

1.5 Publication of This Document

NIEF maintains this policy at an official, publicly accessible publication location. The publication location of this document is:

https://trustmark.nief.org/tat/public/documents/pdf/nief-trustmark-signing-cp-1.3.pdf

1.6 PKI Participants

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

1.6.1 Certification Authorities

NIEF acts as a CA for the X.509 certificates that it generates and manages, and which are used to cryptographically sign all trustmarks that it issues. But NIEF does not generate certificates for any trustmark recipients or trustmark relying parties.

1.6.2 Subscribers

The sole subscriber to this CP is NIEF, acting in the role of a trustmark provider. As noted in Section 1.6.1, NIEF acts as its own CA for the certificates that it generates, manages, and uses.

1.6.3 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 trustmark recipients for and about which the trustmark provider (NIEF) issues trustmarks, as well as all trustmark relying parties that rely on those trustmarks. Both the trustmark recipients and trustmark relying parties rely upon the certificate used by the trustmark provider to cryptographically sign the trustmarks it issues.

2 Certificate Issuance

For the purpose of this policy, and in its role as a trustmark provider, NIEF does not operate a traditional CA, and therefore does not issue certificates in the traditional way. As previously noted, the sole subscriber to this CP is NIEF.

3 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 trustmark provider (NIEF).

3.1 Naming

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

Any certificate covered by this CP must clearly identify the trustmark provider (NIEF) 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 trustmark provider. Accordingly, any certificate covered by this CP shall contain the following Subject information.

Organization Name = NIEF
Organizational Unit = TAT
Common Name = trustmark.nief.org
Email Address = help@nief.org
Country = US
State/Province = GA
Locality = Atlanta

3.2 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 3.1 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.

4 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.

4.1 Trustmark Provider Private Key and Certificate Usage

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

4.2 Trustmark Provider 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 trustmark provider (NIEF). All other uses are prohibited.

5 Protection of Certificate Private Key

5.1 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 trustmark provider, the trustmark provider shall obey the rules outlined in this section.

5.1.1 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.

5.1.1.1 Key Pair Generation

The key pair must be generated by the trustmark provider 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.

5.1.1.2 Key Sizes

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

5.1.1.3 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.

5.1.1.4 Private Key Usage Purposes (As Per X.509 Key Usage Field)

See Section 4. Private key usage is limited to generating digital signatures for trustmarks issued by the trustmark provider.

5.1.2 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]

5.1.3 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 trustmark provider shall do so in a fashion that ensures proper accountability for all actions performed.

[1] For more information about the RSA algorithm, please see http://en.wikipedia.org/wiki/RSA.
[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.

5.1.4 Private Key Archival

Private keys governed by this CP shall not be archived.

5.1.5 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 5.1.3. 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.

5.1.6 Private Key Storage on Cryptographic Module

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

5.1.7 Method of Activating Private Key

The private key shall remain encrypted when not in use, and shall require a pass-phrase or PIN for activation, and the pass-phrase or PIN shall be protected from disclosure to unauthorized personnel.

5.1.7.1 Method of Deactivating Private Key

The cryptographic module containing the private key used by the trustmark provider to sign the trustmarks that it issues shall be deactivated after use, e.g. via a manual logout procedure, or automatically after a period of inactivity.

5.1.7.2 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.

5.1.8 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.

5.1.8.1 Public Key Archival

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

5.1.8.2 Certificate Operational Periods and Key Pair Usage Periods

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

5.1.9 Activation Data

For certificates corresponding to private keys used by the trustmark provider to sign trustmarks issued by the trustmark provider, the following subsections apply.

5.1.9.1 Activation Data Generation and Installation

For certificates corresponding to private keys used by the trustmark provider to sign trustmarks issued by the trustmark provider, 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 trustmark provider uses passwords as activation data for the private key, the activation data shall be changed upon re-key, if not more frequently.

5.1.9.2 Activation Data Protection

For certificates corresponding to private keys used by the trustmark provider to sign trustmarks issued by the trustmark provider, 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.

5.1.10 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.

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

5.1.11 Life Cycle Technical Controls

The following life cycle technical controls pertain to all trustmark provider 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 trustmark-related functions by the trustmark provider.

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 trustmark provider's physical location, (b) creation, storage, transport, or manipulation of trustmark provider key material, and (c) physical or logical access to trustmark provider systems.

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

5.1.12 Network Security Controls

The trustmark provider 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.

5.2 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 trustmark provider, as well as the trustmark provider's operational controls relating to personnel.

5.2.1 Physical Controls

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

5.2.1.1 Site Location and Construction

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

5.2.1.2 Physical Access

Trustmark provider equipment associated with the signing of trustmarks shall always be protected from unauthorized access and subversion as stipulated in Sections 5.1.10 and 5.2.1.1.

5.2.1.3 Re-use and Repurposing of Physical Equipment

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

5.2.1.4 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.

5.2.2 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.

5.2.2.1 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 trustmark provider is weakened. Functions performed by these persons form the basis of trust for all uses of trustmarks issued by the trustmark provider. The trustmark provider shall maintain a list of appropriate trusted persons, per the local procedural controls that it implements.

5.2.2.2 Personnel Redundancy

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

5.2.2.3 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 trustmark provider.

5.2.3 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.

5.2.3.1 Qualifications, Experience, and Clearance Requirements

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

5.2.3.2 Background Check Procedures

The trustmark provider shall conduct appropriate background check procedures for all individuals that play a role in the trustmark provider's operational environment, to ensure that requirements set forth in Section 5.2.3.1 are met.

5.2.3.3 Training Requirements

The trustmark provider 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

5.2.3.4 Retraining frequency and requirements

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

5.2.3.5 Sanctions for Unauthorized Actions

The trustmark provider 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 trustmark provider. This may include revocation of digital credentials.

5.2.3.6 Independent Contractor Requirements

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

5.2.3.7 Documentation Supplied to Personnel

The trustmark provider 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.

5.2.4 Audit Logging Procedures

The trustmark provider shall generate audit log files for all events relating to the security of trustmark provider 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.

5.2.5 Incident Response

As part of its incident and compromise handling procedures, the trustmark provider 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 trustmark provider 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.