# Signature RTD Certificate Policy

Policy Document

Version 1.0

2014-10-03

[SIGNATURE_CP]

NFC Forum™

## RESTRICTIONS ON USE



NFC Forum, Inc.
401 Edgewater Place, Suite 600
Wakefield, MA, USA 01880

# Contents

**1 Introduction....1**
1.1 Overview and Objectives .... 1
1.2 Scope .... 1
1.2.1 Appropriate Certificate Uses .... 1
1.2.2 Prohibited Certificate Uses .... 1
1.3 Audience .... 1
1.3.1 Public Key Infrastructure (PKI) Authorities .... 1
1.3.2 Registration Authorities .... 2
1.3.3 Subscribers .... 2
1.3.4 Relying Parties .... 2
1.3.5 Other Participants .... 2
1.4 Applicable Documents or References .... 2
1.5 Administration .... 3
1.6 Name and Logo Usage .... 4
1.7 Intellectual Property .... 4
1.8 Special Word Usage .... 4
1.9 Abbreviations .... 4
1.10 Glossary .... 5

**2 Publication and Repository Responsibilities .... 8**
2.1 Repositories .... 8
2.2 Publication of Certification Information .... 8
2.3 Time or Frequency of Publication .... 8
2.4 Access Controls on Repositories .... 8

**3 Identification and Authentication .... 9**
3.1 Naming .... 9
3.1.1 Types of Names .... 9
3.1.2 Use Meaningful Names .... 9
3.1.3 Anonymity or Pseudonymity of Subscribers .... 9
3.1.4 Rules for Interpreting Various Name Forms .... 9
3.1.5 Uniqueness of Names .... 9
3.1.6 Recognition, Authentication, and Role of Trademarks .... 9
3.2 Initial Identity Validation .... 9
3.2.1 Method to Prove Possession of Private Key .... 10
3.2.2 Authentication of Organization Identity .... 10
3.2.3 Authentication of Individual Identity .... 11
3.2.4 Validation of Authority .... 13
3.2.5 Verification of Other Information Sources .... 14
3.3 Identification and Authentication for Re-key Requests .... 15
3.3.1 Identification and Authentication for Routine Re-key .... 15
3.3.2 Identification and Authentication for Re-key After Revocation .... 15
3.4 Identification and authentication for revocation request .... 15

**4 Certification Life-cycle Operational Requirements .... 16**
4.1 Certificate Application .... 16
4.1.1 Who Can Submit a Certificate Application .... 16
4.1.2 Enrollment Process and Responsibilities .... 16
4.2 Certificate Application Processing .... 16
4.2.1 Performing Identification and Authentication Functions .... 16

4.2.2 Approval or Rejection of Certificate Applications ..... 16
4.2.3 Time to Process Certificate Applications ..... 17
4.3 Certificate Issuance ..... 17
4.3.1 CA Actions during Certificate Issuance ..... 17
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate ..... 17
4.4 Certificate Acceptance ..... 17
4.4.1 Conduct Constituting Certificate Acceptance ..... 17
4.4.2 Publication of the Certificate by the CA ..... 17
4.4.3 Notification of Certificate Issuance by the CA to Other Entities ..... 17
4.5 Key Pair and Certificate Usage ..... 18
4.5.1 Subscriber Private Key and Certificate Usage ..... 18
4.5.2 Relying Party Public Key and Certificate Usage ..... 18
4.6 Certificate Renewal ..... 18
4.6.1 Circumstance for Certificate Renewal ..... 18
4.6.2 Who May Request Renewal ..... 18
4.6.3 Processing Certificate Renewal Requests ..... 18
4.6.4 Notification of New Certificate Issuance to Subscriber ..... 18
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate ..... 18
4.6.6 Publication of the Renewal Certificate by the CA ..... 19
4.6.7 Notification of Certificate Issuance by the CA to Other Entities ..... 19
4.7 Certificate Re-key ..... 19
4.7.1 Circumstance for Certificate Re-key ..... 19
4.7.2 Who May Request Certificate Re-key ..... 19
4.7.3 Processing Certificate Re-key Requests ..... 19
4.7.4 Notification of Certificate Re-key to Subscriber ..... 19
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate ..... 19
4.7.6 Publication of the Re-keyed Certificate by the CA ..... 19
4.7.7 Notification of Certificate Issuance by the CA to Other Entities ..... 19
4.8 Certificate Modification ..... 20
4.8.1 Circumstance for Certificate Modification ..... 20
4.8.2 Who May Request Certificate Modification ..... 20
4.8.3 Processing Certificate Modification Requests ..... 20
4.8.4 Notification of Certificate Modification to Subscriber ..... 20
4.8.5 Conduct Constituting Acceptance of a Modified Certificate ..... 20
4.8.6 Publication of the Modified Certificate by the CA ..... 20
4.8.7 Notification of Certificate Modification by the CA to Other Entities ..... 20
4.9 Certificate Revocation and Suspension ..... 20
4.9.1 Circumstances for Revocation ..... 20
4.9.2 Who Can Request Revocation ..... 21
4.9.3 Procedure for Revocation Request ..... 21
4.9.4 Revocation Request Grace Period ..... 22
4.9.5 Time within which CA Must Process the Revocation Request ..... 22
4.9.6 Revocation Checking Requirement for Relying Parties ..... 22
4.9.7 CRL Issuance Frequency ..... 22
4.9.8 Maximum Latency for CRLs ..... 22
4.9.9 On-line Revocation/Status Checking Availability ..... 22
4.9.10 On-line Revocation Checking Requirements ..... 22
4.9.11 Other Forms of Revocation Advertisements Available ..... 22
4.9.12 Special Requirements Related to Key Compromise ..... 23
4.9.13 Circumstances for Suspension ..... 23
4.9.14 Who Can Request Suspension ..... 23

4.9.15 Procedure for Suspension Request ..... 23
4.9.16 Limits on Suspension Period ..... 23
4.10 Certificate Status Services ..... 23
4.10.1 Operational Characteristics ..... 23
4.10.2 Service Availability ..... 23
4.10.3 Optional Features ..... 23
4.11 End of Subscription ..... 23
4.12 Key Escrow and Recovery ..... 23
4.12.1 Key Escrow and Recovery Policy Practices ..... 23
4.12.2 Session Key Encapsulation and Recovery Policy and Practices ..... 23

**5 Facility, Management, and Operational Controls ..... 24**

5.1 Physical Controls ..... 24
5.1.1 Site Location and Construction ..... 24
5.1.2 Physical Access ..... 24
5.1.3 Power and Air Conditioning ..... 24
5.1.4 Water Exposures ..... 24
5.1.5 Fire Prevention and Protection ..... 24
5.1.6 Media Storage ..... 24
5.1.7 Waste Disposal ..... 24
5.1.8 Off-site Backup ..... 25
5.1.9 Certificate Status Hosting, CMS and External RA Systems ..... 25
5.2 Procedural Controls ..... 25
5.2.1 Trusted Roles ..... 25
5.2.2 Number of Persons Required per Task ..... 25
5.2.3 Identification and Authentication for Each Role ..... 25
5.2.4 Roles Requiring Separation of Duties ..... 25
5.3 Personnel Controls ..... 25
5.3.1 Qualifications, Experience, and Clearance Requirements ..... 25
5.3.2 Background Check Procedures ..... 26
5.3.3 Training and Skills Level ..... 26
5.3.4 Retraining Frequency and Requirements ..... 26
5.3.5 Job Rotation Frequency and Sequence ..... 26
5.3.6 Sanctions for Unauthorized Actions ..... 26
5.3.7 Independent Contractor Requirements ..... 26
5.3.8 Documentation Supplied to Personnel ..... 26
5.4 Audit Logging Procedures ..... 27
5.4.1 Types of Recorded Events ..... 27
5.4.2 Frequency of Processing Log ..... 30
5.4.3 Retention Period for Audit Log ..... 30
5.4.4 Protection of Audit Log ..... 30
5.4.5 Audit Log Backup Procedures ..... 30
5.4.6 Audit Collection System (internal vs. external) ..... 30
5.4.7 Notification to Event-causing Subject ..... 30
5.4.8 Vulnerability Assessments ..... 30
5.5 Records Archival ..... 31
5.5.1 Types of Records Archived ..... 31
5.5.2 Retention Period for Archive ..... 31
5.5.3 Protection of Archive ..... 31
5.5.4 Archive Backup Procedures ..... 31
5.5.5 Requirements for Time-stamping of Records ..... 31

5.5.6 Archive Collection System (internal or external) ..... 31
5.5.7 Procedures to Obtain and Verify Archive Information ..... 31
5.6 Key Changeover ..... 31
5.7 Compromise and Disaster Recovery ..... 31
5.7.1 Incident and Compromise Handling Procedures ..... 31
5.7.2 Computing Resources, Software, and/or Data Are Corrupted ..... 32
5.7.3 Entity Private Key Compromise Procedures ..... 32
5.7.4 Business Continuity Capabilities after a Disaster ..... 32
5.8 CA or RA Termination ..... 33

**6 Technical Security Controls ..... 34**
6.1 Key Pair Generation and Installation ..... 34
6.1.1 Key Pair Generation ..... 34
6.1.2 Private Key Delivery to Subscriber ..... 34
6.1.3 Public Key Delivery to Certificate Issuer ..... 35
6.1.4 CA Public Key Delivery to Relying Parties ..... 35
6.1.5 Key Sizes ..... 35
6.1.6 Public Key Parameters Generation and Quality Checking ..... 36
6.1.7 Key Usage Purposes ..... 36
6.2 Private Key Protection and Cryptographic Module Engineering Controls ..... 36
6.2.1 Cryptographic Module Standards and Controls ..... 36
6.2.2 Private Key (n out of m) Multi-person Control ..... 36
6.2.3 Private Key Escrow ..... 36
6.2.4 Private Key Backup ..... 36
6.2.5 Private Key Archival ..... 36
6.2.6 Private Key Transfer into or from a Cryptographic Module ..... 36
6.2.7 Private Key Storage on Cryptographic Module ..... 37
6.2.8 Method of Activating Private Key ..... 37
6.2.9 Method of Deactivating Private Key ..... 37
6.2.10 Method of Destroying Private Key ..... 37
6.2.11 Cryptographic Module Rating ..... 37
6.3 Other Aspects of Key Pair Management ..... 37
6.3.1 Public Key Archival ..... 37
6.3.2 Certificate Operational Periods and Key Pair Usage Periods ..... 37
6.4 Activation Data ..... 37
6.4.1 Activation Data Generation and Installation ..... 37
6.4.2 Activation Data Protection ..... 37
6.4.3 Other Aspects of Activation Data ..... 37
6.5 Computer Security Controls ..... 38
6.5.1 Specific Computer Security Technical Requirements ..... 38
6.5.2 Computer Security Rating ..... 38
6.6 Life Cycle Technical Controls ..... 38
6.6.1 System Development Controls ..... 38
6.6.2 Security Management Controls ..... 38
6.6.3 Life Cycle Security Controls ..... 38
6.7 Network Security Controls ..... 38
6.8 Time-stamping ..... 39

**7 Certificate, CRL, and OCSP Profiles ..... 40**
7.1 Certificate Profile ..... 40
7.1.1 Version Number(s) ..... 40
7.1.2 Certificate Extensions ..... 40

7.1.3 Algorithm Object Identifiers ..... 40
7.1.4 Name Forms ..... 40
7.1.5 Name Constraints ..... 41
7.1.6 Certificate Policy Object Identifier ..... 41
7.1.7 Usage of Policy Constraints Extension ..... 41
7.1.8 Policy Qualifiers Syntax and Semantics ..... 41
7.1.9 Processing Semantics for the Critical Certificate Policies Extension ..... 41
7.2 CRL Profile ..... 41
7.2.1 Version number(s) ..... 41
7.2.2 CRL and CRL Entry Extensions ..... 41
7.3 OCSP Profile ..... 41
7.3.1 Version Number(s) ..... 41
7.3.2 OCSP Extensions ..... 41

**8 Compliance Audit and Other Assessments ..... 42**
8.1 Frequency or Circumstances of Assessment ..... 42
8.2 Identity/Qualifications of Assessor ..... 42
8.3 Assessor's Relationship to Assessed Entity ..... 42
8.4 Topics Covered by Assessment ..... 42
8.5 Actions Taken as a Result of Deficiency ..... 43
8.6 Communication of Results ..... 43
8.7 Self-Audits ..... 43

**9 Other Business and Legal Matters ..... 44**
9.1 Fees ..... 44
9.1.1 Certificate Issuance or Renewal Fees ..... 44
9.1.2 Certificate Access Fees ..... 44
9.1.3 Revocation or Status Information Access Fees ..... 44
9.1.4 Fees for Other Services ..... 44
9.1.5 Refund Policy ..... 44
9.2 Financial Responsibility ..... 44
9.2.1 Insurance Coverage ..... 44
9.2.2 Other Assets ..... 44
9.2.3 Insurance or Warranty Coverage for End-Entities ..... 44
9.3 Confidentiality of Business Information ..... 44
9.3.1 Scope of Confidential Information ..... 44
9.3.2 Information Not Within the Scope of Confidential Information ..... 45
9.3.3 Responsibility to Protect Confidential Information ..... 45
9.4 Privacy of Personal Information ..... 45
9.4.1 Privacy Plan ..... 45
9.4.2 Information Treated as Private ..... 45
9.4.3 Information Not Deemed Private ..... 45
9.4.4 Responsibility to Protect Private Information ..... 45
9.4.5 Notice and Consent to Use Private Information ..... 45
9.4.6 Disclosure Pursuant to Judicial or Administrative Process ..... 45
9.4.7 Other Information Disclosure Circumstances ..... 45
9.5 Intellectual Property Rights ..... 45
9.6 Representations and Warranties ..... 45
9.6.1 CA Representations and Warranties ..... 45
9.6.2 RA Representations and Warranties ..... 46
9.6.3 Subscriber Representations and Warranties ..... 46
9.6.4 Relying Party Representations and Warranties ..... 46

9.6.5 Representations and Warranties of Other Participants ..... 46
9.7 Disclaimers of Warranties ..... 47
9.8 Limitations of liability ..... 47
9.9 Indemnities ..... 47
9.9.1 Indemnification by CAs ..... 47
9.9.2 Indemnification by Subscribers ..... 47
9.9.3 Indemnification by Relying Parties ..... 48
9.10 Term and Termination ..... 48
9.10.1 Term ..... 48
9.10.2 Termination ..... 48
9.10.3 Effect of Termination and Survival ..... 48
9.11 Individual Notices and Communications ..... 48
9.12 Amendments ..... 48
9.12.1 Procedure for Amendment ..... 48
9.12.2 Notification Mechanism and Period ..... 49
9.12.3 Circumstances under which OID Must Be Changed ..... 49
9.13 Dispute Resolution Provisions ..... 49
9.14 Governing Law ..... 49
9.15 Compliance with applicable law ..... 49
9.16 Miscellaneous Provisions ..... 49
9.16.1 Entire Agreement ..... 49
9.16.2 Assignment ..... 49
9.16.3 Severability ..... 49
9.16.4 Enforcement (attorneys' fees and waiver of rights) ..... 49
9.16.5 Force Majeure ..... 50
9.17 Other Provisions ..... 50

**A. Revision History ..... 51**

# Tables

Table 1: Object Identifiers ..... 2
Table 2: Abbreviations ..... 5
Table 3: Types of Recorded Events ..... 27
Table 4: Algorithm Object Identifiers ..... 35
Table 5: Revision History ..... 51

# 1 Introduction

## 1.1 Overview and Objectives

This Certificate Policy (CP) defines the procedural and operational requirements that the NFC Forum expects Certificate Authorities (CAs) to adhere to when issuing and managing certificates to create signatures for NDEF messages.

Pursuant to the [RFC3647] framework, this CP is divided into nine parts that cover the security controls, practices, and procedures for certificate or time-stamping services within the NFC Forum Public Key Infrastructure (PKI). To preserve the outline specified by [RFC3647], section headings that do not apply have the statement "Not applicable" or "No stipulation."

## 1.2 Scope

### 1.2.1 Appropriate Certificate Uses

Digital signing of NDEF data is a trustworthy method for providing information about the origin of NDEF data in an NFC Forum Tag and NFC Forum Device. It provides users with the possibility of verifying the authenticity and integrity of data within the NDEF message. This CP specifies the format used when signing single or multiple NDEF records.

A malicious third party could delete the signature record from the NDEF message or attach a new signature record to prevent the application user from noticing any malicious change of content. It must be understood that the verification is only as trustworthy as the tools (signature algorithm, certificate, etc.) and processes (e.g., security policies) that are being used. These risks, along with the use of the Signature record, should be taken into consideration in the development of applications.

### 1.2.2 Prohibited Certificate Uses

This CP does not define or mandate a specific PKI or certification system, or to define a new algorithm for use with [SIGNATURE].Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate issued. Certificates do not indicate that a signed message is safe to install or is free from malware, bugs, or vulnerabilities.

Certificates issued under this CP may not be used (i) for any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

## 1.3 Audience

### 1.3.1 Public Key Infrastructure (PKI) Authorities

Certificate Authorities providing RTD Signatures must comply with the requirements of this CP and all relevant international standards and regulations before asserting an OID under the NFC Forum arc. The NFC Forum is responsible for this CP, the approval of related practice statements, and overseeing the conformance of CA practices with this CP.

### 1.3.2 Registration Authorities

Registration Authorities (RA) operate identity management systems and collect and verify Subscriber information on a CA's behalf. The requirements in this CP apply to all RAs. CAs are required to monitor each RA's compliance with this policy.

### 1.3.3 Subscribers

Subscribers use NFC Forum's services and PKI to support transactions and communications. Subscribers are not always the party identified in a certificate, such as when certificates are issued to an affiliate or service provider. The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the subject of the certificate and the entity that contracted with the Issuer CA for the certificate's issuance. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

### 1.3.4 Relying Parties

Relying Parties are entities that act in reliance on a certificate and/or digital signature issued by the CA. Relying parties should check the appropriate CRL information prior to relying on information featured in a certificate.

### 1.3.5 Other Participants

No stipulation.

## 1.4 Applicable Documents or References

This document is the NFC Forum Signature RTD Certificate Policy. The NFC Forum's OID is joint-iso-ccitt (2) country (16) USA (840) US-company (1) NFC Forum (114513). The NFC Forum uses this OID arc for the various identifiers described in this CP, including:

**Table 1: Object Identifiers**

| Digitally Signed Object | Object Identifier (OID) |
|---|---|
| Policy Documents | 2.16.840.1.114513.0 |
| This CP Document | 2.16.840.1.114513.0.1.0 |
| NDEF Message Signing Intermediate Certificate | 2.16.840.1.114513.0.1.1 |
| NDEF Message Signing End Entity Certificate | 2.16.840.1.114513.0.1.2 |
| ASN.1 Modules | 2.16.840.1.114513.5 |
| M2M Certificate | 2.16.840.1.114513.5.0 |
| Certificate Extensions | 2.16.840.1.114513.29 |
| Extended Key Usage | 2.16.840.1.114513.29.37 |
| RTD Signature | 2.16.840.1.114513.29.37.5 |

This CP applies to any entity or certificate asserting one or more of the OIDs identified above.

Documents referred to in this CP include:

| | |
|---|---|
| [Common_Criteria] | Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408-1, 2009 |
| [FIPS_140_2] | Security Requirements for Cryptographic Modules<br>http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf<br>May 25, 2001. |
| [RFC2119] | Key words for use in RFCs to Indicate Requirement Levels, RFC 2119,<br>S. Bradner,<br>March 1997,<br>Internet Engineering Task Force |
| [RFC3447] | Public-Key Cryptography Standards (PKCS) # 1: RSA Cryptography Specifications Version 2.1,<br>J. Jonsson, B. Kaliski,<br>February 2003,<br>Internet Engineering Task Force |
| [RFC3647] | Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,<br>S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu,<br>November 2003,<br>Internet Engineering Task Force |
| [RFC5280] | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,<br>D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Hously, W. Polk,<br>May 2008 |
| [RFC6960] | X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP),<br>S. Santesson, M. Myers, R. Ankney, A. Malpani, C. Adams,<br>June 2013,<br>Internet Engineering Task Force |
| [SEC1] | Standards for Efficient Cryptography 1 (SEC1): Elliptic Curve Cryptography,<br>Version 2.0,<br>May 2009,<br>Certicom Research |
| [SEC4] | Standards for Efficient Cryptography 4 (SEC4): Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV),<br>Version 1.0,<br>January 2013,<br>Certicom Research |
| [SIGNATURE] | Signature Record Type Definition (RTD)<br>Candidate Technical Specification, Version 2.0 |


## 1.5 Administration

The NFC Forum Signature RTD Certificate Policy is a policy document supported by the Near Field Communication Forum, Inc., located at:

401 Edgewater Place, Suite 600
Wakefield, MA, 01880

Tel.: +1 781-876-8955
Fax: +1 781-610-9864

http://www.nfc-forum.org/

The NFC Forum determines the suitability and applicability of this CP. The NFC Forum also determines the conformance of a CA to this CP based on the results and recommendations received from an independent auditor.

## 1.6 Name and Logo Usage

The Near Field Communication Forum's policy regarding the use of the trademarks *NFC Forum* and the NFC Forum logo is as follows:

- Any company MAY claim compatibility with NFC Forum specifications, whether a member of the NFC Forum or not.
- Permission to use the NFC Forum logos is automatically granted to designated members only as stipulated on the most recent Membership Privileges document, during the period of time for which their membership dues are paid.
- Member's distributors and sales representatives MAY use the NFC Forum logo in promoting member's products sold under the name of the member.
- The logo SHALL be printed in black or in color as illustrated on the Logo Page that is available from the NFC Forum at the address above. The aspect ratio of the logo SHALL be maintained, but the size MAY be varied. Nothing MAY be added to or deleted from the logos.
- Since the NFC Forum name is a trademark of the Near Field Communication Forum, the following statement SHALL be included in all published literature and advertising material in which the name or logo appears:

***NFC Forum and the NFC Forum logo are trademarks of the Near Field Communication Forum.***

## 1.7 Intellectual Property

This document conforms to the Intellectual Property guidelines specified in the NFC Forum's *Intellectual Property Rights Policy* (http://nfc-forum.org/wp-content/uploads/2013/11/NFC-Forum-IPR-Policy.pdf), as outlined in the NFC Forum *Rules of Procedure* (http://nfc-forum.org/wp-content/uploads/2013/11/NFC-Forum-Rules-of-Procedure.pdf).

## 1.8 Special Word Usage

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## 1.9 Abbreviations

The abbreviations as used in this document are defined in Table 2.

**Table 2: Abbreviations**

| Abbreviation | Description |
|---|---|
| CA | Certificate Authority |
| CP | Certificate Policy |
| CPS | Certificate Practice Statement |
| DSA | Digital Signature Algorithm |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ECQV | Elliptic Curve Qu-Vanstone Implicit Certificate Scheme |
| NDEF | NFC Data Exchange Format |
| PKI | Public Key Infrastructure |
| RFU | Reserved for Future Use |
| RSA | Rivest-Shamir-Adleman encryption algorithm (public key encryption algorithm) |
| RTD | Record Type Description |
| SHA-1 | Secure Hash Algorithm, version 1 |
| SHA-256 | Secure Hash Algorithm |
| URI | Uniform Resource Identifier (e.g., http://, ftp://, mailto:, news:) |
| URL | Uniform Resource Locator (a special case of a URI) |

## 1.10 Glossary

*Accounting Practitioner*

A certified public accountant, chartered accountant, or a person with an equivalent license within the country of the Applicant's operation; provided that an accounting standards body in the jurisdiction maintains full (not "suspended" or "associate") membership status with the International Federation of Accountants.

*Applicant*

An entity applying for a certificate.

*Digital Certificate*

A Digital Certificate is an electronic document that uses a digital signature to bind a public key with an identity. The certificate can be used to verify that a public key belongs to an individual.

*End Entity Digital Certificate*

An end entity digital certificate is issued with the intent to create Signature Records on behalf of the Certificate's Subject.

*CRL*

As specified in [RFC5280], a Certificate Revocation List is a list of serial numbers of certificates that have been revoked. Entities presenting those (revoked) certificates should no longer be trusted.

*OCSP*

Online Certificate Status Protocol (OCSP) is used for obtaining the revocation status of a X.509 digital certificate as described in [RFC6960].

*High Risk Applicant*

A request that the CA flags for additional scrutiny prior to issuance.

*Key Pair*

A Private Key and associated Public Key.

*Latin Notary*

A person with legal training whose commission under applicable law not only includes authority to authenticate the execution of a signature on a document but also responsibility for the correctness and content of the document. A Latin Notary is sometimes referred to as a Civil Law Notary.

*Legal Practitioner*

A person who is either a lawyer or a Latin Notary as described in these Guidelines and competent to render an opinion on factual claims of the Applicant.

*Private Key*

The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

*Public Key*

The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

*Reliable Data Source*

An identification document or source of data used to verify information about a Subject and is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

*Relying Party*

An entity that relies upon either the information contained within a certificate or a Signature Record.

*Relying Party Agreement*

An agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using NFC Forum’s Repository.

*Signature Record*

A digital signature related to one or more records within an NDEF message that can be used to verify the integrity and authenticity of the content, i.e., the data records that have been signed.

*Subject*

The legal entity identified in a Certificate and is the entity responsible for any Signature Records created using the Certificate.

*Subscriber*

Either the entity identified as the subject in the certificate or the entity receiving NFC Forum's time-stamping services.

*Subscriber Agreement*

An agreement that governs the issuance and use of a certificate that the Applicant must read and accept before receiving a certificate.

*Suspect Message*

Any NDEF message that (i) is affiliated with an entity or website that qualifies as high risk under this CP, (ii) is affiliated with an entity that is listed on a denied list or blacklist provided by a government authority in the CA's jurisdiction of operation, or (ii) contains or links to malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

*Verified Legal Opinion*

A document meeting the requirements specified in Section 3.2.4 of this CP.

*WebTrust*

The current version of the AICPA/CICA WebTrust Program for Certification Authorities.

# 2 Publication and Repository Responsibilities

## 2.1 Repositories

CAs must publish all root certificates and cross-certificates, issued to and from the CA, revocation data for issued digital certificates, CP, CPS, standard Relying Party agreements, and standard Subscriber agreements related to its issuance of certificates asserting an NFC Forum OID in at least one online repository that is publicly accessible. The CA shall ensure that its root certificate and all revocation data for issued certificates are available through a repository 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.5% annually.

## 2.2 Publication of Certification Information

CAs must make root certificates, cross certificates, CRLs, CPs, and CPSs related to the issuance of certificates asserting the NFC Forum OID publically accessible on the web. CAs may publish a redacted version of their CP and CPS provided the redacted version still shows how the CA is complying with this CP. CPS and CP documents must be structured in accordance with [RFC3647].

## 2.3 Time or Frequency of Publication

CAs must publish CA certificates and revocation data as soon as possible after issuance. CAs should publish new or modified versions of CP and CPS documents as soon as possible after the document is approved by the CA’s policy authority.

## 2.4 Access Controls on Repositories

Information published in a repository is public information. CAs must provide unrestricted read access to its repositories and implement logical and physical controls to prevent unauthorized write access to such repositories.

# 3 Identification and Authentication

## 3.1 Naming

### 3.1.1 Types of Names

CAs must issue certificates with information, including distinguished names, that comply with the requirements of either Appendix A or Appendix B in [SIGNATURE]. CAs must limit distinguished name character encodings to one string type, usually UTF8String (which a profile might limit to IA5 characters) and define modest length constraints on all distinguished name attributes. CAs may use any standard X.509 extension from [RFC5280], but the use of extensions not specified in Appendix A or Appendix B in [SIGNATURE] is highly discouraged.

For applications where a certificate is always accompanied in its transmission by its superior certificate, the CA can eliminate the issuer field from the transmitted form of the certificate (it is still included for signature generation and verification purposes). Because Issuer Name can be reused from the subject field of the superior certificate, this field is optional in the syntax in order to allow two variants of every certificate: the full (to-be-signed) form, and the transmitted form. Similarly, in the ECQV case, the algorithm identifier can be reused rather than transmitted again.

### 3.1.2 Use Meaningful Names

CAs must use names that accurately identify both the subject and issuer of the certificate.

### 3.1.3 Anonymity or Pseudonymity of Subscribers

CAs may issue end-entity anonymous or pseudonymous certificates provided that the certificate still complies with this policy.

### 3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using the formats specified in Appendix A or Appendix B in [SIGNATURE].

### 3.1.5 Uniqueness of Names

No stipulation.

### 3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers may not request certificates with any content that infringes upon the intellectual property rights of another entity. Unless otherwise specifically stated, this CP does not require a CA to verify an Applicant’s right to use a trademark. CAs may reject any application or require revocation of any certificate that is part of a trademark dispute.

## 3.2 Initial Identity Validation

CAs may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant.

### 3.2.1 Method to Prove Possession of Private Key

CAs must verify that the Applicant possesses the Private Key corresponding to the Public Key in the certificate request. This requirement does not apply to the ECQV (see [SEC4])certificate issuance process.

### 3.2.2 Authentication of Organization Identity

#### 3.2.2.1 Identity

CAs must verify the following information for each organizational certificate applicant:

- **Registered Entities:** The CA must verify the Applicant's status as a legally recognized entity directly with a government entity with which the Applicant filed formation documents. The Applicant must not be designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid", "not current", or the equivalent. During verification, the CA must obtain the Applicant's formal legal name, registration number, or (if a registration number is not available), a date of formation, and registered office. The CA may obtain this information directly from the government entity or through a reliable database operated by a government entity operating in Applicant's jurisdiction of operation.
- **Government Entities**: The CA must verify the Applicant's status as a legally recognized government entity. The CA must obtain the Applicant's legal name and (if available) the date of the entity's creation as verified with a legislative act, regulation, or similar government action. The CA must obtain this information directly from a reliable government source of information, from a judge or attorney representing the entity, or from a superior government entity in the same political jurisdiction as the Applicant.
- **Other Entities**: The CA must verify the Applicant's existence as an entity using a reliable database. In addition, the CA must verify an individual, in accordance with Section 3.2.3, who is identified by their title as able to conduct business related to the issuance of the Certificate. The Applicant must not be designated as on the records of a government registration agency responsible for registering organizations that are the same type as the Applicant as "inactive", "invalid", "not current", or the equivalent. The CA must obtain the Applicant's name and either a registration number or, (if a registration number is not available), a date of formation. The CA may obtain this information from a Reliable Data Source but must give preference to government sources that typically provide such information for entities located in the Applicant's jurisdiction of operation.

#### 3.2.2.2 Assumed Name

If the Certificate will include a name other than the legal name verified under Section 3.2.2.1 or Section 3.2.3, then the CA must verify that the included name is either registered to Applicant with an appropriate government agency in Applicant's jurisdiction of operation or a commonly recognized name of the Applicant. The CA may verify this information with a Reliable Data Source or rely on a Verified Opinion Letter that states the Applicant has the right to use the name.

#### 3.2.2.3 Place of Business

The CA must verify that the physical address provided by the Applicant is an address where the Applicant or a parent or subsidiary of the Applicant conducts business operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for an agent of the Applicant). The CA may rely on a Reliable Data Source to verify this information.

#### 3.2.2.4 Reliable Method of Communication

The CA must verify the Applicant's ability to receive communication through email, fax, telephone, or post by communicating with the Applicant through such method of communication. The CA must obtain the address or number from a Reliable Data Source or through a Verified Opinion Letter.

#### 3.2.2.5 Operational Existence

If government records indicate that the Applicant has been in existence for fewer than three years and the Applicant is not listed in a Reliable Data Source, the CA must verify that the Applicant has an active financial account with a financial institution or receive a Verified Opinion Letter stating that the Applicant is operational. For financial documents, the CA may rely on documentation provided by the Applicant if the CA can verify the documentation with the financial institution.

### 3.2.3 Authentication of Individual Identity

The CA, RA, an attorney, a notary, a Latin notary, an agent of the CA or RA, or an entity certified by a government authority in Applicant's jurisdiction of operation to verify identities must verify an individual applicant (and an individual for non-registered business entities as required under Section 3.2.2.1) in a face-to-face setting. The CA may only rely on face-to-face validation by an RA or agent if the CA has evaluated the RA's/agent's validation procedure and concluded that it satisfies the requirements of this CP.

- The individual must present the following documentation (Vetting Documents) directly to the person performing the validation (validator):
    - A signed attestation that includes all of the following information:
        - Full name or names by which the individual is, or has been, known (including all other names used)
        - Residential address at which the individual can be located
        - Date of birth
        - An affirmation that all of the information contained in the Certificate request is true and correct
- A current signed government-issued identification document that includes a photo of the individual and is signed by the Individual such as:
    - A passport
    - A driver's license
    - A personal identification card
    - A concealed weapons permit
    - A military ID
- At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which must be from a financial institution.
    - Acceptable financial institution documents include:
        - A major credit card, provided that it contains an expiration date and it has not expired

- A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired
- A mortgage statement from a recognizable lender that is less than six months old
- A bank statement from a regulated financial institution that is fewer than six months old

- Acceptable non-financial documents include:
  - Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill)
  - A copy of a statement for payment of a lease, provided that the statement is dated within the past six months
  - A certified copy of a birth certificate
  - A local authority tax bill for the current year
  - A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers

The person performing the validation must:

- Attest to the signing of the attestation and the identity of the signer
- Identify the original documents used to perform the identification; and
  - The CA must verify completion of the validation with the validator. If the validator is not an employee or agent of the CA or RA, the CA must first try to contact the validator using information obtained from a government database responsible for registering such validators before attempting other methods of verifying that the completeness of the validation.
  - The CA must obtain the signed affirmation document and a copy of the government-issued photo identification document. The CA must review the documentation to determine that the information is consistent, matches the information in the application, is not expired, and identifies the individual. The CA MAY rely on electronic copies of documentation if the CA confirms the documentation's authenticity.

#### 3.2.3.1 Authentication for Role-based Certificates

A CA may issue certificates that identify a specific role that the Subscriber holds, provided that the role identifies a specific individual within an organization (e.g., *Chief Information Officer* is a unique individual, whereas *Program Analyst* is not). These role-based certificates are used when non-repudiation is desired. The CA may only issue role-based certificates to Subscribers who are verified in accordance with this CP. A CA may issue certificates with the same role to multiple Subscribers. However, the CA shall require that each certificate have a unique key pair. Individuals may not share their issued role-based certificates and are required to protect the role-based certificate in the same manner as individual certificates.

The CA or an RA must verify the identity of the individual requesting a role-based certificate (i.e. the sponsor) in accordance with Section 3.2.3and identify a sponsor for the Certificate before issuing a role-based certificate.

#### 3.2.3.2 Authentication for Group Certificates

No stipulation.

#### 3.2.3.3 Authentication of Devices with Human Sponsors

A CA may issue a Certificate for use on a computing or network device, provided that the entity owning the device is identified in the Certificate. The device must have a human or organization sponsor that is verified in accordance with this CP and who provides the CA with:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name)
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information

Either the CN field or O field of the Certificate must identify the device. If the Certificate's sponsor changes, the new sponsor must review the status of each device to ensure that it is still authorized to receive certificates. The CA's CPS must describe procedures to ensure that certificate accountability is maintained.

#### 3.2.3.4 Non-verified Subscriber Information

Certificates may not contain any non-verified subscriber information.

### 3.2.4 Validation of Authority

The CA must verify the name, title, and authorization of the person requesting the certificate through a source other than the requester. CAs may verify the person's name and title using any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person designated to act in such role. CAs may verify the authorization of the person by:

- Contacting the Applicant's Human Resources Department using a method of communication verified under Section 3.2.2.4
- Obtaining a confirmation from a VP or higher level of employee of the Applicant, who then confirms the requester's authorization through a method of communication verified under Section 3.2.2.4,where the employment level of the confirmed is verified using a Reliable Data Source or Applicant's Human Resources Department
- A Verified Opinion Letter stating that the Applicant is authorized to request the Certificate
- Verifying through a Reliable Data Source that the requester's title is a title typically associated with Certificate management
- For individual Applicants, relying on a representation from the individual that the certificate is authorized

The CA must implement a process that permits entities to limit the number of individuals authorized to request certificates. The CA must provide a list of authorized certificate requesters to an entity after receiving a verified request from the entity for such information.

### 3.2.5 Verification of Other Information Sources

#### 3.2.5.1 Verified Opinion Letter

Before relying on an opinion letter submitted to the CA, the CA MUST verify that such opinion letter meets the following requirements:

- **Status of Author:** The CA must verify that the opinion letter is authored by an Accounting Practitioner or Legal Practitioner that was retained by and representing the Applicant (or an in-house professional employed by the Applicant). The CA must verify the professional status of the author of the opinion letter by directly contacting the authority responsible for registering, licensing, or certifying such Legal Practitioner or Accounting Practitioner in the applicable jurisdiction. The CA must verify an Accounting Practitioner's license through that jurisdiction's member of the International Federation of Accountants (IFAC) or through the regulatory organization in that jurisdiction appropriate to contact when verifying an accountant's license to practice in that jurisdiction.
- **Basis of Opinion:** The CA must verify that the opinion's author based their conclusion on a familiarity with the relevant facts and the author's expertise. The opinion letter may include disclaimers and other limitations customary in the author's jurisdiction, provided the disclaimers and limitations do not eliminate the author's responsibility if the opinion is proven erroneous.
- **Authenticity:** The CA must confirm the opinion's authenticity by contacting the opinion's author using contact information listed with the authority responsible for registering, licensing, or certifying the author, and obtaining confirmation that the opinion letter is authentic. If contact information is not available from a licensing authority, the CA may use contact information obtained from a Reliable Data Source. A digitally signed opinion letter is confirmed by validation of the digital signature.

#### 3.2.5.2 Reliable Data Source

A Reliable Data Source is a regularly-updated and publicly available data source designed for the purpose of accurately providing the information for which it is consulted and which is generally recognized as a dependable source of such information. A database is considered a Reliable Data Source if:

- The database is a source of information that is considered reliable and utilized by industries other than CAs for providing accurate location or contact information;
- The database provider identifies how frequently they update the information in their database; and
- The database is updated on at least an annual basis.

A CA should rely on a government-provided database instead of a commercial database if a government database is available. If information in a commercial database materially contradicts data provided in the government data source, the CA must identify the request as a High Risk Applicant.

Databases in which the CA or its owners or affiliated companies maintain a controlling interest, or in which any RA or subcontractors to whom the CA has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest, do not qualify as a Reliable Data Source.

## 3.3 Identification and Authentication for Re-key Requests

### 3.3.1 Identification and Authentication for Routine Re-key

The CA or RA must re-establish the identity of a Subscriber when a new certificate is requested if more than 13 months have passed since the identity of the Subscriber was last verified. A CA may rely on its previous verification of all of the following:

- The individual associated with “Other Entities” if the individual is the same person as previously verified in connection with a Certificate issued under this CP
- The Applicant's address
- Applicant’s ability to receive communication, provided the CA re-affirms the applicant’s communication using the verified method of communication
- The Applicant's operational existence
- The authority of the certificate requester

### 3.3.2 Identification and Authentication for Re-key After Revocation

CAs must require subscribers of certificates revoked (for reasons other than as the result of a routine certificate renewal, update, or modification action) to undergo the initial registration process (described in Section 3.2) to obtain a new certificate.

## 3.4 Identification and authentication for revocation request

The CA or the RA must authenticate all revocation requests. The CA or RA may authenticate a revocation request using the Certificate’s Public Key, regardless of whether the associated Private Key is compromised.

# 4 Certification Life-cycle Operational Requirements

## 4.1 Certificate Application

### 4.1.1 Who Can Submit a Certificate Application

Any individual, organization, or device that can be verified under this CP may submit a certificate application, provided that issuing the requested certificate will not violate any applicable law or regulation. The CA must verify whether the Applicant or certificate requester is identified on a government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation.

### 4.1.2 Enrollment Process and Responsibilities

The CA is responsible for ensuring that the identity of each Certificate Applicant is verified in accordance with this CP and the applicable CPS prior to the issuance of a certificate. Applicants should submit sufficient information and documentation for the CA or the RA to perform the required verification of identity prior to issuing a Certificate. The CA and RA must authenticate and protect all communication made during the certificate application process.

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

CAs and RAs must identify and verify each Applicant in accordance with their applicable Certification Practice Statements and Registration Practice Statements. CAs must ensure that all communication between the CA and an RA regarding certificate issuance or changes in the status of a certificate are made using secure and auditable methods. If databases or other sources are used to confirm sensitive or confidential attributes of an individual subscriber, then that sensitive information must be protected and securely exchanged in a confidential and tamper-evident manner, protected from unauthorized access, and tracked using an auditable chain of custody.

The CA must follow a documented process to identify High Risk Applicants. The CA should use internal databases to identify High Risk Applicants using previously revoked certificate requests and rejected certificate requests. The CA should also identify High Risk Applicants by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes. If the Applicant is considered high risk, the CA must conduct such additional verification activity and take such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under this CP.

### 4.2.2 Approval or Rejection of Certificate Applications

CAs must reject any certificate application if the identity of the Applicant cannot be verified. The CA may also reject a certificate application on any reasonable basis, including if the certificate could damage the CA's business or reputation. CAs are not required to provide a reason for rejecting a certificate application.

The results of the verification processes and procedures outlined in this CP are intended to be viewed both individually and as a group. After all of the verification processes and procedures are completed, the CA must have a person who did not collect the documentation and information review the application and look for discrepancies or other details requiring further explanation. The CA must obtain and document further explanation or clarification from the Applicant and other sources as necessary to resolve discrepancies or details that require further explanation.

The CA must not issue a certificate until the entire body of information and documentation is assembled in support of the certificate request, or if issuance will communicate factual information that the CA knows, or should know, to be inaccurate.

If some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the CA or an RA must perform the requirements of this section using employees under its control that have appropriate training, experience, and judgment in confirming organizational identification and authorization. When employees under the control of the CA do not possess the language skills necessary to verify the certificate information, the CA may rely on the services of a professional translator.

The CA may authorize the Subject of a specified valid Certificate to perform the RA function and authorize the issuance of additional Certificates provided that the Certificate's subject/sponsor is verified in accordance with this CP. Once these conditions are met, the RA may perform the final approval of the certificate without additional approval from the CA.

### 4.2.3 Time to Process Certificate Applications

No stipulation.

## 4.3 Certificate Issuance

### 4.3.1 CA Actions during Certificate Issuance

CAs and RAs must protect databases under its control that are used to confirm Subscriber identity information from unauthorized modification or use. CAs must perform actions taken during the certificate issuance process in a secure manner. Certificate issuance by the CA must require the actions of at least two individuals operating on behalf of the CA or RA, at least one of which is an individual authorized by the CA (i.e., the CA system operator, system officer, or PKI administrator), to deliberately issue a direct command to perform a certificate signing operation. A CA must not use its root CA Private Keys to sign Certificates. CAs may not root CA private keys to sign end entity certificates.

### 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

No stipulation.

## 4.4 Certificate Acceptance

### 4.4.1 Conduct Constituting Certificate Acceptance

CAs may consider the passage of a reasonable time period after delivery, or notice of issuance of a certificate to the Subscriber, or the Subscriber's use of a certificate to constitute the Subscriber's acceptance of the certificate.

### 4.4.2 Publication of the Certificate by the CA

CAs must publish all CA certificates to the CA's repository. CAs are not required to publicly publish intermediate or end entity certificates.

### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## 4.5 Key Pair and Certificate Usage

### 4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Keys from unauthorized use or disclosure by third parties and may use their Private Keys only to create signatures for NDEF messages.

### 4.5.2 Relying Party Public Key and Certificate Usage

CAs limit the use of Certificates issued under this policy through inclusion of the NFC Forum OID in the extended key usage extension. CAs must provide status information for Certificates using the appropriate CRL. A Relying Party should use discretion when relying on a certificate and should consider the totality of the circumstances and risk of loss prior to relying on a certificate. Relying on a digital signature or Certificate that has not been processed in accordance with applicable standards may result in risks to the Relying Party. The Relying Party is solely responsible for such risks. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate.

## 4.6 Certificate Renewal

### 4.6.1 Circumstance for Certificate Renewal

A CA may renew a Certificate if:

- The associated public key has not reached the end of its validity period
- The associated private key has not been compromised
- The Subscriber name and attributes are unchanged
- Re-verification of subscriber identity is not required by Section 3.3.1

A CA may also renew a Certificate if a CA certificate is re-keyed. After renewing a certificate, the CA may not re-key, renew, or modify the old certificate.

### 4.6.2 Who May Request Renewal

Only an authorized representative of a Subscriber may request renewal of the Subscriber's certificates. A CA may renew a certificate without a corresponding request if the signing certificate is re-keyed.

### 4.6.3 Processing Certificate Renewal Requests

The CA may require reconfirmation or verification of the information in a certificate prior to renewal.

### 4.6.4 Notification of New Certificate Issuance to Subscriber

The CA must notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the certificate to the Subscriber.

### 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

CAs may consider the passage of a reasonable time period after delivery, or notice of issuance of the certificate to the Subscriber, or the Subscriber's use of the certificate, to constitute the Subscriber's acceptance of the certificate.

### 4.6.6 Publication of the Renewal Certificate by the CA

The CA must publish renewed CA certificates to the CA's repository.

### 4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## 4.7 Certificate Re-key

### 4.7.1 Circumstance for Certificate Re-key

Re-keying a certificate consists of creating a new certificate with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may have a different validity period, key identifiers, specify different CRL distribution points, and/or be signed with a different key.

After re-keying a Certificate, the CA may not re-key, renew, or modify the old certificate.

### 4.7.2 Who May Request Certificate Re-key

A CA may initiate certificate re-key at the request of the certificate subject or in its own discretion.

### 4.7.3 Processing Certificate Re-key Requests

A CA may require revalidation of the Subscriber prior to re-keying a certificate. At a minimum, the CA must comply with Section 3.3.1 in identifying the Subscriber prior to re-keying the certificate.

### 4.7.4 Notification of Certificate Re-key to Subscriber

A CA must notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the certificate to the Subscriber.

### 4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

CAs may consider the passage of a reasonable time period after delivery, or notice of issuance of the certificate to the Subscriber, or the Subscriber's use of the certificate to constitute the Subscriber's acceptance of the certificate.

### 4.7.6 Publication of the Re-keyed Certificate by the CA

A CA must publish re-keyed CA certificates to the CA's repository.

### 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## 4.8 Certificate Modification

### 4.8.1 Circumstance for Certificate Modification

Modifying a certificate means creating a new certificate for the same subject with authenticated information that differs slightly from the old certificate (e.g., changes to email address or non-essential parts of names or attributes), provided that the modification otherwise complies with this CP. The new certificate may have the same or a different subject public key. After modifying a client certificate, the CA may not re-key, renew, or modify the old certificate.

### 4.8.2 Who May Request Certificate Modification

The CA may modify a certificate at the request of the certificate subject or in its own discretion.

### 4.8.3 Processing Certificate Modification Requests

After receiving a request for modification, the CA must verify any information that will change in the modified certificate. The CA may issue the modified certificate only after completing the verification process on all modified information.

### 4.8.4 Notification of Certificate Modification to Subscriber

A CA must notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the certificate to the Subscriber.

### 4.8.5 Conduct Constituting Acceptance of a Modified Certificate

CAs may consider the passage of a reasonable time period after delivery, or notice of issuance of the certificate to the Subscriber, or the Subscriber's use of the certificate to constitute the Subscriber's acceptance of the certificate.

### 4.8.6 Publication of the Modified Certificate by the CA

A CA must publish modified CA certificates to the CA's repository.

### 4.8.7 Notification of Certificate Modification by the CA to Other Entities

No stipulation.

## 4.9 Certificate Revocation and Suspension

### 4.9.1 Circumstances for Revocation

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated valid period. Prior to revoking a certificate, the CA must verify that the revocation request was made by either the organization or individual that made the certificate application or by an entity with the legal jurisdiction and authority to request revocation. The CA must revoke a certificate if the CA is aware that:

- The Subscriber or Subject requested revocation of the Certificate.
- The Subscriber did not authorize the Certificate request and did not retroactively grant authorization.
- Either the Private Key associated with the certificate or the Private Key used to sign the Certificate was compromised or misused.
- The Subscriber or cross-certified CA breached a material obligation under the CP, the CPS, or the relevant agreement.
- Either the Subscriber's or the CA's obligations under this CP or the relevant CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised.
- The Applicant has lost its rights to a trademark listed in the certificate.
- The Certificate was not issued in accordance with an applicable CP, an applicable CPS, or applicable industry standards.
- The CA received a lawful and binding order from a government or regulatory body to revoke the certificate.
- The CA is about to cease operations and there will be no future revocation support for the certificate.
- The CA's right to manage certificates under this CP was terminated (unless arrangements have been made to continue providing the CRL services).
- Information appearing in the Certificate was or became inaccurate or misleading.
- The NFC Forum determines that the technical content or format of the Certificate presents an unacceptable security risk to application software vendors, Relying Parties, or others.
- The Certificate was used to sign, publish, or distribute Suspect Code.

### 4.9.2 Who Can Request Revocation

The CA or RA must accept revocation requests from authenticated and authorized parties, such as the certificate Subscriber. The CA must implement a process that permits third parties to request revocation of Certificates used to sign Suspect Messages.

The CA or RA may establish procedures that allow other entities to request certificate revocation for fraud or misuse. CAs may revoke a certificate of its own volition without reason, even if no other entity has requested revocation.

### 4.9.3 Procedure for Revocation Request

The CA or RA must authenticate and log each revocation request. A CA must always revoke a certificate if the request is authenticated as originating from the Subject of the certificate. CAs must be able to internally respond 24/7 to any high priority certificate problem reports. The CA or the RA may forward complaints to law enforcement.

CAs must begin to investigate any report of a Certificate used to sign Suspect Message within one business day after receiving a notice of a Suspect Message. The CA must revoke any Certificate used to sign a Suspect Message within 24 hours after the CA determines the signed message qualifies as a Suspect Message.

### 4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the Subscriber within which the Subscriber must make a revocation request after reasons for revocation have been identified. CAs and RAs must request initiated revocation within one day after confirming a key compromise.

### 4.9.5 Time within which CA Must Process the Revocation Request

CAs must process revocation requests as soon as practical, generally within one business day.

### 4.9.6 Revocation Checking Requirement for Relying Parties

Whenever practical, platforms should check the revocation status of the certificates that they rely upon. Platforms utilizing Signature Records to verify NDEF messages should not rely on any Signature Record if CRL information is not regularly updated and made available. CRL information should be retrieved on at least a daily basis.

A certificate may have a one-to-one relationship with the NDEF message that it verifies. In such cases, revocation of the certificate only invalidates the signature of the Suspect Message. If a certificate has a one-to-many relationship with the NDEF message that it verifies, then revocation of the certificate invalidates the signatures on all those NDEF messages, some of which may be perfectly sound.

### 4.9.7 CRL Issuance Frequency

CAs that operate offline and only issue CA certificates, certificate-status-checking certificates, or internal administrative certificates must publish a CRL at least every 6 months. All other CAs must publish CRLs at least every 24 hours and within 18 hours after confirming a key compromise.

### 4.9.8 Maximum Latency for CRLs

CAs must post irregular, interim, or emergency CRLs to their public repository within four hours of generation. Regular CRLs must be published prior to the nextUpdate field in the previously issued CRL of the same scope.

### 4.9.9 On-line Revocation/Status Checking Availability

CAs must provide online status checking via CRLs. To keep CRL sizes small, CAs should partition their CRLs, keeping certificates issued under this policy separate from CRLs for other types of Certificates. CAs are required to provide accurate and up-to-date revocation status information though CRLs for at least one year following the date the Certificate is revoked.

### 4.9.10 On-line Revocation Checking Requirements

Relying Parties must verify the validity of a certificate using the provided CRLs. Platform operators are expected to download the CRL information on a regular basis (preferably on at least a daily basis) and perform out-of-bands revocation checking by comparing encountered certificates with information on downloaded CRLs

### 4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

### 4.9.12 Special Requirements Related to Key Compromise

CAs must use commercially reasonable efforts to notify potential Relying Parties if compromise of a Private Key is discovered or suspected.

### 4.9.13 Circumstances for Suspension

Not applicable.

### 4.9.14 Who Can Request Suspension

Not applicable.

### 4.9.15 Procedure for Suspension Request

Not applicable.

### 4.9.16 Limits on Suspension Period

Not applicable.

## 4.10 Certificate Status Services

### 4.10.1 Operational Characteristics

CAs must make certificate status information available via CRL for at least one year following revocation of the Certificate.

### 4.10.2 Service Availability

CAs must provide certificate status services 24x7 without interruption.

### 4.10.3 Optional Features

No stipulation.

## 4.11 End of Subscription

CAs must allow Subscribers to end their subscriptions to certificate services and have their certificates revoked.

## 4.12 Key Escrow and Recovery

### 4.12.1 Key Escrow and Recovery Policy Practices

CAs may not escrow, or permit a third party to escrow, Private Keys for Certificates issued under this CP.

### 4.12.2 Session Key Encapsulation and Recovery Policy and Practices

CAs supporting session key encapsulation and recovery must describe their practices in their CPS.

# 5 Facility, Management, and Operational Controls

## 5.1 Physical Controls

### 5.1.1 Site Location and Construction

CAs must operate in a secure data center equipped with logical and physical controls that make the CA operations inaccessible to non-trusted personnel. The site location and construction, when combined with other physical security protection mechanisms such as guards, door locks, and intrusion sensors, must provide robust protection against unauthorized access to CA equipment and records. RAs must protect their equipment from unauthorized access in a manner that is appropriate to the level of threat to the RA, including protecting equipment from unauthorized access while the cryptographic module is installed and activated and implementing physical access controls to reduce the risk of equipment tampering, even when the cryptographic module is not installed and activated.

### 5.1.2 Physical Access

CAs and RAs must protect equipment from unauthorized access and must implement physical controls to reduce the risk of equipment tampering. CAs must manually or electronically monitor its systems for unauthorized access at all times, maintain an access log that is inspected periodically, and require two-person physical access to the CA hardware and systems. CAs shall deactivate and securely store CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and must not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA equipment or private keys.

### 5.1.3 Power and Air Conditioning

CAs must maintain a backup power supply and sufficient environmental controls to protect the CA systems and allow the CA to automatically finish pending operations and record the state of equipment before a lack of power or air conditioning causes a shutdown.

### 5.1.4 Water Exposures

CAs must protect CA equipment from water exposure.

### 5.1.5 Fire Prevention and Protection

CAs must use facilities equipped with fire suppression mechanisms.

### 5.1.6 Media Storage

CAs and RAs must protect all media from accidental damage and unauthorized physical access. CAs and RAs must duplicate and store audit and archive information in a backup location that is separate from its primary operations facility.

### 5.1.7 Waste Disposal

CAs and RAs must destroy all data (electronic and paper) in accordance with generally accepted procedures for permanently destroying such data.

### 5.1.8 Off-site Backup

CAs and RA must make weekly system backups sufficient to recover from system failure and must store the backups, including at least one full backup copy, at an off-site location that has procedural and physical controls that are commensurate with its operational location.

### 5.1.9 Certificate Status Hosting, CMS and External RA Systems

All physical control requirements under this Section 5.1 apply equally to Certificate Status and external RA system.

## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

CA and RA personnel acting in trusted roles include CA and RA system administration personnel and personnel involved with identity vetting and the issuance and revocation of certificates. CAs and RAs must distribute the functions and duties performed by persons in trusted roles in a way that prevents one person from circumventing security measures or subverting the security and trustworthiness of the PKI. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of CA and RA operations. These controls must be auditable.

### 5.2.2 Number of Persons Required per Task

Activation of a CAs' Private Keys, generation of a CA Key Pair, and backup of a CA Private Key must require the actions of two different individuals acting in trusted roles.

### 5.2.3 Identification and Authentication for Each Role

CA personnel must authenticate themselves in the certificate management system before they are allowed access to the systems necessary to perform their trusted roles.

### 5.2.4 Roles Requiring Separation of Duties

CAs and RAs may enforce separation of duties by either using CA equipment or procedurally, or by both means. The CA and RA software and hardware must identify and authenticate its users and ensure that no user can assume multiple identities.

## 5.3 Personnel Controls

### 5.3.1 Qualifications, Experience, and Clearance Requirements

CAs are responsible and accountable for the operation of their PKI and the CA's and RA's compliance with this CP. CAs and RAs must ensure that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CP.

### 5.3.2 Background Check Procedures

To the extent permitted by law, CAs and RAs must require each person fulfilling a trusted role to undergo checks and identification prior to acting in the role, including verification of the individual's identity, employment history, education, character references, social security number, previous residences, driving records, and criminal background. Previous residences must be checked for the past three years. All other checks are for the prior five years. CAs and RAs must verify the highest education degree obtained regardless of the date awarded and shall refresh all background checks at least every ten years.

CAs and RAs must require each individual to appear in person before a trusted agent who is responsible for verifying identity. The trusted agent must verify the identity of the individual using at least one form of government-issued photo identification.

### 5.3.3 Training and Skills Level

The CA must provide all personnel performing information verification duties with skills training that covers basic PKI knowledge, authentication, and vetting policies and procedures, common threats to the information verification process (including phishing and other social engineering tactics), and this CP. The CA must maintain records of such training and ensure that personnel entrusted with Certificate issuance and identity vetting duties maintain a skill level that enables them to perform such duties satisfactorily.

Employees and contractors authorized to approve Certificate issuance must maintain skill levels consistent with the CA's training and performance programs. The CA must document that each person possesses the skills required by a task before allowing the person to perform that task.

### 5.3.4 Retraining Frequency and Requirements

CAs and RAs must ensure that personnel maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles.

### 5.3.5 Job Rotation Frequency and Sequence

No stipulation.

### 5.3.6 Sanctions for Unauthorized Actions

CAs failing to comply with this CP, whether through negligence or malicious intent, may have action taken against them, including revocation of their license to use the NFC Forum OID in a Certificate.

### 5.3.7 Independent Contractor Requirements

CAs may delegate the performance of all or any part of a requirement of this CP to an RA, provided that the process employed by the CA fulfills all of the requirements of this CP. The CA must ensure that all RA personnel must comply with the training and background requirements in this CP. CAs remain responsible for all actions of an RA.

### 5.3.8 Documentation Supplied to Personnel

CAs and RAs must provide personnel in trusted roles with the documentation necessary to perform their duties.

## 5.4 Audit Logging Procedures

### 5.4.1 Types of Recorded Events

CA and RA systems must require identification and authentication at system logon. Important system actions must be logged to establish the accountability of the operators who initiate such actions.

CAs and RAs must enable all essential event auditing capabilities of its CA or RA applications in order to record all events related to the security of the CA or RA, including those listed in Table 3. A message from any source received by the CA or RA requesting an action related to the operational state of the CA is an auditable event. If an application cannot automatically record an event, the CA and RA must implement manual procedures to satisfy the requirements. For each event, the CA and RA must record the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. The CA must make all event records available to its auditors as proof of the CA's and RA's practices.

**Table 3: Types of Recorded Events**

| Auditable Event |
|---|
| **SECURITY AUDIT** |
| Any changes to the audit parameters, e.g., audit frequency, type of event audited |
| Any attempt to delete or modify the audit logs |
| **AUTHENTICATION TO SYSTEMS** |
| Successful and unsuccessful attempts to assume a role |
| The value of maximum number of authentication attempts is changed |
| The maximum number of authentication attempts is exceeded during user login |
| An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts |
| An administrator changes the type of authenticator, e.g., from a password to a biometric |
| **LOCAL DATA ENTRY** |
| All security-relevant data that is entered in the system |
| **REMOTE DATA ENTRY** |
| All security-relevant messages that are received by the system |
| **DATA EXPORT AND OUTPUT** |
| All successful and unsuccessful requests for confidential and security-relevant information |
| **KEY GENERATION** |
| Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys) |
| **PRIVATE KEY LOAD AND STORAGE** |
| The loading of Component Private Keys |

| |
|---|
| All access to certificate subject Private Keys retained within the CA for key recovery purposes |
| **TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE** |
| **SECRET KEY STORAGE** |
| The manual entry of secret keys used for authentication |
| **PRIVATE AND SECRET KEY EXPORT** |
| The export of private and secret keys (keys used for a single session or message are excluded) |
| **CERTIFICATE REGISTRATION** |
| All certificate requests, including issuance, re-key, renewal, and revocation |
| Certificate issuance |
| Verification activities |
| **CERTIFICATE REVOCATION** |
| All certificate revocation requests |
| **CERTIFICATE STATUS CHANGE APPROVAL OR REJECTION** |
| **CA CONFIGURATION** |
| Any security-relevant changes to the configuration of a CA system component |
| **ACCOUNT ADMINISTRATION** |
| Roles and users are added or deleted |
| The access control privileges of a user account or a role are modified |
| **CERTIFICATE PROFILE MANAGEMENT** |
| All changes to the certificate profile |
| **REVOCATION PROFILE MANAGEMENT** |
| All changes to the revocation profile |
| **CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT** |
| All changes to the certificate revocation list profile |
| Generation of CRL entries |
| **TIME STAMPING** |
| Clock synchronization |
| **MISCELLANEOUS** |
| Appointment of an individual to a Trusted Role |
| Designation of personnel for multi-party control |
| Installation of an Operating System |
| Installation of a PKI Application |
| Installation of Hardware Security Modules |

| |
|---|
| Removal of HSMs |
| Destruction of HSMs |
| System Startup |
| Logon attempts to PKI Application |
| Receipt of hardware / software |
| Attempts to set passwords |
| Attempts to modify passwords |
| Backup of the internal CA database |
| Restoration from backup of the internal CA database |
| File manipulation (e.g., creation, renaming, moving) |
| Posting of any material to a repository |
| Access to the internal CA database |
| All certificate compromise notification requests |
| Loading HSMs with Certificates |
| Shipment of HSMs |
| Zeroizing HSMs |
| Re-key of the Component |
| **CONFIGURATION CHANGES** |
| Hardware |
| Software |
| Operating System |
| Patches |
| Security Profiles |
| **PHYSICAL ACCESS / SITE SECURITY** |
| Personnel access to secure area housing CA components |
| Access to a CA component |
| Known or suspected violations of physical security |
| Firewall and router activities |
| **ANOMALIES** |
| System crashes and hardware failures |
| Software error conditions |
| Software check integrity failures |
| Receipt of improper messages and misrouted messages |

| |
|---|
| Network attacks (suspected or confirmed) |
| Equipment failure |
| Electrical power outages |
| Uninterruptible Power Supply (UPS) failure |
| Obvious and significant network service or access failures |
| Violations of a CP or CPS |
| Resetting Operating System clock |

### 5.4.2 Frequency of Processing Log

CA and RAs must review system logs, make system and file integrity checks, and make a vulnerability assessment at least every two months. CAs and RAs may use automated tools to scan for anomalies or specific conditions.

### 5.4.3 Retention Period for Audit Log

CAs and RAs must retain audit logs on-site until after they are reviewed.

### 5.4.4 Protection of Audit Log

CAs and RAs must implement procedures that protect archived data from destruction prior to the end of the audit log retention period. CAs and RAs must configure their systems and establish operational procedures to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. CAs and RAs must make records available to their independent auditors as proof of compliance with this CP.

### 5.4.5 Audit Log Backup Procedures

On at least a monthly basis, CAs and RAs must make backups of audit logs and audit log summaries, and send a copy of the audit log off-site.

### 5.4.6 Audit Collection System (internal vs. external)

CAs and RAs may use automatic audit processes, provided that they are invoked at system startup and end only at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, CAs and RAs should consider suspending Certificate operations until the problem is remedied.

### 5.4.7 Notification to Event-causing Subject

No stipulation.

### 5.4.8 Vulnerability Assessments

At least annually, CAs must perform routine risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. CAs must routinely assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements.

## 5.5 Records Archival

### 5.5.1 Types of Records Archived

CAs must archive information related to the issuance of Certificates under this CP, including CPS versions, contractual obligations, remediation of security and compromise events, destruction of a cryptographic module, appointment to a trusted role, and compliance reports.

### 5.5.2 Retention Period for Archive

CAs must retain archived data for at least 7.5 years.

### 5.5.3 Protection of Archive

CAs must store archived records at a secure off-site location in a manner that prevents unauthorized modification, substitution, or destruction.

### 5.5.4 Archive Backup Procedures

CAs must describe how records are backed up and managed in its CPS or in a referenced document.

### 5.5.5 Requirements for Time-stamping of Records

CAs must time-stamp archive records as they are created. CAs must synchronize its system time at least every eight hours using a real-time value traceable to a recognized UTC(k) laboratory or National Measurement Institute.

### 5.5.6 Archive Collection System (internal or external)

CAs must collect archive information internally.

### 5.5.7 Procedures to Obtain and Verify Archive Information

CA may archive data manually or automatically.

## 5.6 Key Changeover

CAs should periodically change Private Keys in a manner set forth in its CPS that prevents downtime in the CA's operation. After key changeover, the Issuer CA must sign certificates using only the new key, continue to protect its old Private Keys, and make the old certificate available to verify signatures until all of the certificates signed with the Private Key have expired.

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Incident and Compromise Handling Procedures

CAs must develop and implement procedures to be followed in the event of a serious security incident or system compromise. CAs must review, test, and update these procedures annually.

### 5.7.2 Computing Resources, Software, and/or Data Are Corrupted

A CA must make regular back-up copies of its Private Keys and store them in a secure off-site location. If a disaster causes the CA's operations to become inoperative, the CA must, after ensuring the integrity of the CA systems, re-initiate its operations on replacement hardware using backup copies of its software, data, and Private Keys at a secure facility. The CA must give priority to reestablishing the generation of certificate status information.

### 5.7.3 Entity Private Key Compromise Procedures

CAs suspecting a CA Private Key compromise must immediately assess the situation, determine the degree and scope of the incident, and take appropriate action. The CA must notify interested parties, including the NFC Forum, and make available information about which Certificates are affected, unless providing this information will breach the privacy of a Subscriber or compromise an on-going investigation or the security of the CA's services.

### 5.7.4 Business Continuity Capabilities after a Disaster

The CA's disaster recovery plan must follow a process designed to protect certificate status servers from a disaster involving the CA's primary facility. The CA's business continuity and disaster recovery procedures must be designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, and plan for security compromise or business failure. The CA is not required to publicly disclose its business continuity plans but must make the business continuity plan and security plan available to the CA's auditors upon request. The CA must annually test, review, and update these procedures.

The business continuity plan MUST include:

- The conditions for activating the plan
- Emergency procedures
- Fallback procedures
- Resumption procedures,
- A maintenance schedule for the plan
- Awareness and education requirements
- The responsibilities of the individuals
- Recovery time objective (RTO)
- Regular testing of contingency plans
- The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location
- What constitutes an acceptable system outage and recovery time

- How frequently backup copies of essential business information and software are taken
- The distance of recovery facilities to the CA's main site
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site

## 5.8 CA or RA Termination

If a CA's operations are terminated, the CA must provide notice to interested parties, including the NFC Forum, and transfer its responsibilities and records to successor entities. The CA may allow a successor to re-issue certificates if the successor has all relevant permissions to do so and has operations that are at least as secure as the CA's.

# 6 Technical Security Controls

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key Pair Generation

All keys must be generated using a FIPS-approved method or equivalent international standard.

CAs must generate their cryptographic keying material on a FIPS 140 Level 3 validated cryptographic module using multiple individuals acting in trusted roles. When generating key material, the CA must create auditable evidence to show that the CA enforced role separation and followed its key generation process.

For CA key pairs created after adoption of this document by the NFC Forum that are either (i) used as root CA key pairs or (ii) key pairs generated for a subordinate CA, the CA must:

- Prepare and follow a script for generating the key pair
- Have an independent auditor witness the key pair generation process or record a video of the entire key pair generation process
- Have an independent auditor issue a statement that the CA followed its key ceremony during its key pair generation

Subscribers who generate their own keys shall use a FIPS-approved method using a [FIPS_140_2] Level 2 (or equivalent) cryptographic module, except for anNFC Forum device where keys are generated in the application itself. In this case, the host-based systems will take commercially reasonable precautions to protect keying material.

### 6.1.2 Private Key Delivery to Subscriber

Subscribers must protect private keys in a [FIPS_140_2] Level 2 (or equivalent) cryptographic module, except for NFC Forum device where keys are generated in the application itself. CAs MUST verify a Subscriber's compliance with this requirement using one of the following:

- The CA ships a suitable hardware cryptographic module, with a preinstalled key pair, in the form of a smartcard or USB device or similar
- The CA's generates and installs the Certificate and Private Key on a [FIPS_140_2] Level 2 device
- The Subscriber provides the CA a report from an independent auditor that specifically states that the Subscriber's operating environment achieves a level of security at least equivalent to that of [FIPS_140_2] Level 2
- Any other method that provides similar reasonable assurances that the Private Keys are installed on a [FIPS_140_2] Level 2 cryptographic module.

Parties other than the Subscriber may not archive the Subscriber's Private Key. If the CA or RA becomes aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA must revoke all certificates that include the Public Key corresponding to the communicated Private Key.

### 6.1.3 Public Key Delivery to Certificate Issuer

Subscribers must deliver their Public Keys to the CA in a secure fashion and in a manner that binds the Subscriber's verified identity to the Public Key. The certificate request process must ensure that the Applicant possesses the Private Key associated with the Public Key presented for certification.

For ECQV certificate issuance, the certificate request process must ensure that the Applicant is authorized to name the certificate request in a secure fashion and in a manner that binds the Subscriber's verified identity to the public key.

### 6.1.4 CA Public Key Delivery to Relying Parties

CAs may provide their public keys to Relying Parties in a secure fashion and in a manner that precludes substitution attacks, such as (i) part of the certificate validation or path discovery policy file, (ii) trust anchors in commercial browsers and operating system root store, and/or (iii) roots signed by other CAs.

### 6.1.5 Key Sizes

CA certificates, intermediate certificates, and signed CRLs must use keys and a hash algorithm that meets at least one of the following requirements:

- 2048-bit RSA Key with Secure Hash Algorithm Version 2 (SHA-256)
- 256-bit ECDSA Key with Secure Hash Algorithm Version 2 (SHA-256)
- 256-bit ECQV Key with Secure Hash Algorithm Version 2 (SHA-256)

The CA may use higher bit keys in their sole discretion. End-entity certificates must use one of the signatures outlined in [SIGNATURE] and must also use one of the hash algorithms outlined in [SIGNATURE].

This specification defines the following algorithm object identifiers. Each object identifier indicates an algorithm, elliptic curve, and hash function, obviating the need for a separate algorithm parameters field.

**Table 4: Algorithm Object Identifiers**

| Object Identifier | Description |
|---|---|
| 2.16.840.1.114513.1.0 | ecdsa-with-sha256-secp192r1 |
| 2.16.840.1.114513.1.1 | ecdsa-with-sha256-secp224r1 |
| 2.16.840.1.114513.1.2 | ecdsa-with-sha256-sect233k1 |
| 2.16.840.1.114513.1.3 | ecdsa-with-sha256- sect233r1 |
| 2.16.840.1.114513.1.4 | ecqv-with-sha256-secp192r1 |
| 2.16.840.1.114513.1.5 | ecqv-with-sha256-secp224r1 |
| 2.16.840.1.114513.1.6 | ecqv-with-sha256-sect233k1 |
| 2.16.840.1.114513.1.7 | ecqv-with-sha256-sect233r1 |
| 2.16.840.1.114513.1.8 | rsa-with-sha256 |
| 2.16.840.1.114513.1.9 | ecdsa-with-sha256-secp256r1 |

| Object Identifier | Description |
|---|---|
| 2.16.840.1.114513.1.10 | ecqv-with-sha256-secp256r1 |

With these algorithm identifiers, the public key value in a certificate and the certificate digital signature or public key reconstruction value are represented according to the rules in Appendix A in [SIGNATURE].

### 6.1.6 Public Key Parameters Generation and Quality Checking

CAs must generate Public Key parameters for signature algorithms and perform parameter quality checking in accordance with FIPS 186.

### 6.1.7 Key Usage Purposes

CAs must set the KeyUsage bit and include the NFC Forum OID in the extended key usage extension to technically limit the certificate's functionality in X.509v3-compliant software.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic Module Standards and Controls

CAs and all systems that sign CRLs must use cryptographic hardware modules validated to [FIPS_140_2] Level 3 and International [Common_Criteria] (CC) Information Technology Security Evaluation Assurance Level (EAL) 14169 EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) in the European Union (EU).

### 6.2.2 Private Key (n out of m) Multi-person Control

CAs must ensure that multiple trusted personnel are required to act in order to access and use the CA's Private Keys, including any Private Key backups.

### 6.2.3 Private Key Escrow

Neither CAs nor Subscribers may escrow their signature keys.

### 6.2.4 Private Key Backup

A CA must backup its CA and certificate status Private Keys under multi-person control, and store the backup off site.

### 6.2.5 Private Key Archival

CAs must not archive Private Keys used for RTD Signatures.

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. CAs, RAs, and Subscribers may not permit their Private Keys to exist in plain text outside of the cryptographic module. CAs, RAs, and Subscribers may export Private Keys from the cryptographic module to perform key backup procedures, provided that the private key is encrypted and protected when transported between cryptographic modules.

### 6.2.7 Private Key Storage on Cryptographic Module

CAs must store Private Keys on a cryptographic module that has been evaluated to at least [FIPS_140_2] Level 3 and EAL 4+. Subscribers must store Private Keys on a cryptographic module that has been evaluated to at least [FIPS_140_2] Level 2 (or the equivalent).

### 6.2.8 Method of Activating Private Key

CAs and Subscribers must activate Private Keys in accordance with the specifications of the cryptographic module manufacturer.

### 6.2.9 Method of Deactivating Private Key

CAs and Subscribers must deactivate Private Keys and store cryptographic modules in secure containers when not in use.

### 6.2.10 Method of Destroying Private Key

CAs must use individuals in trusted roles to destroy CA, RA, and status server Private Keys when they are no longer needed. Subscribers must destroy their Private Keys when the corresponding certificate is revoked or expired or if the Private Key is no longer needed. Private Key destruction does not require destruction of the hardware containing the Private Key.

### 6.2.11 Cryptographic Module Rating

See Section 6.2.1.

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public Key Archival

CAs must archive a copy of each Public Key.

### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

CAs may issue root certificates with a maximum validity period of 25 years and intermediate certificates with a maximum validity period of 15 years. End Entity certificates should have a maximum validity period of three years.

## 6.4 Activation Data

### 6.4.1 Activation Data Generation and Installation

CAs must generate activation data with sufficient strength to protect their Private Keys.

### 6.4.2 Activation Data Protection

CA and Subscribers must protect data used to unlock private keys from disclosure by using a combination of cryptographic and physical access control mechanisms.

### 6.4.3 Other Aspects of Activation Data

No stipulation.

## 6.5 Computer Security Controls

### 6.5.1 Specific Computer Security Technical Requirements

CAs and RAs must configure systems, including any remote workstations, to:

- Authenticate the identity of users before permitting access to the system or applications
- Manage the privileges of users, and limit users to their assigned roles
- Generate and archive audit records for all transactions
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

CAs must authenticate and protect all communications between a trusted role and its CA system. CAs must enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

### 6.5.2 Computer Security Rating

No stipulation.

## 6.6 Life Cycle Technical Controls

### 6.6.1 System Development Controls

CAs must take proper care to prevent malicious software from being loaded onto the CA equipment. CAs should scan all hardware and software for malicious code on first use and periodically thereafter. CAs should not install any software on its CA systems that are not part of the CA's operations.

### 6.6.2 Security Management Controls

CAs must establish formal mechanisms to document, control, monitor, and maintain the installation and configuration of its CA systems, including any modifications or upgrades. A CA's change control processes must include procedures to detect unauthorized modification to the CA's systems and firewalls, routers, software, and other access controls.

### 6.6.3 Life Cycle Security Controls

No stipulation.

## 6.7 Network Security Controls

CAs must develop, implement, and maintain a comprehensive security program designed to:

- Protect the confidentiality, integrity, and availability of certificate data and Certificate processes
- Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of certificate data and Certificate processes
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any certificate data or certificate processes
- Protect against accidental loss or destruction of, or damage to, any certificate data or certificate processes
- Comply with all other security requirements applicable to the CA by law

CAs must document and control the configurations of its systems, including any upgrades or modifications made. CAs must implement a process for detecting unauthorized modifications to its hardware or software and for installing and maintaining its systems. CAs and RAs must implement appropriate network security controls, including turning off any unused network ports and services and only using network software that is necessary for the proper functioning of the CA and RA systems.

## 6.8 Time-stamping

CAs and RAs must ensure that the accuracy of clocks used for time-stamping are within three minutes. Electronic of manual procedures may be used to maintain system time. Clock adjustments are auditable events.

# 7 Certificate, CRL, and OCSP Profiles

## 7.1 Certificate Profile

### 7.1.1 Version Number(s)

CAs may issue certificates that comply with the profiles listed in Appendix A or Appendix B in [SIGNATURE].

### 7.1.2 Certificate Extensions

CAs must use certificate extensions in accordance with Appendix A or Appendix B in [SIGNATURE].

### 7.1.3 Algorithm Object Identifiers

Refer to Section 6 and Appendix A or Appendix B in [SIGNATURE].

### 7.1.4 Name Forms

As shown in Appendix A or Appendix B in [SIGNATURE], CAs must limit distinguished names to the [RFC5280] mandatory attributes plus others in common use. This includes country, organization, organizational unit, distinguished name qualifier, state or province name, common name, serial number, locality, and domain component. The organization name, locality / state / province name, and country must be included. Only one of each may be present with no more than four total attributes, and no multi-level names may be used. Included attributes may only include verified information.

**A. Organization**

This attribute must be present and must contain either the name of the subject device or a name of the subject as verified under Section 3.2.2 or Section 3.2.3, such as an assumed name, legal name, or individual's name. A CA may abbreviate the organization prefixes or suffixes using abbreviations common in the subject's jurisdiction of operation. The CA must not use abbreviations if it would make the name misleading to a relying party.

**B. Subject Common Name Field**

If present, this attribute must contain name of the subject as either verified under Section 3.2.2or Section 3.2.3 or provided by the sponsor as an identifier of the subject device.

**C. Domain Component**

If present in a Certificate, the Domain Component field must include all components of a registered domain name verified in accordance with Section 3.2.2 in ordered sequence, with the most significant component, closest to the root of the namespace, written last.

**D. Registered ID Attribute**

If present, this attribute must contain the registration number or date of formation of the entity verified under Section 3.2.2.

**E. Address Attributes**

The country is required, and either the state, province name, or locality attribute is required. All included address information must be verified in accordance with Section 3.2.2or Section 3.2.3.

**F. Other Attributes**

All other optional attributes, when present, must contain information verified by the CA. Metadata such as '.', '-', and ' ' characters, and/or any other indication that the field is empty, absent or incomplete, must not be used.

### 7.1.5 Name Constraints

No stipulation.

### 7.1.6 Certificate Policy Object Identifier

CAs issuing a certificate containing the NFC Forum OID are representing that the certificate's issuance and contents conform to this policy. Each Certificate issued to a Subscriber must contain a policy identifier that indicates which CA policy statement relates to that Certificate and asserts the CA's adherence to and compliance with this CP.

### 7.1.7 Usage of Policy Constraints Extension

No stipulation.

### 7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

## 7.2 CRL Profile

### 7.2.1 Version number(s)

CAs must issue version 2 CRLs that conform to [RFC5280].

### 7.2.2 CRL and CRL Entry Extensions

CRLs should conform to [RFC5280].

## 7.3 OCSP Profile

### 7.3.1 Version Number(s)

Because signature verification is often required while a relying party is offline, this policy recommends that platform developers verify the validity of a certificate using CRLs that are regularly downloaded to the user agents instead of through OCSP responses.

### 7.3.2 OCSP Extensions

No stipulation.

# 8 Compliance Audit and Other Assessments

## 8.1 Frequency or Circumstances of Assessment

On at least an annual basis, CAs must retain an independent auditor to assess the CA's compliance with this CP and its CPS. This audit must cover all CAs, RAs, and each status server that is specified in a certificate issued by the CA.

## 8.2 Identity/Qualifications of Assessor

CAs must use an auditor that meets the following qualifications:

- **Qualifications and experience**: Auditing must be the auditor's primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential.
- **Expertise**: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with PKI, certification systems, and Internet security issues.
- **Rules and standards**: The auditor must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.
- **Reputation**: The auditor must have a reputation for conducting its auditing business competently and correctly.
- **Insurance**: Auditors must maintain Professional Liability/Errors and Omissions Insurance, with policy limits of at least $1 million in coverage.

## 8.3 Assessor's Relationship to Assessed Entity

CAs must utilize independent auditors that do not have a financial interest, business relationship, or course any dealings that could foreseeably create a significant bias for the CA.

## 8.4 Topics Covered by Assessment

The audit must conform to industry standards, cover the CA's compliance with its business practices disclosure, and evaluate the integrity of the CA's PKI operations. Audits must cover all CA obligations under these guidelines regardless of whether they are performed directly by the CA or a RA. Unless separate audit criteria are developed and approved by the NFC Forum, the following audits are considered sufficient to show a CA's compliance with this policy:

- WebTrust Program for CAs audit and WebTrust EV Program audit
- ETSI TS 102 042 v2.1.1 audit

If the CA is a Government Entity, an audit of the CA by the appropriate internal government auditing agency is acceptable in lieu of the audits specified above, provided that such internal government auditing agency publicly certifies in writing that its audit addresses the criteria specified in one of the above audit schemes and certifies that the government CA has successfully passed the audit.

## 8.5 Actions Taken as a Result of Deficiency

If an audit reports a material non-compliance with applicable law, this CP, the CA's CPS, or any other contractual obligations related to the CA's services, then (1) the auditor must document the discrepancy, (2) the auditor must promptly notify the CA and NFC Forum, and (3) the CA must develop and submit to the NFC Forum a plan to cure the non-compliance. The NFC Forum may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected certificates.

## 8.6 Communication of Results

CAs must submit the results of its compliance audit to the NFC Forum on an annual basis as evidence of the CA's compliance with this CPS. CAs should make its audit report publicly available no later than three months after the end of the audit period. If there is a delay greater than three months and if requested by the NFC Forum, the CA must provide an explanatory letter signed by its auditor.

## 8.7 Self-Audits

CAs must perform regular internal audits of their and their RAs' operations, personnel, and compliance with this CP using a randomly selected sample of at least six percent of the certificates issued since the last internal audit. Each CA must review the practices and procedures used by its RAs and subcontractors to ensure that the RA and subcontractor are in compliance with this CP.

# 9 Other Business and Legal Matters

## 9.1 Fees

### 9.1.1 Certificate Issuance or Renewal Fees

CAs may charge fees for certificate issuance and renewal.

### 9.1.2 Certificate Access Fees

CAs may charge fees for access to their databases of certificates.

### 9.1.3 Revocation or Status Information Access Fees

CAs must provide freely accessible certificate status information through CRLs.

### 9.1.4 Fees for Other Services

No stipulation.

### 9.1.5 Refund Policy

No stipulation.

## 9.2 Financial Responsibility

### 9.2.1 Insurance Coverage

CA must maintain insurance with policy limits of at least five million US dollars in coverage that covers (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining a Certificate, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright and trademark infringement), and invasion of privacy and advertising injury. Insurance must be with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).

A CA may self-insure provided that it has at least five hundred million US dollars in liquid assets based on audited financial statements in the past twelve months, and a quick ratio (ratio of liquid assets to current liabilities) of not less than 1.0.

### 9.2.2 Other Assets

No stipulation.

### 9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

## 9.3 Confidentiality of Business Information

### 9.3.1 Scope of Confidential Information

CAs should specify what constitutes confidential information in its CPS.

### 9.3.2 Information Not Within the Scope of Confidential Information

CAs may treat any information not listed as confidential as public information.

### 9.3.3 Responsibility to Protect Confidential Information

CAs must contractually obligate employees, agents, and contractors to protect confidential information. CAs must provide training to employees on how to handle confidential information.

## 9.4 Privacy of Personal Information

### 9.4.1 Privacy Plan

CAs must create and follow a privacy policy that specifies how the CA handles personal information.

### 9.4.2 Information Treated as Private

CAs must create a data protection policy that specifies that the information is treated as private. Information classified as private must be protected using a reasonable degree of care and appropriate safeguards.

### 9.4.3 Information Not Deemed Private

Private information does not include certificates or their contents.

### 9.4.4 Responsibility to Protect Private Information

CAs must securely store and protect private information.

### 9.4.5 Notice and Consent to Use Private Information

No stipulation.

### 9.4.6 Disclosure Pursuant to Judicial or Administrative Process

CAs may disclose private information, without notice, when required to do so by law or regulation.

### 9.4.7 Other Information Disclosure Circumstances

No stipulation.

## 9.5 Intellectual Property Rights

CAs should not knowingly violate the intellectual property rights of any third party.

## 9.6 Representations and Warranties

### 9.6.1 CA Representations and Warranties

CAs represent to the NFC Forum, Subscribers, and Relying Parties that they comply, in all material aspects, with this CP, their CPS, and all applicable laws and regulations.

### 9.6.2 RA Representations and Warranties

At a minimum, CAs must require RAs operating on their behalf to represent that they have followed this CP and the relevant CPS when participating in the issuance and management of certificates.

### 9.6.3 Subscriber Representations and Warranties

CAs must impose the following contractual representations on each Subscriber:

- **Accuracy of Information**: The Subscriber will provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA.
- **Protection of Private Key**: The Subscriber will take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token).
- **Acceptance of Certificate**: The Subscriber will review and verify the Certificate contents for accuracy.
- **Use of the Certificate**: The Subscriber will (a) not knowingly create Signature Records for Suspect Messages, (b) only use the Certificate to create signatures that comply with these requirements, and (c) solely use the Certificate in compliance with all applicable laws and for authorized company business.
- **Reporting and Revocation**: The Subscriber will promptly cease using a Certificate and promptly request the CA to revoke the Certificate in the event that (a) there is evidence that the certificate was used to sign Suspect Messages; (b) any information in the Certificate is, or becomes, incorrect or inaccurate; or (c) there is any actual or suspected misuse or compromise of either the key activation data or the Subscriber's Private Key associated with the Public Key included in the Certificate.
- **Termination of Use of Certificate**: The Subscriber will promptly cease all use of the Certificate upon revocation of that Certificate.
- **Acknowledgment and Acceptance**: The CA is entitled to revoke the Certificate immediately if the applicant violates the terms of the subscriber agreement or if the CA discovers that the Certificate is being used to enable criminal or malicious activities such as phishing attacks, fraud, Suspect Messages, or the distribution of malware.
- **Revocation**: If the Certificate holder becomes aware (by whatever means) that it has signed a Suspect Message, then the Subscriber will immediately inform the issuing CA. If the Certificate holder's private key or private key activation data is compromised or believed to be compromised, the Subscriber will contact the CA immediately and request that the certificate be revoked.

### 9.6.4 Relying Party Representations and Warranties

No stipulation.

### 9.6.5 Representations and Warranties of Other Participants

No stipulation.

## 9.7 Disclaimers of Warranties

Your use of this CP is subject to the terms found herein.

THIS CP MAY CHANGE OR NOT BE ADOPTED IN FINAL FORM BY NFC FORUM. NFC FORUM DOES NOT KNOW WHETHER ALL PATENT CLAIMS THAT READ UPON THE CP WILL BE AVAILABLE ON REASONABLE AND NON-DISCRIMINATORY TERMS, OR AT ALL. ANY USE OR IMPLEMENTATION OF THE SPECIFICATION BY YOU IS AT YOUR SOLE RISK. THIS LICENSE IS OF LIMITED DURATION, AS FURTHER PROVIDED BELOW.

THIS CP IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COMPLETENESS AND NONINFRINGEMENT OF THIRD-PARTY RIGHTS. IN NO EVENT SHALL NFC FORUM, ITS MEMBERS, OR ITS CONTRIBUTORS BE LIABLE FOR ANY CLAIM, OR ANY DIRECT, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS CP.

Without limiting the generality of the above, NO ASSURANCE IS GIVEN BY NFC FORUM THAT THIS CP WILL BE ADOPTED IN ITS CURRENT FORM, OR AT ALL. NFC FORUM MAKES NO REPRESENTATION THAT ITS MEMBERS WILL MAKE ANY PATENT CLAIMS OR OTHER INTELLECTUAL PROPERTY OWNED BY THEM THAT WOULD BE INFRINGED BY AN IMPLEMENTATION OF THIS CP AVAILABLE TO YOU ON REASONABLE AND NON-DISCRIMINATORY TERMS, OR AT ALL.

## 9.8 Limitations of liability

CAs may limit their liability to any extent not otherwise prohibited by this CP, provided that the CA remains responsible for complying with this CP and the CA’s CPS.

## 9.9 Indemnities

### 9.9.1 Indemnification by CAs

CAs agree to indemnify, defend, and hold harmless the NFC Forum and its officers, directors, employees, and agents (each, an "Indemnified Party") from all losses, costs, damages, claims, and other expenses (including reasonable attorneys' fees) arising out of any claim by any third party in connection with the use of this CP or participation in the NFC Forum by CA, its affiliates, or its end users, including, without limitation, claims asserting that any process, product, or service infringes any intellectual property rights anywhere in the world of such third party.

### 9.9.2 Indemnification by Subscribers

CAs are free to set their own indemnification rules with respect to Subscribers, provided that all Subscribers contractually agree to indemnify, defend, and hold harmless the NFC Forum and its officers, directors, employees, and agents from all losses, costs, damages, claims, and other expenses (including reasonable attorneys' fees) arising out of any claim by any third party in connection with the use of a certificate issued under this CP, including, without limitation, claims asserting that any process, product, or service infringes any intellectual property rights anywhere in the world of such third party.

### 9.9.3 Indemnification by Relying Parties

CAs are free to set their own indemnification rules with respect to relying parties, provided that all relying parties contractually agree to indemnify, defend, and hold harmless the NFC Forum and its officers, directors, employees, and agents from all losses, costs, damages, claims, and other expenses (including reasonable attorneys' fees) arising out of any claim by any third party in connection with the use of a certificate issued under this CP, including, without limitation, claims asserting that any process, product, or service infringes any intellectual property rights anywhere in the world of such third party.

## 9.10 Term and Termination

### 9.10.1 Term

This CP and any amendments are effective when approved by the NFC Forum and remain in effect until replaced with a newer version.

### 9.10.2 Termination

This CP and any amendments remain in effect until replaced by a newer version.

### 9.10.3 Effect of Termination and Survival

The NFC Forum will communicate the conditions and effect of this CP's termination by notifying participating CAs, generally by posting a notice of the termination on the NFC Forum's website.

## 9.11 Individual Notices and Communications

NFC FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE, OR MAKE PUBLIC ANY MEMBER OR THIRD-PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THIS CP IN ITS CURRENT OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THIS CP, NFC FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

All notices to NFC Forum must be in writing. Notices are effective five days from deposit in the mail. NFC Forum sends notices to participants by posting the notice on its website.

## 9.12 Amendments

### 9.12.1 Procedure for Amendment

The NFC Forum determines what amendments should be made to this CP. Amendments are made by posting an updated version of the CP to the online repository. Controls are in place to reasonably ensure that this CP is not amended and published without the prior authorization of the NFC Forum.

### 9.12.2 Notification Mechanism and Period

The NFC Forum will post notice on its website of any proposed significant revisions to this CP. Although the NFC Forum may include a final date for receipt of comments and the proposed effective date, NFC Forum is not required to have a fixed notice-and-comment period. CAs may make non-material changes to their CPSs without notice to the NFC Forum if the change will not violate the requirements found in this CP.

### 9.12.3 Circumstances under which OID Must Be Changed

If the NFC Forum determines an amendment necessitates a change in an OID, then the revised version of this CP will also contain a revised OID. Otherwise, amendments do not require an OID change.

## 9.13 Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution, a party must notify NFC Forum of the dispute with a view to seek dispute resolution.

## 9.14 Governing Law

This CP is construed and interpreted under the internal laws of the United States and the Commonwealth of Massachusetts, without giving effect to its principles of conflict of law.

## 9.15 Compliance with applicable law

This CP is subject to all applicable laws and regulations.

## 9.16 Miscellaneous Provisions

### 9.16.1 Entire Agreement

CAs must contractually obligate each RA involved in certificate issuance to comply with this CP and applicable industry guidelines. CAs shall contractually obligate parties using products and services issued under this CP, such as Subscribers and Relying Parties, to the relevant provisions herein. This CP does not give any third party rights under such agreements.

### 9.16.2 Assignment

Entities operating under this CP may not assign their rights or obligations without first notifying the NFC Forum.

### 9.16.3 Severability

If a provision of this CP is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP will remain valid and enforceable.

### 9.16.4 Enforcement (attorneys' fees and waiver of rights)

NFC Forum may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. NFC Forum’s failure to enforce a provision of this CP does not waive NFC Forum’s right to enforce the same provision later or right to enforce any other provision of this CP. To be effective, waivers must be in writing and signed by NFC Forum.

### 9.16.5 Force Majeure

NFC Forum is not liable for a delay or failure to perform an obligation under this CP.

## 9.17 Other Provisions

No stipulation.

# A. Revision History

The following table outlines the revision history of Signature RTD Certificate Policy.

**Table 5: Revision History**

| Document Name | Revision and Release Date | Status | Change Notice | Supersedes |
|---|---|---|---|---|
| Signature RTD Certificate Policy | Version 1.0, October 3, 2014 | Approved | | |