CENTER for MEDICAL INTEROPERABILITY

The Center for Medical Interoperability Document
C4MI Trust Platform Certificate Policy

C4MI-TD-TPCP-D04-2020-04-22

Draft

Notice

This document is the result of a cooperative effort undertaken at the direction of the Center for Medical Interoperability™ (C4MI) for the benefit of the healthcare industry and its customers. You may download, copy, distribute, and reference the documents herein only for the purpose of developing products or services in accordance with such documents, and educational use. Except as granted by C4MI in a separate written license agreement, no license is granted to modify the documents herein (except via the Engineering Change process), or to use, copy, modify or distribute the documents for any other purpose.

This document may contain references to other documents not owned or controlled by C4MI. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document. To the extent this document contains or refers to documents of third parties, you agree to abide by the terms of any licenses associated with such third-party documents, including open source licenses, if any.

DISCLAIMER

This document is furnished on an "AS IS" basis and neither C4MI nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and C4MI and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

C4MI reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by C4MI or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from C4MI, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Table of Contents

Tables

Document Status Sheet

Document Control Identifier:	C4MI-TD-TPCP
Document Title:	C4MI Trust Platform Certificate Policy
Revision History:	D04
Date:	04/22/2020
Status:	Draft
Distribution Restrictions:	Public

Key to Document Status Codes

Work in Progress	An incomplete document designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document considered largely complete but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A public document that has undergone Member and Technology Supplier review, cross-vendor interoperability, and is for Certification testing if applicable. Issued Specifications are subject to the Engineering Change Process.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through C4MI.

1 Scope

1.1 Introduction and Purpose

This document defines the certificate policy for the Public Key Infrastructure (PKI) used within the Center for Medical Interoperability (C4MI) ecosystem. The C4MI certificates are the basis for a number of security services including authentication, confidentiality, integrity, and non-repudiation. In order for a certificate to be in compliance with the C4MI specifications, it SHALL comply with this Certificate Policy. This Policy assumes that the reader is generally familiar with Digital Signatures, PKIs, and the C4MI specifications.

1.1.1 Certificate Policy (CP)

This Certificate Policy is consistent with the Internet X.509 PKI Certificate Policy and Certification Practices Framework [IETF-RFC3647]. It governs the certificate PKI operations of components by all individuals and entities within the PKI (collectively, "PKI Participants"). It provides the minimum requirements that PKI Participants are required to meet when issuing and managing Certification Authorities (CAs), digital certificates, and private keys. In addition, it informs potential Relying Parties about what they need to know and SHALL abide by prior to relying on issued certificates.

This CP also defines the terms and conditions under which the CAs operate to issue certificates. Where "operate" includes certificate management (i.e., approve, issue, and revoke) of issued certificates and "issue" refers to the process of digitally signing with the private key associated with its authority certificate a structured digital object conforming to the X.509, version 3 certificate format.

1.1.2 Role of the CP

The CP describes the overall business, legal, and technical infrastructure of the PKI. More specifically, it describes, among other things:

- Appropriate applications for, and the assurance levels associated with the PKI certificates
- Obligations of Certification Authorities (CAs)
- Minimum requirements for audit and related security and practices reviews
- Methods to confirm the identity of Certificate Applicants
- Operational procedures for certificate lifecycle services: certificate application, issuance, acceptance, revocation, and renewal
- Operational security procedures for audit logging, records retention, and disaster recovery
- Physical, personnel, key management, and logical security

- Certificate Profile and Certificate Revocation List content

The CP is an integral part of the C4MI PKI documentation and sets the minimum standards for governing, administering, and operating the PKI. Ancillary security and operational documents may supplement the CP in setting more detailed requirements. Additionally, each C4MI PKI CA is governed by a Certification Practice Statement(s) (CPS), which describes how the applicable CP requirements are met by that particular CA. CAs operating in the C4MI PKI SHALL draft, implement, and maintain a CPS. The CPS SHALL be reviewed and updated when there are changes made to the CP.

1.1.3 Assurance level

The C4MI digital certificates provide assurances that the certificate Subscriber's distinguished name is unique and unambiguous within the C4MI CA's domain, and the identity of the Subscriber's organization is based on a comparison of information submitted by the Subscriber against information in business records or databases. These certificates can be used for digital signatures, encryption, and authentication for proof of identity of components that contain certificates and are compliant with the C4MI specifications and this CP.

1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words, borrowed from [IETF-RFC2119] are:

"SHALL"	This word means that the item is an absolute requirement of this specification.
"SHALL NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 References

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

All references are subject to revision, and parties to agreements based on this specification are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

[CMI-DOC-TD] *The Center for Medical Interoperability Document: Terms and Definitions,* CMI-DOC-TD-D02-2019-05-31.
Available:
https://medicalinteroperability.org/specifications/d02/

[IETF-RFC2119] *Key words for use in RFCs to Indicate Requirement Levels,* RFC2119, March 1997.
Available: https://tools.ietf.org/html/rfc2119

[IETF-RFC2560] *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,* RFC2560, June 1999.
Available: https://tools.ietf.org/html/rfc2560

[IETF-RFC3647] *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,* RFC3647, November 2003.
Available: https://tools.ietf.org/html/rfc3647

[IETF-RFC5019] *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments,* RFC5019, September 2007.
Available: https://tools.ietf.org/html/rfc5019

[IETF-RFC5280] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* RFC5280, May 2008.
Available: https://tools.ietf.org/html/rfc5280

[FIPS-140-2] *Security Requirements for Cryptographic Modules,* FIPS 140-2, May 2001.
Available: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[ITU-T-X.501] *Information technology – Open Systems Interconnection – The Directory: Models*
Available: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.501

[ITU-T-X.500] X.500 : Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services
Available: https://www.itu.int/rec/T-REC-X.500-201910-P/en

[IETF-RFC2986] *PKCS #10: Certification Request Syntax Specification Version 1.7,* RFC2986, November 2000.
Available: https://tools.ietf.org/html/rfc2986

[IETF-RFC5208] *Public-Key Cryptography Standards (PKCS) #8: Private-Key Information Syntax Specification Version 1.2,* RFC5208, May 2008.
Available: https://tools.ietf.org/html/rfc5208

[IETF-RFC7292] PKCS #12: Personal Information Exchange Syntax v1.1, RFC7292, July 2014.
Available: https://tools.ietf.org/html/rfc7292

[C4MI-TD-TPPCH] *Trust Platform PKI Certificate Hierarchy.* C4MI-TD-TPPCH-D01 (not yet released)
Available:

[CMI-SP-TP-IST] C4MI Trust Platform Identity and Secure Transport Requirements
Available:
https://center4mi.jamacloud.com/perspective.req?projectId=126&docId=55193

[CMI-SP-F-ID] *Center for Medical Interoperability Specification: Identity,* CMI-SP-F-ID-D02-2019-05-31.
Available: https://medicalinteroperability.org/specifications

[NIST-VD] *National Vulnerability Database*
Available: https://nvd.nist.gov/

[WebTrust-CA] WebTrust Principles and Criteria for Certification Authorities
Available: http://www.webtrust.org/principles-and-criteria/docs/item85228.pdf

2.2 Informative References

This specification uses the following informative reference:

[CMI-TR-OVERVIEW] *Center for Medical Interoperability Specification: Foundational & Clinical Data Interoperability Efforts Overview,* CMI-TR-OVERVIEW-D02-2019-05-31.
Available: https://medicalinteroperability.org/specifications

3 Terms and Definitions

This specification uses the terms and definitions in [CMI-DOC-TD]:

Audit Requirements Guide	A document that sets forth the security and audit requirements and practices for CAs.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Validity Period, contains a Certificate serial number, and is digitally signed by the CA that issued the certificate.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing a Subscriber Certificate and one or more CA Certificates, which terminates in a root Certificate.
Control Objectives	Criteria that an entity SHALL meet in order to satisfy a Compliance Audit.
Certificate Policy (CP)	The principal statement of policy governing the PKI.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued.
Certificate Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the PKI.
Certificate Practice Statement (CPS)	A statement of the practices that a CA employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates.
Certificate Requesting Account (CRA)	The online portal to assist Certificate Applicants in requesting Certificates.
Compliance Audit	A periodic audit that a CA system undergoes to determine its conformance with PKI requirements that apply to it.

Compromise	A violation of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information has occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
End-entity Certificate	A non-CA certificate of the PKI chain installed in C4MI connected components, applications, etc.
Elliptic Curve Cryptography (ECC)	A public-key cryptography system based on the algebraic structure of elliptic curves over finite fields.
Exigent Audit/Investigation	An audit or investigation by which there is reason to believe that an entity's failure to meet PKI Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the PKI posed by the entity has occurred.
Intellectual Property Rights	Rights under one or more of the following: copyright, patent, trade secret, trademark, or any other intellectual property rights.
Key Generation Ceremony	A procedure whereby a CA's key pair is generated, its private key is backed up, and/or its public key is certified.
PKI Participant	An individual or organization that is one or more of the following within the PKI: C4MI, a CA, a Subscriber, or a Relying Party.
PKI Policy & Management Authority	The entity that establishes the PKI infrastructure and the related Certificate Authority (CA). It establishes the governance, associated policies, and operations. It serves as the primary point of contact for Subscribers, Relying Parties and any other external entities.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #8	Public-Key Cryptography Standard #8, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Processing Center	A secure facility created by an appropriate organization (e.g., Symantec) that houses, among other things, the cryptographic modules used for the issuance of Certificates.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.

Relying Party	An individual or organization that acts with reliance on a certificate and/or a digital signature.
RSA (Algorithm)	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Secret Share	A portion of the activation data needed to operate the private key, held by individuals called "Shareholders." Some threshold number of Secret Shares (n) out of the total number of Secret Shares (m) shall be required to operate the private key.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations.
Security Repository	Database of relevant security information accessible on-line.
Security Policy	The highest-level document describing security policies.
Sub domain	The portion of the PKI under control of an entity and all entities subordinate to it within the hierarchy.
Sub domain Participants	An individual or organization that is one or more of the following within the Subdomain: C4MI, a Subscriber, or a Relying Party.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of a End-entity Certificate, refer to the Subscriber requesting the End-entity certificate.
Subscriber	The entity who requests one or more Certificates (e.g., a manufacturer). The Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate (s).
Digital Certificate Subscriber Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Superior Entity	An entity above a certain entity within the PKI.
Trusted Person	An employee, contractor, or consultant of an entity within the PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.
Trusted Position	The positions within the MFGH entity that SHALL be held by a Trusted Person.

Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
Validity Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.

4 Abbreviations and Acronyms

This specification uses the following abbreviations:

CA	Certification Authority
C4MI or CMI	Center for Medical Interoperability
CP	Certificate Policy
CPS	Certification Practice Statement
CRA	Certificate Requesting Account
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DR	Demand Response
DCSA	Digital Certificate Subscriber Agreement
DRAS	Demand Response Automation Server
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards
HSO	Health Service Organization
id-at	X.500 attribute types. (OID value: 2.5.4)
id-ce	Object Identifier for Version 3 certificate extensions. (OID value: 2.5.29)
IETF	Internet Engineering Task Force
ISO	Independent System Operators
MFG	Manufacturer
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PA	Policy Authority
PKCS	Public-Key Cryptography Standard

PKI Public Key Infrastructure

RA Registration Authority

RFC Request for comment

RSA Rivest, Shamir, Adelman

5 Overview

5.1 Document Name and Identification

This document is the C4MI Trust Platform Certificate Policy. The following policy object identifier value extension is used for certificates issued under this CP:

- The C4MI Trust Platform Certificate Policy (1.3.6.1.4.1.54775.1.1.1.1)

5.2 PKI Participants

The C4MI PKI is a three-tier infrastructure with a C4MI Root CA at tier 1 that issues intermediate CA certificates (i.e., sub-CAs) at tier 2. The tier 2 sub-CAs issue compliant end-entity Subscriber certificates at tier 3.

PKI hierarchy details are defined in [C4MI-TD-TPPCH].

The C4MI Root CA is the apex of its Root CA Domain. The Root CA will issue the sub-CA certificates to approved CA service providers. The sub-CAs will issue certificates to authorized Subscribers, which will embed the certificates in compliant devices

.

Subscribers SHALL install the C4MI authorized Root CA certificate in the trust anchor store of their end entities to validate received certificates.

The end-entity certificate, its private key, and all sub-CA certificates for a given CA chain SHOULD also be installed on the device.

During the authentication messaging exchange, the end-entity and all sub-CA chain certificates SHALL be sent to the other end point unless the chaining can be verified using an alternative mechanism (e.g., via global configuration).

The following describes the relevant participant roles in the C4MI PKI.

5.2.1 The Center for Medical Interoperability (C4MI)

For an overview of The Center see [CMI-TR-OVERVIEW].

C4MI is the PKI Policy & Management Authority and has established the framework for the C4MI PKI.

As the PKI Policy & Management Authority C4MI governs and oversees the operation of the PKI.

This CP was established under the authority of and with the approval of the C4MI.

5.2.2 Certification Authorities

At the heart of the C4MI PKI are entities called "Certification Authorities" or "CAs." CA is an umbrella term that refers to the collection of hardware, software, and operating personnel that create, sign, issue and revoke public key certificates to Subscribers or sub-CAs.

The CAs are responsible for:

- Developing and maintaining a CPS
- Issuing compliant certificates
- Delivery of certificates (via the RA, or directly) to its Subscribers in accordance with the CP, and other applicable documents such as the Subscriber Agreement
- Revocation of Certificates
- Generation, protection, operation, and destruction of CA private keys
- Operating on-line resources to execute automated certificate renewal and make available both Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responder
- CA Certificate lifecycle management ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP
- CAs act as trusted parties to facilitate the confirmation of the binding between a public key and the identity, and/or other attributes of the "Subject" of the Certificate. In the C4MI PKI, the Subject of a CA certificate is the Subscriber (i.e., C4MI, health system etc.) requesting the CA certificate and the Subject of an end-entity certificate is the Subscriber (e.g., trust platform component, trust participant, manufacturer) requesting the end-entity certificate.

The C4MI CAs fall into two categories: (1) Root CA, which is operated by a designated C4MI Root CA service provider and issues sub-CA certificates; and (2) the sub-CAs which are operated by designated C4MI sub-CA service providers and issue end-entity end-entity certificates to Subscribers.

CAs may provide a secure method for the automated issuance of end-entity certificates from sub-CAs. This may be supported onsite at a Subscriber's manufacturing facility using CA approved hardware and software components or using a remote API. These methods SHALL be compliant to the requirements of this CP.

5.2.3 Registration Authorities

C4MI-approved Registration Authorities (RAs) are entities that enter into an agreement with a Certification Authority to collect and verify each Subscriber's identity and information to be entered into the Subscriber's certificates. The RA performs its function in accordance with this CP and its approved CPS and will perform front-end functions of confirming the identity of the

certificate applicant, approving or denying Certificate Applications, requesting revocation of certificates, and managing certificate and account renewals.

C4MI RAs are integral to the life-cycle of certificates and ensure the proactive management of certificates. Specifically, C4MI RAs will approve certificate issuance, renewal and revocation requests and orchestrate alerts to management entities. Subsequently, RAs are responsible for:

- Validating compliant issuance, renewal and revocation requests, and securely transmitting them to the appropriate CA
- Validating that previously issued certificates and certificate renewal requests are issued only to the entities that are authorized as the "Subject" of the certificate as specified in Section 8 of this document.
- Delivering new and renewed certificates from the CA
- Providing notifications to the PKI Policy and Management Authority about issuance, renewal and revocation transactions
- Assisting the associated CAs in certificate lifecycle management as specified in Section 8 of this document for all Subscriber entities for which the RA is responsible

5.2.4 Subscribers

In the C4MI PKI, the Subscriber is the organization named in the Digital Certificate Subscriber Agreement (DCSA).

An authorized representative of the Subscriber, acting as a Certificate Applicant, SHALL complete the certificate application process established by the RA.

In response, the CA relies on the RA to confirm the identity of the Certificate Applicant and to either approve or deny the application.

If approved, the RA communicates to the CA, and the Subscriber can then request certificates.

C4MI requires that Subscribers SHALL adopt the appropriate C4MI certificate policy requirements and any additional certificate management practices to govern the Subscriber's practice for requesting certificates and handling the corresponding private keys.

The Subscriber agrees to be bound by its obligations through execution of the DCSA between the Subscriber and the PKI Policy and Management Authority, and any other applicable agreements.

CAs are also Subscribers of certificates within a PKI. This applies to the Root CA that issues a self-signed Certificate to itself, and to sub-CAs chaining up to the Root CA.

5.2.5 Relying Parties

The Relying Party is any entity that validates the binding of a public key to the Subscriber's name in an end-entity certificate. The Relying Party is responsible for deciding whether or how to check the

validity of the certificate by checking the appropriate certificate status information. The Relying Party SHOULD use the certificate to verify the integrity of a digitally signed message, to check the validity of the certificate (using a CRL or OCSP server), to identify the initiator of a communication, and to establish confidential communications with the holder of the certificate. For instance, an application server can use the end-entity certificate embedded in a medical device to authenticate the device the device requests services from the server.

5.2.6 Auditors

The PKI participants operating under this CP MAY require the services of other security authorities, such as compliance auditors. The CA's CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.

5.3 Certificate Usage

This CP applies to all C4MI PKI Participants, including Subscribers and Relying Parties. This CP sets forth policies governing the use of C4MI PKI Certificates. Each Certificate is generally appropriate for use as set forth in this CP.

5.3.1 Appropriate Certificate Uses

Within the C4MI architectures that will leverage this CP, certificates are suitable for authentication, message and data integrity verification, encryption for confidentiality, support for non-repudiation, and code signing for software updates.

Certain certificates may be restricted for specific purposes. For instance, for trust platform digital signatures only. These are specified within the certificate definitions and the profiles.

5.4 Policy Administration

5.4.1 Organization Administering the Document

The C4MI is responsible for all aspects of this CP.

5.4.2 Contact Person

Inquiries regarding this CP SHALL be directed to C4MI.

5.4.3 Person Determining CPS Suitability for the Policy

The C4MI SHALL approve the CPS for each CA that issues certificates under this policy, such approval should not be unreasonably withheld.

5.4.4 CPS Approval Procedures

CAs and RAs operating under this CP are required to meet all facets of the policy. The C4MI SHALL make the determination that a CPS complies with this policy. The CA and RA SHALL meet all requirements of an approved CPS before commencing operations.

6 Repository Requirements

6.1 Repositories

In the C4MI PKI, there is no separate entity providing repository services. Rather, each CA is responsible for their repository functions.

All CAs that issue certificates under this policy SHALL post all CA certificates and CRLs issued by the CA in a repository that is publicly accessible on the Internet.

6.2 Publication of Certification Information

The CP, CA certificates, and CRLs SHALL be made publicly available, for example, on the C4MI website.

The CPS for the Root CA will not be published; a redacted version of the CPS will be made publicly available upon request.

There is no requirement for the publication of CPSs of sub-CAs that issue certificates under this policy.

The CA SHALL protect information not intended for public dissemination.

6.3 Time or Frequency of Publication

Changes to this CP SHALL be made publicly available within thirty (30) business days of approval by C4MI. CA information SHALL be published promptly after it is made available to the CA.

Root CA certificates SHALL be made publicly available within ten (10) week days after issuance.

Publication requirements for CRLs are provided in Section 8.7.7.

6.4 Access Controls on Repositories

The CAs SHALL implement controls to prevent unauthorized addition, deletion, or modification of repository entries.

The CPS SHALL detail what information in the repository will be exempt from automatic availability and to whom, and under which conditions the restricted information may be made available.

7 Identification and Authorization

7.1 Naming

7.1.1 Types of Names

For certificates issued under this policy the CA SHALL assign X.501 (see: [ITU-T-X.501]) distinguished names. The subject field in certificates SHALL be populated with a non-empty X.500 (see: [ITU-T-X.500]) distinguished name. The issuer field of certificates SHALL be populated with a non-empty X.500 distinguished name.

7.1.2 Need for Names to be Meaningful

Subscriber Certificates SHALL contain meaningful names with commonly understood semantics permitting the determination of the identity of the organization that is the Subject of the Certificate.

The subject name in CA certificates SHALL match the issuer name in certificates issued by the CA, as required by [IETF-RFC5280].

7.1.3 Anonymity or Pseudonymity of Subscribers

CAs SHALL NOT issue anonymous or pseudonymous certificates.

7.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting Distinguished Name forms are specified in [ITU-T-X.501]

7.1.5 Uniqueness of Names

Name uniqueness for certificates issued by CAs SHALL be enforced.

Each CA, either directly or via the RA, SHALL enforce name uniqueness within the X.500 name space within its domain.

Name uniqueness is not violated when multiple certificates are issued to the same Subscriber.

Name uniqueness is enforced for the entire Subject Distinguished Name of the certificate rather than a particular attribute (e.g., the common name).

The CA SHALL identify the method for checking uniqueness of Subject Distinguished Names within its domain. This will be noted in the CPS.

7.1.6 Recognition, Authentication, and Role of Trademarks

CAs operating under this policy SHALL NOT issue a certificate knowing that it infringes the trademark of another entity. The required verification to ensure this may be performed by the CA directly, the RA, or both. This will be documented in the CPS.

Subscriber certificate applicants SHALL NOT use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others.

Neither C4MI nor any CA/RA SHALL be required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property rights.

This includes, without limitation, rights in a domain name, trade name, trademark, or service mark.

C4MI and CA/RAs SHALL be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such disputes.

C4MI SHALL resolve disputes involving names and trademarks.

7.2 Initial Identity Validation

7.2.1 Method to Prove Possession of Private Key

If the Subscriber generates the certificate key pair, then the entities that receive a certificate issuance or renewal requests (i.e., RA, CA) SHALL prove that the Subscriber possesses the private key by verifying the Subscriber's digital signature on the PKCS #10 (see: [IETF-RFC2986]) Certificate Signing Request (CSR) with the public key in the CSR.

If the key pair is generated by the CA on behalf of a Subscriber; then in this case, proof of possession of the private key by the Subscriber is not required.

C4MI MAY approve other methods to prove possession of a private key by a Subscriber.

7.2.2 Authentication of Organization Identity

The certificate issuance process SHALL ensure the validation of the identity of the organization named in the Digital Certificate Subscriber Agreement by confirming that the organization:

- Exists in a business database (e.g., Dun and Bradstreet), or alternatively, has organizational documentation issued by or filed with the applicable government (e.g., government issued business credentials) that confirms the existence of the organization, such as articles of incorporation, Certificate of Formation, Charter Documents, or a business license that allow it to conduct business
- Conducts business at the address listed in the agreement
- Is not listed on any of the following U.S. Government denied lists: U.S. Department of Commerce' Bureau of Industry and Security Embargoed Countries List, and the U.S. Department of Commerce' Bureau of Industry and Security Denied Entities List

Where applicable for the Subscriber, there may be health industry specific registries such as the FDA Device Registry and Listing which might provide higher confidence authentication of organization identity for a given organization.

This validation SHALL be performed by the RA, CA, or both; and, will be documented in the CPS.

7.2.3 Authentication of Individual Identity

The CA's certificate issuance process SHALL authenticate the individual identity of the:

- Representative submitting the Digital Certificate Subscriber Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc. and is authorized to act on behalf of the organization
- Corporate Contact listed in the Digital Certificate Subscriber Agreement is an officer in the organization and can act on behalf of the organization
- Administrator listed in the Digital Certificate Subscriber Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc, and is authorized to act on behalf of the organization.

Where applicable for the Subscriber, there may be health industry specific registries such as the FDA Device Registry and Listing which might provide higher confidence authentication of the individual identity.

This validation SHALL be performed by the RA, CA, or both; and, will be documented in the CPS.

7.2.4 Non-verified Subscriber Information

Non-verifiable information MAY be included in C4MI PKI certificates, such as:

- Organization Unit (OU)
- Any other information designated as non-verified in the certificate

7.2.5 Validation of Authority

The CA's certificate issuance process SHALL confirm that the:

- Corporate Contact listed in the Digital Certificate Subscriber Agreement is an officer in the organization who can sign on behalf of the organization and bind the organization to the terms and conditions of the agreement
- Representative submitting the Digital Certificate Subscriber Agreement and certificate application is authorized to act on behalf of the organization
- Administrators listed on the Digital Certificate Subscriber Agreement and certificate application are authorized to act on behalf of the organization
- Contacts listed on the Digital Certificate Subscriber Agreement are authorized to act on behalf of the organization

This validation SHALL be performed by the RA, CA, or both; and, will be documented in the CPS.

7.3 Identification and Authentication for Certificate Renewal Requests

7.3.1 Identification and Authentication for CA and RA

CA and RA certificate renewal shall follow the same procedures as initial certificate issuance. Identity MAY be established through the use of the entity's current valid signature key by signing the Certificate Signing Request. A new certificate request SHALL be for new public key pairs – legacy keys may not be reused.

7.3.2 Identification and Authentication for Certificate Issuance After Revocation

Once any certificate has been revoked, issuance of a new certificate is required, and the Subscriber MAY be required to go through the initial identity validation process per Section 7.2.

7.3.3 Identification and Authentication for Certificate Renewal of Subscribers

Subscriber certificate renewal identification MAY be facilitated through the initial identity validation process per Section 7.2.

RA SHALL validate the request prior to relaying the request to the CA over a mutually authenticated, auditable, channel.

Alternatively, Subscriber certificate renewal identification and authorization may be facilitated by an automated process. This is necessary to provide automated alerting of certificate life-cycle status of end entities (specifically, imminent certificate expiration and certificate revocation).

Prior to expiration of certificates, Subscribers SHALL submit a signed CSR to their governing RA.

The RA SHALL identify and authorize the CSR and, if the CSR is deemed authorized and necessary, will forward it to the responsible CA over a mutually authenticated, auditable, channel.

The responsible CA SHALL ensure that the request was received over a mutually authenticated, auditable, connection prior to processing the CSR.

The CA SHALL transmit the signed completed certificate to the RA which will in turn provide the completed certificate to the Subscriber.

Subscribers SHALL use new key pairs for new certificate requests. Subscribers SHALL NOT use legacy key pairs.

7.4 Identification and Authentication for Revocation Request

After a certificate has been revoked other than during a renewal or update action, the Subscriber MAY be required to go through the initial registration process described per Section 7.2 to obtain a new certificate.

Revocation requests SHALL be authenticated, and MAY be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

8 Certificate Life-Cycle operational requirements

8.1 Certificate Application

The Certificate Application is a package consisting of the following:

- The Digital Certificate Subscriber Agreement
- The Subscriber profile containing contact information
- The Naming Document, which specifies the content to be bound in the certificate
- Any associated fees

A CA and RA SHALL include the processes, procedures, and requirements of their certificate application process in their CPS.

8.1.1 Who Can Submit a Certificate Application

An application for a CA certificate SHALL be submitted by an authorized representative of the applicant CA.

An application for a Subscriber certificates SHALL be submitted by the Subscriber or an authorized representative of the Subscriber.

8.1.2 Enrollment Process and Responsibilities

The enrollment process, for a Certificate Applicant, SHALL include the following:

- Completing the Certificate Application package
- Providing the requested information
- Responding to authentication requests in a timely manner
- Submitting required payment

Communication of information MAY be electronic or out-of-band.

8.2 Certificate Application Processing

8.2.1 Performing Identification and Authentication Functions

The identification and authentication functions SHALL meet the requirements described in Section 7.2 and Section 8.5

.

8.2.2 Approval or Rejection of Certificate Applications

A CA/RA will approve a certificate application if all of the following criteria are met:

- A fully executed Digital Certificate Subscriber Agreement
- A completed and signed Naming Document

- Successful identification and authentication of all required contact information in the Subscriber profile
- Receipt of all requested supporting documentation

A CA/RA will reject a certificate application for any of the following:

- The Subscriber fails to execute the required agreement
- An authorized representative fails to sign the certificate application
- Authentication and validation of all required information cannot be completed
- The Subscriber fails to furnish requested supporting documentation
- The Subscriber fails to respond to notices within a specified time

8.2.3 Time to Process Certificate Applications

RA/CA SHALL begin processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Digital Certificate Subscriber Agreement or CPS (which must specify processing time for on-line certificate renewal and revocation).

8.3 Certificate Issuance

Upon receiving a request for a Certificate, the RA/CA SHALL verify that the information in the Certificate Application is correct and accurate.

8.3.1 CA Actions During Certificate Issuance

Upon receiving the request, the RA/CA SHALL:

• verify the identity of the requester

• verify the authority of the requester and the integrity of the information in the Certificate request

• create and sign the certificate if all the requirements have been met

• make the certificate available for download to the subscriber via the RA (or directly if it is an onsite Sub-CA)

8.3.2 Notification to Subscriber of Certificate Issuance

When certificates are issued, the Subscriber needs to be notified.

Within the managed CA option, the RA that processes the associated requests SHALL perform this notification and provide information for the signed certificates to be retrieved.

When a sub-CA is onsite and processes the request directly or via an RA the request processing entity SHALL perform this notification and provide information for the signed certificates to be retrieved.

8.3.3 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance by the Subscriber:

- Downloading a Certificate
- Failure to object in a timely manner to the certificate or its content

8.3.4 Publication of the Certificate by the CA

CA certificates SHALL be published in a publicly available repository as specified in Section 6.1

This policy makes no stipulation regarding publication of Subscriber certificates.

8.3.5 Notification of Certificate Issuance by the CA to Other Entities

C4MI SHALL be notified whenever a CA operating under this policy issues a CA certificate.

This notification may come from the CA or the RA, and will be identified in the CPS.

8.4 Key Pair and Certificate Usage

8.4.1 Subscriber Private Key and Certificate Usage

Subscriber private key usage SHALL be specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate. Per the Digital Certificate Subscriber Agreement, Subscribers SHALL protect their private keys from unauthorized use and SHALL discontinue use of the private key following expiration or revocation of the certificate. Private keys SHOULD be destroyed after expiration or revocation of the certificate (and certain C4MI specifications may require private keys to be destroyed as part of certificate life-cycle processes).

Certificate use SHALL be consistent with the KeyUsage field extensions included in the certificate.

8.4.2 Relying Party Public Key and Certificate Usage

Relying Parties SHOULD assess:

- The restrictions on key and certificate usage specified in this CP and which are specified in critical certificate extensions, including the basic constraints and key usage extensions.
- The status of the certificate and all the CA certificates in the certificate chain. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to determine whether reliance on a Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

8.5 Certificate Renewal

Certificate renewal is the issuance of a new certificate to a Subscriber connected component without changing any information in the certificate except the validity period, serial number, and public key. Using a key pair beyond its intended lifetime can increase its vulnerability to attack.

Consequently, certificate renewal requires use of a new key pair. After certificate renewal, the legacy private key SHOULD be destroyed as required by Section 10.2.10.

CA certificates SHALL NOT be renewed in this manner.

8.5.1 Circumstance for Certificate Renewal

End-entity certificate renewal MAY be supported for certificates where the private key associated with the certificate has not been compromised. End-entity certificates MAY be renewed to maintain continuity of operation of necessary and authorized end-entities as judged approved the corresponding RA.

An end-entity certificate MAY NOT be renewed after expiration. After expiration, a new certificate MAY be requested using normal certificate issuance processes as outlined in Section 8.3. The original certificate MAY or MAY NOT be revoked, but SHALL NOT be further re-keyed, renewed, or modified.

8.5.2 Who may Request Renewal

The Subscriber of the certificate or an authorized representative of the Subscriber MAY request a certificate renewal. If automatic renewal is used, the Subscriber connected component with a non-expired, non-revoked certificate MAY request renewal through its governing RA.

8.5.3 Processing Certificate Renewal Requests

For a certificate renewal request, the RA/CA SHALL confirm the identity of the Subscriber in accordance with the requirements specified in Section 8.5.

If online renewal is used, the RA shall indicate validation of the certificate renewal request to the CA via a mutually authenticated, auditable, channel.

8.5.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of certificate renewal to the Subscriber SHALL be in accordance with Section 8.3.2 for standard renewal. Online renewal notification SHALL be provided through the RA/CA.

8.5.5 Conduct Constituting Acceptance of a Renewal Certificate

The end entity receiving the renewed certificate SHALL re-establish all security associations or other functions using the associated new key pairs as soon as practical (e.g., patient care SHALL NOT be disrupted).

Conduct constituting Acceptance of a renewed certificate SHALL be in accordance with Section 8.5.3.

Online renewal that fails SHALL result in appropriate failure notifications to C4MI (as the PKI Policy & Management Authority) and other identified management entities.

8.5.6 Publication of the Renewal Certificate by the CA

Publication of a renewed certificate SHALL be in accordance with Section 8.3.4.

8.5.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of the issuance of certificates SHALL be in accordance with Section 8.6.7.

8.6 Certificate Modification

Modifying a certificate means creating a new certificate that contains a different serial number and that differs in one or more other fields from the original certificate, except for the public key and validity period fields.

8.6.1 Circumstance for Certificate Modification

Certificates MAY be modified:

- For a Subscriber organization name change or other Subscriber characteristic change
- To correct subject name attributes or extension settings.

The original certificate may or may not be revoked. The original certificate SHALL NOT be further re-keyed, renewed, or modified.

If not revoked, the CA will flag the certificate as inactive in its database, but will not publish the certificate on a CRL.

8.6.2 Who May Request Certificate Modification

The following entities may request a certificate modification:

- The Subscriber of the certificate or an authorized representative of the Subscriber
- The CA, for its own certificate
- C4MI, for CA certificates

8.6.3 Processing Certificate Modification Requests

For certificate modification requests, the CA SHALL confirm the identity of the Subscriber in accordance with the requirements specified in Section 7.2 for the authentication of an initial Certificate Application.

CA certificate modification SHALL be approved by the C4MI.

8.6.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a new certificate to the Subscriber SHALL be in accordance with Section 8.3.2.

8.6.5 Conduct Constituting Acceptance of Modified Certificate

Conduct constituting Acceptance of a modified certificate SHALL be in accordance with Section 8.3.3.

8.6.6 Publication of the Modified Certificate by the CA

Publication of a modified certificate SHALL be in accordance with Section 8.3.4.

8.6.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of the issuance of certificates SHALL be in accordance with Section 8.6.7.

8.7 Subscriber Certificate Revocation and Suspension

8.7.1 Circumstances for Revocation

Subscriber certificates are revoked under the following circumstances:

- The Subscriber or an authorized representative of the Subscriber (such as an RA) asks for the certificate to be revoked for any reason whatsoever
- The Subscriber's private key corresponding to the public key in the certificate has been:
    - lost or compromised
    - disclosed without authorization
    - stolen
- The Subscriber can be shown to have violated the stipulations of its subscriber agreement
- The Digital Certificate Subscriber Agreement with the Subscriber has been terminated
- There is an improper or faulty issuance of a certificate
- A prerequisite to the issuance of the certificate can be shown to be incorrect;
    - information in the certificate is known, or reasonably believed, to be false.
    - the Subscriber has not submitted payment when due
- Identifying information of the Subscriber in the certificate becomes invalid
- Attributes asserted in the Subscriber's certificate are incorrect
- The Certificate was issued:
    - in a manner not in accordance with the procedures required by the applicable CPS
    - to a person other than the one named as the Subject of the Certificate
    - without the authorization of the person named as the Subject of such Certificate
- The Subscriber's organization name changes
- The RA/CA suspects or determines that any of the information appearing in the Certificate is inaccurate or misleading
- The continued use of that certificate is harmful to C4MI or the RA/CA
- The RA/CA finds that in the ordinary course of business that the certificate SHOULD be revoked
- In exigent and/or emergency situations
- Any other circumstances that may reasonably be expected to affect the reliability, security, integrity or trustworthiness of the certificate or the cryptographic key pair associated with the certificate.

Whenever any of the above circumstances occur, the associated certificate SHALL be revoked by the CA and update the CRL and OCSP responder. Revoked certificates SHALL be included on all new publications of the certificate status information until the certificates expire.

Whenever a certificate is revoked the CA directly or via the RA SHALL notify C4MI.

8.7.2 Who can Request Revocation

Within the C4MI PKI, revocation requests MAY be made by:

- the Subscriber of the certificate or any authorized representative of the Subscriber
- the RA/CA for certificates within its domain
- C4MI

Automated revocation MAY be requested by the Subscriber connected component or the RA responsible for the Subscriber connected component.

8.7.3 Procedure for Revocation Request

A request to revoke a certificate SHALL identify the date of the request, the certificate to be revoked, the reason for revocation, and allow the requestor to be authenticated.

The CA SHALL specify the steps involved in the process of requesting a certificate revocation in their CPS.

Prior to the revocation of a Subscriber Certificate, the RA/CA SHALL authenticate the request. Acceptable procedures for authenticating revocation requests include:

- Having the Subscriber log in to their Certificate Requesting Account and revoking their Certificates via their account portal. The Subscriber will submit their request via their online Certificate Requesting Account, which will employ two-factor authentication, e.g., a USB token with the account administrator's certificate and a PIN.
- Communication with the Subscriber providing reasonable assurances that the person or organization requesting revocation is, in fact the Subscriber. Such communication will include two or more of the following: telephone confirmation, signed facsimile, digitally signed e-mail, postal mail, or courier service.
- The representative is the Corporate Contact, Administrator, Legal, or Technical contact authenticated in Section 7.2.5

RA/CAs are entitled to request the revocation of Subscriber Certificates within the CA's Subdomain. RA/CAs SHALL obtain approval from the C4MI prior to performing the revocation functions except for revocations pursuant to Section 8.7.1. The RA/CA SHALL send a written notice and brief explanation for the revocation to the Subscriber. Notwithstanding anything to the contrary in this CP, CAs are authorized to take any action they deem necessary, under the circumstances and without liability to any party, to protect the security and integrity of the CA and/or the C4MI PKI.

The requests from RA/CAs to revoke a CA Certificate SHALL be authenticated by the C4MI.

Upon revocation of a certificate, the CA that issued the Certificate SHALL publish notice of such revocation in the CA's repository or issue it upon request from the C4MI.

Automated revocation requested by Subscriber connected components SHALL be sent to the RA. The RA SHALL process the revocation request with the CA online resources. The RA SHALL send Subscriber an alert notification of the revocation on receipt of a confirmation from the CA. Similarly, when automated revocation is executed by the RA, the Subscriber SHALL be alerted upon receipt of the confirmation from the CA.

When CAs mandate revocation, they SHALL notify the RA of the revocation event. The RA SHALL verify that the revocation has taken place with the CRL or OCSP. Once confirmed, the RA SHALL send the Subscriber an alert notification.

8.7.4 Revocation Request Grace Period

Revocation requests SHOULD be submitted as promptly as possible after becoming aware of a revocation circumstance listed in Section 8.7.1.

8.7.5 Time Within Which CA Must Process the Revocation Request

RA/CAs SHALL begin investigation of a normal (not automated) Certificate revocation request within five (5) business days of receipt to decide whether revocation or other appropriate action is warranted based upon the circumstances of the request in Section 8.7.1.

RA/CAs SHALL execute automated revocation requests according to the governing CPS.

Emergency revocation requests that require an expedited process SHALL be specified in the CPS.

8.7.6 Revocation Checking Requirement for Relying Parties

Relying Parties SHOULD check the status of Certificates on which they wish to rely on by checking the certificate status:

- On the most recent CRL from the CA that issued the Certificate
- On the applicable web-based repository
- By using an Online Certificate Status Protocol (OCSP) responder (if available).

CAs SHALL provide Relying Parties with information within the certificate CRL Distribution Point extension on how to find the appropriate CRL, web-based repository, or OCSP responder (if available) to check the revocation status of certificates issued by the CA.

8.7.7 CRL Issuance Frequency

CRLs SHALL be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information MAY be issued more frequently than the issuance frequency described below.

C4MI CAs SHALL update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Certificate, with the value of the nextUpdate field not more than twelve (12) months beyond the value of the thisUpdate field.

8.7.8 Maximum Latency for CRLs

CRLs SHOULD be published immediately. And CRLs SHALL be published within three (3) business days of generation.

8.7.9 On-line Revocation/Status Checking Availability

CAs SHALL have a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. CAs SHALL provide Relying Parties with information on how to find the appropriate repository to check Certificate status and how to find the correct OCSP responder.

8.7.10 On-line Revocation Checking Requirements

A Relying Party SHOULD check the status of a certificate on which they wish to rely. If a Relying Party does not check the status of a Certificate by consulting the most recent CRL, the Relying Party SHOULD check the Certificate status by consulting the applicable on-line repository or by requesting Certificate status using the applicable OCSP responder (where available). If the Relying Party does not check the status of the certificates as described in this paragraph or the CPS, the Relying Party is stopped from asserting any claim against the CA related to or arising out of the Relying Party's reliance on the certificate.

8.7.11 Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method SHALL meet the following requirements:

- The alternative method will be described in the CA's CPS
- The alternative method will meet the issuance and latency requirements for CRLs

8.7.12 Special Requirements Regarding Key Compromise

When a CA certificate is revoked, the CRL and OCSP responder SHALL be updated within 24 hours of notification.

8.7.13 Circumstances for Suspension

The C4MI PKI does not offer suspension services for its Certificates.

8.7.14 Who can Request Suspension

No stipulation.

8.7.15 Procedure for Suspension Request

No stipulation.

8.7.16 Limits on Suspension Period

No stipulation.

8.8 Certificate Status Services

8.8.1 Operational Characteristics

Certificate status SHALL be available via CRL and OCSP through a URL specified in a CA's CPS. Certificate status MAY also be available via LDAP directory or OCSP responder.

8.8.2 Service Availability

Certificate Status Services SHALL be available 24 x 7. CRL and OCSP capability SHOULD respond within the response time specified in the CPS under normal operating conditions.

8.9 End of Subscription

End of subscription SHALL be stipulated in the Digital Certificate Subscriber Agreement.

9 Facility, Management, and Operational Controls

All entities performing CA functions SHALL implement and enforce the following physical, procedural, logical, and personnel security controls for a CA.

9.1 Physical Controls

CA equipment SHALL be protected from unauthorized access while the cryptographic module is installed and activated. The CA SHALL implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens SHALL be protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to the Common Policy Root CA and subordinate CAs, and any remote workstations used to administer the CAs, except where specifically noted.

9.1.1 Site Location and Construction

All CA systems SHALL be located within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. The location and construction of the facility housing the CA equipment SHALL be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, SHALL provide robust protection against unauthorized access to the CA equipment and records.

Such requirements are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door, a closed gate, or an alarm system that provides mandatory access control for individuals and requires a positive response (e.g., door unlocks, gate opens, or alarm system is disarmed) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access.

CAs SHALL construct the facilities housing their CA functions with at least four physical security tiers. CAs SHALL perform all validation operations within Tier 2 or higher. CAs SHALL place Information Services systems necessary to support CA functions in Tier 3 or higher. Online and offline cryptographic modules SHALL be placed in Tier 3 or higher when not in use.

CAs SHALL describe their Site Location and Construction in more detail in their CPS.

9.1.2 Physical Access

Access to each tier of physical security, constructed in accordance with Section 9.1.1, SHALL be auditable and controlled so that only authorized personnel can access each tier.

CAs SHALL control access to their CA facilities including:

- Minimizing exposure of privileged functions through definition of function-specific roles or authorization groups
- Access control enforcement of these roles or groups

- Logging of access into and out of the facility
- The use of tamper resistant physical intrusion alarm systems to detect break-ins or unauthorized access to physical security tiers within the facility
- Video surveillance
- Facility-based guards 24/7, with multi-factor authentication (e.g., Iris scan, hand geometry) required for access.
- Automated and video surveillance based notification to outside alarm monitoring agency of any potential security breach.

At a minimum, the physical access controls for CA equipment, as well as remote workstations used to administer the CAs, SHALL:

- Ensure that industry standard controls are in place to help prevent unauthorized access to the hardware.
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Manually or electronically monitor for unauthorized intrusion at all times.
- Ensure an access log is maintained and inspected periodically.
- Require two-person physical access control to both the cryptographic module and computer systems.

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules SHALL be placed in secure containers.

Activation data SHALL be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and will not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs SHALL occur if the facility is to be left unattended. At a minimum, the check SHALL verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when open, and secured when closed, and for the CA, that all equipment other than the repository is shut down)
- Any security containers are properly secured
- Physical security systems (e.g., door locks, vent covers) are functioning properly
- The area is secured against unauthorized access

A person or group of persons SHALL be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance SHALL be maintained. If the facility is not continuously attended, the last person to depart SHALL initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

9.1.3 Power and Air Conditioning

CA facilities SHALL be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these facilities SHALL be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity.

The CA SHALL have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

9.1.4 Water Exposures

CA facilities SHALL be constructed, equipped, and installed, and procedures SHALL be implemented, to prevent floods or other damaging exposure to water. Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

9.1.5 Fire Prevention and Protection

CA facilities SHALL be constructed and equipped, and procedures SHALL be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures SHALL meet all local applicable safety regulations.

9.1.6 Media Storage

CAs SHALL protect the media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and SHALL use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

Any such backups SHALL be secured via strong encryption mechanisms to be outlined in the CPS.

9.1.7 Waste Disposal

CAs SHALL implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

CA media and documentation that are no longer needed for operations SHALL be destroyed in a secure manner. For example, paper documentation SHALL be shredded, burned, or otherwise rendered unrecoverable.

9.1.8 Off-site Backup

CAs SHALL maintain backups of critical system data or any other sensitive information, including audit data, in a secure off-site facility. Full system backups sufficient to recover from system failure SHALL be made on a periodic schedule, and described in a CA's CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy SHALL be stored at an off-site location (separate from CA equipment). Only the latest full backup need be retained. The backup SHALL be stored at a site with physical and procedural controls commensurate to that of the operational CA. An active/active infrastructure, whereby data are synchronized between two

sites and one site alone is capable of hosting the C4MI PKI in the event of a disaster at the other site, will meet the requirements of off-site backup.

Requirements for CA private key backup are specified in Section 10.2.4.

9.2 Procedural Controls

Procedural controls are requirements on roles that perform functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles SHALL be extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

9.2.1 Trusted Roles

Employees, contractors, and consultants that are designated to manage the CA's trustworthiness SHALL be considered to be "Trusted Persons" serving in "Trusted Positions." Persons seeking to become Trusted Persons SHALL meet the screening requirements of Section 9.3

CAs SHALL consider the categories of their personnel identified in this section as Trusted Persons having a Trusted Position. Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- The validation of information in Certificate Applications
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information
- The issuance, or revocation of Certificates, including (in the case of Processing Centers) personnel having access to restricted portions of its repository
- The handling of Subscriber information or requests

Trusted Persons include, but are not limited to, customer service personnel, CA system administrators, designated engineering personnel, CA operators, auditors, and executives that are designated to manage infrastructural trustworthiness.

9.2.2 Number of Persons Required per Task

Multiparty control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the CA. Access to CA cryptographic hardware SHALL be strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a CA device is activated with operational keys, further access controls SHALL be invoked to maintain split control over both physical and logical access to the device. Persons with physical access to CA modules do not hold "Secret Shares" to activate the CA and vice versa.

Two or more persons are required for the following tasks:

- Access to CA hardware

- Management of CA cryptographic hardware
- CA key generation
- CA signing key activation
- CA private key backup

Where multiparty control is required, at least one of the participants SHALL be an Administrator. All participants SHALL serve in a trusted role as defined in Section 9.2.1. Multiparty control SHALL NOT be achieved using personnel that serve in the Auditor trusted role. CAs SHALL establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Other manual operations such as the validation and issuance of Certificates, not issued by an automated validation and issuance system, require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process. Manual operations for Key Recovery MAY optionally require the validation of two (2) authorized Administrators.

9.2.3 Identification and Authentication for Each Role

CAs SHALL confirm the identity and authorization of all personnel seeking to become Trusted Persons before such personnel are:

- Issued access devices and granted access to the required facilities;
- Given electronic credentials to access and perform specific functions on CA systems.

Authentication of identity SHALL include the personal (physical) presence of such personnel before Trusted Persons performing HR or security functions within an entity and a check of well-recognized forms of identification, such as passports and driver's licenses. Identity SHALL be further confirmed through background checking procedures in Section 9.3.2.

9.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to) the following:

- Validation of information in Certificate Applications
- Acceptance, rejection, or other processing of Certificate Applications, revocation requests, key recovery requests or renewal requests, or enrollment information
- Issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository
- Handling of Subscriber information or requests
- Generation, issuing, or destruction of a CA certificate
- Loading of a CA to a Production environment

No individual SHALL have more than one trusted role. The CA SHALL have in place a procedure to identify and authenticate its users and will ensure that no user identity can assume multiple roles.

9.3 Personnel Controls

9.3.1 Qualifications, Experience, and Clearance Requirements

CAs SHALL require that personnel assigned to Trusted roles have the requisite background, qualifications, and experience or be provided the training needed to perform their prospective job responsibilities competently and satisfactorily. The requirements governing the qualifications, selection, and oversight of individuals who operate, manage, oversee, and audit the CA SHALL be set forth in the CPS.

9.3.2 Background Check Procedures

CAs SHALL conduct background check procedures for personnel tasked to become Trusted Persons. These procedures SHALL be subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity SHALL utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by an applicable agency. Background investigations MAY include a:

- Confirmation of previous employment
- Check of one or more professional references
- Confirmation of the highest or most relevant educational degree obtained
- Search of criminal records (local, state or provincial, and national)
- Check of credit/financial records
- Search of driver's license records

Factors revealed in a background check that MAY be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person (all subject to and in accordance with applicable law) MAY include but are not limited to the following:

- Misrepresentations made by the candidate or Trusted Person
- Highly unfavorable or unreliable personal references
- Certain criminal convictions
- Indications of a lack of financial responsibility

Background checks SHALL be repeated for personnel holding Trusted Positions at least every five (5) years.

9.3.3 Training Requirements

CAs SHALL provide their personnel with the requisite on-the-job training needed for their personnel to perform their job responsibilities relating to CA operations competently and satisfactorily. They SHALL also periodically review their training programs, and their training SHALL address the elements relevant to functions performed by their personnel.

Training programs SHALL address the elements relevant to the particular environment of the person being trained, including, without limitation:

- Security principles and mechanisms of the CA and its environment
- Hardware and software versions in use
- All duties the person is expected to perform
- Incident and Compromise reporting and handling
- Disaster recovery and business continuity procedures
- The stipulations of this policy

9.3.4 Retraining Frequency and Requirements

CAs SHALL provide refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

All individuals responsible for PKI roles SHALL be made aware of changes in the CA operation. Any significant change to the operations SHALL have a training (awareness) plan, and the execution of such plan SHALL be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation SHALL be maintained identifying all personnel who received training and the level of training completed.

9.3.5 Job Rotation Frequency and Sequence

No stipulation.

9.3.6 Sanctions for Unauthorized Actions

CAs SHALL establish, maintain, and enforce policies for the discipline of personnel following unauthorized actions. Disciplinary actions MAY include measures up to and including termination and SHALL be commensurate with the frequency and severity of the unauthorized actions.

9.3.7 Independent Contractor Requirements

CAs SHALL permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly defined outsourcing relationships. CAs SHOULD only use contractors or consultants as Trusted Persons if the CA does not have suitable employees available to fill the roles of Trusted Persons. Otherwise, independent contractors and consultants SHALL be escorted and directly supervised by Trusted Persons when they are given access to the CA and its secure facility.

Contractors fulfilling trusted roles are subject to all personnel requirements stipulated in this policy and SHALL establish procedures to ensure that any subcontractors perform in accordance with this policy.

9.3.8 Documentation Supplied to Personnel

CAs SHALL give their personnel the requisite training and documentation needed to perform their job responsibilities competently and satisfactorily.

9.4 Audit Logging Procedures

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

9.4.1 Types of Events Recorded

All auditing capabilities of the CA operating system and applications SHALL be enabled during installation. All audit logs, whether recorded automatically or manually, SHALL contain the date and time, the type of event, and the identity of the entity that caused the event.

CAs SHALL record in audit log files all events relating to the security of the CA system, including, without limitation:

- Physical Access / Site Security:
    - Personnel access to room housing CA
    - Access to the CA server
    - Known or suspected violations of physical security
- CA Configuration:
    - CA hardware configuration
    - Installation of the operating system
    - Installation of the CA software
    - System configuration changes and maintenance
    - Installation of hardware cryptographic modules
    - Cryptographic module lifecycle management-related events (e.g., receipt, use, de-installation, and retirement)
- Account Administration:
    - System Administrator accounts
    - Roles and users added or deleted to the CA system
    - Access control privileges of user accounts
    - Attempts to create, remove, set passwords or change the system privileges of the privileged users (trusted roles)
    - Attempts to delete or modify audit logs
    - Changes to the value of maximum authentication attempts

  - Resetting operating system clock
  - Electrical power outages
- CA Operational events:
  - Key generation
  - Start-up and shutdown of CA systems and applications
  - Changes to CA details or keys
  - Access to private keys
  - Records of the destruction of media containing key material, activation data, or personal Subscriber information
- Certificate lifecycle events:
  - Issuance
  - Re-key
  - Renew
  - Revocation
- Trusted employee events:
  - Logon and logoff
  - Attempts to create, remove, set passwords or change the system privileges of privileged users
  - Unauthorized attempts to the CA system
  - Unauthorized attempts to access system files
  - Failed read and write operations on the Certificate
  - Personnel changes
- Token events:
  - Serial number of tokens shipped to Subscriber
  - Account Administrator Certificates
  - Shipment of tokens
  - Tokens driver versions

9.4.2 Frequency of Processing Log

CAs SHALL review their audit logs in response to alerts based on irregularities and incidents within their CA systems. Review of the audit log SHALL be required at least once every six months. CAs SHALL compare their audit logs with supporting manual and electronic logs when any action is deemed suspicious.

Audit log processing SHALL consist of a review of the audit logs and documenting the reason for all significant events in an audit log summary. Audit log reviews SHALL include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews SHALL be documented.

9.4.3 Retention Period for Audit Log

Audit logs SHALL be retained onsite at least twelve (12) months after processing and thereafter archived in accordance with Section 9.5. The individual who removes audit logs from the CA system SHALL be different from the individuals who, in combination, command the CA signature key.

9.4.4 Protection of Audit Log

Audit logs SHALL be protected from unauthorized viewing, modification, deletion, or other tampering. CA system configuration and procedures SHALL be implemented together to ensure that only authorized people archive or delete security audit data. Procedures SHALL be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access).

9.4.5 Audit Log Backup Procedures

Incremental backups of audit logs SHALL be created frequently, at least monthly.

9.4.6 Audit Collection System (Internal vs. External)

The audit log collection system MAY or MAY NOT be external to the CA system. Automated audit processes SHALL be invoked at system or application startup and cease only at system or application shutdown. Audit collection systems SHALL be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations SHALL be suspended until the problem has been remedied.

9.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

9.4.8 Vulnerability Assessments

The CA SHALL perform routine self-assessments of security controls for vulnerabilities. Events in the audit process are logged, in part, to monitor system vulnerabilities. The assessments SHALL be performed following an examination of these monitored events. The assessments SHALL be based on real-time automated logging data and SHALL be performed at least on an annual basis as input into an entity's annual Compliance Audit.

The audit data SHOULD be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors SHOULD check for continuity of the audit data.

9.5 Records Archival

CA archive records SHALL be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. Records MAY be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate, reliable, and complete.

9.5.1 Types of Records Archived

The CA records SHALL include all relevant evidence in the recording entity's possession, including, without limitation:

- Time stamps
- Certificate policy
- Certification practice statement
- Contractual obligations and other agreements concerning operations of the CA System and equipment configuration
- Modifications and updates to system or configuration
- Certificate request documentation
- Records of all actions taken on certificates issued and/or published
- Record of re-key
- Revocation request information
- Records of all CRLs issued and/or published
- Compliance Auditor reports
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications

The RA records SHALL include all relevant evidence in the recording entity's possession, including, without limitation:

- Digital Certificate Subscriber Agreements
- Token lifetime (issuance, recovery, destruction, etc.) documentation
- All CRLs issued and/or published
- Compliance Auditor reports
- Destruction of cryptographic modules
- All certificate compromise notifications

9.5.2 Retention Period for Archive

Archive records SHALL be kept for a minimum of 7 years without any loss of data.

9.5.3 Protection of Archive

An entity maintaining an archive of records SHALL protect the archive so that only the entity's authorized Trusted Persons are able to obtain access to the archive. The archive SHALL be protected against unauthorized viewing, modification, deletion, or other tampering. The archive media and the applications required to process the archive data SHALL be maintained to ensure that the archive data can be accessed for the time period set forth in Section 9.5.2.

9.5.4 Archive Backup Procedures

Entities compiling electronic information SHALL incrementally back up system archives of such information on a daily basis and perform full backups on a weekly basis. Copies of paper-based records SHALL be maintained in an off-site secure facility.

9.5.5 Requirements for Time-Stamping of Records

CA archive records SHALL be automatically time-stamped as they are created. System clocks used for time-stamping SHALL be maintained in synchrony with an authoritative time standard.

9.5.6 Archive Collection System (Internal or External)

Archive data may be collected in any expedient manner.

9.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified as usable when it is restored.

9.6 Key Changeover

When a CA certificate is rekeyed only the new key is used to sign certificates from that time on. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key SHALL be retained and protected.

A CA Certificate may be renewed if the CA's Superior Entity reconfirms the identity of the CA. Following such reconfirmation, the Superior Entity SHALL either approve or reject the renewal application.

When a CA updates its private signature key and thus generates a new public key, the CA SHALL notify all CAs, RAs, and Subscribers that rely on the CA's certificate that it has been changed.

9.7 Compromise and disaster recovery

9.7.1 Incident and Compromise Handling Procedures

The C4MI SHALL be notified if any CAs operating under this policy experience the following:

- Suspected or detected compromise of the CA systems

- Physical penetration of the site housing the CA systems
- Successful denial of service attacks on CA components

The C4MI will take appropriate steps to protect the integrity of the C4MI PKI.

The CA's Management Authority SHALL reestablish operational capabilities as quickly as possible in accordance with the procedures set forth in the CA's CPS.

9.7.2 Computing Resources, Software, and/or Data are Corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this policy SHALL respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- The C4MI SHALL be notified as soon as possible.
- A report of the incident and a response to the event, SHALL be promptly made by the affected CA or RA in accordance with the documented incident and Compromise reporting and handling procedures in the applicable CPS.

9.7.3 Entity Private Key Compromise Procedures

In the event of a CA private key compromise, the following operations SHALL be performed.

- The C4MI SHALL be immediately informed.
- If the CA signature keys are not destroyed, CA operation SHALL be reestablished, giving priority to the ability to generate certificate status information.
- If the CA signature keys are destroyed, CA operation SHALL be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.
- The CA SHALL generate new keys in accordance with Section 10.1.1.
- Initiate procedures to notify Subscribers of the compromise.
- Subscriber certificates MAY be renewed automatically by the CA under the new key pair (see Section 8.5), or the CA MAY require Subscribers to repeat the initial certificate application process.

9.7.4 Business continuity capabilities after a disaster

Entities operating CAs SHALL develop, test, and maintain a Disaster Recovery Plan designed to mitigate the effects of any kind of natural or man-made disaster. The Plan SHALL identify conditions for activating the recovery and what constitutes an acceptable system outage and recovery time for the restoration of information systems services and key business functions within a defined recovery time objective (RTO).

Additionally, the Plan SHALL include:

- Frequency for taking backup copies of essential business information and software,
- Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,

- Separation distance of the Disaster recovery site to the CA's main site,
- Procedures for securing the Disaster facility during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

The DRP SHALL include administrative requirements including:

- Maintenance schedule for the plan
- Awareness and education requirements
- Responsibilities of the individuals
- Regular testing of contingency plans

CAs SHALL have the capability of restoring or recovering essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions: Certificate issuance, Certificate revocation, and publication of revocation information. The disaster recovery equipment SHALL have physical security protections comparable to the production CA system, which includes the enforcement of physical security tiers.

A CA's disaster recovery plan SHALL make provisions for full recovery within one week following a disaster at the primary site.

9.8 CA or RA Termination

When a CA operating under this policy terminates operations before all certificates have expired, the CA signing keys SHALL be surrendered to C4MI. Prior to CA termination, the CA SHALL provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.

CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).

The termination of a C4MI CA SHALL be subject to the contract between the terminating CA and its Superior Entity. A terminating CA and its Superior Entity SHALL, in good faith, use commercially reasonable effort to agree on a termination plan that minimizes disruption to Subscribers and Relying Parties. The termination plan MAY cover issues such as:

- Providing notice to parties affected by the termination, such as Subscribers and Relying Parties
- Who bears the cost of such notice, the terminating CA or the Superior Entity
- The revocation of the Certificate issued to the CA by the Superior Entity
- The preservation of the CA's archives and records for the time periods required in Section 9.4.6
- The continuation of Subscriber and customer support services
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services

- The revocation of unexpired unrevoked Certificates of Subscribers and subordinate CAs, if necessary
- The payment of compensation (if necessary) to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, for the issuance of substitute Certificates by a successor CA
- Disposition of the CA's private key and the hardware token containing such private key
- Provisions needed for the transition of the CA's services to a successor CA

10 Technical Security Controls

10.1 Key Pair Generation and Installation

10.1.1 Key Pair Generation

Key pair generation SHALL be performed using [FIPS-140-2] validated cryptographic modules and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. Any pseudo-random numbers used and parameters for key generation material SHALL be generated by a FIPS-approved method.

CA keys SHALL be generated in a Key Generation Ceremony using multi-person control for CA key pair generation, as specified in Section 10.2.2.

CA key pair generation SHALL create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure SHALL be detailed enough to show that appropriate role separation was used. An independent third party SHALL validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

10.1.2 Private Key Delivery to Subscriber

Subscriber key pair generation SHALL be performed by the Subscriber or CA. If the Subscribers themselves generate private keys, then private key delivery to a Subscriber is unnecessary.

When CAs generate key pairs on behalf of the Subscriber, the private key SHALL be delivered securely to the Subscriber. Private keys SHALL be delivered electronically or on a hardware cryptographic module. In all cases, the following requirements SHALL be met:

- The CA SHALL not retain any copy of the key for more than two weeks after delivery of the private key to the Subscriber.
- CAs SHALL use [FIPS-140-2] Level 3 systems and deliver private keys to Subscribers via SSL/TLS and SHALL secure such delivery through the use of a PKCS#8 ([IETF-RFC5208]) package or, at the CAs sole discretion, any other comparably equivalent means (e.g., PKCS#12 package, specified in [IETF-RFC7292]) in order to prevent the loss, disclosure, modification, or unauthorized use of such private keys.
- Where key pairs are pre-generated on hardware tokens, the entities distributing such tokens SHALL use best efforts to provide physical security of the tokens to prevent the loss, disclosure, modification, or unauthorized use of the private keys on them. The RA SHALL maintain a record of the Subscriber acknowledgment of receipt of the token.
- The Subscriber SHALL acknowledge receipt of the private key(s).
- Delivery SHALL be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.

For hardware modules, accountability for the location and state of the module SHALL be maintained until the Subscriber accepts possession of it.

For electronic delivery of private keys, the key material SHALL be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data SHALL be delivered using a separate secure channel.

10.1.3 Public Key Delivery to Certificate Issuer

When a public key is transferred to the issuing CA to be certified, it SHALL be delivered through a mechanism validating the identity of the Subscriber and ensuring that the public key has not been altered during transit and that the Certificate Applicant possesses the private key corresponding to the transferred public key. The Certificate Applicant SHALL deliver the public key in a PKCS#10 CSR or an equivalent method ensuring that the public key has not been altered during transit; and the Certificate Applicant possesses the private key corresponding to the transferred public key. The Certificate Applicant will submit the CSR via their online Certificate Requesting Account, which employs two-factor authentication, e.g., a USB token with the account administrator's certificate and a PIN.

10.1.4 CA Public Key Delivery to Relying Parties

The Root CA public key certificate SHALL be delivered to Relying Parties in a secure fashion to preclude substitution attacks. Acceptable methods for certificate delivery are:

- The Root CA Certificate is delivered as part of a Subscriber's certificate request.
- Secure distribution of Root CA certificates through secure out-of-band mechanisms.
- Downloading the Root CA certificates from trusted web sites (e.g., the C4MI web site). The Root CA SHALL calculate the hash of the certificate before posting it on a website so that it can be made available via out-of-band to Relying Parties to validate the posted Root CA certificate.

10.1.5 Key Sizes

Key pairs SHALL be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs.

C4MI certificates SHALL meet the following requirements for algorithm type and key size:

Table 1. Algorithm Type and Key Size

	Root CA	Sub-CA	End-entity Cert
Digest Algorithm	SHA-384	SHA-384	SHA-384
Minimum RSA modulus size (bits)	4096	4096	2048
Elliptic Curve Cryptography	NIST P-521	NIST P-521	NIST P-256

10.1.6 Public Key Parameters Generation and Quality Checking

Elliptic Curve Cryptography (ECC) public key parameters SHALL be selected from the set specified in Section 11.1.

10.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

10.1.7.1 KeyUsage Extension settings for C4MI CA Certificates

Table 2 shows the specific keyUsage extension settings for C4MI CA certificates and specifies that all CA certificates (i.e., Root CAs, Sub-CAs):

- SHALL include a keyUsage extension
- SHALL set the criticality of the keyUsage extension to TRUE
- SHALL assert the keyCertSign bit and the cRLSign bit in the key usage extension

Table 2. keyUsage Extension for all CA certificates

Field	Format	Criticality	Value	Comment
keyUsage	BIT STRING	TRUE	{ id-ce 15 }	Included in all CA certificates
digitalSignature	(0)		1	Set
nonRepudiation	(1)		0	Not Set
keyEncipherment	(2)		0	Not Set
dataEncipherment	(3)		0	Not Set
keyAgreement	(4)		0	Not Set
keyCertSign	(5)		1	Set
cRLSign	(6)		1	Set
encipherOnly	(7)		0	Not Set
decipherOnly	(8)		0	Not Set

10.1.7.2 KeyUsage Extension settings for C4MI Subscriber End-Entity Certificates

Table 3 shows the specific keyUsage extension settings for C4MI Subscriber end-entity certificates that contain RSA or ECC public keys and specifies that all Subscriber device certificates:

- SHALL include a keyUsage extension
- SHALL set the criticality of the keyUsage extension to TRUE
- SHALL assert the digitalSignature bit
- SHALL assert the keyEncipherment bit for RSA public keys
- SHALL assert the keyAgreement bit for ECC public keys

Table 3. keyUsage Extension for Subscriber Certificates with RSA Public Keys

Field	Format	Criticality	Value	Comment
keyUsage	BIT STRING	TRUE	{ id-ce 15 }	Included in all Subscriber certificates
digitalSignature	(0)		0 or 1	Set per profile in [C4MI-TD-TPPCH]
nonRepudiation	(1)		0 or 1	Set per profile in [C4MI-TD-TPPCH]
keyEncipherment	(2)		0 or 1	Set per profile in [C4MI-TD-TPPCH]
dataEncipherment	(3)		0 or 1	Set per profile in [C4MI-TD-TPPCH]
keyAgreement	(4)		0 or 1	Set per profile in [C4MI-TD-TPPCH]
keyCertSign	(5)		0	Not Set
cRLSign	(6)		0	Not Set
encipherOnly	(7)		0	Not Set
decipherOnly	(8)		0	Not Set

10.2 Private Key Protection and Cryptographic Module Engineering Controls

10.2.1 Cryptographic Module Standards and Controls

CA Private keys within the C4MI PKI SHALL be protected using [FIPS-140-2] Level 3 systems. Private key holders SHALL take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with this CP and contractual obligations specified in the appropriate C4MI Agreement.

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS-140-2].

- Root CAs SHALL perform all CA cryptographic operations on cryptographic modules rated at a minimum of [FIPS-140-2] level 3 or higher.
- Sub-CAs SHALL use a [FIPS-140-2] Level 3 or higher validated hardware cryptographic module.
- Subscribers SHALL support the requirements defined in relevant C4MI specifications for securing end-entity certificate keys.

10.2.2 Private Key (m out of n) Multi-Person Control

Multi-person control is enforced to protect the activation data needed to activate CA private keys so that a single person SHALL NOT be permitted to activate or access any cryptographic module that contains the complete CA private signing key.

CA signature keys SHOULD be backed up only under multi-person control. Access to CA signing keys backed up for disaster recovery SHALL be under multi-person control. The names of the parties used for multi-person control SHALL be maintained on a list that SHALL be made available for inspection during compliance audits.

CAs MAY use "Secret Sharing" to split the private key or activation data needed to operate the private key into separate parts called "Secret Shares" held by individuals called "Shareholders." Some threshold number of Secret Shares (m) out of the total number of Secret Shares (n) SHALL be required to operate the private key. The minimum threshold number of shares (m) needed to sign a CA certificate SHALL be 3. The total number of shares (n) used SHALL be greater than the minimum threshold number of shares (m).

CAs MAY also use Secret Sharing to protect the activation data needed to activate private keys located at their respective disaster recovery sites. The minimum threshold number of shares (m) needed to sign a CA certificate at a disaster recovery site SHALL be 3. The total number of shares (n) used SHALL be greater than the minimum threshold number of shares (m).

10.2.3 Private Key Escrow

CA private keys and Subscriber private keys SHALL NOT be escrowed.

10.2.4 Private Key Backup

CAs SHALL back up their private keys, under the same multi-person control as the original signature key. The backups allow the CA to be able to recover from disasters and equipment malfunction. At least one copy of the private signature key SHALL be stored off-site. Private keys that are backed up SHALL be protected from unauthorized modification or disclosure through physical and cryptographic means and with an audit trail. Backups, including all activation data needed to activate the cryptographic token containing the private key, SHALL be protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within the CA site, such as at a disaster recovery site or at another secure off-site facility, such as a bank safe. All copies of the CA private signature key SHALL be accounted for and protected in the same manner as the original.

End-entity private keys MAY be backed up or copied, but SHALL be held under the control of the Subscriber or other authorized administrator. Backed up device private keys SHALL NOT be stored in plaintext form and storage SHALL ensure security controls consistent with the C4MI security specifications the device is compliant with. Subscribers MAY have the option of using enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys.

10.2.5 Private Key Archival

CA private keys and Subscriber private keys SHALL NOT be archived. Upon expiration of a CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CP. These CA key pairs SHALL NOT be used for any signing events after the expiration date of the corresponding CA Certificate, unless the CA Certificate has been renewed in terms of this CP.

10.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys MAY be exported from the cryptographic module only to perform CA key backup procedures as described in Section 10.2.4. At no time shall the CA private key exist in plaintext outside the cryptographic module.

All other keys SHALL be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key SHALL be encrypted during transport; private keys SHALL never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport SHALL be protected from disclosure.

Entry of a private key into a cryptographic module SHALL use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

Processing Centers generating CA or RA private keys on one hardware cryptographic module and transferring them into another shall securely transfer such private keys into the second cryptographic module to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens.

CAs pre-generating private keys and transferring them into a hardware token, for example transferring generated end-user Subscriber private keys into a smart card, SHALL securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

10.2.7 Private Key Storage on Cryptographic Module

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

10.2.8 Method of Activating Private Key

All CAs SHALL protect the activation data for their private keys against loss, theft, modification, disclosure, or unauthorized use.

CA administrators SHALL be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs, or biometrics. Entry of activation data SHALL be protected from disclosure (e.g., the data should not be displayed while it is entered).

For end-entity certificates, the end-entity MAY be configured to activate its private key, provided that appropriate physical and logical access controls are implemented for the end-entity. The strength of the security controls SHALL be commensurate with the level of threat in the end-entity's environment, and SHALL protect the end-entity's hardware, software, private keys, and its activation data from compromise.

CA Administrator Activation

Method of activating the CA system by a CA Administrator SHALL require:

- the use of a smart card, biometric access end-entity, password in accordance with Section 10.4.1, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, an operating system logon or screen saver password, or a network logon password; and,
- commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

Offline Root CAs Private Key

Once the CA system has been activated, a threshold number of Shareholders SHALL be required to supply their activation data in order to activate an offline CA's private key, as defined in Section 10.2.2. Once the private key is activated, it SHALL be active until termination of the session.

Online Subordinate CAs Private Keys

An online CA's private key SHALL be activated by a threshold number of Shareholders, as defined in Section 10.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline.

Subscriber Private Keys

The C4MI standards for protecting activation data for Subscribers' private keys SHALL be in accordance with the specific obligations appearing in the applicable agreement executed between C4MI and the Subscriber.

10.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated SHALL NOT be available to unauthorized access. After use, the cryptographic module SHALL be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity. CA cryptographic modules SHALL be stored securely when not in use.

When an online CA is taken offline, the CA SHALL remove the token containing the private key from the reader in order to deactivate it, or take similar action based upon the type of hardware used to store the private key.

With respect to the private keys of offline CAs, after the completion of a Key Generation Ceremony, in which such private keys are used for private key operations, the CA SHALL remove the token containing the private keys from the reader in order to deactivate them, or take similar action based upon the type of hardware used to store the private key. Once removed from the reader, tokens SHALL be securely stored.

When an online CA is taken offline, the CA SHALL remove the token containing such CA's private key from the reader in order to deactivate it.

When deactivated, private keys SHALL be kept in encrypted form only.

10.2.10 Method of Destroying Private Key

Private keys SHALL be destroyed in a way that prevents their theft, disclosure, or unauthorized use.

Upon termination of the operations of a CA, individuals in trusted roles SHALL decommission the CA private signature keys by deleting it using functionality of the token containing such CA's private key so as to prevent its recovery following deletion, or the loss, theft, modification, disclosure, or unauthorized use of such a private key. CA private keys SHALL be destroyed in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key. CA private key destruction SHOULD be verified by two or more trusted personnel and the process of verification noted in the CPS.

For Root CAs, C4MI security personnel SHALL witness this process.

Subscribers MAY destroy their private keys when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of hardware is not required.

10.2.11 Cryptographic Module Rating

See Section 10.2.1.

10.3 Other Aspects of Key Pair Management

10.3.1 Public Key Archival

CAs MAY archive their public keys in accordance with Section 9.5.1.

10.3.2 Certificate Operational Periods and Key Pair Usage Periods

The certificate validity period (i.e., certificate operational period and key pair usage period) SHALL be set to the time limits set forth as follows:

- Root CA certificates can have a validity period of up to 30 years
- Sub-CA certificates can have a validity period of up to 20 years
- End-entity certificates can have a validity period of up to 2 years, and may have a larger validity period not exceeding 10 years in some circumstances when explicitly requested.

Validity periods SHALL be nested such that the validity periods of issued certificates will be contained within the validity period of the issuing CA.

As necessary to ensure the continuity and security of the C4MI PKI, C4MI SHALL commission new CAs.

C4MI PKI Participants SHALL cease all use of their key pairs after their usage periods have expired.

10.4 Activation data

10.4.1 Activation Data Generation and Installation

CAs SHALL generate and install activation data for their private keys and SHALL use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, disclosure, or unauthorized use of such activation data.

To the extent passwords are used as activation data, CAs activation participants SHALL generate passwords that cannot easily be guessed or cracked by dictionary attacks. Participants may not need to generate activation data, for example if they use biometric access devices.

10.4.2 Activation Data Protection

CAs SHALL protect the activation data for their private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

CAs SHALL use multi-party control in accordance with Section 10.2.2. CAs SHALL provide the procedures and means to enable Shareholders to take the precautions necessary to prevent the loss, theft, modification, disclosure, or unauthorized use of the Secret Shares that they possess. Shareholders SHALL not:

- Copy, disclose, or make the Secret Share available to a third party, or make any unauthorized use of it whatsoever; or
- Disclose their or any other person's status as a Shareholder to any third party.

The Secret Shares and any information disclosed to the Shareholder in connection with their duties as a Shareholder SHALL constitute Confidential/Private Information.

CAs SHALL include in their disaster recovery plans provisions for making Secret Shares available at a disaster recovery site after a disaster (Note, the important aspect of disaster recovery vis-à-vis shares is that a process exists for making the necessary number of shares available, even if the requisite shareholders are not available.). CAs SHALL maintain an audit trail of Secret Shares, and Shareholders SHALL participate in the maintenance of an audit trail.

10.4.3 Other Aspects of Activation Data

Activation Data Transmission

To the extent activation data for their private keys are transmitted, Activation Data Participants SHALL protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent desktop computer or network logon user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network SHALL be protected against access by unauthorized users.

Activation Data Destruction

Activation data for CA private keys SHALL be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys

protected by such activation data. After the record retention periods in Section 9.5.2 lapses, CAs SHALL decommission activation data by overwriting and/or physical destruction.

10.5 Computer security controls

10.5.1 Specific Computer Security Technical Requirements

CAs SHALL ensure that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 9.4.1. In addition, CAs SHALL limit access to production servers to those individuals with a valid business reason for access. General application users SHALL NOT have accounts on the production servers.

CAs SHALL have production networks logically separated from other components. This separation prevents network access except through defined application processes. CAs SHALL use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

To the extent that passwords are used, CAs SHALL require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and require passwords be changed on a periodic basis and whenever necessary. Direct access to a CA's database maintaining the CA's repository SHALL be limited to Trusted Persons having a valid business reason for such access.

Computer security controls SHALL be required to ensure CA operations are performed as specified in this policy. The following computer security functions MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Require authenticated logins
- Provide discretionary access control
- Provide a security audit capability
- Enforce access control for CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test security-related CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanism for keys and the CA system
- Enforce domain integrity boundaries for security-critical processes

For other CAs operating under this policy, the computer security functions listed below SHALL be required. These functions MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts SHALL include the following functionality:

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Generate and archive audit records for all transactions; (see Section 9.4)
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure

For certificate status servers operating under this policy, the computer security functions listed below SHALL be required:

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

For remote workstations used to administer the CAs, the computer security functions listed below SHALL be required:

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Generate and archive audit records for all transactions; (see Section 9.4)
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure

All communications between any PKI trusted role and the CA SHALL be authenticated and protected from modification.

10.5.2 Computer Security Rating

No stipulation.

10.6 Life Cycle Technical Controls

10.6.1 System Development Controls

The system development controls for the CA are as follows:

- The CA SHALL use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured to operate the CA SHALL be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device).
- Before issuing certificates, the CA SHALL validate that the Subscriber is not listed in [NIST-VD].
- Hardware and software developed specifically for the CA SHALL be developed in a controlled environment, and the development process SHALL be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- The CA hardware and software SHALL be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation. Where the CA operation supports multiple CAs, the hardware platform MAY support multiple CAs.
- Proper care SHALL be taken to prevent malicious software from being loaded onto the CA equipment. All applications required to perform the operation of the CA SHALL be obtained from documented sources.
- Hardware and software updates SHALL be purchased or developed in the same manner as the corresponding original equipment, and SHALL be installed by trusted and trained personnel in a defined manner.

10.6.2 Security Management Controls

The configuration of the CA system, in addition to any modifications and upgrades, SHALL be documented and controlled. There SHALL be a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, SHALL be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

10.6.3 Life Cycle Security Controls

No Stipulation.

10.7 Network Security Controls

A network guard, firewall, or filtering router SHALL protect network access to CA equipment. The network guard, firewall, or filtering router SHALL limit services allowed to and from the CA equipment to those required to perform CA functions.

Protection of CA equipment SHALL be provided against known network attacks. All unused network ports and services SHALL be turned off. Any network software present on the CA equipment SHALL be necessary to the functioning of the CA application.

Any boundary control devices used to protect the network on which PKI equipment is hosted SHALL deny all but the necessary services to the PKI equipment.

Repositories, certificate status servers, and remote workstations used to administer the CAs SHALL employ appropriate network security controls. Networking equipment SHALL turn off unused network ports and services. Any network software present SHALL be necessary to the functioning of the equipment.

The CA SHALL establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

10.8 Time-Stamping

Certificates, CRLs, and other revocation database entries SHALL contain time and date information. Such time information need not be cryptographic-based. Asserted times SHALL be accurate to within three minutes. Electronic or manual procedures MAY be used to maintain system time. Clock adjustments are auditable events (see Section 9.4.1).

11 Certificate, CRL, and OCSP Profiles

11.1 Certificate Profile

C4MI PKI Certificate profile details are defined in [C4MI-TD-TPPCH].

11.2 CRL Profile

CRLs SHALL conform to [IETF-RFC5280] and contain the basic fields and contents specified in the table below:

Table 4. CRL Profile Basic Fields

Field	Referenced Standard	Section	Requirement or Recommendation
version	[IETF-RFC5280]	5.1.2.1	See Section 11.3.1
signature	[IETF-RFC5280]	5.1.2.2	Algorithm used to sign the CRL.
issuer	[IETF-RFC5280]	5.1.2.3	Entity that has signed and issued the CRL.
thisUpdate	[IETF-RFC5280]	5.1.2.4	Indicates the issue date of the CRL. CRLs are effective upon issuance.
nextUpdate	[IETF-RFC5280]	5.1.2.5	Indicates the date by which the next CRL will be issued.
revokedCertificates	[IETF-RFC5280]	5.1.2.6	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.
authoritKeyIdentifier	[IETF-RFC5280]	5.2.1	Follows the guidance in RFC 5280. Criticality is FALSE.
cRLNumber	[IETF-RFC5280]	5.2.3	A monotonically increasing sequence number for a given CRL scope and issuer. Criticality is FALSE.
signatureAlgorithm	[IETF-RFC5280]	5.1.1.2	Follows the guidance in [IETF-RFC5280].
signatureValue	[IETF-RFC5280]	5.1.1.3	Follows the guidance in [IETF-RFC5280].

11.2.1 Version Number(s)

The CAs SHALL support the issuance of X.509 Version two (2) CRLs. The CRL version number SHALL be set to the integer value of "1" for Version 2 [IETF-RFC5280], section 5.1.2.1.

11.2.2 CRL and CRL entry extensions

Critical CRL extensions SHALL NOT be used.

11.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. OCSP Responses SHALL conform to [IETF-RFC5019] and either be:

- Signed by the CA that issued the Certificates whose revocation status is being checked, or
- Signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. Such OCSP Responder signing Certificate SHALL contain the extension id-pkix-ocsp-nocheck as defined by [IETF-RFC2560].

11.3.1 Version Number(s)

OCSP responses SHALL support use of OCSP version 1 as defined by [IETF-RFC2560] and [IETF-RFC5019].

11.3.2 OCSP Extensions

Critical OCSP extensions SHALL NOT be used.

12 Compliance Audit and Other Assessments

12.1 Frequency or Circumstances of Assessment

CAs operating under this policy SHALL be subject to a periodic compliance audit at least once per year. Compliance Audits are conducted at the sole expense of the audited entity. C4MI MAY require a periodic compliance audit report of CAs operating under this policy as stated in Section 12.4.

12.2 Identity/Qualifications of Assessor

The CA MAY select an auditor, subject to the qualifications described herein. The auditor SHALL demonstrate competence in the field of compliance audits, and SHALL be thoroughly familiar with the CA's CPS and this CP. The auditor SHALL be a certified information system auditor (CISA), or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

Audits performed by an independent third party audit firm SHALL be performed by a certified public accounting firm with demonstrated expertise in computer security or by accredited computer security professionals employed by a competent security consultancy. Such firm SHALL also have demonstrated expertise in the performance of IT security and PKI compliance audits.

The qualified audit firm SHALL be bound by law, government regulation, or professional code of ethics and SHALL maintain Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

12.3 Assessor's Relationship to Assessed Entity

The compliance auditor SHALL either be a private firm that is independent from the CA being audited or sufficiently (organizationally) separated from those entities to provide an unbiased, independent evaluation. Compliance auditors SHALL not have a conflict of interest that hinders their ability to perform auditing services. To ensure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or CPS. The C4MI SHALL determine whether a compliance auditor meets this requirement.

12.4 Topics Covered by Assessment

CA's SHALL perform an annual compliance audit for WebTrust Principles and Criteria for Certification Authorities 2.1 [WebTrust-CA] which includes: a Report of Policies and Procedures in Operation and Test of Operational Effectiveness. The purpose of the annual compliance audit shall be to verify that a CA complies with all the mandatory requirements of the current versions of this CP and the CA's CPS.

All aspects of the CA operation SHALL be subject to the compliance audit and SHOULD address the items listed below. A WebTrust for Certification Authorities or equivalent will satisfy this requirement.

- Identify foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

In addition to compliance audits, if the C4MI has a reasonable belief that a CA is not operating in conformance with this CP, the C4MI SHALL be entitled, to perform other reviews and investigations, which include, but are not limited to:

- A "Security and Practices Review," which consists of a review of a CA's secure facility, security documentation, CPS, and any other appropriate material to ensure that the CA meets the CP.
- An "Exigent Audit/Investigation" on CAs, including, for example, in the event the C4MI has reason to believe that the audited entity has failed to meet the CP Standards, has experienced an incident or Compromise, or has acted or failed to act, such that the audited entity's failure, the incident or Compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the C4MI PKI.
- A "Supplemental Risk Management Reviews" on CAs following incomplete or exceptional findings in a Compliance Audit.

The C4MI SHALL be entitled to delegate the performance of these audits, reviews, and investigations to (a) the Superior Entity of the entity being audited, reviewed, or investigated or (b) a third-party audit firm. Entities that are subject to an audit, review, or investigation SHALL provide cooperation with C4MI and the personnel performing the audit, review, or investigation.

12.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions SHALL be performed:

- The compliance auditor will note the discrepancy;
- The compliance auditor will notify the parties identified in Section 12.6 of the discrepancy; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the parties identified in Section 12.6.

In the event the audited entity fails to develop a corrective action plan to be implemented in a timely manner, or if the report reveals exceptions or deficiencies that the C4MI reasonably believes poses an immediate threat to the security or integrity of the C4MI PKI, then the C4MI SHALL:

- determine whether revocation and compromise reporting are necessary
- be entitled to suspend services to the audited entity
- if necessary, terminate such services subject to this CP and the terms of the audited entity's contract

12.6 Communication of Results

Following any Compliance Audit, the audited entity SHALL provide the C4MI with the Audit Compliance Report and identification of corrective measures within 30 days of completion. A special compliance audit MAY be required to confirm the implementation and effectiveness of the remedy.

13 Other Business and Legal Matters

13.1 Fees

13.1.1 Certificate Issuance or Renewal Fees

Subscribers MAY be charged a fee for the issuance, management, and renewal of certificates.

13.1.2 Certificate Access Fees

CAs SHALL not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

13.1.3 Revocation or Status Information Access Fees

CAs SHALL not charge a fee as a condition of making CRLs available in a repository or otherwise available to Relying Parties.

13.1.4 Fees for Other Services

No stipulation.

13.1.5 Refund Policy

Refund policies SHOULD be stipulated in the appropriate agreement (e.g., Subscriber Agreement).

13.2 Financial Responsibility

13.2.1 Insurance Coverage

C4MI PKI Participants SHOULD maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

13.2.2 Other Assets

CAs SHALL have sufficient financial resources to maintain their operations and perform their duties, and they SHALL be reasonably able to bear the risk of liability to Subscribers and Relying Parties.

13.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

13.3 Confidentiality of business information

13.3.1 Scope of Confidential Information

The following Subscriber information SHALL be kept confidential and private:

- Certificate Application records

- CA application status, whether approved or disapproved
- Transactional records (both full records and the audit trail of transactions)
- Audit trail records
- Audit reports
- Contingency planning and disaster recovery plans
- Security measures controlling the operations of CA hardware and software

13.3.2 Information not Within the Scope of Confidential Information

C4MI PKI Participants acknowledge that Certificates, Certificate revocation and other status information, C4MI repositories, and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 13.3.1 SHALL be considered neither confidential nor private.

13.3.3 Responsibility to Protect Confidential Information

C4MI PKI Participants receiving private information SHALL secure it from compromise and disclosure to third parties.

13.4 Privacy of Personal Information

13.4.1 Privacy Plan

CAs SHALL have a Privacy Plan to protect personally identifying information from unauthorized disclosure.

13.4.2 Information Treated as Private

CAs acquiring services under this policy SHALL protect all Subscriber personally identifying information from unauthorized disclosure. Records of individual transactions MAY be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this policy SHALL not be released except as required by law.

13.4.3 Information not Deemed Private

Information included in certificates is deemed pubic information and is not subject to protections outlined in Section 13.4.

13.4.4 Responsibility to Protect Private Information

Sensitive information SHALL be stored securely, and may be released only in accordance with other stipulations in Section 13.4.

13.4.5 Notice and Consent to Use Private Information

CAs are not required to provide any notice or obtain the consent of the Subscriber in order to release private information in accordance with other stipulations in Section 13.4.

13.4.6 Disclosure Pursuant to Judicial or Administrative Process

The C4MI or C4MI CAs SHALL NOT disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

13.4.7 Other Information Disclosure Circumstances

No stipulations.

13.5 Intellectual Property Rights

The C4MI retains all Intellectual Property Rights in and to this CP.

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue.

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

Private keys corresponding to Certificates of CAs and Subscribers are the property of the CAs and Subscribers that are the respective Subjects of these Certificates. Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares.

Without limiting the generality of the foregoing, C4MI's root public keys and Certificates containing them, including all CA and Subscriber public keys and certificates containing them, are the property of the C4MI. The C4MI licenses software and hardware manufacturers to reproduce such public key Certificates to place copies in C4MI compliant hardware devices or software.

13.6 Representations and Warranties

The C4MI SHALL:

- Approve the CPS for each CA that issues certificates under this policy
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSs
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP
- Revise this CP to maintain the level of assurance and operational practicality
- Publicly distribute this CP
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs

13.6.1 CA Representations and Warranties

CAs operating under this CP SHALL warrant the following:

- The CA procedures are implemented in accordance with this CP
- The CA will provide their CPS to the C4MI, as well as any subsequent changes, for conformance assessment
- The CA operations are maintained in conformance to the stipulations of the approved CPS
- Any certificate issued is in accordance with the stipulations of this CP
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application
- Their Certificates meet all material requirements of this CP and the applicable CPS
- The revocation of certificates in accordance with the stipulations in this CP
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects

Subscriber Agreements MAY include additional representations and warranties.

13.6.2 RA Representations and Warranties

RAs that perform registration functions under this CP SHALL warrant that:

- The RA complies with the stipulations of this CP
- The RA complies with and maintains its operations in conformance to the stipulations of the approved CPS
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application
- Their Certificates meet all material requirements of this CP and the applicable CPS
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects

Subscriber Agreements MAY include additional representations and warranties.

13.6.3 Subscriber representations and warranties

Subscribers SHALL sign an agreement containing the requirements the Subscriber shall meet, including protection of their private keys and use of the certificates before being issued the certificates. In addition, Subscribers SHALL warrant that:

- The Subscriber will abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.
- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber, and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created
- Subscriber's private keys are protected from unauthorized use or disclosure
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true
- All information supplied by the Subscriber and contained in the Certificate is true
- The Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CP
- The Subscriber will promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s)
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise

Subscriber Agreements MAY include additional representations and warranties.

13.6.4 Relying Party Representations and Warranties

This CP does not specify a comprehensive set of steps a Relying Party should take to determine whether to rely upon a certificate. The Relying Party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the Relying Party may wish to employ in its determination. Relying Parties acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they SHALL bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP.

13.6.5 Representations and Warranties of Other Participants

No stipulations.

13.7 Disclaimers of warranties

To the extent permitted by applicable law, Subscriber Agreements SHALL disclaim the C4MI's and the applicable Affiliate's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

13.8 Limitations of liability

The liability (and/or limitation thereof) of Subscribers SHALL be as set forth in the applicable Subscriber Agreements.

13.9 Indemnities

To the extent permitted by applicable law, Subscribers are required to indemnify CAs for:

- Falsehood or misrepresentation of fact by the Subscriber on its Certificate Application
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party
- The Subscriber's failure to take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key(s)
- The Subscriber's use of a name (including one that infringes upon the Intellectual Property Rights of a third party)

13.10 Term and termination

13.10.1 Term

The CP becomes effective when approved by the C4MI. Amendments to this CP become effective upon publication. This CP has no specified term.

13.10.2 Termination

This CP SHALL remain in force until it is replaced by a new version. Termination of this CP is at the discretion of C4MI.

13.10.3 Effect of termination and survival

Upon termination of this CP, C4MI PKI Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

13.11 Individual notices and communications with participants

Unless otherwise specified by agreement between the parties, C4MI participants SHALL use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

13.12 Amendments

13.12.1 Procedure for Amendment

The C4MI SHALL review this CP at least once every year. Corrections, updates, or changes to this CP SHALL be made available as per Section 13.12.2. Suggested changes to this CP SHALL be communicated to the contact in Section 5.4.2; such communication SHALL include a description of the change, a change justification, and contact information for the person requesting the change.

13.12.2 Notification Mechanism and Period

C4MI reserves the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The C4MI's decision to designate amendments as material or non-material SHALL be within the C4MI's sole discretion.

Change notices to this CP SHALL be distributed electronically to C4MI PKI Participants and observers in accordance with the C4MI document change procedures.

13.12.3 Circumstances Under Which OID Must be Changed

Object Identifiers (OIDs) will be changed if C4MI determines that a change in the CP reduces the level of assurance provided. If C4MI determines that a change is necessary in the OID corresponding to a Certificate policy, the amendment SHALL contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

13.13 Dispute Resolution Provisions

The C4MI SHALL facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

13.14 Governing Law

Subject to any limits appearing in applicable law, the laws of the State of Tennessee, U.S.A., SHALL govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Tennessee, USA. This choice of law is made to ensure uniform procedures and interpretation for all C4MI Participants, no matter where they are located.

This governing law provision applies only to this CP. Agreements incorporating the CP by reference MAY have their own governing law provisions, provided that this CP governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

13.15 Compliance with Applicable Law

This CP is subject to applicable national, state, local, and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. All CAs operating under this policy are required to comply with applicable law.

13.16 Miscellaneous provisions

13.16.1 Entire Agreement

No stipulation

13.16.2 Assignment

No stipulation

13.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in Section 13.12.

In the event that a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.

13.16.4 Enforcement (Attorneys' fees and waiver of rights)

No stipulation

13.16.5 Force Majeure

To the extent permitted by applicable law, the C4MI PKI agreement (e.g., Digital Certificate Subscriber Agreements) shall include a force majeure clause protecting C4MI and the applicable Affiliate.

13.17 Other Provisions

No stipulation.

Acknowledgements

The Center and its member companies would like to extend a heartfelt thanks to all those who participated in the development of this document.

Stuart Hoggan authored the original draft of this document, with edits by **Steve Goeringer**.

This version contains revisions made by **Sumanth Channabasappa, Bowen Shaner,** and **David Fann.** It also contains input and incorporates comments from **Spencer Crosswy, Chris Riha**, **Shawn Moss, Steve Goeringer**, **Henry Lam, Debs Debs-Faouzi, Abul Salek** and **John Cernazanu.**

Special thanks to the following who contributed via a variety of discussions, reviews and input: **Eldon Metz**, **Ken Fuchs**, and **Kai Hassing**.

For the D02 version of this document, additional comments and suggestions were made by **Jacob Chadwell, Spencer Crosswy, Bowen Shaner , David Fann, Chris Riha, and Trevor Pavey. Christie Poland, Joan Branham, Katy Hoyer** and **Jessie Hanson** have served as editors for the D01 version of this document, while **Katy Hoyer** served as the editor for the D02 version.

Chris Riha is the C4MI Lead for this document. This document was primarily discussed and reviewed within The Center's Security Working Group, with additional input from the Architecture & Requirements and Connectivity Working Groups. The part-time and full-time working group participants, additional offline reviewers, and their affiliations are listed below:

Working Group Participants	Company Affiliation
Abul Salek	Sectigo Ltd.
Aishwarya Muralidharan	vTitan
Alex Poiry	Cerner
Ali Nakoulima	Cerner
Andrew Meshkov	86Borders
Brian Long	Masimo
Brian Scriber	CableLabs
Bruce Friedman	GE Healthcare
Corey Spears	Infor
Darshak Thakore	CableLabs

Working Group Participants	Company Affiliation
David Hatfield	Becton Dickenson
David Niewolny	RTI
Debs Debs-Faouz	Sectigo Ltd.
Eldon Metz	InnoVision Medical
George Cragg	Draeger
Guy Johnson	Zoll
Henry Lam	Sectigo Ltd.
Ian Sherlock	Texas Instruments
James Surine	Smiths-Medical
Jason Mortensen	Bernoulli Health
Jay White	Laird
Jeffrey Brown	GE Healthcare
JF Lancelot	Airstrip
John Barr	CableLabs
John Cernazanu	Kyrio Medical
John Hinke	InnoVision Medical
John Williams	FortyAU
Kai Hassing	Philips Healthcare
Ken Fuchs	Draeger
Logan Buchanan	FortyAU
M Prasannahvenkat	vTitan
Massimo Pala	CableLabs

Working Group Participants	Company Affiliation
Mike Krajnak	GE Healthcare
Milan Buncick	Aegis
Neil Puthuff	RTI
Neil Seidl	GE Healthcare
Ponlakshmi G	vTitan
Scott Eaton	Mindray
Shawn Moss	Kyrio Medical
Stefan Karl	Philips Healthcare
Travis West	Bridge Connector

- Sumanth Channabasappa (Chief Architect), Steve Goeringer (Security Architect), Chris Riha (Working Groups Lead), Paul Schluter, Bowen Shaner, Jacob Chadwell, David Fann, Spencer Crosswy, Dr. Richard Tayrien, Trevor Pavey; and, Ed Miller (CTO) -- The Center